

# Panasonic

## User Guide

---

### Wearable Camera LiveConnect



---

# Contents

---

<b>Chapter 1 Overview</b>	<b>3</b>	<b>Chapter 3 Setup for Starting</b>	<b>52</b>
<b>Introduction</b> .....	<b>4</b>	<b>Registering users</b> .....	<b>53</b>
Trademarks.....	4	Logging in to the portal site .....	53
Information on software used with this application .....	4	Registering users.....	54
Right of publicity .....	4	<b>Chapter 4 Device Management</b>	<b>56</b>
Copyright .....	4	<b>Configuring and confirming device settings</b> .....	<b>57</b>
About this manual.....	4	Approving device registration requests .....	57
Terms in this manual.....	4	Checking the status of devices.....	57
About the network settings .....	4	Changing and deleting device settings.....	58
Usage precautions.....	5		
Notice regarding security.....	5		
About LiveConnect .....	6		
System requirements.....	6		
Compatible operating environments.....	6		
<b>Chapter 2 Preparation Before Use</b>	<b>7</b>		
<b>Installing and setting software</b> .....	<b>8</b>		
Installing PostgreSQL.....	8		
Setting the path.....	12		
Importing and checking data .....	14		
Installing Redis .....	18		
Checking the installation result.....	21		
<b>Installing certificates</b> .....	<b>22</b>		
Importing CA certificates.....	22		
Confirming imported CA certificates .....	24		
Importing server certificates.....	25		
Confirming imported server certificates .....	27		
<b>Enabling Windows functions</b> .....	<b>28</b>		
<b>Creating sites</b> .....	<b>31</b>		
Copying site files and setting access privileges .....	31		
Creating the site for the LiveConnect server .....	32		
Creating the site for the M2M relay server.....	38		
<b>Setting the STUN server environment</b> .....	<b>43</b>		
<b>Installing the server control service</b> .....	<b>44</b>		
Installing the server control service .....	44		
Confirming installation of the server control service .....	45		
<b>Activation</b> .....	<b>46</b>		
Logging in to the kitting site .....	46		
Setting the servers.....	47		
License registration and activation .....	49		
Setting and downloading logs.....	50		
Setting logs.....	50		
Downloading logs .....	51		

# Chapter 1 Overview

---

Read this chapter before use.

## Introduction

### Trademarks

- Microsoft and Windows are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries.
- Screen pictures are used in conformity with the Microsoft Corporation guidelines.
- The other names, company names, and product names are trademarks or registered trademarks of their respective companies.

### Information on software used with this application

This application incorporates the following software:

- (1) Software developed independently by Panasonic Corporation
- (2) Open-source software

The software categorized as (2) is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY, without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

See the license conditions listed in the attached file “License.pdf” for more details.

For information on how to obtain the source codes, see the following website.

<https://panasonic.biz/cns/sav/>

Panasonic does not respond to inquiries regarding the content of the source codes obtained by the users.

### Right of publicity

The user is responsible for the protection of the privacy and the right of publicity of the subject when using this application.

### Copyright

Based on the copyright law, the pictures, video recordings, and audio recordings you have made by yourself can be used only for your personal enjoyment without the authorization of the right holder. Note that recording may be restricted even when the purpose is personal enjoyment.

### About this manual

- Panasonic Corporation shall not be liable for any damage caused as a result of the incorrect setting of the network configured to use this application. Panasonic Corporation shall not be liable for any damage caused by the use of this application.
- In this document, pages to be referred are indicated with (→00).
- The content of this manual is subject to change without notice.
- Unauthorized copying in whole or part of this document is prohibited.

### Terms in this manual

- In this manual, the Wearable Camera Liveviewer\*<sup>1</sup> is referred to as “Liveviewer”.
  - In this manual, Wearable Camera LiveCast\*<sup>2</sup> is referred to as “LiveCast” when no more precise term is required.
- \*<sup>1</sup> AG-NAMS7W or AG-NAMS7A (Panasonic Corporation)  
\*<sup>2</sup> AG-SWN7A or AG-SWN7W (Panasonic Corporation)

### About the network settings

- Depending on the signal, the data may be intercepted. It is highly recommended to use encryption at the wireless access point.
- Information may leak in case changes or modifications are made to the application. Do not make changes in or modify the application.
- When disposing of the computer to which this application has been installed or giving it to another person, it is recommended to delete the data saved on the storage media and uninstall the application.
- The network settings may differ depending on the corporate LAN and the service provider settings. Ask the network administrator regarding the network settings.

## Usage precautions

- Do not do the following when this application is running. Otherwise, troubles (data corruption, etc.) may occur.
  - Turning off or restarting the computer
  - Changing the user or logging out
  - Disconnecting from the network
  - Using another piece of software (especially video recording or encoding software that uses lots of CPU resources and a large amount of memory)
- If this application cannot operate due to insufficient system resources, close the other software applications and then restart this application.

## Notice regarding security

When using this application, you may encounter the following troubles.

- Leaking of the user's private information via this application.
- Illegal operation of this application by malicious third parties.
- Interference with or stopping of this application by malicious third parties.

Take the necessary security measures on the computer.

- Limit the number of users that can log in and set up passwords.
- Use passwords that are hard to guess.
- Change the passwords periodically.
- Panasonic Corporation and its affiliate companies will not directly inquire as to a customer's password. Do not give your password in answers to any such direct inquiries.
- To prevent leakage of information when repairing, maintaining, disposing of, or giving the computer, delete the browsing history of the browsers and the passwords that have been saved.

Caution regarding security when using a wireless LAN product

The wireless LAN will communicate information between computers and mobile devices and the wireless access points using radio waves instead of a LAN cable. It also allows easy LAN connection as long as the device is within the range of the radio waves. However, radio waves can reach anywhere in their range regardless of obstacles (walls, etc.), so they may cause the following problems if the settings regarding security are not configured.

- Interception of communication content  
Malicious third parties may intercept the radio waves, and private information such as ID, passwords, credit card numbers, or the content of emails may be intercepted.
- Unauthorized invasion  
Malicious third parties may access a private or corporate network without authorization and steal private or classified information (leakage of information), release fraud information by impersonating a specific person (spoofing), rewrite and distribute the intercepted content (falsification), or destroy data or systems by spreading computer viruses (destruction), etc.

The wireless LAN adapter and the wireless access point have security mechanisms to deal with these problems. Therefore, using these mechanisms on the wireless LAN product before using the application will decrease the possibility that these problems occur.

Security settings may not be set up on the wireless LAN equipment at the time of purchase. To reduce the possibility that security problems occur, make sure to set up all the security settings on the wireless LAN equipment in accordance with the operating instructions of each wireless LAN device before using it. Note that the security mechanisms may be broken by special methods depending on the specifications of the wireless LAN.

It is recommended to fully understand the risks if the security settings are not set up and to set up these security settings under the judgment and responsibility of the user before using the application.

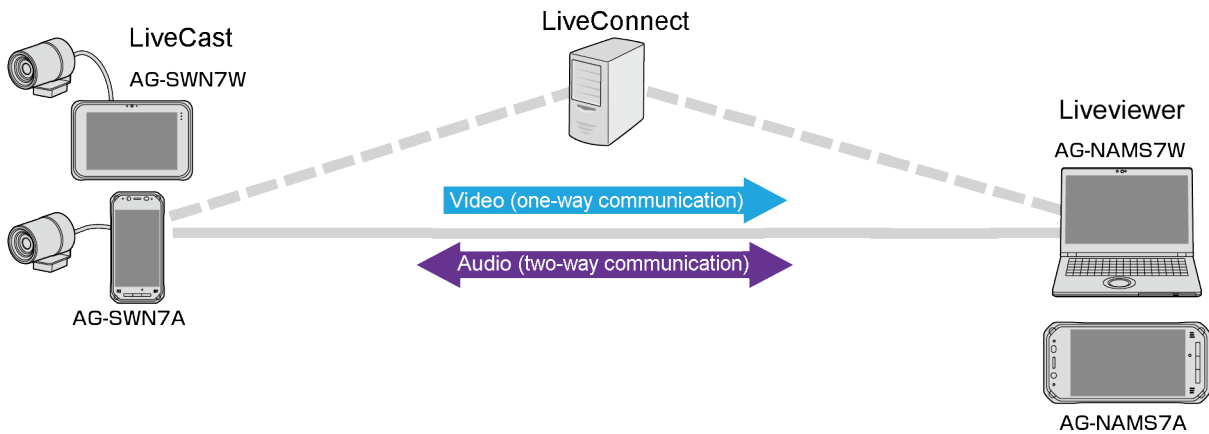
- Panasonic Corporation will offer no compensation for content not recorded in case of problems in the communication environment or failures of the hard disk (HDD).

### Disclaimer

- Information recorded within the application may be modified, be lost or leaked in case of incorrect use, static electricity occurrence, accident, malfunction, repair, if data is saved in a shared folder or on a shared drive, or due to other causes. Panasonic Corporation shall not be liable for any direct or indirect damage caused by the modification or loss of information, including private information.

## About LiveConnect

LiveConnect is an application used to link LiveCast and Liveviewer. This can be used to view LiveCast images in Liveviewer and carry on conversations while viewing images.



## System requirements

- First, confirm that your computer supports wired or wireless LAN connections.
- Operation is not necessarily ensured with all wireless or wired LAN adapters and computers.
- Check the following settings.
  - Device connections may be blocked by security software (specifically, firewalls) or wireless/wired LAN adapter utilities.
  - Confirm that the network is not set up as a bridged network.
  - Confirm that the application is not blocked by a firewall.

## Compatible operating environments

Although operation has been verified in the following environments, operation is not ensured for all devices meeting these requirements.

### Windows PC

OS: Windows 10 Pro

Browser: Google Chrome

Recommended screen resolution: 1440×960 or more

For the latest information about verified versions, refer to the following website.

<https://panasonic.biz/cns/sav/>

## **Chapter 2 Preparation Before Use**

---

This chapter describes preparation before using this application.

## Installing and setting software

Perform the setup procedures before using this application.

**Preparation: Check that a static IP address is assigned to your computer.**

**Download the installer zip file.**

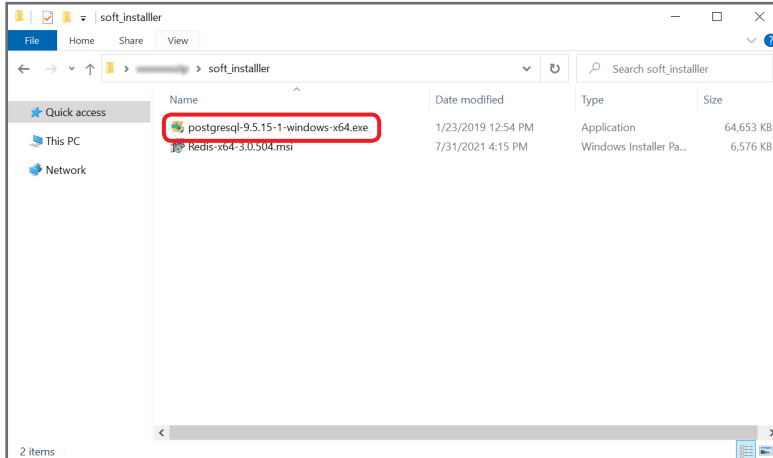
For details on how to download the zip file, refer to the website below.

<https://panasonic.biz/cns/sav/>

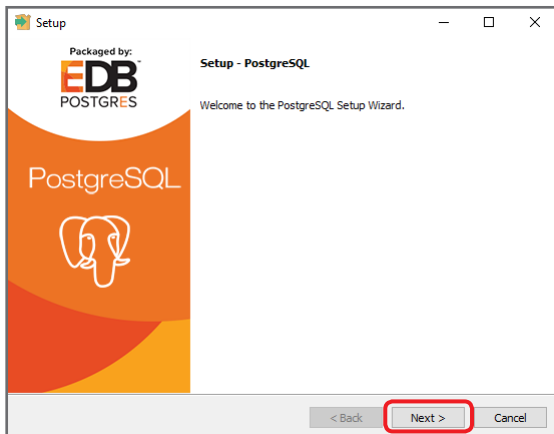
### Installing PostgreSQL

Install PostgreSQL.

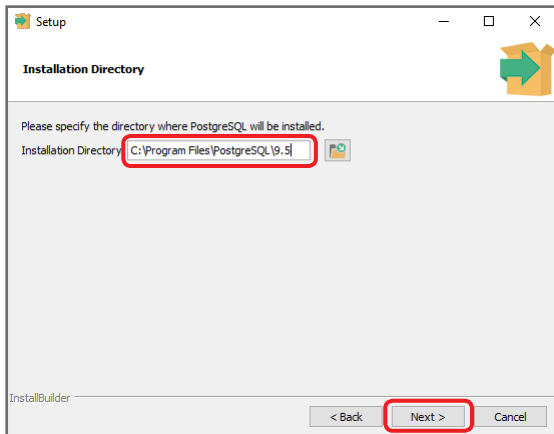
- 1 Open the “soft\_installer” folder among the downloaded files, and double-click “postgresql-9.5.15-1-windows-x64.exe”.



- 2 Click [Next].



- 3 Specify the installation directory, and click [Next].

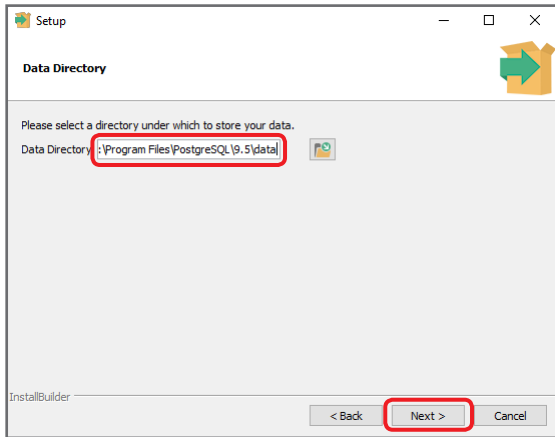


#### Note

- The recommended directory is “C:\Program Files\PostgreSQL\9.5”.



#### 4 Specify the data storage directory for the database, and click [Next].



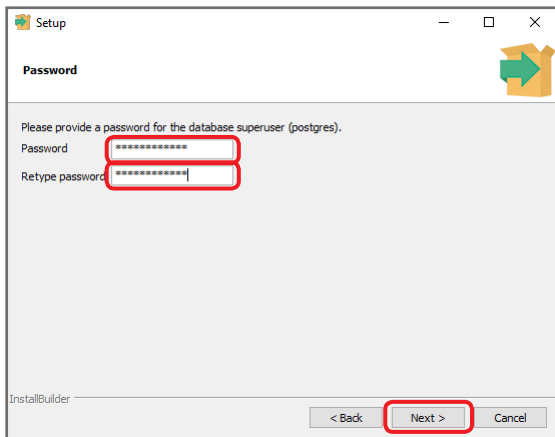
#### Note

- The recommended directory is “C:\Program Files\PostgreSQL\9.5\data”.

#### 5 Specify a password to be used to access the database, and click [Next].

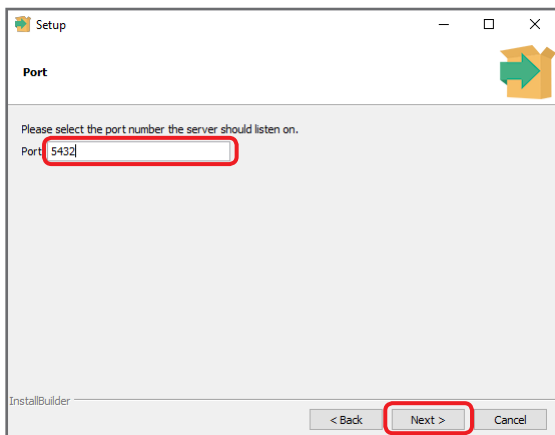
The password is displayed as a series of asterisks (\*).

- Password: Panasonic123



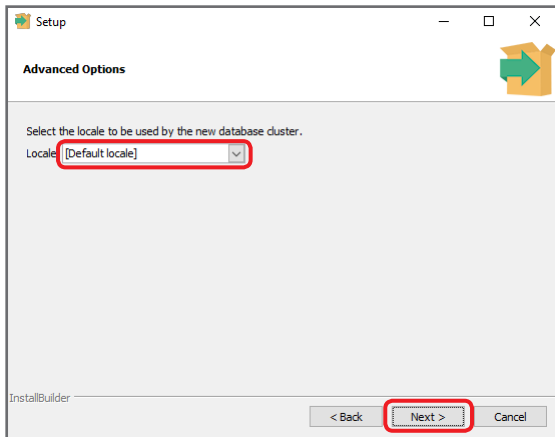
#### 6 Select a port number for the database, and click [Next].

Select the default value of “5432”.

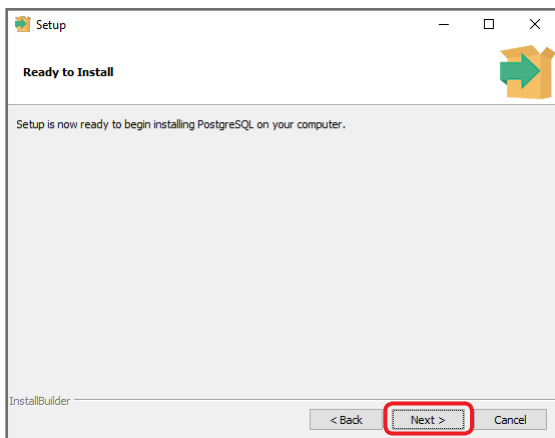


**7 Select the setting for the database cluster from the pull-down menu, and click [Next].**

Select the default value of “Default locale”.

**8 Click [Next].**

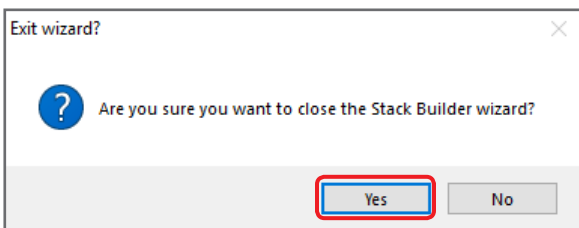
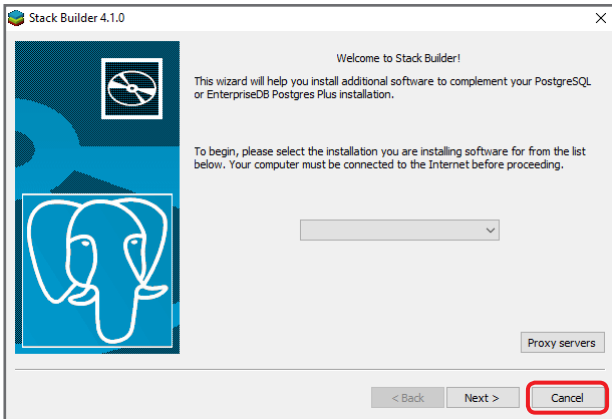
Installation starts.

**9 Click [Finish].**

This completes PostgreSQL installation.

**Note**

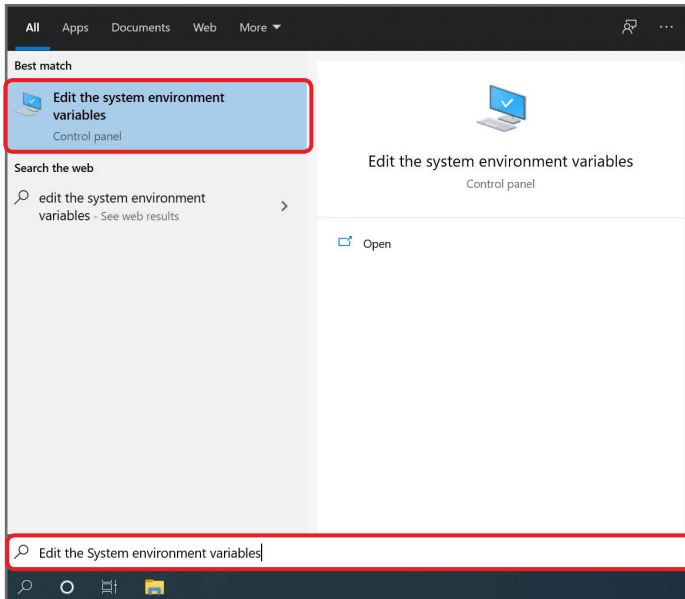
- When PostgreSQL has been installed, the Stack Builder installation window will appear. Since Stack Builder does not need to be installed, click [Cancel] → [Yes], and close the window.



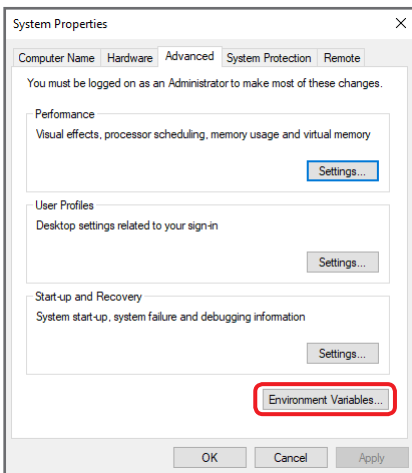
## Setting the path

Set the path to be used in PostgreSQL.

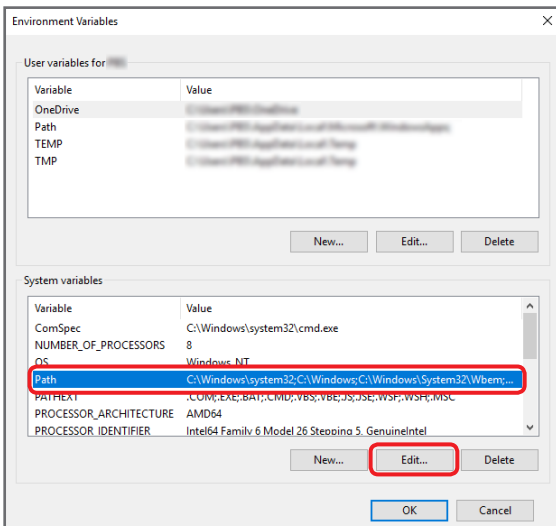
- 1 Enter “Edit the System environment variables” in the Windows search box, and click the appropriate search result.

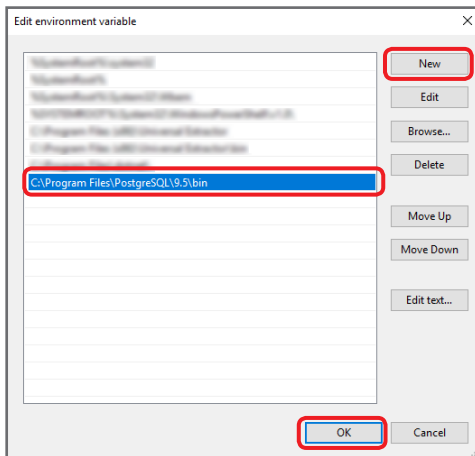


- 2 Click [Environment Variables].



- 3 Select “Path” under System variables, and click [Edit].



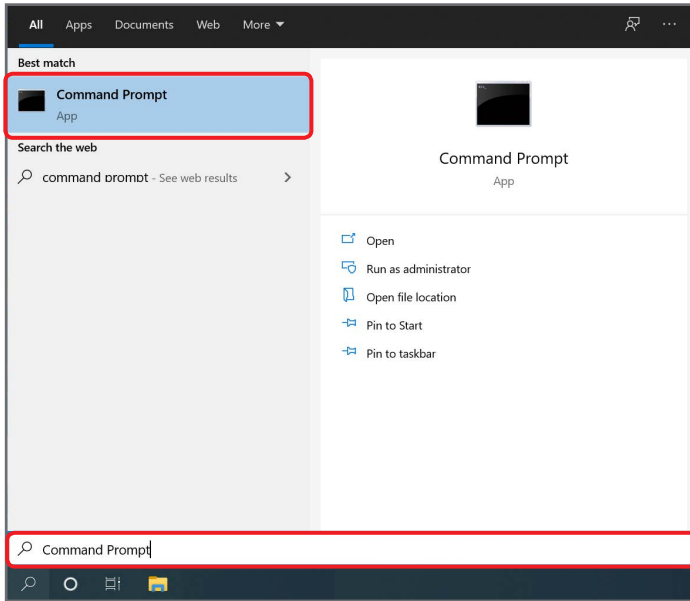
**4** Click [New], add the path of the folder where the psql commands are installed, and click [OK].**Note**

- The psql commands are installed in the "bin" folder in the destination specified in step 3 in "Installing PostgreSQL" (→8).
- If the installation destination specified in step 3 in "Installing PostgreSQL" (→8) is "C:\Program Files\PostgreSQL\9.5", set the path to "C:\Program Files\PostgreSQL\9.5\bin".

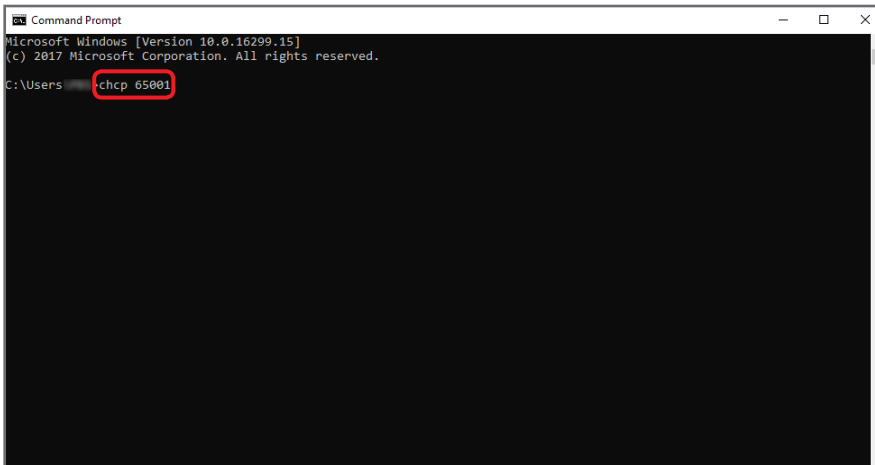
## Importing and checking data

Log in to PostgreSQL using the command prompt, and configure the settings.

### 1 Enter “Command Prompt” in the Windows search box, and click the appropriate search result.

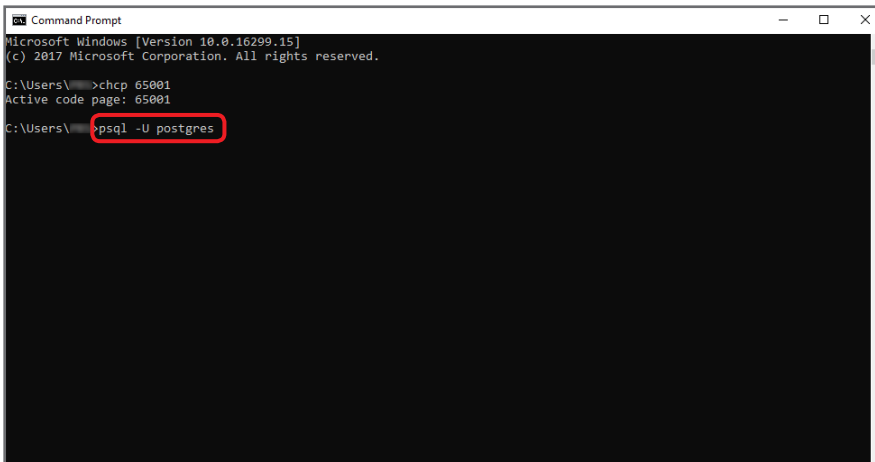


### 2 Enter “chcp 65001”, and press the [Enter] key.



If the command is successful, “Active code page: 65001” is displayed.

### 3 Enter “psql -U postgres”, and press the [Enter] key.



When “Password for user postgres:” is displayed, enter the password set in step 5 in “Installing PostgreSQL” (→8), and press the [Enter] key.

If the command is successful, “postgres=#” is displayed.

#### 4 Enter “create database p2castdb;”, and press the [Enter] key.

```

Command Prompt - psql -U postgres
Microsoft Windows [Version 10.0.16299.15]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\>chcp 65001
Active code page: 65001

C:\Users\>psql -U postgres
Password for user postgres:
psql (9.5.15)
WARNING: Console code page (65001) differs from Windows code page (1252)
         8-bit characters might not work correctly. See psql reference
         page "Notes for Windows users" for details.
Type "help" for help.

postgres=# create database p2castdb;

```

#### 5 Enter “\l”, and press the [Enter] key.

```

Command Prompt - psql -U postgres
Microsoft Windows [Version 10.0.16299.15]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\>chcp 65001
Active code page: 65001

C:\Users\>psql -U postgres
Password for user postgres:
psql (9.5.15)
WARNING: Console code page (65001) differs from Windows code page (1252)
         8-bit characters might not work correctly. See psql reference
         page "Notes for Windows users" for details.
Type "help" for help.

postgres=# create database p2castdb;
CREATE DATABASE
postgres=# \l

```

If the commands entered in steps 4 and 5 are successful, the following output is displayed on the screen. Leave the window open, and go to the next step.

```

Command Prompt - psql -U postgres
Microsoft Windows [Version 10.0.16299.15]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\>chcp 65001
Active code page: 65001

C:\Users\>psql -U postgres
Password for user postgres:
psql (9.5.15)
WARNING: Console code page (65001) differs from Windows code page (1252)
         8-bit characters might not work correctly. See psql reference
         page "Notes for Windows users" for details.
Type "help" for help.

postgres=# create database p2castdb;
CREATE DATABASE
postgres=# \l

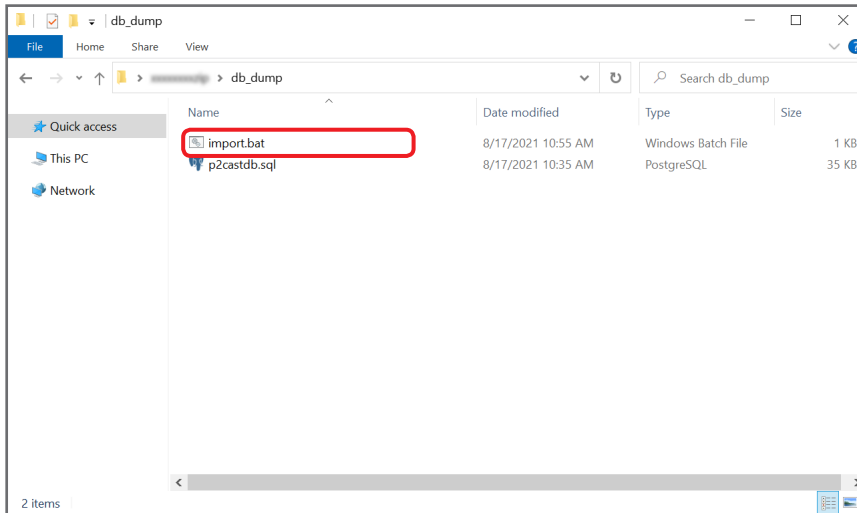
```

List of databases					
Name	Owner	Encoding	Collate	Ctype	Access privileges
p2castdb	postgres	UTF8	English_United Kingdom.1252	English_United Kingdom.1252	
postgres	postgres	UTF8	English_United Kingdom.1252	English_United Kingdom.1252	
template0	postgres	UTF8	English_United Kingdom.1252	English_United Kingdom.1252	=c/postgres +
template1	postgres	UTF8	English_United Kingdom.1252	English_United Kingdom.1252	=c/postgres +
					postgres=CTC/postgres

```

(4 rows)
postgres=#

```

**6** Open the “db\_dump” folder among the downloaded files, and double-click “import.bat”.

A new command prompt window will appear.

When “Password for user postgres:” is displayed, enter the password set in step 5 in “Installing PostgreSQL” (→8), and press the [Enter] key.

When “Press any key to continue...” is displayed, press a key, and close the command prompt window that appears in this step.

**7** Return to the window in step 5, enter “\c p2castdb”, and press the [Enter] key.

```

Command Prompt - psql -U postgres
Microsoft Windows [Version 10.0.16299.15]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\>chcp 65001
Active code page: 65001

C:\Users\>psql -U postgres
Password for user postgres:
psql (9.5.15)
WARNING: console code page (65001) differs from Windows code page (1252)
8-bit characters might not work correctly. See psql reference
page "Notes for Windows users" for details.
Type "help" for help.

postgres=# create database p2castdb;
CREATE DATABASE
postgres=# \l
      Name | Owner  | Encoding | Collate          | Ctype          | Access privileges
-----|-----|-----|-----|-----|-----
 p2castdb | postgres | UTF8     | English_United_Kingdom.1252 | English_United_Kingdom.1252 |
 postgres | postgres | UTF8     | English_United_Kingdom.1252 | English_United_Kingdom.1252 |
 template0 | postgres | UTF8     | English_United_Kingdom.1252 | English_United_Kingdom.1252 | =c/postgres +
          |          |          |          |          | postgres=CTc/postgres
 template1 | postgres | UTF8     | English_United_Kingdom.1252 | English_United_Kingdom.1252 | =c/postgres +
          |          |          |          |          | postgres=CTc/postgres
(4 rows)

postgres=# \c p2castdb

```



## 8 Enter “\dt”, and press the [Enter] key.

```

Command Prompt - psql -U postgres
C:\Users\>psql -U postgres
Password for user postgres:
psql (9.5.15)
WARNING: Console code page (65001) differs from Windows code page (1252)
8-bit characters might not work correctly. See psql reference
page "Notes for Windows users" for details.
Type "help" for help.

postgres=# create database p2castdb;
CREATE DATABASE
postgres=# \l

```

Name	Owner	Encoding	Collate	Ctype	Access privileges
p2castdb	postgres	UTF8	English_United_Kingdom.1252	English_United_Kingdom.1252	
postgres	postgres	UTF8	English_United_Kingdom.1252	English_United_Kingdom.1252	
template0	postgres	UTF8	English_United_Kingdom.1252	English_United_Kingdom.1252	=c/postgres +
template1	postgres	UTF8	English_United_Kingdom.1252	English_United_Kingdom.1252	=c/postgres + postgres=CTC/postgres

```

(4 rows)

postgres=# \c p2castdb
WARNING: Console code page (65001) differs from Windows code page (1252)
8-bit characters might not work correctly. See psql reference
page "Notes for Windows users" for details.
You are now connected to database "p2castdb" as user "postgres".
p2castdb=# \dt

```

If the commands entered in steps 7 and 8 are successful, the following output is displayed on the screen.

```

Command Prompt - psql -U postgres
p2castdb=# \dt

```

Schema	Name	Type	Owner
public	t_app_author	table	postgres
public	t_app_content	table	postgres
public	t_app_entry	table	postgres
public	t_app_p2equipment	table	postgres
public	t_camera_blob	table	postgres
public	t_camera_content	table	postgres
public	t_camera_entry	table	postgres
public	t_camera_ftp	table	postgres
public	t_camera_link	table	postgres
public	t_camera_p2equipment	table	postgres
public	t_camera_properties	table	postgres
public	t_camera_status	table	postgres
public	t_camera_streaming	table	postgres
public	t_camera_summary	table	postgres
public	t_codes	table	postgres
public	t_companys	table	postgres
public	t_equipment_group	table	postgres
public	t_groups	table	postgres
public	t_licenses	table	postgres
public	t_user_equipment	table	postgres
public	t_user_group	table	postgres
public	t_users	table	postgres

```

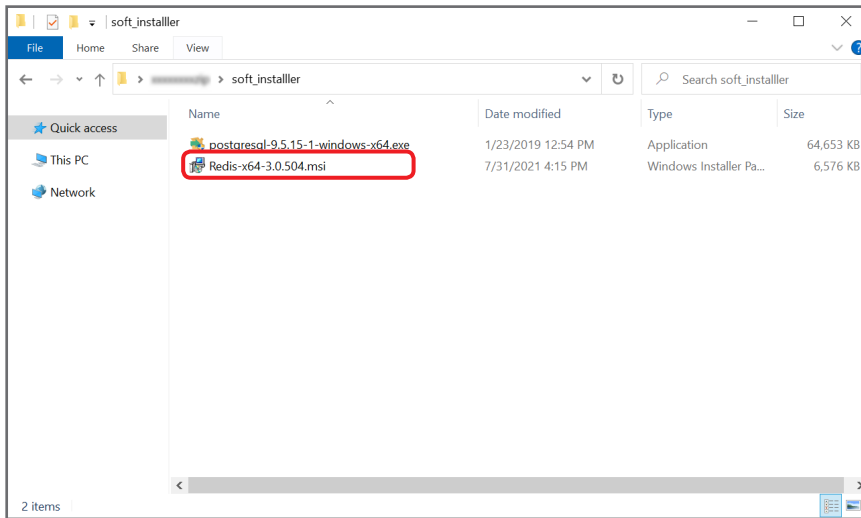
(22 rows)
p2castdb=#

```

## Installing Redis

Install Redis.

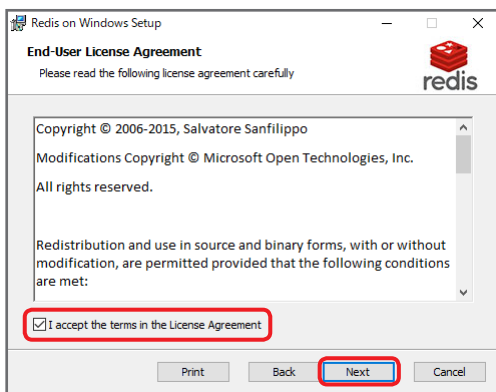
- 1 Open the “soft\_installer” folder among the downloaded files, and double-click “Redis-x64-3.0.504.msi”.



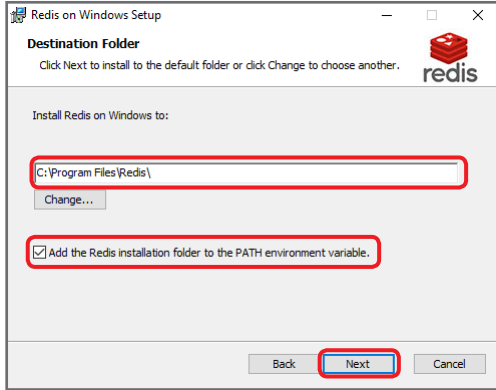
- 2 Click [Next].



- 3 Check the box next to “I accept the terms in the License Agreement”, and click [Next].



**4 Specify the installation directory, check the box next to “Add the Redis installation folder to the PATH environment variable.”, and click [Next].**

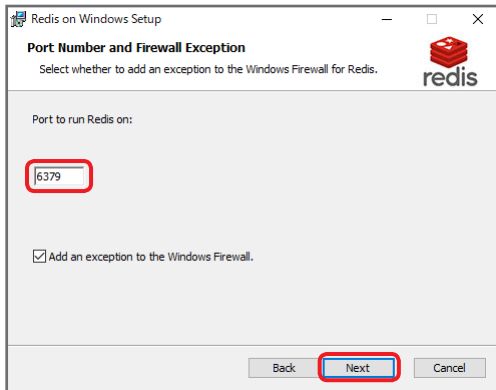


**Note**

- Using the default value for the directory is recommended.

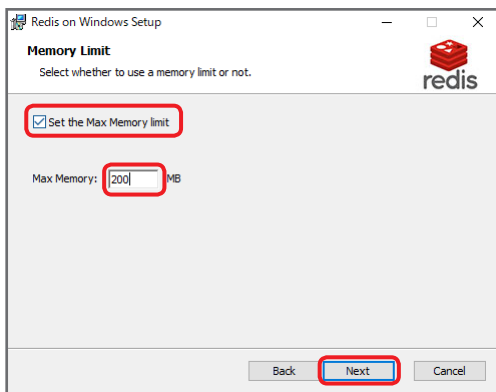
**5 Select a port number for the Redis service, and click [Next].**

Select the default value of “6379”.



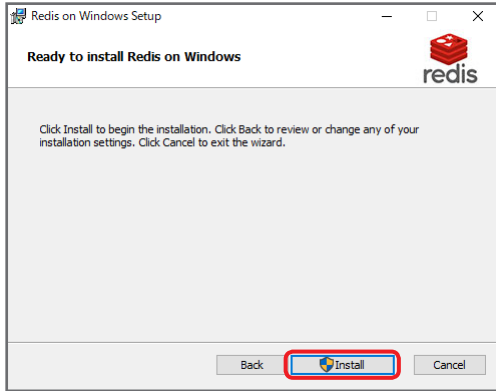
**6 Check the box next to “Set the Max Memory limit”, enter a setting for “Max Memory”, and click [Next].**

Set “Max Memory” to “200” MB.

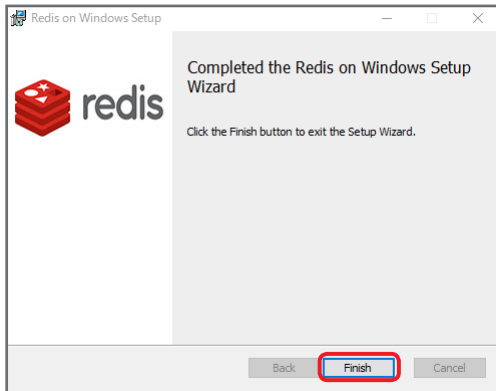


## 7 Click [Install].

Installation starts.



## 8 Click [Finish].

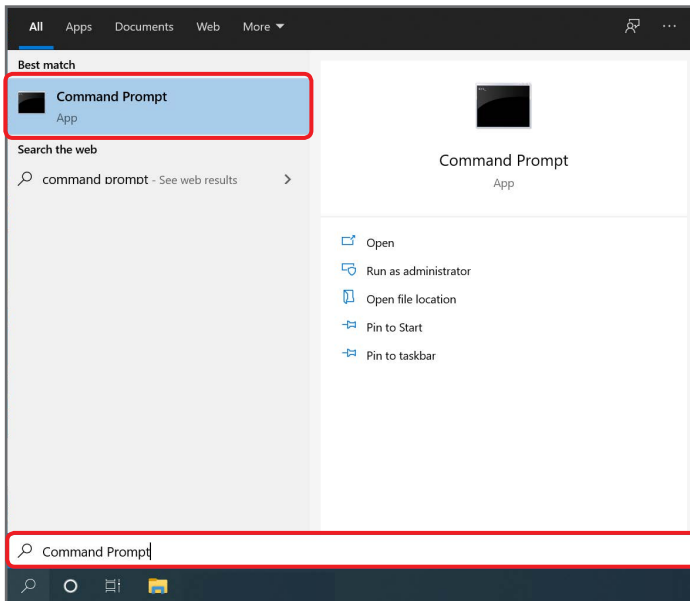


This completes Redis installation.

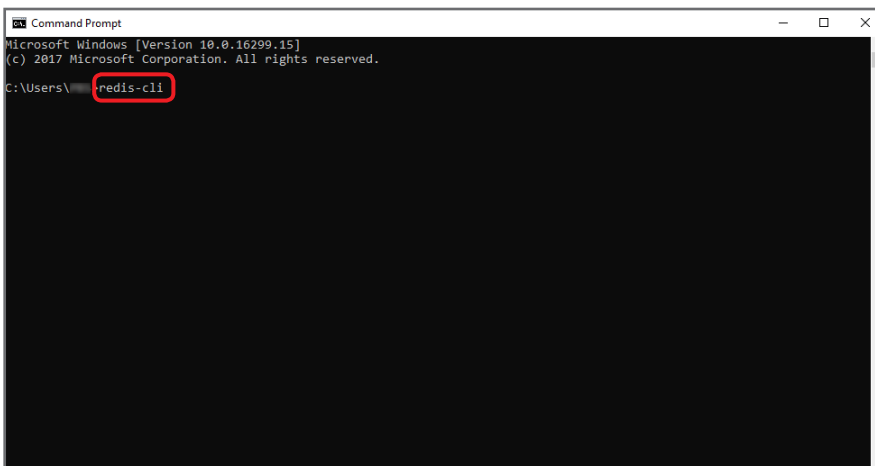
## Checking the installation result

Check that you can connect to the Redis service using the command prompt.

- 1 Enter “Command Prompt” in the Windows search box, and click the appropriate search result.

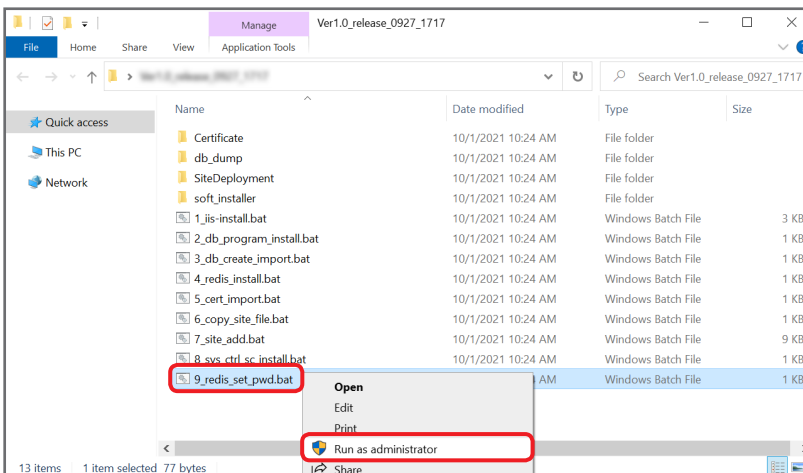


- 2 Enter “redis-cli”, and press the [Enter] key.



If the command is successful, “127.0.0.1:6379” is displayed.

- 3 Right-click “9\_redis\_set\_pwd.bat” among the downloaded files, and click [Run as administrator].



The command prompt window will appear.

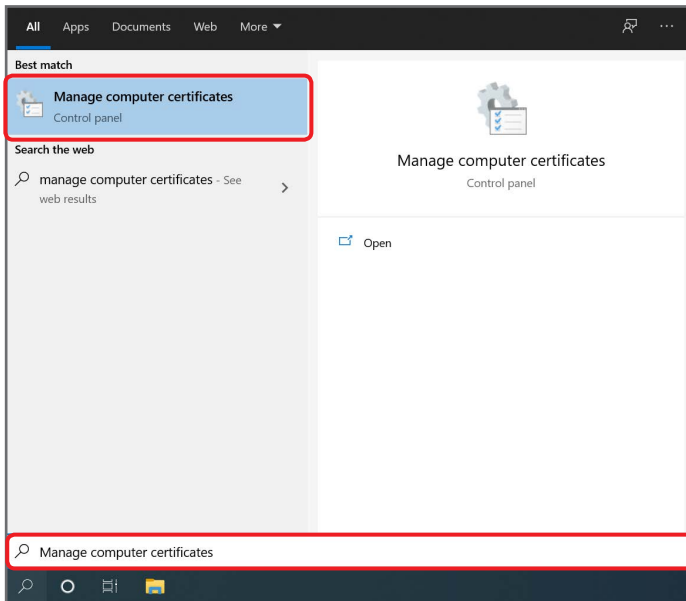
When “Press any key to continue...” is displayed, press a key, and close the window.

## Installing certificates

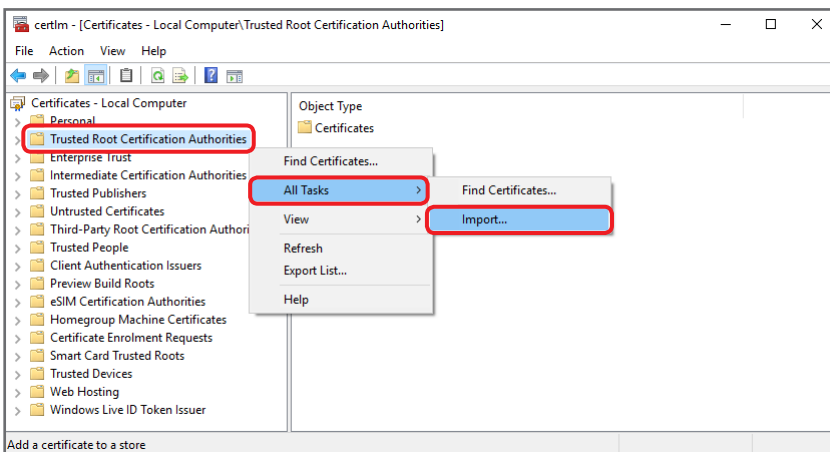
Import the necessary certificates.

### Importing CA certificates

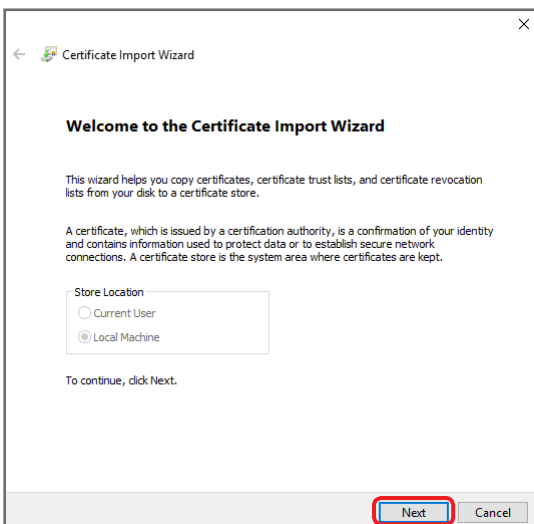
- 1 Enter “Manage computer certificates” in the Windows search box, and click the appropriate search result.



- 2 Right-click “Trusted Root Certification Authorities”, and select [Import] under [All Tasks].



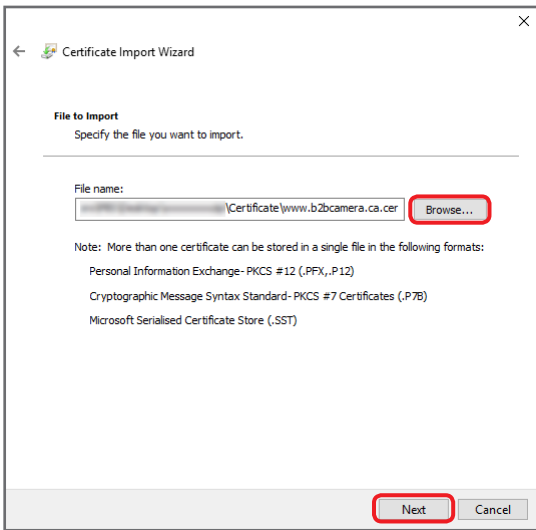
- 3 Click [Next].



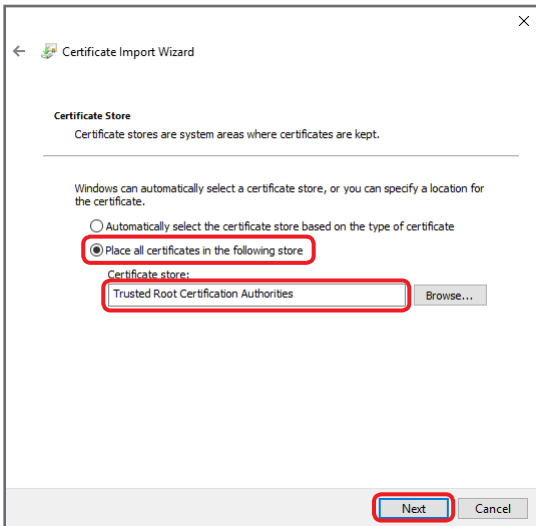
**4 Click [Browse], specify the file to be imported, and click [Next].**

- File name: www.b2bcamera.ca.cer

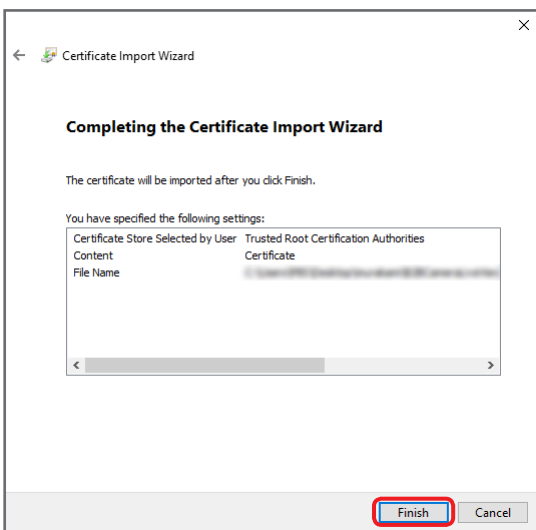
This file is included in the “Certificate” folder among the downloaded files.



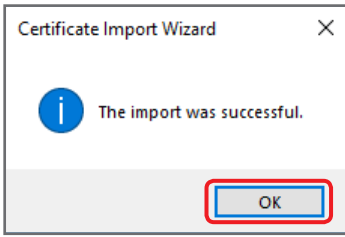
**5 Select “Place all certificates in the following store”, specify “Trusted Root Certification Authorities” as the destination, and click [Next].**



**6 Click [Finish].**

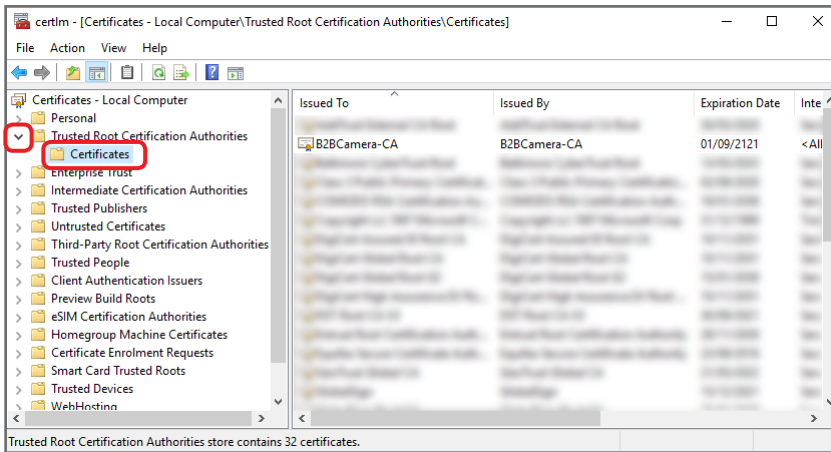


**7** Click [OK].



**Confirming imported CA certificates**

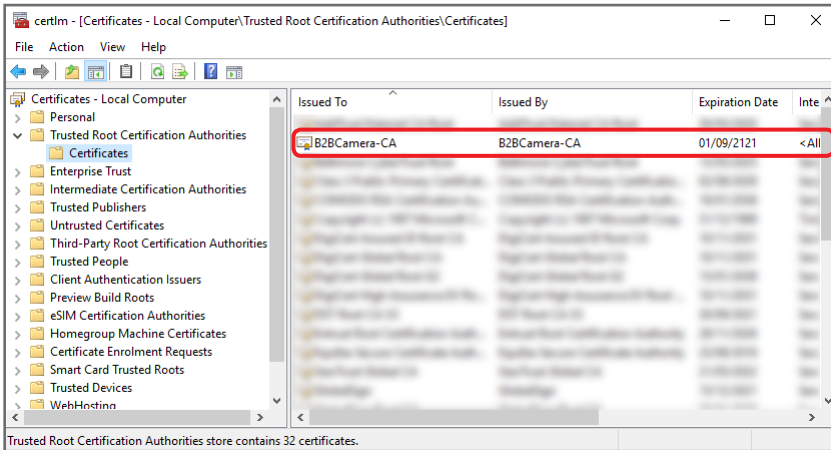
**1** In the Manage computer certificates window, open “Trusted Root Certification Authorities”, and click “Certificates”.



**2** Confirm that the imported certificate is included.

Check the following certificate.

- Issued To: B2BCamera-CA / Issued By: B2BCamera-CA

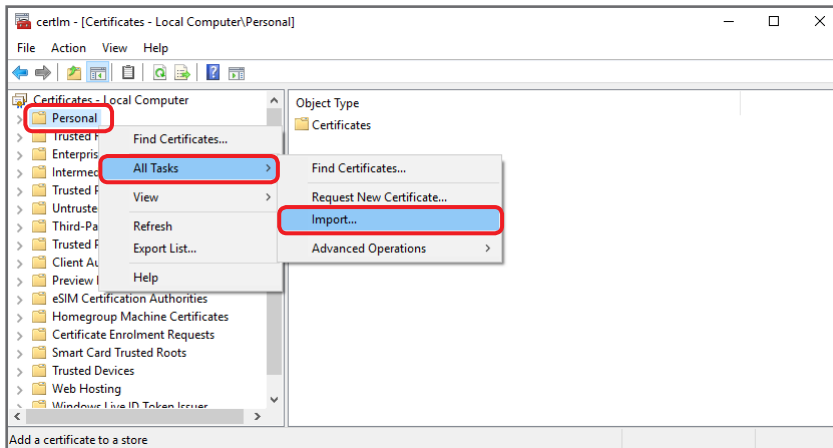




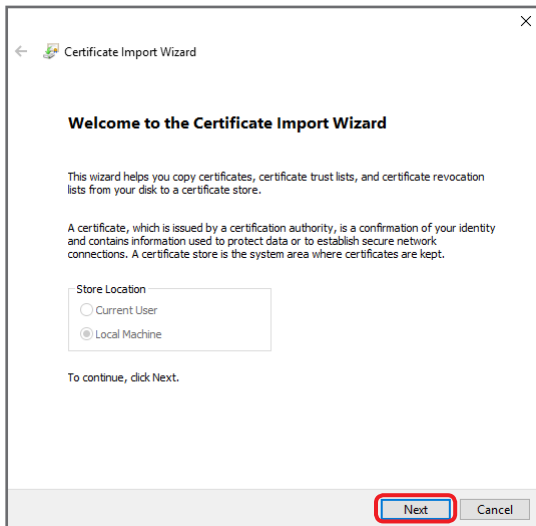
## Importing server certificates

Two types of certificates need to be imported. Perform the steps below twice.

### 1 In the Manage computer certificates window, right-click “Personal”, and select “Import” under “All Tasks”.



### 2 Click [Next].

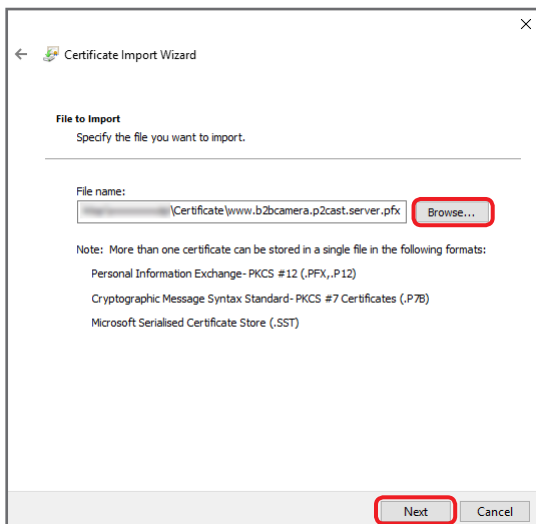


### 3 Click [Browse], specify the file to be imported, and click [Next].

- File names: www.b2bcamera.p2cast.server.pfx  
www.b2bcamera.pcpf.server.pfx

These files are included in the “Certificate” folder among the downloaded files.

If they are not displayed in the “Certificate” folder, select [All files (\*.\*)] from the lower right pull-down menu.

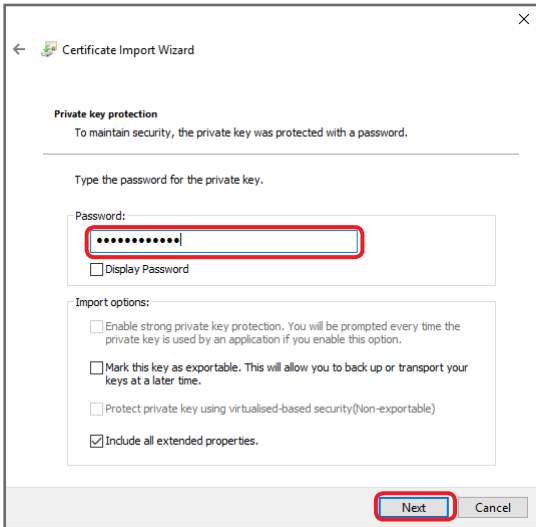


**4 Enter the password, and click [Next].**

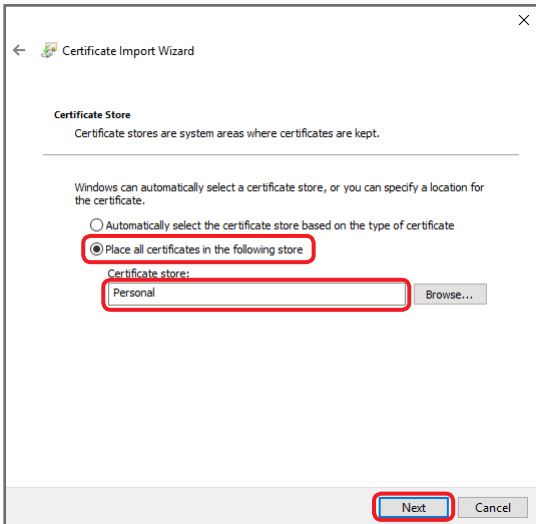
The password is displayed as a series of dots (●).

- Password: Panasonic123

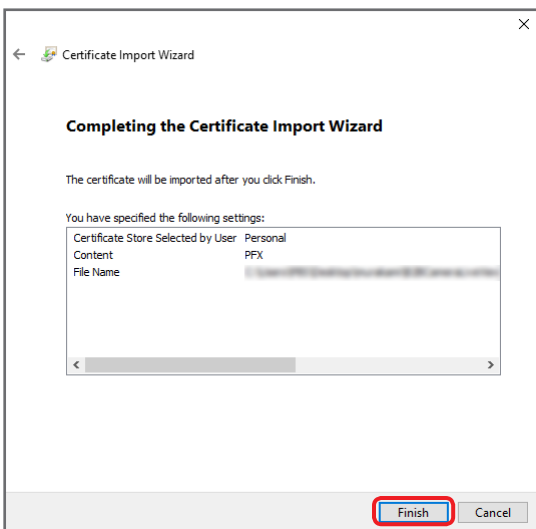
Leave the import options set to the default values.



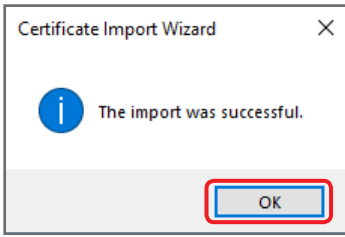
**5 Select “Place all certificates in the following store”, specify “Personal” as the destination, and click [Next].**



**6 Click [Finish].**

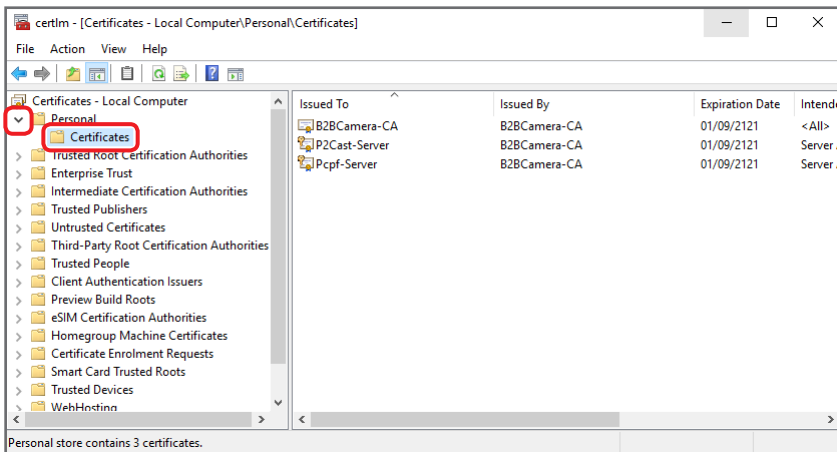


7 Click [OK].



Confirming imported server certificates

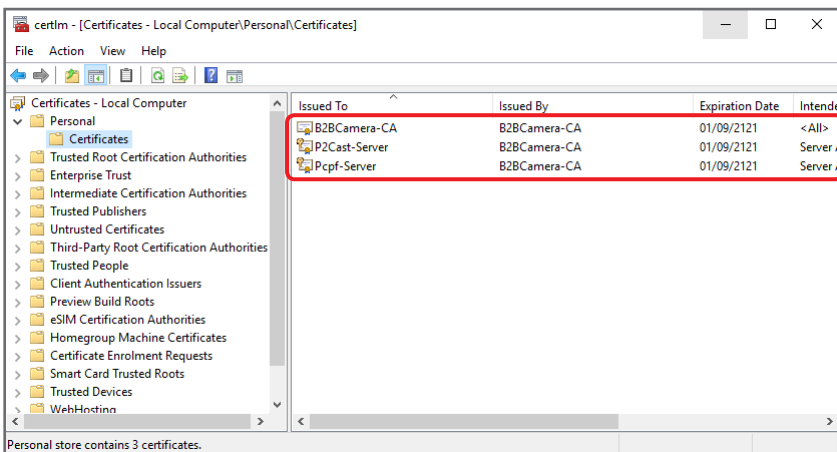
1 In the Manage computer certificates window, open “Personal”, and click “Certificates”.



2 Confirm that the imported certificates are included.

Check the following certificates.

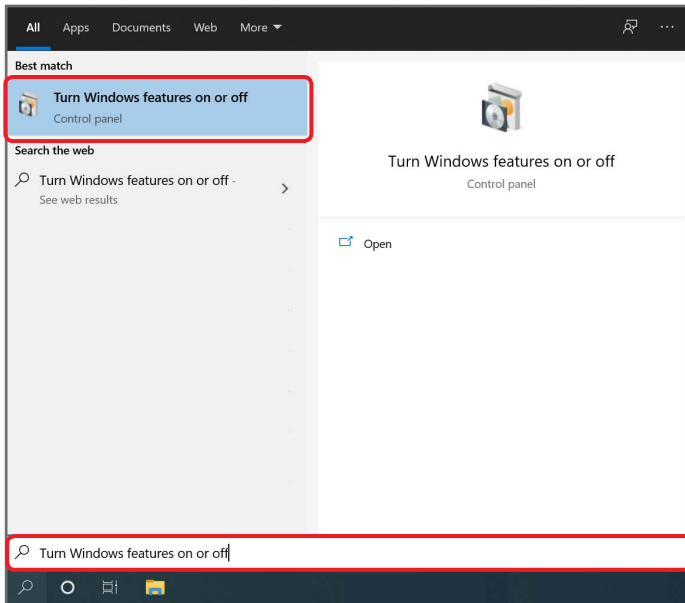
- Issued To: B2BCamera-CA / Issued By: B2BCamera-CA
- Issued To: P2Cast-Server / Issued By: B2BCamera-CA
- Issued To: Pcpf-Server / Issued By: B2BCamera-CA



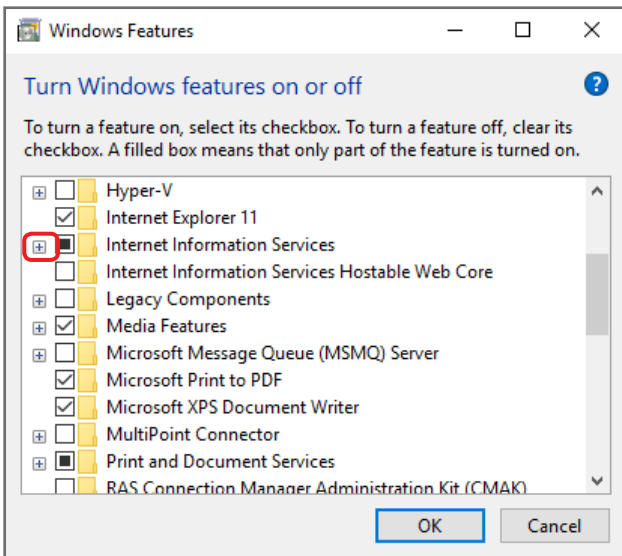
## Enabling Windows functions

Configure the settings to enable Windows functions.

- 1 Enter “Turn Windows features on or off” in the Windows search box, and click the appropriate search result.

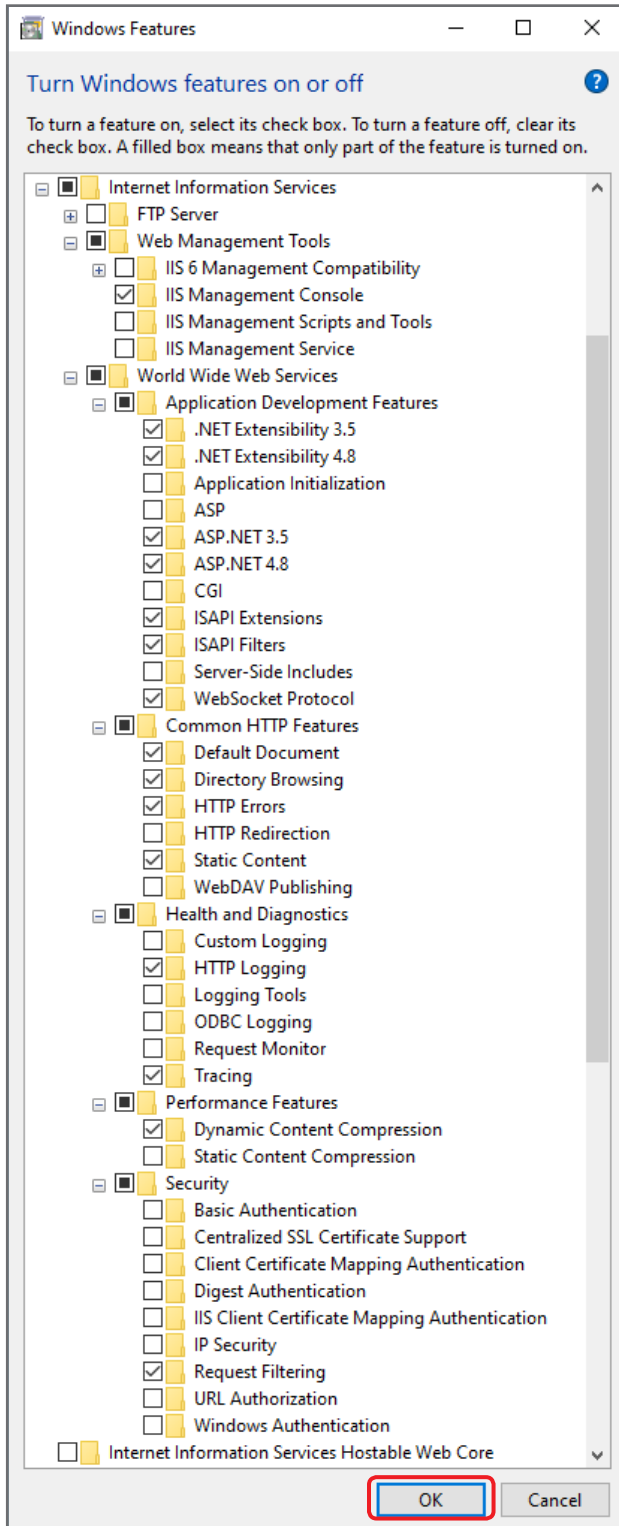


- 2 Open “Internet Information Services”.

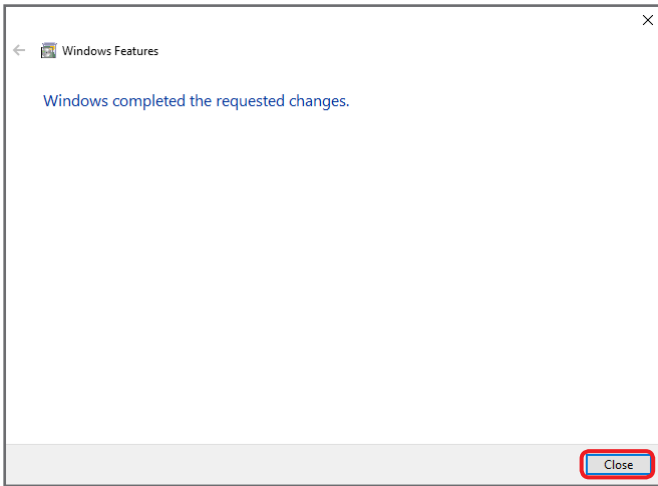


**3 Check the boxes next to the functions to be enabled, and click [OK].**

Check the boxes as shown below.



**4** Click [Close].



This completes all settings to enable Windows functions.

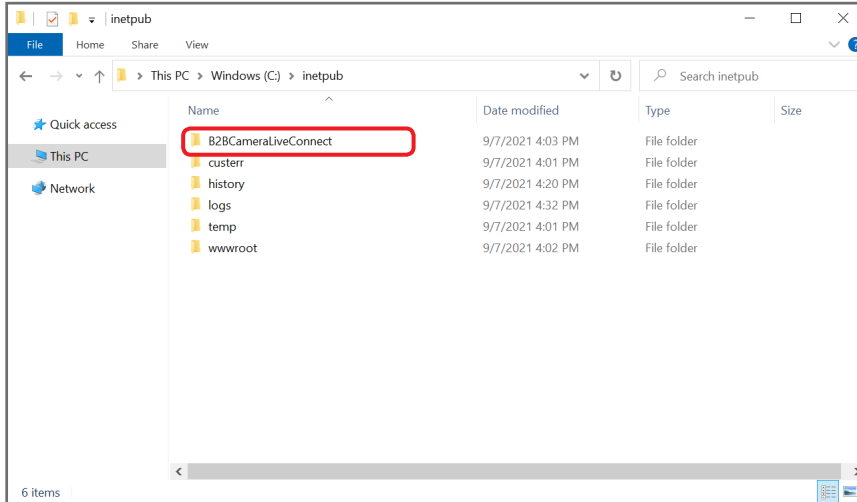
## Creating sites

Install this application, and configure the settings.

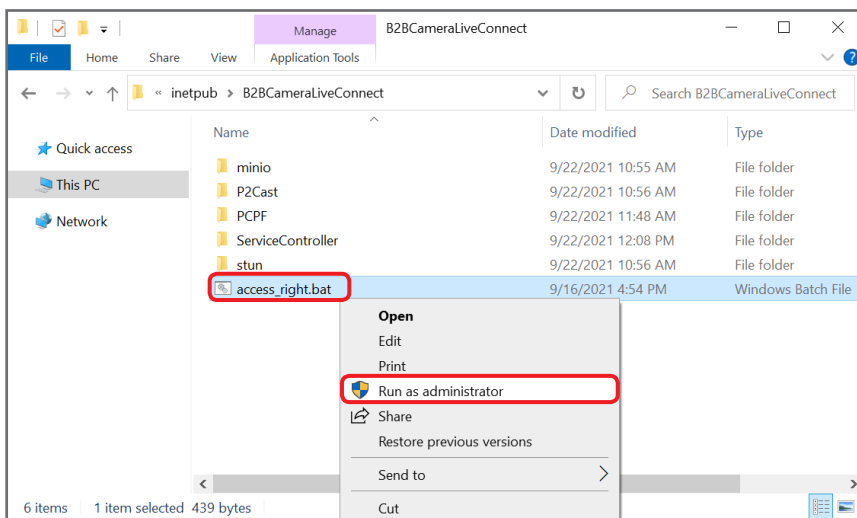
### Copying site files and setting access privileges

Install this application in your computer, and configure access privileges.

- 1 Open the “SiteDeployment” folder among the downloaded files, and copy the “B2BCameraLiveConnect” folder to the “C:\inetpub” folder.



- 2 Open the “B2BCameraLiveConnect” folder, right-click “access\_right.bat”, and select [Run as administrator].



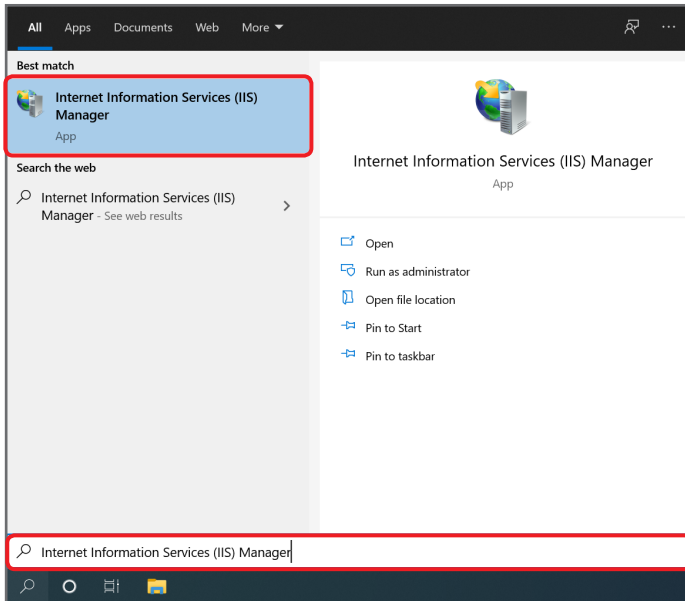
The command prompt window will appear.

When “Press any key to continue...” is displayed, press a key, and close the window.

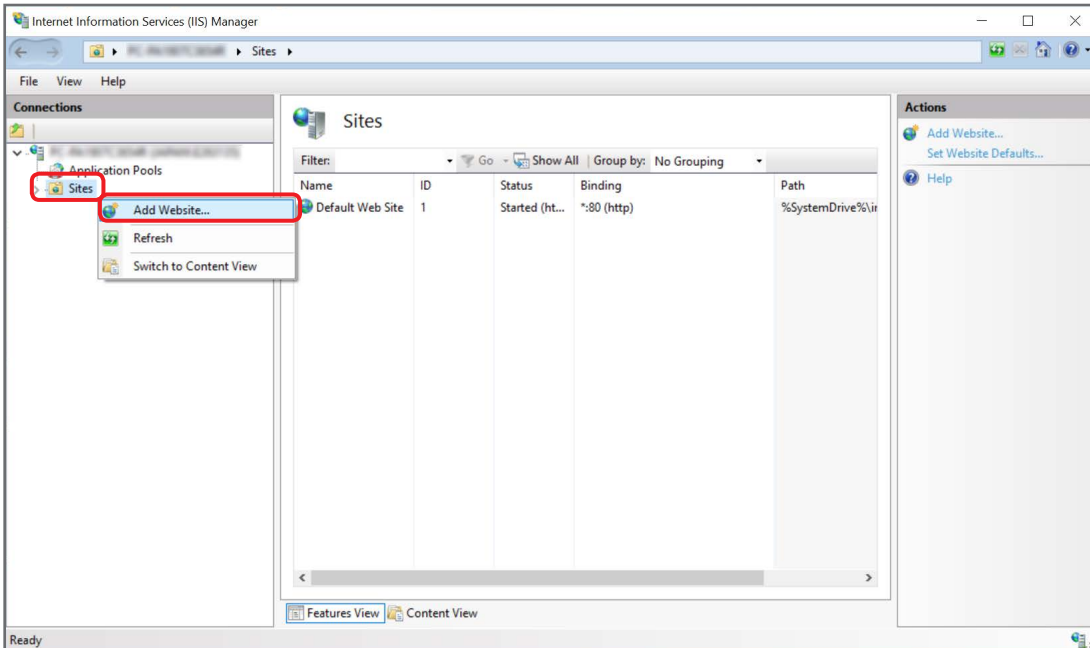
## Creating the site for the LiveConnect server

Create the site for the LiveConnect server.

- 1 Enter “Internet Information Services (IIS) Manager” in the Windows search box, and click the appropriate search result.



- 2 Right-click [Sites], and select [Add Website].





### 3 Configure the site settings, and click [OK].

Enter or select the following items.

- Site name: B2BCamera LiveConnect
- Physical path: C:\inetpub\B2BCameraLiveConnect\P2Cast
- Type: https
- IP address\*1: (Select from the pull-down menu)
- Port\*2: 443
- SSL certificate: www.b2bcamera.p2cast.server

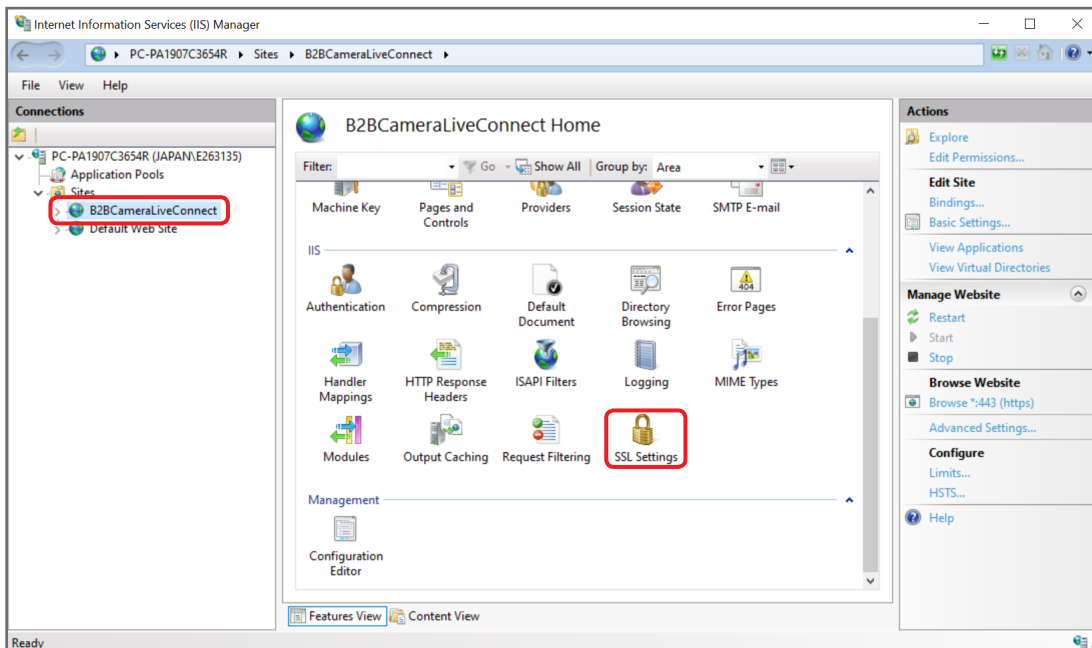
\*1 Select the IP address to be used in the connect server. Do not select “All Unassigned”.

\*2 If port number “443” has already been used by other services, specify an available port number instead.

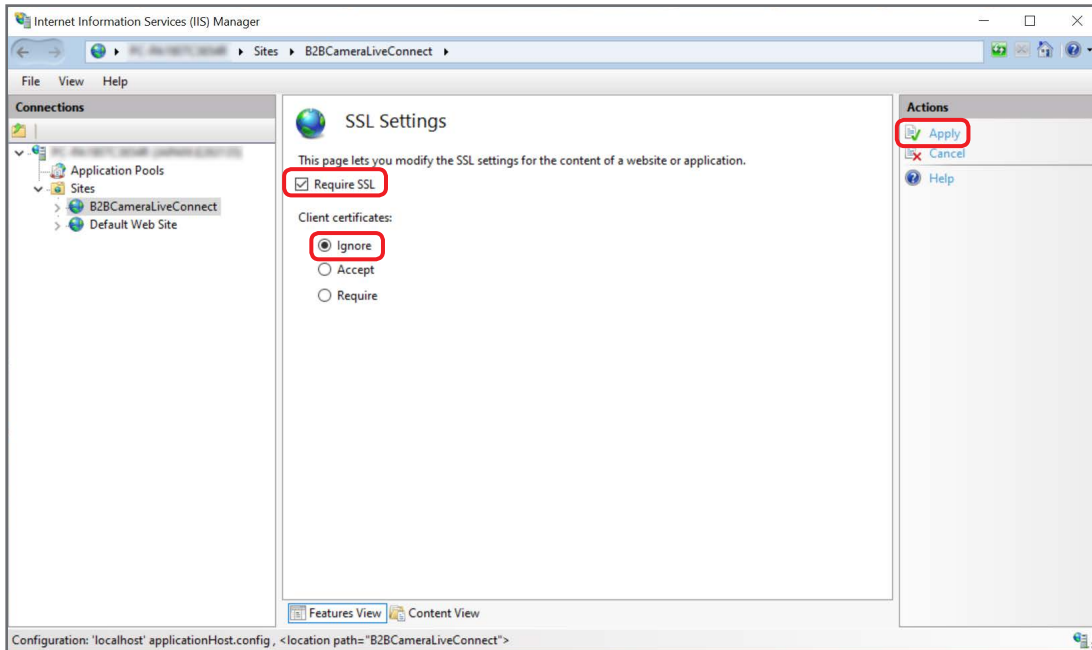
The screenshot shows the 'Add Website' dialog box with the following settings:

- Site name:** B2BCameraLiveConnect
- Physical path:** C:\inetpub\B2BCameraLiveConnect\P2Cast
- Binding Type:** https
- IP address:** 192.168.1.10
- Port:** 443
- SSL certificate:** www.b2bcamera.p2cast.server
- Start Website immediately:**

### 4 Click “B2BCameraLiveConnect”, and double-click “SSL Settings”.



## 5 Check the box next to “Require SSL”, select “Ignore” under client certificates, and click [Apply].

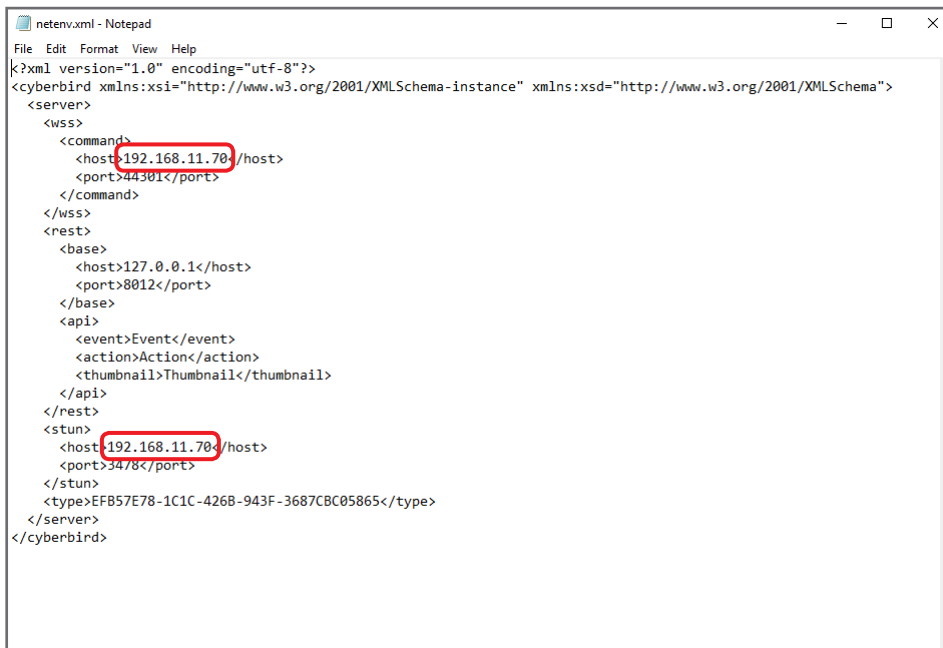


Leave the window open, and go to the next step.

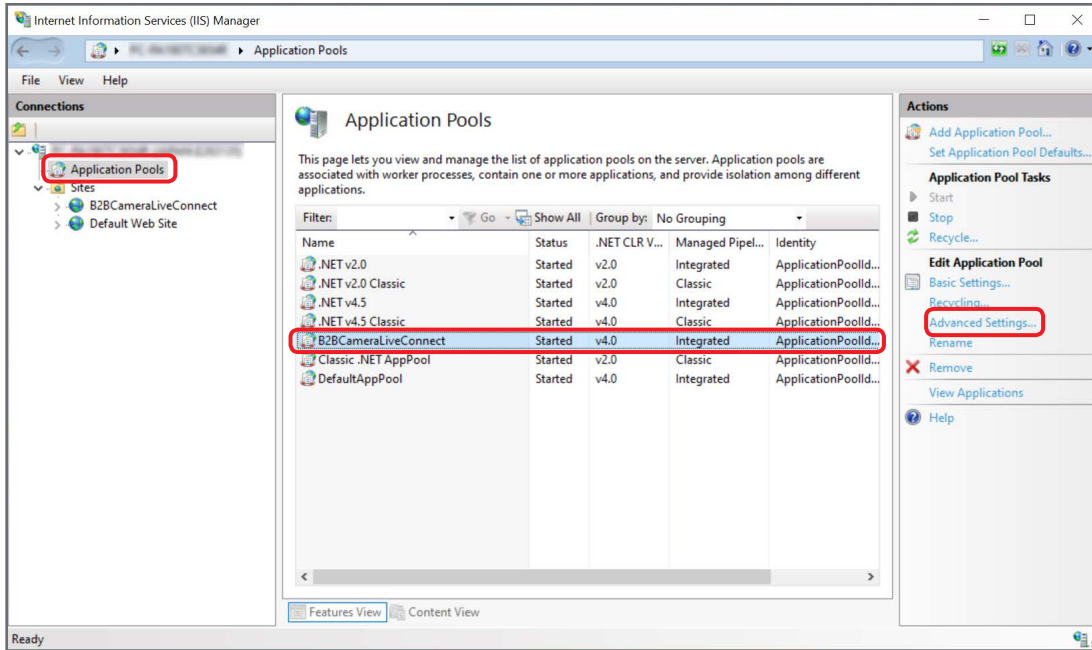
## 6 Open the “C:\inetpub\B2BCameraLiveConnect\IP2Cast\App\_Data” folder, and modify “netenv.xml” using a text editor.

Open a text editor by selecting “Run as administrator”, and modify “netenv.xml”.

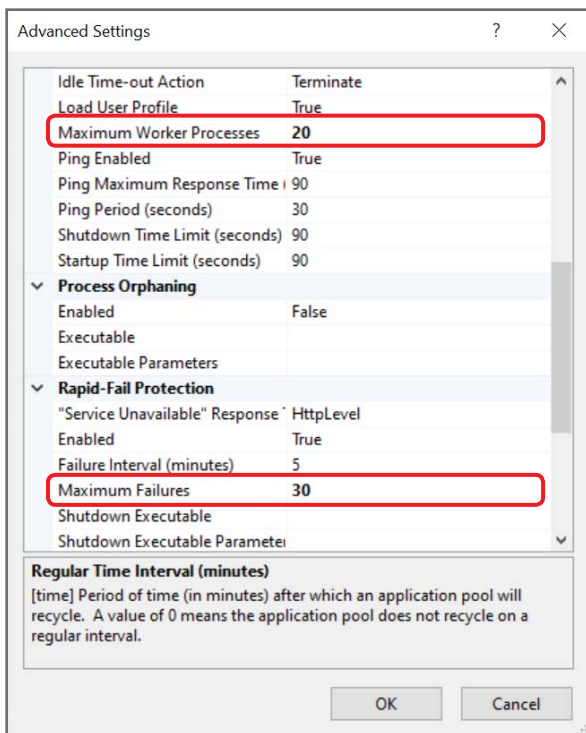
- Location to modify: <host>192.168.3.11</host>  
Replace “192.168.3.11” with the IP address to be used in the connect server.

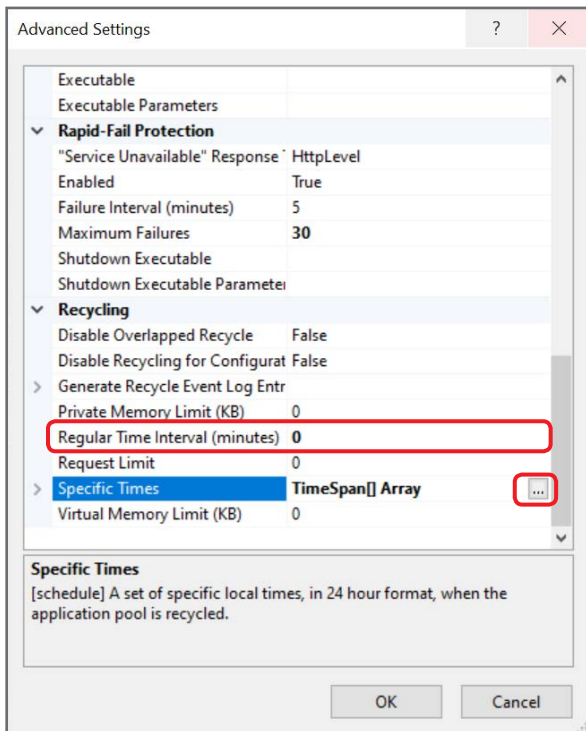
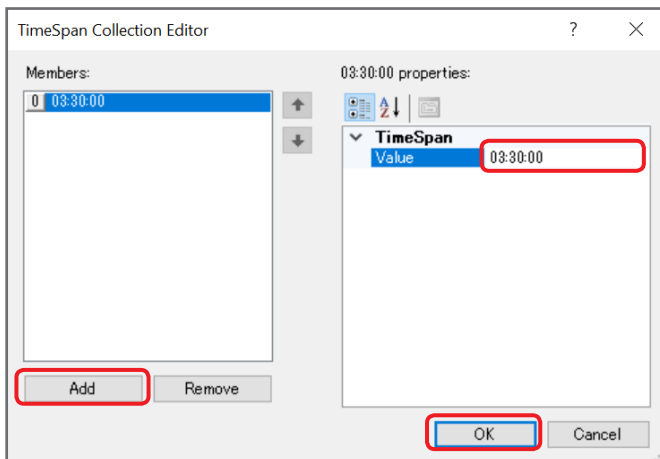


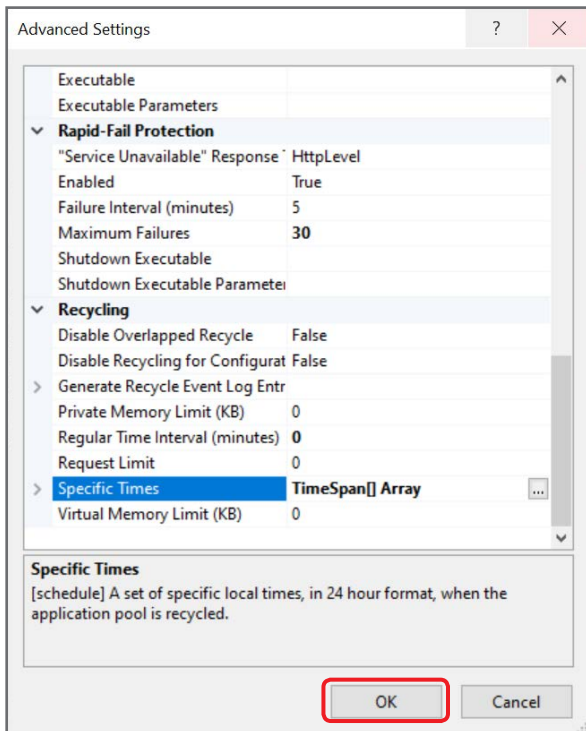
- 7 Return to the window in step 5. Click [Application Pools], select “B2BCameraLiveConnect”, and click [Advanced Settings].



- 8 Set Maximum Worker Processes to “20”, and Maximum Failures to “30”.



**9** Set Regular Time Interval to “0”, and click **...** for Specific Times.**10** Click **[Add]**, set Value to “03:30:00”, and click **[OK]**.

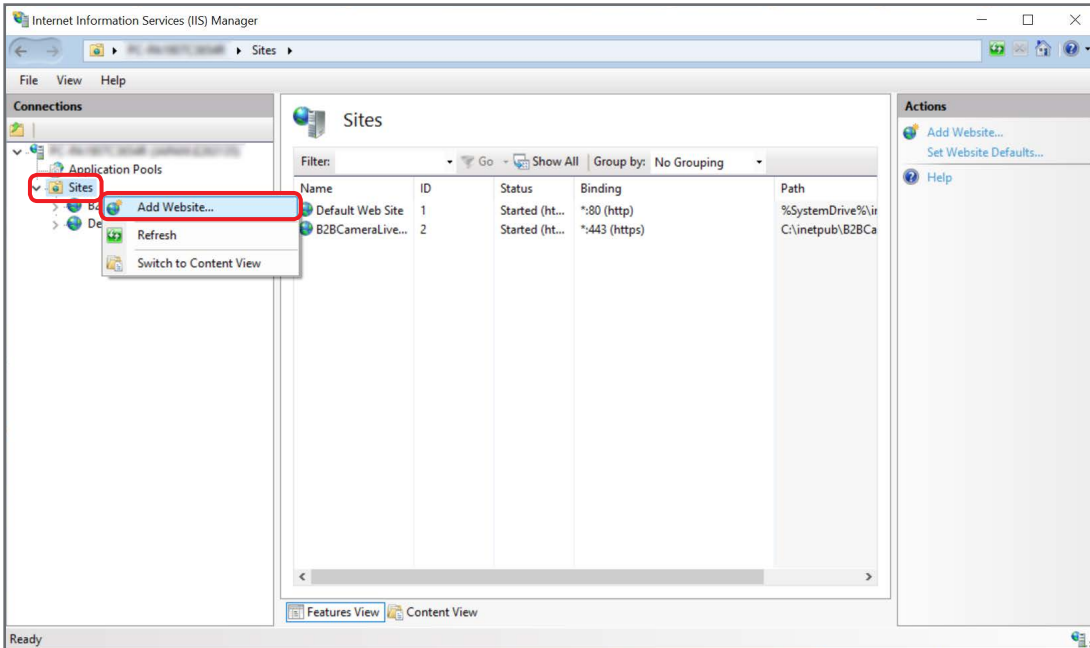
**11** Click [OK].

This completes creation of the LiveConnect server site.

## Creating the site for the M2M relay server

Create the site for the M2M relay server.

### 1 In the Internet Information Services (IIS) Manager window, right-click “Sites”, and select “Add Website”.



### 2 Configure the site settings, and click [OK].

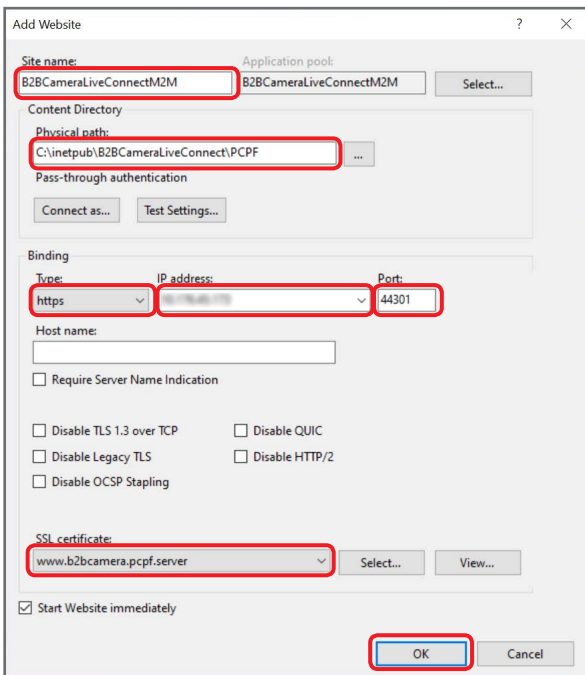
Enter or select the following items.

- Site name: B2BCameraLiveConnectM2M
- Physical path: C:\inetpub\B2BCameraLiveConnect\PCPF
- Type: https
- IP address\*1: (Select from the pull-down menu)
- Port\*2: 44301
- SSL certificate: www.b2bcamera.pcpf.server

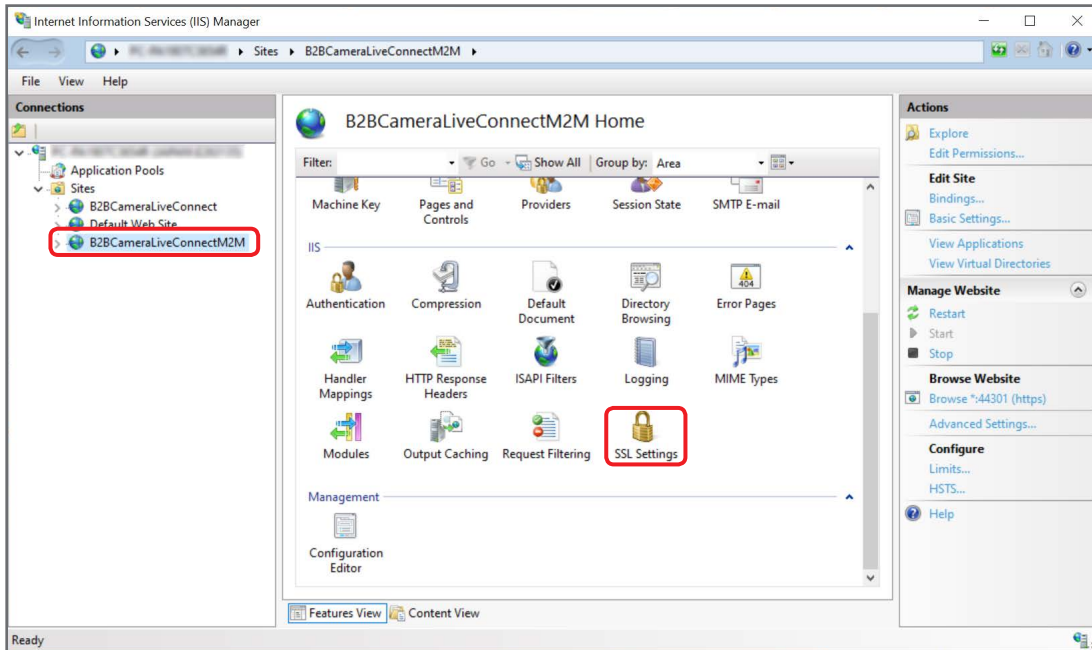
\*1 Select the IP address to be used in the connect server. Do not select “All Unassigned”.

\*2 If port number “44301” has already been used by other services, specify an available port number instead.

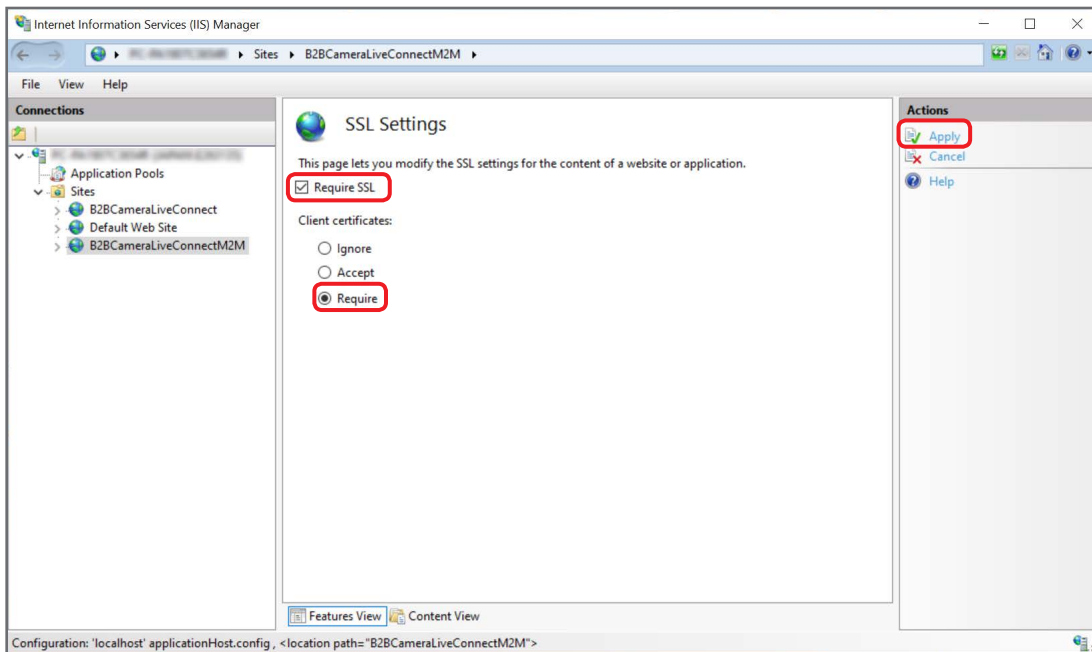
When specifying other port numbers than “44301”, “netenv.xml” needs to be modified (→34). Open a text editor by selecting “Run as administrator”, and replace “44301” of <port>44301<port> with the corresponding port number.



### 3 Click “B2BCameraLiveConnectM2M”, and double-click “SSL Settings”.



### 4 Check the box next to “Require SSL”, select “Require” under client certificates, and click [Apply].



Leave the window open, and go to the next step.

**5** Open the “C:\inetpub\B2BCameraLiveConnect\PCPF” folder, and modify “Web.config” using a text editor.

Open a text editor by selecting “Run as administrator”, and modify “Web.config”.

- Location to modify: `<add key="P2CastUrl" value="https://127.0.0.1:443/">`  
Replace “127.0.0.1” with the IP address to be used in the connect server.  
When specifying other ports than “443” in step 3 in “Creating the site for the LiveConnect server” (→32), replace “443” with the corresponding port number.

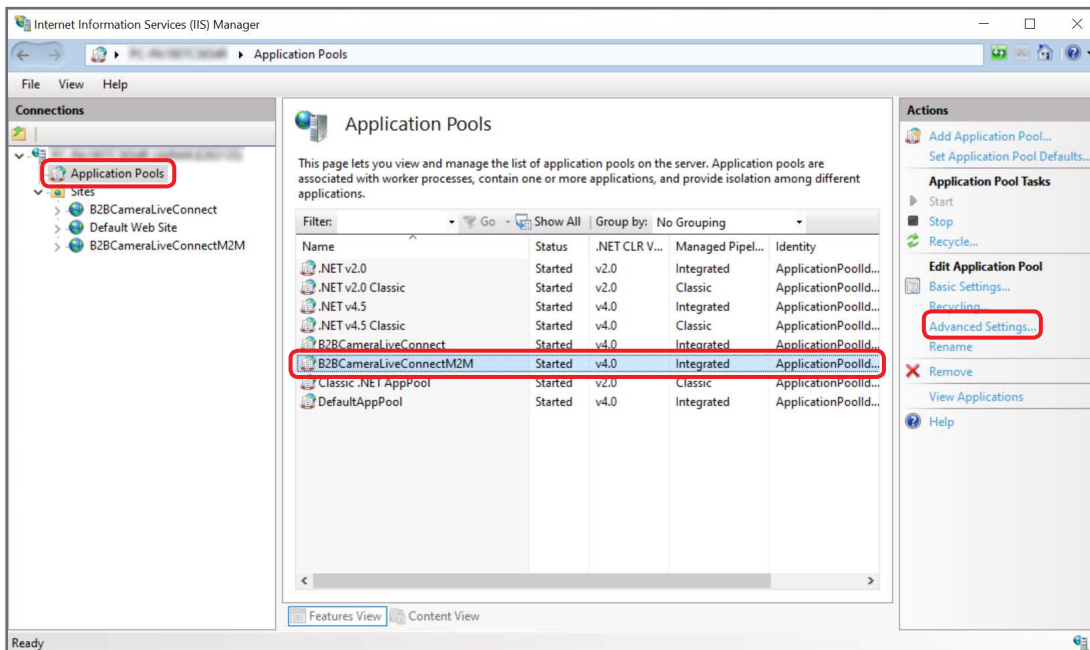


```

Web.config - Notepad
File Edit Format View Help
<?xml version="1.0"?>
<!--
For more information on how to configure your ASP.NET application, please visit
http://go.microsoft.com/fwlink/?LinkId=169433
-->
<configuration>
  <appSettings>
    <add key="webpages:Version" value="2.0.0.0"/>
    <add key="webpages:Enabled" value="false"/>
    <add key="PreserveLoginUrl" value="true"/>
    <add key="ClientValidationEnabled" value="true"/>
    <add key="UnobtrusiveJavaScriptEnabled" value="true"/>
    <add key="MaxLogFile" value="50"/>
    <add key="MaxLogCapacity" value="20"/>
    <add key="LowerLimitHardDiskFreeSpace" value="10"/>
    <add key="P2CastUrl" value="https://127.0.0.1:443/">
  </appSettings>
<!--
For a description of web.config changes see http://go.microsoft.com/fwlink/?LinkId=235367.

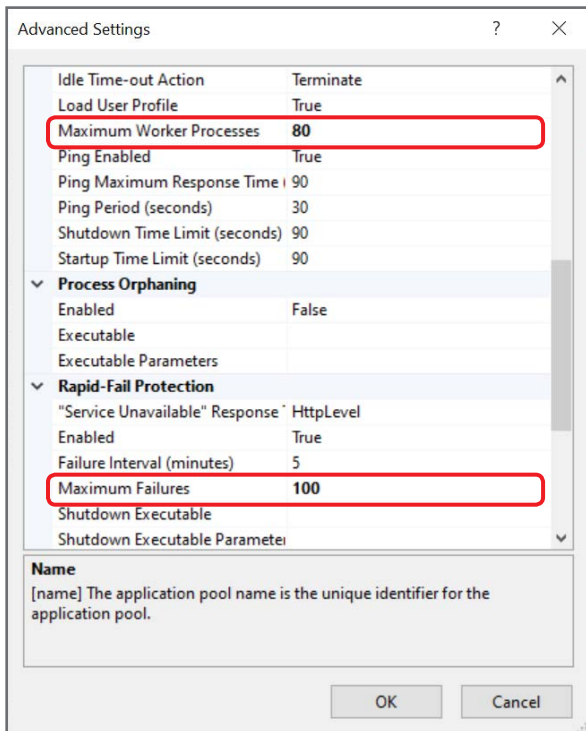
The following attributes can be set on the <httpRuntime> tag.
<system.Web>
  <httpRuntime targetFramework="4.6.2" />
</system.Web>
-->
<system.web>
<httpRuntime targetFramework="4.5"/>
<compilation targetFramework="4.6.2"/>
<pages>
  <namespaces>
    <add namespace="System.Web.Helpers"/>
  </namespaces>
</system.web>

```

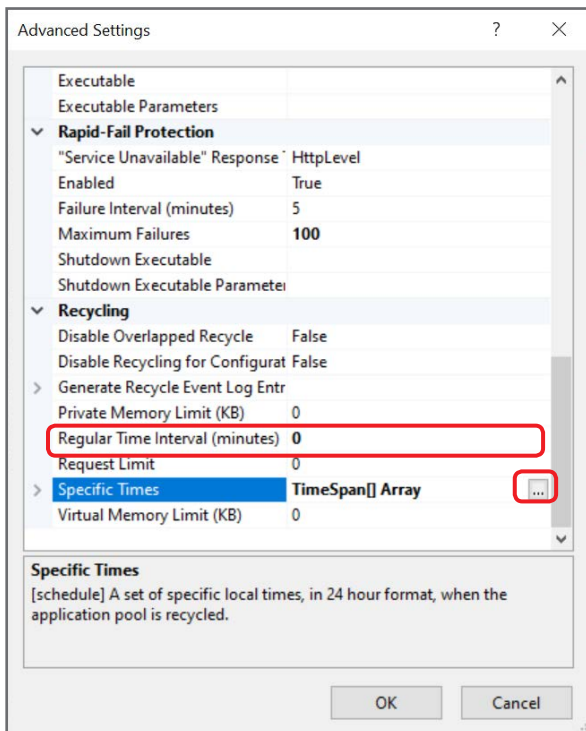
**6** Return to the window in step 4. Click [Application Pools], select “B2BCameraLiveConnectM2M”, and click [Advanced Settings].

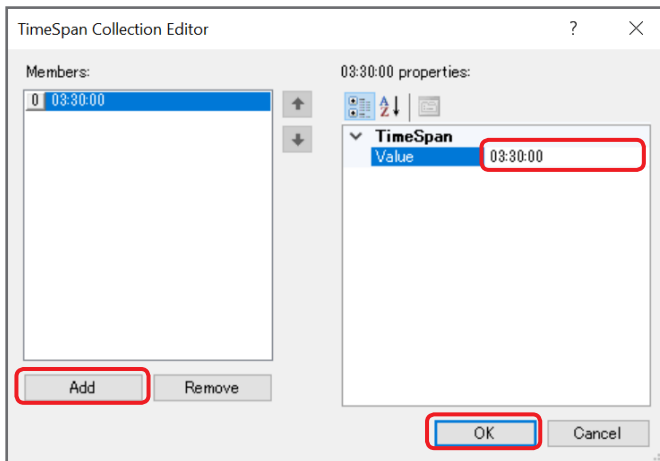
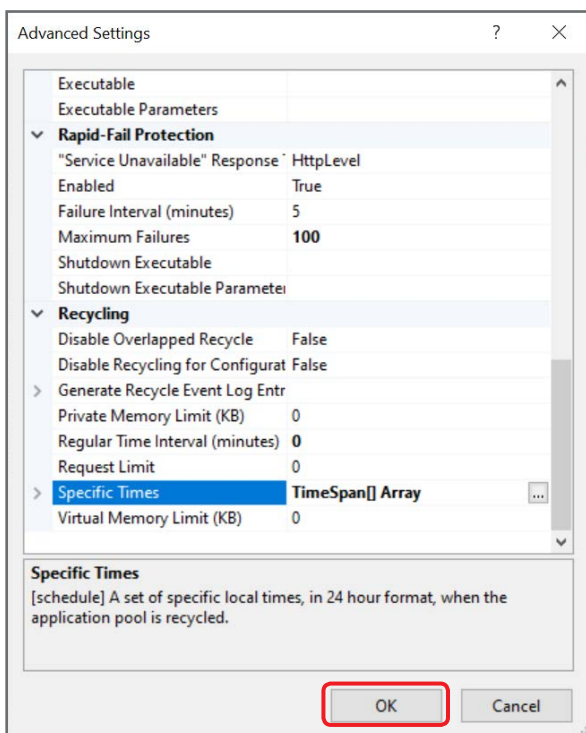


## 7 Set Maximum Worker Processes to “80”, and Maximum Failures to “100”.



## 8 Set Regular Time Interval to “0”, and click ... for Specific Times.



**9** Click [Add], set Value to “03:30:00”, and click [OK].**10** Click [OK].

This completes creation of the M2M relay server site.

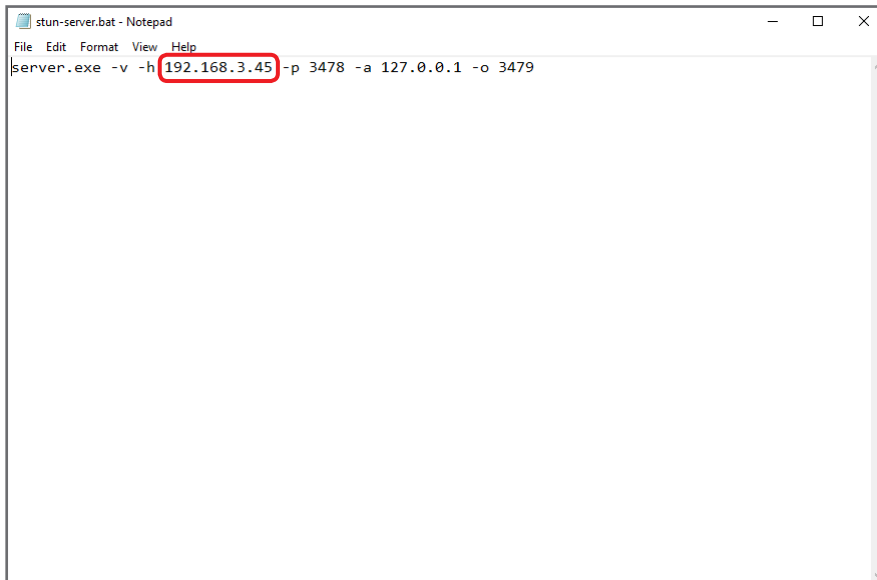
## Setting the STUN server environment

Set the STUN server environment.

### 1 Open the “C:\inetpub\B2BCameraLiveConnect\stun” folder, and modify “stun-server.bat” using a text editor.

Open a text editor by selecting “Run as administrator”, and modify “stun-server.bat”.

- Location to modify: 192.168.3.45  
Replace “192.168.3.45” with the IP address to be used in the connect server.  
When editing, never change the address of “127.0.0.1”.



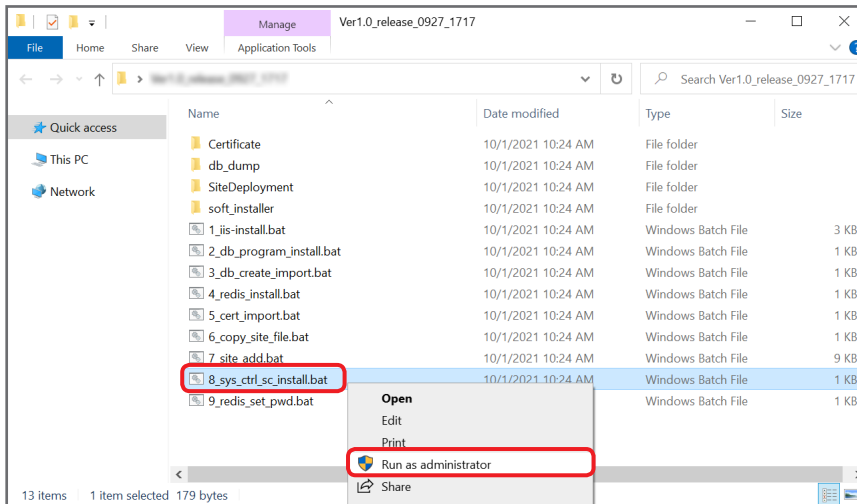
```
stun-server.bat - Notepad
File Edit Format View Help
server.exe -v -h 192.168.3.45 -p 3478 -a 127.0.0.1 -o 3479
```

## Installing the server control service

Install the server control service.

### Installing the server control service

- 1 Right-click “8\_sys\_ctrl\_sc\_install.bat” among the downloaded files, and select [Run as administrator].

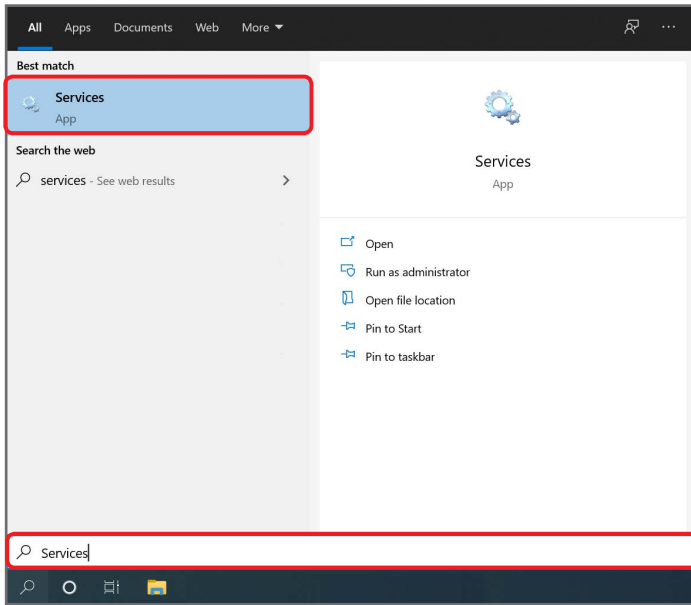


The command prompt window will appear.

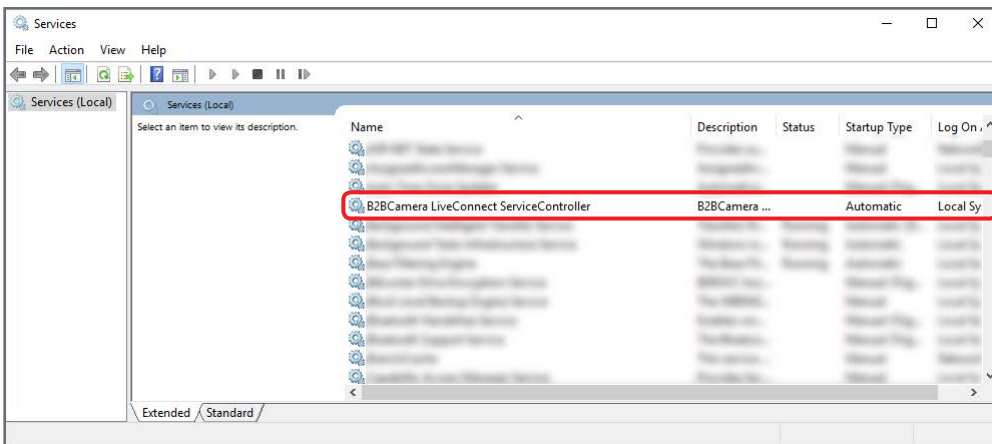
When “Press any key to continue...” is displayed, press a key, and close the window.

## Confirming installation of the server control service

1 Enter “Services” in the Windows search box, and click the appropriate search result.

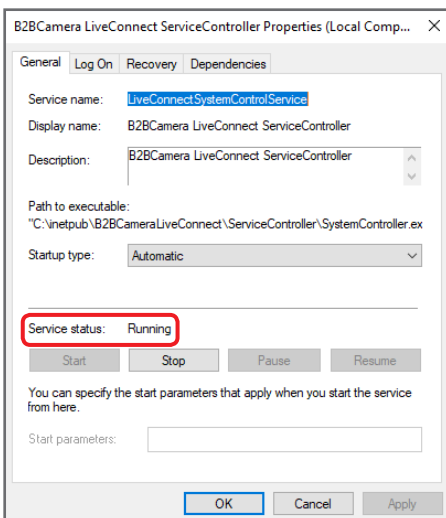


2 Double-click “B2BCamera LiveConnect ServiceController”.



3 Check that the service is “Running”.

If the service is “Stopped”, click [Start].



### Note

- After completing step 3, perform the steps described in “Logging in to the kitting site” (→46) to confirm that you can log in to the site.

## Activation

Activate this application on the kitting site.

### Logging in to the kitting site

#### 1 Enter the URL of the kitting site in the address bar of the web browser.

- URL: `https://***/kitting`  
 Replace “\*\*\*” with the IP address to be used in the connect server.  
 When specifying other ports than “443” in step 3 in “Creating the site for the LiveConnect server” (→32), enter “:” followed by the port number after the IP address.

#### Note

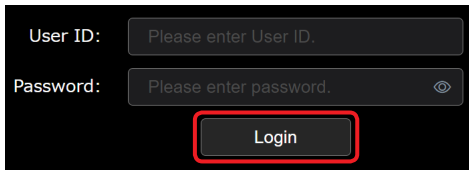
- If a warning message is displayed, select “Advanced” → “Proceed to \*\*\* (unsafe)”.  
 The IP address to be used in the connect server is represented by “\*\*\*”.

#### 2 Enter the user ID and password, and click [Login].

The password is displayed as a series of dots (●).  
 To log in to the site for the first time, use the following user ID and password.



- Initial user ID: panasonic
- Initial password: Panasonic123

After the initial login, change the user ID and password for the kitting account according to “Setting the servers” (→47).



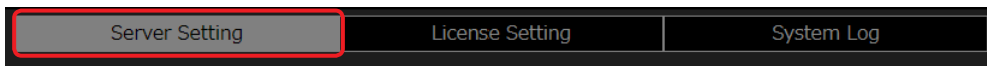
The screenshot shows a login form with two input fields and a button. The first field is labeled 'User ID:' and contains the placeholder text 'Please enter User ID.'. The second field is labeled 'Password:' and contains the placeholder text 'Please enter password.' with a small eye icon to its right. Below the fields is a button labeled 'Login' which is highlighted with a red rectangular border.

#### Note

- To log out, click  in the top right of the window to display the pull-down menu, and select [Logout].
- Click  in the top right of the window to view this application's User Guide (this document), and/or check the license information.

## Setting the servers

### 1 Click [Server Setting] on the menu bar.



### 2 Enter LiveConnect server information, and click [Apply].

Items marked with \* need to be entered.

#### ① [Company Name]:

The name of the company, organization, etc.

#### ② [User ID]:

The user ID used to log in to the kitting site

- Four types of characters can be entered: uppercase / lowercase alphabetic characters, numeric characters, and symbols (~!@#%\$%^&\*()\_+¥}{[<>./?' ).
- Enter using between 8 and 16 characters.

#### ③ [New password]/[Confirm new password]:

The password used to log in to the kitting site

- Enter the same password twice.
- Four types of characters can be entered: uppercase / lowercase alphabetic characters, numeric characters, and symbols (~!@#%\$%^&\*()\_+¥}{[<>./?' ).
- The password must contain at least three of the above four types of characters.
- Enter using between 8 and 16 characters.

#### ④ [Language]:

Language setting (Select from pull-down menu.)

- If you have changed the language setting, the new setting will be enabled after logging out and logging in again.

#### ⑤ [User ID]:

The user ID with administrator privileges used to log in to the portal site

- Four types of characters may be entered: uppercase / lowercase alphabetic characters, numeric characters, and symbols (~!@#%\$%^&\*()\_+¥}{[<>./?' ).
- Enter using between 8 and 16 characters.

#### ⑥ [Last Name]:

The last name of the user

- Enter using between 1 and 20 characters.

#### ⑦ [First Name]:

The first name of the user

- Enter using between 1 and 20 characters.

## ⑧ [Password]/[Password confirm]:

The password used to log in to the portal site, with administrator privileges.

- Enter the same password twice.
- Four types of characters may be entered: uppercase / lowercase alphabetic characters, numeric characters, and symbols (~!@#\$\$%^&\*()\_+¥|}{[<>./?'').
- The password must contain at least three of the above four types of characters.
- Enter using between 8 and 16 characters.

### 3 Enter the port number for the M2M relay server, STUN server, and storage server, then click [Apply].

The port numbers for each server are listed below.

Item	Usable range	Default value
<b>M2M relay server</b>	Any usable port between 1025 and 65535	44301
<b>STUN server</b>	Any usable port between 1025 and 65534	3478
<b>Storage server</b>	Any usable port between 1025 and 65535	2000

#### Note

- When changing the port number to other than the default value, make sure to assign a number that has not been used by other servers.
- Only numeric characters can be entered.

Operation monitoring is as follows:

Status	Description	[Start] button*1	[Stop] button*2
<b>Running</b>	The server is running.	Disabled	Enabled
<b>Stopped</b>	The server is stopped.	Enabled	Disabled

\*1 Click the [Start] button to start the server.

\*2 Click the [Stop] button to shut down the server. However, since this may cause problems, do not click the [Stop] button during normal operation.

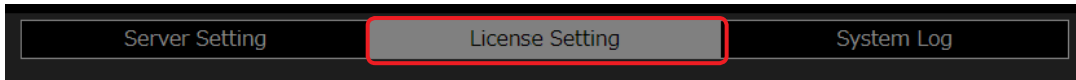


## License registration and activation

In order to use this application, it is necessary to purchase a key code, and complete the license registration procedure (activation).

**1** Insert an SD card into the computer on which this application is installed.

**2** On the menu bar of the kitting site, click [License Setting].



**3** Select the license you have purchased from the pull-down menu, and click [Save].



“SERIAL.LST” will be downloaded. Save it in the SD card.

Do not change the filename.

**4** Prepare a computer connected to the Internet, insert the SD card used in step 3, and access the following URL.

- URL: [https://panasonic.biz/cns/sav/actkey\\_e](https://panasonic.biz/cns/sav/actkey_e)

**5** On the page that is displayed, click the link for obtaining a software key.

**6** Follow the instructions on the screen, and save the activation code to the SD card.

“ACTIVE.LST” will be downloaded. Save it in the SD card.

Do not change the filename.

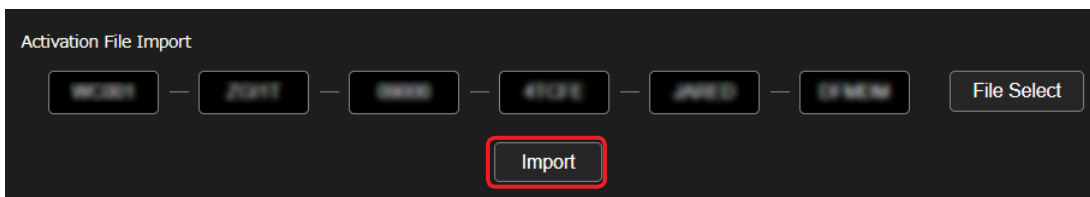
**7** Insert the SD card used in step 6 into the computer on which this application is installed.

**8** Return to the License Setting window on the kitting site. Click [File Select], and select “ACTIVE.LST” that has been saved in step 6.

Confirm that the code is input to [Activation File Import].



**9** Click [Import].



License information will be added to the license list.

This completes activation.

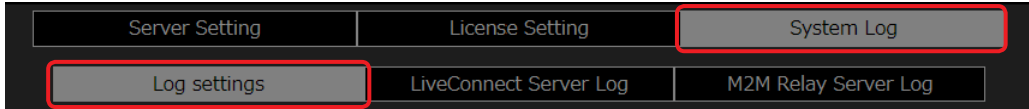
### Note

- Up to 10 licenses can be registered.

## Setting and downloading logs

### Setting logs

- 1 On the menu bar, click [System Log] followed by [Log settings].



- 2 Change the settings, and click [Apply].

Items marked with \* need to be entered.



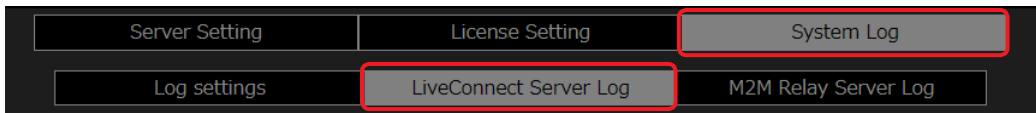
- ① **[Log file max]:**  
Specifies the upper limit on the number of log files created per day.
  - The setting range is between "10" and "100". (Default: 50)
- ② **[Log capacity limit]:**  
Specifies the upper limit on the size of log files.
  - The setting range is between "1" and "100" GB. (Default: 20)

#### Note

- When the log capacity reaches the upper limit, old log files will be deleted automatically, starting from the oldest, even if the number of log files has not reached the upper limit.
- The disk to be used to save log files requires 10 GB of free space in addition to the capacity to save the log. If 10 GB of free space cannot be secured, old log files will be deleted automatically, starting from the oldest.

## Downloading logs

- 1 Click [System Log] on the menu bar, and click [LiveConnect Server Log] or [M2M Relay Server Log].  
The procedure when [LiveConnect Server Log] is selected is described below.



- 2 Select the log you wish to download, and click [Download].

<input type="checkbox"/>	Log Date	Log Size	Download	Delete
<input checked="" type="checkbox"/>	20210917	13KB	↓ Download	🗑️ Delete
<input type="checkbox"/>	20210916	255B	↓ Download	🗑️ Delete

Total 2    20/page    < 1 >    Go to 1

### Note

- Selecting a log and clicking [Delete] will delete the log on that line.
- To download multiple logs collectively, select more than one log, and click [Download Sel].
- To delete multiple logs collectively, select more than one log, and click [Delete Sel].

## Chapter 3 Setup for Starting

---

This chapter describes setting items to be registered in this application.

## Registering users

The portal site is used to register and/or configure users and devices for LiveCast and Liveviewer.

### Logging in to the portal site

#### 1 Enter the following URL in the address bar of the web browser.

- URL: `https://***/portal`  
Replace “\*\*\*” with the IP address to be used in the connect server.

#### Note

- If a warning message is displayed, select “Advanced” → “Proceed to \*\*\* (unsafe)”.  
The IP address to be used in the connect server is represented by “\*\*\*”.

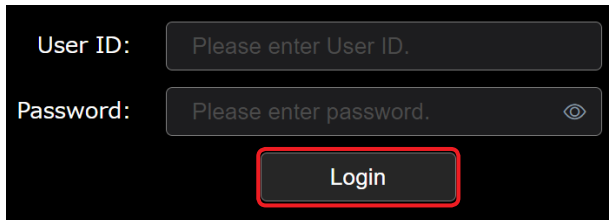
#### 2 Enter the user ID and password, and click [Login].

The password is displayed as a series of dots (●).

To log in to the portal site for the first time, enter the user ID and password with the admin account, which have been specified in “Setting the servers” (→47) for the kitting site.



After completing the procedure described in “Registering users” (→54), all users can log in with their own accounts.

If users have forgotten their passwords, contact a person who owns the admin account (hereinafter referred to as “administrator”). The administrator needs to reset their passwords (→54), and inform them of new passwords.



The screenshot shows a dark-themed login interface. It contains two input fields: 'User ID:' with a placeholder 'Please enter User ID.' and 'Password:' with a placeholder 'Please enter password.' and a toggle icon (an eye) to the right. Below these fields is a 'Login' button, which is highlighted with a red rectangular border.

#### Note

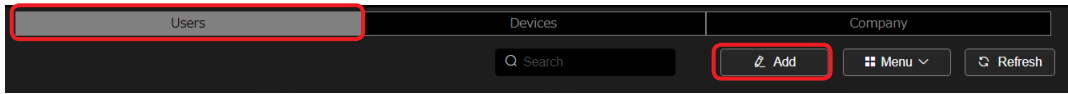
- To log out, click  in the top right of the window to display the pull-down menu, and select [Logout].
- Click  in the top right of the window to view this application's User Guide (this document), or check the license information.

## Registering users

Register new users.

New users can be registered only by administrators.

### 1 Click [Users] on the menu bar, and click [Add].



If you click a registered user (the background of the selected user changes to reddish brown) and click [Menu] to display the pull-down menu, you can enter settings for the following items.

Item	Setting
[Change Password]* <sup>*1</sup>	Changes the password.
[Edit]* <sup>*1</sup>	Edits the settings.
[Delete]* <sup>*1</sup> * <sup>*2</sup>	Deletes the registered account.

\*<sup>1</sup> Only administrators can reset other users' passwords and/or edit their settings.

\*<sup>2</sup> The account of a user who is currently logged in cannot be deleted.

#### Note

- When administrators have added new users, click [Refresh] to display the updated information.

### 2 Enter the user ID and other information, and click [Next].

Items marked with \* need to be entered.

#### ① [User ID]:

The user ID used to log in

- Four types of characters can be entered: uppercase / lowercase alphabetic characters, numeric characters, and symbols (~!@#\$\$%^&\*()\_+¥}{[<>./?').
- Enter using between 8 and 16 characters.

#### ② [Password]:

The password used to log in

- Enter the same password twice.
- Four types of characters can be entered: uppercase / lowercase alphabetic characters, numeric characters, and symbols (~!@#\$\$%^&\*()\_+¥}{[<>./?').
- The password must contain at least three of the above four types of characters.
- Enter using between 8 and 16 characters.

#### ③ [Last Name]:

The last name of the user

- Enter using between 1 and 20 characters.

#### ④ [First Name]:

The first name of the user

- Enter using between 1 and 20 characters.

#### ⑤ [Language]:

Language setting (Select from pull-down menu.)

#### Note

- A message saying "User ID already exists" may appear even if there is no account already registered with the same username. If this happens, try using a different user ID.

**3 Check that the information to be registered is correct, and click [Add].**

A message saying “User registration is complete.” is displayed.

When you edit the information of a registered user, [Apply] will be displayed, instead of [Add].

**4 Click [OK].**

The first and last names and the user ID of the newly registered user will appear on the list of users screen.

**Note**

- Click [Company] on the menu bar to change the company name or language setting.

## Chapter 4 Device Management

---

This chapter describes configuration of device settings.



## Configuring and confirming device settings

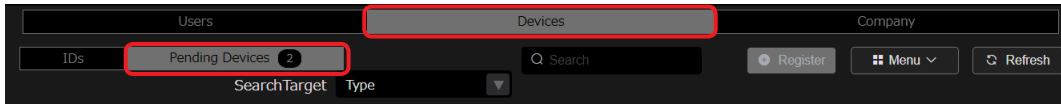
### Approving device registration requests

When this application receives a registration request from LiveCast or Liveviewer, a number other than 0 appears next to [Pending Devices] under device management.

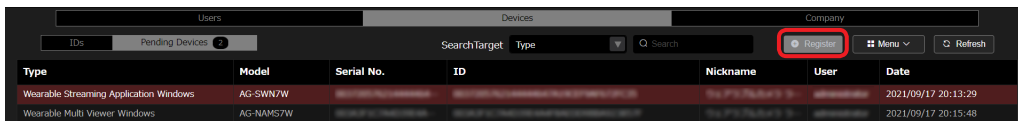
**Preparation: Perform the procedure described in “Logging in to the portal site” (→53).**

#### 1 Click [Devices] on the menu bar, and click [Pending Devices].

The number shown next to [Pending Devices] indicates the number of devices that have not been registered yet. (If the number is 99 or more, 99+ is displayed.)



#### 2 Select the device you wish to register, and click [Register].



#### Note

- To delete pending devices, click [Menu] to display the pull-down menu, and click [Delete].

#### 3 Confirm the registration details, and click [Apply].

Device registration will be complete.  
(Only [Nickname] can be changed.)

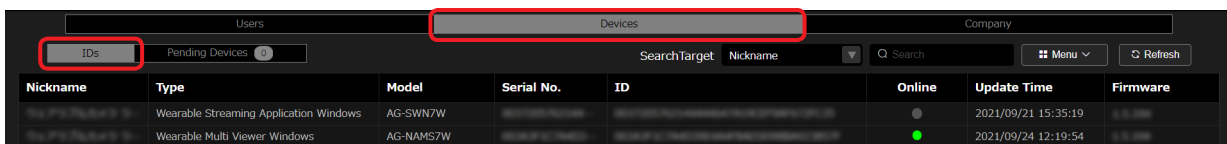
### Checking the status of devices

Information on registered devices can be checked on this application.

#### 1 Click [Devices] on the menu bar, and click [ID].

The devices registered in “Approving device registration requests” (→57) are displayed.

An indicator ● (green) is displayed under [Online] for devices that are currently connected.



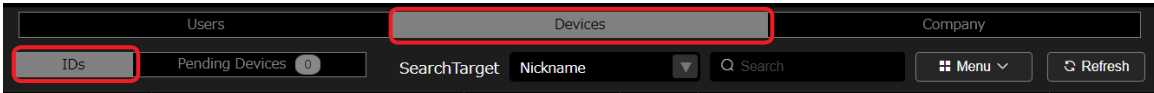
#### Note

- Even if a device becomes disconnected from this application, it may take some time for the [Online] indicator to update.

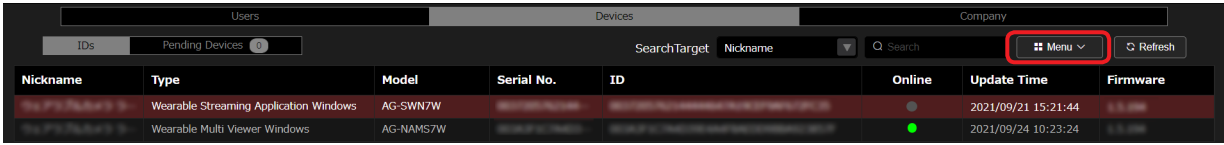
## Changing and deleting device settings

Registered devices can be deleted, and/or their nicknames can be changed.

- 1 Click [Devices] on the menu bar, and click [ID].



- 2 Select a device you want to delete or change its setting, and click [Menu].



Select either of the following items from the pull-down menu, and execute.

Item	Setting
[Edit]	Edits the nickname.
[Delete]	Deletes the registered device.

