Authentication
Access Control
Encryption
Certification

SSCom

User Guide

Hitachi Systems, Ltd.

Introduction

This manual describes the outline of SSCom and the operation method of SSCom Client. It also describes the manual that you need to refer to when using the SSCom.

■Target Readers

It is assumed that you are the following readers:

- Readers who want to have a remote access or access an Intranet by using SSCom Client.
- Readers who have a basic knowledge of Microsoft Windows.
- Readers who have a basic knowledge of the Internet.
- Readers who have a basic knowledge of network.

■Manual Structure

This manual is organized into the following chapters:

Chapter 1 Install/Uninstall

This chapter describes how to install and how to uninstall SSCom Client.

Chapter 2 How to Use

This chapter describes the operation method of SSCom Client.

Chapter 3 Configuration

This chapter describes the necessary environment settings to use SSCom Client.

Chapter 4 Message

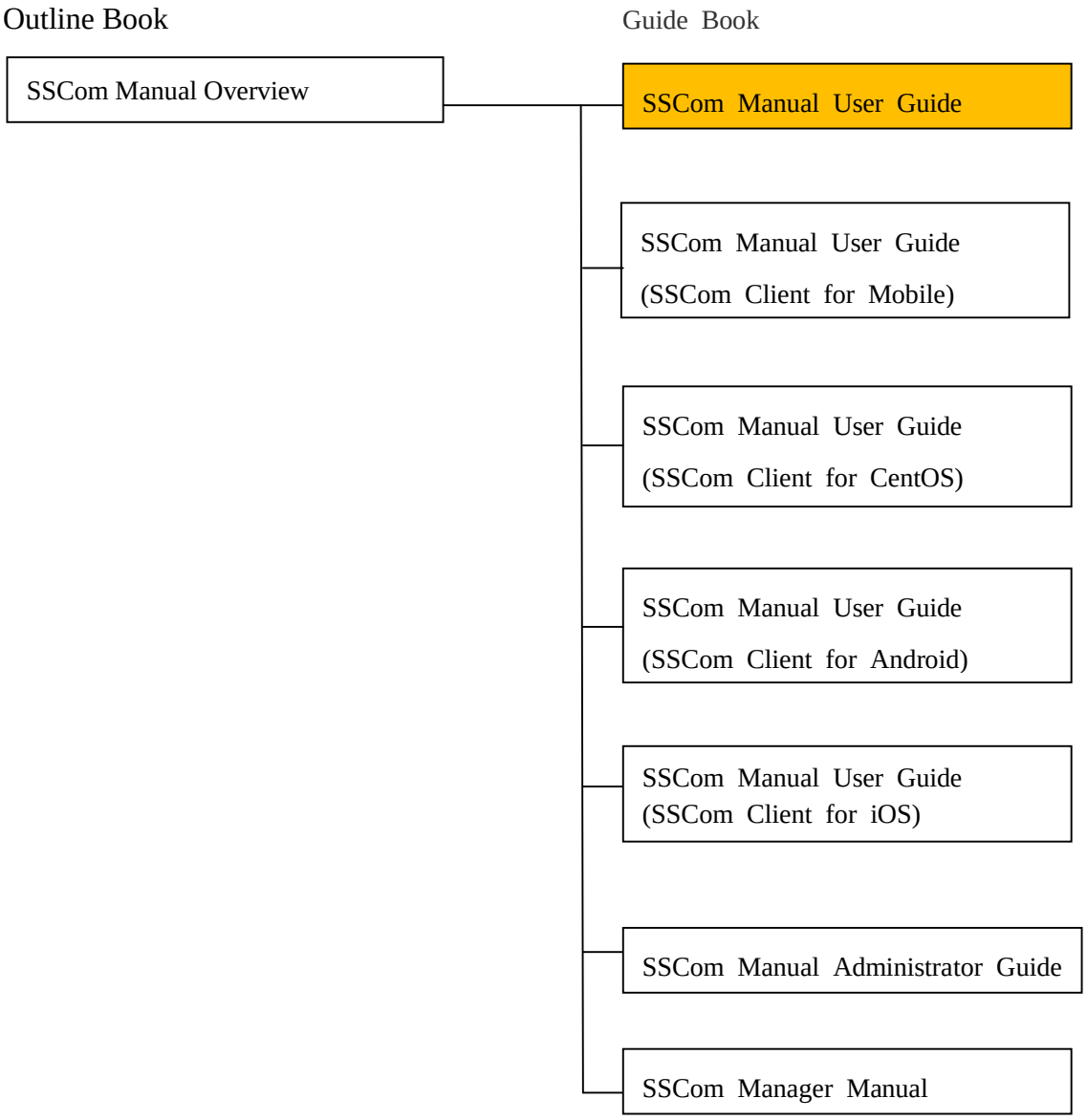
This chapter describes the messages displayed by SSCom Client.

Chapter 5 Troubleshooting

This chapter describes what to do when trouble occurs and how to get the log.

■Organization of the Manual

Organization of SSCom Product Manual is shown as follows:



#	Document Name	Classification	Summary
1	SSCom Manual Overview	Overview	Overview of SSCom.
2	SSCom Manual User Guide (this manual)	Guide Book	Describes installation and operation methods of SSCom Client for PC.
3	SSCom Manual User Guide (SSCom Client for Mobile)	Guide Book	Describes installation and operation methods of SSCom Client for Mobile.
4	SSCom Manual User Guide (SSCom Client for CentOS)	Guide Book	Describes installation and operation methods of SSCom Client for CentOS.
5	SSCom Manual User Guide (SSCom Client for Android)	Guide Book	Describes installation and operation methods of SSCom Client for Android.
6	SSCom Manual User Guide (SSCom Client for iOS)	Guide Book	Describes installation and operation methods of SSCom Client for iOS.
7	SSCom Manual Administrator Guide	Guide Book	Describes how to build remote access system by using SSCom.
8	SSCom Manager Manual	Guide Book	Describes the operation method of SSCom Manager.

■How to read

You can choose the relevant chapters to read by your purpose of using this manual. It is recommended that you refer to specific chapter by your purpose of use:

The Purpose of Reading	Relevant Chapter
Want to know how to install SSCom Client.	Chapter 1
Want to know how to uninstall SSCom Client.	Chapter 1
Want to know how to launch and stop SSCom Client.	Chapter 2
Want to know the Configuration of SSCom Client.	Chapter 3
Want to access Intranet from external network (VPN Function).	Chapter 2 & 3
Want to use Web Authentication Function.	Chapter 2 & 3
Want to inquiry error message of SSCom Client.	Chapter 4
Want to know what to do when trouble occurs.	Chapter 5

■Description of Guide Marks

In this manual, different guide mark is used according to the function. The following table shows the guide mark and its meaning:

Guide Mark	Description
	To know the settings and operation method of VPN Function, please read from here.
	To know the settings and operation method of Web authentication, please read from here.

■Description of Notations

Details of product name for notations used in this manual are shown in the following table:

Notations used in this Manual	Official Name
VPN Server	SSCom VPN Server
AP Server	SSCom AP Server
GAC Server	SSCom GAC Server
Windows 2003	Microsoft Windows Server 2003
Windows Vista	Microsoft Windows Vista
Windows 7	Microsoft Windows 7
Windows 8 / 8.1	Microsoft Windows 8 / 8.1
Windows 2008	Microsoft Windows Server 2008
Windows 2012	Microsoft Windows Server 2012
CentOS	CentOS 5.5 (x86)

Windows Vista, Windows 7, Windows 8 / 8.1 are collectively referred to as Windows in this manual.

Windows 2003, Windows 2008, Windows 2012 are collectively referred to as Windows Server in this manual.

Figures and instructions in this manual are for Windows Vista.

In case you are using Windows other than Windows Vista, these instructions shall be replaced as necessary.

■Description of Abbreviations

Details of abbreviations used in this manual are shown in the following table:

Abbreviation	Official Name
CA	Certificate Authority
DN	Distinguished Name
DNS	Domain Name System
HTTP	HyperText Transfer Protocol
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
URL	Uniform Resource Locator
VPN	Virtual Private Network

■Matters that need attention in export

The product is among the strategic materials and technology which meets all the stipulations of Foreign exchange and foreign trade law.

Please make sure related formalities be followed based on observing relevant laws when exporting the product (including bringing it to foreign countries from Japan, or presenting it to non-domestic residents).

If you have any questions, please contact the purchasing agency of this product.

■Trademark

All company names, brand names and product names recorded in this manual are registered trademark of each company.

■Attention

▪ This manual does not record any machinery products or program products required when using the software. If there is a need, please refer to other supporting manuals.

▪ This manual subjects to change without prior notice.

Table of Contents

1

1. Install/Uninstall

This chapter describes the way to install and set up SSCom Client.

<Chapter Structure>

1.1 Install SSCom Client

1.2 Uninstall SSCom Client

1.1 Install SSCom Client

Install SSCom Client by using the Setup Wizard.
If you install SSCom Client, please do the work as the administrator.

1.1.1 Work before Installation

Before installing SSCom Client, please confirm the following items:

- It cannot be installed on the same PC as the other server products, including SSCom Server.
- There is more than 20MB of disk free space.
- Please install the driver of the authentication device before installing SSCom Client.

1.1.2 Installation

1. Log in as an administrator to install SSCom Client.

2. Exit all other applications.

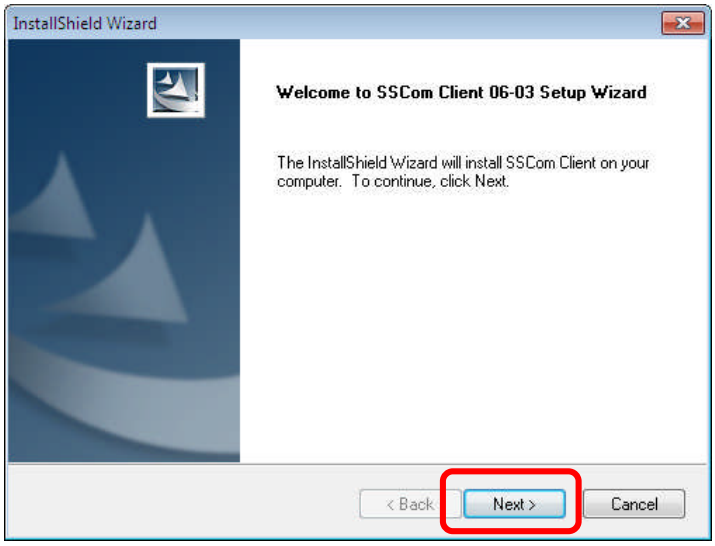
3. Please insert the CD-ROM disc of SSCom Client installer into the CD-ROM drive of your PC.

4. Select "Run…" in Windows Start Menu, and enter the name of the SSCom Client installer in the "Name" box, the Setup Wizard will be launched after you click on OK. Typically the installer, in the case of Virtual IC Card is "Setup.exe" under the "Client\Virtual IC Card" folder, in the case of eToken is "Setup.exe" under the "Client\eToken" folder in the CD ROM. For example, if the CD-ROM drive is drive E and client is Virtual IC Card version, please input "E:\Client\Virtual IC Card\Setup.exe".

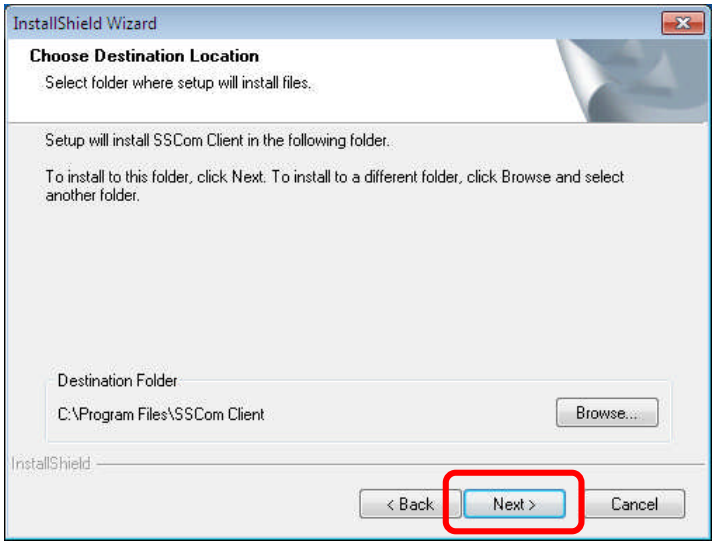
When the installer launched, please follow the directions of installer to finish the installation.

5. When the following dialog displays, click on "Next".

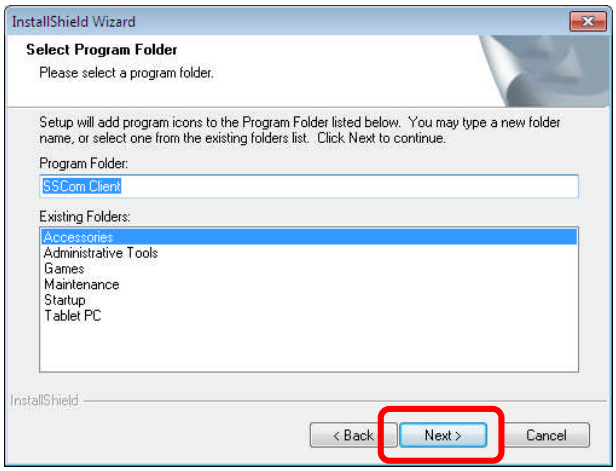
   * User Account Control dialog will be displayed before the Welcome page in Windows Vista, click on "Next" to upgrade privilege when it appears.



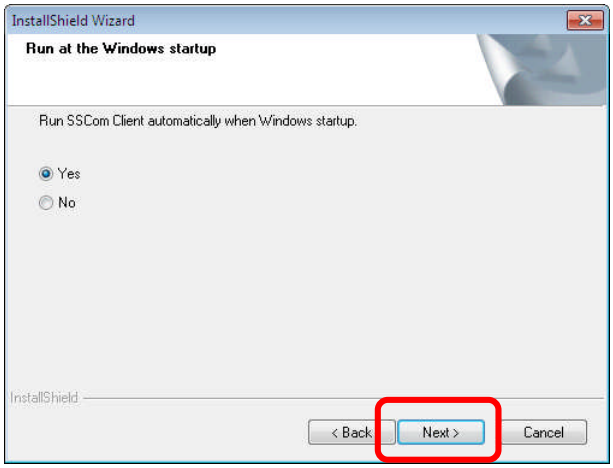
6. The next page will be displayed. After setting destination folder, click on "Next". If you need to change the default destination path, click browse to select the destination folder.



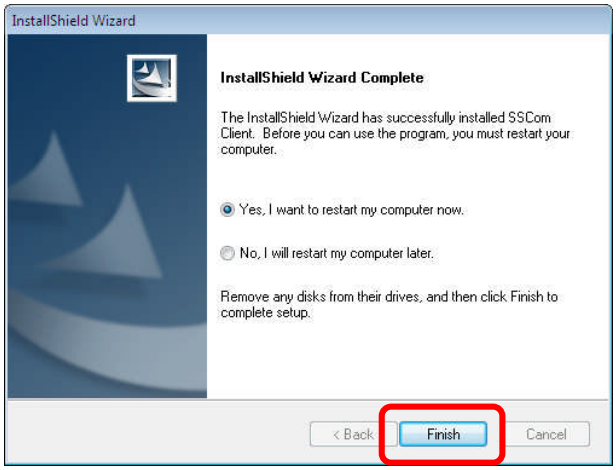
7. The next page will be displayed. Specify the program folder and click on "Next".



8. The next page will be displayed. If you need SSCom Client to automatically start at the Windows startup, select "Yes" and click on "Next".



9. The computer needs to be restarted after installation of SSCom Client completed. If you need to restart it immediately, choose "Yes, I want to restart my computer now." and click on "Finish".



1.2 Uninstall SSCom Client

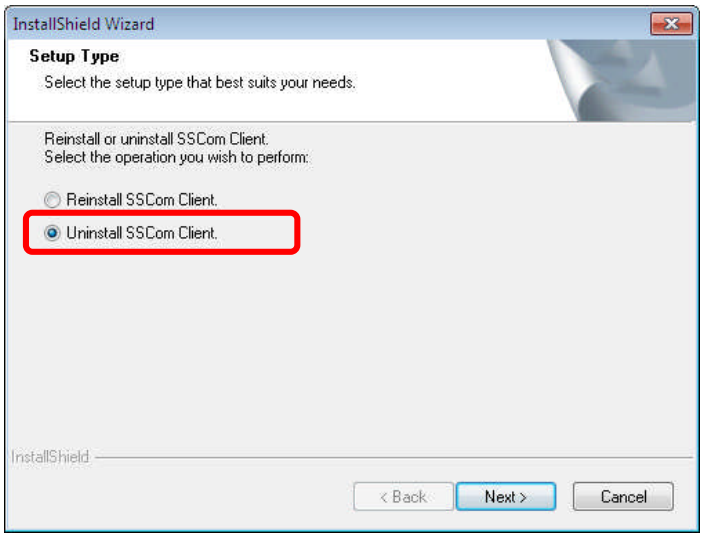
1. Open the control panel by "Settings" – "Control Panel" from Windows Start Menu.

2. Click "Uninstall a program", and the list of "Currently installed programs" will be displayed.

3. Select "SSCom Client" from the list of "Currently Installed Programs".

4. Click on "Change" button.

5. The next dialog will be displayed. Choose "SSCom Client Uninstall." to remove it.



This page is blank.

2

2. How to Use

This section describes how to use SSCom Client.

<Chapter Structure>

2.1 How to Launch

There are 2 following ways to launch SSCom Client:

(1) If you have selected auto-start SSCom Client at the Windows startup in installation process.
(If SSCom Client has been registered to Startup)

SSCom Client will automatically launch whenever you login Windows, the icon will appear in the task tray after it starts.

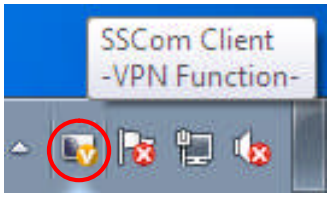


Fig.2.1-1 Start SSCom Client

Icons of SSCom Client vary according to different authentication settings, as shown below:

Table 2.1-1 Icons of SSCom Client shown in the task tray

Icon	Authentication Settings
	Use VPN Function
	Use Web Authentication Function
	Stop SSCom Function

(2) If auto-start SSCom Client at the Windows startup has not been selected in installation process.
(If SSCom Client has not been registered to Startup)

Select "SSCom Client" from "All Programs" - "SSCom Client" in the Windows Start Menu to launch it. The icon will be displayed in the task tray after it launched.

For Windows 8 **/ 8.1**, press "Windows Key" on the keyboard, right-click "Start screen", and click "All apps".

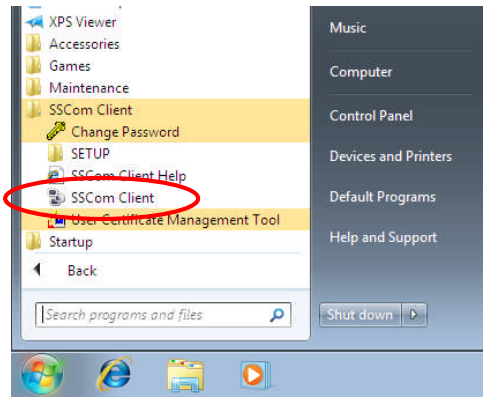


Fig.2.1-2 Launch SSCom Client from the Start Menu

2.2 How to Exit

The following steps need be done to exit SSCom Client:

1. Right-click the SSCom Client icon in the task tray to open the menu.

2. Click on "Exit" from the menu.

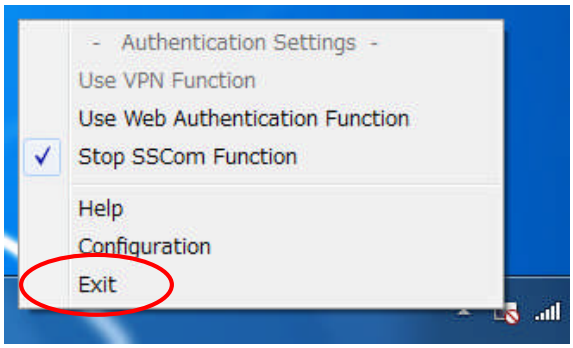


Fig.2.2-1 Exit SSCom Client

2.3 How to Check Authentication Settings

The authentication settings in use can be checked through the following way:

(1) Check from the task tray

Icon of SSCom Client varies in the task tray according to different authentication settings.

Move mouse cursor on the icon in the task tray, the tooltip also shows the authentication setting.

Table 2.3-1 Icons of SSCom Client shown in the task tray

Icon	Tooltip	Authentication Settings
	VPN Function	Use VPN Function
	Web Authentication	Use Web Authentication Function
	Stopped	Stop SSCom Function

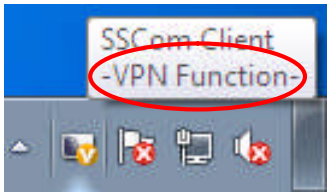


Fig.2.3-1 Check by the tooltip

(2) Check from the Menu

Right-click the SSCom Client icon in the task tray to open the Menu, the item been checked shows the authentication setting in use.

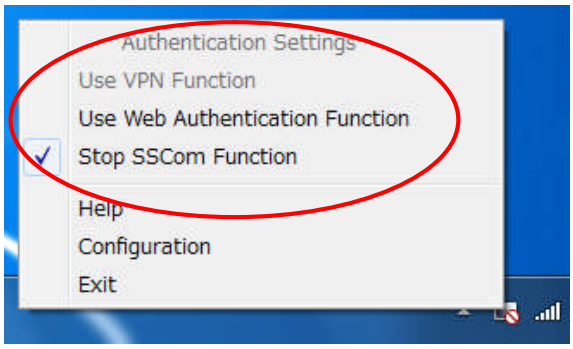


Fig.2.3-2 Check by menu

2.4 How to Modify Authentication Settings

1. Right-click the SSCom Client icon in the task tray to open the menu.

2. Click the desired authentication setting in the menu.
Checkmark shows on to the left edge of the settings menu you clicked and the authentication setting will be changed.

2.5 How to Modify Configuration

Configuration of SSCom Client should be executed in the "Configuration" page. For details of the "Configuration" page, please refer to "3. Configuration".

1. Right-click the SSCom Client icon in the task tray to open the menu.

2. Click on "Stop SSCom Function" to close the menu.

3. Right-click the SSCom Client icon again in the task tray, select "Configuration" from the menu and the "Configuration" page will appear.

4. Update the contents of the required items and click on "Apply".

5. For Windows 8 / 8.1, select "Exit" from the menu again.

6. Run "ResetService.exe" as an administrator from the installation directory.

7. Press "Windows Key" on the keyboard, right-click "Start screen", and click "All apps".

This page is blank.

3

3. Configuration

This section describes Configuration of SSCom Client.

<Chapter Structure>

3.1 Common Operations on the Configuration Page

Configuration of SSCom Client should be executed in the "Configuration" page.
Please follow the steps below before setting the environment:

- ▪Please launch SSCom Client.
- ▪Please select "Stop SSCom Function" of the "Authentication Settings" from the Menu.

3.1.1 How to Show Configuration Page

You can enter "Configuration" page by any ways below:

(1) Enter from the task tray

Under the condition that SSCom Client has been started, double click on the icon of SSCom Client in the task tray.

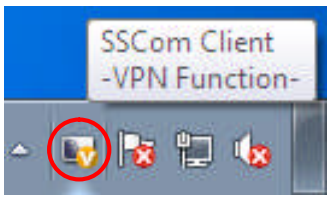


Fig.3.1.1-1 Display "Configuration" Page from the task tray

■Remarks■
Icon of SSCom Client varies in the task tray according to different authentication settings.

(2) Enter from the Menu

Under the condition that SSCom Client has been started, right-click the icon of SSCom Client in the task tray, click "Configuration" in the menu.

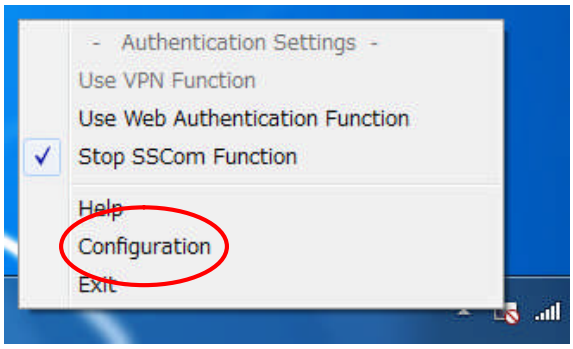


Fig.3.1.1-2 Enter "Configuration" page from the menu

3.1.2 Name and Summary of Each Part in the "Configuration" Page

This section describes name and summary of each part in the "Configuration" page.

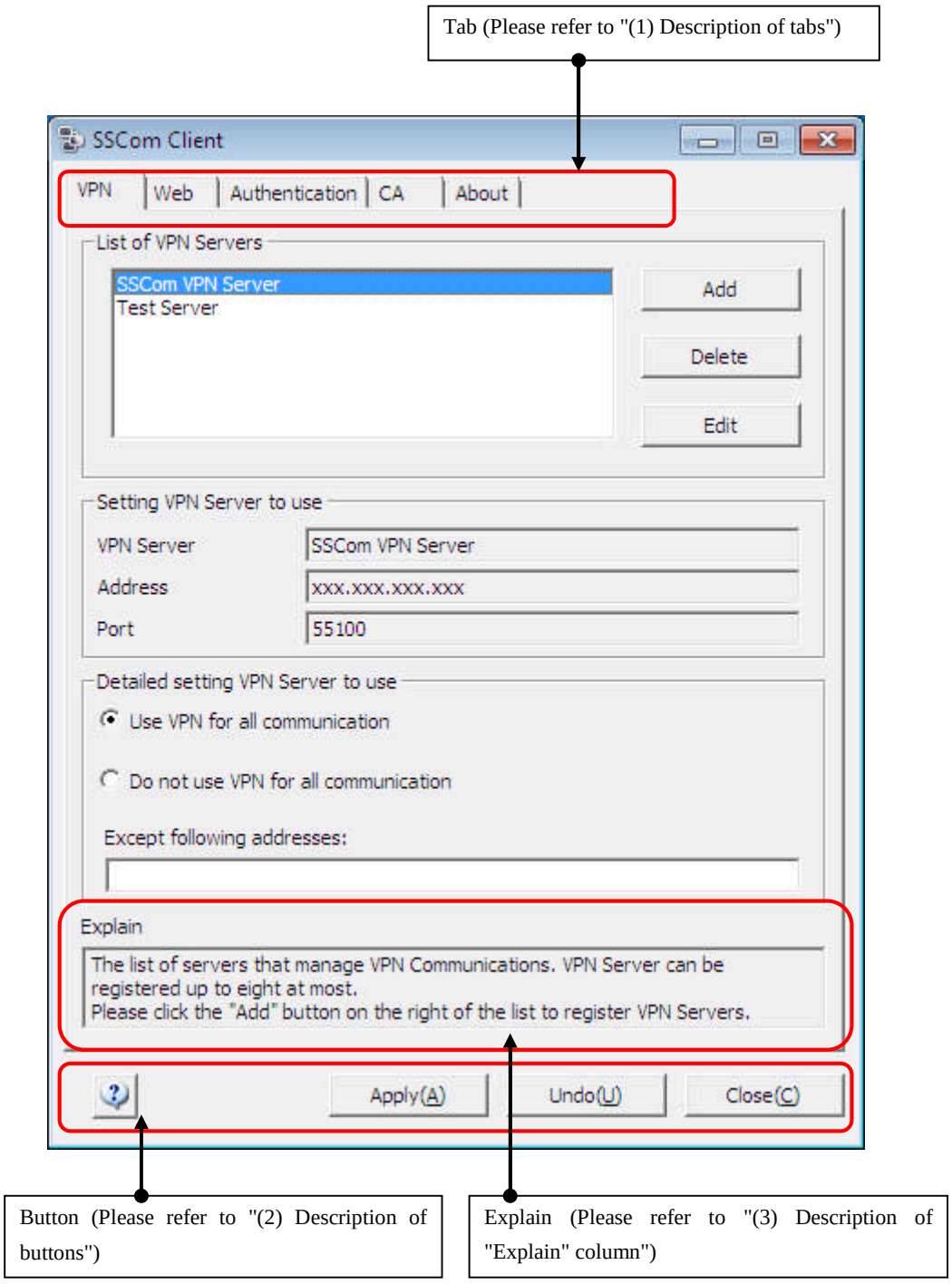


Fig.3.1.2-1 "Configuration" page

(1) Description of tabs

There are 5 tabs in the "Configuration" page. Description of each tab is shown in the table below:

Table 3.1.2-1 Tab Description

Tab Name	Description	Referring Chapter
VPN	Settings needed when using VPN Function. Settings of the SSCom VPN Server to connect by remote access from outside the company.	3.2
Web	Settings needed in Web Authentication Function.	3.3
Authentication	Settings needed when using VPN & Web Authentication Function. Set the authentication method based on your authentication device.	3.4
CA	Settings needed when using VPN & Web Authentication Function. This setting is for certificates issued by the certificate authority that issued the certificate of the server you are connecting from SSCom Client. This is a way for SSCom Client to confirm that the certificate retained by the SSCom Server to connect to from SSCom Client is valid.	3.5
About	Product names and version information of SSCom Client.	3.6

(2) Description of buttons

There are 4 buttons in the "Configuration" page. Description of each button is shown in the table below:

Table3.1.2-2 Button Description

Button Name	Description
Apply	Communication will be reflected only when you click on "Apply" button after setting each item. No settings will be saved without clicking on the "Apply" button.
Undo	Return to the content status at the last click of "Apply".
Close	Close the "Configuration" page.
 (Help)	To show help information.

(3) Description of "Explain" column

Description of the item on the "Configuration" page which has focus by will be displayed. Also, instructions and conditions on how to input method will be shown.

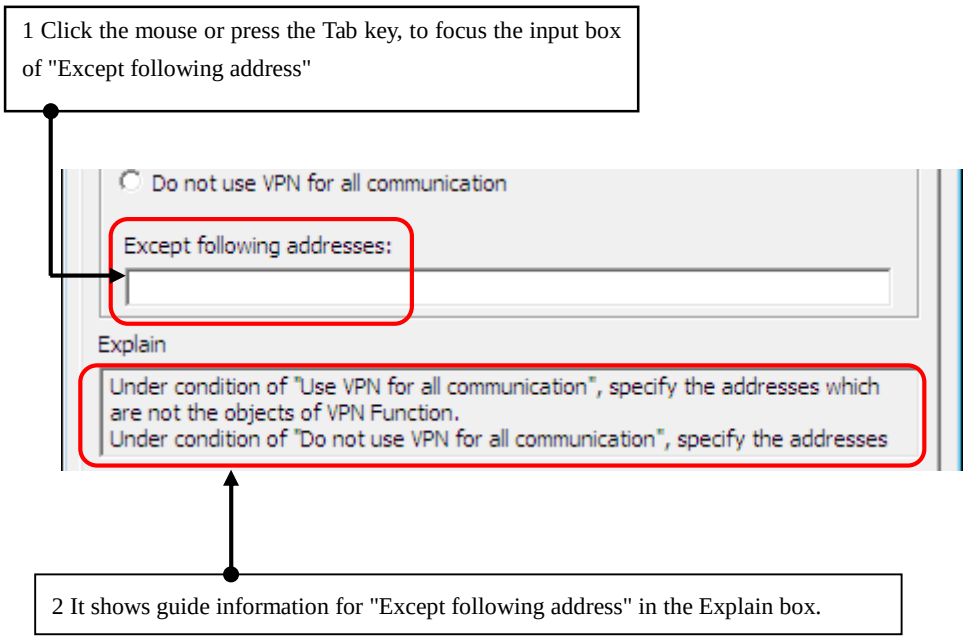


Fig.3.1.2-2 How to show the explanation

3.1.3 How to Update Configuration

It describes how to update settings in the Configuration page.

1. Update contents of necessary items in each tag of Configuration page.

2. Click on the "Apply" button.

3.2 VPN Settings

VPN Function

Necessary settings to use VPN Function can be done in the "VPN" tab.

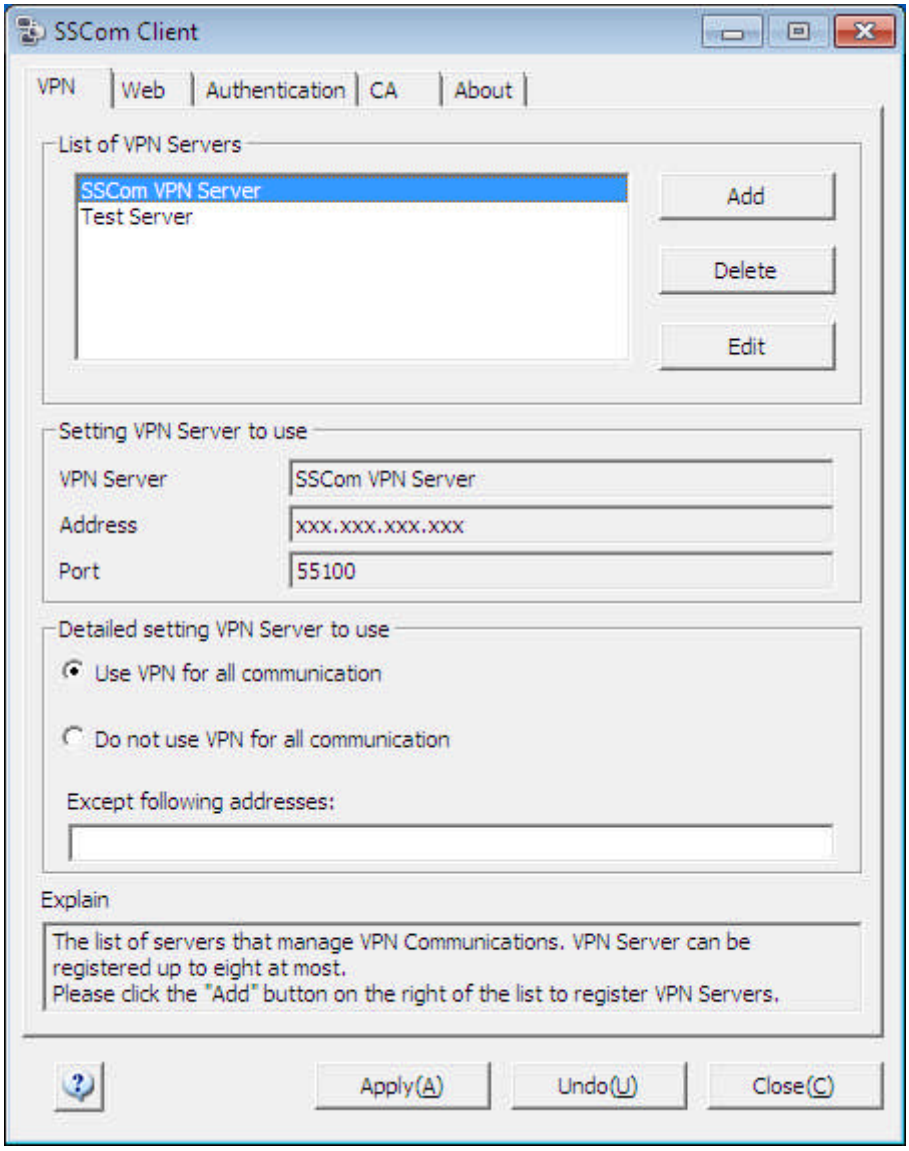


Fig.3.2-1 "VPN" Tab

Each item of "VPN" tab is described below:

"List of VPN Servers": The list of servers (SSCom VPN Server) that manages VPN Communications.

"Add": Add VPN Server to "List of VPN Servers". Click it and "VPN Server Registration" dialog displays. The number of VPN Servers logging can reach 8 at most.
Please refer to "(1) Add VPN Server" for add VPN.

"Delete": Delete VPN Server selected in "List of VPN Servers".

"Edit": Update VPN Server selected in "List of VPN Servers".
Please refer to "(2) Update VPN Server" for Edit VPN.

"VPN Server": Name of the server which VPN Communication uses. Please select VPN Server from "List of VPN Servers" and click on "Apply".

"Address": Address of VPN Server. Address of the VPN Server selected in "List of VPN Servers" will be displayed.

"Port": Port of VPN Server. Port of the VPN Server selected in "List of VPN Servers" will be displayed.

"Use VPN for all communication": Enable VPN for all TCP/IP communication excluding communications specified in "Except following address".

"Do not use VPN for all communication": Disable VPN for all TCP/IP communication excluding communications specified in "Except following address".

"Except following address": Under condition of "Use VPN for all communication", specify the addresses which are not the objects of VPN Function.
Under condition of "Do not use VPN for all communication", specify the addresses which are the objects of VPN Function.
The addresses can be specified in any of the following form:
- Domain name.
- Host name.
- IP address. (xxx.xxx.xxx.xxx form)
- Netmask form. (xxx.xxx.xxx.xxx/nn form)

(xxx is integer in the range of 0 ~ 255 in decimal system. nn is integer in the range of 1 ~ 31 in decimal system).
More than one address can be specified by separating them with "," (comma) or ";" (semicolon). Wildcards (*) cannot be used.
For the usage of "Except following address", please refer to "(3) How to use "Except following address"".

"Explain": Displays explanation of the item that has focus.
For operation method, please refer to "3.1.2 Name and summary of each part in the "Configuration" Page (3) Description of "Explain" column".

(1) Add VPN Server

It describes the way to add a VPN Server which manages VPN Communication.

1. Click on "Add" on the right side of "List of VPN Servers", the dialog box of "VPN Server Registration" pops up.

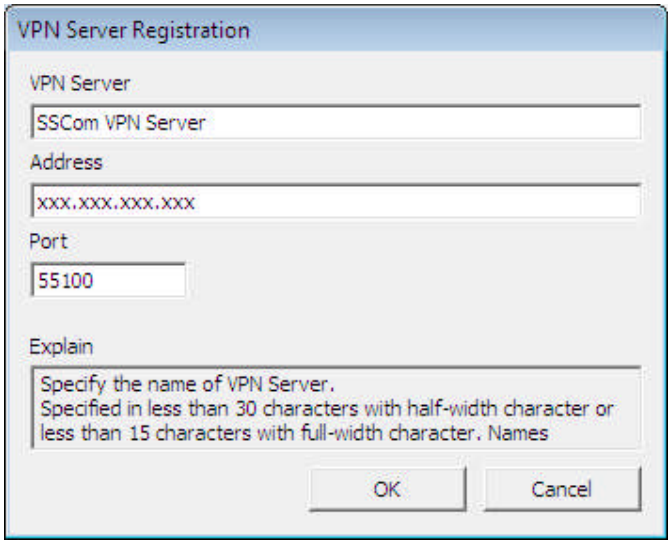


Fig.3.2-2 Dialog box of "Register VPN Server" pops up

"VPN Server": Specify the name of VPN Server. Specified in less than 30 characters with half-width character or less than 15 characters with full-width character. Names specified here will be shown in "List of VPN Servers".
"Address": Specify the IP address of VPN Server. Hostname is specified in less than 255 characters with half-width character, or IP address (xxx.xxx.xxx.xxx form) or in the netmask form (xxx.xxx.xxx.xxx/nn form).
"Port": Specify the port number of VPN Server. Specified in half-width numbers in the range of 1- 65535. The default port is "55100".
"Explain": Displays explanation of the item that has focus.

2. Input the necessary items.

3. Click on "OK" button.

After successful registration, close "VPN Server Registration" dialog and the VPN Server registered will be added to "List of VPN Servers" of the "VPN" tab.

(2) Update VPN Server

It describes the way to modify the VPN Server's contents which has been registered to the "List of VPN Servers".

■Attention■

When updated the VPN Server other than the VPN Server you are using, the VPN Server you are using will be changed to the last updated VPN Server.

Before updating, if necessary make a note of the information of the VPN Server you are using. If you have finished updating, please re-select the VPN Server you are using.

1. Select the VPN Server that needs content updating from the "List of VPN Servers", click "Edit" on the right side. The dialog box of "VPN Server Update" pops up.

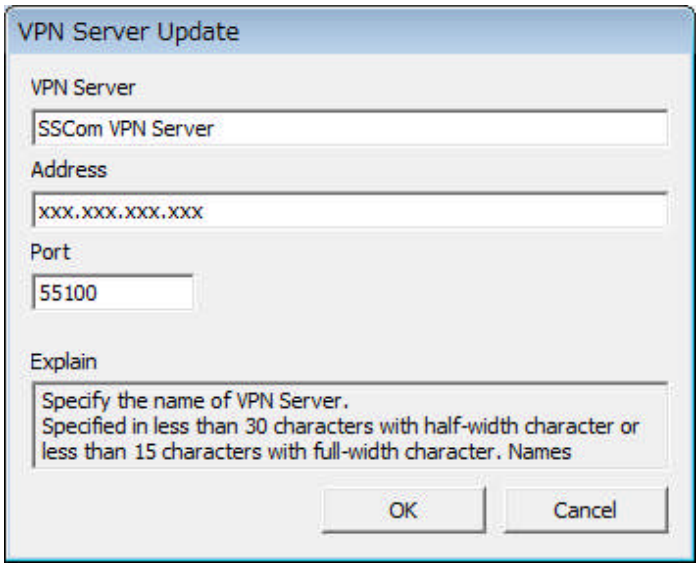


Fig.3.2-3 Dialog Box of "VPN Server Update"

2. Input the items you want to change.

3. Click on "OK".

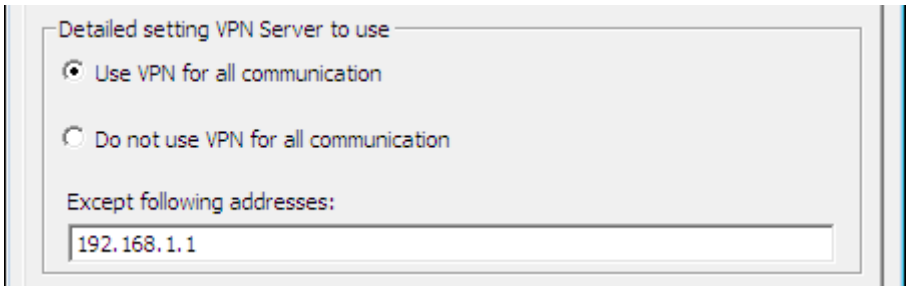
After successful updating, close the dialog box of "VPN Server Update".

(3) How to use "Except following address"

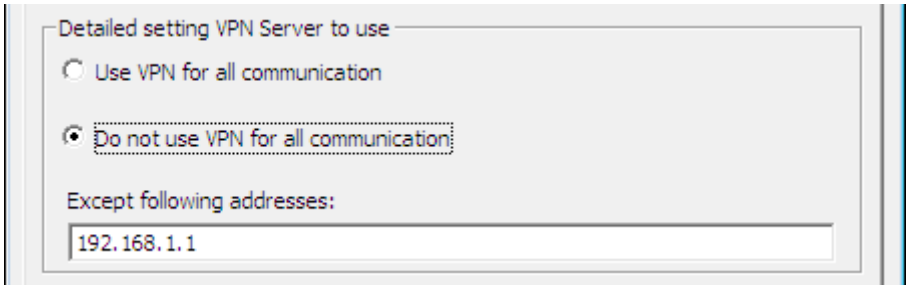
This section describes how to use "Except following address" in the "Detailed setting VPN Server to use".

In "Detailed setting VPN Server to use", the initial setting is all communication using VPN Function, you can set specified server out of the objects of VPN Communication.

For example, choose "Use VPN for all communication" and set "192.168.1.1" in "Except following address", servers besides the server whose IP address is 192.168.1.1 are objects of VPN Communication.



On the contrary, when you select "Do not use VPN for all communication", and set "192.168.1.1" in "Except following address", only the server whose IP address is 192.168.1.1 is the object of VPN Communication.



3.3 Web Settings

Web Authentication

Settings needed to use Web Authentication Function can be done in this tab.

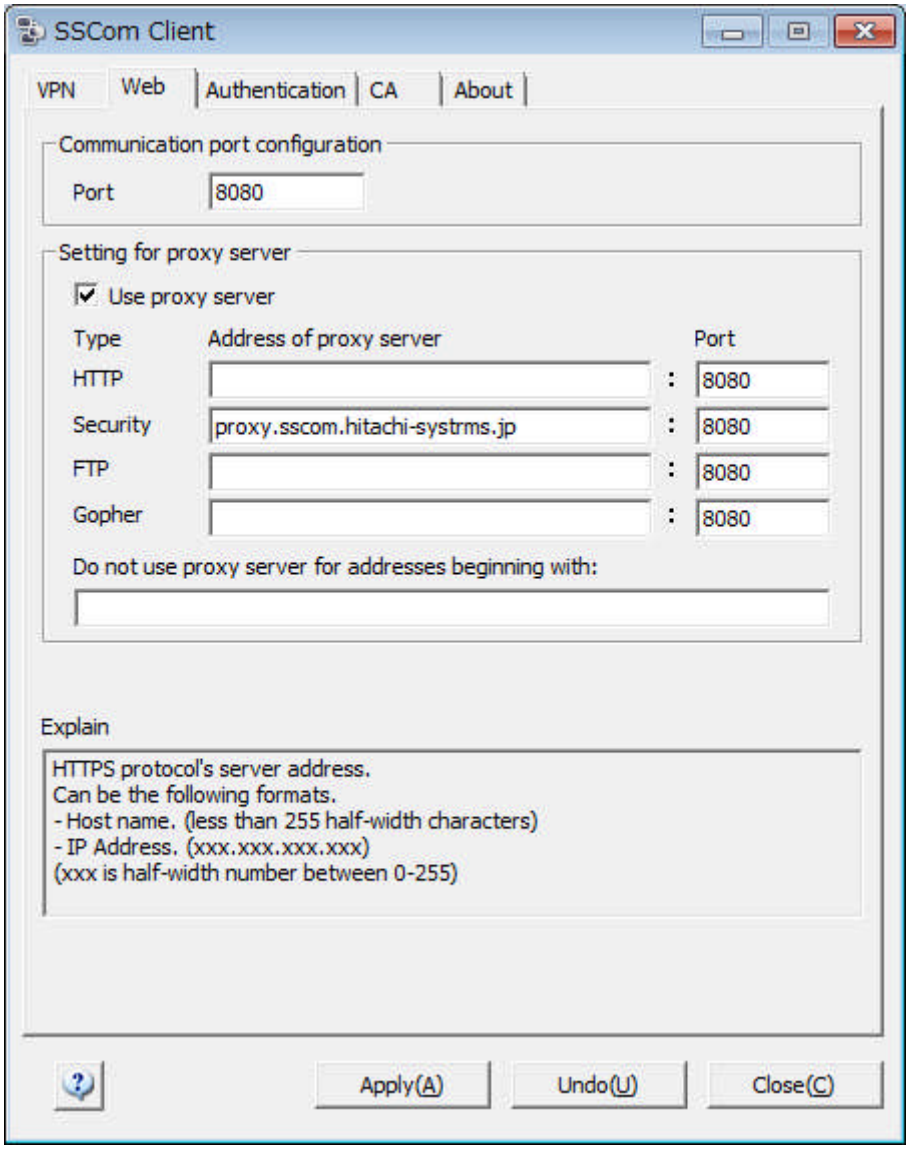


Fig.3.3-1 "Web" Tab

Each item of "Web" tab is described below:

"Port": Port number of the Web browser communicating with SSCom Client should be specified in half-width numbers in the range of 1- 65535. Please specify the same value as the port number specified in the proxy setting of Web browser.

In most cases, the default value (8080) does not need any change. If there is any confliction with other software, it needs to be changed into a value in conjunction with the Web browser.

"Use proxy server": When connecting to the external network through the proxy server under the specified setting, tick off the check box.

"Address of proxy server": Specify the address of proxy server. When a proxy server is not used, the bar is blank. Values such as hostname or IP address (xxx.xxx.xxx.xxx form) can be set.

"Port": Specify the port number of proxy server. Specify port in half-width numbers in the range of 1- 65535.

"Do not use proxy server for addresses beginning with": Specify address of the Web server that needs to access server directly without proxy server.

For example, after specifying "www. hitachi-systems.com", Web page displayed from Web server of www. hitachi-systems.com doesn't go through the proxy server.

The addresses can be specified in any of the following form:

- Domain name.
- Host name.
- IP address. (xxx.xxx.xxx.xxx form)
- Netmask form. (xxx.xxx.xxx.xxx/nn form)

(xxx is integer in the range of 0 ~ 255 by decimal system).

More than one address can be specified by separating them with "," (comma) or ";" (semicolon). Wildcards (*) cannot be used.

(Attention) Please specify the server host name in a fully qualified domain name. Access of "www.hitachi-systems.com" server will not be subject to exception even if you specify " hitachi-systems.com". It will access the server without using the proxy server only when you specify "www.hitachi-systems.com".

"Explain": Displays explanation of the item that has focus.

For operation method, please refer to "3.1.2 Name and summary of each part in the "Configuration" Page (3) Description of "Explain" column".

3.4 Authentication

VPN Function | Web Authentication

Settings about authentication information can be done in this tab. This is the common setting of VPN Function and Web Authentication Function.

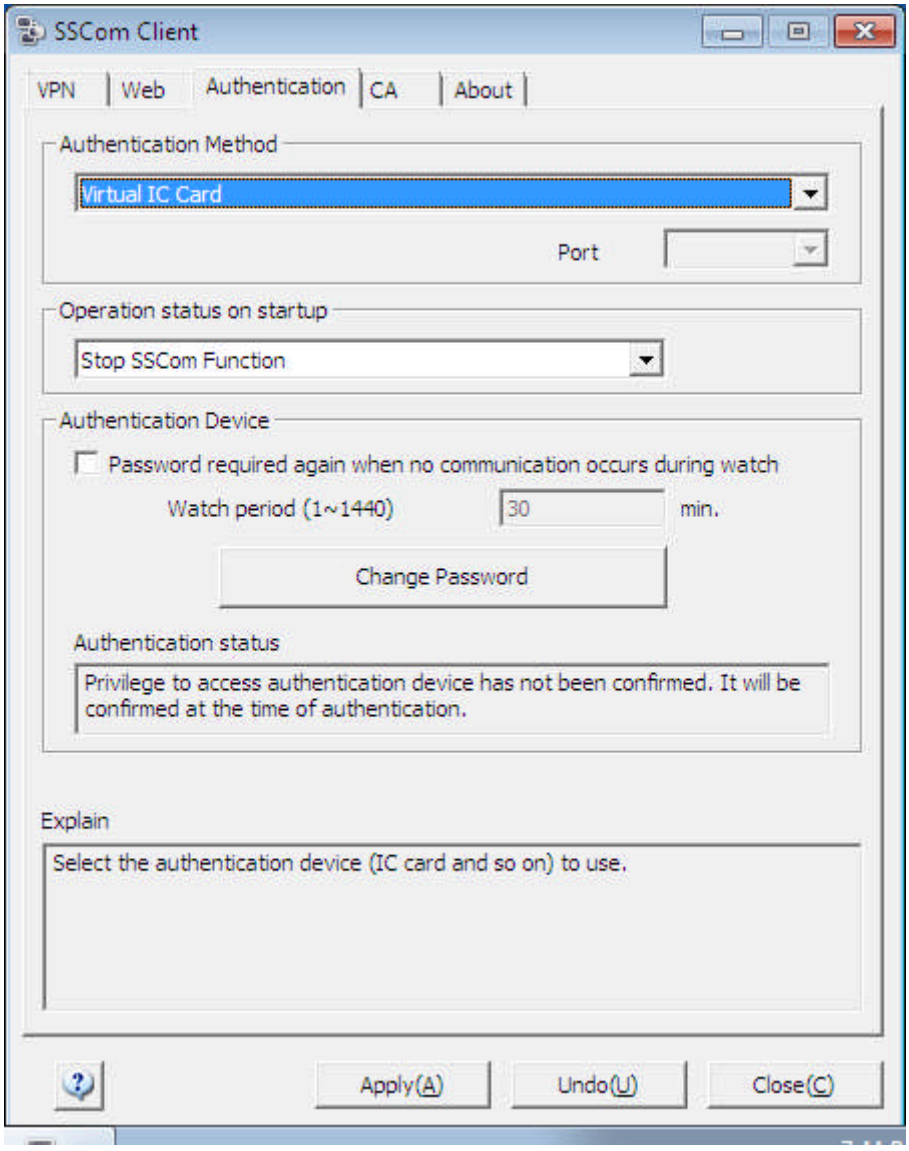


Fig.3.4-1 "Authentication" Tab

Each item of "Authentication" tab is described below:

"Authentication Method": Select the authentication device (IC card and so on) to use.

"Port": If necessary, you can specify the PC's connection port (COM1 ~ COM4, USB) depending on the type of authentication device.

"Operation status on startup":

Choose the operation status when SSCom Client launched.

- Use VPN Function
- Use Web Authentication Function
- Stop SSCom Function

It doesn't set the function (VPN Function or Web Authentication Function) to use when SSCom Client launched. It is necessary to set the function to use when using SSCom. Right-click on the "SSCom Client" icon in the taskbar, and select the function to use from the "Authentication Settings" in the menu displayed.

"Password required again when no communication occurs during watch": During "Watch period", if there is no communication signals that need doing authentication, when the network communication starts again, you need to enter your password.

If device implemented CryptoAPI has been selected in "Authentication Method", this function can't be used.

"Watch period (1~1440)": Specify the number of minutes until it becomes necessary to enter the password in the communications which need authentication. Specify in half-width number in the range of 1 to 1440. Default value is 30 minutes.

"Change Password": Click on "Change Password" to change the password of authentication device, the dialog of "Change Password" will be displayed.

Please refer to"(1) How to change password" to know the way to change password.

If device implemented CryptoAPI has been selected in "Authentication Method", this function can't be used.

"Authentication Status": Status of authentication devices in "Authentication Method".

"Explain": Displays explanation of the item that has focus.

For operation method, please refer to "3.1.2 Name and summary of each part in the "Configuration" Page (3) Description of "Explain" column".

(1) How to change password

It describes how to change the password of authentication device.

1. Click on "Change Password" in the "Authentication" tab, the dialog of "Change Password" pops up.

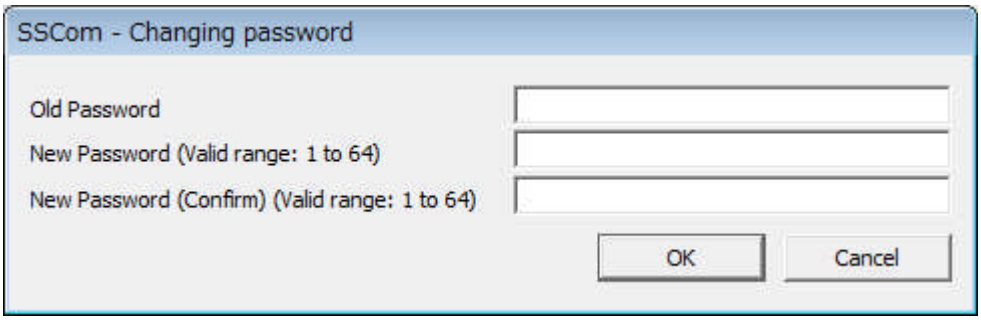


Fig.3.4-2 "Change Password" dialog

"Old Password": Specify current password.
"New Password": Specify new password in less than 64 characters with half-width character.
"New Password (Confirm)": Specify the same password as "New Password".

2. Input the password in use (old password) and the new password.

3. Click on "OK".

If it is done, prompt message of successful changing will pop up. The new password becomes effective in authentication the next time.

■Remarks■

You can change the password of authentication device from "Authentication" tab in the "Configuration" page. Besides, it also can be done by Windows Start menu - "All Programs" - "SSCom Client" - "Change Password".

(2) Certificate Import Steps of Virtual IC Card

If you use the Virtual IC Card as the authentication device, (select "Virtual IC Card" in Authentication Method), certificate need to be imported into the PC in use.

Steps to import a certificate are described below:

1. Click on "Start" - "Programs" - "SSCom Client" - "User Certificate Management Tool", "User Certificate Management" dialog will be shown.

2. Click on "Register a Certificate".

3. Specify the location of the certificate to be imported and double click on it.

4. Input the initial password of the certificate, and click on "OK".

3.5 CA Settings

VPN Function | Web Authentication

Settings about authentication information can be done in this tab. This is the common setting of VPN Function and Web Authentication Function.

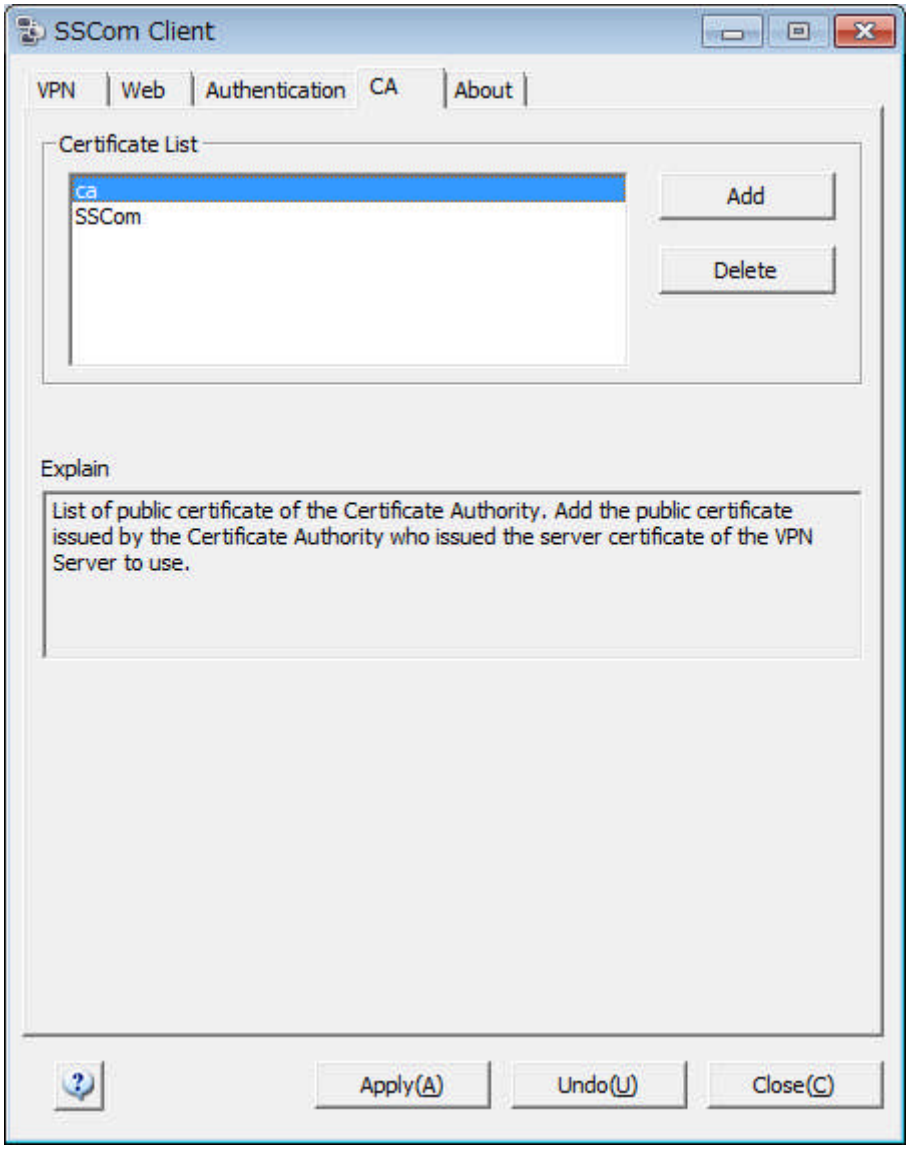


Fig.3.5-1 "CA" Tab

Each item of "CA" tab is described below:

"Certificate List": List of public certificate of the Certificate Authority. Add the public certificate issued by the Certificate Authority who issued the server certificate of the VPN Server to use.
"Add": Add the certificate of Certificate Authority to the list. If you click on it, the dialog of "Select Certificate" will appear. The file with the extension of ".der" or ".cer" can be used as certificate. The change will take effect when SSCom Client restarts.
"Delete": Delete the certificate selected from "Certificate List". The change will take effect when SSCom Client restarts.
"Explain": Displays explanation of the item that has focus. For operation method, please refer to "3.1.2 Name and summary of each part in the "Configuration" Page (3) Description of "Explain" column".

3.6 Version Information

The following product information will be shown on "About" tab:

- Product name
- Release number

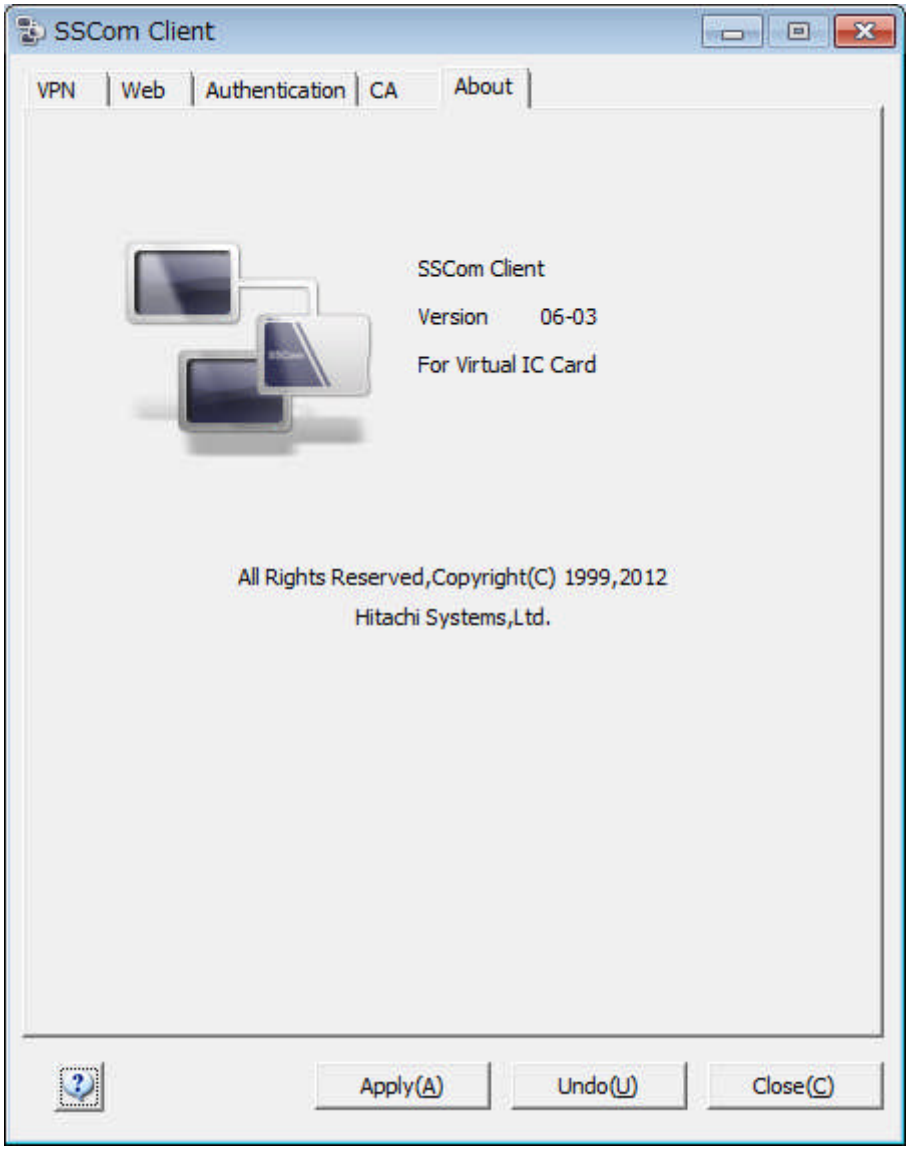


Fig.3.6-1 "About" Tab

This page is blank.

4

4. Message

This chapter describes the message with Message ID, which is outputted by SSCom Client.

<Chapter Structure>

4.1 Message Format

4.2 Message Output Sample

4.3 Message List of SSCom Client

4.1 Message Format

SSCom message system is shown as below:

```
   ┌ Message ID ┐
   S S X X Y Y Y - Z          Message Text

Classification of Message ID
        SS : Product ID (SSCom)
        xx : Component ID
                CL: SSCom Client
                VA: SSCom VPN/AP Server
                GA: SSCom GAC Server
                MA: SSCom Manager
        yyy: Serial number of each component
        z   : Message attribute
                 I: Information message
                 E: Error message
                 W: Warning message (Continue to proceed)
```

The messages of SSCom Client (the component ID part of message ID is "CL") are described in this manual. Please refer to the following manual for other messages.

- Message of SSCom Server (the component ID part of message ID is "VA" or "GA")

  -> Please refer to "SSCom Manual Administrator Guide".
- Message of SSCom Manager (the component ID part of message ID is "MA")

  -> Please refer to "SSCom Manager Manual".

4.2 Message Output Sample

Messages of SSCom Client will be displayed in the form of the following message dialog.

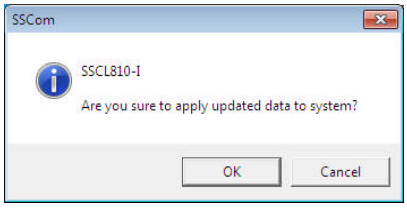


Fig.4.2-1 Message Dialog Sample

4.3 Message List of SSCom Client

This section describes the message that is displayed in the message dialog and how to deal with it.

[Description of message list]

Message ID
Message text

[Meaning] Message content
[Operation] How to deal

SSCL001-E
Not enough memory is available to perform this operation.

[Meaning] Insufficient memory for SSCom Client running.
[Operation] Terminate unnecessary procedures to ensure sufficient memory for SSCom Client running.
If memory space is still insufficient, add memory or expand virtual memory.
To know memory space SSCom Client needed in operating, please refer to "SSCom Manual Overview".

SSCL002-E
Failed to start this program.
Windows system may be unstable.

[Meaning] SSCom Client fails to start because of unstable running of Windows.
[Operation] Restart Windows and do the operation again. If the error circumstance occurs again, please contact the system administrator.

SSCL003-E
Failed to start this program.
Files required for the operation of the SSCom Client cannot be found or files are invalid.

[Meaning] If the message appears, you can consider the following main factors:
▪Executable file of the program has been changed due to some system trouble.
▪Installation of the program was failed.
▪Hard disk of your PC is out of order.
▪Your PC is infected with virus.
▪The behavior of your PC has become unstable.
▪When uninstalling other software, files needed for starting SSCom Client stored in shared files are deleted, etc.
[Operation] Restart Windows with the same action. If the error circumstance occurs again, use "Uninstall Programs" to uninstall SSCom Client and install it again.
Please refer to "1. Install/Uninstall" for specific operation method of installation.

SSCL004-E

Authentication device implemented CryptoAPI is not supported on Windows NT.

Please confirm the combination of OS on which SSCom Client can be used and authentication device.

[Meaning] Authentication device implemented CryptoAPI is not supported on Windows NT.

[Operation] Change into authentication devices compatible with Windows NT, or use SSCom Client on the OS which support authentication device implemented CryptoAPI. Please consult with the system administrator.

SSCL010-E

The network communication environment of PC is abnormal.

Restart Windows, if the error occurs again, please contact the system administrator.

[Meaning] SSCom Client cannot run because behavior of Windows is unstable.

[Operation] Restart Windows and repeat the operation. If the error occurs again, please contact the system administrator.

SSCL020-E

The resource is not found.

[Meaning] The resource is not found.

[Operation] Please place the resource file in the same directory as the exe file or reinstall the program. If the error occurs again, please contact the system administrator.

SSCL042-E

Failed attempt to access the authentication device.

Please check whether the authentication device which SSCom Client uses has been set correctly.

[Meaning] The message will be shown when the authentication device cannot be used normally, you can consider the following main factors:

▪The chip of authentication device is covered with dirt, which causes failure of access.

▪The authentication device is not correctly inserted.

[Operation] Follow the operation below and repeat the operation:

▪Remove the authentication device and insert it again.

▪If there is dirt on the chip surface of the authentication device, please gently wipe the chip surface.

SSCL043-E

Data stored in the authentication device is invalid.

Please check if there is any data been written illegally into the device or it has been destroyed.

Please contact the system administrator.

[Meaning] Wrong write operations have been done to the authentication device or the device has been destroyed.

[Operation] Please consult with the system administrator.

SSCL044-E

Failed to detect authentication device.
Please check the following:
- The drivers of authentication device have been installed into your PC.
- Authentication device has been set correctly.
- "Authentication Method" of the SSCom Client has been set correctly.

[Meaning] The authentication device could not be detected.

The message will be shown when the authentication device cannot be detected. You can consider the following main factors:

▪Driver of the authentication device has not been installed into the client PC.

▪The authentication device has not been connected correctly to PC.

▪IC card reader has not been connected correctly to PC.

▪IC card reader has not been properly set.

▪SSCom Client doesn't specify any authentication device in Configuration of the PC.

▪Wrong port number has been specified of authentication device in Configuration of SSCom Client.

[Operation] Follow the operation below and repeat the operation:

▪If Device Manager fails to detect IC card reader, please install the driver of the authentication device.

▪Please connect the authentication device with the PC.

▪If there is dirt on the chip surface of the authentication device, please gently wipe the chip surface.

▪Please insert the IC card reader into the PC.

▪Please adjust the settings of IC card and the IC card reader.

▪If there is any damage on the chip surface, please replace the authentication device with a new one.

▪Please specify the authentication device which you are using in the "Configuration" page "Authentication" – "Authentication Method" of SSCom Client.

▪Please specify the port number of the authentication device which you are using in the "Configuration" page "Authentication" – "Authentication Method" of SSCom Client.

SSCL045-E

Authentication device has not been set. Please check if the authentication device has been set correctly.

[Meaning] Authentication device has not been set. If the authentication device cannot be detected, this message will be displayed.

You can consider the following causes:

▪IC card reader has not been connected correctly to PC.

▪IC card has not been properly set in IC card reader.

[Operation] Follow the operation below and repeat the operation:

▪Please insert the IC card reader into the PC.

▪Please set the IC card to the IC card reader.

SSCL046-E

Authentication device which cannot be used by the SSCom Client installed to your PC has been set. Authentication device may be applicable to other system.

[Meaning] The authentication device is not compatible with the SSCom Client installed on your PC, and you can consider the following causes:

▪Authentication device is applicable to other version of SSCom Client.

▪Data saved in the authentication device is related to other system rather than SSCom Client.

[Operation] Insert applicable authentication device into PC to ensure proper function of SSCom Client.

SSCL047-E

Certificate for Virtual IC Card has not been registered.
Please set the certificate.

[Meaning] The certificate of Virtual IC Card has not been set in advance.

[Operation] Please set the certificate by using the "User Certificate Management Tool" attached with Virtual IC Card products.

SSCL050-E

This application is already running.

[Meaning] The SSCom Client has initiated two applications. Overlapped operations cannot be completed at the same time.

[Operation] Don't launch above two applications of SSCom Client on the same computer.

SSCL070-E

Failed to get the certificate.
Please check the following:
- Authentication device has been set correctly.
- "Authentication Method" in the "Configuration" has been set correctly.
- The certificate has been registered into the authentication device.

[Meaning] The certificate could not be loaded. You can consider the following main causes:

▪The authentication device has not been set correctly.

▪"Authentication" – "Authentication Method" in "Configuration" page of SSCom Client has not been set correctly, or not click on "Apply" button after any modifications.

▪The certificate has not been imported into authentication device.

[Operation] Follow the measures below according to the causes:

▪Set the authentication correctly.

▪Make sure the settings in "Authentication" – "Authentication Method" in "Configuration" page of SSCom Client are correctly set, and click on "Apply" button after ay modifications.

▪If there is no certificate imported in the authentication device, please get the certificate.

SSCL071-E

Encryption failed.
Please check the following:
- Authentication device has been set correctly.
- "Authentication Method" in the "Configuration" has been set correctly.
- The certificate has been registered into the authentication device.

[Meaning] Encryption failed. You can consider the following causes:

▪Authentication device is pulled down form PC during the authentication process (The authentication process is cancelled).

▪The authentication device has not been set correctly.

▪The certificate has not been logged into authentication device.

▪Damaged authentication device.

[Operation] Follow the measures below according to the causes:

▪Set the authentication device correctly.

▪Make sure the settings in "Authentication" – "Authentication Method" in "Configuration" page of SSCom Client are correctly set, and click on "Apply" button after any modifications.

▪If there is no certificate imported in the authentication device, please get the certificate.

▪Please consult with the system administrator.

SSCL099-E

SSCom Client has an unexpected behavior due to an internal error.
Please contact the system administrator.

[Meaning] SSCom Client had an internal failure causing abnormal behaving.

[Operation] Please consult with the system administrator.

SSCL100-E

The port of proxy server which is used to communicate with Web browser is already in use by another application.

[Meaning] Specified port on "Web" - "Port" in SSCom Client "Configuration" page has been occupied by other application programs.

[Operation] Terminate the program occupying the specified port or change the port number to other un-occupied one for this product.

SSCL110-E

Failed to start the proxy port used to communicate with Web browser.
Windows system may be unstable.

[Meaning] Proxy server which communicates with Web server failed to start in the case of unstable running of Windows.

[Operation] Restart Windows and repeat the operation. If the error circumstance occurs again, please contact the system administrator.

SSCL200-E

Unable to communicate with VPN Server.
Please check if the address or port of VPN Server specified in the SSCom Client Configuration are correct.
If settings is correct, check if SSCom VPN Server has been stopped, or is there any network failure between SSCom Client and SSCom VPN Server, please confirm with the network administrator.

[Meaning] Fail to communicate with SSCom VPN Server. Consider the following reasons:

- ▪Specified address and port of VPN Server in "VPN"-"Setting VPN Server to use" in SSCom Client "Configuration" page are incorrect.
- ▪Unavailability of the VPN Server.
- ▪Security or firewall software settings caused failure in communication between SSCom Client and VPN Server.
- ▪Network failure between SSCom Client and VPN Server.

[Operation] Repeat the operation after follow the measures below:

- ▪Reset the settings of VPN Server if the settings in "VPN" of SSCom Client "Configuration" page are incorrect.
- ▪Check if VPN Server has been launched.
- ▪Please make sure the security software or network equipment are set correctly.
- ▪Please contact the network administrator if there is network failure.

SSCL202-E

Versions of SSCom Client and SSCom Server are not consistent.
Please contact the network administrator to confirm the version of SSCom VPN Server, and install the right version of SSCom Client.

[Meaning] Versions of SSCom Client and SSCom Server are not consistent.

[Operation] Please install the specified version of SSCom Client under instruction of network administrator.

SSCL204-E

Cannot connect to server.

Please check the following:

- Server address specified on your PC is correct.
- Server has been launched.
- Whether there is any network failure between specified VPN Server and SSCom Client.

[Meaning] Fail to access business server from SSCom Client using VPN Function.

Consider the following reasons:

▪Specified address or IP address of the business server is incorrect.

▪The business server is unavailable.

▪Network failure between business server and VPN Server.

[Operation] Repeat the operation after follow the measures below:

▪Reset the IP address of the business server if the address setting is incorrect.

▪Verify with the system administrator if the business server has been launched.

▪Please make sure the security software or network equipment are set correctly.

▪Please contact the network administrator if there is a network failure.

SSCL206-E

No permission to access SSCom VPN Server with the authentication device.

Please check the following with system administrator:

- The user in use has been registered in SSCom VPN Server.
- Certificate is in a valid state.

[Meaning] No access right to SSCom VPN Server with the authentication device. Consider the following reasons:

▪No registration information on SSCom VPN Server.

▪Access right not set on SSCom VPN Server.

▪The certificate has passed its expiry date.

▪The certificate was revoked.

[Operation] Please register the user in the SSCom VPN Server before access. Please contact the network administrator.

SSCL207-E

Unable to communicate with untrusted server.

To ensure security, it cannot communicate with servers other than SSCom VPN Server which has been proven by the Certificate Authority specified in the Configuration of SSCom Client.

[Meaning] Attempt to communicate with untrusted server.

Consider the following reasons:

▪CA Certificate has not been registered in "CA"-"Certificate List" in SSCom Client Configuration.

▪Date setting of the computer installed SSCom Client is incorrect.

[Operation] Repeat the operation after follow the measures below:

▪Please register the certificate of CA issued by system administrator.

▪Correct the Date Setting of the computer.

SSCL210-E

User authentication failed with SSCom VPN Server.

Please check the following with system administrator:

- The user in use has been registered in SSCom VPN Server.
- Certificate is in a valid state.

[Meaning] User authentication failure on SSCom VPN Server.

Consider the following reasons:

▪The user has not been registered as a SSCom user.

▪Access right for the user has not been set.

▪The certificate has passed its expiry date.

▪The certificate was revoked.

[Operation] Please consult with the system administrator.

▪Please register the user before access.

▪Please issue a new certificate if the old one is invalid.

SSCL212-E

No permission to access the server.

Please make sure that the authentication device is set correctly.

If it is set, please check the following with system administrator:

- The user in use has been registered in the server.
- Certificate is in a valid state.

[Meaning] No access rights to SSCom Server.

Consider the following causes:

▪No access rights to the server attempting to access.

▪Communication interrupt happens because of unstable communication between SSCom Client and SSCom VPN Server, or blocked by the firewall settings.

▪Module of SSCom Client conflicted with other software, resulted in incorrect action.

▪The CA certificate of the user certificate and server are different.

▪The authentication device has not been connected correctly to PC.

▪IC card reader has not been connected correctly to PC.
▪IC card has not been properly set into the IC card reader.
▪Password of authentication device has not been entered.

[Operation] Follow the steps below and repeat the operation:

▪Please check with system administrator if the system has been set access right for the user attempting to connect the server.
▪If user certificate registered in the authentication device is not issued by the same CA as which issued the certificate of server, please replace it with the certificate issued by the same CA.
▪Remove the authentication device and insert it into the PC again.
▪Please insert the IC card reader into the PC.
▪Please set the IC card into the IC card reader.
▪Please enter the password to use the authentication device.

SSCL213-E

An error has occurred in SSL connection.

[Meaning] An error has occurred in SSL connection.

Consider the following causes:

▪Communication interrupt happens because of unstable communication between SSCom Client and SSCom VPN Server.
▪Invalid certificate is used on SSCom.
▪Authentication device fails to read the certificate because of unstable working.

[Operation] Please check the following points:

▪Please confirm the network connection with SSCom VPN Server.
▪Certificate settings on SSCom Client and SSCom VPN Server are correct.
▪Authentication device has been properly connected.

SSCL220-E

Unable to enable VPN Communication because authentication device is not set or the authentication has not been done.

[Meaning] You can consider the following main factors when VPN fails to start. Consider the following causes:

▪The authentication device has not been connected correctly to PC.
▪IC card reader has not been connected correctly to PC.
▪IC card has not been properly set into the IC card reader.
▪Password of authentication device has not been entered.

[Operation] Follow the operation below and repeat the operation:

▪Remove the authentication device and insert it into the PC again.
▪Please insert the IC card reader into the PC.
▪Please set the IC card into the IC card reader.
▪Please enter the password to use the authentication device.

SSCL300-E

Unable to find specified HTTP proxy on the proxy server.

HTTP proxy address or port is incorrect, or Proxy Server is unavailable or the proxy settings are incorrect.

[Meaning] Address of HTTP proxy specified in "SSCom Configuration" - "Web" - "Address of proxy server" doesn't exist. Consider the following reasons:

- ▪Specified port number or IP address of the HTTP proxy is incorrect.
- ▪Security software or the firewall settings block communication between SSCom Client and proxy server.
- ▪Unavailability of the Proxy Server.
- ▪Network failure between Proxy Server and SSCom Client.

[Operation] Repeat the operation after follow the measures below:

- ▪If address of HTTP proxy specified in SSCom Client "Configuration" - "Web" - "Address of proxy server" is incorrect, please modify it.
- ▪Launch the Proxy Server.
- ▪Please make sure the security software or network equipment are set correctly.
- ▪Please contact the network administrator if there is network failure.

SSCL301-E

Specified HTTP proxy port on the proxy server is out of range. (Valid range: 1 to 65535)

[Meaning] Port number of HTTP proxy specified in SSCom Client "Configuration" - "Web" - "Address of proxy server" should be integer ranging in 1 ~ 65535.

[Operation] Please specify the port number with integer ranging in 1 ~ 65535.

SSCL305-E

Unable to find specified Security proxy on the proxy server.

Security proxy address or port is incorrect, or Proxy Server is unavailable or the proxy settings are incorrect.

[Meaning] Address of Security proxy specified in SSCom Client "Configuration" - "Web" - "Address of proxy server" doesn't exist. Consider the following reasons:

- Specified port number or IP address of the Security proxy is incorrect.
- Security software or the firewall settings block communication between SSCom Client and proxy server.
- Unavailability of the Security proxy.
- Network failure between Security proxy and SSCom Client.

[Operation] Repeat the operation after following the measures below:

- If address of Security proxy specified in "Configuration" - "Web" - "Address of proxy server" is incorrect, please modify it.
- Launch the Security proxy.
- Please make sure the settings of security software or network equipment are correct.
- Please contact the network administrator if there is network failure.

SSCL306-E

Specified Security proxy port on the proxy server is out of range. (Valid range: 1 to 65535)

[Meaning] Port number of Security proxy specified in SSCom Client "Configuration" - "Web" - "Address of proxy server" should be integer ranging in 1 ~ 65535.

[Operation] Please specify the port number with integer ranging in 1 ~ 65535.

SSCL310-E

Unable to find specified FTP proxy on the proxy server.

FTP proxy address or port is incorrect, or Proxy Server is unavailable or the proxy settings are incorrect.

[Meaning] Address of FTP proxy specified in SSCom Client "Configuration" - "Web" - "Address of proxy server" doesn't exist. Consider the following reasons:

- Specified port number or IP address of the FTP proxy is incorrect.
- Security software or the firewall settings block communication between SSCom Client and FTP proxy.
- Unavailability of the FTP proxy.
- Network failure between FTP proxy and SSCom Client.

[Operation] Repeat the operation after following the measures below:

- If address of FTP proxy specified in "SSCom Environment Setting" - "Web" - "Address of proxy server" is incorrect, please modify it.
- Launch the FTP proxy.
- Please make sure the settings of security software or network equipment are correct.
- Please contact the network administrator if there is network failure.

SSCL311-E

Specified FTP proxy port on the proxy server is out of range. (Valid range: 1 to 65535)

[Meaning] Port number of FTP proxy specified in SSCom Client "Configuration" - "Web" - "Address of proxy server" should be integer ranging in 1 ~ 65535.

[Operation] Please specify the port number with integer ranging in 1 ~ 65535.

SSCL315-E

Unable to find specified Gopher proxy on the proxy server.

Gopher proxy address or port is incorrect, or Proxy Server is unavailable or the proxy settings are incorrect.

[Meaning] Address of Gopher proxy specified in SSCom Client "Configuration" - "Web" - "Address of proxy server" doesn't exist. Consider the following reasons:

- Specified port number or IP address of the Gopher proxy is incorrect.
- Security software or the firewall settings block communication between SSCom Client and Gopher proxy.
- Unavailability of the Gopher proxy.
- Network failure between Gopher proxy and SSCom Client.

[Operation] Repeat the operation after following the measures below:

- If address of Gopher proxy specified in "Configuration" - "Web" - "Address of proxy server" is incorrect, please modify it.
- Launch the Gopher proxy.
- Please make sure the settings of security software or network equipment are correct.
- Please contact the network administrator if there is network failure.

SSCL316-E

Specified Gopher proxy port on the proxy server is out of range. (Valid range: 1 to 65535)

[Meaning] Port number of Gopher proxy specified in "SSCom Configuration" - "Web" - "Address of proxy server" should be integer ranging in 1 ~ 65535.

[Operation] Please specify the port number with integer ranging in 1 ~ 65535.

SSCL320-E

Password that you specified is different from the password has been registered.
Please enter the correct password for using SSCom Client.
Please note uppercase and lowercase letters are case sensitive.

[Meaning] The password is not the one to use SSCom Client.

[Operation] Please enter the right password to use SSCom Client.

SSCL321-E

Invalid new password length. (Valid range: 1 to 64)

[Meaning] Invalid length of the new password.

Consider the following reasons:

▪Length of the new password exceeds the allowable value (64 characters).

▪No new password is specified.

[Operation] Set correct password within length range of 64 characters in half-width mode.

SSCL322-E

Two new passwords mismatch.

[Meaning] The password entered in New Password and New Password (Confirm) is different. In addition, the message appears if one of New Password or New Password (Confirm) is omitted.

[Operation] Please enter the same text with New Password and New Password (Confirm).

SSCL323-E

Invalid old password.
Please enter the correct password for using SSCom Client.
Please note uppercase and lowercase letters are case sensitive.

[Meaning] The password is not the one to use SSCom Client.
Current password entered is not consistent with the one of the authentication device set in SSCom Client "Configuration".

[Operation] Please enter the right password to use SSCom Client.

SSCL324-E

Authentication device became obsolete because invalid password had been entered continuously.

[Meaning] The authentication device cannot be used because of consecutive inputs of incorrect password.

[Operation] Please consult with the system administrator.

SSCL325-E

Specified communication port is invalid. (Valid range: 1 to 65535)

[Meaning] Port number specified is not an integer ranging in 1 - 65535.

[Operation] Please specify the port number with integer ranging in 1 - 65535.

SSCL326-E

You can't use authentication device with default password.
You must change it to your own password.

[Meaning] The authentication device cannot be used because the password of authentication device is a default password.

[Operation] Please change your password setting in SSCom Client "Configuration" - "Authentication" - "Change Password" for the authentication device.

SSCL327-E

Cannot change authentication device password.
Please use compatible program of CryptoAPI to change the password.

[Meaning] You can't change the password of the authentication device implemented CryptoAPI. Please use compatible program of CryptoAPI to change the password.

[Operation] Please use the attached program for authentication device to change the password.

SSCL330-E

Specified port is invalid. (Valid range: COM1 to COM4 or USB)

Confirm on the corresponding interface for the authentication device and reinsert it.

[Meaning] The authentication device is not using the specified interface.

[Operation] Confirm on the corresponding interface for the authentication device and reinsert it.

SSCL335-E

Unable to add an invalid certificate.

[Meaning] Addition of CA certificate is rejected because of wrong file format.

[Operation] Please add a CA certificate with correct file format.

SSCL340-E

Specified watch period is invalid. (Valid range: 1 to 1440)

[Meaning] Watch period is not an integer ranging in 1 - 1440.

[Operation] Set the period in the range of 1 - 1440.

SSCL350-E

Specified VPN Server name is invalid.

Set VPN Server with length below 30 characters in half-width mode or 15 characters in full-width mode.

[Meaning] Invalid name of VPN Server because of improper length.

Consider the following reasons:

▪Length of the name of VPN Server exceeds the allowable value.

▪Name of the VPN Server is not specified.

[Operation] Set VPN Server with length below 30 characters in half-width mode or 15 characters in full-width mode.

SSCL351-E

Specified VPN Server name is already registered.

Use another name.

[Meaning] VPN Server list has recorded the same name with the name you choose for the VPN Server.

[Operation] Please choose name for the VPN Server not registered in VPN Server list.

SSCL352-E

Specified address is invalid.

Please specify the host name of VPN Server with length below 255 characters in half-width mode or the IP address of VPN Server.

[Meaning] Invalid address being specified.

Consider the following reasons:

▪Length of host name exceeds the allowable value (255 characters in half-width).

▪Wrong IP address is entered.

▪Host name is not specified.

[Operation] Specify the host name of VPN Server under the following description:

▪Specify name with length below 255 characters in half-width mode.

▪Specify IP address in the form of (xxx.xxx.xxx.xxx).

SSCL353-E

Specified port is out of range. (Valid range: 1 to 65535)

[Meaning] Port number inputted is not an integer ranging in 1 ~ 65535.

[Operation] Please specify the port number with integer ranging in 1 ~ 65535.

SSCL400-E

No connections are permitted.

The application side which works with SSCom Client does not allow communication with SSCom Client.

Please verify the settings of the application.

[Meaning] Communication can be enabled only when permission from the application works with SSCom Client is obtained.

[Operation] Try to obtain permission from the application works with SSCom Client.

SSCL401-E

Suspended connections timed out. Connections between SSCom Client and the application have no communication for a certain period of time, so it has timed out.

Please verify the settings of the application.

[Meaning] Connection to SSCom Client will be retained in a certain period, communication will be timed out over the period.

[Operation] Please check the settings of the application works with SSCom Client.

SSCL800-I

Are you sure to terminate SSCom Client?

(Attention) Termination process may be delayed while authentication device is not active.

[Meaning] Confirmation message for terminating SSCom Client.

[Operation] Please click on "OK" button when you terminate SSCom Client.

SSCL802-I

Updated data has been applied to system.

[Meaning] Notification of content updates on SSCom Client Configuration.

[Operation] -

SSCL804-I

Are you sure to restore data as before?

[Meaning] Confirmation message for canceling the changes on Configuration.

[Operation] Please click on "OK" button when you cancel the changes on Configuration.

SSCL806-I

No access occurred within the specified period.

Password is required on next access. For security issue, you'd better to remove authentication device and store it in a different location from your PC when will not access continuously.

[Meaning] During setting period of "Watch Period", if there is no communication, when the network communication starts again, you need to enter your password.

To be safe, you might keep the authentication device somewhere away from the PC after it's pulled out. When the status in "Configuration" - "Authentication" - "Authentication Device" - "Password required again when no communication occurs during watch" is ON, the message will be displayed.

[Operation] To be safe, you might keep the authentication device somewhere away from the PC after it’s pulled out when the access ends.

SSCL808-I

Are you sure to delete specified certificate?

[Meaning] Confirmation message for deleting the certificate of Certificate Authority.

[Operation] Please click on "OK" button when you want to delete the certificate of Ceritficate Authority.

SSCL810-I

Are you sure to apply updated data to system?

[Meaning] Confirmation message for applying the settings in "Configuration" to SSCom Client.

[Operation] Please click on "OK" button when you need to save the changes.

SSCL812-I

Are you sure to delete specified server?

[Meaning] Confirmation message for deleting the selected VPN Server.

[Operation] Please click on "OK" button when you delete the selected server.

SSCL820-I

Authentication device is inserted.

For security issue, you'd better to remove authentication device and store it in a different location from your PC.

[Meaning] Safety message for pulling out authentication device when you exit Windows or SSCom Client.

[Operation] Please continue after you pull out the authentication device.

SSCL822-I

Password has been changed.

[Meaning] Confirmation message when password has been successfully changed.

[Operation] -

SSCL900-E

The password you entered doesn't match the registered one.
Please enter the right password for using the specified certificate.
Please note uppercase and lowercase letters are case sensitive.

[Meaning] Please enter the right password for specified certificate. Consider the following causes:

- ▪It is not the password of the specified certificate.
- ▪No password entered.
- ▪Wrong certificate has been chosen.

[Operation] Please enter the right password for specified certificate.

SSCL901-E

Specified file is not a certificate.

[Meaning] The file to be registered is not in the described format of certificate.

[Operation] Please specify a certificate with right format.

SSCL902-E

Registration failed.
Please make sure that the certificate you specified is correct.

[Meaning] Failed to register the certificate.
Consider the following causes:

- ▪Specified certificate file is incorrect.
- ▪There are some errors with the certificate.

[Operation] Please confirm if the specified certificate file is correct. If the problem is still unsolved after specifying the right certificate, send request to the system administrator for a new certificate, please try again after new certificate issued.

SSCL903-I

The certificate has already been registered.
Are you sure to overwrite?

[Meaning] Certificate has been registered.

[Operation] Please click on "OK" button when you need to overwrite the registered certificate.

SSCL904-I

Registration finished.

[Meaning] Confirmation message for successful registration.

[Operation] -

SSCL905-E

This tool is for Virtual IC Card only.

[Meaning] Setting of SSCom Client is for non-Virtual IC Card, so the user certificate management tool cannot be used.

[Operation] Please consult with system administrator.

SSCL910-E

The certificate has not been registered, so it cannot be deleted.

[Meaning] No certificate been installed, you cannot remove any certificate.

[Operation] -

SSCL911-I

Are you sure to delete the certificate?

[Meaning] Confirmation message for deleting certificate.

[Operation] Please click on "OK" button when you need to delete certificate.

SSCL912-I

The certificate has been deleted.

[Meaning] Certificate has been deleted.

[Operation] -

SSCL920-E

Please run the bat file as administrator to restart WFP service.

[Meaning] For Windows 8 / 8.1, you will need to restart the WFP service if you change the environment settings.

[Operation] Please run "ResetService.exe" as an administrator.

5. Troubleshooting

This chapter describes what to do when trouble occurs in using SSCom Client.

<Chapter Structure>

5.1 How to Deal with Trouble
5.2 Troubleshooting Measures
5.3 Log Information
5.4 Data need to be Collected when Trouble Occurs
5.5 How to Collect Data

5.1 How to Deal with Trouble

The following steps describe what to do when trouble occurred in using SSCom Client:

(1) Phenomenon Confirmation

Please confirm the following contents:

- ▪Phenomenon when the trouble occurred.
- ▪Message content (If there is a message output).

For details about the main causes and measures under corresponding messages, please refer to "4 Message".

(2) Data Collection

You need to collect necessary data to investigate on the main causes of the trouble, for details about needed data, please refer to "5.4 Data need to be Collected when Trouble Occurs".

(3) Problem Investigation

You can investigate on the main causes of the trouble according to the data collected, investigate the problem area and range.

5.2 Troubleshooting Measures

This section describes troubleshooting measures in using SSCom Client. When trouble occurred in using SSCom Client, please first check if the following phenomenon happened.

The following table shows the contents of the main troubles that occur with SSCom Client:

Table5.2-1 Trouble List

Types	Trouble Contents	Referring Section
Troubles with setup and service start-up	(1) SSCom Client failed to install. (2) SSCom Client failed to start. (3) VPN Settings in "Configuration" page cannot be modified. (4) SSCom Client failed to uninstall.	5.2.1
Troubles with Authentication Device	(1) Authentication device cannot be detected. (2) Authentication Media (USB) cannot be detected when using USB hub.	5.2.2
Troubles with VPN Communication	(1) "Use VPN Communication" of SSCom Client Menu is not active. (2) FTP cannot be used through VPN Communication.	5.2.3
Other troubles	(1) Authentication device be denied due to continuous password input failure. (2) Forget password. (3) Dialog box does not show up after clicking on "Change Password" menu. (4) Need to disable automatic start of SSCom Client when computer starts. (5) Need to enable automatic start of SSCom Client when computer starts. (6) Refer to FAQ for using support of SSCom.	5.2.4

5.2.1 Troubles with Setup and Service Start-up

The following shows how to deal with the trouble of setup or starting the service:

Table5.2.1-1 Troubles with setup and service start-up

#	Phenomenon
1	SSCom Client failed to install.
2	SSCom Client failed to start.
3	VPN Settings in "Configuration" page cannot be modified.
4	SSCom Client failed to uninstall.

(1)SSCom Client failed to install.

->Check if the work is done under Administrator permission.

(2)SSCom Client failed to start.

Causes and measures are described as below:

- Unstable running of Windows.
  ->Please restart Windows.
- SSCom Client has already been started.
  ->SSCom Client cannot be started for several times on the same PC. Check if SSCom Client has been started up from the icon of SSCom Client on Windows task tray.
- Necessary files for starting SSCom Client cannot be found.
  ->Please reinstall SSCom Client.

(3)VPN Settings in "Configuration" page cannot be modified.

Potential causes and measures are described as below:

- VPN Function is on.
  ->Right-click icon of SSCom Client on Windows task tray, click on "Stop SSCom Function" in the Menu displayed.

(4)SSCom Client failed to uninstall.

->Check if the work is done under Administrator permission.

5.2.2 Troubles with Authentication Device

Potential causes and measures to troubles with authentication device are shown as below:

Table5.2.2-1 Connection failure to server

#	Phenomenon
1	Authentication device cannot be detected.
2	Authentication Media (USB) cannot be detected when using USB hub.

(1)Authentication device cannot be detected.

Potential causes and measures are shown as below:

- Driver of the authentication device hasn't been installed.

->Please install the driver of authentication device.

- When eToken is used, light on the authentication device is still out.

->Possible poor contact of USB port. Please insert eToken again.

(2)Authentication Media (USB) cannot be detected when using USB hub.

- In using bus-powered USB hub, authentication device may not work properly for low power supply. Please use self-powered USB hub.

5.2.3 Troubles with VPN Communication

Potential causes and measures to troubles with VPN Communication are shown as below:

Table5.2.3-1 Troubles with VPN Communication

#	Phenomenon
1	"Use VPN Communication" of SSCom Client Menu is not active.
2	FTP cannot be used through VPN Communication.

(1)"Use VPN Communication" of SSCom Client Menu is not active.

->You have not registered any VPN Server (SSCom VPN/GAC Server).
Register a VPN Server on the "VPN" tab in "Configuration" page of SSCom Client.

(2)FTP cannot be used through VPN Communication.

->FTP only works in passive mode through VPN Communication.

5.2.4 Other Troubles

Table5.2.4-1 Other Troubles

#	Phenomenon
1	Authentication device is denied due to continuous password input failure.
2	Forget password.
3	Dialog box does not show up after clicking on "Change Password" menu (password cannot be changed).
4	Need to disable automatic start of SSCom Client when computer starts.
5	Need to enable automatic start of SSCom Client when computer starts.
6	Refer to FAQ for using support of SSCom.

(1)Authentication device is denied due to continuous password input failure.

->Register certificate by Certificate Writing Tool, Authentication device can be used again. Please contact the system administrator.

(2)Forget password.

->Please contact the system administrator.

(3)Dialog box does not show up after clicking on "Change Password" menu (password cannot be changed).

▪ SSCom Client has not been launched.

->Check if icon of SSCom Client is displayed on the task tray.

(4)Need to disable automatic start of SSCom Client when computer starts.

->Make sure "Run at the Windows startup" is configured to "No" when installing SSCom Client.

When installation completed, delete "SSCom Client" from Startup Menu of Windows.

(5)Need to enable automatic start of SSCom Client when computer starts.

->Make sure "Run at the Windows startup" is configured to "Yes" when installing SSCom Client.

When installation completed, add "SSCom Client" into Startup Menu of Windows.

(6)Refer to FAQ for using support of SSCom.

▪ Refer to FAQ for latest supporting information of SSCom on the Internet.

Questions and answers on SSCom products are consolidated to Q&A.

If you can't find solutions in manual when trouble occurs or need to read the latest Q&A, you are welcome to link to this website.

-> http://www.hitachi-systems.com/solution/s002/sscom/faq.html

5.3 Log Information

There are two kinds of log outputted when using SSCom Client.

▪Message log

▪Trace log

This section describes the two kinds of log.

5.3.1 Message Log

Message log is the log information to notify the trouble. The messages outputted by SSCom Client are collected by time series order.

5.3.2 Trace Log

Trace log is the log information that is collected to analyze how the trouble occurred when trouble occurs or to measure processing time of each process.

5.4 Data need to be collected when Trouble Occurs

If problems cannot be solved using measures introduced in "5.2 Troubleshooting Measures", please collect related data to investigate cause of the trouble and contact the system administrator. This section deals on data need to be collected when trouble occurs.

(1) Information on SSCom Client

You need to collect the following data related with SSCom Client. You also need collect the files on the target PC when network connection trouble occurs. Necessary information on SSCom Client is shown below:

Table5.4-1 Necessary information needs to be collected with SSCom Client

Information Type	Summary	Default File Name
Version information	Release Number.	-
Message log	Message information of SSCom Client.	Install destination folder\SSCom Client\client_message.log
Trace log	Program trace log of SSCom Client.	Install destination folder\SSCom Client\client_trace.log

(2) Operation Procedure

The necessary information about operation procedure when the trouble occurred is shown below:

- ▪Detailed operation procedure.
- ▪The happen time of trouble.
- ▪Machine Configuration (OS version, host name, system configuration of SSCom Client and SSCom Server).
- ▪Whether the trouble can be reproduced.

(3) Error message on the screen

Please collect the following screen hard copy:

- ▪Screen hard copy of each tag in "Configuration" dialog.
- ▪Screen hard copy of error message dialog box.

(4) Power status of the authentication device

Check if the lamp of the authentication device (eToken or card reader) is on.

5.5 How to Collect Data

(1) Confirm Operation Procedures

Please confirm the operation procedures.

Please check the operation procedures when trouble occurred and record it. Information needed to be confirmed is shown as below:

- ▪Detailed operation procedure.
- ▪Happen time of trouble.
- ▪Machine Configuration (OS version and so on).
- ▪Whether the trouble can be reproduced.

(2) Collect error messages on the screen

Please collect the screen hard copy of error message dialog box.

Appendix1. SSCom Interview for Problem Solving

<table>
<tr><td>Occurrence Date</td><td></td><td>Acceptance Date</td><td></td></tr>
<tr><td>Trouble Occurred Customer Name</td><td></td><td>Declaration Customer Name</td><td></td></tr>
<tr><td>SSCom VPN Server Version</td><td></td><td>OS Version</td><td></td></tr>
<tr><td>SSCom GAC Server Version</td><td></td><td>OS Version</td><td></td></tr>
<tr><td>SSCom AP Server Version</td><td></td><td>OS Version</td><td></td></tr>
<tr><td>SSCom Client Version</td><td></td><td rowspan="2">OS Version</td><td rowspan="2"></td></tr>
<tr><td>Client PC (Maker, Model)</td><td></td></tr>
<tr><td colspan="4">Phenomenon (Try to fill in as much detail as possible)

<<Sample>>
No permission to access problem till yesterday, since this morning access failed as the SSCom Client showed XXXX information. Other computers have also met the same situation. Access denied even using IC card.
Successful access can be realized when using other user card on the problem computer.</td></tr>
<tr><td>Recurrence/No recurrence</td><td colspan="3">(Yes or No) Steps to reproduce</td></tr>
<tr><td rowspan="4">Acquisition information (Message/Log)</td><td>Message of SSCom Client</td><td colspan="2"></td></tr>
<tr><td>Access log of SSCom GAC Server</td><td colspan="2"></td></tr>
<tr><td>System log of OS</td><td colspan="2"></td></tr>
<tr><td>Watson Doctor log (Windows Only)
Output File:
{System Folder}\drwtsn.log</td><td colspan="2">Output/No output
File size: ( )</td></tr>
<tr><td>Core document (Solaris only)
Output File:
{Install Directory}/bin/core</td><td colspan="2">Output/No output
File size: ( )</td></tr>
</table>

<table>
<tr><td colspan="2">Host AP
(Name, Version)</td><td colspan="2"></td></tr>
<tr><td rowspan="4">Authentication Device Type</td><td>IC Card</td><td colspan="2">FeliCa, Cryptoflex, Multos, Tosmart or others ( )</td></tr>
<tr><td>Card reader</td><td colspan="2">Maker, Machine Type, Connection Type (USB, Serial, PC Card, FD)
( )</td></tr>
<tr><td>USB Token</td><td colspan="2">eToken PRO, StarKey100, else ( )</td></tr>
<tr><td>Fingerprint Authentication Device</td><td colspan="2">Puppy, else ( )</td></tr>
<tr><td colspan="3">No Authentication Device (Virtual IC card)</td></tr>
<tr><td colspan="4"><Principal Receptionist></td></tr>
<tr><td>Department</td><td></td><td>Name</td><td></td></tr>
<tr><td>TEL (public)</td><td></td><td>TEL (inner line)</td><td></td></tr>
<tr><td>e-mail</td><td></td><td>FAX</td><td></td></tr>
<tr><td colspan="4"><Remarks></td></tr>
</table>

Not all items need to be filled in, you can fill in the contents you know. Earlier reply can be acquired if information provided is as detailed as possible.

July. 2014, 9th Edition.