

Network Camera

User's Guide

Software Version 1.0

Before operating the unit, please read this manual thoroughly and retain it for future reference.

SNC-CH140

SNC-DH140

IPELA

Table of Contents

Overview

Features	4
How to Use This User's Guide	5
System Requirements	5

Preparation

Assigning the IP Address to the Camera	6
Assigning an IP address using SNC toolbox	6
When using Windows XP Service Pack 2 or later	8
When using Windows Vista	10
Accessing the Camera Using the Web Browser	13
Basic Configuration by the Administrator	15

Operating the Camera

Administrator and User	16
Logging in to System	17
Logging in as a user	17
About Viewers	17
Configuration of Main Viewer	18
Main menu	18
Control panel section	18
Monitor image	19
Plug-in free viewer	19
Using the Trigger Button	21
Sending a monitor image via e-mail	21
Sending a monitor image to an FTP server	21
Recording a camera image as a still image	21
Controlling Alarm out 1, 2	21
Controlling the Day/Night function	21
Playing an audio file stored in the camera	21
Switching TCP/UDP Transmission Mode	22
Using the System Utility	23
SNC viewer	23
SNC Desktop viewer	24

Administrating the Camera

Basic Operations of the Administrator

Menu	26
How to setup the Administrator menu	26
Configuration of the Administrator menu	27

Configuring the System — System Menu

System Tab	28
Date & time Tab	28
Superimpose Tab	29
Installation Tab	29
Initialize Tab	30
System log Tab	31
Access log Tab	31

Setting the Camera Image and Audio

— Camera Menu

Common Tab	31
Focus tab — Adjusting the Focus (SNC-CH140 only)	32
Focus/Zoom tab — Adjusting the focus/zoom (SNC-DH140 only)	32
Picture Tab	32
Privacy masking tab	34
Day/Night Tab	35
Video codec Tab	36
Streaming Tab	37

Configuring the Network — Network Menu

Network Tab	38
Wireless Tab — Setting of wireless connection (SNC-CH140 only)	39
QoS Tab	42
Dynamic IP address notification Tab — Notifying the IP Address	44

Setting the SSL function — SSL Menu

SSL tab	46
CA certificate tab — Adding the CA certificate for client authentication	48
How to install the CA certificate	49
To remove an installed CA certificate	50

Using the 802.1X Authentication Function

— 802.1X Menu

System configuration of 802.1X network	51
Common Tab — Basic setting of 802.1X authentication function	51
Client certificate Tab	52
CA certificate Tab	53
Setting the 802.1X authentication function — Example of Windows Server 2003	54

Setting the User — User Menu

Setting the Security — Security Menu

Sending an Image via E-mail — e-Mail (SMTP)	
Menu	58
Common Tab — Setting the e-Mail (SMTP)	
Function	58
Alarm sending Tab — Setting the	
e-mail sending mode when detecting the	
alarm	60
Periodical sending Tab — Setting the periodical	
e-mail sending mode	60
Sending Images to FTP Server	
— FTP client Menu	61
Common Tab — Setting the FTP client	
function	61
Alarm sending Tab — Setting the FTP client	
action when detecting the alarm	62
Periodical sending Tab — Setting the periodical	
FTP client activity	63
Recording Images in Memory	
— Image memory Menu	64
Common Tab — Setting the image memory	
function	64
Alarm recording Tab — Setting the Image	
memory function when detecting the	
alarm	66
Periodical recording Tab — Setting the periodical	
recording mode	66
Folder structure of image memory	67
Downloading Images from the Camera	
— FTP server Menu	68
Setting the Alarm Output	
— Alarm output Menu	68
Alarm out 1, 2 Tab	68
Outputting Audio Linked to Alarm Detection	
— Voice alert Menu	69
Voice alert 1, 2, 3 Tab	69
Setting the Operations from the Viewer	
— Trigger Menu	70
Setting the Schedule — Schedule Menu	72
Setting the Alarm Buffer	
— Alarm buffer Menu	72
Setting the Sensor input/Camera tampering	
detection/Motion detection	
— Event detection Menu	73
Sensor input tab — Set the sensor input	73
Camera tampering detection tab	
— Set the camera tampering detection	73
Motion detection tab — Set the motion/VMF	
detection	73
What are VMF functions	73
Setting items for motion detection	74
VMF settings	76
Configuring the Viewer	
— Viewer Menu	79
Layout tab	79
HTML output tab	81
Others	
Using the SNC toolbox	82
Starting SNC toolbox	82
How to use SNC toolbox	82
Registering in My device	84
Changing the Device list display method	85
Setting SNC toolbox options	86
Using Privacy Masking	
— Masking a Camera Image	87
Using the Custom Homepage	
— Setting the customized homepage	88
Using the Firmware Upgrade	88
Using the Schedule Task	89
Configuring the device setting	91
Device restart and initialization	93
Using the SNC audio upload tool — Transmitting	
Audio to Camera	93
Installing the SNC audio upload tool	93
Connecting the Camera to the Computer	94
Using the SNC audio upload tool	94
Using the SNC video player — Playing a Video/	
Audio File Recorded with the Camera	99
Installing the SNC video player	99
Using the SNC video player	99
Assigning the IP Address to the Camera Using	
ARP Commands	100
Using the SNMP	101
1. Inquiry Commands	101
2. Setting Commands	101
Glossary	102
Index	105

Features

- High-quality HD (720P) live images from camera can be monitored at a maximum frame rate of 30 fps.
- Live images can be streamed in high-quality with maximum SXGA (1280 × 1024) image size.
- Exmor CMOS sensor enables high-quality images for streaming.
- View-DR and Visibility Enhancer enable clearer images for streaming in the high contrast environment.
- XDNR enables clearer images for streaming in the low lightness environment.
- Three video compression modes (video codecs) JPEG/MPEG4/H.264 are supported.
- Single codec mode and dual codec mode are available.
- Easy Focus enables easier focus adjustment when it is installed. (SNC-CH140, DH140)
- Easy Zoom function enables remote adjustment of view angle after installation. (SNC-DH140)
- Inserting the optional wireless card SNCA-CFW5* enables wireless transmission of camera images. (SNC-CH140)
- An optional CF memory card allows you to save images. (SNC-CH140)
- Intelligent motion detection and camera tampering detection alarm functions are provided.
- Up to 10 users can view images from one camera at the same time.
- Date/time can be superimposed on the image.
- PoE (Power over Ethernet) compliant.

* SNCA-CFW5 is not available in some countries and areas. For details, contact your authorized Sony dealer.

NOTICE TO USERS

© 2009 Sony Corporation. All rights reserved. This manual or the software described herein, in whole or in part, may not be reproduced, translated or reduced to any machine readable form without prior written approval from Sony Corporation.

SONY CORPORATION PROVIDES NO WARRANTY WITH REGARD TO THIS MANUAL, THE SOFTWARE OR OTHER INFORMATION CONTAINED HEREIN AND HEREBY EXPRESSLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE WITH REGARD TO THIS MANUAL, THE SOFTWARE OR SUCH OTHER INFORMATION. IN NO EVENT SHALL SONY CORPORATION BE LIABLE FOR ANY INCIDENTAL, CONSEQUENTIAL OR SPECIAL DAMAGES, WHETHER BASED ON TORT, CONTRACT, OR OTHERWISE, ARISING OUT OF OR IN CONNECTION WITH THIS MANUAL, THE SOFTWARE OR OTHER INFORMATION CONTAINED HEREIN OR THE USE THEREOF.

Sony Corporation reserves the right to make any modification to this manual or the information contained herein at any time without notice. The software described herein may also be governed by the terms of a separate user license agreement.

- “IPELA” and **IPELA** are trademarks of Sony Corporation.
- **HD** is trademark of Sony Corporation.
- “Exmor” and **Exmor**™ are trademarks of Sony Corporation.
- Microsoft, Windows, Internet Explorer and Microsoft DirectX are registered trademarks of Microsoft Corporation in the United States and/or other countries.
- Java is a trademark of Sun Microsystems, Inc. in the United States and other countries.
- Intel and Pentium are registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
- Adobe, Adobe Reader and Adobe Flash are trademarks of Adobe Systems Incorporated in the United States and/or other countries.
- CompactFlash and CF are trademarks of SanDisk Corporation, registered in the United States and other countries.

All other company and product names are trademarks or registered trademarks of the respective companies or their respective makers.

How to Use This User's Guide

This User's Guide explains how to operate the Network Camera from a computer.

The User's Guide is designed to be read on the computer display.

This section gives tips on making the most of the User's Guide—read it before you operate the camera.

Jumping to a related page

When you read the User's Guide on the computer display, you can click on a sentence to jump to a related page.

Software display examples

Note that the displays shown in the User's Guide are explanatory examples. Some displays may be different from the ones that appear in actual use.

The illustrations of the camera and menu display in the User's Guide show the SNC-CH140 or SNC-DH140 as an example.

Printing the User's Guide

Depending on your system, certain displays or illustrations in the User's Guide, when printed out, may differ from those that appear on your screen.

Installation Manual (printed matter)

The supplied Installation Manual describes the names and functions of parts and controls of the Network Camera, connection examples, and how to set up the camera. Be sure to read the Installation Manual before hand.

System Requirements

The following computer environment is necessary for the computer to display images and the controls of the camera.

(December 2009)

CPU

Intel Core 2 Duo, 2 GHz or higher.

Memory

1 GB or more.

OS

Microsoft Windows XP, Windows Vista (32-bit version only)

Microsoft DirectX 9.0c or higher

Web Browser

Microsoft Internet Explorer Ver 6.0 or 7.0

Display

1600 × 1200 pixels or higher.

The Preparation section explains what the administrator has to prepare for monitoring images after installation and connection of the camera.

Assigning the IP Address to the Camera

To connect the camera to a network, you need to assign a new IP address to the camera when you install it for the first time.

You can assign an IP address in two ways:

- Using SNC toolbox stored in the supplied CD-ROM (see this page)
- Using the ARP (Address Resolution Protocol) commands (see page 100)

This section explains how to assign an IP address to the camera using the SNC toolbox and how to configure the network.

Before starting, connect the camera, referring to “Connecting the Camera to a Local Network” in the supplied Installation Manual.

Consult the administrator of the network about the assigned IP address.

Notes

- SNC toolbox may not operate correctly if you use a personal firewall or antivirus software in your computer. In that case, disable the software or assign an IP address to the camera using another method. For example, see “Assigning the IP Address to the Camera Using ARP Commands” on page 100.
- If you are using Windows XP Service Pack 2 or later, or Windows Vista, disable the Windows Firewall function. Otherwise SNC toolbox will not operate correctly. For the setting, see “Configuring Windows Firewall” in “When using Windows XP Service Pack 2 or later” on page 9 or “Configuring Windows Firewall” in “When using Windows Vista” on page 11.

Assigning an IP address using SNC toolbox

- 1 Insert the CD-ROM in your CD-ROM drive. A cover page appears automatically in your Web browser. If it does not appear automatically in the Web browser, double-click the index.htm file on the CD-ROM.

When you are using Windows Vista, the “Auto play” pop-up may appear. For details, see “Installing software” in “When using Windows Vista” on page 10.

- 2 Click the **Setup** icon of **SNC toolbox**. The **File Download** dialog opens.

When you are using Windows XP Service Pack 2 or later, or Windows Vista, a message regarding the active contents may appear. For details, see “Installing software” in “When using Windows XP Service Pack 2 or later” on page 8 or “Installing software” in “When using Windows Vista” on page 10.

- 3 Click **File Open**.

Note

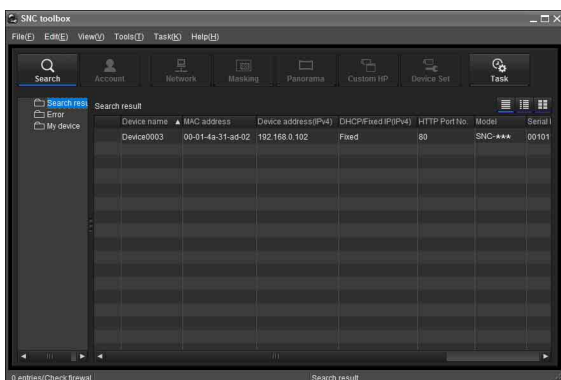
If you click “Save” on the “File Download” dialog, you will not be able to perform set up correctly. Delete the downloaded file, and click the **Setup** icon again.

- 4 Install SNC toolbox on your computer using the wizard. If the Software License Agreement is displayed, read it carefully and click **Accept** to continue with the installation.

- 5 Start SNC toolbox.

When you are using Windows Vista, the message “User Account Control – An unidentified program wants access to your computer” may appear. In this case, click **Allow**.

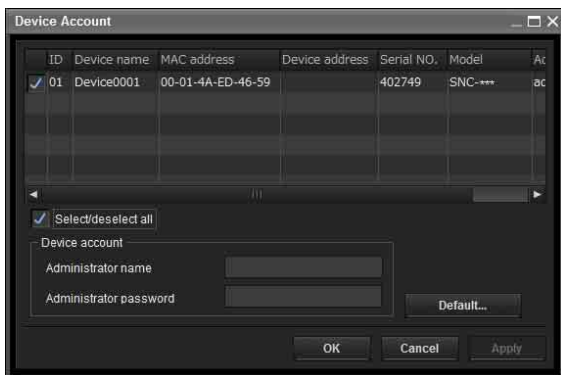
- 6 Click **Search**. SNC toolbox detects the network cameras connected to the local network and lists them.



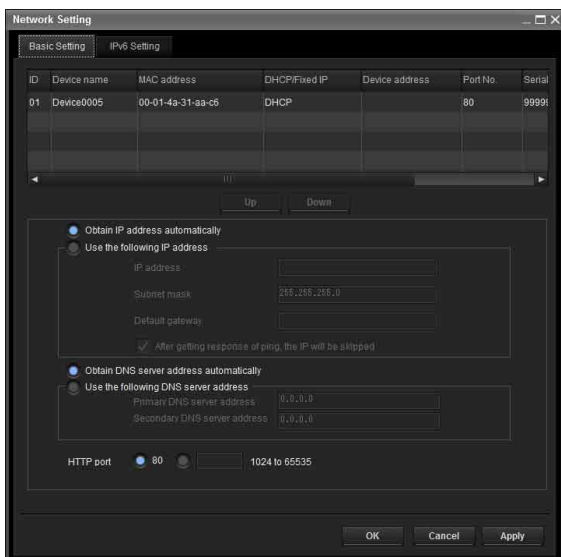
Tip

The factory setting of the camera network is DHCP mode for both LAN and Wireless LAN.

- 7** Select a camera you want to assign an IP address from the list and click **Network**.
The account settings screen is displayed.



- 8** Register the name and password of the administrator and click **OK**.
The factory settings for both items are “admin”.
The **Network Setting** screen is displayed.



- 9** Set the IP address.

To obtain the IP address automatically from a DHCP server:

Select **Obtain an IP address automatically**.

The IP address, Subnet mask and Default gateway are assigned automatically.

Note

When you select **Obtain an IP address automatically**, make sure that the DHCP server is operating on the network.

To specify the IP address manually:

Select **Use the following IP address**, and type the IP address, Subnet mask and Default gateway in the relevant boxes.

- 10** Set the DNS server address.

To obtain the DNS server addresses automatically:

Select **Obtain DNS server address automatically**.

To specify the DNS server addresses manually:

Select **Use the following DNS server address**, and type the Primary DNS server address and Secondary DNS server address in the relevant boxes.

- 11** Set the HTTP port No.

Normally, select **80** for the HTTP port No. To use another port number, type a port number between 1024 and 65535 in the text box.

Note

When using a port number other than **80**, check with the network administrator first.

- 12** Confirm that all items are correctly set, then click **OK**.

If “Setting OK” is displayed, the IP address is correctly assigned.

- 13** When setting is finished, to access the camera directly, double-click the camera name in the list.

[illegible]

The viewer screen of the network camera is displayed on the Web browser.

Display sample



Note

If the IP address is not set correctly, the viewer does not appear after step 13. In that case, try to set the IP address again.

When using Windows XP Service Pack 2 or later

Installing software

A warning message regarding the active contents may appear when you install software such as SNC toolbox from CD-ROM. In this case, operate as follows:

Example: In case of SNC toolbox

If message “Internet Explorer” appears, click **Yes**.



If the message “File Download – Security Warning” appears, click **Run**.



Note

If you select **Save** in the “File Download – Security Warning” dialog, you will not be able to perform the installation correctly. Delete the downloaded file, and click the **Setup** icon again.

If the message “Internet Explorer – Security Warning” appears, click **Run**.

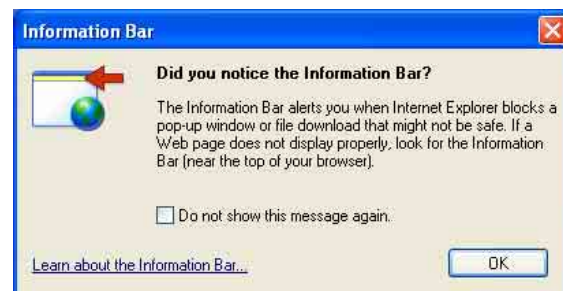


The software installation starts.

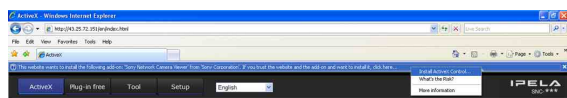
Installing ActiveX Control

During installation of ActiveX Control, the “Information Bar” or “Security Warning” may appear. In this case, operate as follows:

If the message “Information Bar” appears, click **OK**.



If the information bar appears, click on the bar and select **Install ActiveX Control...**



If “Internet Explorer – Security Warning” appears, click **Install**.



The installation of ActiveX Control starts. When installation is completed, the main viewer or the Motion detection menu appears.

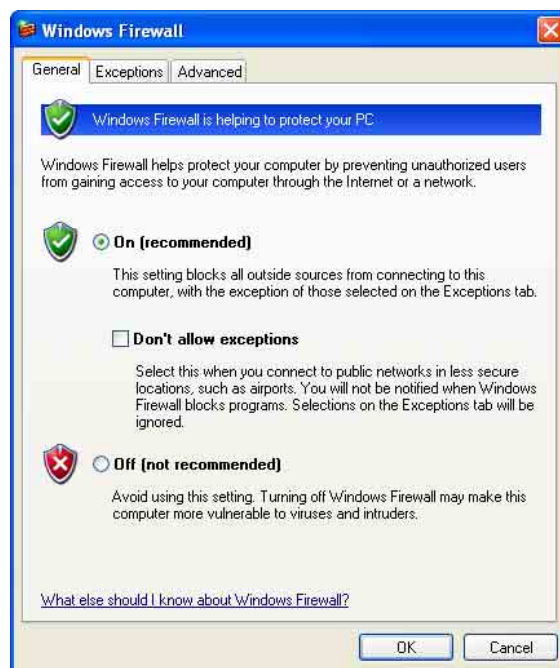
Configuring Windows Firewall

SNC toolbox or SNC audio upload tool may not operate correctly depending on the configuration of Windows Firewall. (No cameras are shown in the list even if they are detected.) In this case, confirm the Windows Firewall configuration as follows:

Example: In case of SNC toolbox

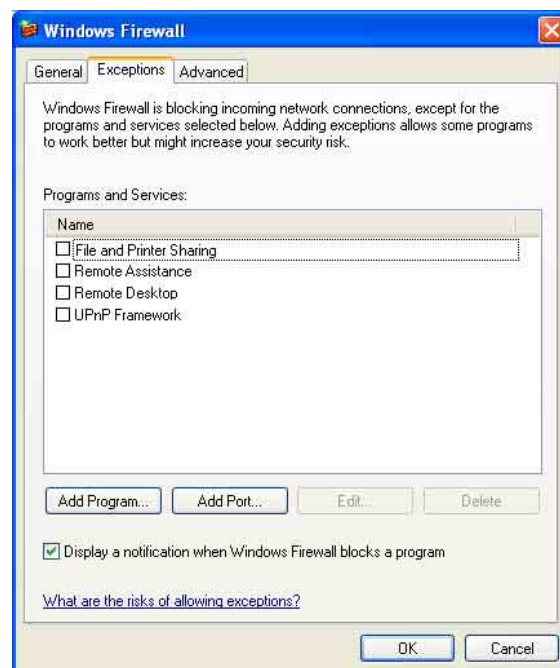
- 1 Select **Control Panel** from the **Start** menu of Windows.
- 2 Select **Security Center** of the working field.

- 3 Select **Off** in the Windows Firewall dialog.



The camera will be displayed in the list.
If you want to keep Windows Firewall **On**, continue with the following steps.

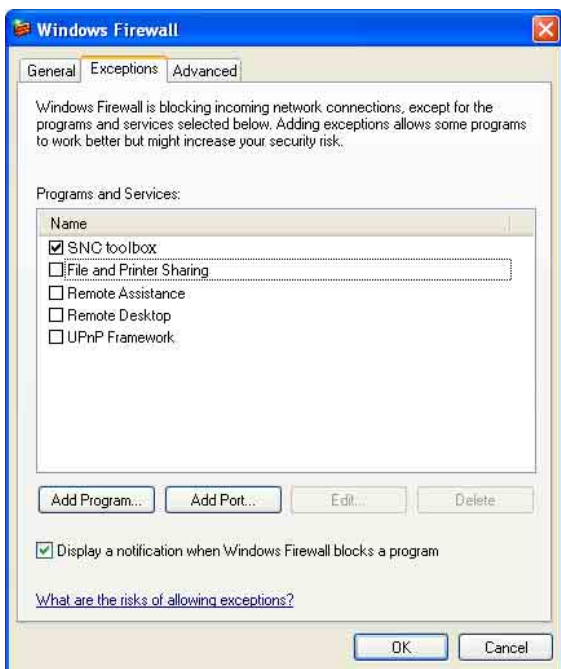
- 4 Select the **Exceptions** tab.
- 5 Click **Add Program...**



- 6 In the Add Program dialog, select SNC toolbox and click **OK**.

SNC toolbox is added to the Programs and Services list.

- 7 Click **OK**.



When the above procedure is completed, the camera connected in the local network are displayed in SNC toolbox.

When using Windows Vista

Installing software

A warning message regarding the active contents may appear when you install software such as SNC toolbox from the CD-ROM. In this case, operate as follows:

Example: In case of SNC toolbox

If the pop-up “AutoPlay” appears when a CD-ROM is inserted into the CD-ROM drive, click **Install or run program**.



Note

If you click **Open folder to view files**, the Web browser will not open automatically. In this case, double-click the “index.htm” file in the CD-ROM.

If the message “Internet Explorer” appears, click **Yes**.



If the message “File Download – Security Warning” appears, click **Run**.



Note

If you select **Save** in the “File Download – Security Warning” dialog, you will not be able to perform installation correctly. Delete the downloaded file, and click the Setup icon again.

If the message “Internet Explorer – Security Warning” appears, click **Run**.



If the message “User Account Control – An unidentified program wants access to your computer” appears, click **Allow**.

The software installation starts.

Starting the software

When you start software such as SNC toolbox, the message “User Account Control – An unidentified program wants access to your computer” may appear. In this case, click **Allow**.

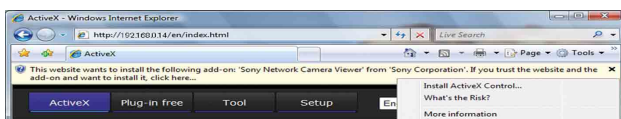
Installing ActiveX Control

During installation of ActiveX Control, the information bar or “Security Warning” may appear. In this case, operate as follows:

If the message “Information Bar” appears, click **Close**.



If the information bar appears, click on the bar and select **Install ActiveX Control...**



If the message “User Account Control – Windows needs your permission to continue” appears, click **Continue**.

If “Internet Explorer – Security Warning” appears, click **Install**.



The installation of ActiveX Control starts. When installation is completed, the main viewer or the Motion detection menu appears.

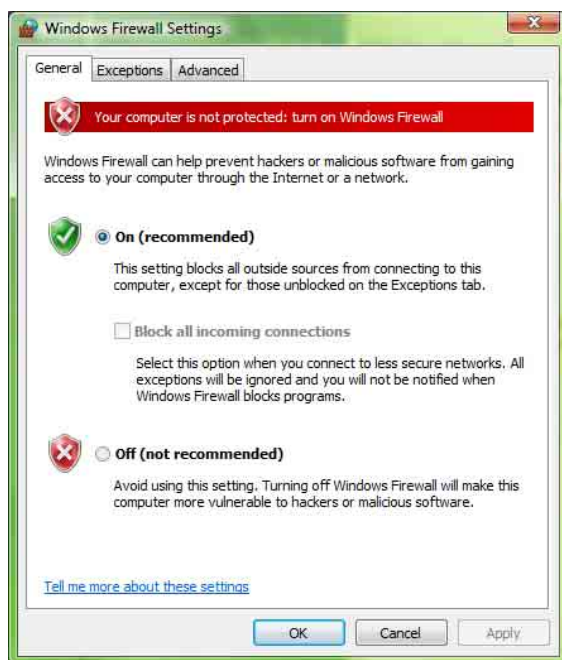
Configuring Windows Firewall

SNC toolbox or SNC audio upload tool may not operate correctly depending on the configuration of Windows Firewall. (No cameras are shown in the list even if they are detected.) In this case, confirm the Windows Firewall configuration as follows:

Example: In the case of SNC toolbox

- 1** Select **Control Panel** from the **Start** menu of Windows.
- 2** Click **Windows Firewall**.
- 3** Select **Turn Windows Firewall on or off**. “User Account Control – Windows needs your permission to continue” may appear. In this case, click **Continue**.

4 Select **Off** in the **General** tab.



The cameras will be displayed in the list.
If you want to keep Windows Firewall **On**, continue with the following steps.

5 Select the **Exceptions** tab.

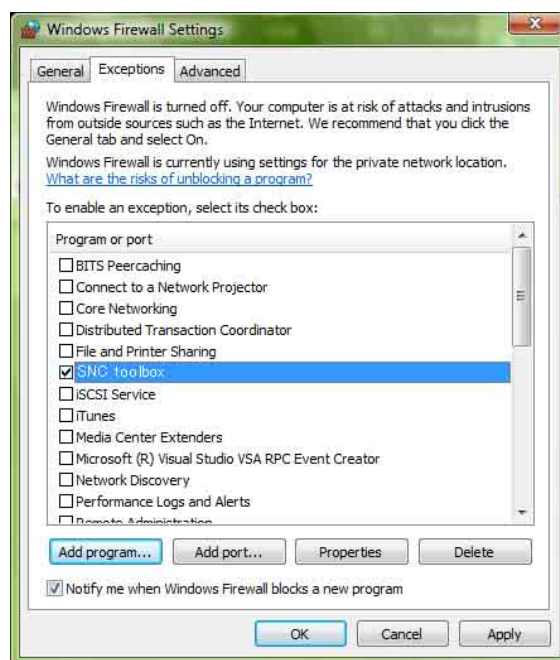
6 Click **Add Program....**

7 If the Add Program dialog appears, select **SNC toolbox** and click **OK**.



SNC toolbox is added to the Program or port list.

8 Click **OK**.

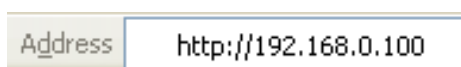


When the above procedure is completed, the cameras connected in the local network are displayed in SNC toolbox.

Accessing the Camera Using the Web Browser

After the IP address has been assigned to the camera, check that you can actually access the camera using the Web browser installed on your computer. Use Internet Explorer as a Web browser.

- 1 Start the Web browser on the computer and type the IP address of the camera in the URL address bar.



The viewer window is displayed.

Display sample



Using the SSL function

Note

The model on sale in China does not support the SSL function.

When Internet Explorer 6 is used

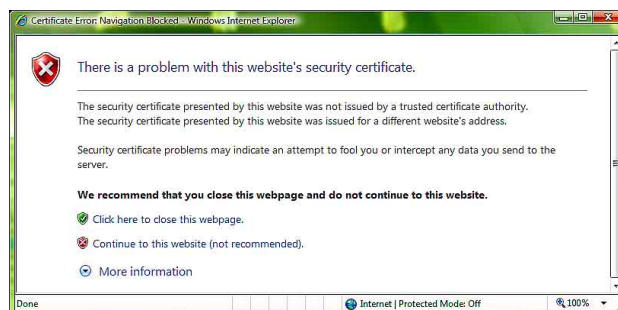
“Security Alert” dialog may appear according to the status of the certificate. In this case, click **Yes** to continue.

The viewer window is displayed (in SSL communication).



When Internet Explorer 7 is used

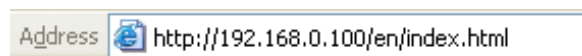
When you enter the camera IP address, “Certificate Error” may appear according to the status of the certificate set on the camera. In this case, click **Continue to this website (not recommended)** to continue. The welcome page appears (in SSL communication).



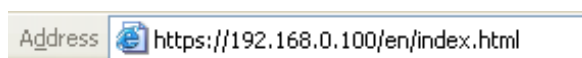
When “Allow HTTP connection for some clients” (page 46) is checked

To use HTTP and SSL connections separately to access, enter the following in the address box of the browser.

For HTTP connection



For SSL connection



When the viewer of the camera is displayed for the first time

“Security Warning” is displayed. When you click **Yes**, ActiveX control is installed and the viewer is displayed.



Notes

- If **Automatic configuration** is enabled in the Local Area Network (LAN) settings of Internet Explorer, the image may not be displayed. In that case, disable **Automatic configuration** and set the Proxy server manually. For the setting of the Proxy server, consult your network administrator.
- When you install ActiveX Control, you should be logged in to the computer as Administrator.
- If you are using Windows XP Service Pack 2 or later, or Windows Vista, the information bar or “Security Warning” may appear. For details, see “Installing ActiveX Control” in “When using Windows XP Service Pack 2 or later” on page 8 or “Installing ActiveX Control” in “When using Windows Vista” on page 11.

Tip

The software is optimized for Internet Explorer using medium font.

To display the viewer correctly

To operate the viewer correctly, set the security level of Internet Explorer to **Medium** or lower, as follows:

- 1 Select **Tools** from the menu bar for Internet Explorer, then select **Internet Options** and click the **Security** tab.
- 2 Click the **Internet** icon (when using the camera via the Internet), or **Local intranet** icon (when using the camera via a local network).
- 3 Set the slider to **Medium** or lower. (If the slider is not displayed, click **Default Level**.)

When using antivirus software, etc., on the computer

- When you use antivirus software, security software, personal firewall or pop-up blocker on your computer, the camera performance may be reduced, for example, the frame rate for displaying the image may be lower.
- The Web page displayed when you log in to the camera uses JavaScript. The display of the Web page may be affected if you use antivirus software or other software described above on your computer.

Basic Configuration by the Administrator

You can monitor the camera image by logging in with the initial conditions set for this network camera. You can also set various functions according to the installing position, network conditions or purpose of the camera. We recommend you configure the following items before monitoring images from the camera.

Setting contents	Setting menu
Set the format of the image sent from the camera.	Video codec Tab (page 36)
Select the White Balance mode according to the installation position.	White balance (page 34)
Select the brightness of the image sent from the camera.	Exposure (page 33) Brightness (page 34)
Select the quality of the image sent from the camera.	Video codec Tab (page 36)
Select the view size of the image.	View size (page 18)
Select whether the audio from the external microphone is sent or not.	Microphone (page 31)
Synchronize the date and time of the camera with those of the computer.	Date & time Tab (page 28)
Make the setting for sending the monitor image attached to an e-mail.	e-Mail (SMTP) Menu (page 58)
Set the user access right for the camera.	User Menu (page 57)

Operating the Camera

This section explains how to monitor the image from the camera using your Web browser (Internet Explorer).

The functions of the camera should be set by the Administrator. For the setting of the camera, see “Adminstrating the Camera” on page 26.

Administrator and User

This network camera identifies those who log in as the **Administrator** or **User**.

The **Administrator** can use all the functions of this network camera, including camera settings. The **User** can use the functions for monitoring the image and audio from the camera, and control the camera. The **Viewer mode** setting is used to restrict the user’s access rights. There are three types of users.

Each type of user can use the corresponding functions below.

Function	Administrator	User		
		Full	Light	View
Monitor a live image	●	●	●	●
View the date and time	●	●	●	●
Control the frame rate (JPEG mode only)	●	●	—	—
Control the image view size	●	●	●	—
Save a still image and movie in the computer	●	●	●	—
Send an image file to the FTP server	●	●	—	—
Send an image attached to an e-mail	●	●	—	—
Record an image in the memory	●	●	—	—
Control the alarm output of the I/O port on the camera	●	●	—	—
Switch the Day/Night function mode	●	●	—	—
Play an audio file (Voice alert)	●	●	—	—
Switch the TCP/UDP transmission mode (Available in MPEG4/H.264 mode only)	●	●	—	—
Receive audio	●	●	●	●
Select the codec mode	●	●	●	—
Control the setting menu	●	—	—	—

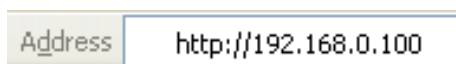
- Usable function
- Not usable function

The access rights of the administrator and the user can be set in “Setting the User — User Menu” of the Administrator menu on page 57.

Logging in to System

Logging in as a user

- 1 Start the Web browser on your computer and type the IP address of the camera you want to monitor.



The viewer is displayed.

Display sample:



Three types of viewer are available: ActiveX viewer, Plug-in free viewer and custom homepage. By default, ActiveX viewer is displayed. To switch the viewer, make changes to the Viewer menu (page 79).

Note

If the main viewer does not start correctly, the security level of the Internet Explorer may be set to higher than **Medium**. See “To display the viewer correctly” on page 14 and check the security level.

About Viewers

You can use the following viewers.

ActiveX viewer

This viewer can monitor the camera image in any of the **JPEG**, **MPEG4** and **H.264** video codecs.

You must install this viewer when you access the main viewer for the first time.

When you display the main viewer of the camera for the first time

When you access the network camera using ActiveX viewer for the first time, the **Security Warning** appears. Click **Yes** and install ActiveX Control. You can use all the functions of the viewer with ActiveX Control.

Plug-in free viewer

This viewer allows the user to select from three image display methods: JPEG, JPEG/FLASH or ActiveX viewer.

JPEG method: JPEG images will be displayed in sequence.

JPEG/FLASH method: JPEG images will be displayed in sequence. Adobe Flash is required to display the image.

ActiveX viewer method: The image can be viewed when the image display is set to JPEG, MPEG4 or H.264.

Notes

- If **Automatic configuration** is enabled in the Local Area Network (LAN) Settings of Internet Explorer, the camera image may not be displayed. In that case, disable **Automatic configuration** and set the Proxy server manually. For the setting of the Proxy server, consult your network administrator.
- When you install ActiveX Control, you should be logged in to the computer as the Administrator.

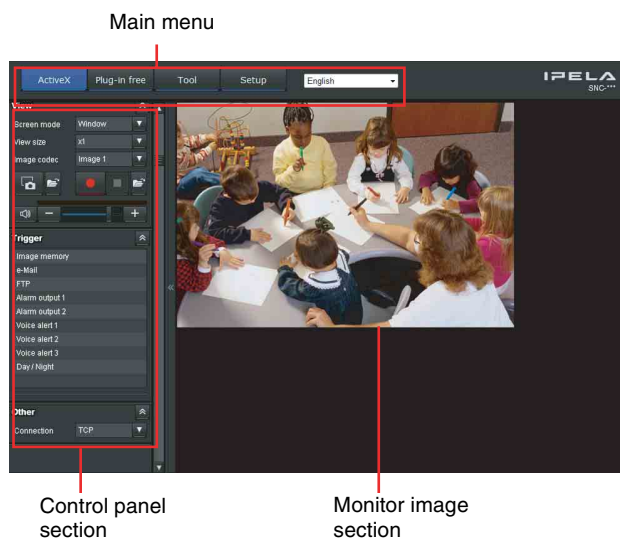
Tip

Every page of this software is optimized for Internet Explorer in **Medium** font.

Configuration of Main Viewer

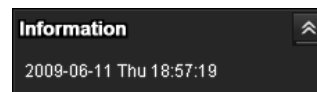
This section explains the functions of the parts and controls of the main viewer. For a detailed explanation on each part or control, see the specified pages.

Main viewer using ActiveX viewer



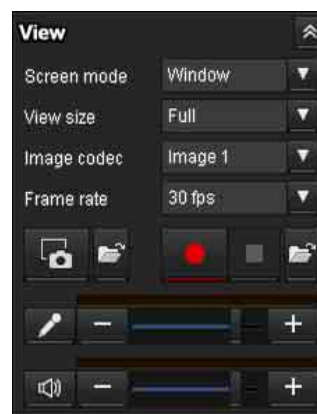
Control panel section

Information panel



Check the date and time here.

View panel



You can change the screen mode, size of the image, image codec mode and frame rate. Also, still images and movies can be saved (movie saving can also be stopped) from here. Microphone and audio output levels can be adjusted.

Main menu

ActiveX

Displays the ActiveX viewer.

Plug-in free

Displays the Plug-in free viewer.

Tool

You can download system utility from here. (page 23)
This operation is only available when you are logged in as administrator.

Setup

Click to display the Administrator menu. (page 26)
You can operate this function only when logging in as the administrator.

Screen Mode

Select Window or Full Screen.

View size

Selects the view size to be displayed.
Click **View size** list box to select the view size.
Select **x1** to display images set in **Image size** of the Camera menu. (page 36)
Select **Full** to display images according to the view size.
Select **Fit** to display images according to the view size, with fixed aspect ratio.

Image Codec

Select an image codec mode.

Frame rate

(Displayed only when the camera image is in JPEG.)
Selects the frame rate to transmit images.

(Capture)

Click to capture a still image shot by the camera and to store it in the computer. Click  to open the folder to be saved.

(Run)/ (Stop Save Video)

Runs and stops Save Video. Click  to open the folder to be saved.

Volume



Use the slide bar to adjust the volume for sound output level.

When you click , the icon changes to  and the output from the speaker stops. To output sound from the speaker, click  again.

Microphone volume

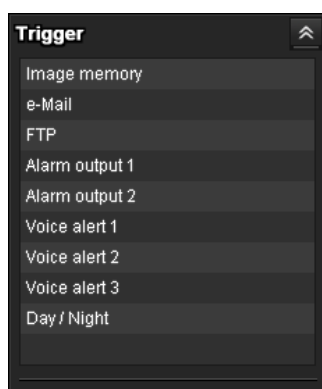
This is displayed when **Microphone** (page 31) in the Common tab of the Camera menu is set to **On**, and a user with audio enabled in the User Menu accesses the device.



Use the slide bar to adjust the microphone volume.

When you click , the icon changes to  and the microphone input stops. To input the microphone, click  again.

Trigger panel



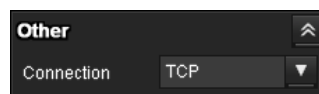
The above is displayed only when **Viewer mode** (page 57) is set to **Full**, and one or more triggers are enabled in the Trigger menu (page 70).

The configured functions are displayed as buttons on this panel.

Click the function button you want to use on the Trigger panel. The selected function is activated. The selectable functions are as follows:

- send still image files attached to an e-mail (page 21)
- send still image files to an FTP server (page 21)
- Record still image files (page 21)
- control the alarm output (page 21)
- switch the Day/Night function on/off (page 21)
- play the audio file stored in the camera (page 21)

Others panel



(Displayed only when the camera image is in MPEG4 or H.264.)

You can switch between TCP and UDP (Unicast/Multicast).

Each click switches the transmission mode of the video/audio data between TCP mode, UDP (Unicast) mode, and UDP (Multicast) mode (page 22).

Monitor image

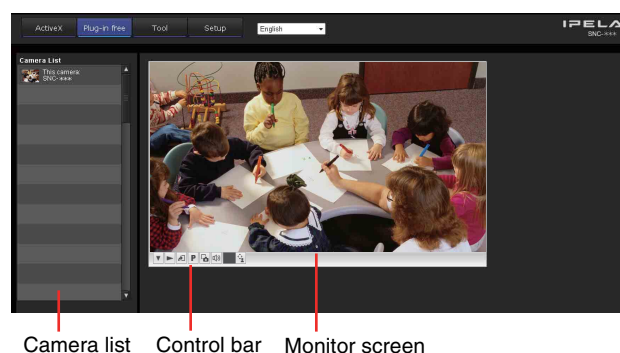


The image shot by the camera is shown here.

Plug-in free viewer

Main viewer using Plug-in free viewer

Display sample:



Monitor screen

(Pan/tilt/zoom functions are not available for this model.)

The image shot by the camera is shown here.

There are two modes for on-screen pan/tilt/zoom operation using a mouse: Area zoom mode and Vector dragging mode. A control bar is displayed on the screen. In the Area zoom mode, clicking will pan or tilt the camera towards the center of the image. The Area zoom will move the camera in the direction that displays the area selected by the operator and zooms in at the same time. The operator can choose a part of the image to view and zoom in by surrounding the area with a frame by dragging the mouse.

In the Vector dragging mode, the camera pans or tilts in the dragged direction. How long you drag the mouse determines the speed. Releasing the button on the mouse after dragging stops the panning or tilting of the camera. You can also use the tool bar to pan or tilt. The zoom operation using the mouse wheel is available in all modes.

Control bar

The following operation buttons are available.



-  **Setting**
You can set the streaming method, image size, frame rate, PTZ operation mode (Not available with this product), and trigger selection.
-  **Streaming start button**
Starts streaming. (Appears while stops streaming.)
-  **Streaming stop button**
Stops streaming. (Appears while streaming.)
-  **Trigger run button**
Runs the selected trigger.
-  **Preset** (Not available with this product.)
Select a preset position to move the camera to the registered preset position.
(Displayed only when a camera preset position is registered.)

-  **Save still image button**
Captures still images taken by the camera and saves them to the computer.
-  **Audio output volume slider**
Use the slider to adjust the volume. Clicking the button will stop sound output.
(Displayed only when **ActiveX** is set for **Streaming method** in **Setting**, and **Microphone** in the Camera Menu (page 31) is set to **On**.)
-  **Control waiting time and control time for exclusive control**
-  **Exclusive control button** (Not available with this product.)

Camera list

The camera list is displayed when **Camera list** is set to **On** in the viewer menu, and at least one camera is registered.

Using the Trigger Button

You can execute various functions by clicking their respective buttons on the Trigger panel.

Sending a monitor image via e-mail

You can send a captured still image by attaching it to an e-mail.

To use this function, you need to make **e-Mail (SMTP)** active and set the address in the Trigger menu of the Administrator menu properly (page 70).

- 1 Click **e-Mail (SMTP)** on the Trigger panel.
The still image of the moment you click is captured, and your e-mail with the image file attached is sent to the specified mail address.

Sending a monitor image to an FTP server

You can send a captured still image to the FTP server.
To use this function, you need to make **FTP** active and set the address in the Trigger menu of the Administrator menu properly (page 71).

- 1 Click **FTP client** on the Trigger panel.
The still image of the moment you click is captured, and the image file is sent to the FTP server.

Recording a camera image as a still image

You can capture a camera image as a still picture and record it.

SNC-CH140 can record images in its built-in memory or CF memory card (not supplied). SNC-DH140 can only record images in its built-in memory.

To use this function, you need to make **Image memory** active and set the details in the Trigger menu of the Administrator menu (page 71).

- 1 Click **Image memory** on the Trigger panel.
The still image of the moment you click is captured, and the image file is recorded.

Controlling Alarm out 1, 2

You can control Alarm out 1, 2.

To use this function, you need to make **Alarm out 1** or **Alarm out 2** active in the Trigger menu of the Administrator menu (page 71).

- 1 Click **Alarm out 1** or **Alarm out 2** on the Trigger panel.
The alarm output is switched by clicking.
The alarm output mode can be selected from **Toggle** or **Timer** of **Alarm out 1, 2** in the Trigger menu (page 71).

Tip

For the connection of peripheral devices to the alarm output of the I/O port, see the supplied Installation Manual.

Controlling the Day/Night function

You can set the Day/Night function to On (night mode) and Off (day mode).

To use this function, you need to make **Day/Night** active in the Trigger menu of the Administrator menu (page 71).

- 1 Click **Day/Night** on the Trigger panel.
Each click switches the Day/Night function alternately between On (night mode) and Off (day mode).

Note

If **Day/Night** in the Trigger-Day/Night menu (page 71) is set to **Auto**, you cannot control the Day/Night function by clicking **Day/Night**.

Playing an audio file stored in the camera

You can play an audio file previously stored in the camera using the SNC audio upload tool.

To use this function, you need to make **Voice alert1**, **Voice alert2** and **Voice alert3** active in the Trigger menu of the Administrator menu (page 71).

- 1 Click **Voice alert1**, **Voice alert2** or **Voice alert3** on the Trigger panel.
Playback of the selected audio file starts and the playback sound is output from the speaker connected to the camera.

Switching TCP/UDP Transmission Mode

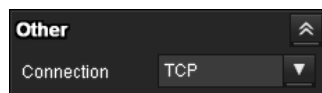
You can select TCP or UDP as the communication port for video/audio data.

This function can be used when Mode (video codec mode) is set to **MPEG4** or **H.264** and the ActiveX viewer is used.

Notes

- The function may not operate correctly if you use personal firewall software or antivirus software on your computer. In that case, disable the software or select the TCP mode.
- If you are using Windows XP Service Pack 2 or later, or Windows Vista, disable “Windows Firewall.” For details, see “Configuring Windows Firewall” in “When using Windows XP Service Pack 2 or later” on page 9, or “Configuring Windows Firewall” in “When using Windows Vista” on page 11.

- 1 Select **TCP**, **UDP (Unicast)** or **UDP (Multicast)** from the **Connection** drop-down list in the Others panel.



TCP: This is normally selected.

When **TCP** is selected as the communication port, HTTP communication is adopted for video/audio communications.

HTTP is the protocol used for reading the usual Web page.

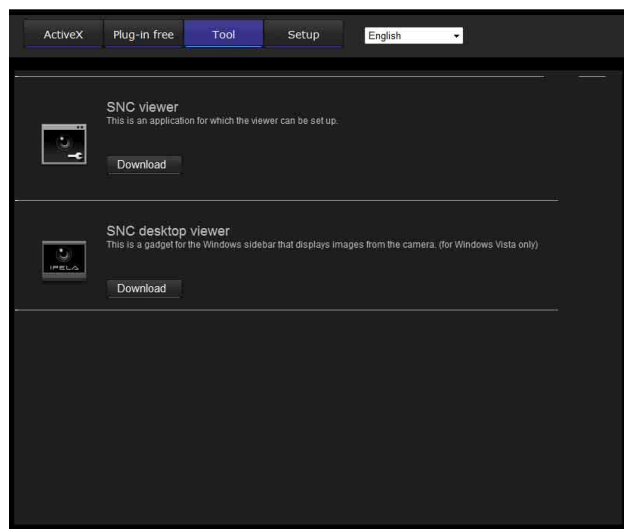
In an environment capable of reading Web pages, you can watch or listen to video/audio by selecting the TCP port.

UDP (Unicast): When **UDP (Unicast)** is selected as the communication port, RTP (Real-time Transport Protocol) is adopted for video/audio communications. Since RTP is the protocol for running video/audio data, the video/audio playback is smoother than when TCP (HTTP) is selected. If a firewall is installed between the camera and the computer, or depending on the network environment, video/audio may not play back properly when **UDP (Unicast)** is selected. In this case, select **TCP**.

UDP (Multicast): This protocol is selectable when **Multicast streaming** (page 38) is **On**. When **UDP (Multicast)** is selected as the transmission port, RTP (Real-time Transport Protocol) and UDP multicast techniques are adopted for video/audio transmission. By selecting it, the network transmission load of the camera can be reduced. If a router that does not correspond to a multicast or firewall is installed between the camera and the computer, video/audio may not play back properly. In this case, select **TCP** or **UDP (Unicast)**.

Using the System Utility

You can download system utility from the tools tab on the main menu.



To use the utility, click **Download** to begin download.

SNC viewer

SNC viewer is an application which allows you to set the initial state of the viewer.

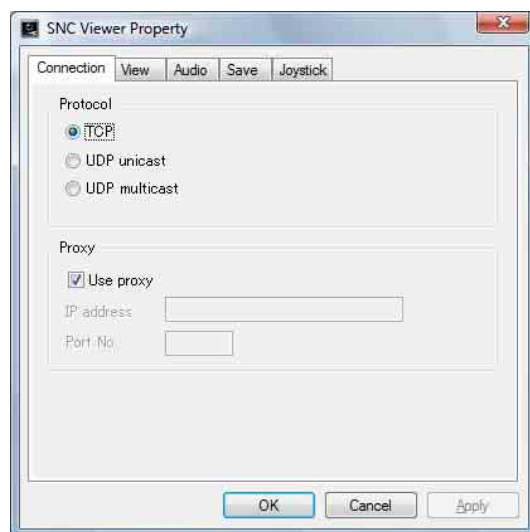
Installing the SNC viewer

- 1 Execute the downloaded SNCViewer.msi file.
- 2 Install the SNC viewer following the instructions on the wizard.
When the license agreement policies are displayed, agree after reading them carefully and install the SNC viewer.

Using the SNC viewer

Click **SNC viewer** in the control panel.

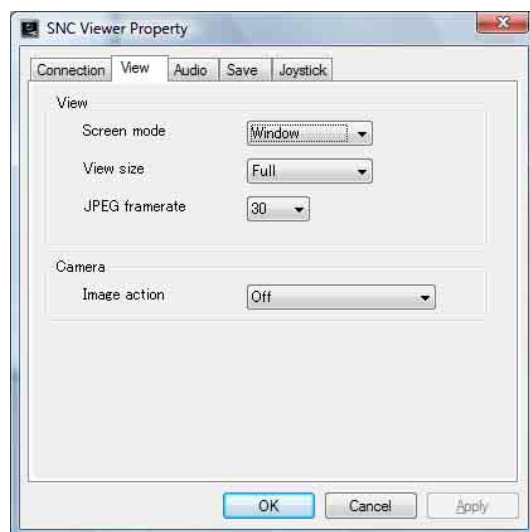
Connection tab



You can set the connection method.
Select the start-up connection from: **TCP**, **UDP Unicast**, and **UDP Multicast**.

If TCP connection is selected, you can configure proxy settings by selecting **Use proxy**.

View tab



Screen mode

You can select **Window** or **Full**.

View size

You can select the view size.

JPEG framerate

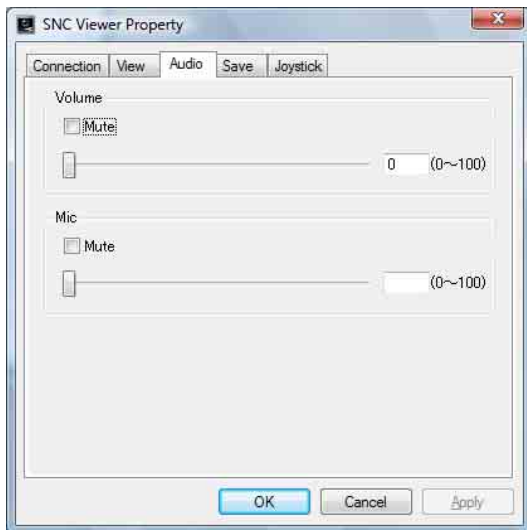
You can set the frame rate for JPEG.

Image action

Select from the image operation modes **Area zoom**, **Vector dragging** and **Off**.

Tip

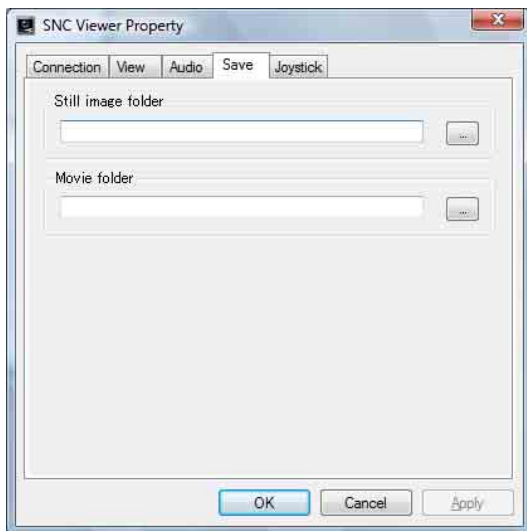
This device is not equipped with operational functions for images.

Audio tab**Volume**

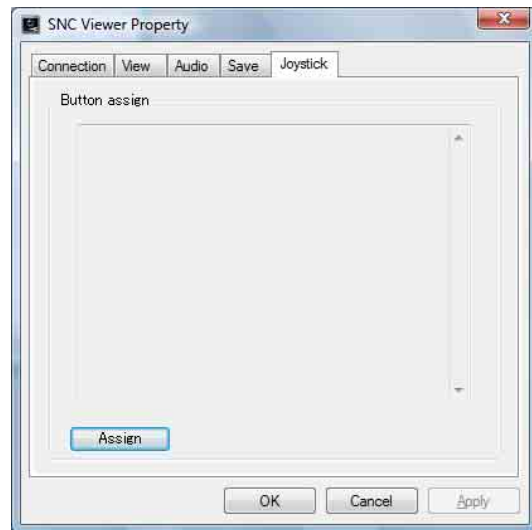
Mute: Select this option for muting the sound at start-up.
Use the slide bar to set the volume for start-up sound output.

Mic

Mute: Select this option for muting the microphone sound at start-up.
Use the slide bar to set the volume for start-up microphone input.

Save tab

Specify a folder to save the still images and movies to.

Joystick tab

You can assign the joystick buttons here.

Tip

This device is not equipped with Joystick functions.

SNC Desktop viewer

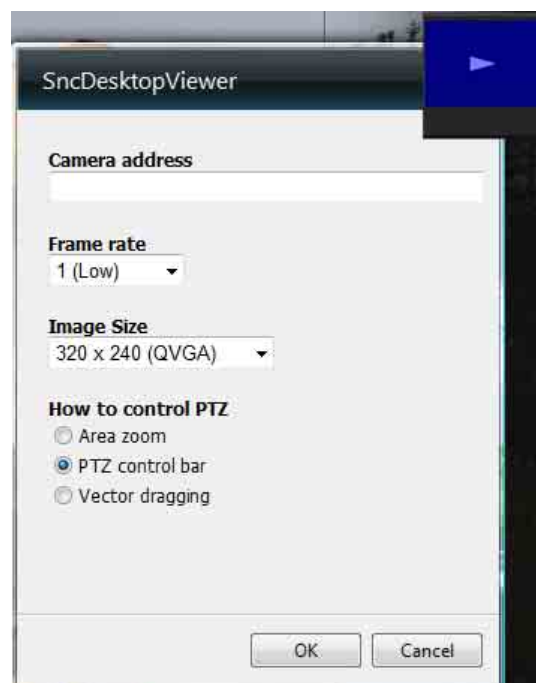
This is a gadget that displays the camera image in the side bar of Windows Vista.

Installing the SNC desktop viewer

- 1** Click **Download**.
When the license agreement policies are displayed on the SNC desktop viewer download screen, agree after reading them carefully and download the SNC desktop viewer.
- 2** Execute the downloaded SncDesktopViewer.gadget file.

Using the SNC desktop viewer

When the SNC desktop viewer is successfully installed, it will appear on the side bar of Windows Vista.



Camera address

Set the IP address for the camera to display on the Gadget.

Frame rate

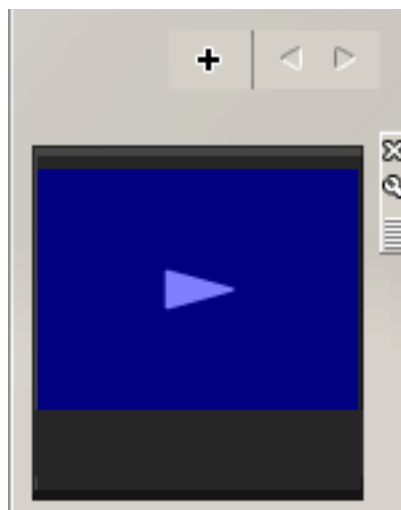
Select the frame rate for the image to display on the Gadget.

Image size

Select the image size for the image to display on the Gadget.

How to control PTZ

Select the PTZ operation mode for the Gadget screen from the options **Area zoom**, **PTZ control bar**, and **Vector dragging**.



Click (Exit) to exit Gadget.

When you click (Set), you will see the following setting screen.

Tip

This device is not equipped with operational functions for PTZ.

Administrating the Camera

This section explains how to set the functions of the camera by the Administrator.

For details about monitoring the camera image, see “Operating the Camera” on page 16.

This section explains the basic operations and each option of the Administrator menu.

Note on the display of menu options

The setting menus of this unit will clearly display only the setting options that you can currently select. Grayed out options cannot be selected.

Basic Operations of the Administrator Menu

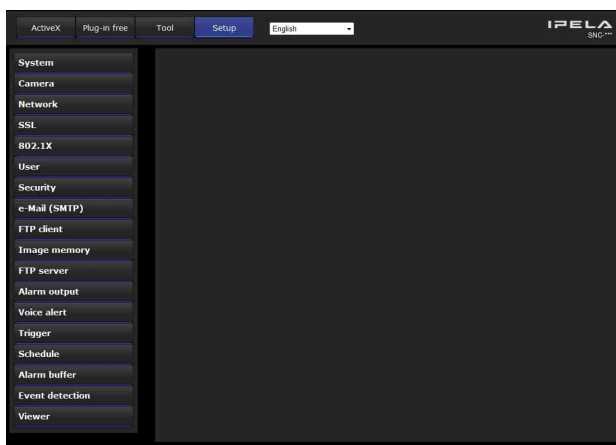
You can use the Administrator menu to set all functions to suit the user's needs.

Click **Setting** in the viewer to display the Administrator menu.

How to set up the Administrator menu

- 1 Log in to the homepage to display the viewer.
For details, see “Logging in as a user” on page 17.
- 2 Click **Setting** on the main menu.
The authentication dialog appears. Enter the user name and password for Administrator.
The user name “admin” and password “admin” are set at the factory for the Administrator.

The Administrator menu appears.



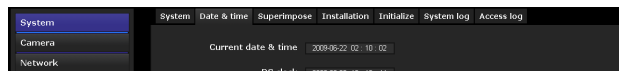
- 3 Click the menu name (example: System) on the left side of the Administrator menu.
The clicked menu appears.

Example: “System” menu



- 4 Select the required tab above the menu, and set each setting option in the tab.

Example: “Date & time” tab of “System” menu



See pages 28 to 81 for details of the menu tabs and setting options.

- 5 After setting, click **OK**.
The settings you have made become active.

Click **Cancel** to nullify the set values and return to the previous settings.

Buttons common to every menu

The following buttons are displayed on all the menus. The functions of the buttons are the same on every menu.



Click this button to confirm the settings.

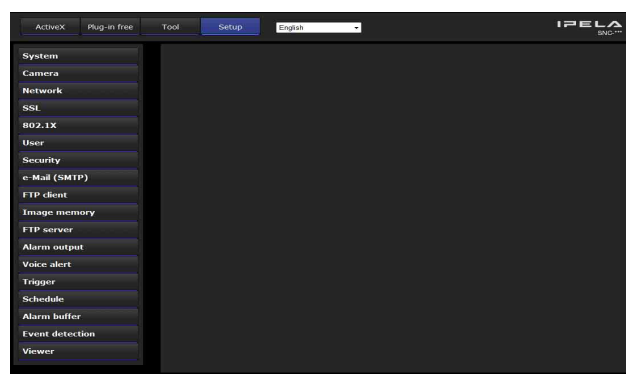


Click this button to nullify the set values and return to the previous settings.

General notes on menus

- One-byte katakana character is not valid for any text field, such as User name.
- After changing a setting on a menu, wait at least 10 seconds before turning off the power of the camera. If the power is turned off immediately, the new setting may not be stored correctly.
- If the camera settings are changed while watching the main viewer, some settings cannot be restored. To reflect the change on the opening main viewer, click **Refresh** on the Web browser.

Configuration of the Administrator menu



System

Displays the System menu. For details, see “Configuring the System — System Menu” (page 28).

Camera

Displays the Camera menu for setting the camera image and audio. For details, see “Setting the Camera Image and Audio — Camera Menu” (page 31).

Network

Displays the Network menu for setting the network connection. For details, see “Configuring the Network — Network Menu” (page 38).

SSL

Displays the SSL menu for performing SSL communication between the client device and camera. (“Setting the SSL function — SSL Menu” on page 46)

802.1X

Displays the 802.1X menu for connecting the camera to a network configured in compliance with the 802.1X standard for port authentication. (“Using the 802.1X Authentication Function — 802.1X Menu” on page 51)

User

Displays the User menu for setting the log in user name and password. (“Setting the User — User Menu” on page 57)

Security

Displays the Security menu for specifying a computer that is allowed to connect to the camera. (“Setting the Security — Security Menu” on page 58)

e-Mail (SMTP)

Displays the e-Mail (SMTP) menu for sending an e-mail. (“Sending an Image via E-mail — e-Mail (SMTP) Menu” on page 58)

FTP client

Displays the FTP client menu for sending an image/audio file, etc., to an FTP server. (“Sending Images to FTP Server — FTP client Menu” on page 61)

Image memory

Displays the Image memory menu for recording an image/audio file, etc. (“Recording Images in Memory — Image memory Menu” on page 64)

FTP server

Displays the FTP server menu for setting the FTP server function of the camera. (“Downloading Images from the Camera — FTP server Menu” on page 68)

Alarm output

Displays the Alarm output menu for setting the alarm output terminal of the camera. (“Setting the Alarm Output — Alarm output Menu” on page 68)

Voice alert

Displays the Voice alert menu for playing an audio file stored in the camera in synchronization with alarm detection by the sensor input or the motion detection function. (“Outputting Audio Linked to Alarm Detection — Voice alert Menu” on page 69)

Trigger

Displays the Trigger menu for designating the operation to execute when you run a trigger. (“Setting the Operations from the Viewer — Trigger Menu” on page 70)

Schedule

Displays the Schedule menu for the Day/Night function, e-Mail (SMTP) function, FTP client function, Image memory function and Alarm output function, Voice alert function, etc. (“Setting the Schedule — Schedule Menu” on page 72)

Alarm buffer

Displays the Alarm buffer menu for the buffer for storing the image and audio related to alarm detection. (“Setting the Alarm Buffer — Alarm buffer Menu” on page 72)

Event Detection

Displays the setting menu for all built-in detection functions. (“Setting the Sensor input/Camera tampering detection/Motion detection — Event detection Menu” on page 73)

Viewer

Displays the Viewer menu from which you can select the viewer to use and configure advanced settings. (“Configuring the Viewer — Viewer Menu” on page 79)

Configuring the System

— System Menu

When you click **System** in the Administrator menu, the System menu appears.

Use this menu to perform the principal settings of the software.

The System menu has seven tabs: **System**, **Date & time**, **Superimpose**, **Installation**, **Initialize**, **System log** and **Access log**.

System Tab

Title bar name

Type a name of up to 48 characters to be displayed on the title bar. The characters typed here are displayed on the title bar of the Web browser.

Serial number

The serial number of the camera is displayed.

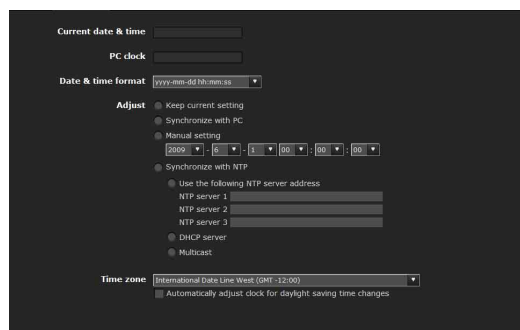
Software version

The software version of this camera is displayed.

OK/Cancel

See “Buttons common to every menu” on page 26.

Date & time Tab



Current date & time

Displays the date and time set on the camera.

Note

After you have purchased the camera, be sure to check the date and time of the camera and set as necessary.

PC clock

Displays the date and time set on your computer.

Date & time format

Select the format of date and time to be displayed in the main viewer from the drop-down list.

You can select the format between **yyyy-mm-dd hh:mm:ss** (year-month-day hour:minutes:seconds), **mm-dd-yyyy hh:mm:ss** (month-day-year hour:minutes:seconds), and **dd-mm-yyyy hh:mm:ss** (day-month-year hour:minutes:seconds).

Adjust

Select how to set the day and time.

Keep current setting: Select if you do not need to set the date and time.

Synchronize with PC: Select if you want to synchronize the camera's date and time with the computer.

Manual setting: Select if you want to set the camera's date and time manually.

Select the year, month, date, hour, minutes and seconds from each drop-down list.

Synchronize with NTP: Select if you want to synchronize the camera's date and time with those of the time server called NTP server (Network Time Protocol).

Set the NTP server when **Synchronize with NTP** is selected.

Use the following NTP server address: Synchronize with the selected NTP server address.

NTP server 1: Enter the first choice for NTP server address.

NTP server 2: Enter the second choice for NTP server address.

NTP server 3: Enter the third choice for NTP server address.

DHCP server: Select DHCP server when you need to get NTP server information from DHCP server.

Multicast: Select Multicast when you search for an NTP server with Multicast.

Time zone

Set the time difference from Greenwich Mean Time in the area where the camera is installed.

Select the time zone in the area where the camera is installed from the drop-down list.

Automatically adjust the clock for daylight saving time changes

When selected, the clock is automatically adjusted according to the daylight saving time of the selected time zone.

Note

If the time zone selected in **Time zone** is different from that set on the computer, the time is adjusted using the time zone difference and set on the camera.

OK/Cancel

See “Buttons common to every menu” on page 26.

Superimpose Tab

Select whether to superimpose the camera ID, date & time and other information on the image or not. The camera ID is also superimposed on images recorded by the Pre-alarm or Post-alarm function.

Superimpose

On/Off

When using the Superimpose function, select **On**.

Font size

Set the font size.

Style

Set the items to superimpose and the format to display in. Superimpose settings are available for the following items:

- **Date:** Set the display settings for date and time.
- **Camera ID:** Set the display settings for Camera ID and string.
- **Event:** Configure the display setting for when an event occurs.
- **Codec:** Configure the bit rate and frame rate display settings. Displays the codec information for Image 1.
- **Custom string:** Set Custom string to display the text of your choice.

Display format, including color, can be individually set for each item.

Color: Select the font color of the superimposed text.

Blink: Select **On** to enable blinking for the superimposed text. However, the blinking display is not available for **Date**.

String Effect: Enable a string effect for displayed text.

Advanced: Click the **Setting** button in **Date** to configure the format of date/time and the separator. Click the **Setting** button in **Camera ID** to configure the Camera ID string setting and upload Logo. Images that can be used as a Logo must be in gif89a format with an image size up to 640 × 120. The number of pixels horizontally is even numbered and the maximum file size is approximately 50 KB. The Camera ID string and logo can not be used at the same time.

Superimpose format

Click **Edit** to edit the content to superimpose over each display position.

Only one **Date** and one **Camera ID** can be specified for the **Superimpose format**.

You can set the content to superimpose in the bottom left, bottom right, top left, top right, center, top middle, and bottom middle parts, respectively. However, if you specify the top middle, superimposed content will not appear on the top left or top right. Similarly, if you specify bottom middle, superimposed content will not appear on the bottom left or bottom right.

Click **Date & Time**, **Camera ID**, **Codec** or **Event** to insert the corresponding tag into the string.

OK/Cancel

See “Buttons common to every menu” on page 26.

Installation Tab

You can perform settings related to installation.

Maximum image size

1280 × 720: Image will have an aspect ratio of 16:9, and an image size up to 1280 × 720 can be specified for the video codec.

1280 × 1024: Image will have an aspect ratio of 5:4, and an image size up to 1280 × 1024 can be specified for the video codec.

Notes

- The camera restarts when the Maximum image size is changed. It takes about 2 minutes.
- The settings below are changed when the Maximum image size is changed.
 - Camera menu-privacy mask tab: returns to the factory setting.
 - Camera menu-video codec tab: returns to the factory setting except:
 - Image size of image1: to be 1280 × 720 when set to 1280 × 720, or 1280 × 1024 when set to 1280 × 1024.
 - Frame rate of image1: to be 30fps when set to 1280 × 720, or 20fps when set to 1280 × 1024
 - Alarm buffer menu: returns to the factory setting.
 - Event detection menu- motion detection tab: returns to the factory setting except:
 - Maximum detection size of motion diction: to be width of 1280 and height of 720 when set to 1280 × 720, or 1280 and height of 1024 when set to 1280 × 1024.

- Maximum detection size of VMF: to be width of 1280 and height of 720 when set to 1280 × 720 or 1280 and height of 1024 when set to 1280 × 1024.

Video out

You can configure the output setting for the analog image output terminal of the camera. Select **On** to output an NTSC or PAL signal.

Note

The output signal format is determined according to the setting of the camera's NTSC/PAL switch.

OK/Cancel

See “Buttons common to every menu” on page 26.

Initialize Tab

Reboot

Used when rebooting the system. Click **Reboot**, and the message “This System will be rebooted. Are you sure?” appears. Click **OK** to reboot the camera. It takes about two minutes to restart.

Factory default

Resets the camera to the factory settings.

Retain current network settings

When this item is checked, only the current network settings will be retained after reset.

Click **Factory default**, and the message “Setup data will be initialized. Are you sure?” appears. When you click **OK**, the network indicator on the camera starts to blink. After adjustments of the default settings have finished, the camera reboots automatically. Do not turn off the camera until the camera reboots.

Tip

The camera can also be reset to the factory settings by turning on the power of this unit while pressing the reset button on the camera. For details, see the supplied Installation Manual.

Backup setting data

Saves the setting data of the camera in a file. Click **Save**, and follow the instructions on the Web browser to specify the folder and save the setting data of the camera. The file name preset at the factory is “snc-ch140.cfg” for SNC-CH140.

Restore setting

Loads the stored setting data of the camera. Click **Browse** and select the file in which the setting data is stored. Click **OK**, and the camera is adjusted according to the loaded data, and restarted.

Notes

- With **Restore setting**, some items in the Network menu (page 38) cannot be restored.
- The following items cannot be stored or restored with **Backup setting data** or **Restore setting**.
 - audio files uploaded using SNC audio upload tool
 - a homepage created using Custom Homepage of SNC toolbox
 - a client certificate and CA certificate to be used in the 802.1X authentication function
 - Header logo
 - superimpose logo

Format CF memory card (SNC-CH140 only)

Click **Format** to format the CF memory card (not supplied) inserted into the CF card slot of the camera. The files and folders stored in the CF memory card are deleted while formatting.

Notes

- Before formatting, disable the image memory function and FTP server function to protect the CF memory card from writing.
- Do not activate the **Format CF memory card** function when no card is inserted into the CF card slot.

Delete custom homepage

Click **Delete** to delete the homepages recorded in the flash memory of the camera with Custom Homepage of SNC toolbox (page 88).

Delete voice alert file

Click **Delete** to delete all the audio files stored in the camera using SNC audio upload tool (page 93).

Notes

- Clicking **Delete** deletes all the stored audio files simultaneously. To delete a specified audio file only, perform deletion of the audio file in the corresponding Voice alert tab of the Voice alert menu (page 69).
- Before deleting the audio file, set **Voice alert** to **Off** in each tab of the Voice alert menu (page 69).

Delete header logo

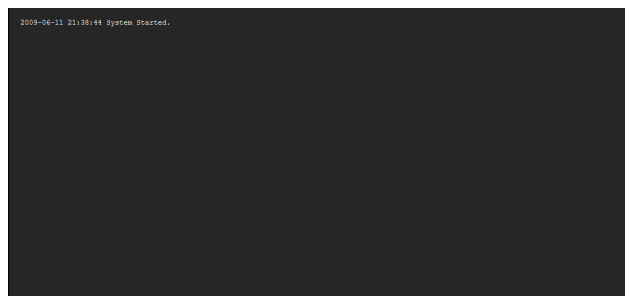
Click **Delete** to delete the header logo set in the Viewer menu.

Delete superimpose logo

Click **Delete** to delete the superimposed logo, set in the Advance of the camera ID on the Superimpose tab of the System menu, from the camera.

To set whether to show or hide the superimpose logo, you need to configure the setting under the Superimpose tab.

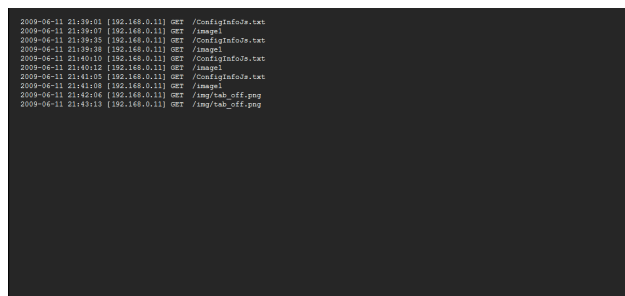
System log Tab



The data of the software activity of the camera is recorded in this log. It includes data that is useful if a problem occurs.

Click **Reload** to reload the latest data.

Access log Tab



The access record of the camera is displayed. Click **Reload** to reload the latest data.

Setting the Camera Image and Audio

— Camera Menu

When you click **Camera** in the Administrator menu, the Camera menu appears.

Use this menu to set the functions of the camera.

The camera menu consists of the following 7 tabs.

SNC-CH140: Common, Focus, Picture, Privacy masking, Day/Night, Video codec, and Streaming.

SNC-DH140: Common, Focus/Zoom, Picture, Privacy masking, Day/Night, Video codec, and Streaming.

Common Tab

Color

Select **Color** or **Monochrome** for the image.

Microphone

Select whether you are going to send audio from the microphone input connector. Select **On** to send the audio from the network camera.

Note

When you change the **Microphone** setting, click **Refresh** on the Web browser to reflect the change on the opening main viewer page.

Mic volume

Set the volume level of the audio input from the microphone input connector. It is adjustable from **-10** to **+10**.

Audio in

Select microphone input or line input.

Audio codec

Select the bit rate of audio from the microphone input connector. **G.711 (64kbps)**, **G.726 (40kbps)**, **G.726 (32kbps)**, **G.726 (24kbps)** or **G.726 (16kbps)** can be selected.

Note

No audio is output if JPEG or JPEG/FLASH is used for the Plug-in free viewer.

Echo suppressor

Select **On** to reduce echo from audio transmission.

Audio noise reduction

Select **On** to use Audio noise reduction.

Audio upload

Using SNC audio upload tool stored in the supplied CD-ROM, you can output audio that is input to the computer's audio input terminal from a powered speaker connected to the line output jack of the camera. Select **On** to output audio from the speaker.

Volume

Set the speaker volume level from **- 10** to **+ 10**.

OK/Cancel

See "Buttons common to every menu" on page 26.

Focus tab — Adjusting the Focus (SNC-CH140 only)

Adjust the focus by moving the flange back position of the imaging device.

Preview screen

Preview the image and adjust the focus. The current image focus position is superimposed when adjusting the focus. For the details on each button, refer to the Control bar of the Plug-in free viewer (page 20).

Note

If you click the buttons in this tab, in order to adjust the focus easily, the settings below are temporarily changed:

- **Privacy masking** and **Cropping** are deactivated.
- The current image focus position is superimposed.
- The alarm of **Motion detection** is deactivated.
- View-DR is turned on.

Adjusting the focus

Click **Start** button in **Easy Focus** to set the focus to the optimum position.

Note

The most suitable focus position may not be available depending on imaging conditions. If so, click the **-20**, **-5**, **-1**, **+1**, **+5** or **+20** buttons to adjust the focus accordingly.

Focus reset

Click the **Reset** button to return to the default flange back position.

Focus/Zoom tab — Adjusting the focus/zoom (SNC-DH140 only)

Adjust the focus and zoom position by looking at the image.

Preview screen

Preview the image and adjust the focus. The current image focus position is superimposed when adjusting the focus/zoom. For the details of each button, please refer to the Control bar of the Plug-in free viewer (page 20).

Note

If you click the buttons in this tab, in order to adjust the focus easily, the settings below are temporarily changed:

- **Privacy masking** and **Cropping** is deactivated.
- The current image focus position is superimposed.
- The alarm of **Motion detection** is deactivated.
- View-DR is turned on.

Adjusting the zoom

Click the **-500**, **-100**, **-10**, **+10**, **+100** or **+500** buttons to adjust the zoom position accordingly.

Note

The focus is moved slightly after adjusting; adjust the focus again, as necessary.

Adjusting the focus

Click **Start** button in **Easy Focus** to set the focus to the optimum position.

Note

The most suitable focus may not be available depending on imaging conditions. If so, click the **-20**, **-5**, **-1**, **+1**, **+5**, **+20** buttons to adjust the focus.

Picture Tab

You can set the color conditions, exposure, etc., of the camera.

Preview screen

Preview the image and adjust the picture setting. For details on each button, refer to the Control bar of the Plug-in free viewer (page 20).

View-DR

In high-contrast scenes such as against a back light, this function reduces overexposure and underexposure. Select **On** to turn on the View-DR function.

Note

When the View-DR function is on, exposure-related settings cannot be configured.

Visibility Enhancer

Using the Visibility Enhancer function will make the darker part of a camera image brighter as well as automatically correct brightness and contrast to show bright parts clearly without overexposure. When the Visibility Enhancer is **On**, select the correction level: **Low**, **Middle** or **High**. If you set it to **Off**, it will disable the Visibility Enhancer and activate the AGC function.

Note

When View-DR is **On**, the Visibility Enhancer is fixed to **On**.

Exposure

Adjust the settings of exposure.

Exposure compensation

Select the exposure correction value from the list box to adjust the target brightness for the automatic exposure setting.

A larger value brightens the image, and a smaller value darkens the image. Selectable values are as follows:

+2.0, +1.6, +1.3, +1.0, +0.6, +0.3, 0, -0.3, -0.6, -1.0, -1.3, -1.6, -2.0

Note

This cannot be selected when Visibility Enhancer is **On**.

AGC

Select the gain-controlled automatic exposure setting level: **Low**, **Middle** or **High**.

If you select **Off**, the automatic exposure setting by gain control is not performed.

Note

This cannot be selected when Visibility Enhancer is **On**.

Lens type (SNC-CH140 only)

Select the type of lens used.

Auto iris lens: Select this when the auto iris lens is used. This will turn on the iris-controlled automatic exposure function.

Manual iris lens: Select this when the fixed iris lens is used. This will not turn on the iris-controlled automatic exposure function.

Notes

- This cannot be selected when View-DR is **On**.
- If you select **Manual iris lens** while the auto iris lens is attached, the iris will be fixed to fully open.
- When the fixed iris lens is attached, selecting **Auto iris lens** will not activate the iris-controlled automatic exposure function.

Shutter speed

For SNC-CH140

Select the shutter speed control mode.

Auto: Auto-controlled shutter speed automatically sets the exposure.

Fixed: Select the shutter speed from list box. Selectable shutter speed values are as follows:

1, 1/2, 1/4, 1/8, 1/15, 1/30, 1/50, 1/60, 1/100, 1/250, 1/500, 1/1000, 1/2000, 1/4000, 1/10000 (sec.)

For SNC-DH140

Select the shutter speed from list box. Selectable shutter speed values are as follows:

1, 1/2, 1/4, 1/8, 1/15, 1/30, 1/50, 1/60, 1/100, 1/250, 1/500, 1/1000, 1/2000, 1/4000, 1/10000 (sec.)

Notes

- This cannot be selected when View-DR is **On**.
- For SNC-CH140, if the **Lens type** is set to **Auto iris lens**, the shutter speed control mode cannot be set to **Auto**.

Auto slow shutter

The automatic exposure setting including long term exposure is set to compensate for the brightness of a scene.

Select the minimum shutter speed in the long term exposure mode from the list box.

Selectable shutter speed values are as follows:

1, 1/2, 1/4, 1/8, 1/15 (sec.)

When **Off** is selected, the automatic exposure function cannot be set in the long term exposure mode.

Notes

- This cannot be selected when View-DR is **On**.
- If the shutter speed is 1, 1/2, 1/4, 1/8 or 1/15, this setting will be fixed to **Off**.

Tip

Depending on the setting, the range of Auto-controlled shutter speed is as follows

For SNC-CH140 (Shutter speed: Fixed) or SNC-DH140

- When Auto slow shutter is **Off**
Shutter speed is fixed to the value set in **Shutter speed**
- When Auto slow shutter is set except for **Off**
The range of shutter speed is from the value set in **Auto slow shutter** to the value set in **Shutter speed**.

For SNC-CH140 (Shutter speed: Auto)

- When Auto slow shutter is **Off**
The range of shutter speed is from 1/30 sec. to 1/10000 sec.
- When Auto slow shutter is set except for **Off**
The range of shutter speed is from the value set in **Auto slow shutter** to 1/10000 sec.

White balance

Select the White Balance mode.

ATW: Eliminating the influences caused by environmental illumination or lights, adjust the white balance automatically to reproduce original colors of the objects. (approximately 2000 K to 10000 K).

ATW-PRO: Automatically adjusts the color to be closest to the image you are viewing (approximately 3000 K to 7500 K).

Fluorescent lamp: Sets the white balance to that suitable for photography under three-band fluorescent lighting with a neutral white color.

Mercury lamp: Sets the white balance to that suitable for photography under a mercury lamp.

Sodium vapour lamp: Sets the white balance to that suitable for photography under a high-pressure sodium vapor lamp.

Metal halide lamp: Sets the white balance to that suitable for photography under a metal halide lamp.

White LED: Sets the white balance to that suitable for photography under the light of white LEDs.

One push WB: The **One push trigger** button becomes active. Click the button to adjust the white balance instantly.

Manual: When this option is selected, **R gain** and **B gain** become active. Selectable gain values are from 0 to 4095.

Note

When View-DR is **On**, **ATW-PRO** cannot be selected.

XDNR

Image noise can be reduced by using the XDNR function. The level can be selected among **High**, **Middle** and **Low**. Select **Off** to disable the function.

Brightness

Select the brightness in 11 steps, from **-5** to **+5**.
Selecting **+5** provides the brightest picture.

Saturation

Select the saturation in 7 steps, from **-3** to **+3**. Selecting **+3** provides the highest image saturation.

Sharpness

Select the sharpness in 7 steps, from **-3** to **+3**. Selecting **+3** provides the sharpest picture.

Contrast

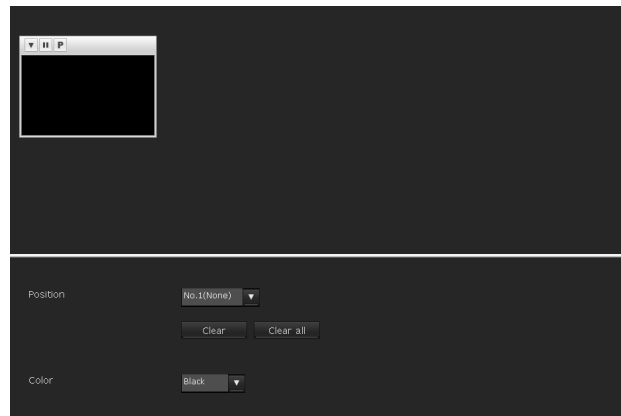
Select the contrast in 7 steps, from **-3** to **+3**. Selecting **+3** provides the highest contrast.

OK/Cancel

See “Buttons common to every menu” on page 26.

Privacy masking tab

Using the privacy masking enables you to hide images by masking specified parts of the images when streaming.



Preview screen

This screen is for monitoring images and configuring privacy masking.

For details on each button, refer to the Control bar of the Plug-in free viewer (page 20).

Position

Available to call out the privacy masks, delete them one by one or delete all at one time.

After completing the configuration, register by clicking **OK**.

Clear: Click the button to delete the privacy mask set.

All clear: Click the button to delete all privacy mask.

Color

Specify the color of privacy masks. This setting is common to every privacy mask.

The colors used are as follows:

Black, Gray1, Gray2, Gray3, Gray4, Gray5, Gray6, White, Red, Green, Blue, Cyan, Yellow, Magenta.

Setting a privacy mask

Operate according to the following procedure to set a privacy mask in the position of your choice:

- 1 Face the camera to the position where you want to set a privacy mask using the control button on the preview screen.
- 2 Specify the privacy mask area by dragging the mouse on the preview screen.
- 3 Select the number to register from the **Position** drop-down list.
- 4 Select the color of the mask from the **Color** drop-down list.

Note

The color is common to every privacy mask. The color selected last is applied.

- 5 Click **OK**.
The mask is displayed on the preview screen.

OK/Cancel

See “Buttons common to every menu” on page 26.

Day/Night Tab

Use this tab to set the day/night function of the camera.

Preview screen

This screen is for monitoring images and configuring day/night settings.

For details on each button, refer to the Control bar of the Plug-in free viewer (page 20).

Day/Night mode

Select the day/night mode from among four modes.

Auto: Normally works in day mode; switches automatically to night mode in a dark place.

Threshold: Set the brightness to **High** or **Low** when night mode is set.

Hold time: Set the reaction time of changes in brightness from **2 sec.** to **30 sec.**

Notes

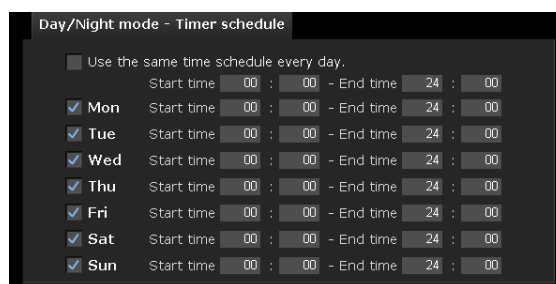
- If bright light is directed at the camera while it is in night mode it may cause hunting in the camera. In such cases, switch settings according to the lighting using the **Sensor** mode, or switch the Day/Night mode using the **Manual** mode.
- The day/night mode is not switched to night mode automatically when **Visibility Enhancer** and **AGC** are set to **Off** in the **Picture** tab.

Manual: Switch the day/night mode manually. When you select **Manual**, **On** and **Off** become active.

When you select **On**, the camera works in night mode. When you select **Off**, it works in day mode.

Timer: Normally the camera works in day mode. It switches to night mode at the time you set in the Schedule menu.

Click **Schedule** to display the setting menu for the effective period. (“Setting the Schedule — Schedule Menu” on page 72)



Sensor input: Controls the day/night mode by synchronizing it with the sensor input.

While a sensor input is detected, the camera works in night mode.

Easy Focus

When **Sync with Day/Night** is selected, Easy Focus will be activated once Day/Night mode switched, and the focus readjusted automatically.

For details on Easy Focus, refer to the “Focus tab — Adjusting the Focus (SNC-CH140 only)” (page 32) and “Focus/Zoom tab — Adjusting the focus/zoom (SNC-DH140 only)” (page 32).

Notes

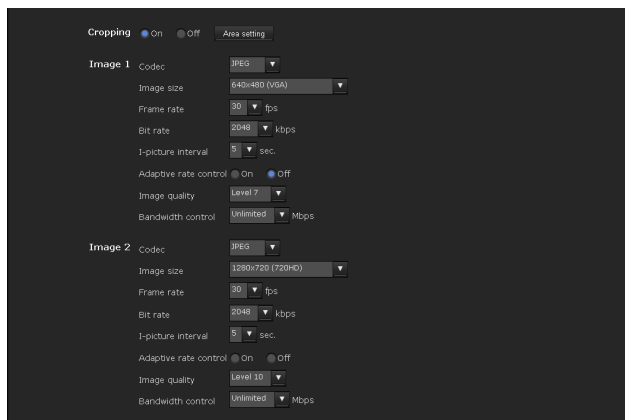
- When using Easy Focus, satisfactory focus may not be achieved.
- When using Easy Focus, the alarm of motion detection is deactivated.
- When using Day/Night link, confirm the focus condition under both Day and Night mode.

OK/Cancel

See “Buttons common to every menu” on page 26.

Video codec Tab

Use this tab to set the items for the video codec.



Cropping

You can crop a portion of the image and display the cropped image on the computer. Cropping reduces the transmitting data size and thus the network load, and a higher frame rate is achieved.

Select **On** to crop the image, or **Off**.

Note

Motion detection (page 73) operates for an image in the image size that is not cropped even if **Cropping** is set to **On**.

To crop an image

- 1 Set **Cropping** to **On** and click the **Area setting** button.
The area setting window appears.
- 2 Setting the trimming portion
Hold down the left button of the mouse on the still image and drag the cursor diagonally. The area in a red frame is the trimming portion.
- 3 Click **OK** at the bottom of the window.
The cropped image is displayed on the main viewer.
- 4 To close the image, click  in the upper-right corner.

Image 1 and Image 2

Up to two image codec modes can be set. Configure the following setting for each image mode.

Codec

Select **JPEG**, **MPEG4**, **H.264** or **Off**. Note that Image 1 cannot be set to **Off**.

Note

The selectable size of images and frame rate for Image 2 may be limited depend on the setting of codec type, size of images and/or frame rate for Image 1.

Image size

You can select the size of images sent from the camera. The selectable size of images are depend on the setting of maximum image size. For details on selecting maximum image size, refer to “Installation tab” in “System menu” in page 29.

When you set the different image size to Image 1 and Image 2, the available combinations are as follows:

Maximum image size [1280x720]

	Image 1	Image 2
1280 × 1024	×	×
1280 × 960	×	×
1280 × 800	×	×
1280 × 720	-	×
1024 × 768	×	×
1024 × 576	-	×
800 × 480	-	×
768 × 576	-	×
640 × 480	-	-
640 × 368	-	-
384 × 288	-	-
320 × 240	-	-
320 × 192	-	-

Maximum image size [1280x1024]

	Image 1	Image 2
1280 × 1024	-	×
1280 × 960	-	×
1280 × 800	-	×
1280 × 720	-	×
1024 × 768	-	×
1024 × 576	-	×
800 × 480	-	×
768 × 576	-	×
640 × 480	-	-
640 × 368	-	-
384 × 288	-	-
320 × 240	-	-
320 × 192	-	-

Frame rate

Set the frame rate of the image.

Selectable frame rates are as follows:

1, 2, 3, 4, 5, 6, 8, 10, 15, 20, 25, 30 (fps)

“fps” is a unit indicating the number of frames transmitted per second.

Configurable frame rates are as follows:

Image size (1280 × 1024)

	Image 1		Image 2	
	Codec	Frame rate (fps)	Codec	Frame rate (fps)
Single codec	H.264	20	-	-
	MPEG4	25	-	-
	JPEG	30	-	-
Dual codec	H.264	15	H.264	5
	H.264	15	JPEG	10
	H.264	15	MPEG4	8
	MPEG4	25	MPEG4	3
	MPEG4	25	JPEG	6
	JPEG	30	JPEG	10

Bit rate

Set the bit rate of MPEG4 or H.264 image transmission for a line. When the bit rate is set to a high level, better image quality can be enjoyed.

Selectable bit rates are as follows:

64, 128, 256, 384, 512, 768, 1024, 1536, 2048, 3072, 4096, 5120, 6144, 7168, 8192 (kbps)

I-picture interval

Set the I-picture insertion interval.

Adaptive rate control

This function adjusts the frame rate and the bit rate automatically so that the camera plays back a smooth image to suit the connected computer environment. If

On is selected, the MPEG4 or H.264 image rate is automatically adjusted.

Notes

- The actual frame rate and bit rate may be different depending on the image size, shooting scene, or network condition.
- When **Adaptive rate control** is set to **On**, the actual frame rate and bit rate change within the range that does not exceed the values set in **Frame rate** and **Bit rate**.

Image quality

Set the JPEG image quality.

Selectable values are from **Level 1** to **Level 10**.

When **Level 10** is selected, the best image quality is achieved.

Bandwidth control

Limits the network bandwidth for the JPEG image data output from the camera.

Note

Audio may be interrupted depending on the selected bandwidth. In this case, select a wider bandwidth.

OK/Cancel

See “Buttons common to every menu” on page 26.

Streaming Tab

Use this tab to set the items for the transmission by unicast or multicast.

Unicast streaming

Specify the transmission port numbers of the MPEG4/H.264 video data and audio data to be used when **UDP (Unicast)** is selected from the **Connection** drop-down list in the **Other** panel on the main viewer.

Video port number 1, 2

Specify the transmission port number of the MPEG4/H.264 video data. It is initially set to 50000. Specify an even number from 1024 to 65534. Two port numbers (the number specified here and an odd number with 1 added to the specified number) are actually used for video data communication and control.

The setting for Image 1 and Image 2 apply for Video port number 1 and 2 respectively.

Audio port number

Specify the transmission port number of the audio data. It is initially set to 50002. Specify an even number from 1024 to 65534. Two port numbers (the number specified here and an odd number with 1 added to the specified number) are used for audio data communication and control.

Note

Specify different numbers for the video port number and the audio port number.

Multicast streaming

Set whether the camera uses multicast streaming for MPEG4/H.264 video data and audio data or not. It reduces the transmission load on the camera by having a computer of the same segment network receive the same transmitting data.

Select **On** to allow, or **Off** not to allow multicast sending.

When you select **On**, set **Multicast address**, **Video port number** and **Audio port number** properly.

Multicast address

Type the multicast address used on the multicast streaming.

Video port number 1, 2

Specify the MPEG4/H.264 video transmission port number used for the multicast streaming. It is initially set to 60000. Specify an even number from 1024 to 65534. Two port numbers (the number specified here and an odd number with 1 added to the specified number) are used for video data communication and control.

The setting for Image 1 and Image 2 apply for Video port number 1 and 2 respectively.

Audio port number

Specify the audio transmission port number used for the multicast streaming. It is initially set to 60002. Specify an even number from 1024 to 65534. Two port numbers (the number specified here and an odd number with 1 added to the specified number) are used for audio data communication and control.

Note

Specify different numbers for the video port number and the audio port number.

OK/Cancel

See “Buttons common to every menu” on page 26.

Configuring the Network — Network Menu

When you click **Network** in the Administrator menu, the Network menu appears.

Use this menu to configure the network to connect the camera and the computer.

The Network menu consists of four tabs: **Network**, **Wireless**, **QoS** and **Dynamic IP address notification**.

Network Tab

This section provides the menus for connecting the camera through the network cable.

MAC address

Displays the MAC address of the camera.

Ethernet status

Displays the current transmission rate.

Auto-MDI/MDIX

According to the port of the connected Ethernet device, automatically switches the port of the unit between MDI and MDI-X for transmission.

Displays the Ethernet port mode of the unit.

IPv4 setting

Configure the IPv4 network setting.

IP address

Configure the IP address.

Obtain an IP address automatically (DHCP): Select this option when a DHCP server is installed on the network to allow IP address assignment. With this setting, the IP address is assigned automatically.

Use the following IP address: Select this option when you set a fixed IP address. With this setting, specify the **IP address**, **Subnet mask** and **Default gateway** manually.

Note

When you select **Obtain an IP address automatically (DHCP)**, make sure that a DHCP server is operating on the network.

IP address

Type the IP address of the camera.

Subnet mask

Type the subnet mask.

Default gateway

Type the default gateway.

DNS server

Configure the DNS server address.

Obtain DNS server address automatically: Select this option to obtain the IP address of DNS server automatically. It can be set only when **Obtain an IP address automatically (DHCP)** is selected in the Network tab.

Use the following DNS server address: Select this when you set a fixed address as the IP address of the DNS server. With this setting, specify the addresses on **Primary DNS server** and **Secondary DNS server** manually.

Note

When you select **Obtain DNS server address automatically**, make sure that a DHCP server is operating on the network.

Primary DNS server

Type the IP address of the primary DNS server.

Secondary DNS server

Type the IP address of the secondary DNS server, if necessary.

MTU

Enter the MTU value for the Ethernet port. (1000 - 1500)
If IPv6 is enabled, the value must be 1280 or greater.

Host name

Type the host name of the camera to be transmitted to the DHCP server. This setting is valid only when **Obtain an IP address automatically (DHCP)** is selected in the Network tab.

Domain suffix

Type the domain suffix of the camera to be transmitted to the DHCP server. This setting is valid only when **Obtain an IP address automatically (DHCP)** is selected in the Network tab.

Note

The domain suffix is sent to the DHCP server as FQDN (Fully Qualified Domain Name) information when **Host name** is set.

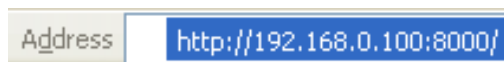
HTTP port number

Normally select **80**. If you want to use a port number other than 80, select the text box and type a port number between 1024 and 65535.

Note

When you have set the **HTTP port number** to a number other than 80 in the Network menu or in SNC toolbox, access the camera again by typing the IP address of the camera on your Web browser as follows:

Example: Setting port number 8000 when IP address is 192.168.0.100



IPv6 setting

Configure the IPv6 network settings.

IPv6 can be used simultaneously with IPv4.

Only IPv6-specific details are explained here. For common details, see “IPv4 setting” on page 38.

On/Off

To use IPv6, select **On**.

Prefix

Enter the Prefix value. (0 to 128)

IPv6 MTU

Enter the MTU value for IPv6. (1280 -1500)

The value must not exceed the MTU value for the Ethernet port.

OK/Cancel

See “Buttons common to every menu” on page 26.

Wireless Tab — Setting of wireless connection (SNC-CH140 only)

Insert the specified wireless card into the CF card slot of the camera, and set the items for connecting to the wireless network.

Before setting, read the operation manual and installation manual supplied with the wireless card together with this guide.

Verified wireless cards

- Sony Wireless Card SNCA-CFW5* sold separately.

* SNCA-CFW5 is not available in some countries and areas. For details, contact your authorized Sony dealer.

Notes

- Before inserting or removing the wireless card from the camera, turn off the power of the camera.

- The throughput of data transmission/reception via the network cable may decrease when the wireless card is in use.

MAC address

Displays the MAC address of the wireless card inserted in to the CF card slot.

If a wireless card is not inserted, “00:00:00:00:00:00” will be displayed.

IPv4 setting

Configure the IPv4 network setting.

IP address

Configure the IP address for a wireless network.

Obtain an IP address automatically (DHCP): Select this option when a DHCP server is installed on the network to allow IP address assignment. With this setting, the IP address is assigned automatically.

Use the following IP address: Select this option when you set a fixed IP address. With this setting, specify the **IP address**, **Subnet mask** and **Default gateway** manually.

Note

When you select **Obtain an IP address automatically (DHCP)**, make sure that a DHCP server is operating on the network.

IP address

Type the IP address of the camera.

Subnet mask

Type the subnet mask.

Default gateway

Type the default gateway.

DNS server

Configure the DNS server address.

Obtain DNS server address automatically: Select this option to obtain the address of the DNS server automatically. This can be set only when **Obtain an IP address automatically (DHCP)** is selected in the Wireless tab.

Use the following DNS server address: Select this option when you set a fixed address as the IP address of the DNS server. With this setting, specify the addresses on **Primary DNS server** and **Secondary DNS server** manually.

Note

When you select **Obtain DNS server address automatically**, make sure that a DHCP server is operating on the network.

Primary DNS server

Type the IP address of the primary DNS server.

Secondary DNS server

Type the IP address of the secondary DNS server, if necessary.

MTU

Enter the MTU value for wireless network. (1000 -1500)
If IPv6 is enabled, the value must be 1280 or greater.

Host name

Type the wireless network host name of the camera to be transmitted to the DHCP server. This setting is valid only when **Obtain an IP address automatically (DHCP)** is selected in the Wireless tab.

Domain suffix

Type the wireless network domain suffix of the camera to be transmitted to the DHCP server. This setting is valid only when **Obtain an IP address automatically (DHCP)** is selected in the Wireless tab.

Note

The domain suffix is sent to the DHCP server as FQDN (Fully Qualified Domain Name) information when **Host name** is set.

IPv6 setting

Configure the IPv6 network settings.

IPv6 can be used simultaneously with IPv4.

Only IPv6-specific details are explained here. For common details, see “IPv4 setting” on page 40.

On/Off

To use IPv6, select **On**.

Prefix

Enter the Prefix value. (0 to 128)

IPv6 MTU

Enter the MTU value for IPv6. (1280 - 1500)

The value must not exceed the MTU value for the wireless network.

Common setting

Type

Select the network connection type.

Ad hoc mode: Select this when connecting to a computer directly. With this setting, specify a wireless channel.

Infrastructure mode: Select this when connecting to a computer via an access point or wireless router.

Notes

- The setting of the HTTP port number is common to the setting in the Network tab.
- With **Ad hoc mode**, you cannot select **Use WEP key automatically generated** of **WEP**, or **WPA** or **WPA2** on **Security**.
- When you set **Security** to **WPA** or **WPA2** and change **Infrastructure mode** to **Ad hoc mode**, **Security** setting is automatically changed to **None**.

Antenna

Select one of the following antenna settings when you use the SNCA-CFW5 wireless card (optional), or the SNCA-AN1 wireless LAN antenna (optional).

Internal: Select this when you perform communications using the antenna built in to the wireless card. This setting is suitable for short-range and omnidirectional communications.

External: Select this when you perform long-range communications using the SNCA-AN1 wireless LAN antenna connected to the wireless card.

Diversity: Select this when you perform both short-range and long-range communications using the SNCA-AN1 wireless LAN antenna connected to the wireless card. The antenna of higher sensitivity is selected automatically.

Note

When you are using SNCA-CFW5 and select **Diversity**, SNCA-AN1 is selected on the transmitting side and an antenna is selected automatically on the receiving side.

SSID

Type the ID to identify the wireless network you want to access using up to 32 ASCII alphanumeric characters. For your security, be sure to change the factory setting.

Security

Configure wireless network security.

None: Select this option when no security is set.

Note

This setting is not recommended for reasons of protecting your computer from harm.

WEP: Select this option when WEP (Wired Equivalent Privacy) security method is used.

WPA: Select this option when WPA (Wi-Fi Protected Access) security method is used.

WPA2: Select this option when WPA2 security method is used.

Easy setting: Select this option when you use **Easy setting**.

WEP

Set up this item when **WEP** is selected on **Security**.

Use WEP key automatically generated

Checking this box allows you to use an automatically generated WEP key. Uncheck the box when you enter a WEP key manually.

To use the automatically generated WEP key, you need to enable the 802.1X (wireless) function. After checking this box, click **OK** at the bottom of the window. The 802.1X function is enabled.

Note

For correct operation of the 802.1X function, you need to configure the 802.1X settings, such as certificate setting, appropriately. For details on the 802.1X settings, see “Using the 802.1X Authentication Function — 802.1X Menu” on page 51.

802.1X

This button is active when **Use WEP key automatically generated** is selected.

When you click **802.1X**, the 802.1X menu appears, allowing you to configure the 802.1X (wireless) function.

WEP key

Type and select the WEP key information. This section is active when **Use WEP key automatically generated** is not selected.

Up to 4 WEP keys can be set in the following manner.

- 1 Select one of the WEP key numbers.
- 2 Type the same information in the **WEP key** and **Retype WEP key** text boxes.
The length of a WEP key is 40 or 104 bit. A 104-bit WEP key has a higher security level than a 40-bit key.
You can type the WEP key either in hexadecimal numbers (0 to 9 and A to F) or ASCII characters (alphanumeric). In hexadecimal, type 10 characters

for a 40-bit key, or 26 characters for a 104-bit key. In ASCII, type 5 characters for a 40-bit key, or 13 characters for a 104-bit key.

When **Type** is set to **Infrastructure mode**, the WEP key should be the same as that of the access point. When **Type** is set to **Ad hoc mode**, the WEP key should be the same as that of the communication client.

WPA/WPA2

Set up this item when **WPA** or **WPA2** is selected on **Security**.

WPA and WPA2 use TKIP and AES encryption systems. This unit supports TKIP for WPA, and AES for WPA2.

Authentication

Select the authentication method.

PSK: Select for PSK authentication. When this option is selected, **Passphrase** setting is required.

EAP: Select for EAP authentication. When this option is selected, enabling the 802.1X (wireless) function is required. After selecting **EAP**, click **OK** at the bottom of the window. The 802.1X function is enabled.

Note

For correct operation of the 802.1X function, you need to configure the 802.1X settings, such as certificate setting, appropriately. For details on the 802.1X settings, see “Using the 802.1X Authentication Function — 802.1X Menu” on page 51.

802.1X

This button is active when **EAP** is selected on **Authentication**.

When you click **802.1X**, the 802.1X menu appears, allowing you to configure the 802.1X (wireless) function.

Passphrase

Set a passphrase when **PSK** is selected on **Authentication**.

Type 8 to 63 ASCII characters (alphanumeric), or up to 64 hexadecimal digits (0 to 9 and A to F).

Re-type passphrase

To confirm the passphrase, retype the passphrase that you typed in the **Passphrase** box.

Easy setting

Set up this item when **Easy setting** is selected on **Security**.

You can easily connect to an access point compatible with WPS.

Note

This function is available only for some models.

OK/Cancel

See “Buttons common to every menu” on page 26.

QoS Tab

In this tab, you can mark the data traffic packets sent from the device and configure the settings for QoS control. Rules for the types of data traffic can be created using IPv4/IPv6 address, port number, protocol, etc. A maximum of 10 rules can be registered for IPv4 and IPv6, respectively.

The screenshot shows two sections for QoS configuration: IPv4 QoS and IPv6 QoS. Each section has a toggle switch (On/Off) and a table for rules. The IPv4 QoS section has a table with columns: No., Network address, Subnet, Port, Protocol, and DSCP. The IPv6 QoS section has a table with columns: No., Network address, Prefix, Port, Protocol, and DSCP. Both sections have buttons for Set, Delete, Up, and Down.

IPv4 QoS

Select **On** to configure the QoS setting for IPv4.

Rule

Used to register, edit and delete QoS.

No.

Select the number to use when registering on the QoS table.

When you select a registered number, the registered QoS information is displayed.

Network address

Enter the network address of the target on which to perform QoS.

Subnet

Enter the subnet mask values of the target on which to perform QoS.

Tip

The subnet mask value represents the number of bits from the left side of the network address.

Port

Enter the port number for the data traffic of the device (e.g. HTTP:80).

Protocol

Select the protocol.

DSCP

Set a value to mark the data traffic (0 ~ 63).
This value is set in the DSCP field included in the IP header of the data traffic.

Set

Used when registering on the QoS table.
QoS is set according to the following procedure:

- 1** Select No. from **No.** and enter the necessary conditions for **Network address**, **Subnet**, **Protocol** and/or **Port No.**
- 2** Enter values in **DSCP**.
- 3** Click **Set** and configure the QoS.

Delete

select **No.** to delete the setting and click **Delete**.

Up

Increases the priority of the rule.
Select a rule from the QoS table to prioritize and click **Up**.

Down

Decreases the priority of the rule.
Select a rule from the QoS table to lower its priority and click **Down**.

QoS table

Displays the list of registered QoS information. If multiple conditions match, the rule with the smallest number has priority.

IPv6 QoS

Select **On** to configure the QoS setting for IPv6.

Rule

Used to register, edit and delete QoS.

No.

Select the number to use when registering on the QoS table.

When you select a registered number, the registered QoS information is displayed.

Network address

Enter the network address of the target on which to perform QoS.

Prefix

Enter the prefix value of the target on which to perform QoS.

Tip

The prefix value represents the number of bits from the left side of the network address.

Port

Enter the port number for the data traffic of the device (e.g. HTTP:80).

Protocol

Select the protocol.

DSCP

Set a value to mark the data traffic (0 ~ 63).
This value is set in the DSCP field included in the IP header of the data traffic.

Set

Used when registering on the QoS table.
QoS is set according to the following procedure:

- 1** Select the number you want to register from **No.** and enter the necessary conditions for **Network address**, **Subnet**, **Protocol** and **Port No.**
- 2** Enter values in **DSCP**.
- 3** Click **Set** and configure the QoS.

Delete

select **No.** to delete the setting and click **Delete**.

Up

Increases the priority of the rule.
Select a rule from the QoS table to prioritize and click **Up**.

Down

Decreases the priority of the rule.
Select a rule from the QoS table to lower its priority and click **Down**.

QoS table

Displays the list of registered QoS information. If multiple conditions match, the rule with the smallest number has priority.

Tip

To attain QoS of data traffic, the target device must be connected to a router or switch that supports the QoS function.

OK/Cancel

See “Buttons common to every menu” on page 26.

Dynamic IP address notification Tab — Notifying the IP Address

When **Obtain an IP address automatically (DHCP)** is selected in the Network tab or Wireless tab, you can send notification of completion of the network settings using the SMTP or HTTP protocol.

e-Mail (SMTP) notification

Select **On** to send an e-mail when the DHCP setting is completed.

SMTP server name

Type the name or IP address of the SMTP server for sending an e-mail, using up to 64 characters.

SMTP port number

Enter a port number from 25 to 65535.

The standard port number is 25. If TLS is enabled, the standard port number for SMTPs is 465.

Use TLS

To use the encryption function by TLS, set to **On**.

Note

The model on sale in China does not support the TLS function.

STARTTLS

To use the encryption function by STARTTLS, set to **On**.

Note

The model on sale in China does not support the STARTTLS function.

Authentication

Select the authentication required when you send an e-mail.

Off: Select if no authentication is required when an e-mail is sent.

On: Select if authentication is required when an e-mail is sent. Select one of the authentication methods from the following and specify the **POP server name**, **User name** and **Password** as required.

SMTP: Select when SMTP authentication is required.

POP before SMTP: Select when POP before SMTP authentication is required.

Note

When you set **Authentication** to **On**, make sure to select either or both **SMTP** or/and **POP before SMTP**.

POP mode

Select POP3 or APOP as the authentication method for POP authentication.

Note

The model on sale in China does not support the APOP authentication.

Wait time after POP

Set the waiting time in **POP before SMTP** before SMTP authentication after POP authentication is completed. Timeout can be set from 0 to 10,000 msec.

POP server name

It is necessary when **POP before SMTP** is selected for **Authentication**.

Type the POP (receiving mail) server name, using up to 64 characters. Or type the IP address of the POP server. This setting is necessary when the SMTP server that sends e-mails performs authentication using the POP user account.

POP port number

Enter a port number from 110 to 65535.

The standard port number is 110. If TLS is enabled, the standard port number for POP3s is 995.

Authentication mode

Select **Login** or **CRAM-MD5** as the authentication method for SMTP authentication.

Note

The model on sale in China does not support the CRAM-MD5 authentication.

User name, Password

Type the user name and password of the owner of the mail account, using up to 64 characters. This setting is necessary when the SMTP server that sends e-mails performs authentication.

Recipient e-mail address

Type the recipient e-mail address, using up to 64 characters. You can specify only one recipient e-mail address.

Administrator e-mail address

Type the e-mail address of the camera administrator, using up to 64 characters. This is used as the reply address or the address for a system mail from the mail server.

Subject

Type the subject/title of the e-mail, using up to 64 characters.

Message

Type the text of the e-mail using up to 384 characters. (A line break is equivalent to 2 characters.) You can describe the information of the acquired IP address, etc., using the special tags mentioned below.

HTTP notification

Select **On** to output a command to the HTTP server when the DHCP setting is completed. Using this function, you can configure a useful system, for example, to view the access log stored in the HTTP server, or start an external CGI program.

URL

Specify the URL to send an HTTP request, using up to 256 characters. The URL is normally written as follows:

`http://ip_address[:port]/path?parameter`

ip_address: Type the IP address or host name of the host to which you want to connect.
To enter an IPv6 address:

`http:// [IPv6 address]`

`http:// [IPv6 address]: port`

[:port]: Specify the port number to which you want to connect. If you want to use the established port number 80, you do not need to input a value.

path: Type the command.

parameter: Type the command parameter if necessary. You can use the special tags mentioned below for the parameters.

Proxy server name

When you send an HTTP request via a proxy server, type the name or IP address of the proxy server, using up to 64 characters.

Proxy port number

Specify the port number when you send an HTTP request via the proxy server. Set a port number between 1024 and 65535.

Method

Select the HTTP method **GET** or **POST**.

OK/Cancel

See “Buttons common to every menu” on page 26.

About the special tags

You can use the following five special tags to allow notification of the settings acquired by DHCP, such as an IP address. Type the tags in the parameter section of the URL that you described in the Message field of the HTTP.

<IP>

Use this tag to embed the IP address acquired by DHCP in the text or parameter.

<HTTPPORT>

Use this tag to embed the specified HTTP server port number in the text or parameters.

<MACADDRESS>

Use this tag to embed the MAC address of the interface, whose IP address was acquired by DHCP, in the text or parameter.

<MODELNAME>

Use this tag to embed the camera’s model name in the text or parameter.

<SERIAL>

Use this tag to embed the camera’s serial number in the text or parameter.

Setting the SSL function — SSL Menu

When you click **SSL** in the Administrator menu, the SSL menu appears.
Use this menu to configure the SSL or TLS function. (called “SSL” hereafter)
The settings allows the camera to communicate with the client PC by using SSL.

Notes

- The model on sale in China does not support the SSL function.
- When using the SSL function, always configure the settings after setting the date and time of the camera. If the date and time are not correctly set, it may cause browser connection problems.

SSL tab

SSL function

On: Select this to use the SSL function. When **Allow HTTP connection for some clients** is selected, both HTTP and SSL connections are allowed. When **Allow HTTP connection for some clients** is not selected, only SSL connection is allowed.

When Microsoft Internet Explorer Ver.6.0 is used

When SSL session is established, appears in the status bar on your web browser.

When Microsoft Internet Explorer Ver.7.0 is used

When SSL session is established, appears in the right of the address bar on your web browser.

Off: Select this to not use the SSL function. Only HTTP connection is allowed with the camera.

When you use SSL connection for the first time

When you use SSL connection only with the SSL function **On**, you cannot access the camera if the SSL function does not work properly.

In this case, you must reset the camera to the factory settings. (All settings will be initialized.)
To avoid this, check that SSL connection is possible by performing the following steps.

- 1 Set the SSL function to **On**, and select **Allow HTTP connection for some clients**.
- 2 Click **OK** to close the main viewer and the setting window.
- 3 Display the main viewer in SSL connection. Refer to “Using the SSL function” on page 13 for connection.
- 4 After checking that SSL connection is possible, cancel **Allow HTTP connection for some clients** selected in step 1.

Even if the setting window or the browser is closed as SSL connection is impossible, http connection will be possible if **Allow HTTP connection for some clients** is selected. First check the setting contents of SSL tab in http connection, then check the SSL connection again.

If **Allow HTTP connection for some clients** is not selected, you will not be able to access the camera if SSL connection becomes impossible. In this case, turn on the power of the main unit while pressing the reset switch on the camera to initialize. For details, refer to the supplied Installation Manual.

Note

SSL connection will load the camera down; therefore, not all images may be downloaded, and the mark may appear when the camera accesses the setting window from the browser. In this case, reload the window. Press the F5 key on the keyboard to reload.

Certificate options

Select an installation mode of the certificate.

Use an external certificate: Uses the certificate including private key information issued by a CA. The PKCS#12 and PEM formats are supported.

Note

Even if the SSL function is set to **On**, it is not active in the following cases:

- When **Use an external certificate** is selected in “Certificate options,” and also when the certificate and the private key password are not set properly.

Use a self-signed certificate (For test use): This mode uses the certificate and private key pair generated by “Generating a self-signed certificate” on page 47. Private key information corresponding to the certificate is stored in the camera. You do not need to install an external certificate. However, you cannot execute the existence proof that is one of the SSL functions for the following reasons.

- The private key generated in the camera is self-signed by the camera.
- A prepared value is set for a distinguished name (Common name, etc).
- The certificate is not issued by a trusted CA.

For reasons of security, we recommend using this mode only when there is no problem even if perfect security is not saved.

Notes

- When **Use a self-signed certificate (For test use)** is selected, the **Security Alert** dialog appears on the SSL connection with a browser. For details, refer to “Using the SSL function” (page 13).
- SSL connection may be impossible due to the type of certificate installed in the camera. In this case, refer to “How to install the CA certificate” on page 49 and install.

Certificates

Import, display or delete the certificate.

To import the certificate

Click **Browse...** to select the certificate to be imported. Click **Submit** to import the certificate, and the selected file to the camera.

Note

The import process becomes invalid if the selected file is not a certificate or the imported certificate is not allowed.

Generating a self-signed certificate

A self-signed certificate can be generated in the camera to be used when **Use a self-signed certificate (For test use)** is selected from **Certificate options**.

Click **Generate** to generate a self-signed certificate in the camera. Clicking **Generate** again after **Generate** has been clicked once will update the self-signed certificate stored in the camera.

Note

Make sure to set the date and time on the camera correctly before performing this operation. If the date and time are not correctly set, it may cause browser connection problems.

To display certificate information

When the certificate has been set in the camera correctly, its information appears on **Status**, **Issuer DN**, **Subject DN**, **Validity Period** and **Extended Key Usage**.

Status

Shows if the status of the certificate is valid or invalid. The following statuses are recognised.

Valid: The certificate is correctly stored and set.

Invalid: The certificate is not correctly stored and set.

Possible causes are as follows:

- **Use an external certificate** is selected and the private key password included in the certificate is not specified correctly.
- **Use an external certificate** is selected and the private key password is specified in spite of the fact that the key pair in the certificate is not encrypted.
- **Use an external certificate** is selected and the key pair is not included in the certificate.
- **Use a self-signed certificate (For test use)** is selected without the self-signed certificate being generated.

Note

When the certificate to be imported is of PKCS#12 format and the private key password is not set correctly, <Put correct private key password> is displayed in the boxes of **Issuer DN**, **Subject DN**, **Validity Period** and **Extended Key Usage**. Specify the correct private key password to confirm the information of the certificate.

To delete the imported certificate or self-signed certificate

Click **Delete** to delete the certificate or self-signed certificate imported to the camera.

Private key password

Type the password for the private key information included in the certificate using up to 50 characters. This text box is active only when **Certificate options** is set to **Use an external certificate**.

Leave the text box blank if the private key information included in the certificate is not encrypted.

If no private key password is set in the camera, an active text field is displayed and this allows a password to be entered.

If a private key password is already set, it is displayed as an inactive text field.

Reset

To change the private key password, click this button. The current password is cleared and the password text box becomes active to allow a new password entry.

Note

Click **Cancel** at the bottom of the menu if you want to cancel changing the private key password after clicking **Reset**. Doing so restores the other setting items in the Client certificate tab to the previous settings.

OK/Cancel

See “Buttons common to every menu” on page 26.

Note

When you click **OK** after changing SSL setting, close the main viewer and the setting window once.

CA certificate tab — Adding the CA certificate for client authentication

In this tab, you can manage the CA certificate needed for the camera to use the client authentication of the SSL function.

Note

When using the client authentication, the personal certificate must be successfully installed on the PC to use it. If this preparation cannot be performed, do not configure settings on this tab. Otherwise, you may not be able to connect to the camera.

SSL client authentication

You can configure whether to enable the client authentication of the SSL function.

Trusted CA certificate 1 to 4

You can import a trusted CA certificate (route certificate, etc.) to the camera.

Up to four certificates from trusted CAs can be imported to the camera. Only PEM format is supported.

To import the CA certificate

- 1 Click **Browse...** to select the CA certificate to be saved in the camera.
- 2 Click **Submit**
The selected file will be imported to the camera.

Note

Import process will be invalid if the selected file is not a CA certificate.

To display the information of the CA certificate

When the CA certificate has been saved in the camera correctly, its information appears on **Issuer DN**, **Subject DN**, **Validity Period**, and **Extended Key Usage** for your reference.

To delete the CA certificate

Click **Delete** to delete the selected CA certificate from the camera.

Tip

To enable a client certificate, it is recommended that the settings are configured following the procedure below:

- ① **Import the necessary CA certificate.**
- ② **Set SSL client authentication to On and click OK.**

Note

When you set SSL client authentication to **On** and click **OK**, the camera will immediately operate to enable client authentication. Make sure that the personal certificate on your PC is successfully installed.

OK/Cancel

See “Buttons common to every menu” on page 26

How to install the CA certificate

The camera may not be connected because the browser (Internet Explorer) does not display whether the certificate will be accepted or not due to the type of certificate. In this case, install the CA certificate as follows.

- 1 Save in the PC the certificate of CA which has signed the certificate to be installed in the camera. The extension of the certificate file is normally “.cer.” Double-click this file. The following **Certificate** dialog appears.



- 2 Click **Installation Certificate...**. The **Certificate Import Wizard** appears.



- 3 Click **Next**.



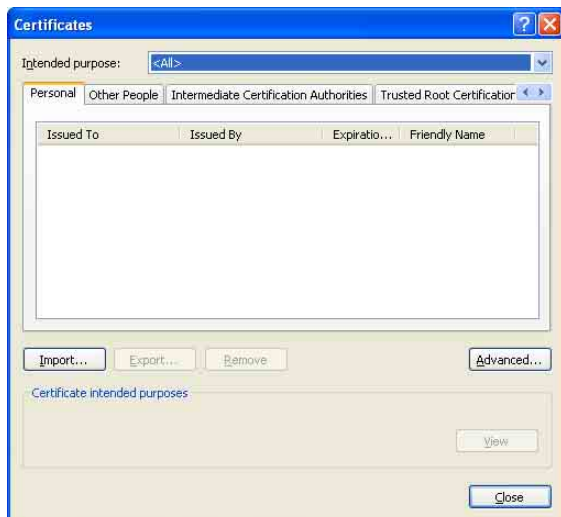
- 4 Select **Automatically selects the certificate store based on the type of certificate** and click **Next**. Completing the Certificate Import Wizard appears.



- 5 Check the contents, then click **Finish**. The CA certificate will be installed.

To remove an installed CA certificate

- 1 In Internet Explorer, click in the order **Tools**, **Internet options**, **Content tab** and **Certificates**. The **Certificates** dialog appears.



- 2 Select the certificate you want to remove. The CA certificate is usually stored in **Trusted Root Certification Authorities**.
- 3 Click **Remove**. **Do you want to delete the certificate** appears to confirm.
- 4 Click **Yes**. The certificate will be removed. There may be a case that a certificate cannot be removed by the steps above due to the type of certificate. Check the installation condition and remove it following the steps below.

Note

You need to log in as Administrator to perform these steps.

- 1 Open **Run...** of the Windows menu, then enter **mmc** and click **OK**.
- 2 Select **File** in the **Console 1** window and **Add/Remove Snap-in...** (when Windows XP Professional is used) **Add/Remove Snap-in...** dialog appears.
- 3 Click **Add** to display **Add Stand-alone Snap-in** dialog. You need to follow this step if using Windows XP Professional.

- 4 Select **Certificates** from the list, then click **Add**. **Certificate Snap-in** is displayed.
- 5 Select **Computer account** as the certificate administrated in this Snap-in, then click **Next**.
- 6 Select **Local Computer** as the computer administrated in this Snap-in, then click **Finish**.
- 7 Close **Add Standalone Snap-in** (for Windows XP Professional only) and **Add/Remove Snap-in...** dialogs. The items for administrating **Certificates** appears in the **Console Route** window. Confirm the relevant certificate, then remove it.

Using the 802.1X Authentication Function

— 802.1X Menu

When you click **802.1X** in the Administrator menu, the 802.1X menu appears.

Use this menu to configure the wired or wireless port-based authentication in compliance with the 802.1X standard.

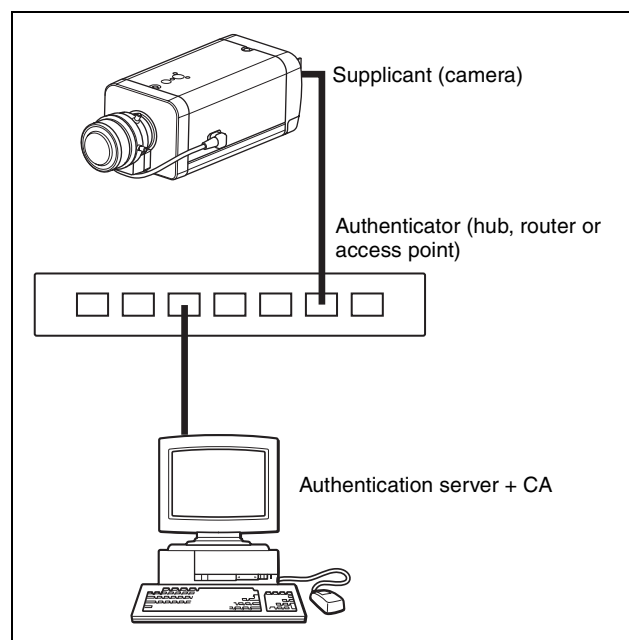
The 802.1X menu consists of three tabs: **Common**, **Client certificate** and **CA certificate**.

Notes

- To use the 802.1X authentication function, you need knowledge of the 802.1X authentication (WPA and WPA2) and digital certificate. To establish an 802.1X network, you need to configure the authenticator, access point, authentication server and other elements. For details on these settings, refer to the manual of the corresponding equipment.
- When using the 802.1X authentication function, always configure the settings after setting the date and time of the camera. If the date and time are incorrect, port authentication may not be performed correctly.

System configuration of 802.1X network

The following figure shows a general system configuration of an 802.1X network.



Supplicant

A supplicant is a device that connects to the authentication server to join the network. This camera serves as a supplicant in the 802.1X network. The supplicant can enter the 802.1X network after appropriate authentication by the authentication server.

Authenticator

An authenticator forwards certificate request data or response data that the supplicant or authentication server issues to the other party. Normally a hub, router or access point serves as an authenticator.

Authentication server

An authentication server has a database of connecting users and verifies if the supplicant is a valid user or not. It can also be called RADIUS server.

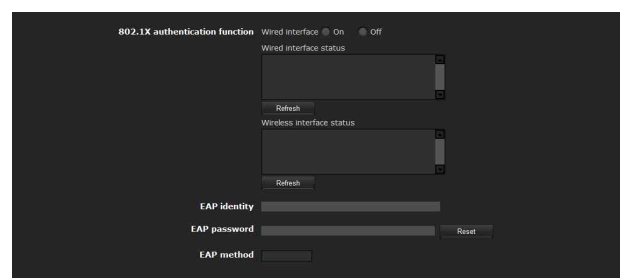
CA (Certificate Authority)

A CA issues and manages certificates of the authentication server (CA certificates) and user certificates. The CA is essential for certificate-based user authentication. Normally a CA is located inside an authentication server.

Note

This camera supports EAP mode in which the supplicant and the server authenticate using the certificate. This mode requires a CA to issue the certificate.

Common Tab – Basic setting of 802.1X authentication function



802.1X authentication function

This item is used for enabling/disabling the 802.1X authentication function for wired ports. The wired interface status and the wireless interface status can also be checked here.

Note

To use the 802.1X authentication function for wireless networks, set up **Security** in the Wireless tab of the Network menu. For details, see “Security” on page 41.

Wired interface

To activate the 802.1X authentication function for wired ports, select **On**.

Wired interface status

Shows the authentication status of the 802.1X authentication function for wired ports.

Click **Refresh** to update the status.

Wireless interface status (SNC-CH140 only)

Shows the authentication status of the 802.1X authentication function for wireless networks.

Click **Refresh** to update the status.

EAP identity

Type the user name to identify the client in the 802.1X authentication server using 3 to 253 characters.

EAP password

A supplicant EAP password is needed to be inputted when PEAP is selected with EAP condition. The password can contain half-width letters and the length should be between 1 to 50.

Reset

To change the once set EAP password, click **Reset** and clear the current password. A new password can be entered.

Note

After you click **Reset**, if you wish to cancel the EAP password change, click **Cancel** at the bottom of the screen. This will cancel other changes made to the settings.

EAP method

You can select the authentication method used with the authentication server. This device supports TLS and PEAP.

TLS: By this method, the supplicant and the server authenticate each other using a certificate. This enables secure port authentication.

PEAP: By this method, an EAP password is used for the supplicant authentication and a certificate is used for server authentication.

OK/Cancel

See “Buttons common to every menu” on page 26.

Client certificate Tab

When TLS is selected as the EAP method, client certificate is imported for authentication at the camera.

Client certificate request

Import, display or delete the client certificate.

To import the client certificate

Click **Browse...** to select the client certificate to be imported.

Then click **Submit**, and the selected file will be imported to the camera.

Note

The import process becomes invalid if the selected file is not a client certificate or the imported client certificate is not allowed.

To display the information of the client certificate

When the client certificate has been saved in the camera correctly, its information appears on **Status**, **Issuer DN**, **Subject DN**, **Validity Period** and **Extended Key Usage**.

Status: Shows if the status of the client certificate is valid or invalid.

Valid means the client certificate is correctly stored and set.

Invalid means the client certificate is not correctly stored and set.

Possible causes of **Invalid** are as follows:

- The private key password included in the client certificate is not specified correctly.
- The private key password is specified in spite of the fact that the key pair in the client certificate is not encrypted.
- The key pair is not included in the client certificate.

Note

When the client certificate to be imported is of PKCS#12 format and the private key password is not set correctly, “<Put correct private key password>” is displayed in the boxes of **Issuer DN**, **Subject DN**, **Validity Period** and **Extended Key Usage**. Specify the correct private key password to confirm the information of the certificate.

To delete the client certificate

Click **Delete**, and the client certificate stored in the camera will be deleted.

Private key password

Type the password for the private key information included in the client certificate using up to 50 characters.

Leave the text box blank if the private key information included in the client certificate is not encrypted.

If no private key password is set in the camera, the text box is activated to allow entering of a password.

If a private key password is already set, it is displayed as turned letters.

Reset

To change the private key password, click this button. The current password is cleared and the password text box is activated to allow new password entry.

Note

Click **Cancel** at the bottom of the menu if you want to cancel changing the private key password after clicking **Reset**. Doing so restores the other setting items in the Client certificate tab to their previous settings.

OK/Cancel

See “Buttons common to every menu” on page 26.

CA certificate Tab

You can import a trusted CA certificate (server certificate or route certificate) to the camera. Up to four certificates from trusted CAs can be imported to the camera. Only the PEM format is supported.

The screenshot shows a dark-themed interface for managing CA certificates. It contains four identical sections, each for a 'Trusted CA certificate' (numbered 1 to 4). Each section has four text input fields: 'Issuer DN', 'Subject DN', 'Validity Period', and 'Extended Key Usage'. Below these fields are three buttons: 'Delete', 'Import', and 'Browse...'. At the bottom of each section is a 'Submit' button. The 'Import' button is disabled, and the 'Browse...' button is active.

To import the CA certificate

Click **Browse...** to select the CA certificate to be imported.

Then click **Submit**, and the selected file will be imported to the camera.

Note

Import process becomes invalid if the selected file is not a CA certificate.

To display the information of the CA certificate

When the CA certificate has been saved in the camera correctly, its information appears on **Issuer DN**, **Subject DN**, **Validity Period** and **Extended Key Usage**.

To delete the CA certificate

Click **Delete**, and the CA certificate stored in the camera will be deleted.

Setting the 802.1X authentication function – Example of Windows Server 2003

This section explains how to configure the authentication server and CA using Microsoft Windows Server 2003.

Note

As this section describes authentication based on the user interface in English on Windows Server 2003, the UI terminology and page configuration may be different depending on the version of the Operating System or Service Pack and patch update status.

Before setting

Perform the following settings before configuring an 802.1X network.

Active Directory (domain controller)

The following setting example is based on the assumption that the Active Directory has been configured.

Windows IAS configuration

Configure **Remote access/VPN server** in **Manage Your Server** of Windows Server 2003. Open **Add or Remove Programs** from **Control Panel** of Windows menu. Install **Internet Authentication Service** in **Add/Remove Windows Components**.

CA configuration

To configure the CA, perform the following steps:

- 1 Open **Add or Remove Programs** from **Control Panel** of the Windows menu.
- 2 Select **Add/Remove Windows Components**.
- 3 Add **Certificate Services** in the Component menu.
- 4 Select **Enterprise root CA** on **CA Type**.
- 5 Type the CA name on **Common Name for this CA**, and configure the CA.

Creating a security group for Active Directory

- 1 Open **Active Directory Users and Computers** from **Administrative Tools** of the Windows menu.
- 2 Select **Users** of the domain with which you want to perform 802.1X connection.

- 3 Select **New** from the context menu, then select **Group** and configure the group for 802.1X connection.
For example, the group “Wired_802.1X_Group” is assumed for explanation purposes.

Configuring the Internet Authentication Service

- 1 Open **Internet Authentication Service** from **Administrative Tools** of the Windows menu.
- 2 Click **Register Server in Active Directory** on the operation menu.
- 3 Read the displayed precautions carefully and click **OK** to accept them.

Then, continue to configure the EAP-TLS policy.

- 4 Select **Remote Access Policy** and right-click.
- 5 Select **New** from the context menu, and select **Remote Access Policy** to open “New Remote Access Policy Wizard.”
- 6 Select **Set up a custom policy**.
- 7 Set the following items:
Policy name: Type “Allow 802.1X Access” as an example.
Policy conditions: Click **Add** and add the following items:
– NAS Port-Type: Ethernet, Wireless-IEEE802.11, Wireless-Other and Virtual (VPN)
– Windows-Groups: Wired_802.1X_Group
Permissions: Select **Grant remote access permission**.
Edit Profile:
– Dial-in Constraints tab: Specify the session time out period during which the client is allowed to be connected, as required.
– Authentication tab: Delete checks from all the boxes. Click **EAP Method** and add **Smart Card or other certificates**.

Then, continue to configure the RADIUS client.

- 8 Select **RADIUS Clients** and right-click.
- 9 Select **New RADIUS Client** from the context menu.

- 10 Set the following items:
Friendly name: Type “authenticator” as an example.
Client address (IP or DNS): IP address of the authenticator
Client-Vender: RADIUS Standard
Shared secret: Specify the shared secret to be set in the authenticator.

Adding a user

- 1 Open **Active Directory Users and Computers** from **Administrative Tools** of Windows menu.
- 2 Select **Users** of the domain with which you want to add a user and right-click.
- 3 Select **New** from the context menu, then select **User**.
- 4 Set the following items to configure a new user:
 For example, the log-on user name “1XClient” is assumed for explanation purposes.
First name: 1XClient
User logon name: 1XClient@<domain name>
Password: Specify a password. Then select **Password never expires** in account options.
- 5 Select the user to be added and right-click.
- 6 Select **Properties** from the context menu.
- 7 Set the following items:
Dial-in tab: Select **Allow access in Remote Access Permission (Dial-in or VPN)**
Member Of tab: Add “Wired_802.1X_Group.”

The preparations for configuring a 802.1X network are now completed.
 Proceed to issue the certificate to be imported to the camera.

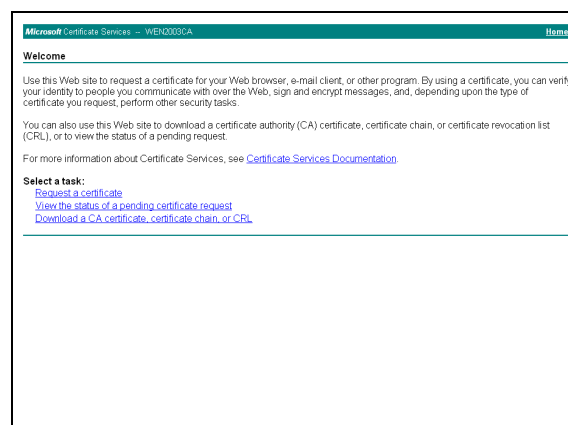
Issuing the CA certificate

Prepare a Windows client PC (called “client PC” hereafter) to temporarily store the certificate, and configure so that the client PC and Windows Server 2003 computer can be connected through the network.

- 1 Start Internet Explorer on the client PC.
- 2 Type the CA’s URL in the address bar, and click **Go To**.
 The CA’s URL is normally as follows:

http://<address of the CA>/CertSrv/

The “Microsoft Certificate Services” page opens.



Note

If the Microsoft Certificate Service page does not appear using the URL above, check the following:

- Is the service of Web site enabled on Internet Information Service (IIS)?
- Is Certificate Services enabled?
- Does the firewall or antivirus software setting on the client PC block connection?
- Are the network configuration and Internet Explorer settings on the client PC correct?

- 3 When Internet Explorer prompts entering the log-in user and password, type the user name as follows.
 Example: when the user name is “1XClient” and the domain name “localnetwork.net”

1XClient@localnetwork.net

- 4 Click **Download a CA certificate, certificate chain, or CRL**.
- 5 Select **Base 64** in **Encoding method** and click **Download CA certificate**.
 The “File Download” dialog opens.
- 6 Specify the file storage location and save the CA certificate.

After saving the CA certificate, import it to the camera.
 The CA certificate import procedure is completed.

Downloading the client certificate

The procedures of the client certificate download differs depending on the TLS mode of the camera. This section explains the procedures for each mode.

When “Use a key pair from a CA” is selected

- 1 Start Internet Explorer on the client PC and type the CA’s URL in the address bar.
The CA’s URL is normally as follows:
http: //<address of the CA>/CertSrv/
- 2 Click **Go To**.
- 3 Type the log-in user name and password correctly.
The “Microsoft Certificate Services” page opens.
- 4 Click **Request a certificate, advanced certificate request** and **Create and submit a request to this CA** in sequence.
- 5 Set the following items.

Certificate Template: User

Key Options: Create new key set

– CSP: Microsoft Enhanced Cryptographic Provider v1.0

– Key Size: 1024

– Check **Mark keys as exportable**.

Additional Options: Select **SHA-1** for Hash Algorithm.

- 6 Click **Submit**.
The message “The certificate you requested was issued to you.” appears.
- 7 Click **Install this certificate**, to install the certificate in the certificate store on the client PC.
- 8 Click **Internet Options, Content** and **Certificates** of Internet Explorer in sequence.
The new client certificate is displayed in the Personal tab.
- 9 Select the installed certificate and click **Export...**
The “Certificate Export Wizard” opens.

- 10 Click **Next** and select as follows.

Do you want to export the private key with the certificate?: Select **Yes, export the private key**.

Select the format you want to use: Select

Personal Information Exchange – PKCS#12(PFX).

Password: Specify the private key password.

File to export: Specify the name of the file to be exported.

The certificate is exported. Import the exported file to the camera as the camera’s client certificate.

For details, see “To import the client certificate” in the Client certificate tab on page 52.

Setting the User

— User Menu

When you click **User** in the Administrator menu, the User menu appears.
Use this menu to set the user names and passwords of Administrator and up to 9 kinds of users (User 1 to User 9), and the access right of each user.

	User name	Password / Re-type password	FTP	Audio	Viewer mode
Administrator					
User 1			☒	☒	Full
User 2			☒	☒	Full
User 3			☒	☒	Full
User 4			☒	☒	Full
User 5			☒	☒	Full
User 6			☒	☒	Full
User 7			☒	☒	Full
User 8			☒	☒	Full
User 9			☒	☒	Full

Viewer authentication: ☒ On ☐ Off Full

Administrator

Specify **User name**, **Password** and **Re-type password**.

User 1 to 9

Specify **User name**, **Password**, **Re-type password**, **FTP**, **Audio** and **Viewer mode** for each user ID.

User name

Type a user name between 5 and 16 characters.

Password

Type a password between 5 and 16 characters.

Re-type password

To confirm the password, retype the password that you typed in the **Password** box.

FTP

Set whether this user is allowed to log in to an FTP server or not. Check the box if the user is allowed to log in to an FTP server.

Audio

Select whether audio output to a speaker connected to the line output jack of the camera is allowed or not by using the SNC audio upload tool stored in the supplied CD-ROM. Check this box to allow audio output.

Note

To output audio using the SNC audio upload tool, set **Audio upload** to **On** in the Common tab of the Camera menu (page 32).

Viewer mode

When the user is authenticated for logging in the main viewer, select the viewer mode to be displayed after authentication.

Full: The user can operate all functions in this mode.

Light: In addition to the **View** mode, the user can select the image size of the main viewer, select codec and capture a still image.

View: The user can only monitor the camera image.

For the functions available for each viewer mode, see “Administrator and User” on page 16.

Viewer authentication

Set whether the user is authenticated or not when the main viewer is displayed.

On: The main viewer is displayed in accordance with the viewer mode of the authenticated user.

Off: Select the viewer mode of the main viewer which is displayed without authentication from **Full**, **Light** or **View**.

OK/Cancel

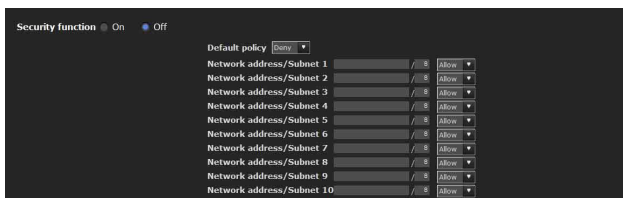
See “Buttons common to every menu” on page 26.

Setting the Security — Security Menu

When you click **Security** in the Administrator menu, the Security menu appears.

This allows you to control which computers can have access to the camera.

Likewise, when using IPv6, security settings can be configured for each network.



Security function

To activate the security function, select **On**.

Default policy

Select the basic policy of the limit from **Allow** and **Deny** for the computers specified in the Network address/Subnet 1 to Network address/Subnet 10 menus below.

Network address/Subnet 1 to Network address/Subnet 10

Type the network addresses and subnet mask values that you want to allow or deny access to the camera.

You can specify up to 10 network addresses and subnet mask values. For a subnet mask, type 8 to 32.

(In the case of IPv6, enter a value between 8 and 128.)

Select **Allow** or **Deny** from the drop-down list on the right for each network address/subnet mask.

Tip

The subnet mask value represents the bit number from the left of the network address.

For example, the subnet mask value for “255.255.255.0” is 25.

If you set **192.168.0.0/24** and **Allow**, you can allow access from computers having an IP address between “192.168.0.0” and “192.168.0.255.”

Note

You can access the camera even from a computer having an IP address whose access right is set to **Deny**, if you enter the user name and password set for the **Administrator** boxes in the User menu.

OK/Cancel

See “Buttons common to every menu” on page 26.

Sending an Image via E-mail — e-Mail (SMTP) Menu

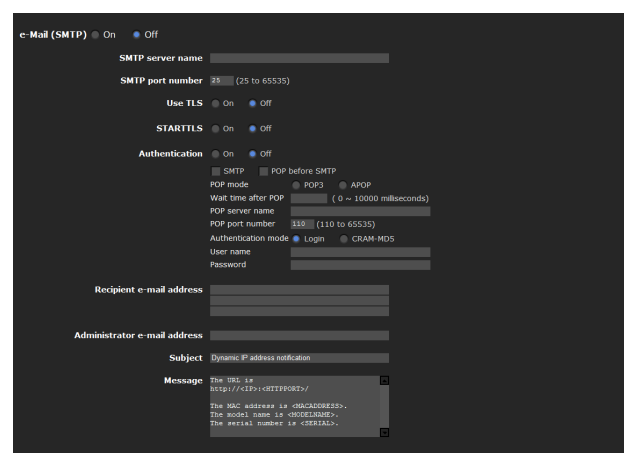
When you click **e-Mail (SMTP)** in the Administrator menu, the e-Mail (SMTP) menu appears.

Using the e-Mail (SMTP) function, you can send an e-mail with an attached image file that has been shot linked with an external sensor input or with the built-in motion detection function. The image file can also be sent periodically.

The e-Mail (SMTP) menu consists of three tabs:

Common, **Alarm sending** and **Periodical sending**.

Common Tab — Setting the e-Mail (SMTP) Function



e-Mail (SMTP)

Select **On** when you use the e-Mail (SMTP) function.

Notes

- You cannot send an audio file by using the e-mail sending function.
- The frame rate and operability on the main viewer may be reduced while a file is being transmitted by the e-Mail (SMTP) function.

SMTP server name

Type the SMTP server name using up to 64 characters, or the IP address of the SMTP server.

SMTP port number

Enter a port number from 25 to 65535.

The standard port number is 25. If TLS is enabled, the standard port number for SMTPs is 465.

Use TLS

To use the encryption function by TLS, select **On**.

Note

The model on sale in China does not support the TLS function.

STARTTLS

To use the encryption function by STARTTLS, select **On**.

Note

The model on sale in China does not support the STARTTLS function.

Authentication

Select whether authentication is required when you send an e-mail.

Off: No authentication is required when an e-mail is sent.

On: Authentication is required when an e-mail is sent. Select one of the authentication methods from the following and specify the **POP server name**, **User name** and **Password** as required.

SMTP: Select when SMTP authentication is required.

POP before SMTP: Select when POP before SMTP authentication is required.

Note

When you set **Authentication** to **On**, be sure to select either or both **SMTP** or/and **POP before SMTP**.

POP mode

Select POP3 or APOP as the authentication method for POP authentication.

Note

The model on sale in China does not support the APOP authentication.

Wait time after POP

Set the waiting time in **POP before SMTP** before SMTP authentication after POP authentication is completed. Timeout can be set from 0 to 10,000 msec.

POP server name

This is necessary when **POP before SMTP** is selected for **Authentication**.

Type the POP (receiving mail) server name using up to 64 characters, or type the IP address of the POP server. This setting is necessary when the SMTP server that sends e-mails performs authentication using the POP user account.

POP port number

Enter a port number from 110 to 65535.

The standard port number is 110. If TLS is enabled, the standard port number for POP3s is 995.

Authentication mode

Select **Login** or **CRAM-MD5** as the authentication method for SMTP authentication.

Note

The model on sale in China does not support the CRAM-MD5 authentication.

User name, Password

Type the user name and password of the user who owns the mail account using up to 64 characters. This setting is necessary when the SMTP server that sends e-mails performs authentication.

Recipient e-mail address

Type the recipient e-mail address using up to 64 characters.

You can specify up to three recipient e-mail addresses.

Administrator e-mail address

Type the Administrator e-mail address using up to 64 characters.

This address is used for reply e-mails and sending system messages from the mail server.

Subject

Type the subject/title of the e-mail using up to 64 characters.

When **Alarm sending** of the Alarm sending tab is set to **On**, an e-mail sent in response to alarm detection will indicate the type of alarm in the subject. **S1** is added for sensor input detection, **TP** for camera interference detection and **VM** for VMF. **MD** is additionally available for motion detection.

Message

Type the text of the e-mail using up to 384 characters. (A line break is equivalent to 2 characters.)

OK/Cancel

See “Buttons common to every menu” on page 26.

Alarm sending Tab — Setting the e-mail sending mode when detecting the alarm

Set to send an e-mail linked with alarm detection by the external sensor input or by the built-in motion detection function.

Alarm sending

Select **On** to set sending an e-mail linked with alarm detection.

File attachment

Set whether an image file (JPEG file) is to be attached to the e-mail or not.

When **On** is selected, the image file made using the settings below is attached. When **Off** is selected, only the message is sent.

Image file name

Type the file name you want to assign to the image to be attached to an e-mail. You can use up to 10 alphanumeric characters, - (hyphen) and _ (underscore) for naming.

Suffix

Select a suffix to be added to the file name.

None: No suffix is added. The image file name is assigned to the image to be sent via e-mail.

Date & time: The date & time suffix is added to the image file name.

The date/time suffix consists of lower two-digits of the year (2 digits), month (2 digits), date (2 digits), hour (2 digits), minute (2 digits), second (2 digits), and sequential number (2 digits), thus adding 14-digit number to the image file name.

Sequence number: A sequential number of 10 digits between 0000000001 and 4294967295 and two fixed digits 00 are added to the image file name.

Sequence number clear

Click **Clear** to reset the **Sequence number** suffix to 1.

Alarm

Select the alarm to be linked with e-mail notification.

Sensor input 1: The external sensor that is connected to sensor input of the camera I/O port.

Camera tampering detection: An alarm that is triggered when the camera detects vibration or shaking.

Interval: Set the interval at which you want to send an e-mail periodically after detection.

E-mails are sent after a specified interval time until the Camera tampering detection setting is cleared or the detection setting is turned off. You can set the hour (H) and minutes (M) between 30 minutes and 24 hours (one day).

When file attachment is set to ON, a file is only attached to an initial mail and will not be attached to the following mails.

VMF: An alarm of the VMF detection function.

Motion detection: The alarm detected by the motion detection function.

Click **Detection**, and the motion detection menu is displayed to allow you to set the motion detection function (page 73).

Effective period

Set the period during which alarm detection is effective.

Always: Alarm detection is always effective.

Schedule: You can specify the period during which alarm detection is effective.

Click **Schedule** and the menu for the effective period is displayed. ("Setting the Schedule — Schedule Menu" on page 72)

OK/Cancel

See "Buttons common to every menu" on page 26.

Periodical sending Tab — Setting the periodical e-mail sending mode

You can set to send e-mails periodically.

Periodical sending

Select **On** when you want to use periodical e-mail sending.

Image file name

Type the file name of the image attached to the e-mail using up to 10 alphanumeric characters, - (hyphen) and _ (under score).

The actual image file name will be the specified image file name with a suffix and the extension .jpg.

Suffix

Select a suffix to be added to the file name used when the e-mail is sent.

None: The name of the sent file will be the image file name.

Date & time: The date & time suffix is added to the image file name.
The date & time suffix consists of the year (2 digits), month (2 digits), date (2 digits), hour (2 digits), minutes (2 digits) and seconds (2 digits), and sequential number (2 digits), thus adding a 14-digit number to the image file name.

Sequence number: A sequential number of 10 digits between 0000000001 and 4294967295 and two fixed digits 00 are added to the image file name.

Sequence number clear

Click **Clear** to reset the **Sequence number** suffix to 1.

Interval

Type the interval at which you want to send an e-mail periodically. You can set the hour (H) and minutes (M) between 30 minutes and 24 hours (one day).

Effective period

Set the period during which periodical sending will be effective.

Always: Periodical sending is always effective.

Schedule: You can specify the period during which periodical sending is effective.

Click **Schedule** and the menu for the effective period is displayed. (“Setting the Schedule — Schedule Menu” on page 72)

OK/Cancel

See “Buttons common to every menu” on page 26.

Sending Images to FTP Server

— FTP client Menu

When you click **FTP client** in the Administrator menu, the FTP client menu appears.

Use this menu to set up for capturing and sending still images to an FTP server. Using FTP client function, you can send an image and audio file that has been shot and recorded linked with the external sensor input or with the built-in motion detection function to an FTP server. The image file can also be sent periodically.

The FTP client menu consists of three tabs: **Common**, **Alarm sending** and **Periodical sending**.

Common Tab — Setting the FTP client function



FTP client function

To activate the FTP client function, select **On**.

Note

The frame rate and operability on the main viewer may be reduced while a file is being transmitted by the FTP client function.

FTP server name

Type either the FTP server name to upload still images using up to 64 characters, or the IP address of the FTP server.

User name

Type the user name for the FTP server using up to 64 characters.

Password

Type the password for the FTP server using up to 64 characters.

Re-type password

To confirm the password, type the same characters as you typed in the **Password** box.

Passive mode

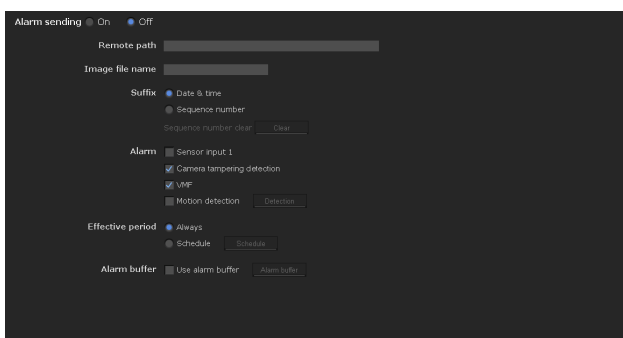
Set whether you use the passive mode of FTP server or not when connecting to the FTP server. Select **On** to connect to the FTP server using the passive mode.

OK/Cancel

See “Buttons common to every menu” on page 26.

Alarm sending Tab — Setting the FTP client action when detecting the alarm

Set to forward an image and audio file to the specified FTP server linked with alarm detection by the external sensor input or by the built-in motion detection function.



Alarm sending

Select **On** to send the image and audio file to the FTP server linked with alarm detection.

Remote path

Type the path to the destination using up to 64 characters.

Image file name

Type the file name you want to assign to the images when sending to the FTP server. You can use up to 10 alphanumeric characters, - (hyphen) and _ (underscore) for naming.

Suffix

Select a suffix to be added to the file name.

Date & time: The date & time suffix is added to the image file name.
The date/time suffix consists of the year (2 digits), month (2 digits), date (2 digits), hour (2 digits), minute (2 digits) and second (2 digits), and sequential number (2 digits), thus adding a 14-digit number to the image file name.

Sequence number: A sequential number of 10 digits between 0000000001 and 4294967295 and a sequential 2-digit number are added to the image file name.

Tip

A sequential number added to **Date & time** and **Sequence number** is used to identify individual files created with consecutive alarm events.

Sequence number clear

Click **Clear** to reset the **Sequence number** suffix to 1.

Alarm

Select the alarm to be linked with the file to be forwarded to the FTP server.

Sensor input 1: The external sensor that is connected to sensor input of the camera I/O port.

Camera tampering detection: An alarm that is triggered when the camera detects vibration or shaking.

VMF: An alarm of the VMF detection function.

Motion detection: The alarm detected by the motion detection function.

Click **Detection**, and the Motion detection menu is displayed to allow you to set the motion detection function (page 73).

Effective period

Set the period during which alarm detection is effective.

Always: Alarm detection is always effective.

Schedule: You can specify the period during which alarm detection is effective.

Click **Schedule** and the menu for the effective period is displayed. (“Setting the Schedule — Schedule Menu” on page 72)

Alarm buffer

Select **Use alarm buffer** to forward the image/audio at a specified time before or after alarm detection (pre-alarm, post-alarm).

If you do not select the alarm buffer, only the image at the moment of alarm detection is forwarded.

Click **Alarm buffer** to display the Alarm buffer menu. For details, see “Setting the Alarm Buffer — Alarm buffer Menu” on page 72.

OK/Cancel

See “Buttons common to every menu” on page 26.

Periodical sending Tab — Setting the periodical FTP client activity

You can set to send image files (JPEG files) to an FTP server periodically.

Periodical sending

Select **On** when you want to use periodical sending.

Remote path

Type the remote path using up to 64 characters.

Image file name

Type the file name of the image sent to the FTP server using up to 10 alphanumeric characters, - (hyphen) and _ (under score).

The actual image file name will be the specified image file name with a suffix and extension .jpg.

Note

You cannot send an audio file using periodical sending of the FTP client function.

Suffix

Select a suffix to be added to the file name sent to the FTP server.

None: The name of the sent file will be the image file name.

Date & time: The date & time suffix is added to the image file name.

The date & time suffix consists of the year (2 digits), month (2 digits), date (2 digits), hour (2 digits), minute (2 digits) and second (2 digits), and sequential number (2 digits), thus adding a 14-digit number to the image file name.

Sequence number: A sequential number of 10 digits between 0000000001 and 4294967295 and two fixed digits 00 are added to the image file name.

Sequence number clear

Click **Clear** to reset the **Sequence number** suffix to 1.

Interval

Type the interval at which you want to send images to the FTP server periodically. You can set the hour (H), minutes (M) and seconds (S) between 1 second and 24 hours (one day).

Note

The actual interval may be longer than the set value, depending on the image size, image quality setting, bit rate and the network environments.

Effective period

Set the period during which periodical sending is effective.

Always: Periodical sending is always effective.

Schedule: You can specify the period during which periodical sending is effective.

Click **Schedule** to display the menu for the effective period. (“Setting the Schedule — Schedule Menu” on page 72)

OK/Cancel

See “Buttons common to every menu” on page 26.

Recording Images in Memory

— Image memory Menu

When you click **Image memory** in the Administrator menu, the Image memory menu appears. By using the image memory function, you can record an image and audio file (shot being linked with the external sensor input or built-in motion detection function) in the built-in memory (approx. 8 MB), or in a CF memory card (not supplied. Applicable for SNC-CH140 only) inserted in the camera. The image file can also be recorded periodically.

The recorded image and audio files can be found or downloaded to the computer using the FTP server function. (See “Downloading Images from the Camera — FTP server Menu” on page 68.)

The Image memory menu consists of three tabs: **Common**, **Alarm recording** and **Periodical recording**. For details on usable memory cards, contact your authorized Sony dealer.

Notes

- The image and audio files recorded in the built-in memory are deleted when the power of the camera is turned off, or the **Selected root directory** setting is changed.
- The frame rate and operability on the main viewer may be reduced during image storage.
- Set Image memory recording function to **Off** when you remove the CF memory card from the camera or turn off the power of the camera with a CF memory card inserted.
- When ever you remove or insert a card, wait at least 10 seconds.
- Before using a CF memory card, format it using the computer, or by **Format CF memory card** in the Initialize tab of the System menu (page 30).

Common Tab — Setting the image memory function

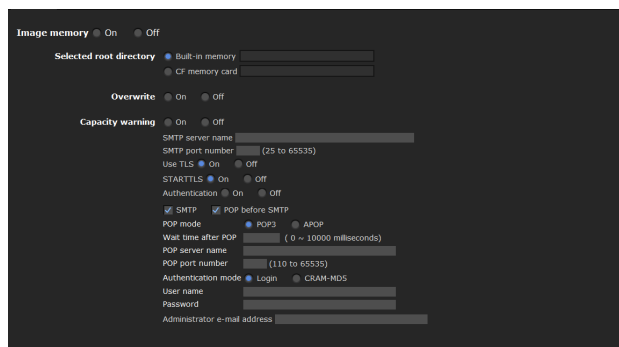


Image memory

To use the image memory function, select **On**.

■ SNC-CH140

Selected root directory

Select a memory in which you want to save an image. The current memory space is displayed on the right.

Built-in memory: Built-in memory of this camera
CF memory card: CF memory card inserted into the CF card slot of the camera

Note

The image and audio files recorded in the built-in memory are deleted when the **Selected root directory** setting is changed.

■ SNC-DH140

Built-in memory

The current memory space of the built-in memory is displayed.

Overwrite

Select **On** to overwrite the file when there is insufficient memory space to record the image in the built-in memory.

On: Overwrite is enabled and old files will be overwritten in the order of date.

Off: Overwrite is prohibited. No recording will be performed.

Capacity warning

This is the function to send a warning mail to the Administrator when the memory space of the built-in memory is low or full.

On: A warning mail is sent to the Administrator.

Off: A warning mail is not sent to the Administrator.

Note

When **Overwrite** is set to **On**, a warning mail is not sent to the Administrator.

SMTP server name

Type the name of the SMTP server for sending an e-mail, using up to 64 characters.
Otherwise type the IP address of the SMTP mail server.

SMTP port number

Enter a port number from 25 to 65535.
The standard port number is 25. If TLS is enabled, the standard port number for SMTPs is 465.

Use TLS

To use the encryption function by TLS, select **On**.

Note

The model on sale in China does not support the TLS function.

STARTTLS

To use the encryption function by STARTTLS, select **On**.

Note

The model on sale in China does not support the STARTTLS function.

Authentication

Select whether authentication is required when you send an e-mail.

Off: No authentication is required when an e-mail is sent.

On: Authentication is required when an e-mail is sent.
Select one of the authentication methods from the following and specify the **POP server name**, **User name** and **Password** as required.

SMTP: SMTP authentication is required.

POP before SMTP: POP before SMTP authentication is required.

Note

When you set **Authentication** to **On**, be sure to select either or both **SMTP** or/and **POP before SMTP**.

POP mode

Select POP3 or APOP as the authentication method for POP authentication.

Note

The model on sale in China does not support the APOP authentication.

Wait time after POP

Set the waiting time in **POP before SMTP** before SMTP authentication after POP authentication is completed. Timeout can be set from 0 to 10,000 msec.

POP server name

This is necessary when **POP before SMTP** is selected for **Authentication**.

Type a POP (receiving mail) server name using up to 64 characters, or type the IP address of the POP server. This setting is necessary when the SMTP server that sends e-mails performs authentication using the POP user account.

POP port number

Enter a port number from 110 to 65535.
The standard port number is 110. If TLS is enabled, the standard port number for POP3s is 995.

Authentication mode

Select **Login** or **CRAM-MD5** as the authentication method for SMTP authentication.

Note

The model on sale in China does not support the CRAM-MD5 authentication.

User name, Password

Type the user name and the password of the user who owns the e-mail account. This setting is necessary when the SMTP server that sends e-mails performs authentication.

Administrator e-mail address

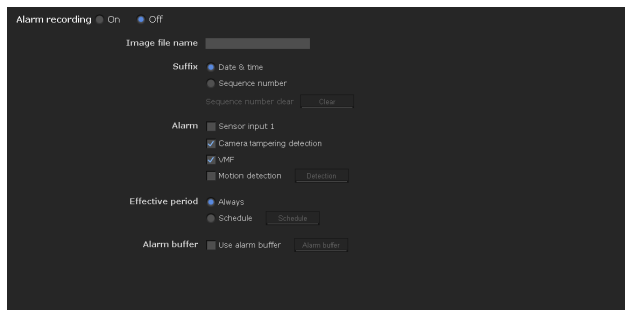
Type the e-mail address of the recipient of a warning mail (e-mail address of the camera Administrator), using up to 64 characters.

OK/Cancel

See “Buttons common to every menu” on page 26.

Alarm recording Tab — Setting the Image memory function when detecting the alarm

You can set to record image and audio file to the memory linked with an external sensor input or built-in motion detection function.



Alarm recording

Select **On** to configure the settings for recording image and audio files linked with alarm detection.

Image file name

Type the file name you want to assign to the image(s) to be recorded. You can use up to 10 alphanumeric characters, - (hyphen) and _ (underscore) for naming.

Suffix

Select a suffix to be added to the file name.

Date & time: The Date & time suffix is added to the image file name.

The Date & time suffix consists of the year (2 digits), month (2 digits), date (2 digits), hour (2 digits), minute (2 digits), second (2 digits) and sequential number (2 digits), thus adding a 14-digit number to the image file name.

Sequence number: A sequential number of 10 digits between 0000000001 and 4294967295 and an sequential 2 - digit number is added to the image file name.

Tip

A sequential number added to **Date & time** and **Sequence number** is used to identify individual files created with consecutive alarm events.

Sequence number clear

Click **Clear** to reset the **Sequence number** suffix to 1.

Alarm

Select the alarm to be linked with the recording of image and audio files.

Sensor input 1: The external sensor that is connected to sensor input of the camera I/O port.

Camera tampering detection: An alarm that is triggered when the camera detects vibration or shaking.

VMF: An alarm of the VMF detection function.

Motion detection: The alarm by the motion detection function.

Click **Detection**, and the Motion detection menu is displayed to allow you to set the motion detection function (page 73).

Effective period

Set the period during which alarm detection is effective.

Always: Alarm detection is always effective.

Schedule: You can specify the period during which alarm detection is effective.

Click **Schedule** to display the setting menu for the effective period. (“Setting the Schedule — Schedule Menu” on page 72)

Alarm buffer

Select **Use alarm buffer** when you record the image/audio at a specific time before or after alarm detection (pre-alarm, post-alarm).

If you do not select the alarm buffer, only the image at the moment of alarm detection is recorded.

Click **Alarm buffer** to display the Alarm buffer menu. For details, see “Setting the Alarm Buffer — Alarm buffer Menu” on page 72.

OK/Cancel

See “Buttons common to every menu” on page 26.

Periodical recording Tab — Setting the periodical recording mode

You can set to record video files (JPEG files) periodically.

Periodical recording

Select **On** when you want to use periodical recording.

Image file name

Type the file name of the image to be recorded to the memory using up to 10 alphanumeric characters, - (hyphen) and _ (under score).

The actual image file name will be the specified image file name with a suffix and the extension .jpg.

Note

You cannot record an audio file using the periodical recording function.

Suffix

Select a suffix to be added to the file name.

None: The recording file name will be the image file name.

Date & time: The date & time suffix is added to the image file name.

The Date & time suffix consists of the year (2 digits), month (2 digits), date (2 digits), hour (2 digits), minute (2 digits), second (2 digits) and sequential number (2 digits), thus adding a 14-digit number to the image file name.

Sequence number: A sequential number of 10 digits between 0000000001 and 4294967295 and two fixed digits 00 are added to the image file name.

Sequence number clear

Click **Clear** to reset the **Sequence number** suffix to 1.

Interval

Type the interval at which you want to record an image in the memory periodically. You can set the hour (H), minutes (M) and seconds (S) between 1 second and 24 hours (one day).

Note

The actual interval may be longer than the set value depending on the image size, image quality, bit rate, or recording media.

Effective period

Set the period during which periodical recording is effective.

Always: Periodical recording is always effective.

Schedule: You can specify the period during which periodical recording is effective.

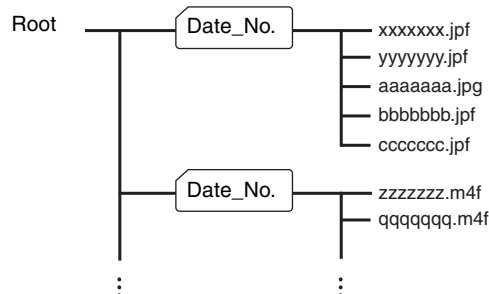
Click **Schedule** and the menu for the effective period is displayed. ("Setting the Schedule — Schedule Menu" on page 72)

OK/Cancel

See "Buttons common to every menu" on page 26.

Folder structure of image memory

When the image memory function is used, images are recorded with the following folder structure.



A  represents a folder created automatically.

The Date_No. folder has an 11-digit name consisting of the year (last 2 digits), month (2 digits), day (2 digits), underscore and sequential number (4 digits).

In the built-in memory, one folder automatically created can store image files of about 1 MB. If the size of the image files exceeds that value, a new folder is created automatically to continue recording.

Note

In the CF memory card of SNC-CH140, the folder size varies depending on the capacity of the CF memory card.

About the extension of a file

A file to be recorded/sent using the image memory function or the Mail (SMTP)/FTP client function has one of the following four extensions depending on the video mode setting and the recording/sending settings of the camera.

.m4f: MPEG4 image files (including sound)

.jpg: JPEG image files (including sound)

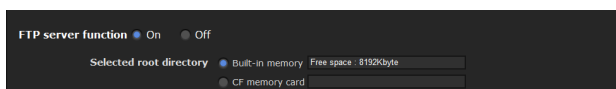
.jpg: JPEG still image files

.maf: H.264 image files (including sound)

The SNC video player (page 99) allows playback of ".m4f", ".maf" and ".jpg" files.

Downloading Images from the Camera — FTP server Menu

When you click **FTP server** in the Administrator menu, the FTP server menu appears. This menu allows you to search image and audio files stored in the built-in memory (approximately 8 MB) or CF memory card (not supplied. Applicable for SNC-CH140 only) inserted in the camera, or configure the FTP server function for downloading, using the FTP client software on the computer.



FTP server function

To activate the FTP server function, select **On**.

■ SNC-CH140

Selected root directory

Select the memory that contains the file you want to download.

The current memory space is displayed on the right.

Built-in memory: Built-in memory of this camera

CF memory card: CF memory card inserted into the CF card slot of the camera

■ SNC-DH140

Built-in memory

The current memory space of the built-in memory is displayed.

Note

The frame rate and operability on the main viewer may be reduced when you logged in to the FTP server of this unit using the FTP client software installed in the computer.

OK/Cancel

See “Buttons common to every menu” on page 26.

Setting the Alarm Output — Alarm output Menu

When you click **Alarm output** in the Administrator menu, the Alarm output menu appears.

You can perform setting in this menu to control the alarm output of the I/O port on the rear of the camera linked to alarm detection, the timer and the Day/Night function.

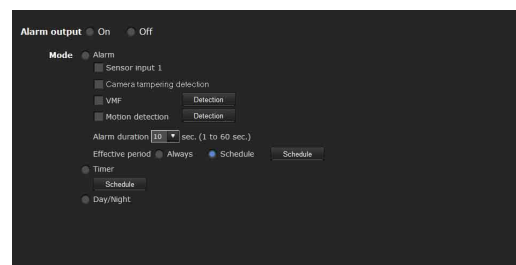
The Alarm output menu consists of two tabs:

Alarm out 1 and **Alarm out 2**.

Tip

For details on connection of peripheral devices to the alarm output of the I/O port, refer to the supplied Installation Manual.

Alarm out 1, 2 Tab



Alarm output

To activate the alarm output function, select **On**.

Mode

Select the mode of the alarm output function.

Alarm: Controls alarm output by synchronizing it with an external sensor input or the built-in motion detection function.

When **Alarm** is selected, the items **Sensor input 1**, **Camera tampering detection**, **VMF**, **Motion detection**, **Alarm duration** and **Effective period** become active.

Timer: Controls alarm output using the timer.

Click **Schedule** and the menu for the effective period is displayed. (“Setting the Schedule — Schedule Menu” on page 72)

Day/Night: Controls the alarm output linked to the day/night function.

Sensor input 1

Select this option when you link the alarm output to an external sensor that is connected to sensor input of the camera I/O port.

Camera tampering detection

Select this option when you link the alarm output to the vibration/shaking detection of the camera.

VMF

Select this option when you link the alarm output to the VMF detection function.

Motion detection

Select this option when you link the alarm output to the motion detection function.

Click **Detection**, and the Motion detection menu is displayed to allow you to set the motion detection function (page 73).

Alarm duration

Select the duration for which the alarm is output, between 1 and 60 sec.

Effective period

This item becomes active when **Mode** is set to **Alarm**. Set the period during which the alarm detection is effective.

Always: Alarm detection is always effective.

Schedule: You can specify the period during which alarm detection is effective.

Click **Schedule** and the menu for the effective period is displayed. (“Setting the Schedule — Schedule Menu” on page 72)

OK/Cancel

See “Buttons common to every menu” on page 26.

Outputting Audio Linked to Alarm Detection

— Voice alert Menu

Click **Voice alert** in the Administrator menu to display the Voice alert menu.

Use this menu to set the voice alert function to output audio from the line output jack of the camera when an alarm is detected by the sensor input or motion detection function.

You can output the audio from the speaker connected to the camera in synchronization with an alarm event triggered by the sensor input or the motion detection function.

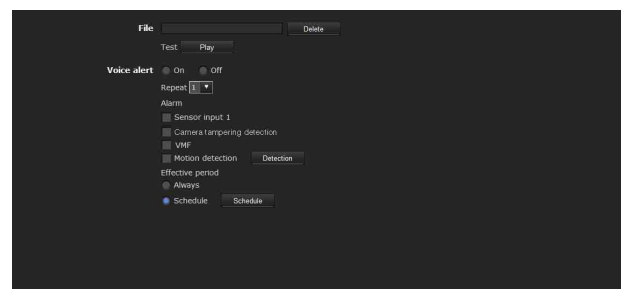
The Voice alert menu consists of 3 tabs: **Voice alert 1**, **Voice alert 2** and **Voice alert 3**. You can configure an individual audio file on each tab.

Note

Before using the voice alert function, you need to save the audio file to the camera using the SNC audio upload tool stored in the supplied CD-ROM.

For details on use of the SNC audio upload tool, see page 93.

Voice alert 1, 2, 3 Tab



File

Displays the name of the audio file saved in the camera. “Not uploaded” is displayed dimly if no audio file is saved.

To delete the audio file saved in the camera, click **Delete**.

Note

Before deleting an audio file, set **Voice alert** to **Off**.

Test

When an audio file is saved in the camera, you can check it by playing it back.

Click **Play** to play back the audio file once.

Voice alert

To use the voice alert function linked with the sensor input or the motion detection function, select **On**.

Repeat

Select playback repeat time from **1** to **3**.

Alarm

Select the alarm to be linked with the voice alert function.

Sensor input 1: The external sensor that is connected to sensor input of camera I/O port.

Camera tampering detection: An alarm that is triggered when the camera detects vibration or shaking.

VMF: An alarm of the VMF detection function.

Motion detection: The alarm detected by the motion detection function.

Click **Detection** to display Motion detection menu to allow you to set the motion detection function (page 73).

Notes

- If voice alert is actively linked with a different alarm type while another voice alert is occurring, the first voice alert is cancelled and the second one is output.
- If two or three audio files are set to be output simultaneously linked with the same alarm type, priority is given in the order **Voice alert 1, 2** then **3**.

Effective period

Set the period during which alarm detection is effective.

Always: Alarm detection is always effective.

Schedule: You can specify the period during which alarm detection is effective.

Click **Schedule**, and the menu for the effective period is displayed. ("Setting the Schedule — Schedule Menu" on page 72)

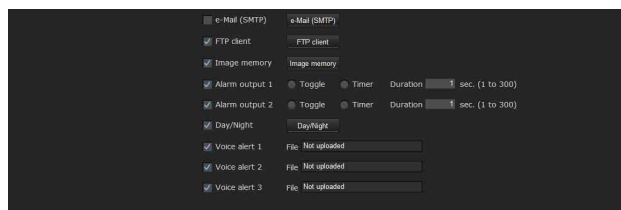
OK/Cancel

See "Buttons common to every menu" on page 26.

Setting the Operations from the Viewer — Trigger Menu

Click **Trigger** in the Administrator menu to display the Trigger menu.

This allows you to select the activities that can be performed when the button on the Trigger panel is clicked on the main viewer.



e-Mail (SMTP)

Checking this box allows you to select **e-Mail (SMTP)** on the Trigger panel in the main viewer.

By clicking **e-Mail (SMTP)** a still image of the moment you click is captured, and your e-mail with the image file attached is sent to the specified mail address.

When you click **e-Mail (SMTP)**, the **Trigger-e-Mail (SMTP)** menu is displayed. You can set the necessary options here. The setting options and setting procedures are the same as those of the e-Mail (SMTP) menu (page 58).

FTP client

Checking this box allows you to select **FTP client** on the Trigger panel in the main viewer.

By clicking **FTP client** a still image of the moment you click is captured, and the image file is sent to the FTP server.

When you click **FTP client**, the **Trigger-FTP client** menu is displayed. You can set the necessary options here. The setting options and setting procedures are the same as those of the FTP client menu (page 61).

Image memory

Checking this box allows you to select **Image memory** on the Trigger panel in the main viewer.

By clicking **Image memory** a still image of the moment you click is captured, and the image file is recorded.

For details on usable cards, contact your authorized Sony dealer.

Click **Image memory** to display the **Trigger-Image memory** menu. You can set the necessary options here. The setting options and setting procedures are the same as those of the Image memory menu (page 64).

Alarm out 1, 2

Checking this box allows you to select **Alarm out 1** or **Alarm out 2** on the Trigger panel in the main viewer. You can control the alarm output by clicking **Alarm out 1** or **Alarm out 2**.

Select the alarm output control mode from **Toggle** or **Timer**.

Toggle: Each time you run a trigger, On (short circuit) or Off (open) is switched.

Timer: When you run a trigger, the alarm output is switched to On, and will automatically set to Off after the time specified in **Duration** has elapsed.

Duration

When **Timer** is selected, specify the time for which the alarm output remains off, from 1 to 300 seconds.

Day/Night

Checking this box allows you to select **Day/Night** on the Trigger panel in the main viewer. You can set the day/night function to On (night mode) or Off (day mode) by clicking **Day/Night**.

When you click **Day/Night**, the **Trigger-Day/Night** menu is displayed. You can set the necessary options here. The setting options and setting procedures are the same as those in the Day/Night tab of the Camera menu (page 35).

Note

The day/night function is invalid when **Day/Night** is set to **Auto** in the **Trigger-Day/Night** menu, even if you click **Trigger**.

Voice alert 1, 2, 3

Checking this box allows you to select **Voice alert 1**, **Voice alert 2** or **Voice alert 3** on the Trigger panel in the main viewer. You can output audio from the audio file saved in the camera by clicking **Voice alert 1**, **2** or **3**.

File

Displays the name of the audio file saved in the camera. "Not uploaded" is displayed dimly if no audio file is saved.

OK/Cancel

See "Buttons common to every menu" on page 26.

Setting the Schedule

— Schedule Menu

When you click **Schedule** in the Administrator menu, the Schedule menu appears.
The Schedule menu consists of seven tabs.
This is the same menu as the Schedule menu that is displayed when you click **Schedule** to set the **Effective period** in the following menus.

Day/Night: **Schedule** in the Day/Night tab of the Camera menu

e-Mail: **Schedule** in the Alarm sending or Periodical sending tab of the e-Mail (SMTP) menu

FTP: **Schedule** in the Alarm sending or Periodical sending tab of the FTP client menu

Image memory: **Schedule** in the Alarm recording or Periodical recording tab of the Image memory menu

Alarm out: **Schedule** in the Alarm out 1 or Alarm out 2 tab of the Alarm output menu

Voice alert: **Schedule** in the Voice alert 1, 2 or 3 tab of the Voice alert menu

Example: When setting e-Mail (SMTP) (Periodical sending) in the Schedule menu

Use the same time schedule every day

When this item is checked, the same **Start time** and **End time** are applied to all days. In that case, the **Start time** and **End time** of the day from **Mon** (Monday) to **Sun** (Sunday) cannot be input.

Mon (Monday) to Sun (Sunday)

The time period on the right of the checked day is the effective period of the schedule.

Start time, End time

Specify the start time and the end time.

OK/Cancel

See “Buttons common to every menu” on page 26.

Setting the Alarm Buffer

— Alarm buffer Menu

When you click **Alarm buffer** in the Administrator menu, the Alarm buffer menu appears.

You can set the Pre-alarm image and audio (the image and audio before alarm detection) and the Post -alarm image and audio. These can be set when **Alarm sending** of FTP client menu or **Alarm recording** of the Image memory menu is set to **On**, besides when **Use alarm buffer** is selected.

Codec

Select the image to be used for the alarm buffer.

Recording capacity

Displays the maximum recording capacity of the alarm buffer in the present camera setting of the video mode, image size, bit rate and frame rate.

Recording time

Set the recording time for the Pre-alarm image/audio and Post alarm image/audio.

Pre-alarm duration: Type the recording time of the image/audio before alarm detection.

Post-alarm duration: Type the recording time of the image/audio after alarm detection.

Note

The value of **Recording capacity** differs depending on the image size and image quality settings in the Camera menu.

OK/Cancel

See “Buttons common to every menu” on page 26.

Setting the Sensor input/ Camera tampering detection/Motion detection

— Event detection Menu

When you click Event detection in the Administrator menu, the **Event detection** menu appears. Event detection menu is constituted by **Sensor input**, **Camera tampering detection** and **Motion detection** tabs.

Sensor input tab — Set the sensor input

Sensor input mode

Set the direction of the detected input signal to the sensor input terminal of the camera.

Normally open: Detects the alarm when the sensor input is short-circuited.

Normally closed: Detects the alarm when the sensor input is open-circuited.

OK/Cancel

See “Buttons common to every menu” on page 26.

Camera tampering detection tab — Set the camera tampering detection

Camera tampering detection

Select **On** to activate the function to detect the camera shaking. When you select **On**, you can select the Sensitivity.

Detection status: Display the tampering detection state of the time when Camera tampering detection tab is opened. To clear the detection status, click **Clear** button.

OK/Cancel

See “Buttons common to every menu” on page 26.

Motion detection tab — Set the motion/VMF detection

Motion detection detects moving objects in the camera image and outputs an alarm. In VMF, an alarm is notified when a motion detected under the motion detection setting passes, appears in, disappears from or shows any movement in a specified area or on an inspection line.

The motion detection function and the VMF function can independently set off an alarm at the time of detection.

What are VMF functions

VMF is a function for inspecting whether a motion detected under the motion detection setting passed, appeared in, disappeared from or shows any movement in a specified area or on an inspection line.

The inspection method is selected from Pass/Presence/Appear/Disappear/Volume, and allows for a maximum combined inspection method of three, which can be simultaneously or sequentially executed.

Passing

A passage line is determined, and when a moving object passes the setting line, an alarm is set off.

FTP client alarm sending, image memory alarm recording and/or audio file playback can be performed in synchronization with this alarm.

Existing

When a moving object in the designated area exists after a certain period of time has elapsed, it will set off an alarm. FTP client alarm sending, image memory alarm recording and/or audio file playback can be performed in synchronization with this alarm.

Appearance

When a moving object appears in the designated area, it will set off an alarm. FTP client alarm sending, image memory alarm recording and/or audio file playback can be performed in synchronization with this alarm.

Disappearance

When a moving object disappears from the designated area, it will set off an alarm. FTP client alarm sending, image memory alarm recording and/or audio file playback can be performed in synchronization with this alarm.

Capacity

When the Capacity of moving objects in the reference area reaches definite number, an alarm is set off. FTP client alarm sending, image memory alarm recording and/or audio file playback can be performed in synchronization with this alarm.

Notes

- Before actual use, perform an operation test and confirm that the motion detection function works correctly.
- Even when privacy masking is used, the motion detection function operates based on the images before masking is processed.
- When cropping is enabled, the motion detection menu is not displayed. To use the motion detection menu, disable this function first.

When the Motion detection menu is displayed for the first time

When you click **Motion detection**, “Security Warning” is displayed.

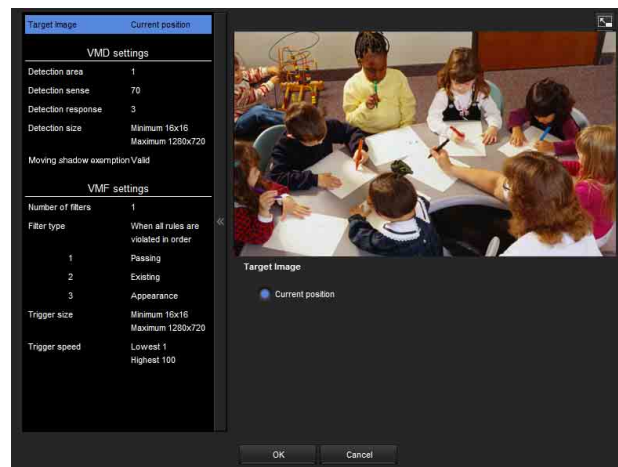
When you click **Yes**, ActiveX control is installed and the Motion detection menu is displayed.

Notes

- If **Automatic configuration** is enabled in the Local Area Network (LAN) settings of Internet Explorer, the image may not be displayed. In that case, disable **Automatic configuration** and set the Proxy server manually. For the setting of the Proxy server, consult your network administrator.
- When you install ActiveX control, you should be logged in to the computer as Administrator.
- When you are using Windows XP Service Pack 2 or later, or Windows Vista, the information bar or “Security Warning” may appear as you click **Motion detection**. For details, see “Installing ActiveX Control” in “When using Windows XP Service Pack 2 or later” on page 8 or “Installing ActiveX Control” in “When using Windows Vista” on page 11.

Setting items for motion detection

Use the settings tab to set the conditions for the motion detection function while observing camera images. This menu is the same as the settings menu displayed when you click **Detection** on Alarm transmission on the e-Mail (SMTP) menu, or on Alarm recording on the Image memory menu.



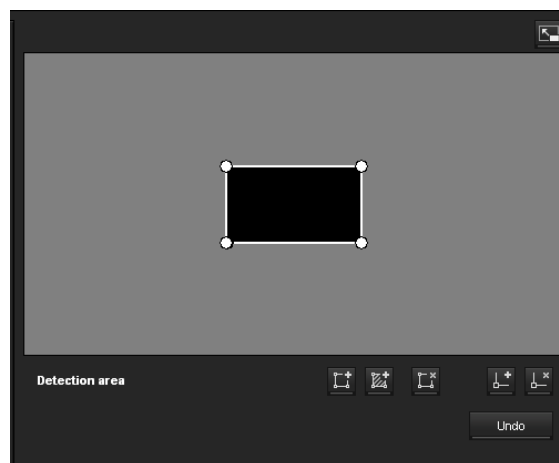
Target image

Current position is always selected.

VMD settings

Detection area

Specify the effective scope of motion detection.



Note

The frames shown on the monitor screen are not displayed on the image files sent or recorded with motion detection.

Configuring the detection area

The following procedure is used to configure the motion detection area:

- 1 Use the following buttons to specify the active area(s) and inactive area(s).

Add detection area

Clicking this button will add an active area window in the center of the screen.

When you place the cursor on the area, the cursor changes to a crossed arrow, which you can drag to move the area.

When you place the cursor on the vertex of the area, the cursor changes to , which you can drag to move the vertex.

Add non detection area

Clicking this button will add an inactive area window in the center of the screen.

When you place the cursor on the area, the cursor changes to a crossed arrow, which you can drag to move the area.

When you place the cursor on the vertex of the area, the cursor changes to , which you can drag to move the vertex.

Delete Area

Clicking this button will change the cursor to a button. While the cursor is a button, click on a part of the area to delete that area.

After the deletion, the cursor will return to its original form. To exit this operation, click this button again.

It is the same function as the button displayed under VMF settings.

Add vertex

Clicking this button will change the cursor to a button. In that state, when you click on a part of the side of the area, a vertex is added to that point. After the addition, the cursor will return its original form.

To exit this operation, click this button again.

It is the same function as the button displayed in VMF settings.

Delete vertex

Clicking this button will change the cursor to a button. In that state, when you click on a part of the vertex of the area, the vertex added to that point is deleted. After the deletion, the cursor will return its original form. To exit this operation, click this button again.

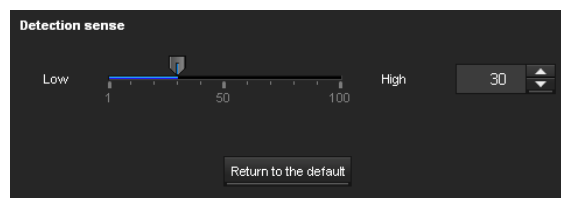
It is the same function as the button displayed in VMF settings.

Note

The vertex can be moved in an outward direction but cannot be moved toward the inside of an area.

Detection sense

Set the sensitivity of motion detection.

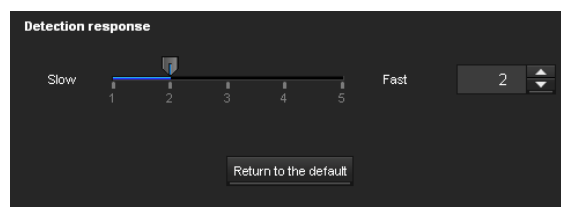


A value from **1** to **100** can be specified.

Clicking **Return to the default** changes the value to the default value.

Detection response

Set the response velocity of motion detection.

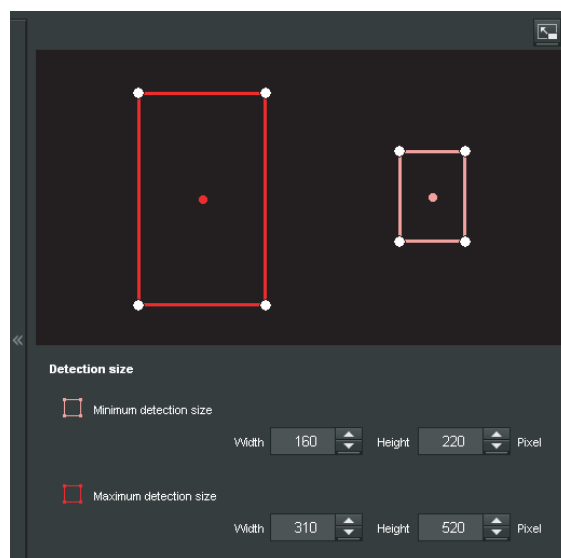


A value from **1** to **5** can be specified.

Clicking **Return to the default** changes the value to the default value.

Detection size

Specify the minimum detection size and maximum detection size of motion detection. To specify the detection size, you can either enter values or drag the vertices of the area.



The area size is measured in pixels.

- When you place the cursor on the area, the cursor changes to a crossed arrow, which you can drag to move to the minimum detection size area and maximum detection size area.
- When you place the cursor on the vertex of the area, the cursor changes to . Drag and move the vertex to adjust the detection size.

Moving shadow exemption

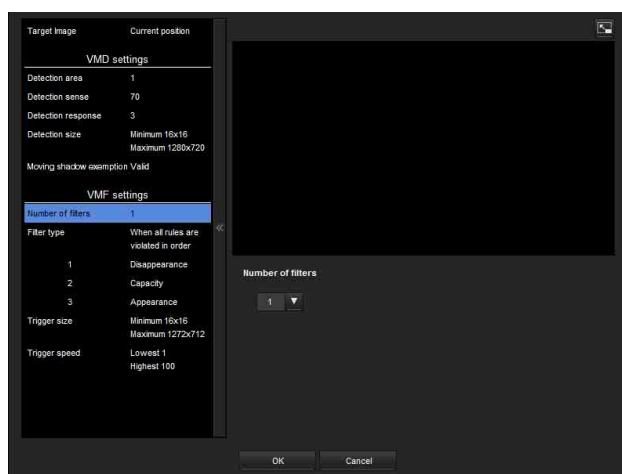
Set ON/OFF for the moving shadow exemption function of motion detection.

Selecting **Do not respond to shadows** will prevent the shadows of a moving object from being recognized as moving objects.

Remove the check to disable the shadow removal function of motion detection.

VMF settings

Up to three VMF settings (package number 1 to 3) can be retained for the current camera position. You can select one of those settings for use. You can configure the inspection method and the size and speed of object to inspect individually for each package number.



Number of filters

Select the setting number to set from 1, 2 or 3.

The following VMF setting is saved for the individual setting number selected here.

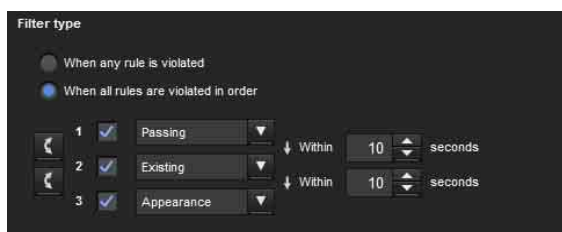
The set of the setting numbers selected here is valid for current VMF setting.

Note

package1, **package2** and **package3** of the VMF setting cannot be simultaneously enabled.

Filter type

Specify the VMF filter type.



Select the filter type from **When any rule is violated** or **When all rules are violated in order**.

When any rule is violated: An alarm will be set off when any one of the three conditions is met.

When all rules are violated in order: An alarm will be set off when the three conditions are met in the sequence specified. If the conditions occur in an order different from the sequence specified, such as 1, 3 and then 2, there will be no alarm.

Each filter type can include up to 3 criteria.

Select the inspection method from **Passing**, **Existing**, **Appearance**, **Disappearance**, **Capacity** and **None**.

Enable/Disable checkbox for filter

Set enable/disable for individual filter types.

Filter order switching button

Clicking  switches the order of filter between the neighbouring methods.

e.g., If you click the button between 1 and 2, they will switch order. If you click the button between 2 and 3, they will switch order.

Specifying the time for “When all occurs in order”

Specify the reference interval in seconds between 1 and 2, or 2 and 3.

For example, if 1 and 2 are set and “3 seconds” is specified, an alarm will be set off when the inspection conditions of 2 are met within 3 seconds from when the inspection conditions of 1 are met.

Filter settings

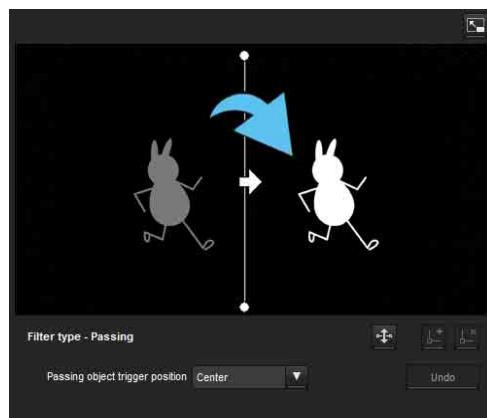
Settings for each filter can be edited here.

The inspection line and active window are set to default values. Edit according to use.

Tip

The buttons displayed on the edit screen for filter is used in the same way as those for detection setting. See page 74.

Passing



Edit the pass inspection line according to the following procedure:

Passing object trigger line

By default, one passing object trigger line is displayed. The number of vertexes is 2.

Placing the cursor on the line will turn the cursor into a cross, and when you drag the line, the whole line will move.

Placing the cursor on the vertex will turn the cursor into , and when you drag the line, the vertex will move. The arrow displayed in the center of the passing object trigger line shows the direction of inspection. trigger is performed when an object passes the passing object trigger position in this direction.

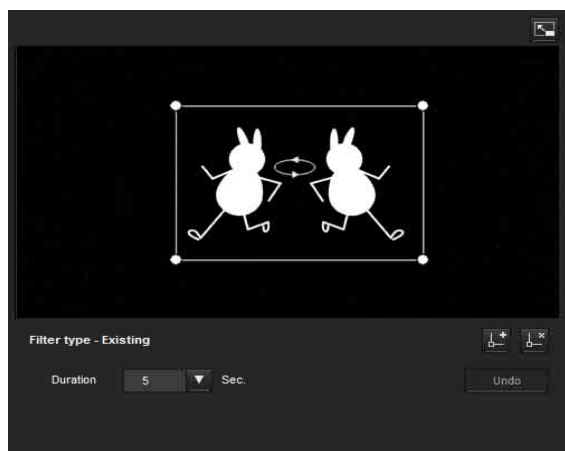
Trigger direction setting

Each time you click , the trigger direction toggles among the directions left, right and both.

Passing object trigger position

Select the passing object trigger position from **Center**, **Left side**, **Top side**, **Right side** and **Bottom side**.

Existing

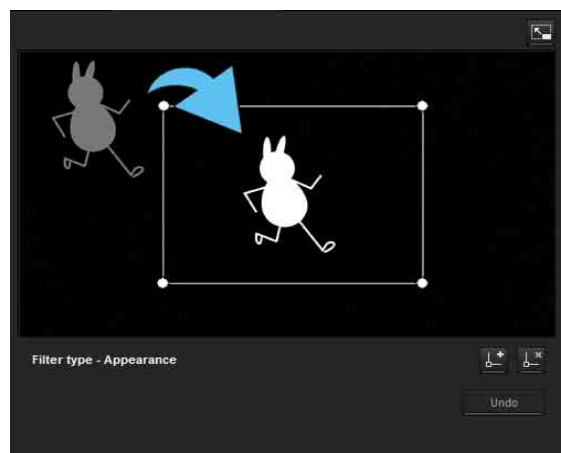


Similar to a active window an trigger area can also be moved and vertexes can be moved/added or deleted. If an object exists within the window longer than the specified time, existing is acknowledged.

Duration

Specify the time of existing.

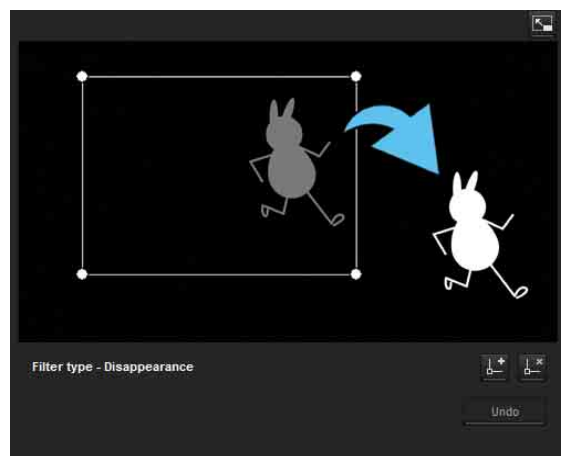
Appearance



This criterion is whether an object appeared in the trigger area.

Similar to an active window, a trigger area can also be moved and vertexes can be moved/added or deleted.

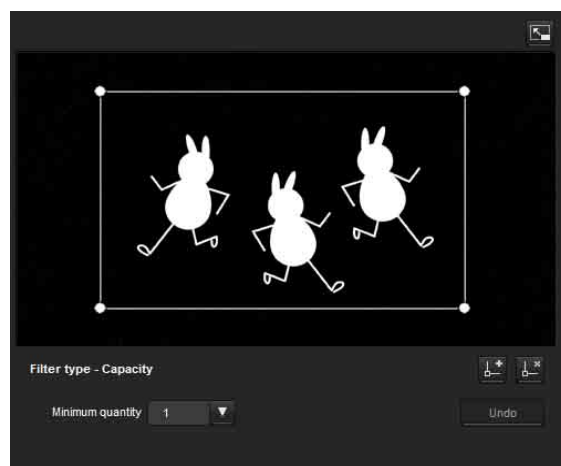
Disappearance



This criterion is whether an object disappeared in the trigger area.

Similar to an active window, a trigger area can also be moved and vertexes can be moved/added or deleted.

Capacity

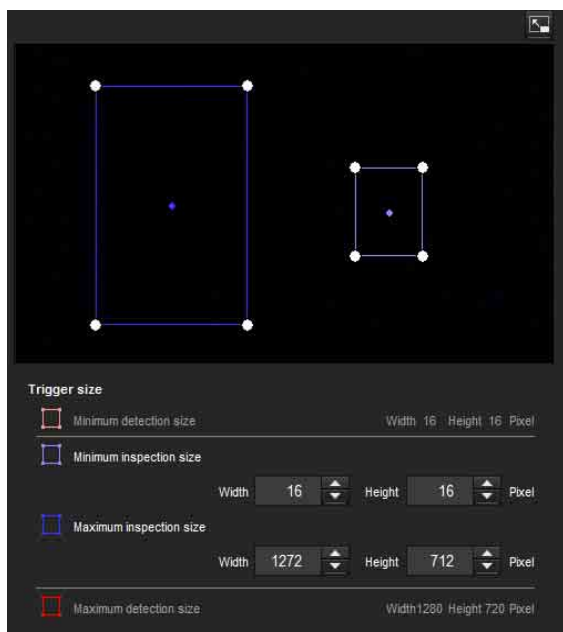


This criterion is the number of objects found in the trigger area.
The quantity is specified from the pull-down list.
Similar to a active window, the trigger area can also be moved and its vertexes can also be moved, added or deleted.

Minimum quantity: The quantity is specified from the “Minimum quantity” pull-down.

Trigger size

Specify the minimum trigger size and maximum trigger size of the object. To specify the size, you can either enter values or drag the vertexes of the area.



The size of an object is measured in pixels.

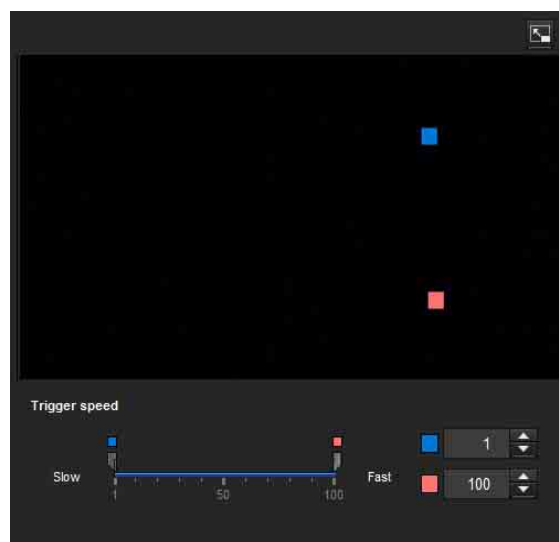
- When you place the cursor on the area, the cursor changes to a crossed arrow, which you can drag to move the minimum trigger size area and maximum trigger size area.
- Placing the cursor on the vertex of the minimum trigger size area or maximum trigger size area will change the cursor to $\leftrightarrow$, then you can drag the vertex to change the inspection size.

Tip

The minimum and maximum detection sizes configured in the VMD setting are displayed, but the size of the area cannot be modified from here.

Trigger speed

Specify the range of the speed of object to inspect by determining Min. speed and Max. speed.



- Min. speed and Max. speed can be specified within a scale of 100.
- The blue marker for minimum speed cannot be set to the right of the red marker for maximum speed.
- The squares indicating Min. speed and Max. speed move on the right and left sides of the preview screen.

Note

The set value is only valid under the conditions of **Passing**, **Appearance** or **Disappearance**.

Full-screen display button

Click  to display the ActiveX area in full screen. Clicking again will show the normal display.

Stretch bar

Click  to hide the menu list on the left and enlarge the preview screen. Clicking again will show the menu list as it was before.

OK/Cancel

Click **OK** to finalize any changes made to the settings and send them to the camera.

If you click **Cancel**, changes made to the settings will be discarded and the screen will be reloaded with the current camera settings.

Configuring the Viewer

— Viewer Menu

Click **Viewer** in the Administrator menu to display the Viewer menu.

Using this menu, you can select the viewer to use and configure advanced settings.

Layout tab

Homepage

Set the viewer or homepage to be displayed at the time of access.

ActiveX viewer: Displays the ActiveX viewer at time of access.

Plug-in free viewer: Displays the Plug-in free viewer at time of access.

Custom: Select the homepage to be displayed.

With SNC-CH140, you can write data in the built-in flash memory or CF memory card (not supplied) to use your favorite homepage. With SNC-DH140, write data to the built-in flash memory to use your favorite homepage.

To store a homepage HTML file in the built-in flash memory, use the Custom Homepage function of SNC toolbox included in the supplied CD-ROM. To learn how to use the Custom Homepage, see page 88.

For details on supported cards, contact your authorized Sony dealer.

To display your Custom homepage perform the following operation:

- 1 Select **Custom**.
- 2 Type the path of the HTML file using up to 64 characters in the text box on the right of **Path**.
- 3 In **Selected memory**, select the memory in which the homepage is stored.
You can select **Flash memory** or **CF memory card**.
The directory displayed in the text box on the right of **Path** changes according to the selected memory.

Header

Configure the setting for the bar menu displayed at the top of the viewer screen. Select **On** to display the header, and **Off** to hide it.

Tip

Even when you select **Off**, the Administrator menu can be displayed by entering the following URL in the address box of your Web browser.

Example: When the IP address of the camera is set to 192.168.0.100

`http://192.168.0.100/<TAG>/l4/index.html`

Enter the following value to <TAG> according to the language you wish to use.

en : English

ja : Japanese

fr : French

de : German

it : Italian

es : Spanish

zh : Chinese

Button Style

Select **Standard** or **Simple**.

Logo

To set the logo image, click **Browse** and specify the URL of the logo image to display.

Text color, Background color 1, and Background color 2

Specify the background colors and font color.

To specify the color, enter “#” followed by an RGB value in 6-digit hexadecimal.

The first 2 digits after # represent red, the next 2 digits green, and the last 2 digits blue. Specify the brightness for each color. 256 brightness levels are available (00-FF).

Camera list

You can register cameras in the camera list. By selecting a registered camera on the viewer screen, you can see the images from the registered camera.

Note

The camera list can be set only when Plug-in free viewer is selected as the homepage.

On/Off

Select **On** to show the camera list, and **Off** to hide it.

Style

You can configure the camera list style.

Background color

Specify the background color of the camera list. The colors are specified in the same way as those for the header.

Registering in Cameras

Specify a number on the camera list and set the IP address, port number, and comment for each camera.

Insert: Click to register a camera in the camera list.

Modify: Click to edit a selected camera list.

Delete: Click to delete a selected camera list.

Down: Click to decrement the number indicating registered camera numbers.

Up: Click to increment the number indicating registered camera numbers.

Text

Note

The camera list can be set only when Plug-in free viewer is selected as the homepage.

Text1 text, Text2 text and Text3 text

Enter the text to be displayed on the viewer screen.

Text1 link, Text2 link and Text3 link

Specify the URL of the link to assign a link to the text.

Text color, Background color 1, and Background color 2

Specify the font color of the text and background colors. The colors are specified in the same way as specifying those for the header.

Show comment if camera selected

Select this option to display comments on the viewer screen.

Monitor

Configure the setting for the camera image display part of Plug-in free viewer.

Note

The camera list can be set only when Plug-in free viewer is selected as the homepage.

Initial streaming

Set the display method for camera image for streaming.

Initial image size

Set the initial camera image size.

Initial PTZ

Set the pan/tilt/zoom operation modes for streaming.

Tip

This device is not equipped with operational functions for PTZ.

Initial frame rate

Set the initial camera image frame rate.

Initial image

Set what to initially display on the camera image display area.

Still image

JPEG still images are acquired from the camera and displayed at start-up.

Specified image (URL)

Specify a still image of your choice by URL at start-up.

Auto play

Run to start playback.

Blank

No display at start-up.

Click to start streaming

By ticking this when **Still image** or **Specified image** is selected, you can start play by clicking on the image.

Tip

If the menu display is **Off**, **Blank** cannot be selected.

Initial sound

Set the initial volume for when streaming starts. Check **Mute** for muting sound.

Note

This setting is valid only when **SNC ActiveX viewer** is selected for **Streaming method** from **Setting** of the Plug-in free viewer control bar.

Show menu

Set whether to have a frame or not in the camera image area.

Set whether to show or hide operation buttons at the bottom of the camera image area.

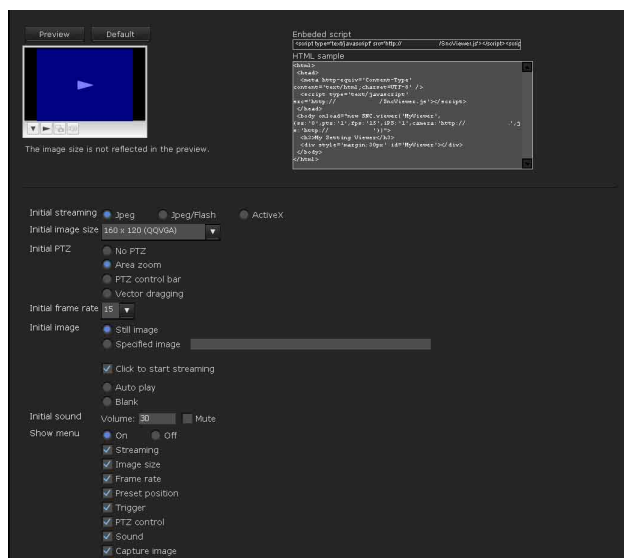
OK/Cancel

See “Buttons common to every menu” on page 26.

HTML output tab

If the monitor is for personal use, this tab can be used to output sample source for HTML and script.

For details on the setting, refer to “Monitor” of the Layout tab.



Monitor

Displays a preview.

Preview: Displays a preview on the monitor based on the current settings.

Default: Resets the setting.

Note

The selected image size is not used for the preview screen.

Embedded script

Displays the sample source for script.

HTML sample

Displays the sample source for HTML.

This section explains how to use the application software and commands, including the supplied CD-ROM.

Using the SNC toolbox

Explains the functions except those of the Network tab in SNC toolbox.

To install SNC toolbox, to assign an IP address and to set the network, see “Assigning the IP Address to the Camera” on page 6 in “Preparation.”

Notes

- SNC toolbox may not operate correctly if you use a personal firewall or antivirus software in your computer. In this case, disable the software or assign an IP address to the camera using another method. For an example, see “Assigning the IP Address to the Camera Using ARP Commands” on page 100.
- If you are using Windows XP Service Pack 2 or later, or Windows Vista, disable the Windows Firewall function. Otherwise SNC toolbox will not operate correctly. For the setting, see “Configuring Windows Firewall” in “When using Windows XP Service Pack 2 or later” on page 9 or “Configuring Windows Firewall” in “When using Windows Vista” on page 11.
- The model on sale in China does not support the SSL function.

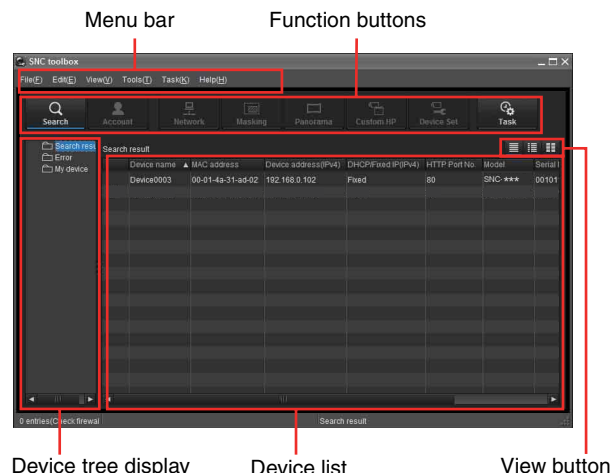
Starting SNC toolbox

Select **Program** from the Start menu of Windows, then select **SNC toolbox** and **SNC toolbox** in sequence. SNC toolbox starts.

The main screen appears. SNC toolbox detects cameras connected to the local network and lists them on the Network tab window.

When you are using Windows Vista, message “User Account Control – An unidentified program wants access to your computer” may appear. In this case, click **Allow**.

How to use SNC toolbox



Menu bar

All functions can be selected from here.

File (F) menu

Import: Reads the Device list file (CSV format).

Export: Outputs the Device list in a CSV format file.

Close: Exits SNC toolbox.

Edit (E) menu

Cut: Cuts off a device or folder.

Copy: Copies a device or folder.

Paste: Pastes a device or folder.

Select All: Selects all devices in the Device list.

Add Folder: Creates a folder.

Add Device Entry: Manually registers a device.

Modify Device Entry: Edits the device information.

Remove: Removes a device from a folder.

Delete: Deletes a device or folder.

View (V) menu

Status Bar: Switches show/hide of status at the bottom of the screen.

Normal: Displays detailed information on a device.

Snapshot small: Displays detailed information on a device with a small thumbnail.

Snapshot large: Lists devices with large thumbnails.

Column Setting: Displays the setting screen for the items to display on the list.

Tools (T) menu

Search: Searches again for devices.

Login Setting: Displays the management screen for user names and passwords related to the device.

Network Setting: Displays the screen for modifying the address settings for the selected device.

Device Setting: Displays the settings screen for the selected device.

Privacy Masking: Displays the Privacy Masking screen.

Panorama Creator: Displays the Panorama Creator screen.

Not available with this product.

Custom Homepage: Displays the Custom Homepage screen.

Firmware Upgrade: Displays the Firmware Upgrade screen.

Initialize Device:

- Reboot:** Restarts the device.
- Factory Default:** Initializes the device to factory default.

Backup setting data: Backs up setting data on a computer.

Device Homepage: Connects to the device.

Device Log:

- System Log:** Obtains system log for the device.
- Access Log:** Obtains access log for the device.

Tool Log: Obtains SNC toolbox log.

Option: Displays the screen for modifying SNC toolbox settings.

Task (K) menu

Task List: Displays the Task list screen.

Add Task: Displays the Task Wizard screen.

Modify Task: Displays the Task editing screen.

Delete Task: Deletes task.

Help (H) menu

Version: Displays SNC toolbox version information.

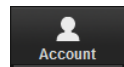
Function buttons

Function buttons are used for updating lists and displaying dialog.



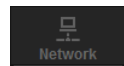
Search

Updates the Device list in the search result.



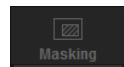
Account

Sets the administrator for each device.



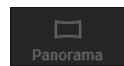
Network

Displays the **Network Setting** dialog.



Masking

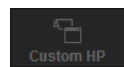
Displays the **Privacy Masking** dialog.



Panorama

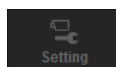
Displays the **Panorama Creator** dialog.

Not available with this product.



Custom HP

Displays the **Custom Homepage** dialog.



Setting

Displays the settings screen for the device.



Task

Displays the **Task List** dialog.

Device tree view

This function allows you to customize folders. The registration details of My device can be displayed in tree format.

Search result folder

When this folder is selected, devices in the same segment detected at time of startup or by **Search** are displayed in the Device list.

Error folder

When this folder is selected, devices registered in My device folder that can not be connected are displayed in the Device list.

Also, if a registered device is not found on the network, it will also be registered in this folder.

My device folder

When this folder is selected, devices in the Search result folder or registered manually are displayed in the Device list.

Device list

Devices registered in the folder selected at Device tree view are displayed in a list.

Device name

Displays individual device names.

Status (Only for Error folder and My device folder)

You can check the current connection status.

MAC address

You can check the MAC address of the device.

Device address

You can check the IP address of the device.

Port No.

You can check the port number of the device.

DHCP/Fixed IP

Displays whether the IP address of the selected device is DHCP or fixed IP.

Model

Displays the model name.

Serial No.

Displays the serial number.

Version No.

Displays the version of firmware.

Admin name

Displays the administrator user name.

Tips

- A camera with which SSL communication has been performed will show  on the left side of its IP address.
- The model on sale in China does not support the SSL function.

View button

You can change the display format of the Device list (page 85) .

Registering in My device

The device tree has three folders by default: **Search result**, **Error** and **My device**.

The **Search result** folder and **Error** folder are fixed, so you cannot edit the content or rename the folder.

The **My device** folder can be renamed, and you can add, delete and move folders.

Search result folder

Displays devices detected by search.

Error folder

Displays devices that are not connected.

My device folder

You can sort and manage devices using any folder.

Adding a folder

- 1 Select the parent folder to which you want to add a folder.
- 2 Right click the mouse and select **Add Folder** from the displayed menu.
A folder is added. Enter a folder name of your choice.

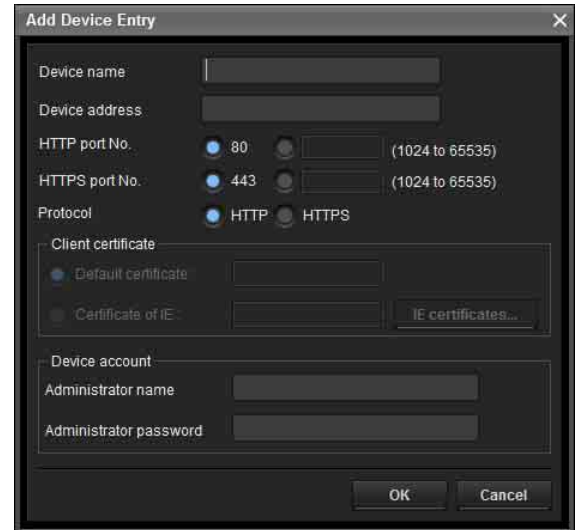
Registering a device

To register a device, follow the procedure below:

- Registering by **Add Device Entry** dialog
- Registering by drag & drop
- Registering by copy & paste

Registering by Add Device Entry dialog

- 1 Select the folder to register the device.
- 2 Right click the mouse and select **Add Device Entry** from the displayed menu.
The **Add Device Entry** dialog appears.

The image shows a screenshot of the 'Add Device Entry' dialog box. It has a title bar with a close button. The dialog contains several input fields and radio buttons. 'Device name' and 'Device address' are text boxes. 'HTTP port No.' and 'HTTPS port No.' are spinners with values 80 and 443 respectively, and a range '(1024 to 65535)' shown. 'Protocol' has radio buttons for 'HTTP' (selected) and 'HTTPS'. 'Client certificate' has radio buttons for 'Default certificate' (selected) and 'Certificate of IE', with a button 'IE certificates...' next to the second option. 'Device account' has fields for 'Administrator name' and 'Administrator password'. At the bottom are 'OK' and 'Cancel' buttons.

- 3 Enter the following items:
Device name: Enter a device name of your choice.
Device address: Enter the address of the device to register.
HTTP port No.: Normally, 80 should be selected. When setting a value other than 80, select the textbox and enter a port number.
HTTPS port No.: Normally select 443. When setting a value other than 443, select the textbox and enter a port number.
Device account: Enter the user name and password of the administrator who will access the device in the **Administrator name** field and **Administrator password** field, respectively.
- 4 Click **OK** to finish registration.

Registering by drag & drop

To add a device, select a device from the Device list in the Search result folder, and drag & drop to the folder to register it in.

Registering by copy & paste

Select a device from the Device list in the Search result folder and right click the mouse. Select **Copy** from the displayed menu (or select **Copy** from the **Edit** menu). Next, select the folder to register in and right click the mouse. Select **Paste** from the displayed menu.

Renaming the device/folder

Select the folder or device to rename and right click the mouse. Select **Rename** from the displayed menu. The device/folder name is highlighted. Enter the new name.

Deleting a device/folder

Select the device/folder to be deleted from the Device list or Device tree and right click the mouse. Select **Delete** from the displayed menu (or select **Delete** from the **Edit** menu).

Moving a device/folder

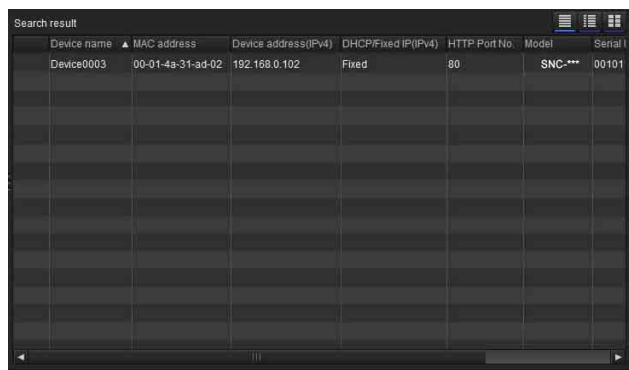
You can move a device/folder by following either of the methods below:

- Select a device/folder from the Device list or Device tree and drag & drop in the folder to move it to, which will move the device/folder.
- Select a device/folder from the Device list or Device tree and right click the mouse. Select **Cut** from the displayed menu (or select **Cut** from the **Edit** menu). Next, select the folder to move to and select **Paste**.

Changing the Device list display method

Details display

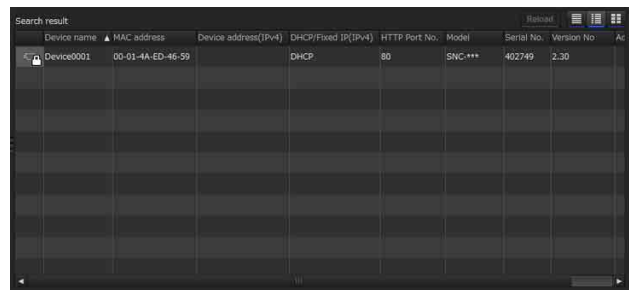
Select **Normal** from the **View** menu or click  to set to the details display.



Device name	MAC address	Device address(IPv4)	DHCP/Fixed IP(IPv4)	HTTP Port No.	Model	Serial
Device0003	00-01-4a-31-ad-02	192.168.0.102	Fixed	80	SNC***	00101

Details display with thumbnails

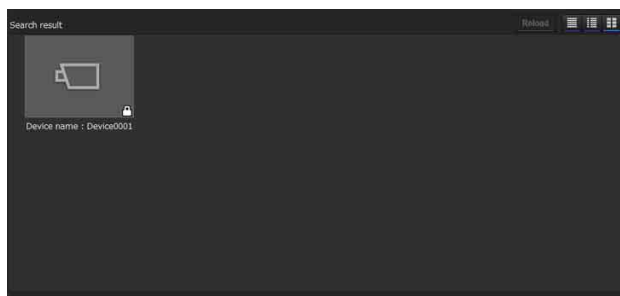
Select **Snapshot(S)** from the **View** menu or click  to set to the details display with thumbnails.



Device name	MAC address	Device address(IPv4)	DHCP/Fixed IP(IPv4)	HTTP Port No.	Model	Serial No.	Version No.	Action
Device0001	00-01-4A-ED-46-59		DHCP	80	SNC***	402749	2.30	Ac

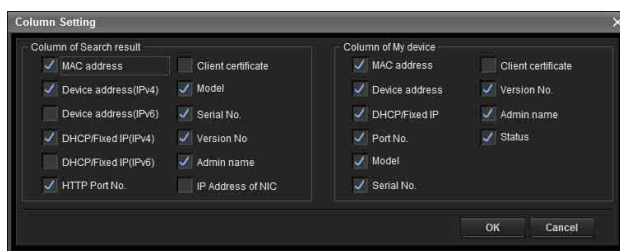
Display with large thumbnails

Select **Snapshot(L)** from the **View** menu or click  to set to display with large thumbnails.



Modifying the items to show on list

Select **Column setting** from the **View** menu to display the “Column Setting” dialog.



Check the items you want to display and remove the checks from items you want to hide.

Click **OK** after making the changes. The new setting is reflected on the list and the display returns to the main screen.

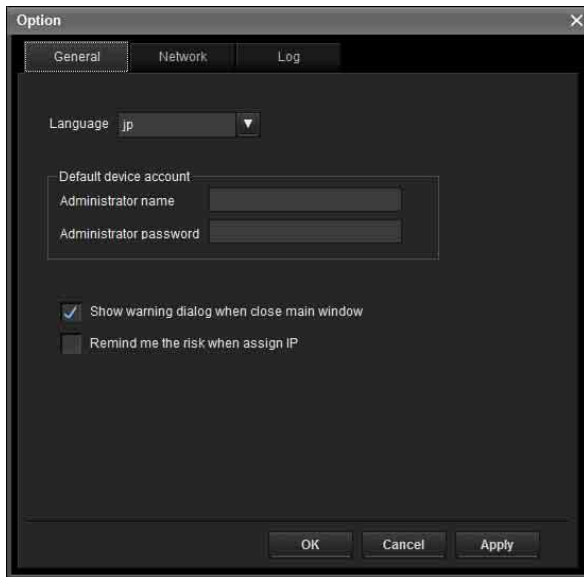
Updating thumbnail images

To display the thumbnail, select the camera of the thumbnail you wish to update and click **Reload** to display the current camera image as the thumbnail.

Setting SNC toolbox options

Select **Option** from the **Tools** menu to display the “Option” dialog. This dialog consists of three tabs: **General**, **Network** and **Log**.

General tab



Language

Set language.

Default device account

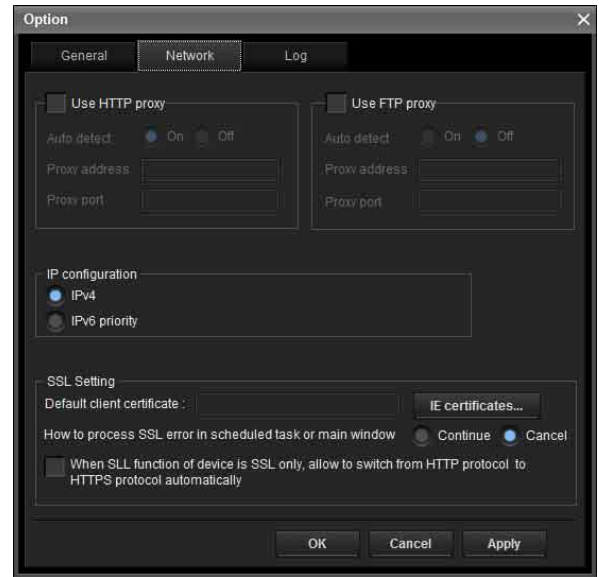
Set the initial values of user name and password for the administrator accessing the device for each device.

Show warning dialog when closing main window:

Select to display the warning message.

Remind me the risk when assigning IP: Select to display the warning message.

Network tab



Configure the HTTP proxy and FTP proxy. When using HTTP proxy, check **Use HTTP proxy**. When using FTP proxy, check **Use FTP proxy**. To auto-detect the proxy server, select **On** for **Auto detect**.

If you are not auto-detecting the proxy server, select **Off** for **Auto detect**, and enter the proxy address and proxy port number.

IP configuration

Select IPv4 or IPv6 priority for combined use of IPv6 and IPv4.

SSL Setting

Configure the SSL setting.

Default client certificate: Enter the client certificate to use.

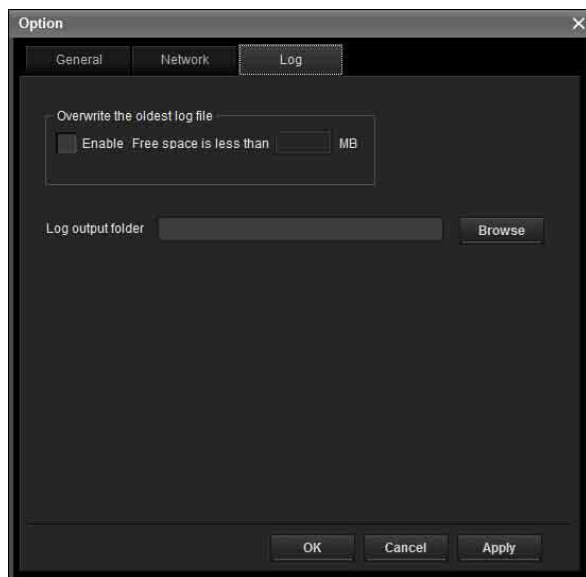
How to process SSL errors in scheduled task or main window: Select **Continue** or **Cancel**.

When SSL function of device is SSL only, allow to switch from HTTP protocol to HTTPS protocol automatically: Check this box if necessary.

Notes

- When you have changed the SSL setting, restart the SNC toolbox.
- The model on sale in China does not support the SSL function.

Log tab



Overwrite the oldest log file

To set the size of the log file, check **Enable** and specify the minimum required space for a log file.

Log output folder

Click **Browse** to display the folder selection dialog. Specify the folder to save the log.

Using Privacy Masking — Masking a Camera Image

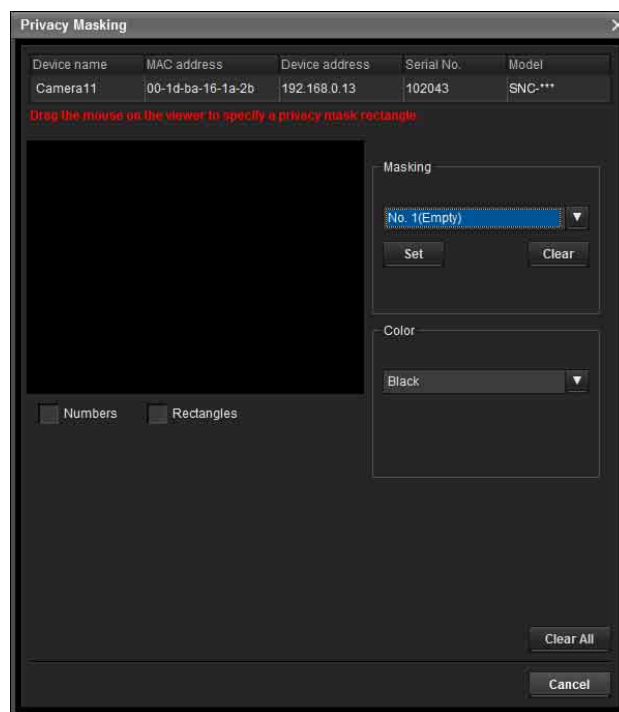
The Privacy Masking function of SNC toolbox allows you to mask parts of the camera image to be transmitted.

- 1 Select the camera to set a privacy mask from the Device list.
- 2 Click **Masking**.

Using the Privacy Masking

The Privacy Masking screen enables you to set the privacy mask position. Click **Masking** to display the Privacy Masking screen.

Privacy Masking screen



Viewer

A live image of the camera is displayed. You can specify the position of the privacy mask in this area.

Number

The set mask number is displayed in Viewer.

Frame

Display the frame of the set mask to distinguish the mask area when the set mask is overlapped.

Privacy mask setting section

Allows you to set or delete the privacy mask. You can set up to eight privacy masks.

Set: Register the area specified on the viewer as a privacy mask area.

Click **Set** and the portion of the viewer image is masked with the privacy mask. The color of the privacy mask is that selected with the **Color** drop-down list.

Note

If the mask area is close to the bottom of the image, the background at the bottom may still be visible.

Color

Specify the color or mosaic of privacy masks. This setting is common to every privacy mask.

The selectable colors are as follows:

Black, White, Gray, Red, Green, Blue, Cyan, Yellow, Magenta

Clear all

Click to delete all privacy masks simultaneously.

Setting a privacy mask

To set a privacy mask in a desired position, do the following:

- 1 Specify the privacy mask area by dragging the mouse on the viewer.
- 2 Select the color or mosaic of the mask from the **Color** drop-down list.

Note

The color is common to every privacy mask. The color last selected is applied.

- 3 Select the desired privacy mask number in the privacy mask setting section, and then click **Set** of the corresponding number.
The mask is displayed on the viewer.

Using the Custom Homepage — Setting the customized homepage

The Custom Homepage function of the SNC toolbox allows you to store the homepage that you have created in the camera and watch it.

Notes on creating the homepage

When you are creating the homepage, note the following points.

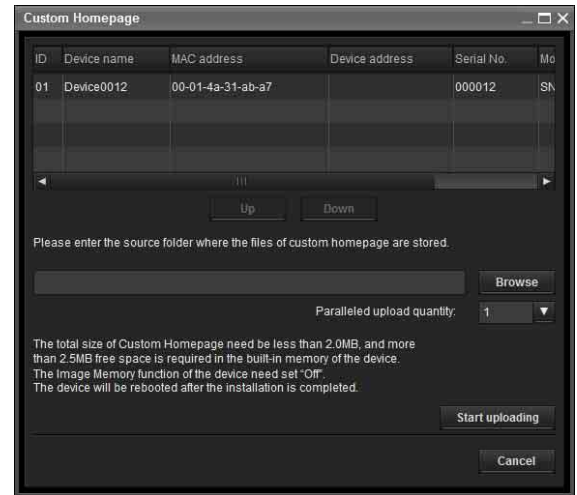
- The file name should be typed using up to 24 characters including the extension.
- The file size of the homepage should be 2.0 MB or less.
- To see the created homepage, set the **Homepage** in the Layout tab from viewer menu.

Uploading the homepage to the camera using the Custom Homepage

- 1 Select the device to upload from the Device list.
You can select multiple devices at the same time.
- 2 Click the **Custom Homepage**.
The “Custom Homepage” dialog opens.
Read the notes carefully.

Note

If you cannot establish communications with the camera using the proxy server being used, connect the camera to the local network and run the Custom Homepage without using the proxy server.



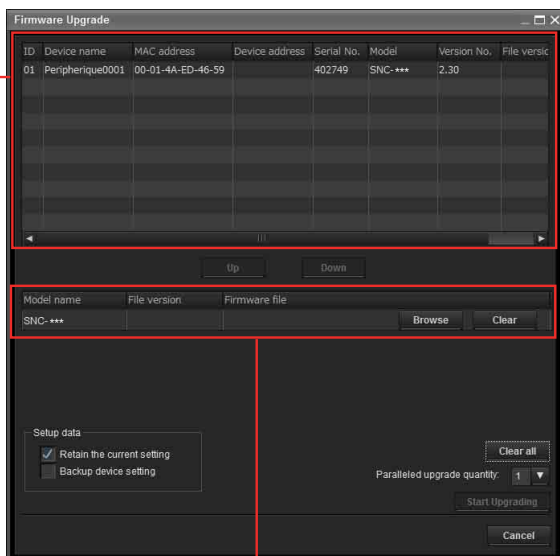
- 3 Type the path in which your homepage is stored.
- 4 Click **Start uploading**.
Uploading of the homepage file to the camera starts.
- 5 Click **Cancel** to exit the program.

Using the Firmware Upgrade

Using the Firmware Upgrade function of the SNC toolbox allows you to upgrade the firmware of the device.

Starting the Firmware Upgrade

- 1 Select the device to upgrade its firmware from the Device list.
You can select multiple devices at the same time.
- 2 Right click the mouse. Click **Firmware Upgrade** from the displayed menu.
The Firmware Upgrade screen is displayed.



Device list

Module list

Tip

The Firmware Upgrade screen can also be displayed using the following method:

- Select **Firmware Upgrade** from the **Tools** menu.

Device list

Select the device to upgrade.

A progress bar is displayed when updating is in process. The status field shows current status.

Module list

To display the dialog, click the **Browse** button on the right side of the model to update (listed in the module list). Select the target SVU file from the dialog. You can select one file for each model.

Updating

- 1 Set the order of devices perform update using **Up** and **Down**.
- 2 Click **Browse** and select an upgrade file for each model.
- 3 Select how many devices to upgrade in **Paralleled upgrade quantity**.
- 4 To back up the camera setting, check **Backup device setting**.
- 5 Click **Start upgrading**. Upgrading starts.

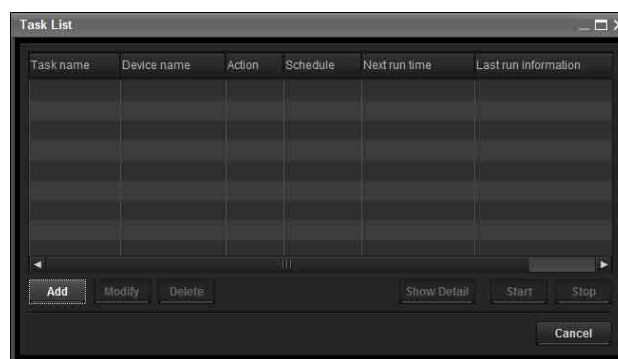
Notes

- To stop upgrading, click **Stop upgrading**. To protect some devices, during the process of upgrading, upgrading cannot be canceled.
- Do not turn off the power until the device restarts after upgrading.

Using the Schedule Task

You can specify the time or interval to change the Device setting or perform Firmware upgrade.

Click **Task** to display the Task List, which shows a list of scheduled executable tasks.



Task List

Displays the list of scheduled executable tasks.

Add

Displays the Task Wizard.

Modify

You can edit a task.

Delete

You can delete a task.

Start

This reserves a task.

Stop

You can cancel a task reservation.

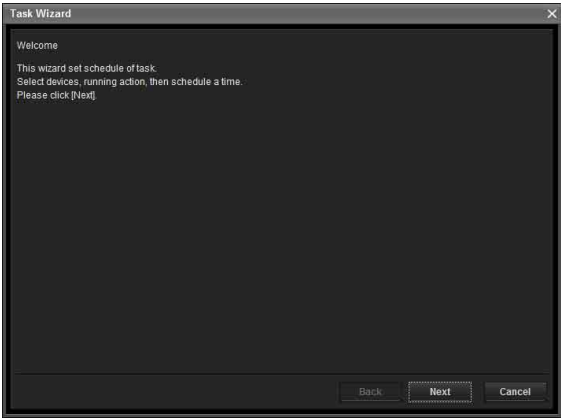
Cancel

Closes the Task List.

Creating a task

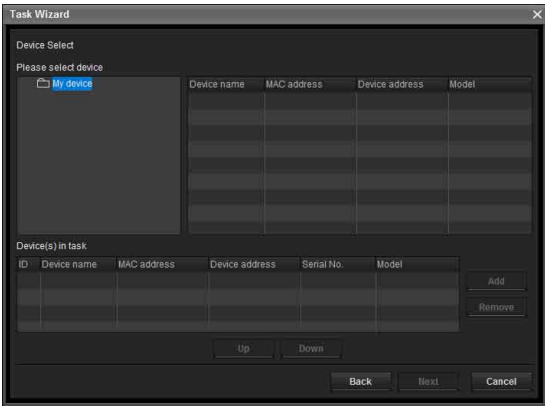
- 1 Click **Add**.

Displays **Task Wizard**.



2 Click **Next**.

3 Select a device to which the task is assigned.
A list of devices registered in My device is displayed. Select the device you want to assign the task to from the My device list, and register in Device(s) in task list.



My Device: Display a list of cameras registered in My devices.

Device(s) in task: Display a list of devices set to execute a task.

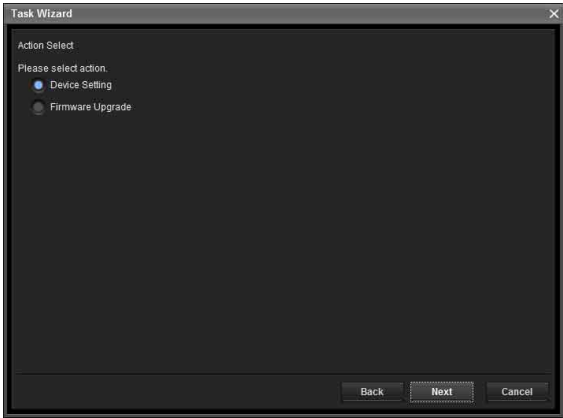
Add: Register a device in Device(s) in task.

Remove: Removes a device from Device(s) in task.

Up/Down: Changes the order of devices in Device(s) in task.

4 Click **Next**.

5 Select the task action.
Select **Device Setting** or **Firmware Upgrade**.



6 Click **Next**.

For Device Setting:

Edit the value for the setting you wish to change. See “Device Setting” on page 91 for changing the values.

Click **Next** to display the confirmation screen for setting change. Check to see if the setting is correct. If correction is needed, click **Back** to return to the previous screen to redo the setting.

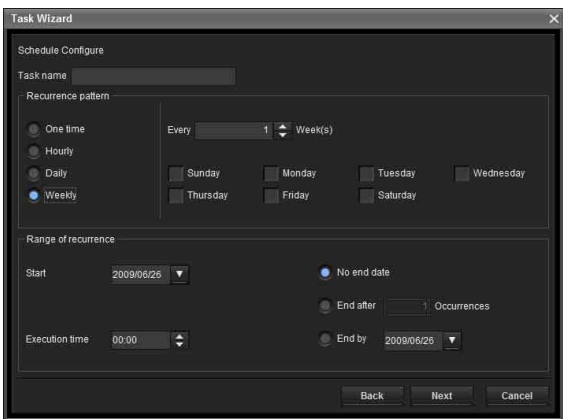
For Firmware Upgrade:

Set the firmware for the device you want to upgrade.

See “Using the Firmware Upgrade” on page 88 for setting firmware.

7 Click **Next**.

8 Set the schedule.



Task name
Name the task.

Others

Recurrence pattern

Specify the operation interval.

Onetime: Runs the task once.

Hourly: Specify the operation frequency in units of hours. (Possible set value: 1 to 99)

Daily: Specify the operation frequency in units of days. (Possible set value: 1 to 99)

Weekly: Specify the operation frequency in units of weeks and days of the week. (Possible set value: 1 to 99)

Range of recurrence

Specify the starting date and time, and the end date and time.

Start: Set the starting date.

Execution time: Set the starting time.

No end date: This setting does not set an end date.

End after: Specify the number of times to execute the operation.

End by: Set the end date.

- 9
- Click **Next**.
Check the setting when the final confirmation screen for task setting is displayed.
If correction is needed, click **Back** to return to the previous screen to redo the setting.

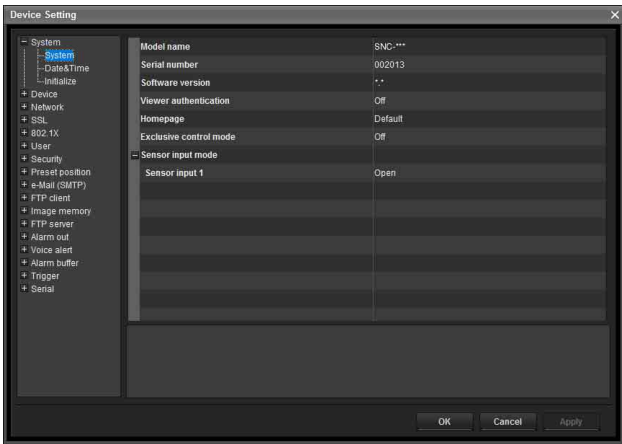
- 10
- Click **Finish**.

Configuring the device setting

You can configure advanced settings for a device on the Device Setting screen.

When you select a device(s) on the Device list and select **Device Setting** from the **Tools** menu, or when you right click on the device selection screen and click **Device Setting** in the displayed menu, the Device Setting screen is displayed.

Display sample:



Setting tree

All settings are sorted into categories. Click + to display the subcategories under a category. Click – to hide the subcategories.

Select a subcategory to display setting items on the right side of the screen.

Item

Displays the setting items. Select a line to change its value.

Value

Displays the value of an item. Select or enter a value to change the value.

Explanation

Displays the range of value for setting and supplementary explanations.

OK

Apply the setting and close the Device Setting screen. The main screen of SNC Toolbox is displayed.

Cancel

Close the Device Setting screen without changing the setting. The main screen of SNC Toolbox is displayed.

Apply

Apply the setting.

Other settings

See the relevant pages in “Administrating the Camera” when configuring the settings.

Setting items	Pages to refer to in “Administrating the Camera”
System	“Configuring the System — System Menu” on page 28
System	“System Tab” on page 28
Date	“Date & time Tab” on page 28
Superimpose	“Superimpose Tab” on page 29
Installation	“Installation Tab” on page 29
Initialization	“Initialize Tab” on page 30

Setting items	Pages to refer to in “Adminstrating the Camera”
Device	“Setting the Camera Image and Audio — Camera Menu” on page 31
Common	“Common Tab” on page 31
Picture	“Picture Tab” on page 32
Higher sensitivity	“Day/Night Tab” on page 35
Video codec	“Video codec Tab” on page 36
Streaming	“Streaming Tab” on page 37
Network	“Configuring the Network — Network Menu” on page 38
Network	“Network Tab” on page 38
Wireless	“Wireless Tab — Setting of wireless connection (SNC-CH140 only)” on page 39
QoS	“QoS Tab” on page 42
IP address notification	“Dynamic IP address notification Tab — Notifying the IP Address” on page 44
SSL	“Setting the SSL function — SSL Menu” on page 46
Setting	“SSL tab” on page 46
CA certificate	“CA certificate tab — Adding the CA certificate for client authentication” on page 48
802.1X	“Using the 802.1X Authentication Function — 802.1X Menu” on page 51
Common	“Common Tab – Basic setting of 802.1X authentication function” on page 51
Client certificate	“Client certificate Tab” on page 52
CA certificate	“CA certificate Tab” on page 53
User	“Setting the User — User Menu” on page 57
Security	“Setting the Security — Security Menu” on page 58

Setting items	Pages to refer to in “Adminstrating the Camera”
e-Mail (SMTP)	“Sending an Image via E-mail — e-Mail (SMTP) Menu” on page 58
Common	“Common Tab — Setting the e-Mail (SMTP) Function” on page 58
Alarm sending	“Alarm sending Tab — Setting the e-mail sending mode when detecting the alarm” on page 60
Periodical sending	“Periodical sending Tab — Setting the periodical e-mail sending mode” on page 60
FTP client	“Sending Images to FTP Server — FTP client Menu” on page 61
Common	“Common Tab — Setting the FTP client function” on page 61
Alarm sending	“Alarm sending Tab — Setting the FTP client action when detecting the alarm” on page 62
Periodical sending	“Periodical sending Tab — Setting the periodical FTP client activity” on page 63
Image memory	“Recording Images in Memory — Image memory Menu” on page 64
Common	“Common Tab — Setting the image memory function” on page 64
Alarm sending	“Alarm recording Tab — Setting the Image memory function when detecting the alarm” on page 66
Periodical sending	“Periodical recording Tab — Setting the periodical recording mode” on page 66
FTP server	“Downloading Images from the Camera — FTP server Menu” on page 68
Alarm Output	“Setting the Alarm Output — Alarm output Menu” on page 68
Alarm out 1	“Alarm out 1, 2 Tab” on page 68
Alarm out 2	

Setting items	Pages to refer to in “Administering the Camera”
Voice Alert	“Outputting Audio Linked to Alarm Detection — Voice alert Menu” on page 69
Voice alert 1	“Voice alert 1, 2, 3 Tab” on page 69
Voice alert 2	
Voice alert 3	
Alarm buffer	“Setting the Alarm Buffer — Alarm buffer Menu” on page 72
Trigger	“Setting the Operations from the Viewer — Trigger Menu” on page 70

Device restart and initialization

You can restart and initialize (restore factory default) a selected device. Multiple devices can be selected simultaneously for restart and initialization.

Restarting a device

Click **Tools**, **Initialize Device** and **Reboot** in this order on the menu bar to restart the device.

Initializing a device

Click **Tools**, **Initialize Device** and **Factory Default** in this order on the menu bar to initialize the device (restore factory default).

Using the SNC audio upload tool — Transmitting Audio to Camera

The supplied SNC audio upload tool allows you to transmit sound from the computer to the camera. This section explains the setup and operations of the SNC audio upload tool.

The SNC audio upload tool supports the following audio data to be transmitted.

Audio CODEC	Transmission rate
G.711 (μ-LAW)	64 kbps
G.726	40 kbps
G.726	32 kbps
G.726	24 kbps
G.726	16 kbps

Note

Only one user can transmit sound to the camera. Meanwhile, another user will not be able to transmit sound to the camera.

Installing the SNC audio upload tool

- 1 Insert the CD-ROM in your CD-ROM drive. A cover page appears automatically in your Web browser. If it does not appear automatically in the Web browser, double-click on the index.htm file on the CD-ROM.

When you are using Windows Vista, pop-up “**Auto Play**” may appear. For details, “Installing software” in “When using Windows Vista” on page 10.

- 2 Click the **Setup** icon of **SNC audio upload tool**. The “File Download” dialog opens.

When you are using Windows XP Service Pack 2 or later, or Windows Vista, a message regarding the active contents may appear. For details, see “Installing software” in “When using Windows XP Service Pack 2 or later” on page 8 or “Installing software” in “When using Windows Vista” on page 10.

3 Click **Open**.

Note

If you click “Save this program to disk” on the “File Download” dialog, you cannot install the tool correctly. Delete the downloaded file, and click the **Setup** icon again.

4 Install the SNC audio upload tool following the wizard displayed.

If the Software License Agreement is displayed, read it carefully and accept the agreement to continue with the installation.

Connecting the Camera to the Computer

1 Connect a speaker to the (line output) jack on the camera.

2 Connect a microphone to the microphone input jack on the computer.

Note

If the microphone input jack of the computer is not set correctly, no sound is transmitted from the computer and nothing is output from the speaker connected to the camera.

Set the microphone input jack from the control panel of Windows.

On Windows XP

- 1 Select **Sounds and Audio Device** from Control Panel.
- 2 Click **Volume** in the **Sound Recording** section on the Audio tab.
The Recording Control window opens.
- 3 Check **Select** in the **Microphone** section.

On Windows Vista

There are no settings regarding the microphone jack. If recording cannot be made, connect a microphone device to the computer and check that the recording device operates correctly, as follows:

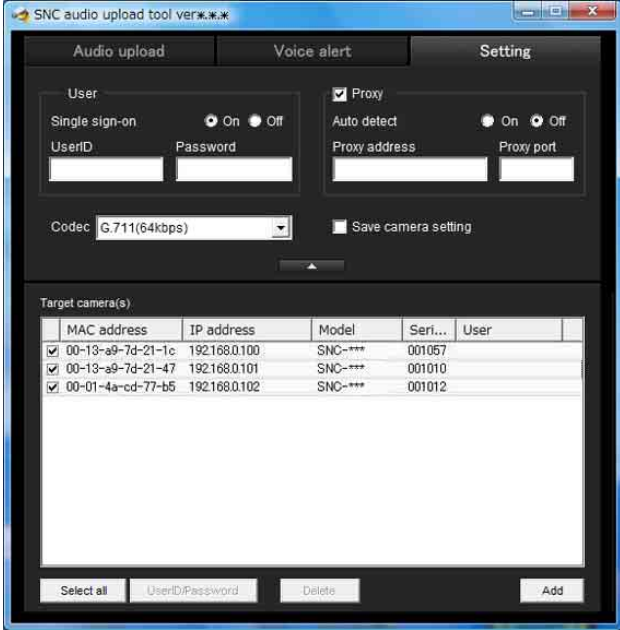
- 1 Select **Sound** from Control Panel.
- 2 Open the Recording tab and check that Windows has recognized the hardware correctly.

Using the SNC audio upload tool

When you start the SNC audio upload tool, the Setting tab is displayed.

Setting tab

Use this menu to set the camera to transmit audio from a computer or upload an audio file.



MAC address	IP address	Model	Seri...	User
00-13-a9-7d-21-1c	192.168.0.100	SNC-***	001057	
00-13-a9-7d-21-47	192.168.0.101	SNC-***	001010	
00-01-4a-cd-77-b5	192.168.0.102	SNC-***	001012	

User

Set the **User ID** and **Password** for the administrator. The factory setting of the User ID for the Administrator is “admin,” and the Password is “admin.”

Single sign-on: Select **On** to use the same user ID and same password for all the cameras. Select **Off** to set the user ID and password individually for each camera.

For details on setting with **Off**, see “User ID/Password” on page 95.

User ID: This item can be set when **Single sign-on** is set to **On**. The user ID specified here is applicable to all cameras.

Password: This item can be set when **Single sign-on** is set to **On**. The administrator password specified here is applicable to all cameras.

Proxy

Check this box when you use a proxy server for communications. When it is not checked, direct communication with the camera is performed.

Auto detect: Select **On** to obtain the proxy setting automatically from Internet Explorer.

Proxy address: Type the IP address or host name of the proxy server.

Proxy port: Type the port number used for communication with the proxy server.

Note

The Proxy setting is applicable to all cameras. You cannot use individual proxy settings for each camera.

Codec

Select the audio mode (Codec) from the drop-down list.

Save camera setting

Check this box to store the current settings and camera list in the Setting tab. The same settings will be recalled when the camera is rebooted.



Click this button repeatedly to hide/show the camera list.

Target camera(s) (Camera list)

When the SNC audio upload tool starts, it automatically detects Sony network cameras connected to the local network and displays them in the camera list. Up to 256 cameras can be displayed in the list.

Select the check box on the left of the row to enable audio transmission and audio file uploading for that camera. You can then enable these functions simultaneously for multiple cameras.

Notes

- If you are using Windows XP Service Pack 2 or later, or Windows Vista, disable the Windows Firewall function. Otherwise the camera list may not be displayed automatically. For details, see “Configuring Windows Firewall” in “When using Windows XP Service Pack 2 or later” on page 9 or “Configuring Windows Firewall” in “When using Windows Vista” on page 11.
- The SNC audio upload tool cannot detect cameras that are subsequently connected to the local network after the program has started.
- The SNC audio upload tool cannot detect network cameras that are not equipped with audio.

Camera select checkbox: The check box is located on the left end of the row. Select this check box to enable audio transmission and audio file uploading for that network camera.

MAC address: Displays the MAC address of the network camera.

IP address: Displays the IP address of the network camera. “DHCP” is shown at the end of the IP address when the IP address is obtained with a DHCP server.

Model: Displays the model name of the network camera.

Serial: Displays the serial number of the network camera.

User: Displays the specified user ID and password. The password is shown as turned letters.

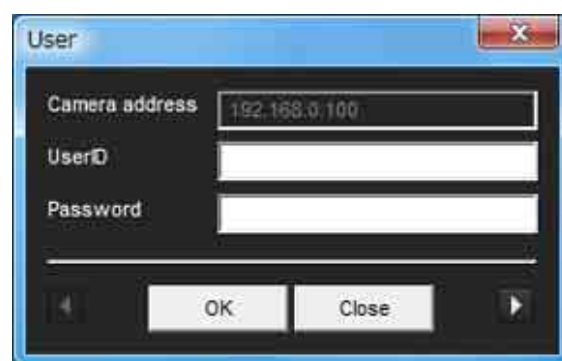
Select all

Click to select all the cameras in the camera list. This is useful, for example, when you delete all the cameras from the list or specify the same user ID and password for all cameras.

User ID/Password

Use this item when you specify the user ID and password to communicate with selected camera(s) only. Select camera(s) from the camera list and click this button. The following dialog opens.

Type the user ID and password for the administrator and click **OK**.



Note

If you select multiple cameras from the camera list, the same user ID and password are set for all those selected cameras. The factory setting for both items is “admin.”

Add

Use this item when you add a new network camera to the camera list manually. Click this button to open the following dialog.

Type the IP address and port number of the camera to be added and click **OK**.



Notes

- An error dialog appears if the specified IP address in the camera list is assigned for a device other than the network camera, or does not exist in the network.
- You cannot add new cameras if the maximum of 256 cameras has been reached.

Delete

Click this button to delete the selected camera(s) from the camera list.

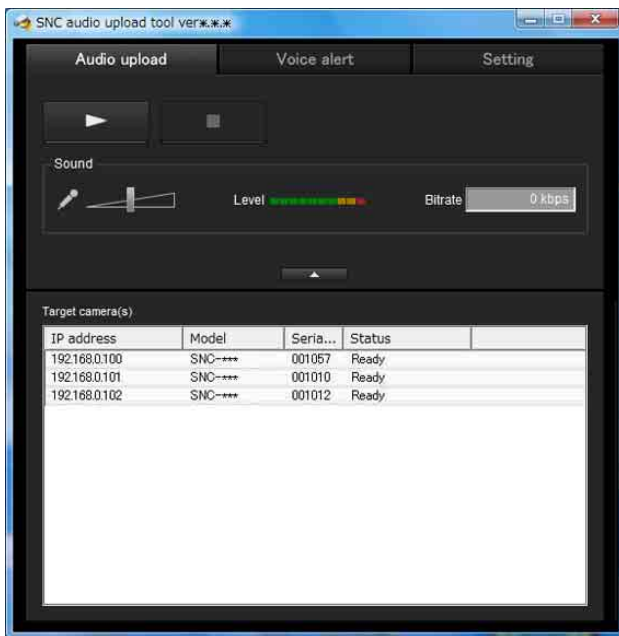
Note on switching the tab

If an error occurs when you switch from the Setting tab to the Audio upload tab or the Voice alert tab, the camera is shown in red. In this case, check the camera settings and the user ID and password settings.

Audio upload tab

Use this menu to transmit audio from the computer to the camera. You can transmit audio to multiple cameras displayed in the camera list simultaneously.

Before transmitting, set **Audio upload** to **Enable** on the Common tab of the Camera menu.



(start) / (stop)

Click (start) to start audio transmission. The transmission speed is displayed in the Bitrate box during transmission. You can adjust the microphone volume and enable/disable muting, if necessary.

To stop audio transmission, click (stop).

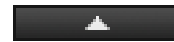
Notes

- Audio transmission stops if you switch the tab during transmission.
- Audio may be interrupted when the IP address is changed if **Obtain an IP address automatically (DHCP)** is set on **IP address** in the Network menu.
- Audio may be interrupted if you transmit it to many cameras simultaneously.

Sound adjustment and indicators

Adjust the microphone input volume by moving the slider bar. You can adjust the volume even during transmission.

Click to enable/disable sound muting. The microphone input volume level is displayed. The transmission rate is displayed in the Bitrate box.



Click this button to hide the camera list. Click it again to display the camera list.

Target camera(s) (Camera list)

Displays the cameras selected with the camera select checkbox of the camera list in the Setting tab.

The list shows the information and status of the selected cameras.

IP address: Displays the IP address of the network camera. "DHCP" is shown at the end of the IP address when the IP address is obtained with a DHCP server.

Tip

During SSL communication, appears on the left side of the IP address of the camera.

The model on sale in China does not support the SSL function.

Model: Displays the model name of the network camera.

Serial: Displays the serial number of the network camera.

Status: Displays the current status of the camera.

Ready: The camera is ready for connection.

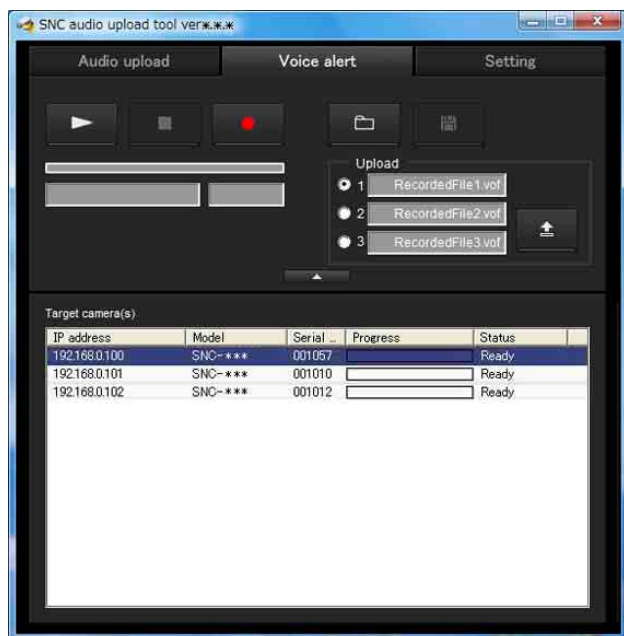
Connected: Camera connection was successful.

Fault: Camera connection failed.

Sending: Audio data is being transmitted.

Voice alert tab

Use this menu to record sound via a microphone connected to the computer, and upload the recorded audio file to the camera. You can upload the audio file to multiple cameras selected from the camera list simultaneously.



(playback)

To start playback, open the recorded file or another audio file and click this icon.

You can check the recorded sound or the contents of the selected audio file. During playback, the progress bar shows playback progress.

(stop)

Click to stop recording or playback.

When you click it during recording, recording stops, and you can review the recorded sound or upload the recording to the camera.

When you click it during playback, playback stops and the progress bar returns to the start position.

(recording)

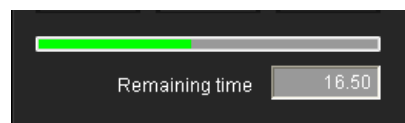
Click to start recording of sound via the computer's microphone. Maximum recording time is 30 seconds. The codec specified in the Setting tab is used for the recording.

The recorded file is displayed as "RecordedFile.vof."

Notes

- Recording or playback stops if you switch the tab during recording or playback.
- The recorded file is not stored in the computer.

Recording/playback progress bar



You can check recording or playback progress with this bar.

During recording, the far right of the bar represents 30 seconds, and the remaining recording time is numerically displayed below the bar.

During playback, the length of the bar depends on the recorded time.

(file open)

Click to select a previously saved audio file. You can play the selected audio file or upload it to the camera.

(save)

Click to save a recorded audio file to the computer.

Voice alert number select



Specify the voice alert number to which you want to upload an audio file. For example, select **1** when uploading to voice alert 1.

The name of the uploaded audio file is displayed to the right of the number.

"Not uploaded" is displayed if no audio file is uploaded to the camera.

The audio file name will be "RecordedFile" + "Voice alert number" + ".vof" if you upload an audio file recorded using  and not stored in the computer.

Note

The audio file name for the camera selected in the camera list is displayed here. To check the uploaded file name, click on the camera in the camera list.

(upload)

Click to upload the recorded or selected audio file to the camera specified in the Setting tab. Only one audio file can be uploaded to the camera at a time.

Note

Uploading a new audio file overwrites the audio file previously uploaded to the camera.



Click this button to hide the camera list. Click it again to display the camera list.

Target camera(s) (Camera list)

Displays the cameras selected with the camera select checkbox of the camera list in the Setting tab.

The list shows information and status of selected cameras.

IP address: Displays the IP address of a network camera. “DHCP” is shown at the end of the IP address when the IP address is obtained from a DHCP server.

Tip

During SSL communication,  appears on the left side of the IP address of the camera.

The model on sale in China does not support the SSL function.

Model: Displays the model name of the network camera.

Serial: Displays the serial number of the network camera.

Progress: Displays the progress of audio file transmission.

Status: Displays the current status of the camera.

Ready: The camera is ready for connection.

Inquiry: Camera information is being requested.

No func: The camera does not support the Voice alert function.

Uploading: An audio file is being uploaded.

Fault: Audio file uploading failed.

No Privilege: The camera is not authorized to upload audio files.

Succeeded: The audio file uploaded successfully.

Uploading a recorded audio file to the camera

Tip

Before operating, create an audio file and set the camera to upload using the Setting tab.

- 1 Click  (recording) in the Voice alert tab to start recording.
- 2 Click  (stop) to stop recording.
Recording will stop automatically in 30 seconds.
- 3 Select the voice alert number.
- 4 Click  (upload) to transmit the audio file to the camera.

Saving the recorded audio file to the computer

- 1 Click  (recording) in the Voice alert tab to start recording.
- 2 Click  (stop) to stop recording.
Recording will stop automatically in 30 seconds.
- 3 Click  (save).
The **Save as** dialog appears. Type the file name and save it.

Uploading the saved audio file to the camera

- 1 Click  (file open) in the Voice alert tab and select the audio file to be uploaded.
- 2 Select the voice alert number.
- 3 Click  (upload) to transmit the audio file to the camera.

Using the SNC video player — Playing a Video/Audio File Recorded with the Camera

The supplied SNC video player allows you to play video/audio data recorded with the camera on your computer.

This section explains the setup and operations of the SNC video player.

Installing the SNC video player

- 1 Insert the CD-ROM in your CD-ROM drive. A cover page appears automatically in your Web browser. If it does not appear automatically in the Web browser, double-click on the index.htm file on the CD-ROM.

When you are using Windows Vista, the pop-up “Auto Play” may appear. For details, see “Installing software” in “When using Windows Vista” on page 10.

- 2 Click the **Setup** icon of **SNC video player**. The “File Download” dialog opens.

When you are using Windows XP Service Pack 2 or later, or Windows Vista, a message regarding the active contents may appear. For details, see “Installing software” in “When using Windows XP Service Pack 2 or later” on page 8, or “Installing software” in “When using Windows Vista” on page 10.

- 3 Click **File open**.

Note

If you click “Save this program to disk” on the “File Download” dialog, you cannot install the player correctly.

Delete the downloaded file, and click the **Setup** icon again.

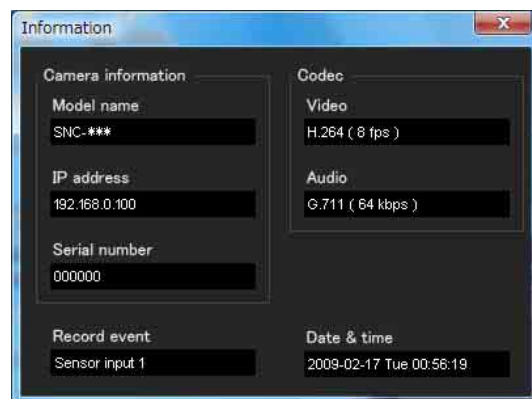
- 4 Install the SNC video player following the wizard displayed. If the Software License Agreement is displayed, read it carefully and accept the agreement to continue installation.

Using the SNC video player

- 1 Start the SNC video player.



- 2 Click the  (browse) icon. The Select File dialog opens.
- 3 Select the file you want to play. Click **INFO** on the top of the screen to open the file information dialog.



File dialog

Model name: Model name of the camera with which the file was recorded.

IP address: IP address of the camera with which the file was recorded.

Serial number: Serial number of the camera with which the file was recorded.

Date&time: Recording date and time

Movie: Video Codec

Audio: Audio Codec

Record event: Type of event used for the recording: **Sensor input, Camera tampering detection, VME, Motion detection**

Playing a video/audio file

Click  (start) to start playback from the beginning of the selected file.

To freeze the movie temporarily, click  (pause).

Click  again to resume playback from the freeze point.

To stop playback, click  (stop).

To start playback from the beginning, click  (start) again.

Playback stops when the file is played to the end.

Playing from a specified point

Move the slider bar below the image display, and playback will start from the position of the slider bar.

Adjusting the sound

Adjust the playing sound volume by moving the  slider bar. Move it to the left end for minimum volume, and to the right end for maximum volume.

Click  (speaker) to enable/disable sound (muting).

When sound muting is on, no sound will be heard, even if you move the slider bar.

Saving an image

Click the  (capture) icon during playback or pause and the captured image is displayed in a pop-up dialog. To save the image, click **Save** on the dialog. You can specify the destination to which the image is to be stored, and select the JPEG or Bitmap format.

How to change the image display size

Click **× 1/4**, **× 1/2**, **× 1**, **× 2** or **Full** at the top of the image to display the image in the selected magnification.

If you select **× 1**, the image is displayed in the original image display size of the file.

The **× 2** button is only available when image size is 640 × 480 (VGA) or smaller.

The selected image display size is highlighted.

Assigning the IP Address to the Camera Using ARP Commands

This section explains how to assign an IP address to the camera using ARP (Address Resolution Protocol) commands without using the SNC toolbox.

Note

When you turn on the camera, execute the ARP and PING commands within 5 minutes. Also when you restart the camera, execute the operation within 5 minutes.

- 1 Open the command prompt on the computer.
- 2 Enter the IP address and the MAC address of the camera to assign a new IP address, using the following ARP commands.

```
arp -s <Camera's IP address> <Camera's MAC address>
ping -t <Camera's IP address>
```

Example:

```
arp -s 192.168.0.100 08-00-46-21-00-00
ping -t 192.168.0.100
```

- 3 When the following line is displayed on the command prompt, hold down **Ctrl** and press **C**. Display stops.

```
Reply from 192.168.0.100:bytes=32 time...
```

You will normally receive a reply after about 5 repetitions of "Request time out."

- 4 Wait until the execution of PING finishes, then input the following code.

```
arp -d 192.168.0.100
```

Note

If you do not receive a reply, check the following:

- Did you enter the ARP commands within 5 minutes after it was turned on?
If not, turn off the camera and restart the operation.
- Is a NETWORK indicator turned on?
If the indicator goes off, the network connection has a problem. Connect the network correctly.
- Did you enter the IP address previously used for another device?
Assign a new IP address to the camera.
- Do the computer and the camera have the same network address?
If not, set the same network address on the computer and the camera.

Using the SNMP

This unit supports SNMP (Simple Network Management Protocol). You can read MIB-2 objects using software such as SNMP manager software. This unit also supports the coldStart trap which occurs when the power is turned on or the unit restarts, and the Authentication failure trap, which informs of any illegal access using SNMP.

Using CGI commands, you can set the community name and access limitation, host to send traps, and some MIB-2 objects. To allow these settings, you need authentication by the camera administrator.

1. Inquiry Commands

You can check the SNMP Agent settings using the following CGI commands.

<Method>

GET, POST

<Command>

http://ip_adr/snmpdconf/inquiry.cgi?inqjs=snmp
(JavaScript parameter format)

http://ip_adr/snmpdconf/inquiry.cgi?inq=snmp
(standard format)

With the above inquiry, you can obtain the following setting information. The following explains the setting information using the inqjs=snmp (JavaScript parameter) format.

```
var sysDescr="SNC-CH140", "SNC-DH140" ...①
var sysObjectID="1.3.6.1.4.1.122.8501" ...②
var sysLocation="" ...③
var sysContact="" ...④
var sysName="" ...⑤
var snmpEnableAuthenTraps="1" ...⑥
var community="1,r,public,0.0.0.0,v2c" ...⑦
var community="2,r,private,192.168.0.101,v2c" ...⑧
var trap="1,public,192.168.0.101,v2c" ...⑨
```

- ① Describes the case of “mib-2.system. sysDescr.0”. You cannot change this parameter.
- ② Describes the case of “mib-2.system. sysObjectID.0”. You cannot change this parameter.
- ③ Describes the case of “mib-2.system. sysLocation.0”. This field is used to describe information on the location of this camera. Nothing is set at the factory.

- ④ Describes the case of “mib-2.system. sysContact.0”. This field is used to describe information on the administrator of this camera. Nothing is set at the factory.
- ⑤ Describes the case of “mib-2.system. sysName.0”. This field is used to describe the administration node of this camera. Nothing is set at the factory.
- ⑥ Describes the case of “mib-2.snmpEnable AuthenTraps.0”. This example shows when “1” (enable) is set. In this setting, a trap occurs when there is an authentication failure. When “2” (disable) is set, no authentication failure trap occurs.
- ⑦ Describes the community attributes. This example shows the identification number “ID=1,” the community name “public,” and enables read from any IP address (0.0.0.0).
- ⑧ Describes the community attributes, similar to ⑦. This example shows the identification number ID=2, the community name “private,” and enables reading by SNMP request packet from the host “192.168.0.101”.
- ⑨ Describes the attributes to send a trap. This example shows the identification number “ID=1,” the community name “public,” and enables sending of traps to the host having the IP address “192.168.0.101”.

2. Setting Commands

The unit supports the following SNMP setting commands.

<Method>

GET, POST

<Command>

http://ip_adr/snmpdconf/snmpdconf.cgi?
<parameter>=<value>&<parameter>=...&...

First, perform the settings of the following parameters.

- 1) sysLocation=<string>
Set the case of “mib-2.system.sysLocation.0” in the <string> position. The maximum length of <string> is 255 characters.
- 2) sysContact=<string>
Set the case of “mib-2.system.sysContact.0” in the <string> position. The maximum length of <string> is 255 characters.

- 3) sysName=<string>
Set the case of “mib-2.system.sysName.0” in the <string> position. The maximum length of <string> is 255 characters.
- 4) enaAuthTraps=<value>
Set the case value of “mib-2.snmp.snmpEnableAuthenTraps.0” in the <string> position. Type “1” (enable) or “2” (disable) in the <value> position.
- 5) community=<ID>,r,<communityName>,<IpAddressString>
Set the community attributes. <ID> describes the setting identification number (1 to 8) <communityName> describes the community name to be set, and <IpAddressString> describes the IP address of the host you allow access (0.0.0.0 for any host).
Example: To allow reading by any host in the “private” community and having the ID number “2”.
community=2,r,private,0.0.0.0
- 6) trap=<ID>,<communityName>,<IpAddressString>
Set the attributes to send traps to. <ID> describes the setting identification number (1 to 8), <communityName> describes the community name to send traps to, and <IpAddressString> describes the IP address of the host to send traps to.
Example: To specify the destination of traps as the public community and the ID number “1”.
trap=1,public,192.168.0.101
- 7) delcommunity=<ID>
This parameter is used to delete the previous community setting. <ID> describes the community setting identification number (1 to 8).
- 8) deltrap=<ID>
This parameter is used to delete the previous setting of the host to send traps to. <ID> describes the trap setting identification number (1 to 8).

When you have finished changing the SNMP setting information using the above parameters 1) to 8), check the changed settings using an inquiry command. If the changed settings are OK, restart the SNMP using the following CGI command.

SNMP restart command

<Method>

GET, POST

<Command>

```
http://ip_addr/snmpdconf/snmpdconf.cgi?
snmpd=restart
```

Glossary

ActiveX control

A component program object that can be used with web pages or other application programs. The technology for creating ActiveX control is part of software developed by Microsoft.

AES

Abbreviation for Advanced Encryption Standard. This is the next-generation standard of encryption, adopted by the U.S. government.

ARP commands

The commands for checking the entry of the IP address and MAC address in a host computer, or for updating them.

Bandwidth control

To limit the amount of transmitted data.

Bit rate

The rate at which data bits are transmitted.

CA (Certificate Authority)

A private authority that issues and controls digital certificates to be used for authentication regarding network access.

Capture

To send audio and video converted to digital data from video devices to a computer.

Codec

Software/hardware for coding/decoding video and audio data.

Common name

A URL to be typed in the browser when you access a website employing SSL (Secure Sockets Layer) protocol with the security function. Access is successful after the URL of the website is verified as matching the server's common name.

Contrast

The difference in tone between the lightest and darkest portions of the image.

Default gateway

Device that can be used to access another network.

DHCP server

Acronym for Dynamic Host Configuration Protocol server. The IP address of a terminal without an individual IP address can be automatically distributed by the Dynamic Host Configuration Protocol (DHCP). The DHCP server assigns the IP addresses to the terminals.

Digital certificate

An electronic certificate that a CA (Certificate Authority) attests that a public key to cancel a secret code is issued by an authentic publisher.

Digital zoom

Zooming in/out function of an image without using an optical zooming function.

DNS server

Acronym for Domain Name System server. As an IP address required for connecting to the device on an IP network is numerical and difficult to remember, the Domain Name System was established. A domain name is alphabetic and is easier to remember. When a client computer uses a domain name to connect to another computer, it asks a DNS server to translate the name into the corresponding IP address. The client computer can then obtain the IP address of the computer to be connected.

EAP method

Acronym for Extensible Authentication Protocol. This is a protocol extended from PPP (Point-to-Point Protocol) and having an authentication function.

EAP-TLS authentication

TLS is an authentication protocol of the EAP methods using Transport Layer Security. By using digital certificates and other methods, EAP-TLS prevents data falsification, eavesdropping and spoofing.

Frame rate

The number of frames of a moving image that can be transmitted per a second.

FTP client

Software to be used for accessing the FTP server.

FTP server

A server to be used to transfer files via a network.

HTTP port

A port used to communicate between the web server and the web client, such as a web browser.

H.264

An image compression format. The standard written by the JVT (Joint Video Team) a joint organization for standardization (composed of ISO and ITU-T. H.264), is capable of transmitting video data at a higher compression rate than that of MPEG4.

IP address

Acronym for Internet Protocol Address. An individual IP address is basically assigned to each piece of equipment connected to the Internet.

JPEG

Acronym for Joint Photographic Expert Group. The still image compression technology or standards of ISO (International Organization for Standardization) and ITU-T. Popularly used as an image compression format on the Internet, etc.

MAC address

A network address that uniquely identifies each LAN card.

MPEG4

Acronym for Moving Picture Experts Group4. One of the MPEG standards for image compression format aiming to transmit images at a high compression rate with lower picture quality.

Multicast

The class D IP address assigned between 224.0.0.0 and 239.255.255.255. Using this IP address enables you to transmit the same data to multiple equipment.

Network address

The portion that identifies the local network (subnet) in an IP address.

Network bandwidth

Bit rate that can be used for networking.

NTP server

Network time server that transmits and receives time information over the networks.

Passive mode

The mode whereby a client FTP allows TCP connection for data transmission to the FTP server.

POP server

A server for storing incoming e-mail until you have read it.

Primary DNS server

One of the DNS servers that can first reply to a request by connected devices or other DNS servers.

Proxy server

A server or software that acts as an intermediary between a local network and the Internet so that it can connect to the Internet in place of a computer on a local network.

PSK

Abbreviation for Pre-Shared Key. This is a shared key to make an encryption key, used with TKIP in WPA encryption standard. PSK sometimes means an authentication system using a key previously shared.

QoS

Enter a value in the DSCP (Differential Service Code Point) field included in the IP header to control communication service quality.

RADIUS client

RADIUS (Remote Authentication Dial-in User Service) is an authentication and accounting protocol managing network access, and a RADIUS client is a party that accesses the network.

In Internet connecting service, a Network Access Server (NAS) such as that for dial-up and broadband access server is a RADIUS client. In a wireless LAN system, a wireless LAN access point is a RADIUS client.

Saturation

The degree to which a color is pure.

Secondary DNS Server

Subsidiary DNS server used when a primary DNS server cannot be used.

Shared secret

A character string to be used for mutual authentication between a RADIUS server and RADIUS client.

Sharpness

The degree to which the boundary of two portions is clearly distinguished.

SMTP server

A server for sending or relaying e-mail messages between servers.

SNMP

A protocol for monitoring and managing network devices.

SSL

Acronym for Secure Sockets Layer. This is a protocol developed by Netscape Communications Corporation to be used for communications of encrypted data on the Internet.

Subnet mask

32-bit stream used to distinguish the subnet address from an IP address.

TCP

Acronym for Transmission Control Protocol. A standard protocol used for Internet connection. Compared with the other protocol, UDP, TCP provides reliable communication but communication speed is slower.

TKIP

Acronym for Temporal Key Integrity Protocol. This is used in WPA encryption for a wireless LAN. TKIP provides high security since it changes encryption keys based on PSK during on-going communication.

UDP

Acronym for User Datagram Protocol. A standard protocol used for Internet connection. Compared with the other protocol, TCP, UDP can transmit data faster, but reliable communication is not guaranteed.

Unicast

Transmission of data to specified equipment on a network by specifying a single address.

WPA

Acronym for Wi-Fi Protected Access. This is an encryption standard for a wireless LAN. It provides higher security than the conventional WEP (Wired Equivalent Privacy) standard. In WPA, TKIP is used for the encryption method, and PSK and EAP are used for the authentication protocol.

WPA2

Abbreviation for Wi-Fi Protected Access 2. WPA2 is a standard with which AES (Advanced Encryption Standard) is added to WPA.

802.1X

A standard that performs user authentication and dynamic key generation and traffic on a LAN.

Index

Numerics

802.1X.....41, 42, 51, 104

A

Access log 31
Active Directory..... 54
ActiveX control.....8, 11, 13
ActiveX viewer 17, 18
Adaptive rate control..... 37
Adjust..... 28
Administrator 16, 57
Administrator e-mail
 address45, 59, 65
Administrator menu 26
AES 102
Alarm 60, 62, 66, 70
Alarm buffer.....27, 62, 66, 72
Alarm buffer Menu 72
alarm detection..... 60, 62
Alarm duration..... 69
Alarm output21, 27, 68, 71
Alarm output Menu..... 68
Alarm recording 66
Alarm sending..... 60, 62
Antenna 41
ARP commands 100
Audio 57
audio..... 31, 32
Audio codec 31
Audio output 69
Audio port number..... 37, 38
Audio upload..... 32
Authentication.....42, 44, 59, 65
Authentication server 51
Authenticator 51
Automatically adjust clock for
 daylight saving time changes..... 28

B

Backup setting data..... 30
Bandwidth control..... 37
Bit rate..... 37

C

CA (Certificate Authority) 51, 102
CA certificate 53, 55
CA certificate tab 48
Camera 27, 31
Camera list 20, 79
Camera Menu..... 31
Cancel button 26
Capacity warning 64
Capture 18
certificate request 52
CF memory card30, 64, 68
CGI commands 101
Client certificate..... 52
client certificate..... 52
Codec 72
Color 31
Common.....31, 58, 61, 64
Common name 102
Cropping 36
Current date & time 28
Custom Homepage Installer..... 88

D

Date & time..... 28
date and time 28
Date and time format 28
Date_No. 67
Day/Night..... 21, 71
Day/night mode..... 35
daylight saving time 28
Default gateway 39, 40
Default policy..... 58
delete 30
Delete custom homepage 30
Delete voice alert file 30
device setting..... 91
DHCP server 38, 40
Digital certificate..... 103
DNS server..... 39, 40
Domain suffix..... 39, 40
Downloading images..... 68
Dynamic IP address notification 44

E

EAP 42
EAP method 52, 103
EAP-TLS authentication 103
Effective period
 60, 61, 62, 63, 66, 67, 69, 70
e-mail 44, 58
e-Mail (SMTP)..... 27, 58, 70
e-Mail (SMTP) Menu..... 58
e-Mail (SMTP) notification..... 44
e-mail address 45
End time 72
extension 67

F

Factory default 30
factory settings 30
File 69, 71
File attachment..... 60
file name.....60, 62, 63, 66
Firmware Upgrade 88
folder structure 67
format 30
Format CF memory card 30
format of date and time 28
Frame rate 18, 37
FTP..... 57
FTP client..... 27, 71
FTP client function..... 61
FTP client Menu..... 61
FTP server..... 27, 61
FTP server function..... 68
FTP server Menu..... 68
FTP server name 61

G

Glossary 102

H

H.264..... 103
Home 18
Homepage 79
Host name 39, 40
HTML output tab 81
HTTP method..... 45
HTTP notification 45
HTTP port number 39
HTTP request 45
HTTP server 45

I

image file	21
Image file name	60, 62, 63, 66
Image memory	21, 27, 64, 71
Image memory Menu	64
Image quality	37
Image size	36
information bar	9
Information Bar message	8
Initialize	30
Installation Tab	29
Internet Authentication Service	54
Internet Explorer	13
Interval	61, 63, 67
IP address	6, 38, 40
IP Setup Program	6, 82
IPv4 setting	38
IPv6 setting	39

J

JPEG	17
------------	----

L

Layout	79
Logging in	17

M

MAC address	38, 40
Main viewer	18
Masking	87
memory	64, 68
Message	45, 59
Method	45
Mic volume	31
Microphone	31
Mode	68
Monitor image	19
Motion detection	27, 69
multicast	37
Multicast address	38
Multicast streaming	38
My device	84

N

Network	27, 38
Network address/Subnet	58
network bandwidth	37
network connection type	41

Network Menu	38
--------------------	----

O

OK button	26
Overwrite	64

P

Passive mode	62, 103
Passphrase	42
Password	45, 57, 59, 61, 65
PC clock	28
periodical e-mail sending	60
Periodical recording	66
Periodical sending	60, 63
Picture	32
Play	69
playing audio	21
Plug-in free viewer	19
POP server	44, 59, 65
POP server name	44, 59, 65
port number	45
Portable module	80
Post-alarm period	72
Pre-alarm period	72
Primary DNS server	39, 40
Privacy Masking tab	34
Private key password	53
Proxy port number	45
proxy server	45
Proxy server name	45
PSK	42, 104

Q

QoS Tab	42
---------------	----

R

RADIUS client	104
Reboot	30
Recipient e-mail address	45, 59
Recording capacity	72
recording capacity of the alarm buffer	72
recording images	21, 64
Recording time	72
Remote path	62, 63
Repeat	70
Restore setting	30
Re-type password	57, 61

S

saves the setting data	30
Schedule	27, 72
Schedule Menu	72
Schedule Task	89
Secondary DNS server	39, 40
Security	27, 41, 58
Security function	58
Security Menu	58
Security Warning	8, 9, 11, 74
Selected root directory	64, 68
sending images	21
Sensor input 1	68
Sequence number clear	60, 61, 62, 63, 66, 67
Serial number	28
Setting	18
Shared secret	104
SMTP server	44, 58, 65
SMTP server name	44, 58, 65
SNC audio upload tool	93
SNC Desktop viewer	24
SNC privacy masking tool	87
SNC toolbox	82
SNC video player	99
SNC viewer	23
SNMP	101
Software version	28
special tags	45
SSID	41
SSL Menu	46
SSL	104
Start time	72
Streaming	37
Subject	45, 59
Subnet mask	38, 40
Suffix	60, 62, 63, 66, 67
Superimpose	29
Supplicant	51
System	27, 28
System log	31
System Menu	28
System Utility	23

T

TCP	22
TCP/UDP	22
Test	69
Text	80
time difference	28
Time zone	28
Timer	71
title bar	28
Title bar name	28
TKIP	104
Toggle	71
Tool	18
transmission port number	37
Trigger	27
Trigger Menu	70
Type	41

U

UDP	37
UDP (Multicast)	22
UDP (Unicast)	22
Unicast streaming	37
URL	45
Use the same time schedule every day	72
User	16, 55, 57
User Menu	57
User name	45, 57, 59, 61, 65

V

Video codec	36
Video port number	37, 38
View size	18
Viewer authentication	57
Viewer Menu	79
Viewer mode	16, 57
Voice alert	27, 70, 71
Voice alert Menu	69
voice alert number select	97
volume	19, 31

W

welcome page	13
WEP	41
WEP key	41
Windows Firewall	9
Windows Vista	10
Windows XP Service Pack 2	8
Wireless	39
wireless cards	39
WPA	42, 104
WPA2	42, 104

