Panasonic

# Quick Reference Guide
# Communication Assistant Server

Model No. KX-NCP Series
KX-TDE Series

Thank you for purchasing this Panasonic product.
Please read this manual carefully before using this product and save this manual for future use.

In this manual, the suffix of each model number is omitted (e.g., KX-NCP500**NE**).

# Introduction

Communication Assistant (CA) Server is a program to manage users and the operation of CA Client. CA Web Manager is a web client used to control CA Server settings from any computer on the PBX's network.

### About the Quick Reference Guide

This Quick Reference Guide is designed to serve as an overview of the features, setup and installation of CA Server and CA Web Manager.

The Quick Reference Guide is divided into the following sections:

**1 Specifications**

This section provides general information about the features in CA Server and CA Web Manager.

**2 System Connection Diagram**

This section shows how CA Server fits into your network.

**3 System Requirements**

This section provides the minimum and recommended system requirements for installing CA Server on a PC.

**4 Starting CA Server**

This section explains how to install and uninstall CA Server, and how to start CA Web Manager.

### IMPORTANT

CA Server stores personal information. In order to prevent data theft and leakage, we recommend the following:

- Set a password-protected screensaver to activate after your computer has been idle for a set amount of time.
- Use Windows Update to keep your system up-to-date with the latest software patches.
- Carefully manage access to the CA Server computer, and install a firewall to prevent unauthorised access from the internet.
- Whenever possible, use SSL or other forms of secure data communication.
- Set a login password that is at least 5 characters long, and contains a combination of letters and numbers.
- Periodically change all login passwords to prevent unauthorised access by third parties.
- Set a password as soon as possible after CA Server is installed. Ensure a password is always set; if the password is reset for any reason, set the new password immediately.
- Make regular backups of program databases and store them securely in a different location. Record any settings information should you need to re-install CA Server, and store it securely.
- Care should be taken when sending e-mail via program features. Specifying an incorrect e-mail address may result in the transmission of personal information to an unauthorised party. When e-mail settings are made, send a test e-mail to confirm the settings are correct.
- Restrict access to CA Server and CA Web Manager to designated administrators. Whenever possible, do not install or run unnecessary programs on the computer used to run CA Server.
- When using an external authorisation server, periodically check to make sure all security certificates are valid and up-to-date.
- When users change extensions, desks, etc., make sure that the access rights for their previous and new extensions and computers are correct.
- When having the computer serviced, use only authorised technicians, and before servicing, password protect or encrypt access to database files.
- When the computer used for CA Server is transferred, disposed of, or taken out of service, ensure all sensitive data is securely erased.

### Trademarks:

- Microsoft, Windows, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

- Intel, Celeron and Pentium are trademarks of Intel Corporation in the U.S. and other countries.
- All other trademarks identified herein are the property of their respective owners.
- Microsoft product screen shots reprinted with permission from Microsoft Corporation.

**Notice**

- The use of this Software may be limited under the terms of the licence agreement for your system. Please confirm the terms of your licence before using this Software.
- This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)
  This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
  This product includes software written by Tim Hudson (tjh@cryptsoft.com).

# Table of Contents

# 1 Specifications

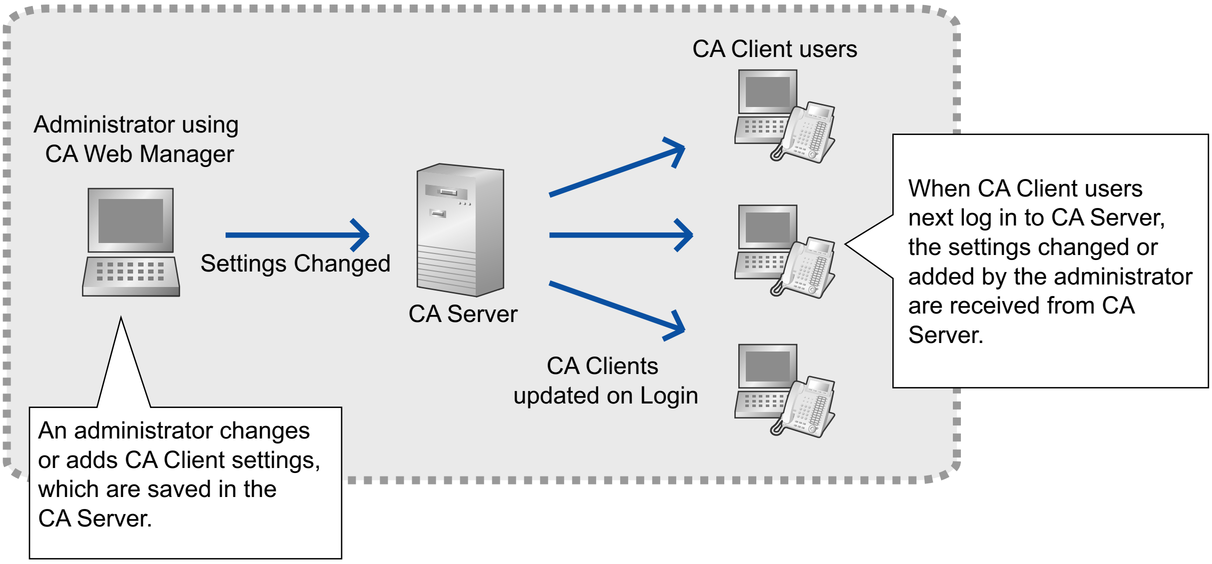
## 1.1 Overview

### The functionality of CA Server

CA Server is an application that is installed on a computer on your PBX's network. When CA Client users log in to the CA Server (instead of directly to the PBX), the following functions become available:

- The maximum number of simultaneous CA Client users is increased. For more information on the number of simultaneous CA Client users, see "Login Capabilities" in the CA Client Quick Reference Guide.
- A CA Client user's available contacts can be restricted based on their presence settings. For example, when the "Out of Office" presence is used, only a cellular phone will be available to be called by other CA Client users.
  For more information on this feature, see "Restricting Contacts by Presence" in the CA Client Quick Reference Guide.
- Missed calls made to logged off CA Client users are recorded by CA Server. The missed call information is sent to the CA Client user’s call history when they next log in to CA Server.
- Settings for CA Client users (e.g. extension user information, dial modification settings, etc.) can be edited by an administrator using CA Web Manager, a Web client program for CA Server. Settings are updated for each CA Client user when they log in to CA Server.

**Example: Updating user settings with CA Server**


CA Client users
Administrator using CA Web Manager
Settings Changed
CA Server
CA Clients updated on Login

When CA Client users next log in to CA Server, the settings changed or added by the administrator are received from CA Server.

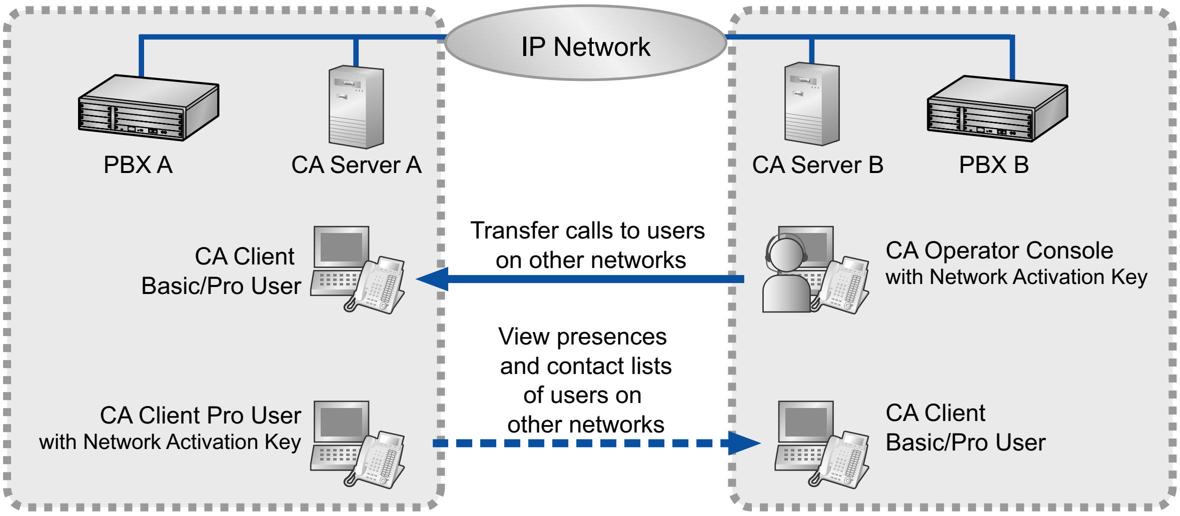
An administrator changes or adds CA Client settings, which are saved in the CA Server.

For more information about CA Client features, see the CA Client Quick Reference Guide.

### Network Features

When CA Server is also installed on another PBX's network, CA Client users can view the presence of CA Client users of that network. After viewing the presence of a CA Client user on another network, it is possible to make calls, transfer calls, and initiate chat with that user. A network activation key and CA Pro activation key are required to use these network features.

### Example of CA Server Network Features

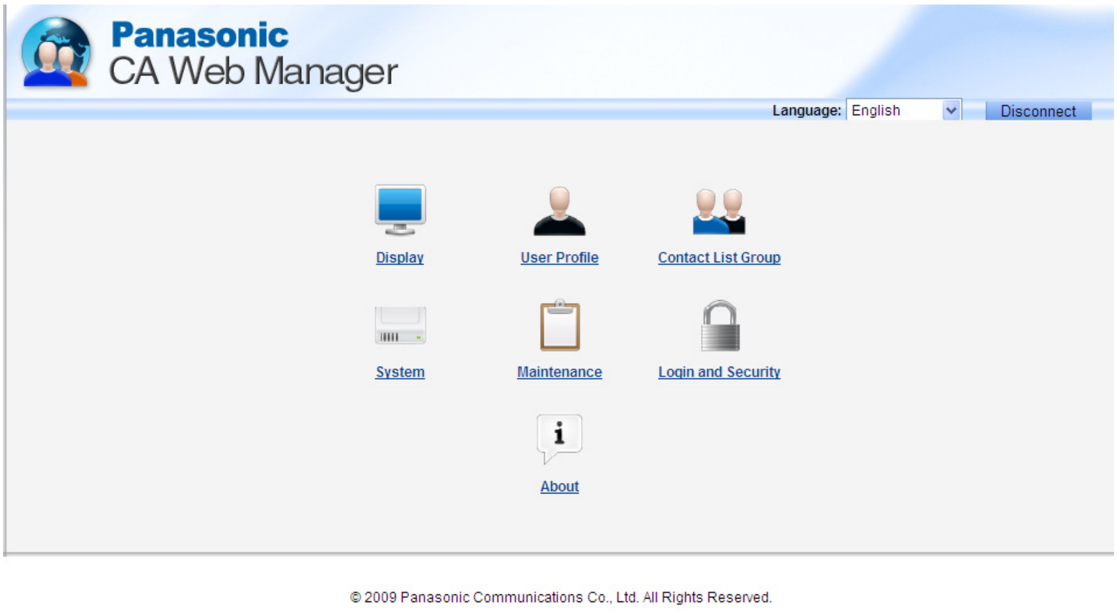


### PBX System Alarm Notification by E-mail

In the event of a PBX system alarm, CA Server will send an e-mail containing the alarm information to a specified e-mail address.

# 1.2 CA Web Manager Features

All CA Server functions are controlled through CA Web Manager, a client program that can be accessed by a networked computer's web browser once CA Server is installed. For information on how to access CA Web Manager, see **4.2 Starting CA Web Manager**. After you enter the login password, the main menu appears. From this menu, you can access the features of CA Web Manager.



© 2009 Panasonic Communications Co., Ltd. All Rights Reserved.

### Display

You can load different language files for use with CA Web Manager.

## User Profile

You can set user profile information for PBX extensions. Contact information, voice mail settings, and CA Client function settings for each extension can be set. User information can be imported from or exported to a CSV file.

**Note**

If a CA Client user's login password becomes locked, they will not be able to log in to CA Server until the password lock is cleared.
To clear a locked password, check the box next to the locked user's extension number on the User Profile screen, and click **Clear Password**.

## Contact List Group

You can set the names of Contact List Groups. Once set, a Contact List Group can be added in user profiles to organise users into groups, for example by office or by department.

## System

- **Preference Setting**
  You can enable/disable profile editing by users and set the number of times a password can be incorrectly entered before the password becomes locked.
- **VM Setting**
  You can set IP addresses of voice mail systems for CA Client users.
- **Dial Modification**
  You can set dial modification for dialled phone numbers, such as adding to or removing dialled digits.
- **LDAP Setting**
  You can set the server, account name and password of an LDAP directory service.
- **Network Setting**
  You can set network information for the main CA Server and other networked CA Servers.

## Maintenance

- **PBX System Alarm**
  You can enable/disable PBX System Alarm notifications by e-mail, as well as set the e-mail address and e-mail subject line.
- **CA Server Alarm**
  You can enable/disable CA Server log notifications by e-mail. You can set the frequency and time logs are sent, and the e-mail address and subject line used.
- **SMTP Setting**
  You can set SMTP server information for the sending of e-mails by various CA Server features.
- **Backup Database**
  You can set the frequency, schedule, and save location of CA Server database backups, as well as the maximum number of backups to store before older backups are overwritten.
- **Restore Database**
  You can restore a database backup from the default location or from a specific folder.
- **Activation Key (For KX-TDE Series PBXs only)**
  CA Client (Basic, Pro, Supervisor, and Operator Console), and CA network activation key registration information is displayed.

## Login and Security

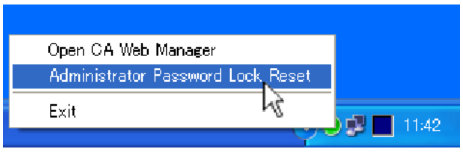
You can change the current CA Web Manager login password.

## About

Provides information about the current installation of CA Server.

## Conditions

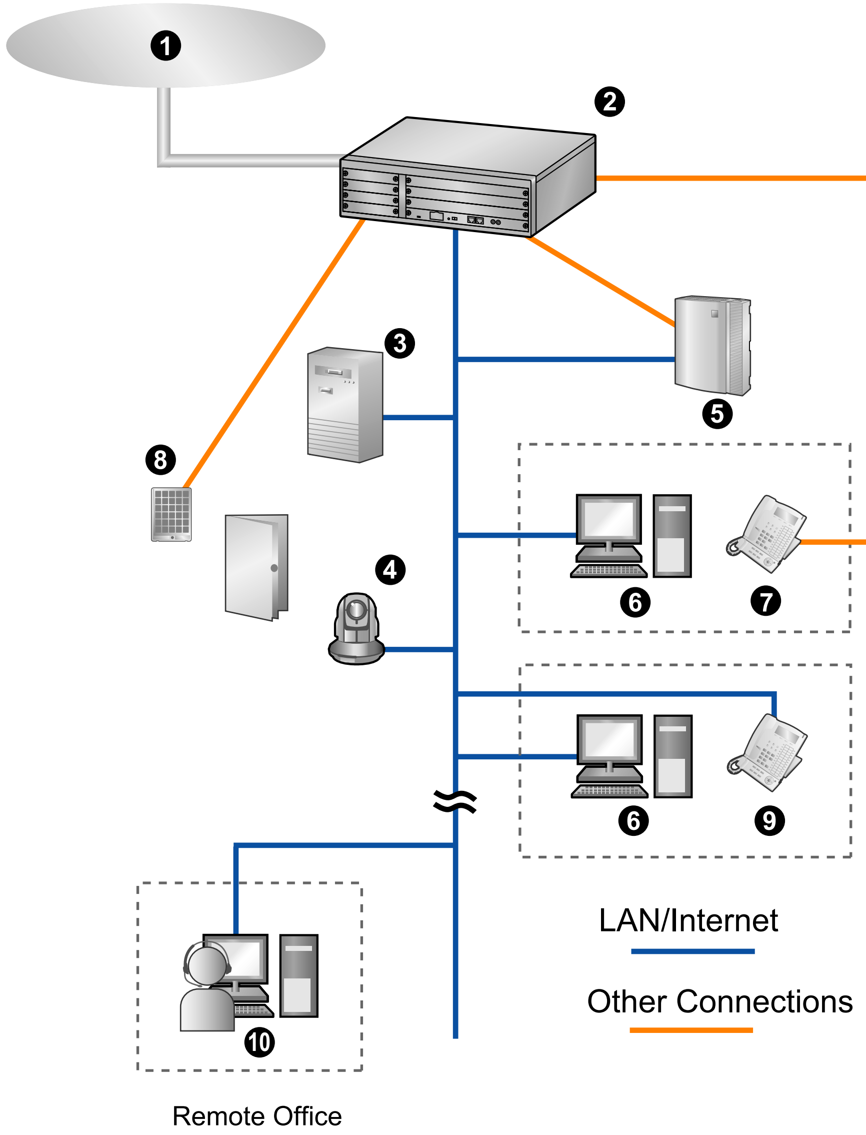
- CA Client users can use CA Server features only when the computer installed with CA Server is turned on and the CA Server program is running.
- When running, CA Server prevents computer shutdown procedures. The computer running CA Server cannot be shut down until the CA Server program is terminated.
- For security reasons, CA Web Manager will automatically log off after 5 minutes of inactivity.
- When logging in to CA Web Manager, if you enter the wrong password a pre-programmed number of times, the CA Server Web Manager password will be locked.
  If the CA Web Manager administrator password becomes locked, it can by reset from the CA Server, through the CA Server options menu. Right-click on the CA Server icon in the task tray and choose **Administrator Password Lock Reset**.

  This will reset the CA Web Manager administrator password. CA Web Manager will automatically launch to the Login and Security screen, where you can specify a new password.

# 2 System Connection Diagram

The figure below illustrates an example network setup using CA Server.



1. Telephone Company
2. Panasonic PBX
3. CA Server
4. Panasonic Network Camera
5. Voice Processing System
6. PC running CA Client
7. Proprietary Telephone or Single Line Telephone
8. Doorphone and Door Opener
9. IP Proprietary Telephone
10. PC running CA Client with Softphone

# 3 System Requirements

The tables below summarise the minimum and recommended requirements for running CA Server.

## PC

| | Minimum | Recommended |
|---|---|---|
| **CPU** | 1.0 GHz Intel® Pentium®/Celeron® processor or comparable CPU | 3.2 GHz Intel Pentium 4 or comparable CPU |
| **RAM** | 1024 MB | 2048 MB |
| **OS** | Microsoft® Windows® XP Professional Service Pack 2 or later<br>Windows Vista® Business | Microsoft Windows XP Professional Service Pack 2 or later<br>Windows Vista Business<br>Windows Server® 2003 Standard Edition<br>Windows Server 2008 Standard Edition |
| **Hard Disk** | 1.5 GB available space | 10 GB or more available space |
| **Video Resolution** | 1024 × 768 | 1280 × 1024 |
| **Interface** | 10Base-T | 10/100Base-T |

## PBX

To use CA Server, your PBX must have the correct software file version installed. Confirm your PBX matches the requirements listed below.

| PBX Model | Required Software File Version |
|---|---|
| KX-NCP500/KX-NCP1000 | PBMPR Software File Version 2.0000 or later |
| KX-TDE100/KX-TDE200 | PMMPR Software File Version 2.0100 or later[*1] |
| KX-TDE600 | PGMPR Software File Version 2.0000 or later[*1] |

[*1] The PBX's Activation Key for Software Upgrade to Enhanced Version (KX-NCS4910/KX-NCS4950) is also required. Without the activation key, calls put on hold to transfer cannot be retrieved.

## Activation Keys

Activation keys are files that need to be registered to your PBX with the PC Maintenance Console. For details on how to install activation keys, refer to your PBX's Installation Manual.
For a CA Client user to use thin client and network features with CA Server, the following activation keys are required:

| Model No. | Activation Key Type | Description |
|---|---|---|
| KX-NCS2010 | CA Thin Client | Allows the use of CA Client in a thin-client environment. |
| KX-NCS2901 | CA Network 1user | Allows the use of CA Server network features for 1 user. |
| KX-NCS2905 | CA Network 5users | Allows the use of CA Server network features for 5 users. |

| Model No. | Activation Key Type | Description |
|---|---|---|
| KX-NCS2910 | CA Network 10users | Allows the use of CA Server network features for 10 users. |
| KX-NCS2940 | CA Network 40users | Allows the use of CA Server network features for 40 users. |
| KX-NCS2949 | CA Network 128users | Allows the use of CA Server network features for 128 users. |

### CAUTION

The activation key file can only be installed in the PBX with the MPR ID number entered when the activation key file was downloaded. The activation key file cannot be reissued unless the MPR card crashes.

# 4 Starting CA Server

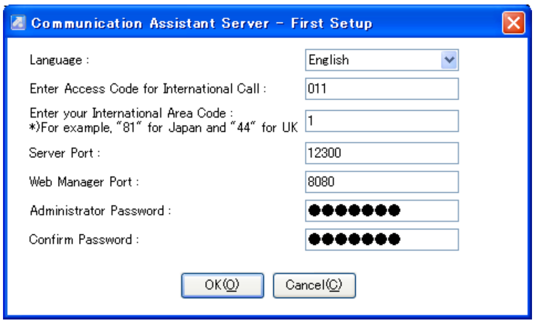
## 4.1 Installing CA Server

1. Double-click "Setup.exe", and follow the on-screen guidance to install CA Server.

   **Note**

   You can choose to install CA Server in "Windows service mode", or in "executable mode". If you choose "Windows service mode", CA Server will launch automatically each time the computer is started. If you choose "executable mode", you must manually launch CA Server from the Start menu each time the computer is started.

2. When installation is complete, CA Server starts, and the setup screen is displayed:



Communication Assistant Server - First Setup

Language : English

Enter Access Code for International Call : 011

Enter your International Area Code :
*)For example, "81" for Japan and "44" for UK 1

Server Port : 12300

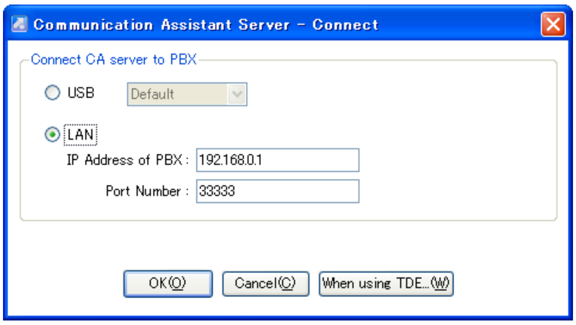
Web Manager Port : 8080

Administrator Password : ●●●●●●●

Confirm Password : ●●●●●●●

   Set your language, dialling codes for your country/area, port numbers to be used by CA Server and by CA Web Manager, enter and verify the Administrator password, and click **OK**. You must enter a country/area code to proceed.

3. The PBX settings screen is displayed:



Communication Assistant Server - Connect

Connect CA server to PBX

○ USB Default

● LAN

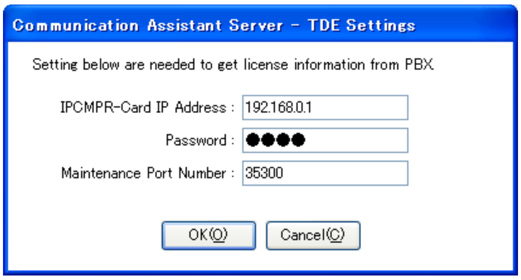
IP Address of PBX : 192.168.0.1

Port Number : 33333

   Choose a USB or LAN connection to the PBX. If using a LAN connection, specify the IP address and port number of the PBX on your network and click **OK**.

**Note**

When using a KX-TDE Series PBX, you must also click **When using TDE...**:



Communication Assistant Server - TDE Settings

Setting below are needed to get license information from PBX

IPCMPR-Card IP Address : 192.168.0.1

Password : ●●●●

Maintenance Port Number : 35300

Enter the IP address of the PBX's IPCMPR card, the PBX's administrator password (the same password used to log on to the Maintenance Console), and the Maintenance Console's Port Number. Click **OK**.

Once these settings are made, they are saved, and each time CA Server starts it will automatically attempt to connect to the PBX if no setting changes are made.

## CA Server Status

Once CA Server is running on your computer, an icon will appear on the computer's task tray.

🟢

Hovering your mouse over the icon will display a status message for CA Server. The icon will also turn red if there is an error, or if CA Server is not functioning properly.

🔴

Right-clicking the icon brings up a menu where you can reset the administrator password, open CA Web Manager, or terminate the CA Server program.

## Updating CA Server

It is important to always use the latest version of CA Server to ensure all features work properly. Contact your dealer for more information.

# 4.2 Starting CA Web Manager

### When using a computer other than the computer running CA Server

1. Start a web browser program.
2. In the browser's address bar, enter the CA Server's IP address and port number for CA Web Manager using the following format:
   http://[IP address of the computer running CA Server]:[Web manager port number specified in CA Server setup]
   For example, if the IP address of the computer running CA Server is [101.155.0.1] and the specified Web manager port number is [8080], the address entered would be the following:
   http://101.155.0.01:8080
   If you are unsure of the IP address of the computer running CA Server, contact your network's administrator.

### When using the computer running CA Server

There are three methods:

- – Double-click the CA Server icon in your computer’s task tray.
- – Right-click the CA Server task bar icon and choose **Open CA Web Manager**.
- – Manually enter the CA Web Manager address into your Web browser, as outlined above.

### Logging on to CA Web Manager

Once you access CA Web Manager, a login prompt will appear. Enter the Administrator password and the main menu appears. From this menu, you can access the features of CA Web Manager.

## 4.3 Uninstalling CA Server

1. To uninstall CA Server, perform one of the following procedures:
   - From the **Start** menu, point to **All Programs** → **Panasonic** → **CA Server**, and select **Uninstall**.
   - From the Control Panel, double-click **Add or Remove Programs**, select **CA Server**, and then click **Remove**.

Panasonic Communications Co., Ltd.
1-62, 4-chome, Minoshima, Hakata-ku, Fukuoka 812-8531, Japan