New functions and addendum

- This document contains descriptions of how to set the new functions and their restrictions. It is recommended to read them while referring to the Operating Instructions provided with this product together.
- Depending on the model used, the screens shown in the explanations may differ to the actual camera screens.
- The model number is abbreviated in some descriptions in this manual.

About notations

The following notations are used when describing the functions limited for specified models. The functions without the notations are supported by all models.

- **S11x2**: WV-S1132, WV-S1112
- **S11x1**: WV-S1131, WV-S1111
- **S15x1**: WV-S1531LTN, WV-S1531LN, WV-S1531LNS, WV-S1511LN
- **S25x1**: WV-S2531LTN, WV-S2531LN, WV-S2511LN
- **S22x1**: WV-S2231L, WV-S2211L
- **S21x1**: WV-S2131L, WV-S2131, WV-S2111L
- **S21x0**: WV-S2130, WV-S2110
- **S11x2**: WV-S1132, WV-S1112
- **S111x**: WV-S1112, WV-S1111
- **S15x**: WV-S1531LTN, WV-S1531LN, WV-S1531LNS
- **S151x**: WV-S1511LN
- **S25x**: WV-S2531LTN, WV-S2531LN
- **S251x**: WV-S2511LN
- **S22x**: WV-S2231L
- **S221x**: WV-S2211L
- **S21x**: WV-S2131L, WV-S2131, WV-S2130
- **S211x**: WV-S2111L, WV-S2110
- **X531**: WV-X6531N, WV-X6531NS
- **X511**: WV-X6511N
- **S530**: WV-S6530N
- **S6131**: WV-S6131
- **S6111**: WV-S6111
- **S6130**: WV-S6130
Due to software upgrade, the following functions have been added and changed to this product.

**Firmware Ver.1.20**

<table>
<thead>
<tr>
<th>No.</th>
<th>Functions</th>
<th>Item (Page)</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Addition of “IEEE 802.1X” function.</td>
<td>User mng.</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>Addition of “SNMPv3” function.</td>
<td>Advanced (Network)</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>Addition of “1280x720” setting to Stream(3).</td>
<td>Image (Image/Audio)</td>
<td>6</td>
</tr>
</tbody>
</table>

**Firmware Ver.1.40**

<table>
<thead>
<tr>
<th>No.</th>
<th>Functions</th>
<th>Item (Page)</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>“Data encryption” added to “User mng.” menu</td>
<td>User mng.</td>
<td>8</td>
</tr>
<tr>
<td>5</td>
<td>[-FREE ENTRY--] added to [Max bit rate (per client)∗]</td>
<td>Image (Image/Audio)</td>
<td>10</td>
</tr>
<tr>
<td>6</td>
<td>&quot;On (Advanced)&quot; added to [Smart coding]</td>
<td>Image (Image/Audio)</td>
<td>11</td>
</tr>
<tr>
<td>7</td>
<td>Support for 256 GB SDXC memory cards</td>
<td>SD memory card (Basic)</td>
<td>12</td>
</tr>
</tbody>
</table>

**Firmware Ver.1.70**

<table>
<thead>
<tr>
<th>No.</th>
<th>Functions</th>
<th>Item (Page)</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Add “Support” menu</td>
<td>-</td>
<td>13</td>
</tr>
</tbody>
</table>

**Firmware Ver.1.80**

<table>
<thead>
<tr>
<th>No.</th>
<th>Functions</th>
<th>Item (Page)</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>“SD memory card password lock” added to “SD memory card security settings”</td>
<td>SD memory card (Basic)</td>
<td>14</td>
</tr>
</tbody>
</table>

**Firmware Ver.1.90**

<table>
<thead>
<tr>
<th>No.</th>
<th>Functions</th>
<th>Item (Page)</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Change in restrictions on characters for password</td>
<td>For administrator registration</td>
<td>17</td>
</tr>
<tr>
<td>11</td>
<td>Description for video distribution method is added</td>
<td>Monitor images from multiple cameras</td>
<td>18</td>
</tr>
<tr>
<td>12</td>
<td>[Drawing method], [Decoding Options], [Frame Skip Options (When PC is Heavy Processing Load)] are added to Viewer software</td>
<td>Basic (Basic)</td>
<td>19</td>
</tr>
<tr>
<td>13</td>
<td>Change of authentication method default setting</td>
<td>User auth. (User mng.)</td>
<td>21</td>
</tr>
<tr>
<td>14</td>
<td>User authentication function for host authentication is added</td>
<td>Host auth. (User mng.)</td>
<td>22</td>
</tr>
<tr>
<td>15</td>
<td>“EAP-TLS” is added to the EAP method for IEEE 802.1X</td>
<td>IEEE 802.1X (User mng.)</td>
<td>23</td>
</tr>
<tr>
<td>16</td>
<td>Change of default setting of “Bandwidth control(bit rate)”</td>
<td>Network (Network)</td>
<td>27</td>
</tr>
<tr>
<td>17</td>
<td>“Reboot” added to “Schedule”</td>
<td>Schedule</td>
<td>28</td>
</tr>
<tr>
<td>18</td>
<td>Add [&lt;&lt; Latest 100], [Number of pages display] in [Systemlog]</td>
<td>System log (Maintenance)</td>
<td>29</td>
</tr>
<tr>
<td>19</td>
<td>Encryption of the settings</td>
<td>Data (Maintenance)</td>
<td>30</td>
</tr>
<tr>
<td>20</td>
<td>“Login failure” indication added to the login-related display</td>
<td>About the displayed system log</td>
<td>31</td>
</tr>
</tbody>
</table>
1. Addition of “IEEE 802.1X” function.

[IEEE 802.1X] tab of the “User mng.” page has been added.

This function can be used when building a secure network using authentication LAN switches. Refer to the network administrator for information on authentication LAN switches.

Click [IEEE802.1X] tab on the “User mng.” page.

[IEEE 802.1X]
Select On/Off to determine whether or not to perform port authentication using IEEE 802.1X.
• Default: Off

[User name]
Enter the user name to access the authentication LAN switch.
• Available number of characters: 1-32 characters
• Unavailable characters: Alphanumeric characters " & : ; ¥

[Password] [Retype password]
Enter the password to access the authentication LAN switch.
• Available number of characters: 4-32 characters
• Unavailable characters: Alphanumeric characters " &

[EAP method]
Select the authentication method as EAP-MD5 or EAP-PEAP.
2. Addition of “SNMPv3” function.

(Operating Instructions Configuring the network settings [Network] - Configure advanced network settings [Advanced] - Configure the settings relating to SNMP)

<table>
<thead>
<tr>
<th>[SNMP version]</th>
<th>Select the SNMP version to be used.</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>SNMPv1/v2</strong>: SNMPv1/v2 is activated.</td>
<td></td>
</tr>
<tr>
<td>• <strong>SNMPv3</strong>: SNMPv3 is activated.</td>
<td></td>
</tr>
<tr>
<td>• <strong>SNMPv1/v2/v3</strong>: SNMPv1/v2/v3 is activated.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Default</strong>: SNMPv1/v2</td>
<td></td>
</tr>
</tbody>
</table>

**[SNMPv1/v2] - [Community]**
Enter the community name to be monitored.
- **Available number of characters**: 0 - 32 characters
- **Default**: None (blank)

**IMPORTANT**
- When using the SNMP function, it is necessary to enter the community name. When no community name is entered, the SNMP function will not work.

**[SNMPv3] - [User name]**
Set the SNMPv3 user name.
- **Available number of characters**: Empty field or 1-32 characters
- **Unavailable characters**: “& ; ¥

**[SNMPv3] - [Authentication]**
Select the SNMPv3 authentication method from MD5/SHA1.
- **Default**: MD5
[SNMPv3] - [Encryption method]
Select the SNMPv3 encryption method from DES/AES.
• Default: DES

[SNMPv3] - [Password (8 to 32 characters)]
Set the SNMPv3 password.
• Available number of characters:
  – If the authentication method is MD5: Empty field or 8-16 characters
  – If the authentication method is SHA1: Empty field or 8-20 characters
• Unavailable characters: " &

[System name]
Enter a system name to be used to manage the camera with the SNMP function.
• Available number of characters: 0 - 32 characters
• Default: None (blank)

[Location]
Enter the name of the location where the camera is installed.
• Available number of characters: 0 - 32 characters
• Default: None (blank)

[Contact]
Enter the E-mail address or the phone number of the SNMP manager.
• Available number of characters: 0 - 255 characters
• Default: None (blank)
3. Addition of “1280x720” setting to Stream(3)

(Operating Instructions Configure the settings relating to images and audio [Image/Audio]
- Configure the settings relating to Stream [Image])

<table>
<thead>
<tr>
<th>Image capture mode</th>
<th>Stream(1)</th>
<th>Stream(2)</th>
<th>Stream(3)</th>
<th>Stream(4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 mega pixel [16:9]</td>
<td>1920 x 1080</td>
<td>1920 x 1080</td>
<td><strong>1280 x 720</strong></td>
<td>640 x 360</td>
</tr>
<tr>
<td>(30fps mode)</td>
<td>1280 x 720</td>
<td>1280 x 720</td>
<td>640 x 360</td>
<td>320 x 180</td>
</tr>
<tr>
<td></td>
<td>640 x 360</td>
<td>640 x 360</td>
<td>320 x 180</td>
<td></td>
</tr>
<tr>
<td></td>
<td>320 x 180</td>
<td>320 x 180</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 mega pixel [16:9]</td>
<td>1920 x 1080</td>
<td>1920 x 1080</td>
<td><strong>1280 x 720</strong></td>
<td>640 x 360</td>
</tr>
<tr>
<td>(60fps mode)</td>
<td>1280 x 720</td>
<td>1280 x 720</td>
<td>640 x 360</td>
<td>320 x 180</td>
</tr>
<tr>
<td></td>
<td>640 x 360</td>
<td>640 x 360</td>
<td>320 x 180</td>
<td></td>
</tr>
<tr>
<td></td>
<td>320 x 180</td>
<td>320 x 180</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 mega pixel [4:3]</td>
<td>2048 x 1536</td>
<td>1280 x 960</td>
<td>VGA 400 x 300</td>
<td>VGA 400 x 300</td>
</tr>
<tr>
<td>(30fps mode)</td>
<td>1280 x 960</td>
<td>800 x 600</td>
<td>VGA 400 x 300</td>
<td>QVGA</td>
</tr>
<tr>
<td></td>
<td>800 x 600</td>
<td>VGA 400 x 300</td>
<td>QVGA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>400 x 300</td>
<td>400 x 300</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>QVGA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Image capture mode</td>
<td>Stream(1)</td>
<td>Stream(2)</td>
<td>Stream(3)</td>
<td>Stream(4)</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------</td>
<td>--------------------</td>
<td>--------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>1.3 mega pixel [16:9] (30fps mode)</td>
<td>1280 x 720 640 x 360 320 x 180</td>
<td>1280 x 720 640 x 360 320 x 180</td>
<td><strong>1280 x 720</strong> 640 x 360 320 x 180</td>
<td>640 x 360 320 x 180</td>
</tr>
<tr>
<td>1.3 mega pixel [16:9] (60fps mode)</td>
<td>1280 x 720 640 x 360 320 x 180</td>
<td>1280 x 720 640 x 360 320 x 180</td>
<td><strong>1280 x 720</strong> 640 x 360 320 x 180</td>
<td>640 x 360 320 x 180</td>
</tr>
<tr>
<td>1.3 mega pixel [4:3] (30fps mode)</td>
<td>1280 x 960 800 x 600 VGA 400 x 300 QVGA</td>
<td>1280 x 960 800 x 600 VGA 400 x 300 QVGA</td>
<td>VGA 400 x 300 QVGA</td>
<td>VGA 400 x 300 QVGA</td>
</tr>
</tbody>
</table>
4. “Data encryption” added to “User mng.” menu

[Data encryption] was added to the “User mng.” page. Click the [Data encryption] tab in the “User mng.” page.

Click the “+” mark on the left of the setup menu to expand the respective item, and enable detailed settings.
Click the “-” mark on the left of an expanded item to return to the screen displayed before the item was expanded.

[Data encryption (Batch change)]
Select “On” or “Off” to determine whether or not to activate data encryption.
**On:** Activates data encryption. Encrypts Stream(1), Stream(2), JPEG(1), JPEG(2), JPEG(3), and “AAC-LC” audio.
**Off:** Deactivates data encryption.
**Default:** Off

[Stream(1)], [Stream(2)], [JPEG(1)], [JPEG(2)], [JPEG(3)]
Select “On” or “Off” independently for Stream(1), Stream(2), JPEG(1), JPEG(2), and JPEG(3) to determine whether or not to activate data encryption.
**Default:** Off

[Encryption password], [Retype encryption password]
Set the password for data encryption.
**Available number of characters:** 4 - 16 characters
**Unavailable characters:** " &

**IMPORTANT**
• The initial password is displayed in "MAC address" on the [Upgrade] screen. When using data encryption, make sure to change the password.
• If you set data encryption to “On”, “Stream(3)” and “Stream(4)” become “Off”.
• When the image capture mode is “3 mega pixel [4:3](30fps mode)” and data encryption is “On”, 2048x1536 JPEG or stream cannot be selected.
• If you set data encryption to “On”, the upper limit of the possible bit rate for stream transmissions will be limited to maximum 16 Mbps.
• If you set data encryption to “On”, the snap shot button on the “Live” page will be hidden.
• If you set data encryption to “On” for JPEG, images cannot be monitored using a cellular phone/mobile terminal. Additionally, the [Refresh interval] pull-down on the “Live” page is not displayed for JPEG with data encryption set to “On”.

8
• Data encrypted JPEG cannot be viewed on the browser’s “Playback” page. Download it to a PC and use the decryption tool to confirm it. Refer to our website (https://security.panasonic.com/support/info/) for further information about the decryption tool.
• If you set data encryption to “On”, audio on the [Audio detection] screen will become inaudible.

**Note**
• In order to view streams with data encryption set to “On”, you must install the viewer software.
• If you confirm streams with data encryption set to “On” on the “Live” page, password entry for decryption is displayed. If you correctly enter the “Encryption password” that was set, you will be able to view images. When “Mic input”, “Interactive(Full-duplex)”, or “Interactive(Half-duplex)” is selected for [Audio transmission mode], only audio may be played until the password is entered.

• Streams that have data encryption enabled for them are wrapped in <> in the [Live view] pull-down menu. Additionally, streams that have data encryption enabled for them are indicated by <Encrypted> in the setup menu pull-down menu.
  Example: When Stream(1) and JPEG(3) are data encrypted
• [Live view] pull-down menu on the “Live” page

• Pull-down menu in the setup menu

• When [Data encryption (Batch change)] is “On”, “AAC-LC” audio is data encrypted (“G.726” and “G.711” are not data encrypted). To encrypt both the image and audio, set [Data encryption (Batch change)] to “On” and set [Audio input encoding format] to “AAC-LC”.
• For encrypted MP4 files and JPEG images, you can use the decryption tool to confirm the images.
5. [--FREE ENTRY--] added to [Max bit rate (per client)\(^*\)]
(Operating Instructions Configure the settings relating to images and audio [Image/Audio] Configure the settings relating to Stream [Image])

When setting “Max bit rate (per client)\(^*\)” of Stream(1) – (4), in addition to selecting an item from the pull-down menu, you can now set the item freely.

![Configuration settings](image)

[Max bit rate (per client)\(^*\)]

<table>
<thead>
<tr>
<th>Bit Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>64kbps/ 128kbps</td>
</tr>
<tr>
<td>256kbps</td>
</tr>
<tr>
<td>512kbps / 768kbps</td>
</tr>
<tr>
<td>1024kbps / 1536kbps/ 2048kbps</td>
</tr>
<tr>
<td>3072kbps/ 4096kbps</td>
</tr>
<tr>
<td>6144kbps/ 8192kbps</td>
</tr>
<tr>
<td>10240kbps/ 14336kbps</td>
</tr>
<tr>
<td>16384kbps/ 20480kbps</td>
</tr>
<tr>
<td>24576kbps/ --FREE ENTRY--</td>
</tr>
</tbody>
</table>

When “--FREE ENTRY--” is selected, you can freely enter the bit rate.

**Note**
The range that can be configured differs depending on the “Transmission priority” and “Image capture size”.

When “Constant bit rate”, “Frame rate”, or “Best effort” is selected for “Transmission priority”

- QVGA, 400x300, VGA, 320x180, and 640x360 : 64kbps - 4096kbps
- 800x600 : 64kbps - 4096kbps
- 1280x960 and 1280x720\(^*1\) : 128kbps - 8192kbps
- 1920x1080\(^*1\) : 256kbps - 12288kbps
- 2048x1536 : 512kbps - 16384kbps

When “VBR” is selected for “Transmission priority”

- QVGA, 400x300, VGA, 320x180, and 640x360 : 64kbps - 12288kbps
- 800x600 : 64kbps - 12288kbps
- 1280x960 and 1280x720\(^*1\) : 128kbps - 12288kbps
- 1920x1080\(^*1\) : 256kbps - 24576kbps
- 2048x1536 : 512kbps - 24576kbps

\(^*1\) When 60fps mode is selected, settings up until 24576kbps can be configured.
6. “On(Advanced)” added to [Smart coding]
(Operating Instructions Configure the settings relating to images and audio
[Image/Audio] Configure the settings relating to Stream [Image])

Previously “Smart Coding” was only available for Stream(1) – (4) when the [Transmission priority] was “VBR”; now “Smart Coding” “GOP control” can be set to “On(Advanced)” even when “VBR” is not selected.

[Smart Coding] - [GOP control]
By using “GOP control”, the transmission data volume can be reduced when there is little motion in the image.
When “H.265” is selected as the “Stream encoding format”: Off/On(Low)/On(Mid)/On(Advanced)
When “H.264” is selected as the “Stream encoding format”: Off/On(Low)/On(Mid)
Default: Off

**IMPORTANT**
- If “On(Low)”, “On(Mid)”, or “On(Advanced)” is selected, data cannot be recorded to the SD memory card.

**Note**
- “On(Low)”/“On(Mid)” are only available when [Transmission priority] is “VBR”.
- “On(Advanced)” is available regardless of [Transmission priority].
7. Support for 256 GB SDXC memory cards

(Functional Instructions Configure the basic settings of the camera [Basic]
Configure the settings relating to the SD memory card [SD memory card])

The upper limit for supported SD memory cards is 256 GB.

Compatible SD memory card (option)
Manufactured by Panasonic (SD speed class 4 or higher)
miniSD and microSD cards cannot be used.
SDXC memory card: 64 GB, 128 GB, 256 GB
SDHC memory card: 4 GB, 8 GB, 16 GB, 32 GB
SD memory card: 2 GB
8. Add “Support” menu

Methods for accessing the Panasonic support website are explained on the “Support” page.

To access the Panasonic support website from a web browser, click the link for the support page. To access from a cellular phone/mobile terminal, scan the “Data Matrix” or “QR Code” with your cellular phone/mobile terminal to display the Panasonic support website. If you cannot display the website, access the Panasonic website (https://security.panasonic.com/support/qr_sp_select/).
9. “SD memory card password lock” added to “SD memory card security settings”

(Operating Instructions Configure the basic settings of the camera [Basic]
Configure the settings relating to the SD memory card [SD memory card])

[SD memory card password lock] function added to SD memory card security setting.

[SD memory card password lock]
Configure a password for the SD memory card. When configuring a password, devices other than the camera will be unable to write to or read the SD memory card. If the SD memory card is stolen or lost, the risk of recorded data being leaked can be reduced.

[Set]
When an SD memory card with no configured password is inserted, a password can be configured using the [Set] button.

[Password]/[Retype password]
Enter the password.
Available number of characters: 4 - 16 characters
Unavailable characters: " &
Default: None (blank)
[Remove]
When an SD memory card with a configured password is inserted, the password can be removed using the [Remove] button.

[Password]
Enter the password.
Available number of characters: 4 - 16 characters
Unavailable characters: " &

[Change]
When an SD memory card with a configured password is inserted, the password can be changed using the [Change] button.

[Old password]/[New password]/[Retype new password]
Enter the password.
Available number of characters: 4 - 16 characters
Unavailable characters: " &

[Status]
Display the configuration status of the password lock.
• Lock: A password is configured on the SD memory card, and the lock function is enabled.
• Unlock: The lock function is disabled.
Also display the password configuration status of SD memory card respectively.
Password is set.: The password is configured correctly.
• Error(Unsupported SD memory card): A card that does not support password lock is inserted. Check that an SDHC memory card or SDXC memory card is inserted.
• Error(Password mismatch): The SD memory card cannot be used because the password configured for the SD memory card and the password configured for the camera do not match. Check that the passwords are correct.

Note
• The password lock function supports only SDHC memory cards and SDXC memory cards.
• If you will use the SD memory card on a device other than the camera with password lock configured, remove the password using the password lock remove button before removing the SD memory card.
The password cannot be removed on devices (such as PCs) other than the camera.
• When the “Status” of “SD memory card password lock” is “Lock”, if an SD memory card with no configured password is inserted, the password is automatically configured to the SD memory card.
IMPORTANT

- If you forget the configured password, the password cannot be removed. The SD memory card with the configured password will become unusable, so manage passwords with great care.
- If you forget the configured password and you want to replace the SD memory card with a new one, perform the following step to set the “Status” of “SD memory card password lock” to “Unlock” before replacing the SD memory card.
  - Initialize settings from the “Maintenance” page.
10. Change in restrictions on characters for password
(Operating Instructions For administrator registration)

[Password (8 to 32 characters)]/[Retype password]
Enter the administrator password.
Available number of characters: 8 - 32 characters
Unavailable characters: 2-byte characters, and 1-byte symbols " &

**Note**
- Distinguish between upper- and lower cases.
- Use three or more types of characters from upper- and lowercase alphabetic characters, numbers, and symbols.
- Set the password which does not include the user name.
11. Description for video distribution method is added
(Operating Instructions  Monitor images from multiple cameras)

③ [Refresh interval] pull-down menu
Select from the pull-down menu and switch between video (H.265/H.264/MJPEG) and still images (JPEG).
For still images (JPEG), select the refresh interval (Refresh interval : 1s/Refresh interval : 3s/Refresh interval : 5s/Refresh interval : 10s/Refresh interval : 30s/Refresh interval : 60s) for camera images. When the 16 screen layout is used, Refresh interval : 1s cannot be selected.

Note
• When “On” is selected for Stream(1), “H.265” or “H.264” can be selected.
• When “H.265” is selected, H.264 or MJPEG video may be displayed depending on the settings of the connected camera.
• When “H.264” is selected, H.265 or MJPEG video may be displayed depending on the settings of the connected camera.
12. [Drawing method], [Decoding Options], [Frame Skip Options (When PC is Heavy Processing Load)] are added to Viewer software

(Viewer software (nwcv4Ssetup.exe)) - [Drawing method]
Perform image display settings when displaying camera images with the viewer software.
- **GDI**: The drawing method generally used in Windows.
- **Direct2D**: Can reduce choppy drawing of images.
- **Default**: GDI

**IMPORTANT**
- Use “Direct2D” with a computer that has the latest graphic driver version installed to it.
- When using “Direct2D”, set “Smother live video display on the browser (buffering)” to “On”.
  - If “Off” is selected for “H.264 Smoother live video display on the browser (buffering)”, “Direct2D” may not be very effective.

**Note**
- If your computer’s operating system is Windows 7 and the Aero function is disabled, “Direct2D” may not be very effective.
- When “Direct2D” is selected for “Drawing method”, video may not be displayed or the displayed image may be seen as it is partially corrupted depending on the PC in use.
- Refer to the Panasonic support website for information of PCs for which “Direct2D” is selectable.
  Panasonic website (https://security.panasonic.com/support/info/ <Control No.: C0313>)

(Viewer software (nwcv4Ssetup.exe)) - [Decoding Options]
Select the decoding method for H.265/H.264 images on the “Live” page.
- **Software**: Decoding is performed by software.
- **Hardware**: Uses the Hardware Acceleration (QSV/DXVA) function that performs fast decoding.
- **Default**: Software

**IMPORTANT**
- “Hardware” may not be able to be used depending on the computer used.
  - One of the following messages is displayed when the [Confirm] button is clicked.
    - The hardware decode is available for both H.265 and H.264 on your PC.
      → Depending on your PC environment, images may not be able to be outputted. In this case, select “Software” for “Decoding Options”.
    - The hardware decode is available for H.264 on your PC, but unavailable for H.265 on your PC.
      → Depending on your PC environment, images may not be able to be outputted. In this case, select “Software” for “Decoding Options”.
    - “The hardware decode is not available on your PC.”
      → Select “Software” for “Decoding Options”.

(Viewer software (nwcv4Ssetup.exe)) - [Frame Skip Options (When PC is Heavy Processing Load)]
Note
• When “Hardware” is selected for “Decoding Options”, video may not be displayed or the displayed image may be seen as it is partially corrupted depending on the PC in use.
• Refer to the Panasonic support website below for information of PCs for which “Hardware” is selectable.
  Panasonic website (https://security.panasonic.com/support/info/ <Control No.: C0313>)

[Viewer software (nwcv4Ssetup.exe)] - [Frame Skip Options (When PC is Heavy Processing Load)]
Perform settings to display camera images on the viewer software.
• Auto: If there is a delay in displaying images from the camera, the delay can be resolved by automatically skipping frames.
• Manual: If there is a delay in displaying images from the camera, frames are not skipped automatically.
• Default: Auto

Note
• When “Manual” is selected, “Off”, “1 Frame Skip”, “2 Frames Skip”, “4 Frames Skip”, “6 Frames Skip”, or “8 Frames Skip” can be selected for frame skip by right-clicking on the “Live” page. The value selected here will revert to “Off” when the browser is closed.
13. Change of authentication method default setting

(Operating Instructions  Configure the settings relating to the authentication [User mng.] - Configure the settings relating to the user authentication [User auth.])

[Authentication]
Set the user authentication method.
• **Digest or Basic**: Uses “Digest or Basic” authentication.
• **Digest**: Uses “Digest” authentication.
• **Basic**: Uses “Basic” authentication.
• **Default**: Digest

**IMPORTANT**

- About the system devices (Panasonic network disk recorder and others)
  - When connection with a system device cannot be established, upgrade the system device.
  - For information on upgrading system devices, refer to the following web site: https://security.panasonic.com/support/info/ <Control No.: C0701>
  - Support may already be ended for some system devices (discontinuation). In such a case, it may be possible to connect by setting “Basic” for the authentication method of the user authentication.
14. User authentication function for host authentication is added
   (Operating Instructions Configure the settings relating to the authentication [User 
   mng.]- Configure the settings relating to the host authentication [Host auth.])
   After the host authentication, execute the user authentication according to the setting of the "User auth." (On/Off) to allow the access subject to the authentication.

   ![User authentication settings](image)

   **Note**
   When "On" is set for "User auth.":
   The user authentication is required when connecting to this camera using an IP address set as the host authentication.

   When "Off" is set for "User auth.":
   The user authentication is not required when connecting to this camera using an IP address set as the host authentication.
   However, if accessing to the outside of the access level, the user authentication is required.

   **IMPORTANT**
   • With the host set by an old version, the user authentication is not required within the access level even if the "User auth." is "On".
   For the host set by an old version, asterisk (*) will be displayed at the beginning of the IP address in the "Host check" field.
15. “EAP-TLS” is added to the EAP method for IEEE 802.1X

(Operating Instructions Configure the settings relating to the authentication [User mng.]- Configure IEEE 802.1X [IEEE 802.1X]

“EAP-TLS” is added to the EAP method for IEEE 802.1X, and the settings (CA Certificate, private key, Client Certificate) are added.

This function can be used to configure a secure network environment using the authentication LAN switch. Contact your network administrator for how to configure the authentication LAN switch and each setting.

Set up in the following procedure since the procedure differs depending on the EAP method.

If “On” is already selected for “IEEE 802.1X”, start setup once selecting “Off” for “IEEE 802.1X”.

**EAP-MD5/EAP-PEAP**
1. Select “On” for “IEEE 802.1X”.
2. Select “EAP-MD5” or “EAP-PEAP” for “EAP method”.
3. Click the [Set] button after entering the user name, the password, and confirming the password.

**EAP-TLS**
1. Click the [Browse] button of “CA Certificate” - “Certificate install”. Then, select a CA Certificate and click the [Execute] button. “installed” will be displayed for “Information”
2. Click the [Browse] button of “Private key or Client Certificate including private key”, and select a private key or Client Certificate that includes Private key.
3. Enter the password if the private key is encrypted or the password is set for Client Certificate for the PFX method. Leave password blank when not encrypted.
4. Click the [Execute] button to start installation. “installed” will be displayed for “Install status of private key”. In the case of selecting Client Certificate including the private key, “installed” will be displayed for “Client Certificate” - “Information” as well.

5. When the private key is installed in step 2, select a Client Certificate after clicking the [Browse] button of “Client Certificate”, and then click the [Execute] button. “installed” will be displayed for “Information”.

6. Select “On” for “IEEE 802.1X”. Then, select “EAP-TLS” for “EAP method”.

7. Enter the user name registered to the server in “User name”. Then, click the [Set] button. If no user name is registered to the server, enter an arbitrary user name. “Password” and “Retype password” can be left blank.

**Note**
- To delete each certificate, set [IEEE 802.1X] to “Off”.

The following explains each setting.

**[IEEE 802.1X]**
Select “On” or “Off” to determine whether or not to perform port authentication using IEEE 802.1X.
- **Default:** Off

**[User name]**
Enter the user name accessing to the authentication LAN switch or the user name registered to the server. If no user name is registered to the server, enter an arbitrary user name.
- **Available number of characters:** 1 - 32 characters
- **Unavailable characters:** " & ; ¥

**[Password]**
**[Retype password]**
Enter the password to access the authentication LAN switch.
- **Available number of characters:** 4 - 32 characters
- **Unavailable characters:** " &

**[CA Certificate] - [Certificate install]**
Install the root CA Certificate. Do not include the intermediate CA Certificate. Installation is possible only when “Off” is selected for “IEEE 802.1X”.

**[Specification of CA Certificate]**

<table>
<thead>
<tr>
<th>Item</th>
<th>Specifications</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data format</td>
<td>Format: PEM or DER</td>
<td>Extension: pem or der</td>
</tr>
<tr>
<td>Max. number of certificates</td>
<td></td>
<td></td>
</tr>
<tr>
<td>included in the PEM format</td>
<td>1 pc.</td>
<td></td>
</tr>
<tr>
<td>Max. size of certificate</td>
<td></td>
<td>Approx. 10 Kbyte</td>
</tr>
</tbody>
</table>

**[CA Certificate] - [Information]**
- **not installed:** indicates that the certificate is not installed.
- **CA certificate host name:** indicates that the certificate is installed.
- **Expired:** indicates that the certificate is expired.

The details of CA Certificate can be checked with the [Confirm] button.

**[Private key or Client Certificate including private key] - [Install]**
Install the private key or Client Certificate that includes private key. Installation is possible only when “Off” is selected for “IEEE 802.1X”.

---
### Specification of private key and Client Certificate including private key

<table>
<thead>
<tr>
<th>Item</th>
<th>Specifications</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data format</td>
<td>Format: PEM or PFX</td>
<td>Extension: pem or pfx</td>
</tr>
<tr>
<td>Key size [bit]</td>
<td>1024 /1536 /2048 /3072 /4096</td>
<td></td>
</tr>
<tr>
<td>Max. number of certificates</td>
<td>6 pc.</td>
<td></td>
</tr>
<tr>
<td>included in the PEM format</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max. size of certificate</td>
<td>Approx. 10 Kbyte</td>
<td></td>
</tr>
<tr>
<td>(including intermediate CA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**[Private key or Client Certificate including private key] - [Password]**

Enter the password if the private key is encrypted or the password is set for Client Certificate for the PFX method. Leave password blank when not encrypted.

**Available number of characters:** 0 - 30 characters

**[Private key or Client Certificate including private key] - [Install status of private key]**

- **not installed:** Private key is not installed.
- **installed:** Private key is installed.

**[Client Certificate] - [Install]**

Install the Client Certificate.

If signed by the intermediate CA Certificate, install the Client Certificate including the intermediate CA Certificate.

Installation is possible only when “Off” is selected for “IEEE 802.1X”.

### Specification of Client Certificate

<table>
<thead>
<tr>
<th>Item</th>
<th>Specifications</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data format</td>
<td>Format: PEM</td>
<td>Extension: pem</td>
</tr>
<tr>
<td>Max. number of certificates</td>
<td>6 pc.</td>
<td></td>
</tr>
<tr>
<td>included in the PEM format</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max. size of certificate</td>
<td>Approx. 10 Kbyte</td>
<td></td>
</tr>
<tr>
<td>(including intermediate CA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**[Client Certificate] - [Information]**

- **not installed:** indicates that the certificate is not installed.
- **Certificate host name:** indicates that the certificate is installed.
- **Expired:** indicates that the certificate is expired.

The details of Client Certificate can be checked with the [Confirm] button.

**[EAP method]**

Select the authentication method from EAP-MD5, EAP-PEAP or EAP-TLS.

**Example of CA Certificate check screen**
Example of Client Certificate check screen

**IMPORTANT**

- After selecting “On” for “IEEE 802.1X”, if access to the camera fails for some reason, connect to a switch or port without authentication. It disables IEEE 802.1X, and enables access to the camera.
- If the Client Certificate includes intermediate CA Certificate, the Client Certificate needs to come first, then the intermediate CA Certificate.
- When a certificate over 10 Kbyte is installed, no error will be displayed during installation. However, an error may occur at the time of connection.
16. Change of default setting of “Bandwidth control(bit rate)”

(Operating Instructions  Configuring the network settings [Network]-
Configure the network settings [Network])

Change of default setting of “Bandwidth control(bit rate)”

[Bandwidth control(bit rate)]
Select the total bit rate for data transmission from the following.
Unlimited/ 64kbps/ 128kbps/ 256kbps/ 384kbps/ 512kbps/ 768kbps/ 1024kbps/ 2048kbps/ 4096kbps/
6144kbps/ 8192kbps/ 10240kbps/ 15360 kbps/ 20480kbps/ 25600kbps/ 30720kbps/ 35840kbps/
40960kbps/ 51200kbps

• Default: 51200kbps
17. “Reboot” added to “Schedule”

(Operating Instructions Configure the settings relating to the schedules [Schedule])

The camera reboot function is added to “Schedule”.

Reboot: The camera reboots at the scheduled time. Can only be selected with Schedule 5.
18. Add [<< Latest 100], [Number of pages display] in [Systemlog]

(Operating Instructions  Maintenance of the camera [Maintenance]-
Check the system log [System log])

The following items will be displayed when using an SD memory card.

[<< Latest 100]
When clicking “<< Latest 100”, the latest 100 system logs will be displayed.

[Number of pages display]
The currently opened page will be displayed in the “page/total page” format.
19. Encryption of the settings
(Operating Instructions Maintenance of the camera [Maintenance] - Settings data/backing up or restoring logs [Data])

Backup
[Setup data]
Click the [Execute] button to backup the setup data of the camera to a PC.

Note
• The settings backed up after this version of software will be encrypted. Therefore, if using the software of older version, the settings cannot be restored.
20. “Login failure” indication added to the login-related display
(Operating Instructions About the displayed system log)

Error indications relating to the login errors

<table>
<thead>
<tr>
<th>Category</th>
<th>Indication</th>
<th>Description</th>
</tr>
</thead>
</table>
| Login failure    | User name  | • The user name that has failed in login will be displayed when “On” is selected for “User auth.”.
|                  |            | • If no user is registered, “Guest User” will be displayed.                  |