

# Installation

IM 32Q01C50-31E

---

**vigilantplant<sup>®</sup>**

---

# Introduction

This manual describes the procedure for setting up ProSafe-RS.

When you integrate ProSafe-RS with FAST/TOOLS, replace "Vnet/IP" in the descriptions in this manual with "Vnet/IP-Upstream."

This manual consists of the following parts:

- Part A: Overview  
This part provides an overview of ProSafe-RS setup.
- Part B: New Setup  
This part describes the procedure for a new setup of ProSafe-RS.
- Part C: Maintenance  
This part describes the tasks to be done while a ProSafe-RS system is used.
- Part D: Connection with Other Products  
This part describes how to connect ProSafe-RS to other YOKOGAWA products and provides cautionary notes.
- Appendix  
This section describes hardware settings, compatibility of ProSafe-RS software revisions, and cautionary notes.

# Safety Precautions for Use

## ■ Safety, Protection, and Modification of the Product

- To protect the system controlled by the Product and the Product itself and to ensure safe operation, please observe the safety precautions described in this Manual. Yokogawa Electric Corporation ("YOKOGAWA") assumes no liability for safety if users fail to observe the safety precautions and instructions when operating the Product.
- If the Product is used in a manner not specified in the User's Manuals, the protection provided by the Product may be impaired.
- If any protection or safety circuit is required for the system controlled by the Product or for the Product itself, please install it externally.
- Use only spare parts that are approved by YOKOGAWA when replacing parts or consumables of the Product.
- Do not use the Product and its accessories such as power cords on devices that are not approved by YOKOGAWA. Do not use the Product and its accessories for any purpose other than those intended by YOKOGAWA.
- Modification of the Product is strictly prohibited.
- The following symbols are used in the Product and User's Manuals to indicate the accompanying safety precautions:



Indicates that caution is required for operation. This symbol is labeled on the Product to refer the user to the User's Manuals for necessary actions or behaviors in order to protect the operator and the equipment against dangers such as electric shock. In the User's Manuals, you will find the precautions necessary to prevent physical injury or death, which may be caused by accidents, such as electric shock resulting from operational mistakes.



Identifies a protective conductor terminal. Before using the Product, you must ground the protective conductor terminal to avoid electric shock.



Identifies a functional grounding terminal. A terminal marked "FG" also has the same function. This terminal is used for grounding other than protective grounding. Before using the Product, you must ground this terminal.



Indicates an AC supply.



Indicates a DC supply.



Indicates the ON position of a power on/off switch.



Indicates the OFF position of a power on/off switch.

## ■ Notes on Handling User's Manuals

- Hand over the User's Manuals to your end users so that they can keep the User's Manuals on hand for convenient reference.
- Thoroughly read and understand the information in the User's Manuals before using the Product.
- For the avoidance of doubt, the purpose of the User's Manuals is not to warrant that the Product is suitable for any particular purpose but to describe the functional details of the Product.
- Contents of the User's Manuals are subject to change without notice.

- 
- Every effort has been made to ensure the accuracy of contents in the User's Manuals. However, should you have any questions or find any errors, contact us or your local distributor. The User's Manuals with unordered or missing pages will be replaced.

## ■ Warning and Disclaimer

- Except as specified in the warranty terms, YOKOGAWA shall not provide any warranty for the Product.
- YOKOGAWA shall not be liable for any indirect or consequential loss incurred by either using or not being able to use the Product.

## ■ Notes on Software

- YOKOGAWA makes no warranties, either expressed or implied, with respect to the Software Product's merchantability or suitability for any particular purpose, except as specified in the warranty terms.
- Purchase the appropriate number of licenses of the Software Product according to the number of computers to be used.
- No copy of the Software Product may be made for any purpose other than backup; otherwise, it is deemed as an infringement of YOKOGAWA's Intellectual Property rights.
- Keep the software medium of the Software Product in a safe place.
- No reverse engineering, reverse compiling, reverse assembling, or converting the Software Product to human-readable format may be performed for the Software Product.
- No part of the Software Product may be transferred, converted, or sublet for use by any third-party, without prior written consent from YOKOGAWA.

# Documentation Conventions

## ■ Symbols

The following symbols are used in the User's Manuals.



**CAUTION**

Identifies instructions that must be observed to avoid physical injury, electric shock, or death.



**WARNING**

Identifies instructions that must be observed to prevent damage to the software or hardware, or system failures of the Product.



**IMPORTANT**

Identifies important information required to understand operations or functions.

**TIP**

Identifies additional information.

**SEE  
ALSO**

Identifies referenced content.

In online manuals, you can view the referenced content by clicking the links that are in green text. However, this action does not apply to the links that are in black text.

## ■ Typographical Conventions

The following typographical conventions are used throughout the User's Manuals.

### ● Commonly Used Conventions throughout the User's Manuals

- **Δ Mark**  
Indicates that a space must be entered between character strings.  
**Example:**

```
.ALΔPIC010Δ-SC
```

- **Character string enclosed by braces { }**  
Indicates character strings that may be omitted.

**Example:**

```
.PRΔTAG{Δ.sheet name}
```

### ● Conventions Used to Show Key or Button Operations

- **Characters enclosed by brackets [ ]**  
When characters are enclosed by brackets in the description of a key or button operation, it indicates a key on the keyboard, a button name in a window, or an item in a list box displayed in a window.

**Example:**

To alter the function, press the [ESC] key.

### ● Conventions of a User-defined Folder

- **User-defined folder name enclosed by parenthesis ( )**  
User definable path is written in a pair of parentheses.

**Example:**

```
(RS Project Folder)\SCS0101
```

If the RS Project Folder is C:\MYRSPJT, the above path becomes C:\MYRSPJTSCS0101.

## ■ Drawing Conventions

Drawings used in the User's Manuals may be partially emphasized, simplified, or omitted for the convenience of description.

Drawings of windows may be slightly different from the actual screenshots with different settings or fonts. The difference does not hamper the understanding of basic functionalities and operation and monitoring tasks.

## ■ Integration with CENTUM

The Product can be integrated with CENTUM VP or CENTUM CS 3000. In the User's Manuals, the integration with CENTUM VP or CENTUM CS 3000 is referred to as "Integration with CENTUM."

In the User's Manuals, the explanations for integrating the Product with CENTUM VP or CENTUM CS 3000, the glossary for various features of CENTUM VP is used instead of the glossary for CENTUM CS 3000. For example, the term "CENTUM VP System Alarm View" is used instead of "CENTUM CS 3000 System Alarm window." Nevertheless, if the features for integrating the Product with CENTUM VP and CENTUM CS 3000 are different, both features will be explained separately.

### SEE ALSO

For more information about the functions and usage of CENTUM VP components for integrating the Product with CENTUM VP, refer to:

User's Manuals (IM), Technical Information (TI), and General Specifications (GS) of CENTUM VP

For more information about the features and usage of CENTUM CS 3000 components for integrating the Product with CENTUM CS 3000, refer to:

User's Manuals (IM), Technical Information (TI), and General Specifications (GS) of CENTUM CS 3000

## ■ Explanation of Hardware and Software Behaviors in the User's Manuals

In the User's Manuals, system behaviors are explained assuming that the latest versions of YOKOGAWA software and hardware at the time of publication of the User's Manuals are installed.

If additional precise information about the safety of legacy versions of software or hardware is required, a link to the corresponding explanation is provided. Please refer to the information according to your system.

## ■ Station Types

A safety control station (hereafter referred to as SCS) is named according to the type of the safety control unit used in it.

**Table Info-1 Names of SCS and Safety Control Unit Used**

Name of SCS	Model of the safety control unit
SCSV1-S	SSC10S/SSC10D
SCSP1-S	SSC50S/SSC50D
SCSP2-S	SSC60S/SSC60D
SCSU1-S	SSC57S/SSC57D

In the User's Manuals, the following abbreviations may be used to describe functions of these SCS as a whole.

- SCSV1: Abbreviation of SCSV1-S
- SCSP1: Abbreviation of SCSP1-S
- SCSP2: Abbreviation of SCSP2-S
- SCSU1: Abbreviation of SCSU1-S

---

# Copyright and Trademark Notices

## ■ All Rights Reserved

The copyright of the programs and online manuals contained in the software medium of the Software Product shall remain with YOKOGAWA.

You are allowed to print the required pages of the online manuals for the purposes of using or operating the Product; however, reprinting or reproducing the entire document is strictly prohibited by the Copyright Law.

Except as stated above, no part of the online manuals may be reproduced, transferred, sold, or distributed to a third party in any manner (either in electronic or written form including, without limitation, in the forms of paper documents, electronic media, and transmission via the network). Nor it may be registered or recorded in the media such as films without permission.

## ■ Trademark Acknowledgments

- CENTUM, ProSafe, Vnet/IP, and STARDOM are registered trademarks of YOKOGAWA.
- Microsoft, Windows, Windows Vista, Windows Server, Visual Basic, Visual C++, and Visual Studio are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.
- Adobe, Acrobat, and Adobe Reader are registered trademarks of Adobe Systems Incorporated.
- Ethernet is a registered trademark of Xerox Corporation.
- HART is a registered trademark of the HART Communication Foundation.
- Modicon and Modbus are registered trademarks of Schneider Electric SA.
- All other company and product names mentioned in the User's Manuals are trademarks or registered trademarks of their respective companies.
- TM or ® mark are not used to indicate trademarks or registered trademarks in the User's Manuals.
- Logos and logo marks are not used in the User's Manuals.



Installation

IM 32Q01C50-31E 4th Edition

CONTENTS

**PART-A Overview.....A-1**

**A1. How to Read This Document..... A1-1**

**A2. Overview of Setup Tasks.....A2-1**

**A2.1 Before You Set Up.....A2-2**

**A2.2 Procedures for New Setup..... A2-3**

A2.2.1 Setup Procedure for a ProSafe-RS System.....A2-4

A2.2.2 Setup Procedure for SENG.....A2-6

A2.2.3 Setup Procedure for a File Server..... A2-9

A2.2.4 Setup Procedure for a Computer Dedicated to License Management  
..... A2-10

**A2.3 Explanation for Maintenance..... A2-11**

**A3. Requirements for Operation..... A3-1**

**A3.1 Hardware Requirements.....A3-2**

**A3.2 Software Requirements..... A3-3**

# Installation

IM 32Q01C50-31E 4th Edition

## CONTENTS

<b>PART-B</b>	<b>New Setup.....</b>	<b>B-1</b>
<b>B1.</b>	<b>Preparing for the Setup.....</b>	<b>B1-1</b>
<b>B2.</b>	<b>Setting Up the Windows Domain Environment.....</b>	<b>B2-1</b>
B2.1	Overview of Setting Up the Domain Environment.....	B2-2
B2.2	Configuring the Domain Controller (Windows Server 2008/Windows Server 2008 R2).....	B2-3
B2.3	Configuring Security Settings for the Domain Controller.....	B2-5
B2.4	Creating Domain Users.....	B2-9
B2.5	Adding Client Computers to the Domain.....	B2-13
B2.6	Setting Up Redundant Domain Controllers.....	B2-18
B2.7	Setting Up Time Synchronization in Windows Domain Environment.....	B2-19
B2.7.1	Implementing Time Synchronization in a System Consisting of Only ProSafe-RS.....	B2-20
B2.7.2	Implementing Time Synchronization When Integrated with CENTUM.....	B2-23
<b>B3.</b>	<b>Setting Up the SENG.....</b>	<b>B3-1</b>
B3.1	Setting Up the Hardware.....	B3-2
B3.2	Setting Up Windows.....	B3-7
B3.2.1	Configuring on Windows 7.....	B3-8
B3.2.2	Configuring on Windows Vista.....	B3-15
B3.2.3	Configuring on Windows Server 2008 R2.....	B3-21
B3.2.4	Configuring on Windows Server 2008.....	B3-27
B3.3	Configuring Network Settings.....	B3-32
B3.3.1	Installing the Control Bus Driver.....	B3-33
B3.3.2	Installing the Vnet/IP Open Communication Driver.....	B3-35
B3.3.3	Configuring Windows Network Settings.....	B3-37
B3.4	Installing the ProSafe-RS Software.....	B3-54
B3.5	Configuring IT Security Settings.....	B3-58
B3.5.1	IT Security Tool.....	B3-59
B3.5.2	Running the IT Security Tool.....	B3-62
B3.6	Distributing and Accepting Licenses.....	B3-67
B3.7	Creating User Accounts.....	B3-68

	B3.7.1	When the Standard Model with Standalone Management Security Settings are Applied.....	B3-69
	B3.7.2	When the Legacy Model of Security Settings are Applied.....	B3-71
<b>B3.8</b>		<b>Configuring Windows Environment Settings for Each User.....</b>	<b>B3-72</b>
	B3.8.1	Configuring on Windows 7.....	B3-73
	B3.8.2	Configuring on Windows Vista.....	B3-76
	B3.8.3	Configuring on Windows Server 2008 R2.....	B3-78
	B3.8.4	Configuring on Windows Server 2008.....	B3-81
<b>B3.9</b>		<b>Configuring the Uninterruptible Power Supply (UPS) Service.....</b>	<b>B3-83</b>
<b>B4.</b>		<b>Configuring Function-Specific Settings on SENG.....</b>	<b>B4-1</b>
	B4.1	Online Manual Setting.....	B4-2
	B4.2	Settings of Project Database Folder.....	B4-3
	B4.3	Settings for Message Cache Tool.....	B4-4
	B4.4	Settings Required for OPC Communication.....	B4-5
	B4.5	Setup when Using the Access Control and Operation History Management Package.....	B4-6
	B4.5.1	Setup Procedure when Using Access Control and Operation History Management Functions.....	B4-8
	B4.5.2	Security Settings for the Operation History Database.....	B4-9
<b>B5.</b>		<b>Setting Up a File Server.....</b>	<b>B5-1</b>
	B5.1	Setting Up a Computer that Serves Only as a File Server.....	B5-2
	B5.2	Setting Up the File Server Function on SENG.....	B5-8
	B5.3	Setting Up the Computer that Serves as Both File Server and License Management Station.....	B5-9
<b>B6.</b>		<b>Setting Up the Computer Dedicated to License Management.....</b>	<b>B6-1</b>
<b>B7.</b>		<b>Configuring the Hardware of SCS and Devices for Connection between Domains.....</b>	<b>B7-1</b>
<b>B8.</b>		<b>Installing the Functions that Operate with CENTUM VP Licenses.....</b>	<b>B8-1</b>

# Installation

IM 32Q01C50-31E 4th Edition

## CONTENTS

<b>PART-C</b>	<b>Maintenance.....</b>	<b>C-1</b>
<b>C1.</b>	<b>Adding Licenses and Changing License Assignments.....</b>	<b>C1-1</b>
C1.1	Adding a License.....	C1-2
C1.2	Changing License Assignments.....	C1-3
<b>C2.</b>	<b>Setting Up the Windows Domain Environment Later.....</b>	<b>C2-1</b>
<b>C3.</b>	<b>Backing Up the System.....</b>	<b>C3-1</b>
<b>C4.</b>	<b>Upgrading the ProSafe-RS Software.....</b>	<b>C4-1</b>
C4.1	Installation for Upgrading.....	C4-2
C4.2	Settings after Upgrading ProSafe-RS Software.....	C4-5
C4.3	Upgrading the Computer Dedicated to License Management.....	C4-10
<b>C5.</b>	<b>Upgrading to R3.02.20.....</b>	<b>C5-1</b>
<b>C6.</b>	<b>Uninstalling the ProSafe-RS Software.....</b>	<b>C6-1</b>
C6.1	Uninstallation on SENG.....	C6-2
C6.1.1	Uninstalling the ProSafe-RS Software.....	C6-3
C6.1.2	Uninstalling the Network Drivers.....	C6-5
C6.2	Uninstallation on the computer Dedicated to License Management.....	C6-7
<b>C7.</b>	<b>Reinstalling the ProSafe-RS Software.....</b>	<b>C7-1</b>
C7.1	When the Computer Used is the Same.....	C7-2
C7.2	When the Computer Used is Not the Same.....	C7-6
<b>C8.</b>	<b>Maintenance Tasks Related to IT Security.....</b>	<b>C8-1</b>
C8.1	Changing the IT Security Settings.....	C8-2
C8.1.1	Procedures for SENG PC.....	C8-3
C8.1.2	Procedures for a File Server or Domain Controller.....	C8-5
C8.2	Saving the IT Security Settings.....	C8-8
C8.2.1	Procedure for SENG PC.....	C8-9
C8.2.2	Procedure for a File Server or Domain Controller.....	C8-12
C8.3	Restoring the IT Security Settings.....	C8-13
C8.3.1	Procedure for SENG PC.....	C8-14
C8.3.2	Procedure for a File Server or Domain Controller.....	C8-16
C8.4	Changing the Security Setting File Password.....	C8-17
C8.4.1	Procedures for SENG PC.....	C8-18

	C8.4.2	Procedure for a File Server or Domain Controller.....	C8-20
<b>C9.</b>		<b>Troubleshooting.....</b>	<b>C9-1</b>
<b>C9.1</b>		<b>Windows Related Troubleshooting.....</b>	<b>C9-2</b>
<b>C9.2</b>		<b>Troubleshooting Related to Network.....</b>	<b>C9-3</b>
	C9.2.1	Precaution on Network Cable Connection.....	C9-4
	C9.2.2	Problems Related to Installation and Deletion of Drivers.....	C9-5

# Installation

IM 32Q01C50-31E 4th Edition

## CONTENTS

### PART-D Connection with Other Products..... D-1

#### D1. Connecting YOKOGAWA products..... D1-1

##### D1.1 CENTUM VP and ProSafe-RS.....D1-3

D1.1.1 CENTUM VP Standard Operation and Monitoring Function and ProSafe-RS Safety System Generation and Maintenance Function Package.....D1-4

D1.1.2 CENTUM VP Standard Operation and Monitoring Function and ProSafe-RS SOE OPC Interface Package..... D1-5

D1.1.3 CENTUM VP System Builder Function and ProSafe-RS CENTUM VP/CS 3000 Integration Engineering Package.....D1-9

D1.1.4 CENTUM VP System Builder Function and ProSafe-RS Safety System Generation and Maintenance Function Package.....D1-10

D1.1.5 Required Settings when Integrating with CENTUM VP R4.01 to R4.03.....D1-11

D1.1.6 Required Settings when Integrating with CS 3000 R3.06 to R3.09.....D1-12

##### D1.2 ProSafe-RS and PRM..... D1-13

D1.2.1 SOE OPC Interface Package and PRM Server..... D1-14

##### D1.3 ProSafe-RS and Exaquantum..... D1-16

D1.3.1 ProSafe-RS SOE OPC Interface Package and Exaquantum PIMS Server..... D1-17

# Installation

IM 32Q01C50-31E 4th Edition

## CONTENTS

### Appendix

<b>Appendix 1. Setting Switches.....</b>	<b>App.1-1</b>
<b>Appendix 2. Procedure for Erasing VI702 Internal Settings.....</b>	<b>App.2-1</b>
<b>Appendix 3. Antistatic Precautions When Handling Hardware.....</b>	<b>App.3-1</b>
<b>Appendix 4. Compatibility between Revisions and Cautionary Notes for Upgrading.....</b>	<b>App.4-1</b>
<b>Appendix 4.1 Upgrading to R1.01.30.....</b>	<b>App.4-2</b>
<b>Appendix 4.2 Upgrading to R1.01.40/R1.01.50.....</b>	<b>App.4-6</b>
<b>Appendix 4.3 Upgrading to R1.02.....</b>	<b>App.4-8</b>
<b>Appendix 4.4 Upgrading to R1.03.....</b>	<b>App.4-11</b>
<b>Appendix 4.5 Upgrading to R2.01.....</b>	<b>App.4-15</b>
<b>Appendix 4.6 Upgrading to R2.02.....</b>	<b>App.4-17</b>
Appendix 4.6.1 Cautionary Notes for Upgrading.....	App.4-18
Appendix 4.6.2 Compatibility with Earlier Revisions.....	App.4-20
<b>Appendix 4.7 Upgrading to R2.03.....</b>	<b>App.4-22</b>
Appendix 4.7.1 Cautionary Notes for Upgrading.....	App.4-24
Appendix 4.7.2 Compatibility with Earlier Revisions.....	App.4-26
<b>Appendix 4.8 Upgrading to Version R3.01.....</b>	<b>App.4-29</b>
Appendix 4.8.1 Cautionary Notes for Upgrading.....	App.4-30
Appendix 4.8.2 Compatibility with Earlier Revisions.....	App.4-31
<b>Appendix 4.9 Upgrading to Version R3.02.00.....</b>	<b>App.4-36</b>
Appendix 4.9.1 Cautionary Notes for Upgrading.....	App.4-37
<b>Appendix 4.10 Upgrading to R3.02.10.....</b>	<b>App.4-39</b>
Appendix 4.10.1 Cautionary Notes for Upgrading.....	App.4-40
Appendix 4.10.2 Compatibility with Earlier Revisions.....	App.4-41

# A. Overview

This section explains how to read this document, types of ProSafe-RS setup tasks and their workflows, and system requirements.



# A1. How to Read This Document

This document explains the setup procedures for the ProSafe-RS software. This document does not touch upon installation procedures of Windows OS, related service packs, and Microsoft security patches.

To use the software packages installed on an SENG, licenses must be distributed to and activated on the SENG using a program called License Manager. Procedures for the tasks performed using License Manager is described in the License Management IM. You are guided to refer to the License Management IM as necessary in the explanation of setup procedures.

You are also guided to refer to the Security Guide IM for information about functions that reinforce security of the system.

## SEE ALSO

For more information about the procedure for installing the Windows operating systems, related service packs and the Microsoft security patches, refer to:

the information provided by Microsoft

For more information about Microsoft security patches, refer to:

Microsoft Security Update Policy (TI 33Y01B30-02E)

For more information about the procedure for distributing and activating the licenses on the stations, refer to:

1., "Overview of license management" in License Management (IM 32Q01C60-31E)

For more information about system security, refer to:

1., "Overview" in ProSafe-RS Security Guide (IM 32Q01C70-31E)

## ■ Structure of This Document

This document consists of the following parts:

- Part A: Overview

This part describes how to read this document, various types of ProSafe-RS setup tasks along with their workflows, and hardware and software requirements.

- Part B: New Setup

This part explains the procedures for setting up each station.

- Part C: Maintenance

This part describes maintenance tasks that are required after the stations have been set up and went into operation.

- Part D: Connection with Other Products

This part describes the required settings when connecting ProSafe-RS with other YOKOGAWA products, such as CENTUM VP, PRM, and Exaquantum.

## ■ Regarding Explanation of Setup Procedures

The procedure for setting up Windows and device drivers vary with the Windows operating systems. For the procedure that are common to all the operating systems that are supported, the explanation will mainly use the user interfaces of Windows 7. However, for the procedures typical for each operating system, the explanation will use the user interfaces of each system and describe the procedure separately.

---

## A2. Overview of Setup Tasks

This section describes the workflows of setup tasks and provides the information you should understand before you set up individual stations.

## A2.1 Before You Set Up

This section describes the relationship between installation of ProSafe-RS software and licensing for it.

### ■ Installation and Licensing of Software Packages

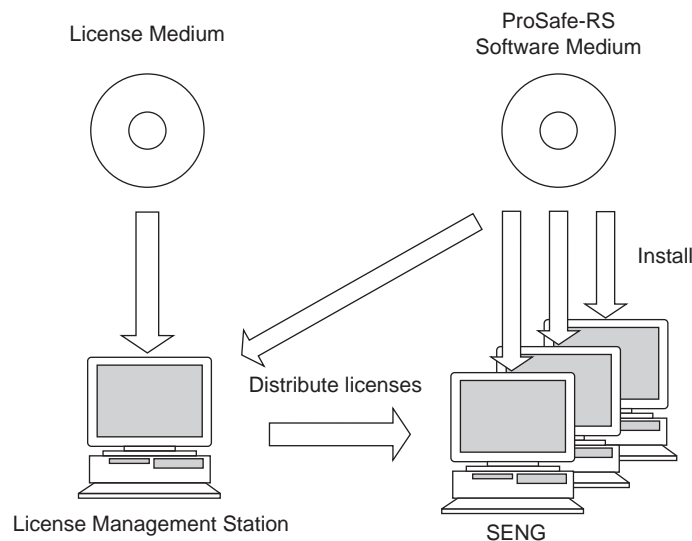
In order to use ProSafe-RS software packages, it is necessary to install the ProSafe-RS software on a computer and then grant licenses to the computer to enable the use of the software packages.

The tasks of installing the software packages on each computer are performed using a program called an installer. The tasks of giving licenses are executed using software called License Manager. License Manager is automatically installed when the ProSafe-RS software is installed on a computer.

Among computers installed with License Manager, the computer that is given the role of managing licenses of each computer in the system is called the license management station. The license management station distributes licenses to each computer on which the software packages are installed. On a computer to which licenses have been distributed, the software packages can be made available for use by accepting the distributed licenses.

#### TIP

It is possible to install only License Manager on a computer and use it as the computer dedicated to license management.



**Figure A2.1-1 License Distribution**

#### SEE ALSO

For more information about the details of licenses, refer to:

1., "Overview of license management" in License Management (IM 32Q01C60-31E)

---

## **A2.2 Procedures for New Setup**

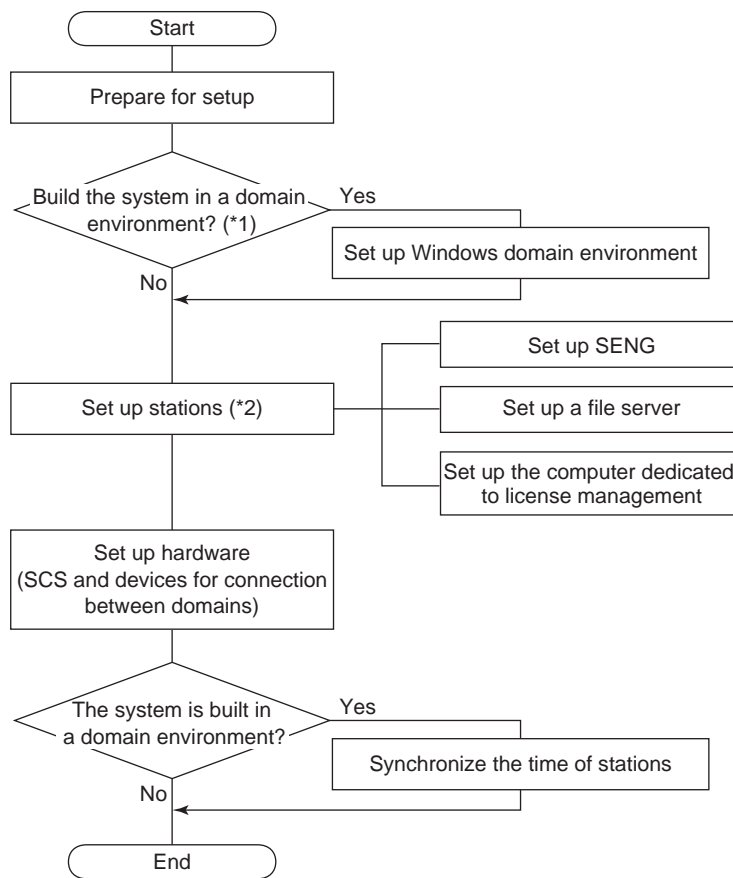
This section describes the overall procedures for setting up a ProSafe-RS system and for setting up each type of station or computer using flowcharts.

The procedures for the following types of stations and computers are described.

- Safety engineering PC (SENG)
- File server
- Computer dedicated to license management

## A2.2.1 Setup Procedure for a ProSafe-RS System

The following figure shows the overall procedure for setting up a ProSafe-RS system.



\*1: You may set up the domain environment at a later stage.

\*2: Start by setting up the station that is to be used as the license management station.

**Figure A2.2.1-1 Setup Procedure for a ProSafe-RS System**

You can jump to the explanation of each task that appears in the flowchart from the reference link that is provided in the following subsections.

### ■ Prepare for Setup

Determine the required items for setting up a ProSafe-RS system.

**SEE  
ALSO**

For more information about the items that must be determined before setting up a ProSafe-RS system, refer to:

[B1., "Preparing for the Setup" on page B1-1](#)

### ■ Set Up the Windows Domain Environment

When using ProSafe-RS in a Windows domain environment, set up the Windows domain environment. You may also set up the Windows domain environment at a later stage.

**SEE  
ALSO**

For more information about setting up a Windows domain environment, refer to:

[B2., "Setting Up the Windows Domain Environment" on page B2-1](#)

## ■ Set Up Each Station

Set up SENG, file server, and other stations to be used in the ProSafe-RS system.

**SEE  
ALSO**

For more information about the procedure for setting up an SENG, refer to:

[A2.2.2, "Setup Procedure for SENG" on page A2-6](#)

For more information about the procedure for setting up a file server, refer to:

[A2.2.3, "Setup Procedure for a File Server" on page A2-9](#)

For more information about the procedure for setting up a computer dedicated to license management, refer to:

[A2.2.4, "Setup Procedure for a Computer Dedicated to License Management" on page A2-10](#)

### ● The Station You Must Set Up First

In a ProSafe-RS system, you must first set up the license management station, which is used to grant licenses for software packages.

Software packages installed on other stations become available for use once the stations accept the licenses distributed from the license management station.

## ■ Set Up the Hardware of SCS and Devices Used for Connection between Domains

Set up the hardware of SCS and devices used for connection between domains.

**SEE  
ALSO**

For more information about setting up the hardware of SCS and devices for connection between domains, refer to:

[B7., "Configuring the Hardware of SCS and Devices for Connection between Domains" on page B7-1](#)

## ■ Set Up Time Synchronization in Windows Domain Environment

When using ProSafe-RS in a Windows domain environment, synchronize the time on the domain controller with the time on computers used in the ProSafe-RS system.

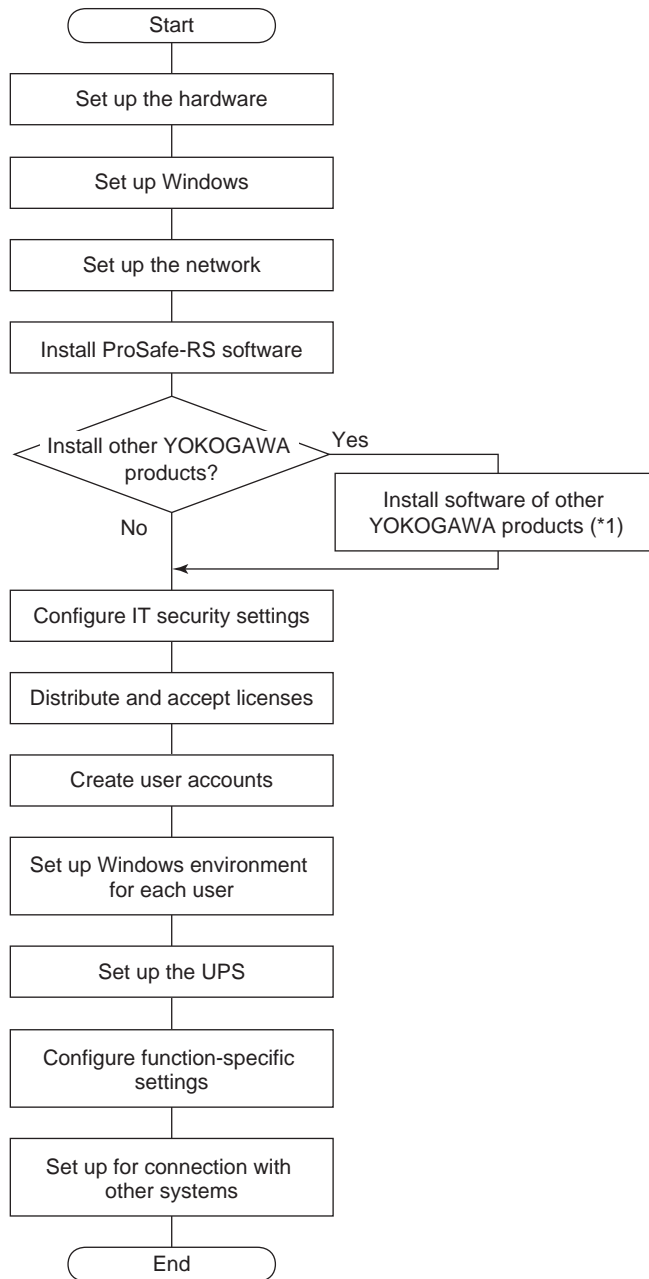
**SEE  
ALSO**

For more information about setting up time synchronization in a Windows domain environment, refer to:

[B2.7, "Setting Up Time Synchronization in Windows Domain Environment" on page B2-19](#)

## A2.2.2 Setup Procedure for SENG

The following figure shows the setup procedure for SENG.



\*1: You may install other products later. If you install later, you need to configure IT security settings again.

**Figure A2.2.2-1 Setup Procedure for SENG**

You can jump to the explanation of each task that appears in the flowchart from the reference link that is provided in the following subsections.

### ■ Set Up the Hardware

Set up the hardware for the SENG.

---

**SEE ALSO** For more information about setting up the hardware of SENG, refer to:

[B3.1, "Setting Up the Hardware" on page B3-2](#)

---

## ■ Set Up Windows

Configure Windows settings on the computer.

---

**SEE ALSO** For more information about setting up Windows, refer to:

[B3.2, "Setting Up Windows" on page B3-7](#)

---

## ■ Set Up the Network

Configure the network settings.

---

**SEE ALSO** For more information about configuring network settings, refer to:

[B3.3, "Configuring Network Settings" on page B3-32](#)

---

## ■ Install the ProSafe-RS Software

Install the ProSafe-RS software.

---

**SEE ALSO** For more information about installing the ProSafe-RS software, refer to:

[B3.4, "Installing the ProSafe-RS Software" on page B3-54](#)

---

## ■ Configure IT Security Settings

Configure IT security settings.

---

**SEE ALSO** For more information about configuring IT security settings, refer to:

[B3.5, "Configuring IT Security Settings" on page B3-58](#)

---

## ■ Distribute and Accept Licenses

Distribute licenses to the SENG from the license management station, and accept the licenses on the SENG.

---

**SEE ALSO** For more information about distributing and accepting licenses, refer to:

[B3.6, "Distributing and Accepting Licenses" on page B3-67](#)

---

## ■ Create User Accounts

Create user accounts.

---

**SEE ALSO** For more information about creating user accounts, refer to:

[B3.7, "Creating User Accounts" on page B3-68](#)

---

## ■ Configure Windows Environment Settings for Each User

Configure Windows environment settings for each user.



**SEE  
ALSO**

---

For more information about configuring Windows environment settings for each user, refer to:  
[B3.8, "Configuring Windows Environment Settings for Each User" on page B3-72](#)

---

## ■ Set Up the Uninterruptible Power Source (UPS) Service

If necessary, set up the uninterruptible power source (UPS) service.

**SEE  
ALSO**

---

For more information about configuring the UPS service, refer to:  
[B3.9, "Configuring the Uninterruptible Power Supply \(UPS\) Service" on page B3-83](#)

---

## ■ Configure Function-Specific Settings

Configure the settings specific to certain functions of the SENG.

**SEE  
ALSO**

---

For more information about configuring the settings specific to each function of SENG, refer to:  
[B4., "Configuring Function-Specific Settings on SENG" on page B4-1](#)

---

## ■ Set Up for Connection with Other Systems

As necessary, set up for connection with other YOKOGAWA products.

**SEE  
ALSO**

---

For more information about the settings required to connect with other YOKOGAWA products, refer to:  
[D1., "Connecting YOKOGAWA products" on page D1-1](#)

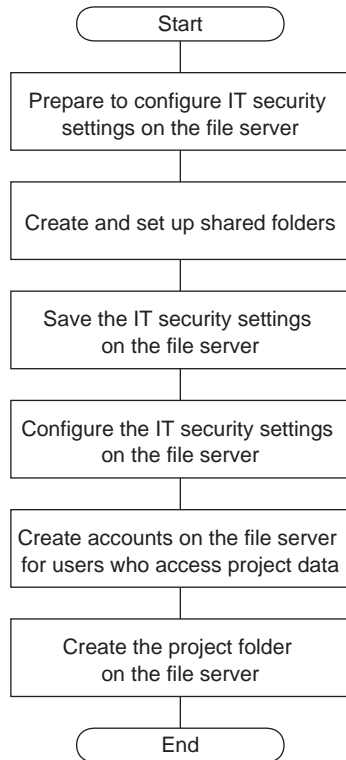
---

## A2.2.3 Setup Procedure for a File Server

You can provide a file server in the system if centralized management is required for project databases. The following figure shows the setup procedure for a file server.

**TIP**

This flowchart illustrates the procedure for setting up a computer that serves only as a file server.



**Figure A2.2.3-1 Setup Procedure for a File Server**

**SEE  
ALSO**

For more information about setting up a computer that serves only as a file server, refer to:

[B5.1, "Setting Up a Computer that Serves Only as a File Server" on page B5-2](#)

For more information about the procedure to set up a computer as both a file server and a license management station, refer to:

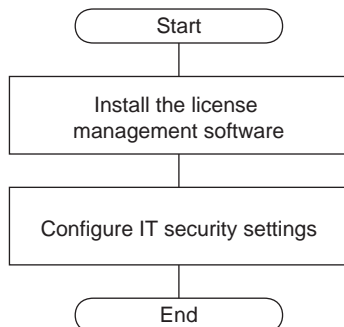
[B5.3, "Setting Up the Computer that Serves as Both File Server and License Management Station" on page B5-9](#)

For more information about setting up the file server function on SENG, refer to:

[B5.2, "Setting Up the File Server Function on SENG" on page B5-8](#)

## A2.2.4 Setup Procedure for a Computer Dedicated to License Management

You can provide a computer dedicated to license management according to the scale and operation policy of the system. The following figure shows the setup procedure for a computer dedicated to license management.



**Figure A2.2.4-1 Setup Procedure for a Computer Dedicated to License Management**

**SEE  
ALSO**

For more information about setting up a computer dedicated to license management, refer to:

[B6., "Setting Up the Computer Dedicated to License Management" on page B6-1](#)

---

## A2.3 Explanation for Maintenance

When you perform the following maintenance tasks, refer to Part C.

- Add licenses and change license assignments
- Set up the domain environment later
- Back up the system
- Upgrade the ProSafe-RS software
- Find out cautionary notes for upgrading and compatibility with the previous revision
- Uninstall the ProSafe-RS software
- Reinstall the ProSafe-RS software
- Change, save, and restore the IT security settings
- Troubleshooting

---

## A3. Requirements for Operation

This section explains the hardware and software requirements. It also explains the software that can collaborate with ProSafe-RS and software that can co-exist on the same computer.

## A3.1 Hardware Requirements

This section describes the hardware requirements for SENG and the file server that are used in a ProSafe-RS system.

### ■ Hardware Requirements for SENG

You must ensure that the computer that is used as SENG meets the hardware requirements as shown in the following table.

If CENTUM software is also installed on the same computer, the computer must also meet the requirements for CENTUM.

**Table A3.1-1 Hardware Requirements for SENG**

Component	OS			
	Windows 7	Windows Vista	Windows Server 2008 R2	Windows Server 2008
CPU	<ul style="list-style-type: none"> <li>Intel Core 2 Duo Processor 2.13 GHz or higher</li> <li>Intel Xeon Dual-Core 2.0 GHz or higher</li> </ul>		Intel Xeon Dual-Core 2.93 GHz or higher	<ul style="list-style-type: none"> <li>Intel Core 2 Duo Processor 2.13 GHz or higher</li> <li>Intel Xeon Dual-Core 2.0 GHz or higher</li> </ul>
Main memory	4 GB or more	2 GB or more	4 GB or more	2 GB or more
Hard disk space	<ul style="list-style-type: none"> <li>20 GB or more free space (mandatory)</li> <li>40 GB or more free space (recommended)</li> </ul> However, if you store an operation history database, 100 GB or more is recommended			
Display	<ul style="list-style-type: none"> <li>SXGA (1280 x 1024) or higher resolution, True color (mandatory)</li> <li>WXGA+ (1440×900) or higher resolution for wide monitoring</li> </ul>			
Graphics	DirectX 9 graphic processing unit or equivalent, and supports the following: <ul style="list-style-type: none"> <li>Windows Driver Display Model (WDDM)</li> <li>Pixel Shader 2.0</li> <li>32 bits per pixel</li> <li>128 MB graphic memory</li> </ul>			N/A
Peripheral unit	<ul style="list-style-type: none"> <li>DVD-ROM drive</li> <li>A PCI slot or PCI Express slot for the control bus interface card or Vnet/IP interface card</li> <li>A DAT drive or hard disk unit for backing up engineering data, which encompasses project databases and various databases used during operation</li> </ul>			

### ■ Hardware Requirements for a File Server

The hardware requirements for the computer used as a file server are as follows:

**Table A3.1-2 Hardware Requirements for a File Server**

Component	Windows Server 2008 R2/Windows Server 2008
CPU	2 GHz or higher
Main memory	2 GB or more
Hard disk space	<ul style="list-style-type: none"> <li>20 GB or more free space (mandatory)</li> <li>50 GB or more free space (recommended)</li> </ul> However, if you store an operation history database, 100 GB or more is recommended
Display	SuperVGA (800 x 600) or higher (mandatory)
Peripheral unit	<ul style="list-style-type: none"> <li>DVD-ROM drive (mandatory)</li> <li>Network adapter (mandatory)</li> </ul>

## A3.2 Software Requirements

This section describes the software requirements for SENG. It also explains the software that can collaborate with ProSafe-RS and software that can co-exist on the same computer.

### ■ Software Requirements for SENG

This section describes the software requirements for SENG.

#### ● Supported OS

The following table shows the correspondence between Windows OS versions/service packs and ProSafe-RS release numbers.

**Table A3.2-1 Correspondence between ProSafe-RS Software Release Numbers and Windows OS Versions**

ProSafe-RS release num- ber	Windows 7 Professional	Windows Vis- ta Business Edition	Windows Server 2008 R2 Standard Edition R2	Windows Server 2008 Standard Edi- tion	Windows Server 2003 R2 Standard Edition	Windows Server 2003 Standard Edi- tion
	64 bits	32 bits	64 bits	32 bits	32 bits	32 bits
	SP1	SP2	SP1	SP2	SP2	SP2
R3.01 / R3.02.00 / R3.02.10	Yes	Yes	Yes	Yes	No (*1)	No (*1)
R3.02.20	Yes	Yes	Yes	Yes	No	No

\*1: Only allowed for use as a file server.

Before installing ProSafe-RS, make sure that a Windows OS version and service pack appropriate for the ProSafe-RS software release number are installed on the computer.



### IMPORTANT

- On a Windows pre-installed computer, various Windows utilities and other software may have been installed in addition to the Windows OS. These additional functions are not only unnecessary for SENG but also can disturb its operations. To avoid disturbance to operations, reinstall the Windows OS.
- This document describes the procedure for setting up a computer from the initial state where the OS has been installed. Do not change the OS settings or add any functions other than the OS, unless so described in the document.
- It is assumed that security patches are applied according to the customer's security policy. YOKOGAWA recommends to apply security patches to ProSafe-RS systems. It is recommended to apply all required security patches before the system goes into operation and also apply security patches that are released after the system went into operation as promptly as possible. YOKOGAWA offers security patch application services. Contact YOKOGAWA Service for more information.

#### ● About .NET Framework and MDAC

- .NET Framework (Version 3.5 SP1)  
ProSafe-RS supports version 3.5 SP1.

When the ProSafe-RS software is installed, .NET Framework is automatically installed. However, .NET Framework (Version 3.5 SP1) included in the ProSafe-RS software medium will not be installed automatically if a newer version has already been installed in the computer, to avoid downgrading of .NET Framework.

- MDAC/Windows DAC  
ProSafe-RS supports MDAC version 2.8 SP1 or later and Windows DAC 6.0 or later.

It is not installed when the ProSafe-RS software is installed because Windows DAC 6.0 or later version with advanced MDAC is provided in Windows Vista and later OS.

- MSXML  
ProSafe-RS supports version 4.0 SP3.

MSXML is automatically installed during installation of the ProSafe-RS software.

However, MSXML (Version 4.0 SP3) included in the ProSafe-RS software medium will not be installed automatically if a newer version has already been installed in the computer, to avoid downgrading of MSXML.

## ● Software that can Coexist with ProSafe-RS

The ProSafe-RS software can coexist with the following software programs.

The following table lists the software that has been confirmed to function without problems together with ProSafe-RS.

**Table A3.2-2 List of Software that can Coexist with ProSafe-RS**

Classification	Software name	Version (*1) (*2) (*3)	Remarks
Spread sheet (*4)	Microsoft Excel	2013 SP1, 2010 SP2, 2007 SP3	
Word processor (*4)	Microsoft Word	2013 SP1, 2010 SP2, 2007 SP3	
Software development	Microsoft Visual C++	2008 SP1	
	Microsoft Visual Basic	2008 SP1	
WWW browser	Microsoft Internet Explorer	9.0, 8.0	
UPS software	APC PowerChute Business Edition	9.0.1	
Security	Anti-virus Software for Endpoint Security Service (*5)	-	Model: AV11000
Document viewer	Adobe Acrobat	11.0, 10.1, 9.5 (*6)	Used for the Instruction Manual Package
	Adobe Reader	11.0, 10.1, 9.5 (*6)	

\*1: Please confirm the required operation environment of each software for OS on which each software operates.

\*2: SP is an abbreviation of Service Pack.

\*3: The software version has been confirmed at the time of the release of this document. For more information about the latest supported version, contact YOKOGAWA.

\*4: If CENTUM software is installed on the same computer, make sure that installed software also meets the software requirements for CENTUM.

\*5: Dedicated for YOKOGAWA's control systems. Includes misdetection prevention of YOKOGAWA software products and customized support in conjunction with McAfee Inc.

\*6: Version 11.0 does not support Windows Vista Business Edition SP2.

## ■ CENTUM Integration System

When ProSafe-RS is integrated with CENTUM, available ProSafe-RS functions are limited depending on the software release number of CENTUM. This section explains such limitations and precautions to be taken when installing the ProSafe-RS and CENTUM software on the same computer.



**SEE  
ALSO**

For more information about precautions on each revision of ProSafe-RS, refer to:

ProSafe-RS Release Information (IM 32Q01A50-31E)

For more information about precautions on each revision of CENTUM, refer to:

- CENTUM VP Release Information (IM 33K01A50-50E) and CENTUM VP Installation (IM 33K01C10-50E)
- CENTUM VP Electronic Document Addendum (IM 33M01A50-40E) and CENTUM VP Installation (IM 33M01A20-40E)
- CS 3000 Electronic Document Addendum (IM 33Q01A50-01E) and CS 3000 Installation (IM33Q01C10- 01E)

## ● Combination of Release Numbers that can be Integrated

The following table shows the release numbers of ProSafe-RS and CENTUM that can be integrated into a single system.

**Table A3.2-3 Release Numbers of ProSafe-RS and CENTUM that can be Integrated**

ProSafe-RS	CS 3000 (*1)	CENTUM VP
R3.01 /R3.02.00 /R3.02.10 / R3.02.20	R3.06 or later	R4.01 or later

\*1: You cannot install ProSafe-RS R3.01 or later and CS 3000 software on the same computer.

## ● Functions of ProSafe-RS and CENTUM Release Numbers

When using ProSafe-RS R3.02.20, CENTUM of release number R5.04.00 or later is recommended.

The following table shows the CENTUM software release numbers that are required to use new functions added in each release of ProSafe-RS.

**Table A3.2-4 CENTUM VP Release Numbers Required to Use Each Function of ProSafe-RS**

Function of ProSafe-RS	Release number of CENTUM
Display of SMB icon and system alarm messages related to license management (when installed on the same computer as HIS)	R5.01 or later
<ul style="list-style-type: none"> <li>• Operation and monitoring of SCSP2</li> <li>• Display of annunciator message corresponding to ANN_FUP function blocks</li> <li>• Display of system alarm messages added in ProSafe-RS R2.03 (*1)</li> </ul>	R4.02 or later

\*1: In CENTUM VP of earlier than R4.02, system alarm messages added in R2.03 are not displayed. The same messages displayed as when manually executing IOM download are displayed at execution of automatic IOM download.

**Table A3.2-5 CS 3000 Release Numbers Required to Use Each Function of ProSafe-RS**

Function of ProSafe-RS	Release number of CS 3000
<ul style="list-style-type: none"> <li>• Operation and monitoring of SCSP2</li> <li>• Display of annunciator message corresponding to ANN_FUP function blocks</li> <li>• Display of system alarm messages added in ProSafe-RS R2.03 (*1)</li> </ul>	R3.09 or later

Continues on the next page

**Table A3.2-5 CS 3000 Release Numbers Required to Use Each Function of ProSafe-RS** (Table continued)

Function of ProSafe-RS	Release number of CS 3000
<ul style="list-style-type: none"> <li>SCS simulation test</li> <li>Interface functions for plant training</li> <li>SCS link transmission</li> <li>Override function blocks with group function</li> <li>Functional changes of password function blocks</li> <li>Specification changes to ANLG_S function blocks in ProSafe-RS R1.03 (process alarms etc.) R3.08.50 or later</li> </ul>	R3.08.50 or later
<ul style="list-style-type: none"> <li>Manual operation function blocks (MOB_11, MOB_21, MOB_RS, MOA)</li> <li>Vnet/IP network connection of SCS</li> </ul>	R3.08 or later
<ul style="list-style-type: none"> <li>Sub-system communication function (Modbus communication)</li> <li>SYS_SEC_CTL (security level protection) function blocks</li> </ul>	R3.07 or later

\*1: In CS 3000 of earlier than R3.09, system alarm messages added in R2.03 are not displayed. The same messages displayed as when manually executing IOM download are displayed at execution of automatic IOM download.

### SEE ALSO

For more information about system alarm messages of R2.03 that cannot be displayed on CS 3000 earlier than R3.09 and CENTUM VP of earlier than R4.02, refer to:

Appendix 1., "Differences in limitations and specifications among software release numbers of CENTUM" in Integration with CENTUM VP/CS 3000 (IM 32Q01E10-31E)

## ● IT Security Setting

- Integration with CENTUM VP
  - You can fortify computer security. To fortify the security, select "Standard model" with the IT Security Tool at installation of both ProSafe-RS and CENTUM VP.
  - If you integrate ProSafe-RS with CENTUM VP earlier than R5.01, manually relax some security items according to the IT security setting of CENTUM VP.
- Integration with CS 3000
 

You cannot fortify computer security. Select "Legacy model" with the IT Security Tool at installation of ProSafe-RS.

## ● Co-existence with ProSafe-RS on a Computer

Observe the following precautions when installing the ProSafe-RS and CENTUM software on the same computer.

- Unless specially instructed, install the control bus driver from the ProSafe-RS software medium.  
If one of the systems has been upgraded, follow the instruction provided for each revision.
- ProSafe-RS R3.01 or later and CS 3000 cannot be installed on the same computer.
- On a computer installed with both the ProSafe-RS and CENTUM software, configure Windows settings according to the instructions in the installation manual of CENTUM.

## ■ FAST/TOOLS Integration System

### ● Coexistence of ProSafe-RS and FAST/TOOLS on the Same Computer

FAST/TOOLS and ProSafe-RS software cannot run on the same computer.

### ● Version

When using ProSafe-RS R3.02.20, the recommended version of FAST/TOOLS is R10.01, which is identical with R9.05 SP2. If the version is earlier than R10.01, ProSafe-RS functions are restricted as follows:

- The new station type SSC57 is not supported.
- The Narrowband mode of Vnet/IP-Upstream is not supported.
- The function to set gas flow rate calculation related parameters is not available.
- The function to read buffered data from SCS is not available.
- IOM models supported from ProSafe-RS R3.02.00 are not displayed.

In addition, the following restrictions apply if the revision of FAST/TOOLS is earlier than R9.03.

- The number of I/O nodes in SCS displayed on FAST/TOOLS is up to 9.
- The number of inter-SCS safety communication locks is not displayed in the SCS Status Display window of FAST/TOOLS.

## ■ Use of PRM

### ● Coexistence of ProSafe-RS and PRM on the Same Computer

Whether or not the PRM and ProSafe-RS software can run on the same computer is as follows:

- A PRM server and ProSafe-RS software cannot run on the same computer.
- A PRM client and ProSafe-RS software can run on the same computer. Note, however, that a PRM client cannot run on the same computer if the computer has a license of SOE OPC Interface Package of ProSafe-RS.
- If you install the PRM client on SENG that is connected to the narrowband Vnet/IP-Upstream network, you need additional Ethernet wiring for PRM client communications.

### ● Version

When using ProSafe-RS R3.02.10 or later, the recommended version of PRM is R3.12 or later. Because the earlier than R3.12 of versions of PRM cannot connect to the narrowband mode.

Because PRM R3.01 does not support IT security function, be sure to use ProSafe-RS with the Legacy model of IT security settings. PRM R3.04 or earlier version does not support the SCSP2 station.

## ■ Use of Exaopc

### ● Coexistence of ProSafe-RS and Exaopc on the Same Computer

Exaopc and ProSafe-RS software cannot run on the same computer.

### ● Version

ProSafe-RS can be connected to Exaopc R3.21.00 or later.

When using ProSafe-RS R3.02.20 or later, the recommended version of Exaopc is R3.72.00 or later.

## ■ Use of Exaquantum

- **Coexistence of ProSafe-RS and Exaquantum on the Same Computer**

Exaquantum and ProSafe-RS software cannot run on the same computer.

- **Version**

ProSafe-RS R3.01 or later can be connected to Exaquantum R2.20 or later.

When using ProSafe-RS R3.02.20 or later, the recommended version of Exaquantum is R2.60 or later. Because the version of Exaquantum that is earlier than R2.60 does not support IT security function, you must select Legacy model for ProSafe-RS.

## B. New Setup

This section explains the procedures for setting up stations.

# B1. Preparing for the Setup

This section explains the items that must be determined before you start setting up a station and precautions for the setup.

## ■ Items to be Determined Before the Setup

This section lists the items that need to be determined before you start the setup tasks.

### ● Domain Number/Station Number

A domain number is a number assigned to a group of stations connected on a control bus network. Domain numbers should be set within a range from 1 to 31 (when integrating with CENTUM, 1 to 16 ).

A station number is a number assigned to each station. In each domain, station numbers should be set within a range from 1 to 64.

### ● Computer Name/Station Name

A computer name is a name used to identify each computer on the Windows network. You can set the computer name from Windows Control Panel.

A station name is a unique name that is assigned based on the control bus address in the ProSafe-RS system.

Examples: SENGddss (SENG)

STNddss (computers other than SENG)

(ddss: “dd” is the domain number and “ss” is the station number.)

It is recommended to match the computer name and the station name of a station.

### ● IP Address

Determine the IP addresses of stations for control bus and Ethernet.

When using Vnet/IP without installing Ethernet, also determine the IP addresses for Vnet/IP open communication.

### ● Subnet Mask

Determine the subnet masks of stations for control bus and Ethernet.

When using Vnet/IP without installing Ethernet, also determine the subnet masks for Vnet/IP open communication.

#### SEE ALSO

For more information about IP addresses and subnet mask for control bus, refer to:

● [Setting IP Address for Vnet](#) on page B3-46

For more information about IP addresses and subnet mask for VnetIPOpen, refer to:

● [IP Address for VnetIPOpen](#) on page B3-47

For more information about IP addresses and subnet mask for Ethernet, refer to:

● [Setting IP Address for Ethernet](#) on page B3-48

### ● Administrative User's Account and Password

Determine the name and password for the administrative user account of the computer.

If the system is used in a domain environment, determine the name and password for the administrative user of the domain.

## ● Security Model and User Management Type

Determine the security model and user management type, which are set by running the IT security tool, to be set on the computer you are going to set up.



### IMPORTANT

Some of the setup procedures vary depending on the “security model” and “user management type,” which are set using the IT Security Tool. Be sure to determine the policies for security settings of the entire system before you start the setup tasks.

#### SEE ALSO

For more information about IT security, refer to:

1., “Overview” in ProSafe-RS Security Guide (IM 32Q01C70-31E)

## ● License Assignment

Determine the license assignments for the computers you are going to set up.



### IMPORTANT

In a ProSafe-RS system, you need to decide on one computer for use as the license management station. The license management station can be set up on a computer where SENG runs.

Among stations of the system, you must set up the license management station first. Then, set up the computers that will be used as license-assigned stations. The software packages installed on the license-assigned stations become available for use after the licenses are distributed from the license management station and accepted on the license-assigned stations.

If an independent license management station is desired, you can also set it up as the computer dedicated to license management.

#### SEE ALSO

For more information about licenses, refer to:

1., “Overview of license management” in License Management (IM 32Q01C60-31E)

## ■ Precautions for Setup

Take note of the following precautions before you start the setup.

### ● Changes in Windows Settings

Installing the ProSafe-RS Software changes the following Windows settings.

Table B1-1 Changes in Windows Settings

Items	Setting	Purpose
Account name display in logon screen	Disable	To protect logon account names from unauthorized use.
Fast user switching	Disable	Simultaneous logon of multiple users is not supported.

### ● When the System Contains Different Revisions

- SENGs in the same RS project should have the software of the same release number.

- The SCS system program release number of SCSs in a system should basically be the same, but mixture of different release numbers is allowed. However, release numbers of SCSs communicating with each other by Inter-SCS safety communication must be in accordance with the explanation in this manual.

**SEE  
ALSO**

For more information about compatibility in inter-SCS safety communication between different revisions, refer to:

- [Appendix 4.9, "Upgrading to Version R3.02.00" on page App.4-36](#)
- [Appendix 4., "Compatibility between Revisions and Cautionary Notes for Upgrading" on page App.4-1](#)

---

- **When a User Account Control Dialog Box Appears**

During installation, a user account control dialog box may be displayed on certain circumstances.

If displayed, click [Yes] or [Continue] (for uninstallation, [Yes] or [Allow]) to continue.

- **Display Style of Control Panel**

Some setup procedures may include instructions to display Windows Control Panel.

In this manual, instructions to select a menu item on Control Panel of Windows 7 are written assuming that the display style of Control Panel is set to "Categories."

- **When Connecting with Other Products**

When connecting ProSafe-RS to other YOKOGAWA products, configuration of IT security settings or other tasks may be required.

**SEE  
ALSO**

For more information about the tasks when connecting CENTUM VP with other products, refer to:

[D., "Connection with Other Products" on page D-1](#)

---



---

## B2. Setting Up the Windows Domain Environment

This section describes the required settings when ProSafe-RS is used in a Windows domain environment. You may also set up the Windows domain environment at a later stage.

---

**SEE  
ALSO**

For more information about setting up the Windows domain environment at a later stage, refer to:

[C2., "Setting Up the Windows Domain Environment Later" on page C2-1](#)

---

## B2.1 Overview of Setting Up the Domain Environment

This section explains the overview of setting up the Windows domain environment.

It is recommended to provide dual-redundant domain controllers because the entire system will have troubles if the only domain controller fails.

### ■ Workflow

The following figure shows the procedure for setting up the Windows domain environment.

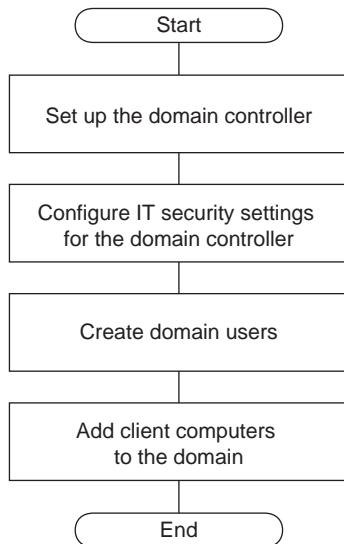


Figure B2.1-1 Flow of setting up the Windows domain environment

### ■ Items to be Determined in Advance

- Domain name
- IP Address of the domain controller

### ■ Items to be Prepared

- Computer for the domain controller
- ProSafe-RS software medium (Model: CHSKM30)  
This is required for IT security configuration.

## B2.2 Configuring the Domain Controller (Windows Server 2008/Windows Server 2008 R2)

This section describes the procedure for configuring the domain controller on Windows Server 2008 or Windows Server 2008 R2.

### ■ Setup Procedure

1. From the Start menu, select [All Programs] > [Administrative Tools], and then select [Server Manager].  
The Server Manager appears.
2. Open [Server Manager] > [Roles], and then select [Add Roles].  
The Add Roles wizard appears.
3. Click [Next].  
The Select Server Roles page appears.
4. For Server Roles, select the [Active Directory Domain Services] check box and then click [Next].  
An overview of the selected settings is displayed.

#### TIP

If you are using Windows Server 2008 R2, a dialog box for adding features appears before an overview of the selected settings is displayed. Click [Add Required Features]. An overview of the selected settings is displayed.

5. Review the content and click [Next].  
The Confirm Installation Selections page appears.
6. Click [Install] .  
The installation starts, and the results of installation is displayed when completed.
7. Click [Close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe)].  
Active Directory Domain Services Installation Wizard appears.

#### TIP

If you are using Windows Server 2008 R2, .NET Framework 3.5.1 is enabled in addition to Active Directory Domain Services.

8. Click [Next].  
The information regarding Operating System Compatibility is displayed.
9. Confirm the information and then click [Next].  
The Choose a Deployment Configuration page appears.
10. Select [Create a new domain in a new forest], and then click [Next].  
The Name the Forest Root Domain page appears.
11. In the FQDN of the forest root domain text box, type the predetermined domain name in the format "Domain name + .local" and then click [Next].  
The Set Forest Functional Level page appears.
12. In the Forest functional level drop-down list, select [Windows Server 2003] and then click [Next].  
The Set Domain Functional Level page appears.
13. In the Domain functional level drop-down list box, select [Windows Server 2008] and then click [Next].  
The Additional Domain Controller Options page appears.

14. Confirm that the [DNS server] check box is selected and click [Next].  
The Location for Database, Log Files, and SYSVOL page appears.
15. Specify the locations of the database folder, log files folder, and SYSVOL folder, and then click [Next].  
The Directory Services Restore Mode Administrator Password (DSRM) dialog box appears.
16. Enter the password of the Administrator account used when starting in the Directory Services Restore Mode and click [Next].  
The Summary page appears.
17. Confirm your selections displayed in the summary, and then click [Next].  
The setups for Active Directory Domain Services starts. The Completing the Active Directory Domain Services Installation Wizard page appears.
18. Click [Finish].  
A message box for restarting the computer to validate the active directory domain services is displayed.
19. Click [Restart Now].

## B2.3 Configuring Security Settings for the Domain Controller

In a system that uses the Standard model of security settings, you need to run the IT Security Tool on the domain controller as well to apply the Standard model of security settings.

### ■ Preparing for Running the IT Security Tool

1. Log on to the domain controller as an administrative user.
2. Perform the following operations regarding .NET Framework.
  - On Windows Server 2008 R2, enable .NET Framework 3.5.1.
  - On Windows Server 2008, enable .NET Framework 3.0.
3. From the Start menu, select [All programs] > [Administrative Tools] > [Active Directory Users and Computers].  
The Active Directory Users and Computers window appears.
4. In the left pane, right-click the [Users] folder and then select [New] > [Group].  
The New Object - Group dialog box appears.

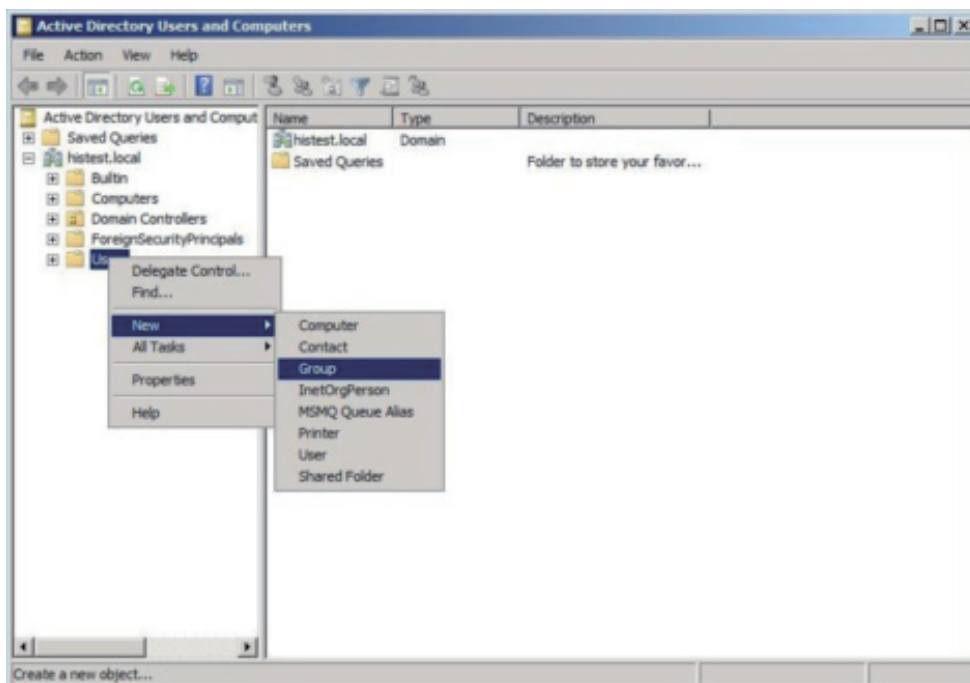


Figure B2.3-1 Active Directory Users and Computers

5. Enter `PSF_MAINTENANCE` in the Group name box, select the Group scope and Group type options, and then click [OK].

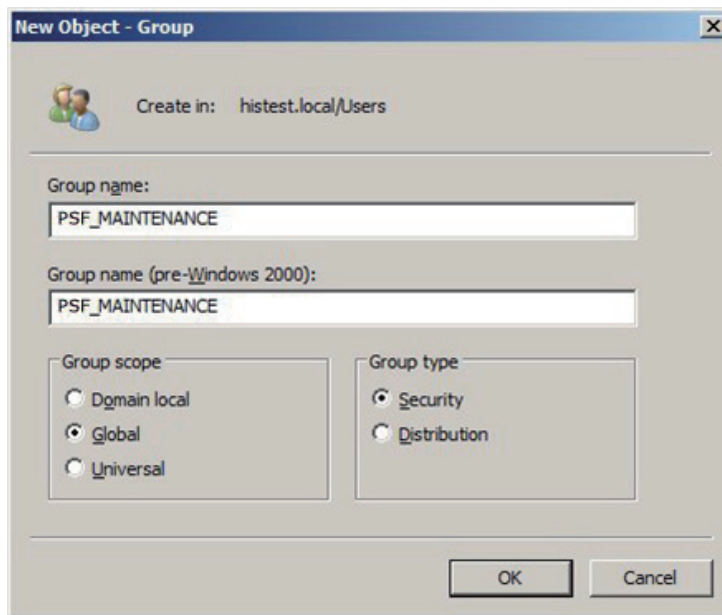


Figure B2.3-2 New Object - Group

6. Check the right pane to confirm that the PSF\_MAINTENANCE group has been created in Users.

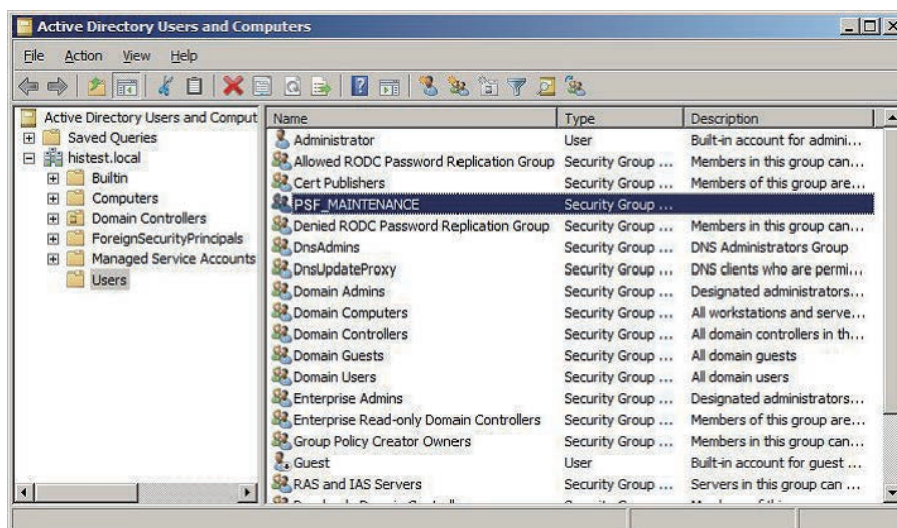


Figure B2.3-3 Active Directory Users and Computers (after creating a new group)

7. Add the logged on user to the PSF\_MAINTENANCE and Domain Admins groups.

#### SEE ALSO

For more information about how to enable .NET Framework 3.5.1 and 3.0, refer to:

“■ Enabling .NET Framework 3.5.1” on page B3-25

For more information about how to add uses to user groups, refer to:

“■ Adding Domain Users to Domain Groups” on page B2-10

## ■ Saving the Initial IT Security Settings



### IMPORTANT

When you use the IT Security Tool to configure IT security settings for the first time after the Windows domain has been set up, be sure to save the security settings on the computer before you use the tool. Keep the saved data in a safe place because the data will be required when you initialize the configured security settings.

Follow these steps to save the security settings before your run the IT Security Tool:

1. Log on to the computer as the user who belongs to the Domain Admins and PSF\_MAINTENANCE groups.
2. Insert the ProSafe-RS software medium into the drive.
  - If the AutoPlay dialog box appears, click [Run Launcher.exe].
  - If the AutoPlay dialog box does not appear, use Explorer and double-click Launcher.exe in the top folder of the software medium.

The installation menu appears.

3. Click [Setting IT Security (File server/domain controller use)].  
The IT Security Tool starts.

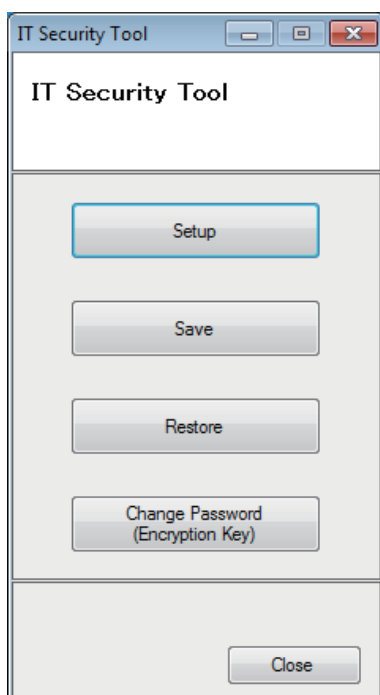


Figure B2.3-4 IT Security Tool menu

4. Click [Save] to save the security settings.

### SEE ALSO

For more information about the subsequent steps to save the IT security settings, refer to:

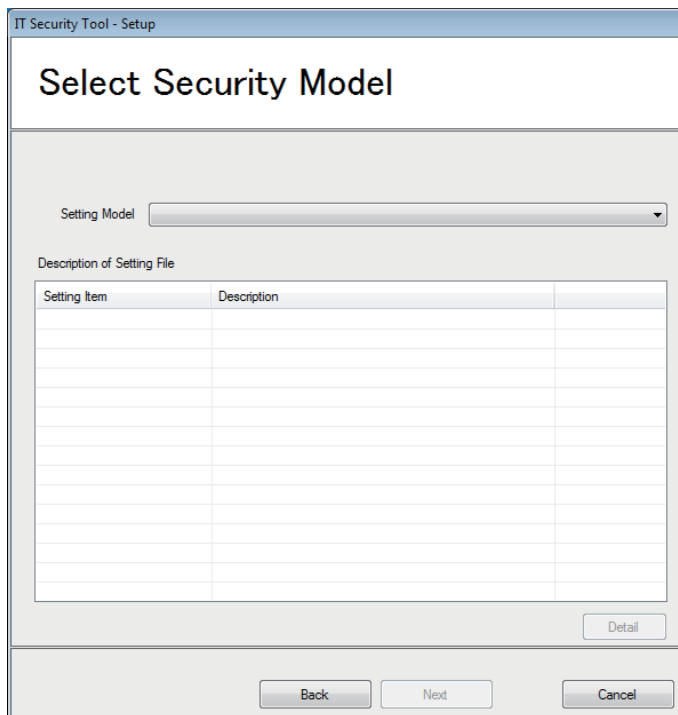
[C8.2.1, "Procedure for SENG PC" on page C8-9](#)

## ■ Configuring IT Security Settings

1. From the IT Security Tool menu, click [Setup].  
A confirmation dialog box appears.
2. If you have saved the aforementioned security setting data for initialization, click [OK].  
The Select Security Model page appears.

**TIP**

If you have not saved the initial security setting data, click [Cancel] to go back to the main menu and save the current security settings.



### Figure B2.3-5 Select Security Model

3. From the Setting Model drop-down list, select [Domain Controller Standard Model Domain/Combination Management].
4. Click [Next].  
The Confirm Setting Information page appears.

**TIP**

If you click [Details], the Select Setting Items page appears.

- For the rest of steps, perform the same operations as when the IT Security Tool is run immediately after installing the ProSafe-RS software.

**SEE  
ALSO**

For more information about the IT security setting operations that are performed following the ProSafe-RS software installation, refer to:

B3.5.2, “Running the IT Security Tool” on page B3-62



## B2.4 Creating Domain Users

This section explains how to create domain users and add them to the domain groups.



### IMPORTANT

When you change the rights of domain users, the changes may not be applied immediately. If this happens, log on and log off twice on each computer after you have changed users' rights.

Do the same thing when you have deleted rights from domain users.

### ■ Creating a Domain User

1. From the Start menu, select [All programs] > [Administrative Tools] > [Active Directory Users and Computers].  
The Active Directory Users and Computers window appears.
2. In the left pane, right-click the [Users] folder and then select [New] > [User].

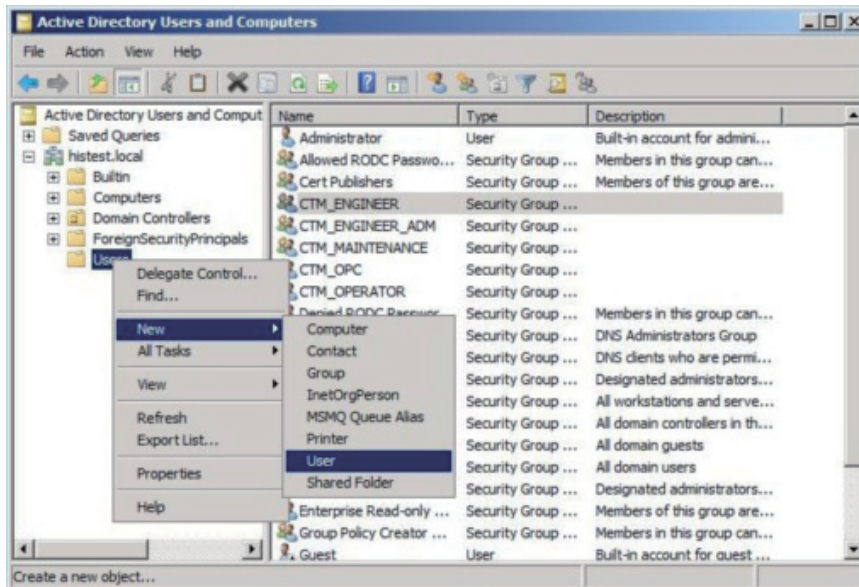
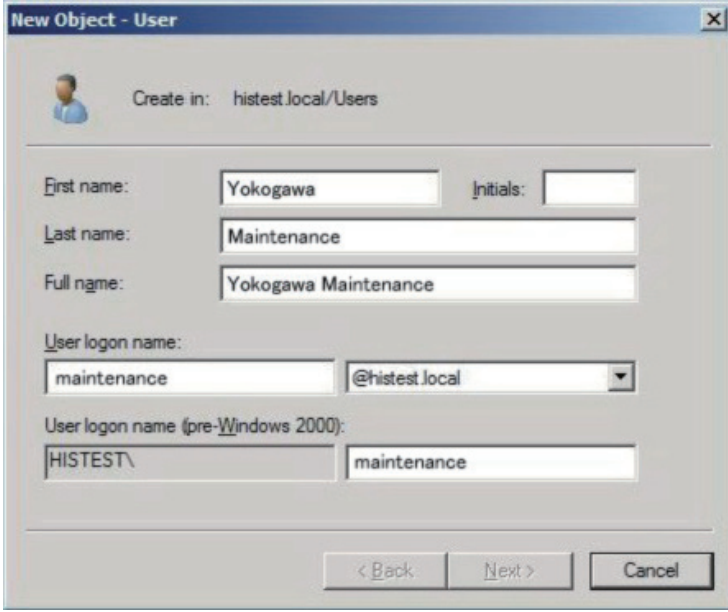


Figure B2.4-1 Activate Directory Users and Computers

3. The New Object-User dialog box is displayed. Input the necessary information.

### TIP

Full name and User logon name have to be input in this dialog box. Additionally, if the User logon name is input, another logon name which is located under the above-mentioned User logon name is automatically input. However, the name is changeable.



The 'New Object - User' dialog box is shown. It has a title bar 'New Object - User' and a close button. Below the title bar is a user icon and the text 'Create in: histest.local/Users'. The form contains the following fields:

- First name: Yokogawa
- Initials: (empty)
- Last name: Maintenance
- Full name: Yokogawa Maintenance
- User logon name: maintenance
- @histest.local (dropdown menu)
- User logon name (pre-Windows 2000): HISTEST\
- maintenance

At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

Figure B2.4-2 New Object-User

4. Click [Next].  
A dialog box appears, prompting you to enter the password.
5. Enter the password, select the check boxes of the required items, and click [Next].  
A confirmation dialog box appears.
6. Click [Finish].
7. Open the Users folder and check the right pane to confirm that the new domain user has been added.

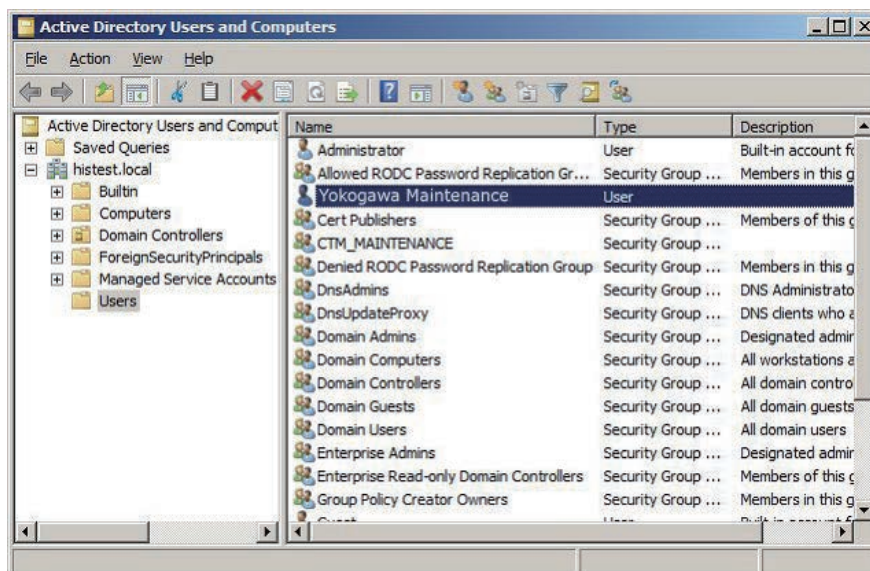


Figure B2.4-3 Active Directory Users and Computers (confirmation of newly created user)

## ■ Adding Domain Users to Domain Groups

When applying the Standard model of security settings, you must add the domain users to appropriate domain groups.

After you run the IT Security Tool on the domain controller, the following ProSafe-RS domain groups have been created.

- PSF\_OPERATOR
- PSF\_ENGINEER
- PSF\_OPC
- PSF\_MAINTENANCE

### ● Adding a Domain User to a Domain Group

This section describes an example of adding a domain user (the user "yokogawa") to the PSF\_MAINTENANCE group.

#### TIP

For domain users who belong to a domain group which requires administrative rights, you also need to perform the procedure in the next section "●Setting Administrative Rights."

1. In the Active Directory Users and Computers window, double click the user that you want to grant the group's rights.  
The properties dialog box for the selected user appears.
2. Select the [Member Of] tab and click [Add].  
The Select Groups dialog box appears.
3. Click [Advanced].  
The advanced settings are displayed in the Select Groups dialog box.
4. Click [Find Now] to display the list of available groups. Select the PSF\_MAINTENANCE group and click [OK].

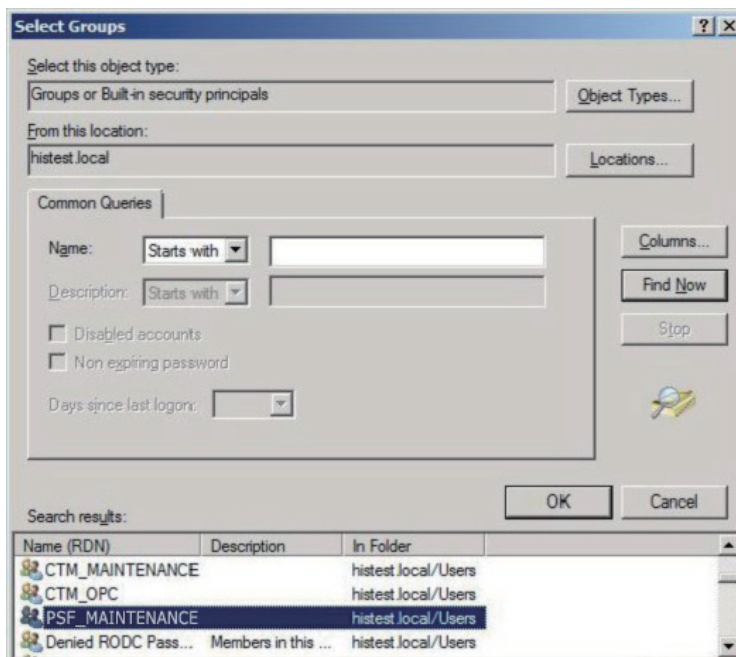


Figure B2.4-4 Select Groups dialog box - Search results

5. In the Select Groups dialog box, ensure that PSF\_MAINTENANCE appears and click [OK].
6. In the user's properties dialog box, ensure that PSF\_MAINTENANCE appears in the Member of list.

- **Setting Administrative Rights**

Follow these steps to assign administrative rights to a domain user who belongs to a domain group which requires administrative rights:

1. Add the domain user to the Domain Admins group.
2. Open the properties dialog box for the user. Click the [Member Of] tab, select [Domain Admins], and click [Set Primary Group].  
The primary group of the user changes to Domain Admins.
3. Select [Domain Users] and click [Remove].
4. Confirm that Domain User has been removed from the Member of list and click [OK].

## B2.5 Adding Client Computers to the Domain

To add client computers to a domain, computer accounts of the client computers need to exist on the domain controller. Computer accounts can be created in two ways: creating on the domain controller computer or on client computers.

When creating a computer account on the domain controller, the client computer can be added to the domain by configuring on the client computer after the computer account is created. When creating a computer account on the client computer, the client computer is added to the domain at the same time the computer account is created.

This section explains the procedure for the case where computer accounts are created on the domain controller. In the procedure, you are required to enter the user name and password of the administrative user of the domain when you configure on a client computer.

### ■ Precautions When Setting Up Client Computers

- When ProSafe-RS is used in a domain environment, add the client computer to the domain before you install the ProSafe-RS software. In the IT security setting configuration that is performed following the ProSafe-RS software installation, select the Standard model applying either the Domain management or Combination management.
- If you are unable to add the client computer to the domain in advance, set the Legacy model or the Standard model applying Standalone management temporarily in the IT security setting configuration that is performed following the ProSafe-RS software installation. Then, add the computer to the domain and change to the Standard model applying Domain management or Combination management.
- When you install the ProSafe-RS software on a client computer that is a domain member, you need to log on as the administrative user of the domain. So, in advance, create on the domain controller computer an administrative user who installs the ProSafe-RS software and add the user to the Domain Admins and PSF\_MAINTENANCE groups.
- After installing the ProSafe-RS software, add the administrative user of the client computer to the PSF\_MAINTENANCE\_LCL group.

#### SEE ALSO

For more information about changing the security model, refer to:

[C8.1, "Changing the IT Security Settings" on page C8-2](#)

### ■ Configuration on the Domain Controller

1. From the Windows Start menu, select [All programs] > [Administrative Tools] > [Active Directory Users and Computers].  
The Active Directory Users and Computers window is displayed.
2. Right-click the Computers folder, and select [New] > [Computers].  
The New Object - Computer dialog box appears.

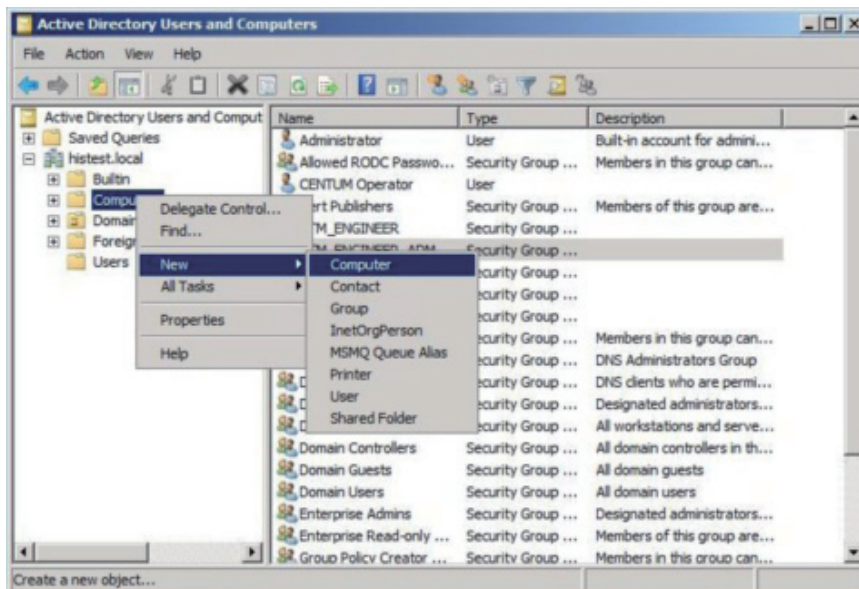


Figure B2.5-1 Active Directory Users and Computers (Create new-Computers)

3. Enter the [Computer Name], and click [OK].

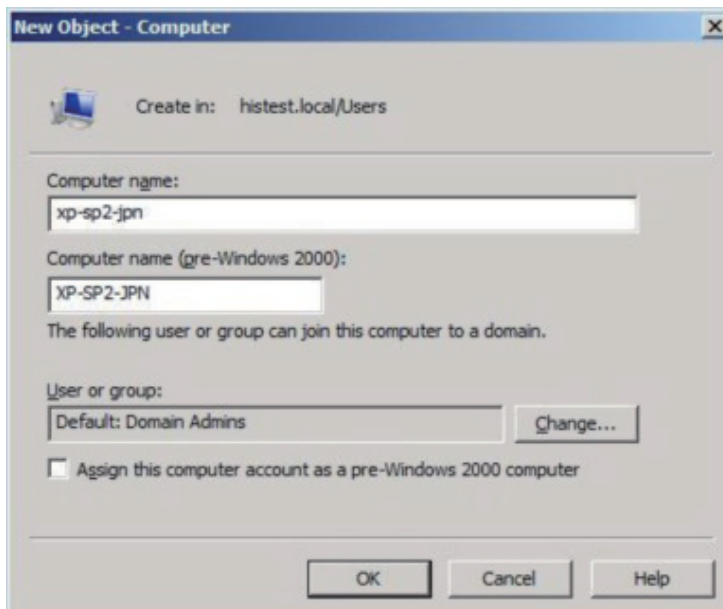


Figure B2.5-2 New Object-Computer (Input of Computer Name)

4. Confirm that the new computer has been added in the Computers folder.



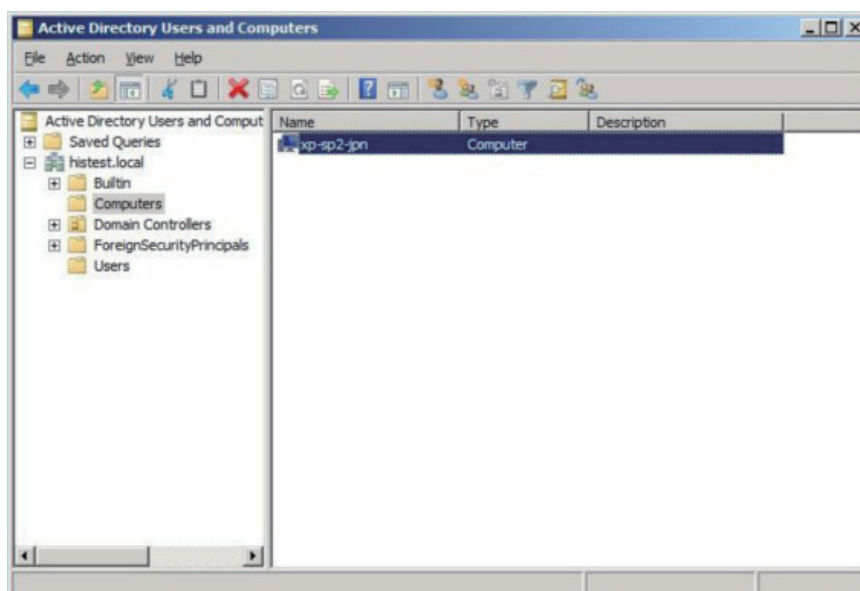


Figure B2.5-3 Active Directory Users and Computers (confirmation of newly added computers)

Configuration on the domain controller is now finished. Go on to the procedure for configuration on the client computer.

## ■ Configuration on a Client Computer (Windows 7)

Follow these steps to add a Windows 7 computer to the domain:

1. From the Start menu, select [Computer].  
The Computer window appears.
2. In the Computer window, click [System Properties].  
The System window appears.
3. In the System window, click [Change settings].  
The System Properties dialog box appears.
4. In the System Properties dialog box, select the [Computer Name] tab and click [Change].  
The Computer Name/Domain Changes dialog box appears.
5. On the Computer Name/Domain Changes dialog box, select [Domain], enter the domain name, and click [OK].

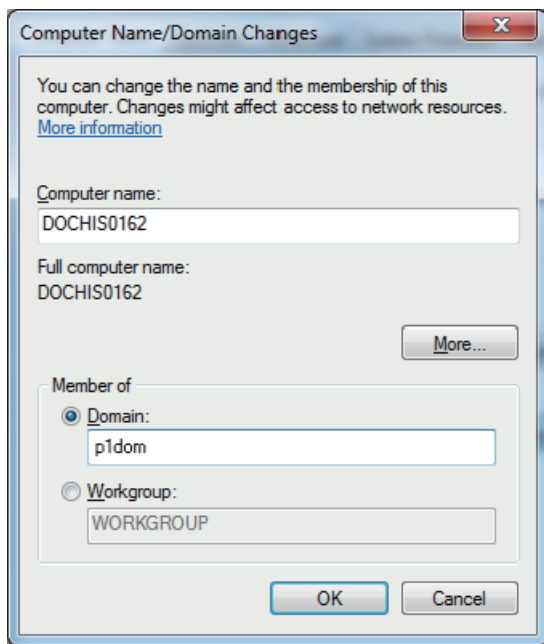


Figure B2.5-4 Computer Name/Domain Changes Dialog Box

6. In the dialog box that is displayed, enter the user name and password of the administrative user of the domain and click [OK].

**TIP**

An error message dialog box may appear, indicating that the domain name cannot be changed. However, you can click [OK] to proceed because the computer has been added to the domain successfully.

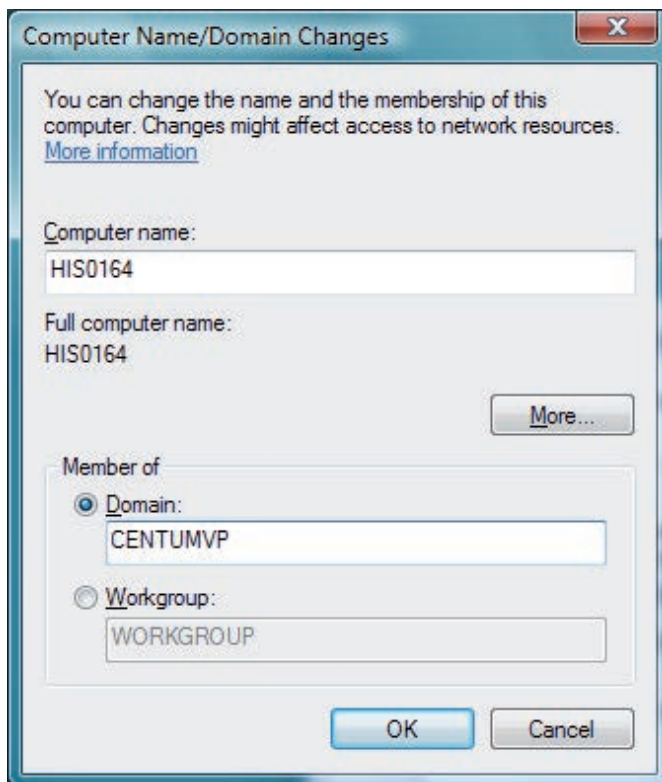
7. On the Computer Name/Domain Changes dialog box, click [OK].
8. On the dialog box for confirmation of restarting, click [Restart Now] to restart the computer.

## ■ Configuration on a Client Computer (Windows Vista)

Follow these steps to add a Windows Vista computer to the domain:

1. From the Start menu, select [Computer].  
The Computer window appears.
2. In the Computer window, click [System Properties].  
The System window appears.
3. In the System window, click [Advanced system settings].  
The System Properties dialog box appears.
4. In the System Properties dialog box, select the [Computer Name] tab and click [Change].  
The Computer Name/Domain Changes dialog box appears.
5. On the Computer Name/Domain Changes dialog box, select [Domain], enter the domain name, and click [OK].





**Figure B2.5-5 Computer Name/Domain Changes Dialog Box**

6. In the dialog box that is displayed, enter the user name and password of the administrative user of the domain and click [OK].
7. On the Computer Name/Domain Changes dialog box, click [OK].
8. On the dialog box for confirmation of restarting, click [Restart Now] to restart the computer.

---

## B2.6 Setting Up Redundant Domain Controllers

It is recommended to provide another domain controller for redundancy because the entire system will have troubles if the only domain controller fails.

### ■ Setup Procedure

1. Add the second domain controller computer to the existing domain.
2. Configure IT security settings.

---

**SEE  
ALSO**

For more information about configuring the IT security settings, refer to:

[B2.3, “Configuring Security Settings for the Domain Controller” on page B2-5](#)

---

## B2.7 Setting Up Time Synchronization in Windows Domain Environment

When using ProSafe-RS in a Windows domain environment, the time on computers used in the ProSafe-RS system and the time on the domain controller must be synchronized.

Because the time synchronization service of a ProSafe-RS system uses the time on the control bus as the time master, the time of the domain controller should be synchronized to the time of client computers if the system is used in a domain environment.

This section describes how to set up time synchronization in a system that consists of only ProSafe-RS.

### ■ Cautionary Note on Time Synchronization

A computer installed with the ProSafe-RS software is automatically configured so as not to use the domain controller as the time master for time synchronization, even if the computer is added to the Windows domain.

## B2.7.1 Implementing Time Synchronization in a System Consisting of Only ProSafe-RS

This section describes how to implement time synchronization in a system consisting of only ProSafe-RS for the following cases:

- V net — Not synchronize to the Coordinated Universal Time (UTC)
- Vnet/IP — Synchronize to the Coordinated Universal Time (UTC)
- Vnet/IP — Not synchronize to the Coordinated Universal Time (UTC)

### ■ For V net — Not Synchronize to the Coordinated Universal Time (UTC)

Configure a station connected to the V net domain as the SNTP server. Times on the computers within the V net domain are synchronized using the V net time synchronization function. Time synchronization of the entire system is achieved by synchronizing the time on the domain controller to the SNTP server.

#### TIP

When a station is used as the SNTP server, the system time is not synchronized to UTC but to the time on the hardware of the SNTP server.

- On the computers connected on V net, do not use the Windows W32Time service to perform time synchronization. If used, times on the computers are synchronized to the time on the domain controller and synchronization with the SNTP server is prevented.
- On the domain controller, use the Windows W32Time service to synchronize its time with the SNTP server.

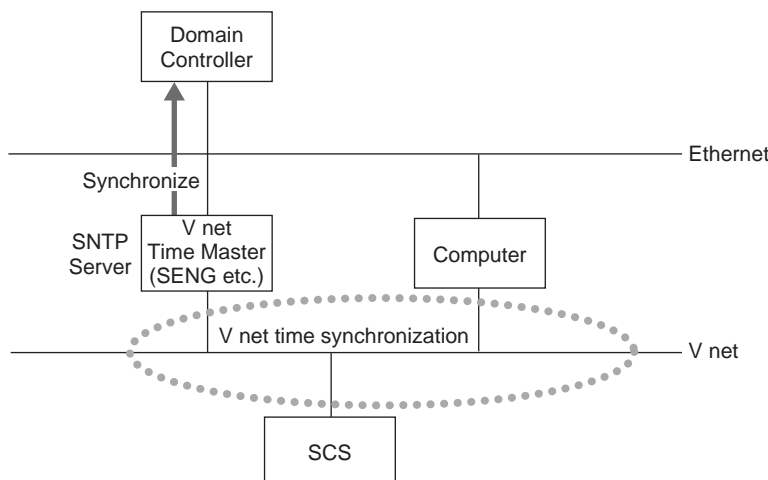


Figure B2.7.1-1 Implementing Time Synchronization (V net — Not Synchronize to UTC)

#### SEE ALSO

For more information about how to configure a station as the SNTP server, refer to:

■ [Setting a Station as the SNTP Server](#) on page B2-22

### ■ For Vnet/IP — Synchronize to the Coordinated Universal Time (UTC)

- Introduce an SNTP server and make it synchronize with UTC. Configure the domain controller and the Vnet/IP system so that they will reference the time of the same SNTP server.

- On the computers connected on Vnet/IP, do not use the Windows W32Time service to perform time synchronization. If used, times on the computers are synchronized to the time on the domain controller and synchronization with the SNTP server is prevented.

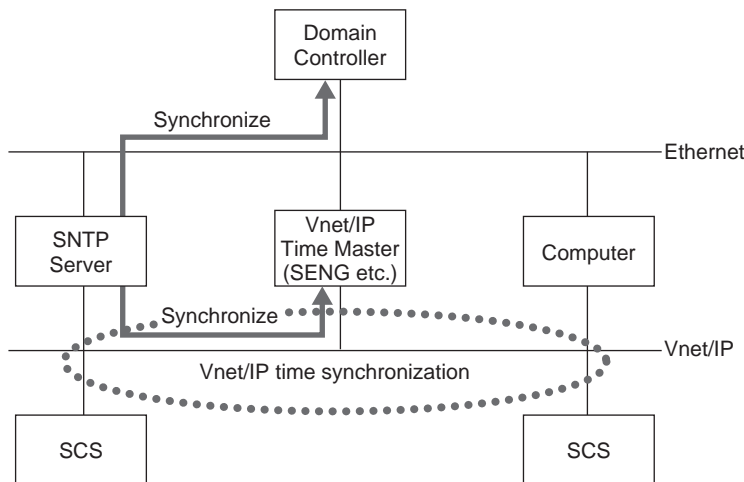


Figure B2.7.1-2 Implementing Time Synchronization (Vnet/IP — Synchronize to UTC)

## ■ For Vnet/IP — Not Synchronize to the Coordinated Universal Time (UTC)

Configure a station connected to the Vnet/IP domain as the SNTP server. Times on the computers within the Vnet/IP domain are synchronized using the Vnet/IP time synchronization function. Time synchronization of the entire system is achieved by synchronizing the time on the domain controller to the SNTP server.

### TIP

When a station is used as the SNTP server, the system time is not synchronized to UTC but to the time on the hardware of the SNTP server.

- On the computers connected on Vnet/IP, do not use the Windows W32Time service to perform time synchronization. If used, times on the computers are synchronized to the time on the domain controller and synchronization with the SNTP server is prevented.
- On the domain controller, use the Windows W32Time service to synchronize its time with the SNTP server.

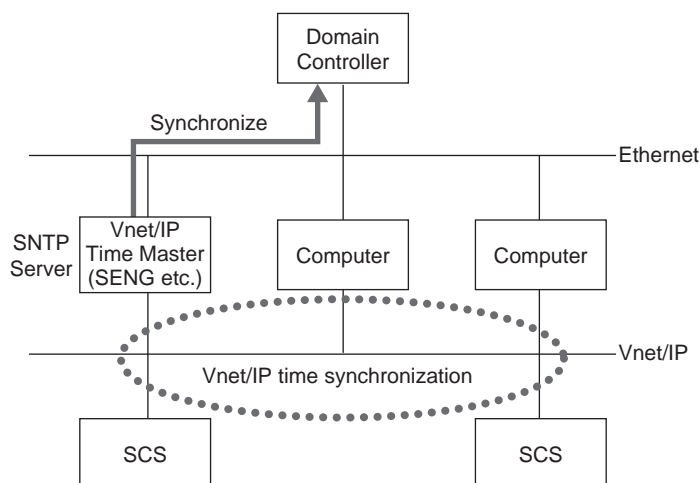


Figure B2.7.1-3 Implementing Time Synchronization (Vnet/IP — Not Synchronize to UTC)

## ■ Setting a Station as the SNTP Server

1. Use an administrative user account to log on to the station you want to set as the SNTP server, and run the following command as the administrator.

(ProSafe-RS software medium drive):\ProSafe-RS\TOOLS\BeNtpServer.cmd

The Command Prompt window appears and displays "Enable NTP Server? (y/n/quit)."

### TIP

If the IT security settings have been configured to apply software restriction policies, run the command prompt (cmd.exe) as the administrator and then run the command from the command prompt window.

2. Enter "y," and then press the [Enter] key.

---

## B2.7.2 Implementing Time Synchronization When Integrated with CENTUM

When the system is integrated with CENTUM, set up time synchronization by following the explanation provided in the manual of CENTUM. If the system consists of multiple V net domains or a mixture of Vnet/IP domain and V net domain, also follow the explanation in the manual of CENTUM.

---

**SEE  
ALSO**

For more information about how to set up time synchronization in Windows domain environment for a system integrated with CENTUM, refer to:

B2.8, "Setting Up Time Synchronization in Windows Domain Environment" in CENTUM VP Installation (IM 33K01C10-50E)

---

## B3. Setting Up the SENG

This section describes the tasks required for the new setup of SENG.



### IMPORTANT

In a ProSafe-RS system, you need to decide on one computer for use as the license management station. The license management station can be set up on a computer where SENG runs.

Among stations of the system, you must set up the license management station first. Then, set up the computers that will be used as license-assigned stations. The software packages installed on the license-assigned stations become available for use after the licenses are distributed from the license management station and accepted on the license-assigned stations.

If an independent license management station is desired, you can also set it up as the computer dedicated to license management.

### SEE ALSO

For more information about how to set up the computer dedicated to license management, refer to:

[B6., "Setting Up the Computer Dedicated to License Management" on page B6-1](#)

### ■ Items to be Prepared

Have the following items at hand before new installation of the ProSafe-RS software.

- ProSafe-RS software medium (Model: CHSKM30)

Also have the following items at hand if the SENG is to be used as a license management station. These are required when distributing licenses.

- ProSafe-RS license medium (Model: CHSCM30)
- ProSafe-RS license sheet (with project ID)



## B3.1 Setting Up the Hardware

This section describes the hardware setups required for an SENG.



### WARNING

When removing and installing the cards to set DIP switches, take measure to prevent the damages caused by static electricity.

### SEE ALSO

For more information about antistatic measures, refer to:

[Appendix 3., “Antistatic Precautions When Handling Hardware” on page App.3-1](#)

### ■ Setting Up the Control Bus Interface Card

The following two types of control bus interface cards are available. These cards have the same functionality.

- VF702 (for PCI Express)
- VF701 (for PCI bus)

The Control Bus interface card has DIP switches for setting the domain number and the station number. The combination of domain number and station number determines the station address.

You must set the DIP switches before you configure network settings.

This section describes how to set the DIP switches. The DIP switch locations are the same on VF702 and VF701 cards.

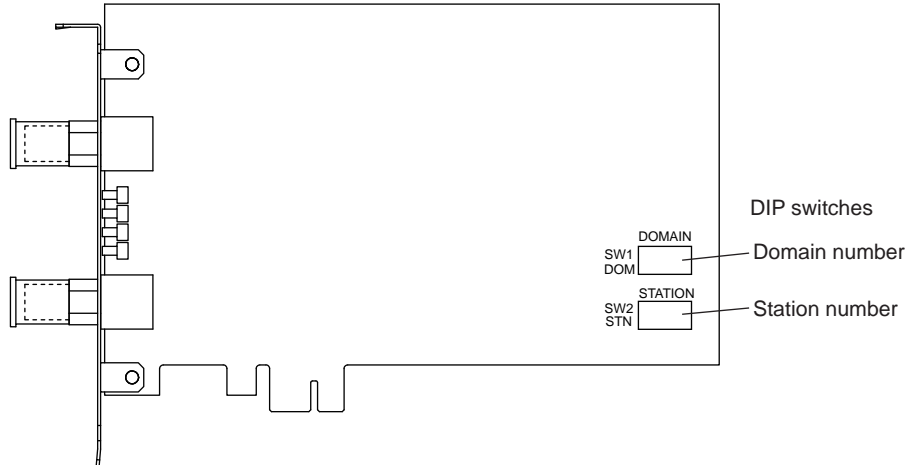


Figure B3.1-1 Location of DIP Switches

#### ● Setting the Domain Number

A domain is a collection of stations that are connected on one control bus network. Set a domain number from 1 to 31 (1 to 16 when integrating with CENTUM).

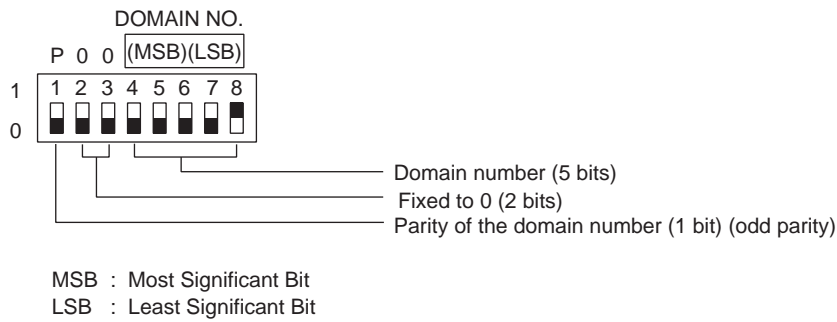


Figure B3.1-2 Domain Number Setting DIP Switches

**SEE  
ALSO**

For more information about domain numbers and corresponding DIP switch positions, refer to:

“■ Domain Numbers and DIP Switch Positions” on page App.1-1

### ● Setting the Station Number

Station numbers should be set in the range of 1 to 64; it is recommended to set starting from 64 in the descending order.

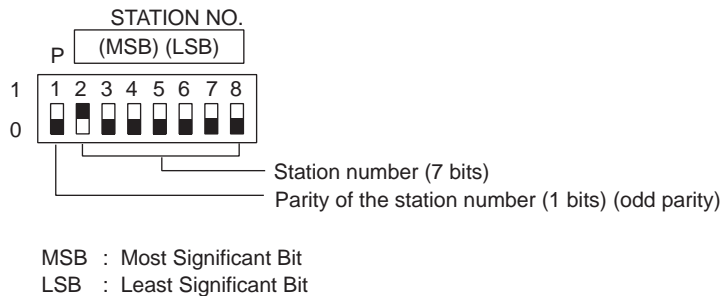


Figure B3.1-3 Station Number Setting DIP Switches

**SEE  
ALSO**

For more information about station numbers and corresponding DIP switch positions, refer to:

“■ Station Numbers and DIP Switch Positions” on page App.1-2

### ● Precautions on Installing the Control Bus Interface Card

- Install VF702/VF701 in the computer after setting up Windows but before configuring the network settings.
- Install the control bus driver when you restart the computer after installing VF702/VF701. Follow the procedure in this manual to install the driver.

**SEE  
ALSO**

For more information about the procedure to install the control bus driver in a computer, refer to:

B3.3.1, “Installing the Control Bus Driver” on page B3-33

### ● Installing the Control Bus Interface Card

After you have set the station address on the VF702/VF701 card, follow these steps to install it in the computer:

1. Turn off the power of the computer. For safety, remove the power plug from the outlet.
2. Remove the cover of the main unit of the computer.
3. Unscrew the screws fixing the slot cover and remove the slot cover.

4. Insert the VF702/VF701 card in the corresponding slot and fix it to the slot.
5. Mount the cover back on the computer.
6. Write the station address on the label that comes with the VF702/VF701 card and paste it in the front or other easy-to-see location of the computer.

## ■ Setting Up the Vnet/IP Interface Card

You need to install a Vnet/IP interface card (VI702/VI701) in the computer that is to be connected on a Vnet/IP network.

VI702 is for PCI Express, and VI701 is for PCI. Because VI702 and VI701 have the same functionality, VI702 is used as an example in the following explanation.

The Vnet/IP interface card has DIP switches for setting the domain number, station number and action mode. The combination of domain number and station number determines the station address.

You must set the DIP switches before you configure network settings.

This section describes how to set the DIP switches.

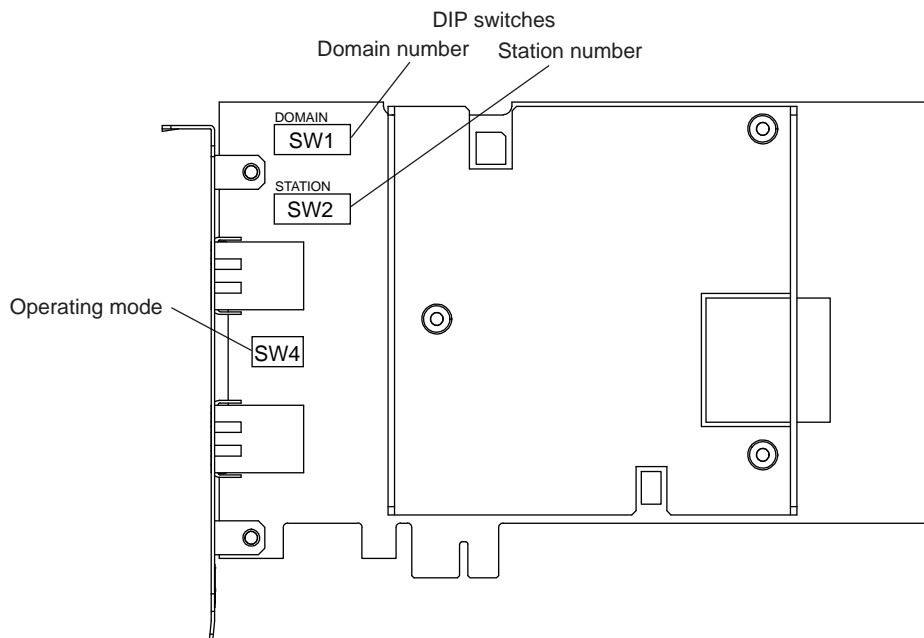


Figure B3.1-4 Locations of DIP Switches

### ● Setting the Domain Number

A domain is a collection of stations that are connected on one control bus network. Set a domain number from 1 to 31 (1 to 16 when integrating with CENTUM).

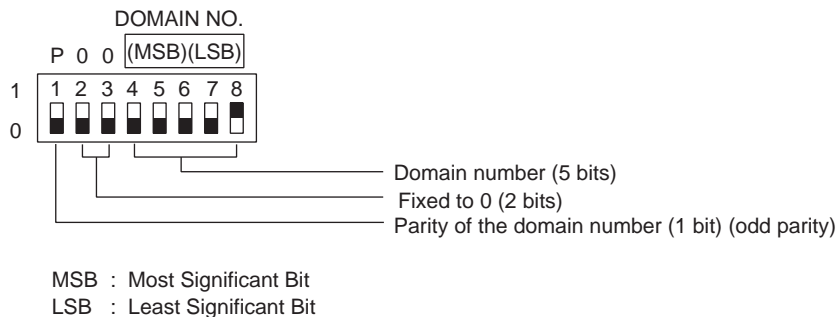


Figure B3.1-5 Domain Number Setting DIP Switches

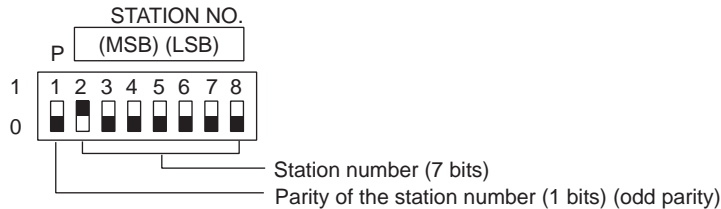
**SEE  
ALSO**

For more information about domain numbers and corresponding DIP switch positions, refer to:

“■ Domain Numbers and DIP Switch Positions” on page App.1-1

### ● Setting the Station Number

Station numbers should be set in the range of 1 to 64; it is recommended to set starting from 64 in the descending order.



MSB : Most Significant Bit  
LSB : Least Significant Bit

**Figure B3.1-6 Station Number Setting DIP Switches**

**SEE  
ALSO**

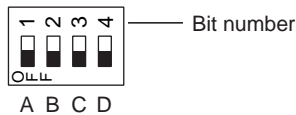
For more information about station numbers and corresponding DIP switch positions, refer to:

“■ Station Numbers and DIP Switch Positions” on page App.1-2

### ● Action Mode Switch

SW4 on the printed circuit board is the action mode switch.

Use the card with all the bits of this DIP switch set to OFF (factory set defaults). The meaning of DIP switch bits are as follows:



**Figure B3.1-7 Action Mode Switch**

**Table B3.1-1 DIP Switch Usage**

	DIP switch ON	DIP switch OFF	Remarks
A (bit 1)	-	Always OFF	Reserved
B (bit 2)	100 Mbps	1 Gbps	Communication speed (Default : OFF)
C (bit 3)	Force	Auto	Negotiation (Default : OFF)
D (bit 4)	-	Always OFF	Reserved

### ● Precautions on Installing the Vnet/IP Interface Card

- Install VI702 in the computer after setting up Windows but before configuring the network settings.
- Install network drivers when you restart the computer after installing VI702. Follow the procedure in this manual to install the drivers.
- If you use VI702 that was used in another system for a system consists of only ProSafe-RS, erase the settings in the VI702 before installing it in the computer. When using such VI702 in a system integrated with CENTUM, you do not need to erase the settings in the VI702.

**SEE  
ALSO**

For more information about how to erase the internal settings of a VI702 card, refer to:

[Appendix 2., "Procedure for Erasing VI702 Internal Settings" on page App.2-1](#)

For more information about the procedure to install the network driver in a computer, refer to:

- [B3.3.1, "Installing the Control Bus Driver" on page B3-33](#)
- [B3.3.2, "Installing the Vnet/IP Open Communication Driver" on page B3-35](#)

## ● Installing the Vnet/IP Interface Card

After you have set the station address and action mode on the VI702 card, follow these steps to install it in the computer:

1. Turn off the power of the computer. For safety, remove the power plug from the outlet.
2. Remove the cover of the main unit of the computer.
3. Unscrew the screws fixing the slot cover and remove the slot cover.
4. Insert the VI702 card in the corresponding slot and fix it to the slot.
5. Mount the cover back on the computer.
6. Connect both the BUS1 and BUS2 cables to VI702 and Layer 2 switch. There is no need to turn off the power of the Layer 2 switch.
7. Connect the power cord of the computer back to the outlet and turn on the computer.
8. Make sure that the RDY lamp on VI702 is lit.
9. Write the station address on the label that comes with the VI702 card and paste it in the front or other easy-to-see location of the computer.

---

## B3.2 Setting Up Windows

Before installing the ProSafe-RS software, you need to change the Windows settings on your computer to the recommended settings.

This configuration should be performed on the computer where the Windows OS and its service packs have been installed.

## B3.2.1 Configuring on Windows 7

Follow these procedures when you use a Windows 7 computer.

### ■ File System

Ensure that the file system is in the NTFS format. If it is already formatted in the FAT format, reinstall the operating system and reformat partitions into NTFS. Partitions not installed with OS should also be formatted into NTFS.

### ■ System Performance

Follow these steps to configure the system performance setting:

1. Log on as an administrative user.
2. From the Start menu, select [Control Panel] > [System and Security] > [System] > [Advanced system settings].  
The System Properties dialog box appears.
3. Select the [Advanced] tab, and click [Settings] in the Performance section.  
The Performance Options dialog box appears.
4. Click the [Visual Effects] tab and select [Let Windows choose what's best for my computer].

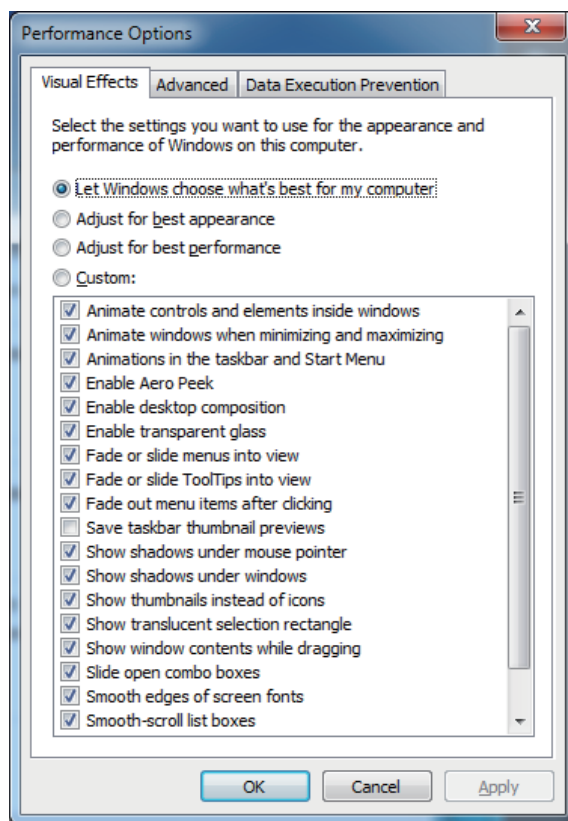


Figure B3.2.1-1 Performance Options Dialog Box (Visual Effects Tab)

5. Click [OK].

## ■ Virtual Memory

ProSafe-RS does not require virtual memory configuration. However, if the ProSafe-RS and CENTUM VP software coexist on the same computer, virtual memory should be configured according to the instruction of CENTUM VP.

## ■ Power Options

This section describes how to configure the Power Options settings. Some of the items in the explanation may not be displayed on your computer, depending on the computer's hardware configuration. If not displayed, the function of that item is not available on your computer.

1. Log on as an administrative user.
2. From the Start menu, select [Control Panel] > [Hardware and Sound] > [Power Options]. The Power Options window appears.
3. Select [High performance] under Preferred plans, click [Change plan settings] to the right of it. The Edit Plan Settings window appears.

**TIP** If High performance does not appear under Preferred plan, click [Show additional plans]. Select [High performance] and then click [Change plan settings] to the right of it.

4. Click [Change advanced power settings]. The Power Options dialog box appears, showing the advanced settings.

**TIP** Depending on the computer configuration, the items of unavailable functions will not be displayed in the step results hereafter.

5. Under Hard disk, set the setting for Turn off hard disk after to [Never].

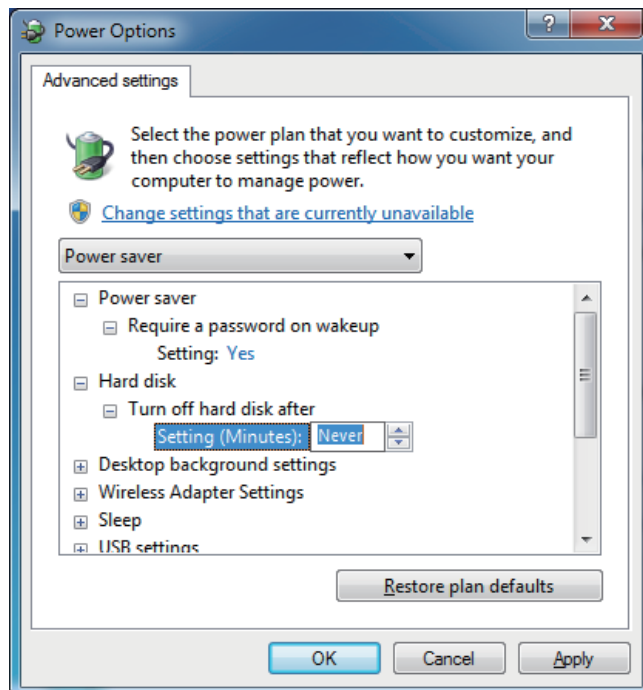


Figure B3.2.1-2 Power Options Advanced Settings

6. Configure the Sleep settings as follows:



- [Sleep after]: Never
- [Allow hybrid sleep]: Off
- [Hibernate after]: Never
- [Allow wake timers]: Disable

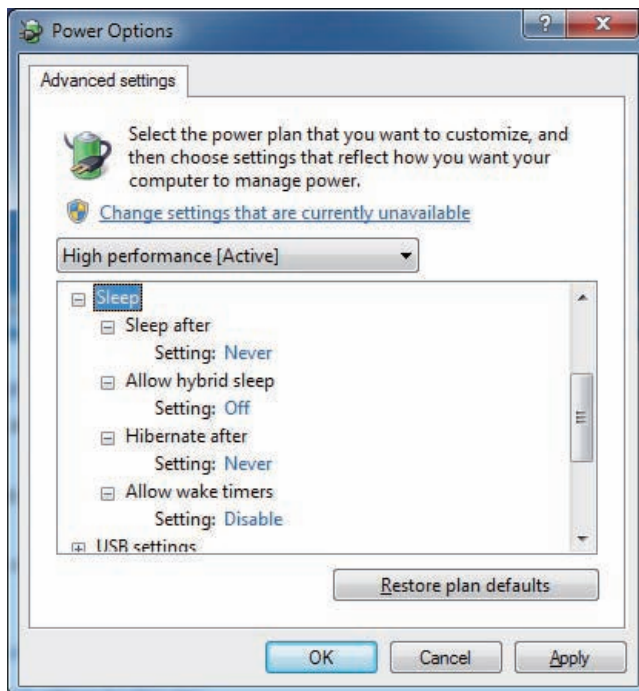


Figure B3.2.1-3 Power Options Advanced Settings

7. Set the setting for Power button action under Power buttons and lid to [Shut down].

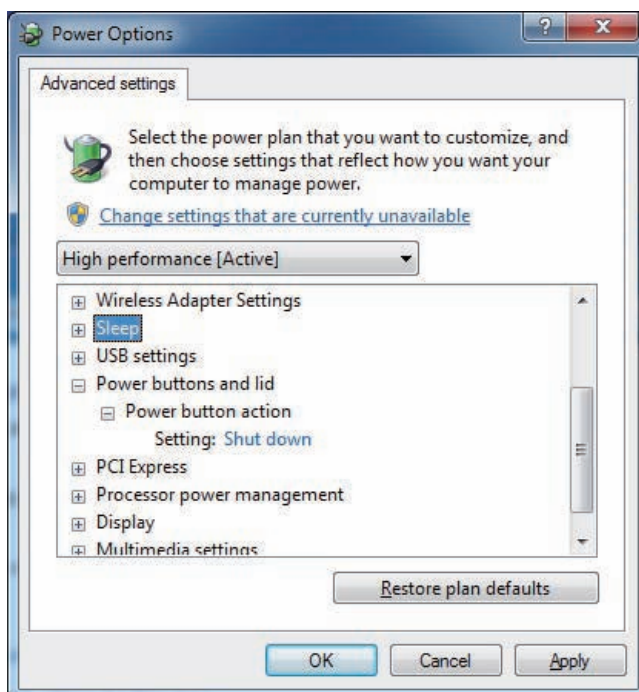


Figure B3.2.1-4 Power Options Advanced Settings

8. Under Display, set the setting for Turn off display after to [Never].

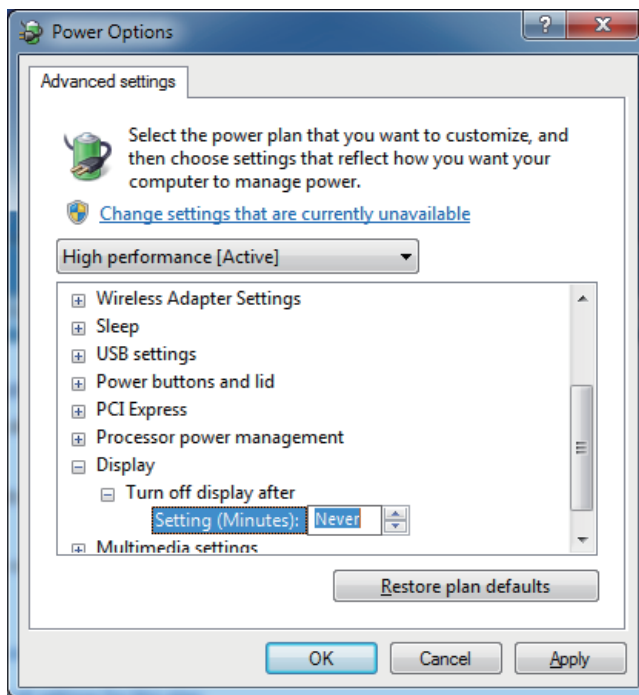


Figure B3.2.1-5 Power Options Advanced Settings

9. Click [OK].

**TIP**

Configure UPS service settings after installing the ProSafe-RS software.

**SEE ALSO**

For more information about setting up UPS services, refer to:

[B3.9, "Configuring the Uninterruptible Power Supply \(UPS\) Service" on page B3-83](#)

## ■ Windows Defender

The Windows Defender software detects and removes spy ware.

It is recommended to turn off this function because it is not used in ProSafe-RS.

In a domain environment, turn off Windows Defender on domain member PCs at a time by means of a domain management operation such as Group Policies.

In a workgroup environment, turn off Windows Defender by using either of the following procedures.

- Turning Off Windows Defender in Control Panel
- Turning Off Windows Defender in Local Group Policy Editor

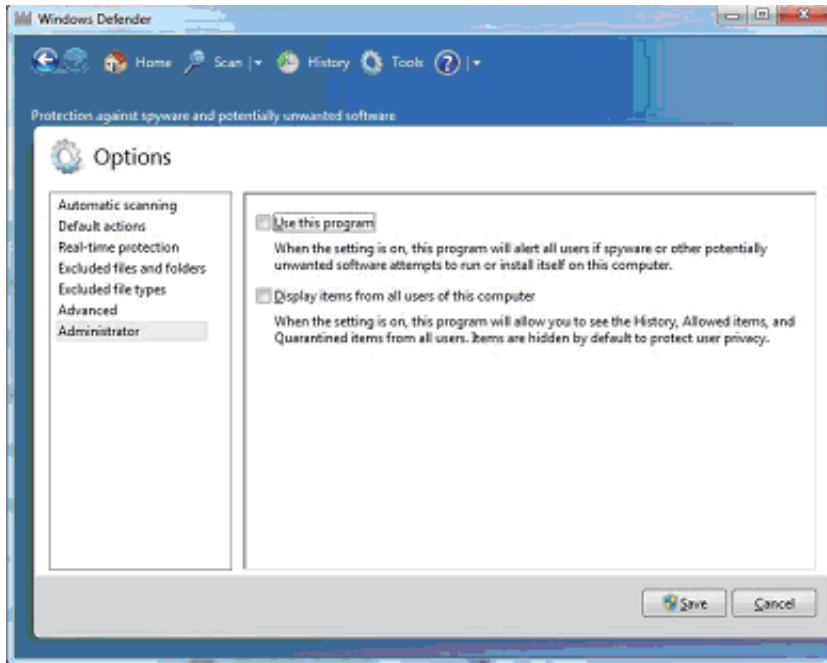
**TIP**

If Tools of Windows Defender is grayed out, turn off Windows Defender in Local Group Policy Editor.

### ● Turning Off Windows Defender in Control Panel

1. Log on as an administrative user.
2. From the Start menu, select [Control Panel].
3. Select [Large icons] or [Small icons] for the display style, and then select [Windows Defender].  
The Windows Defender window appears.

4. Click [Tools] displayed at the top.  
The Tools and Settings window appears.
5. Click [Options].  
The Options window appears.
6. From the menu on the left, select [Administrator] and clear the check box for [Use this program].



**Figure B3.2.1-6 Options**

7. Click [Save].  
A dialog box appears, informing that Windows Defender is turned off.
8. Click the [x] button.

### ● Turning Off Windows Defender in Local Group Policy Editor

If Tools of Windows Defender is grayed out, you can turn off Windows Defender in Local Group Policy Editor.

Follow these steps to turn off Windows Defender:

1. Log on as an administrative user.
2. Click the Start button of Windows, and enter `gpedit.msc` in the Program and file search box.  
The Local Group Policy Editor window appears.
3. Select [Computer Configuration] > [Administrative Templates] > [Windows Components] > [Windows Defender], and double-click [Turn off Windows Defender] in the right pane.  
The Turn off Windows Defender dialog box appears.
4. Select [Enabled] and click [OK].

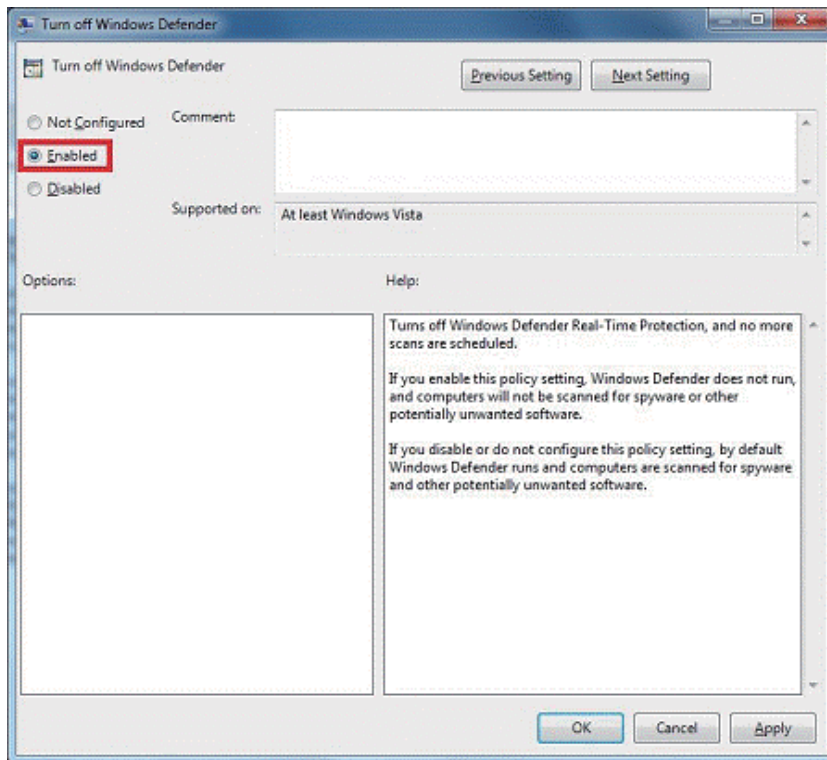


Figure B3.2.1-7 Turn Off Windows Defender Dialog Box

## ■ Disk Defragmenter

Disk Defragmenter Tool can be used to reorganize the fragmented files on computer hard disk so as to improve the computer performance. With the default setting of Windows 7, the Disk Defragmenter Tool is scheduled to start periodically at 1:00 on Wednesday. Because the performance of ProSafe-RS may be affected significantly, it is recommended to disable the periodic disk defragmentation.

Moreover, you may manually start the disk defragmenter when you feel the disk performance is getting worse or when you perform system maintenance.

1. Log on as an administrative user.
2. From the Start menu, select [All Programs] > [Accessories] > [System Tools] > [Disk Defragmenter].  
The Disk Defragmenter window appears.
3. Click [Configure schedule...].  
The Modify Schedule dialog box appears.
4. Clear the [Run on a schedule (recommended)] check box and click [OK].

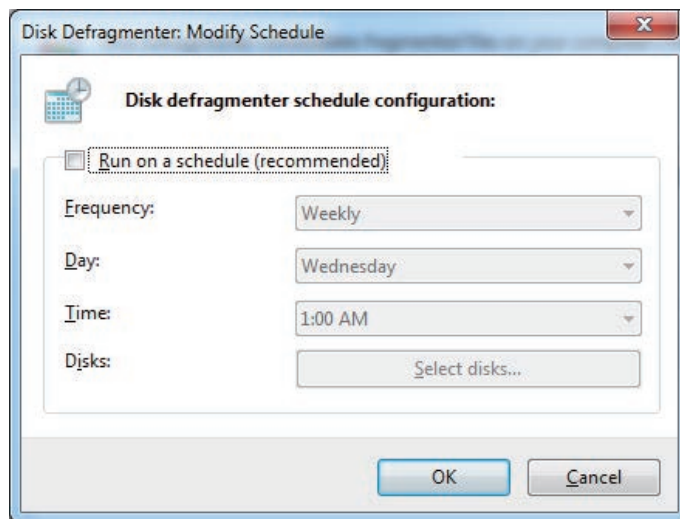


Figure B3.2.1-8 Modify Schedule Dialog Box

## B3.2.2 Configuring on Windows Vista

Follow these procedures when you use a Windows Vista computer.

### ■ File System

Ensure that the file system is in the NTFS format. If it is already formatted in the FAT format, reinstall the operating system and reformat partitions into NTFS. Partitions not installed with OS should also be formatted into NTFS.

### ■ System Performance

Follow these steps to configure the system performance setting:

1. Log on as an administrative user.
2. From the Start menu, select [Control Panel] > [System and Maintenance] > [System] > [Advanced system settings].  
The System Properties dialog box appears.
3. Select the [Advanced] tab, and click [Settings] in the Performance section.  
The Performance Options dialog box appears.
4. Click the [Visual Effects] tab and select [Let Windows choose what's best for my computer].

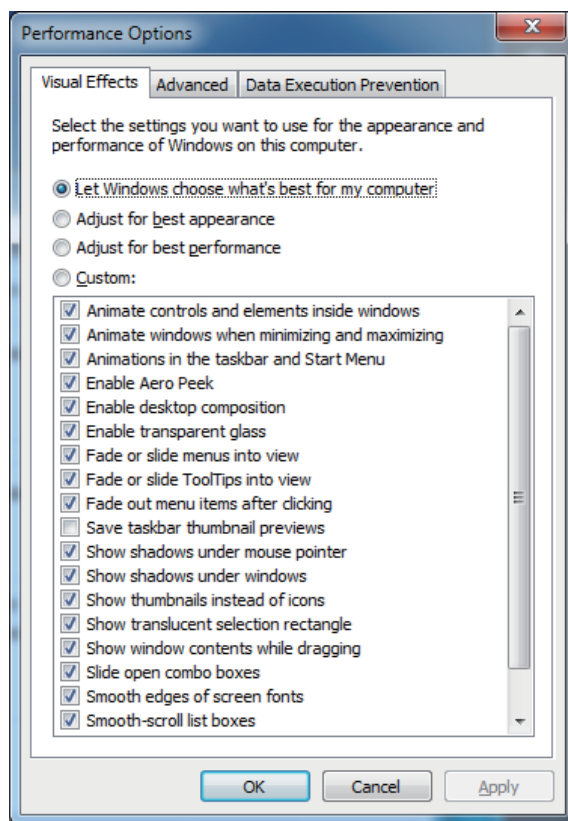


Figure B3.2.2-1 Performance Options Dialog Box (Visual Effects Tab)

5. Click [OK].

## ■ Virtual Memory

ProSafe-RS does not require virtual memory configuration. However, if the ProSafe-RS and CENTUM VP software coexist on the same computer, virtual memory should be configured according to the instruction of CENTUM VP.

## ■ Power Options

This section describes how to configure the Power Options settings. Some of the items in the explanation may not be displayed on your computer, depending on the computer's hardware configuration. If not displayed, the function of that item is not available on your computer.

1. Log on as an administrative user.
2. From the Start menu, select [Control Panel] > [Hardware and Sound] > [Power Options]. The Power Options window appears.
3. Select [High performance] under Preferred plans, and click [Change plan settings] below it. The Edit Plan Settings window appears.
4. Click [Change advanced power settings]. The Power Options dialog box appears, showing the advanced settings.
5. Under Hard disk, set the setting for Turn off hard disk after to [Never].

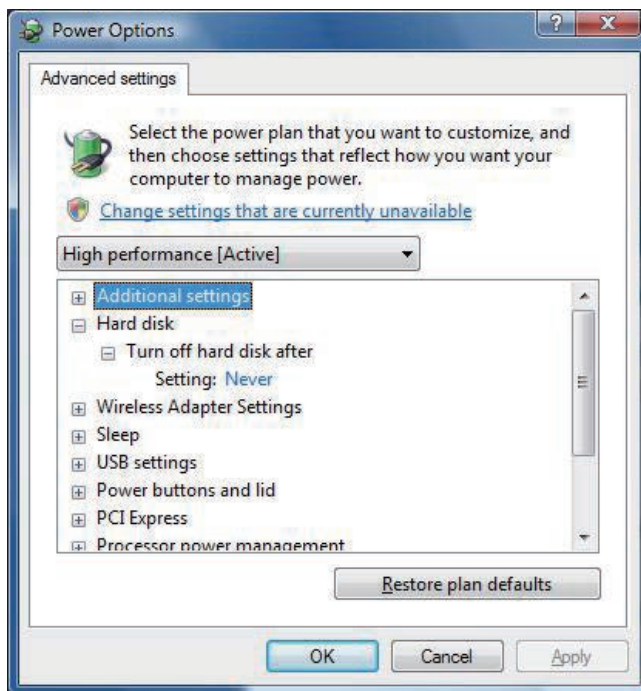


Figure B3.2.2-2 Advanced Settings in Power Options Dialog Box (Hard Disk Setting)

6. Configure the Sleep settings as follows:
  - [Sleep after]: Never
  - [Allow hybrid sleep]: Off
  - [Hibernate after]: Never



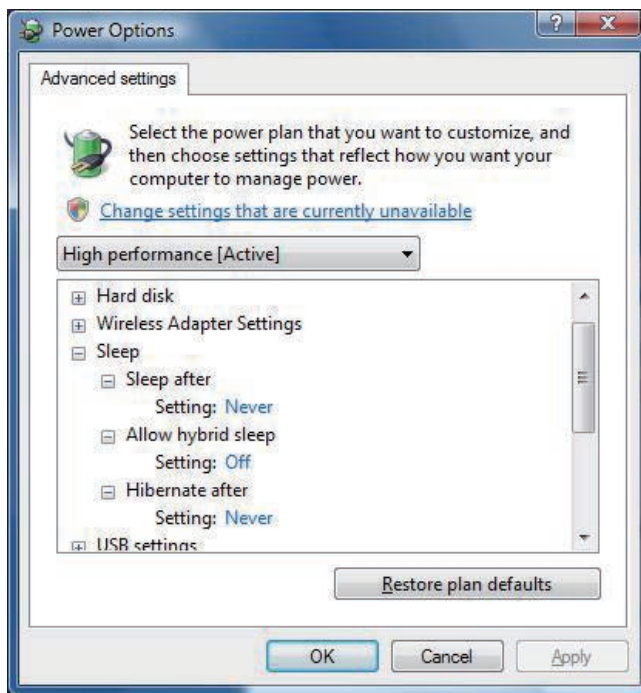


Figure B3.2.2-3 Advanced Settings in Power Options Dialog Box (Sleep Setting)

7. Configure the Power button and lid settings as follows:
  - [Power button action]: Shut down
  - [Start menu power button]: Shut down

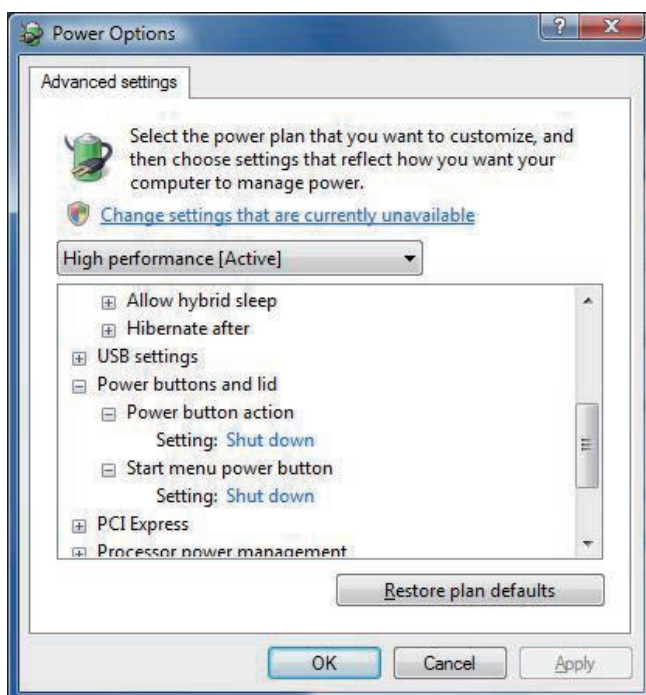


Figure B3.2.2-4 Advanced Settings in Power Options Dialog Box (Power Button and LID Settings)

8. Under Display, set the setting for Turn off display after to [Never].



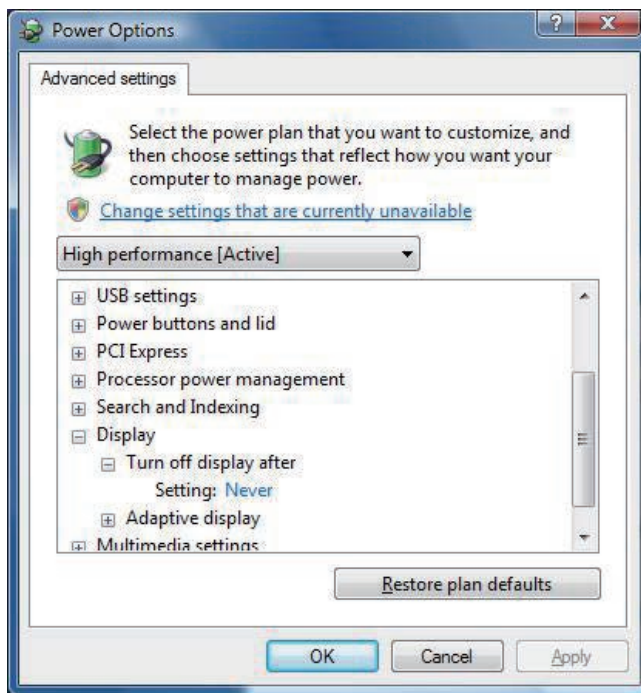


Figure B3.2.2-5 Advanced Settings in Power Options Dialog Box (Display Setting)

9. Click [OK].

**TIP**

Configure UPS service settings after installing the ProSafe-RS software.

**SEE ALSO**

For more information about setting up UPS services, refer to:

[B3.9, "Configuring the Uninterruptible Power Supply \(UPS\) Service" on page B3-83](#)

## ■ Windows Defender

The Windows Defender software detects and removes spy ware.

It is recommended to turn off this function because it is not used in ProSafe-RS.

In a domain environment, turn off Windows Defender on domain member computers at a time by means of a domain management operation such as Group Policies.

In a workgroup environment, turn off Windows Defender by using either of the following procedures.

- Turning Off Windows Defender in Control Panel
- Turning Off Windows Defender in Local Group Policy Editor

**TIP**

If Tools of Windows Defender is grayed out, turn off Windows Defender in Local Group Policy Editor.

### ● Turning Off Windows Defender in Control Panel

1. Log on as an administrative user.
2. From the Start menu, select [Control Panel] > [Security] > [Windows Defender].  
The Windows Defender window appears.
3. Click [Tools] displayed at the top.  
The Tools and Settings window appears.

4. Click [Options].  
The Options window appears.

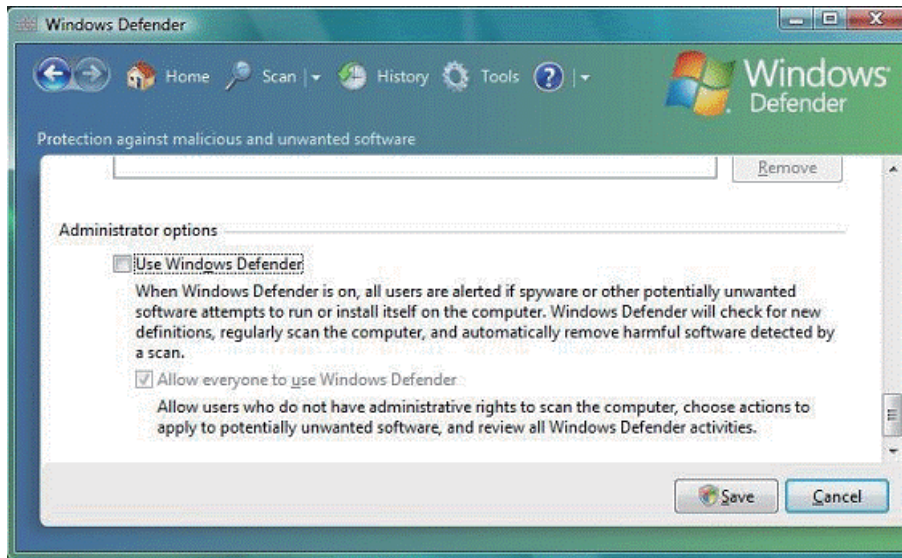


Figure B3.2.2-6 Options

5. Clear the check box for [Use Windows Defender], and click [Save].  
A confirmation dialog box appears.
6. Click [Close].

### ● Turning Off Windows Defender in Local Group Policy Editor

If Tools of Windows Defender is grayed out, you can turn off Windows Defender in Local Group Policy Editor.

Follow these steps to turn off Windows Defender:

1. Log on as an administrative user.
2. Click the Start button of Windows, and enter `gpedit.msc` in the Program and file search box.  
The Local Group Policy Editor window appears.
3. Select [Computer Configuration] > [Administrative Templates] > [Windows Components] > [Windows Defender], and double-click [Turn off Windows Defender] in the right pane.  
The Turn off Windows Defender Properties dialog box appears.
4. Select [Enabled] and click [OK].

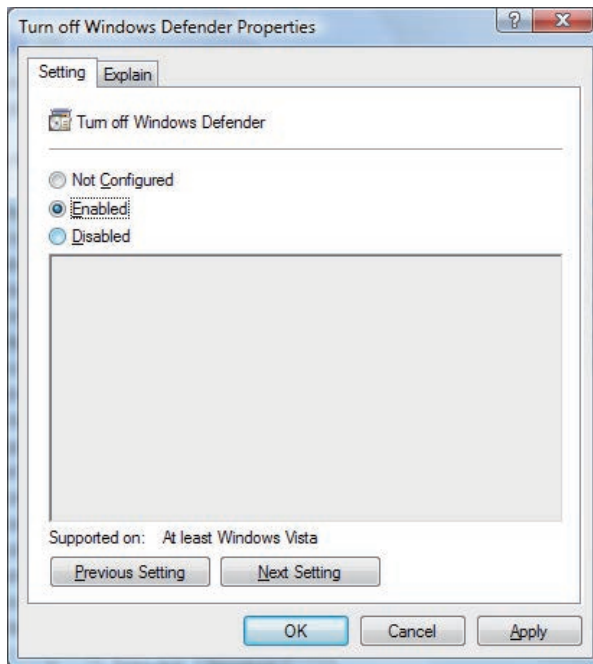


Figure B3.2.2-7 Turn off Windows Defender Properties Dialog Box

## ■ Disk Defragmenter

Disk Defragmenter Tool can be used to reorganize the fragmented files on computer hard disk so as to improve the computer performance. With the default setting of Windows Vista, the Disk Defragmenter Tool is scheduled to start periodically at 1:00 on Wednesday. Because the performance of ProSafe-RS may be affected significantly, it is recommended to disable the periodic disk defragmentation.

Moreover, you may manually start the disk defragmenter when you feel the disk performance is getting worse or when you perform system maintenance.

1. Logon as an administrative user.
2. From the Start menu, select [All Programs] > [Accessories] > [System Tools] > [Disk Defragmenter].  
The Disk Defragmenter dialog box appears.
3. Clear the [Run on a schedule (recommended)] check box and click [OK].

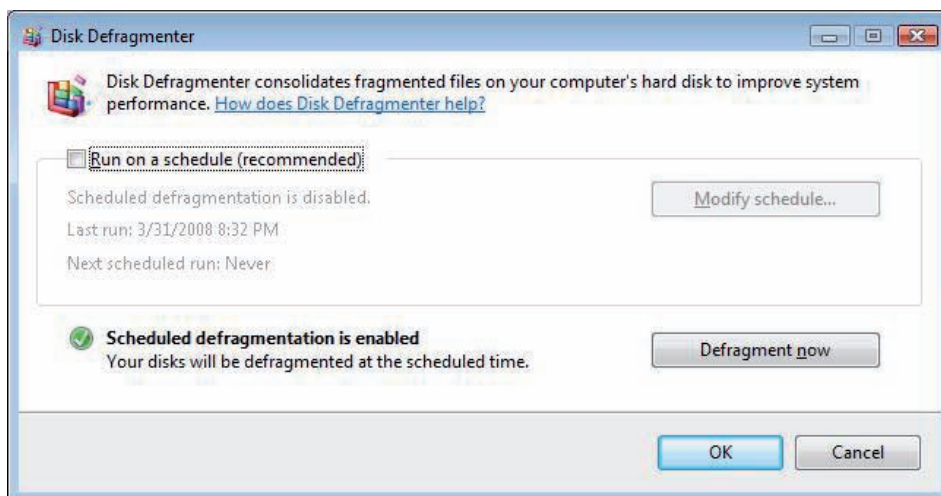


Figure B3.2.2-8 Disk Defragmenter Dialog Box

## B3.2.3 Configuring on Windows Server 2008 R2

Follow these procedures when you use a Windows 2008 R2 computer.

### ■ File System

Ensure that the file system is in the NTFS format. If it is already formatted in the FAT format, reinstall the operating system and reformat partitions into NTFS. Partitions not installed with OS should also be formatted into NTFS.

### ■ System Performance

Follow these steps to configure the system performance setting:

1. Log on as an administrative user.
2. From the Start menu, select [Control Panel] > [System and Security] > [System] > [Advanced system settings].  
The System Properties dialog box appears.
3. Select the [Advanced] tab, and click [Settings] in the Performance section.  
The Performance Options dialog box appears.
4. Select the [Visual Effects] tab and select [Adjust for best performance].

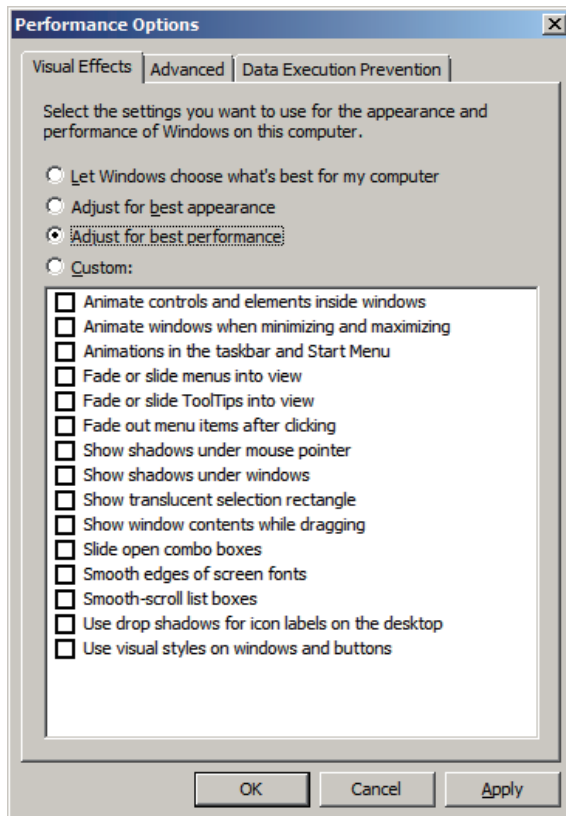


Figure B3.2.3-1 Performance Options Dialog Box (Visual Effects Tab)

5. Click [OK].

### ■ Virtual Memory

ProSafe-RS does not require virtual memory configuration. However, if the ProSafe-RS and CENTUM VP software coexist on the same computer, virtual memory should be configured according to the instruction of CENTUM VP.

## ■ Power Options

This section describes how to configure the Power Options settings. Some of the items in the explanation may not be displayed on your computer, depending on the computer's hardware configuration. If not displayed, the function of that item is not available on your computer.

1. Log on as an administrative user.
2. From the Start menu, select [Control Panel] > [Hardware] > [Power Options].  
The Power Options window appears.
3. Select [High performance] under Preferred plans, and click [Change plan settings] to the right of it.  
The Edit Plan Settings window appears.

### TIP

If High performance does not appear under Preferred plan, click [Show additional plans]. Select [High performance] and then click [Change plan settings] to the right of it.

4. Click [Change advanced power settings].  
The Power Options dialog box appears, showing the advanced settings.

### TIP

Depending on the computer configuration, the items of unavailable functions will not be displayed in the step results hereafter.

5. Under Hard disk, set the setting for Turn off hard disk after to [Never].

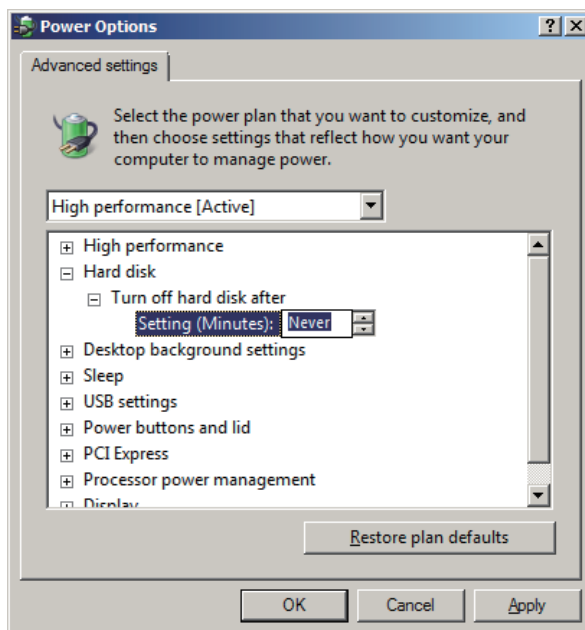
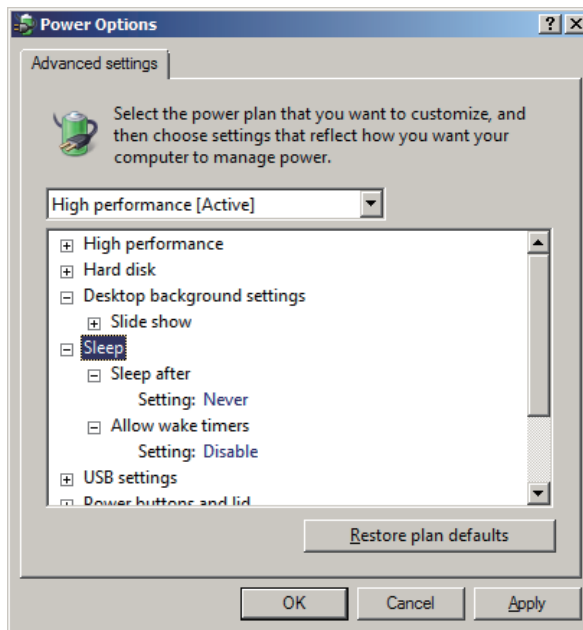


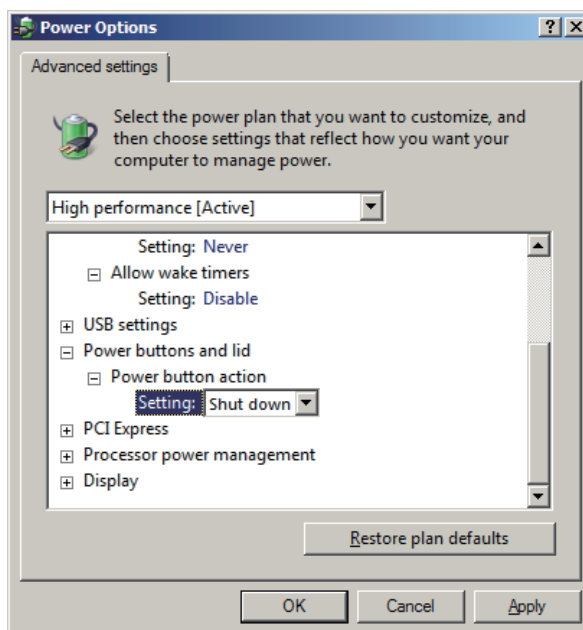
Figure B3.2.3-2 Power Options Advanced Settings

6. Configure the Sleep settings as follows:

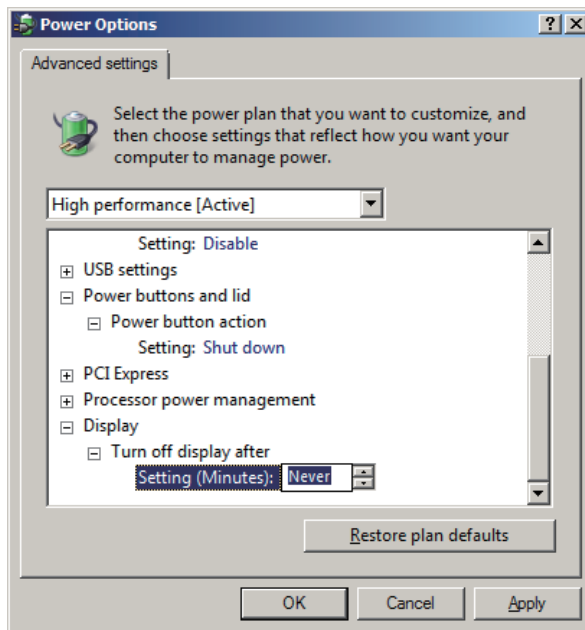
- [Sleep after]: Never
- [Allow hybrid sleep]: Off
- [Hibernate after]: Never
- [Allow wake timers]: Disable

**Figure B3.2.3-3 Power Options Advanced Settings**

7. Set the setting for Power button action under Power buttons and lid to [Shut down].

**Figure B3.2.3-4 Power Options Advanced Settings**

8. Under Display, set the setting for Turn off display after to [Never].



**Figure B3.2.3-5 Power Options Advanced Settings**

9. Click [OK].

#### **TIP**

Configure the UPS settings after installing the ProSafe-RS software.

#### **SEE ALSO**

For more information about setting up UPS services, refer to:

[B3.9, “Configuring the Uninterruptible Power Supply \(UPS\) Service” on page B3-83](#)

## ■ Password Setting

Because security is enhanced in Windows Server 2008 R2, complexity may be required when you set a user password or you may not be able to set a password as intended.

In this case, do the following:

1. Log on as an administrative user.
2. From the Start menu, click [Administrative Tools] > [Local Security Policy].  
The Local security policy window appears.
3. In the left pane, select [Security Settings] > [Account Policies] > [Password Policy].  
A list of policies is displayed.
4. In the right pane, double-click [Password must meet complexity requirements].  
The properties dialog box for the policy Password must meet complexity requirements appears.
5. Select [Disabled] and click [OK].
6. Confirm that Disabled is indicated for the policy Password must meet complexity requirements.



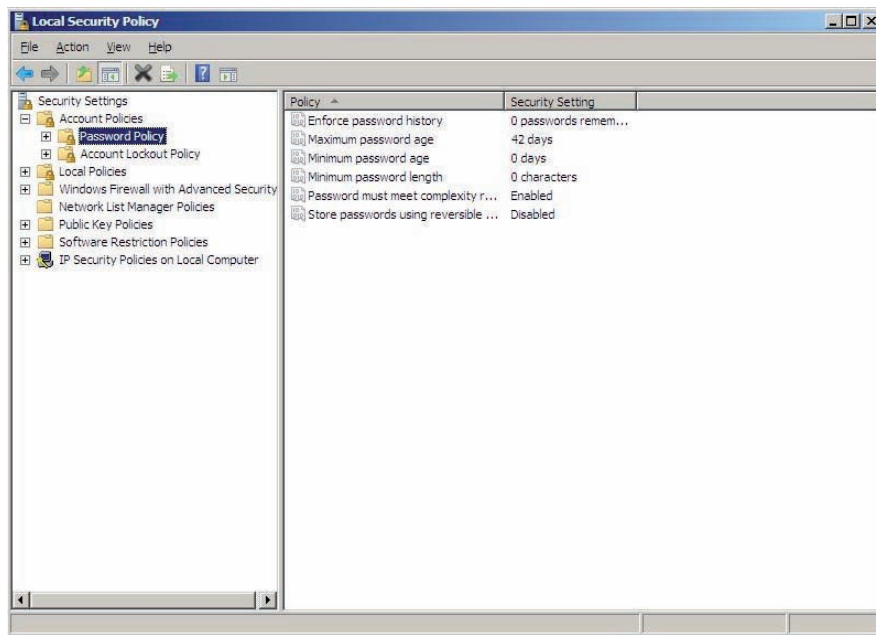


Figure B3.2.3-6 Local Security Policy Window

## ■ Enabling .NET Framework 3.5.1

If you are using Windows Server 2008 R2, you must enable .NET Framework 3.5.1 as it is disabled by default. Follow these steps to enable .NET Framework 3.5.1:

**TIP** .NET Framework 3.0 is also enabled by the same procedure. In this case, you can follow the same procedure to enable .NET Framework 3.0.

1. Log on as an administrative user.
2. From the Start menu, select [Administrative Tools] > [Server Manager].  
The Server Manager window appears.
3. In the left pane, select [Features] and select [Add Features] in the right pane.  
The Add Features Wizard appears.
4. Select the [.NET Framework 3.5.1] check box under .NET Framework 3.5.1 Features, and click [Next].
5. Confirm that the correct feature has been selected for installation and click [Install].
6. Confirm that the installation is completed, and click [Close].



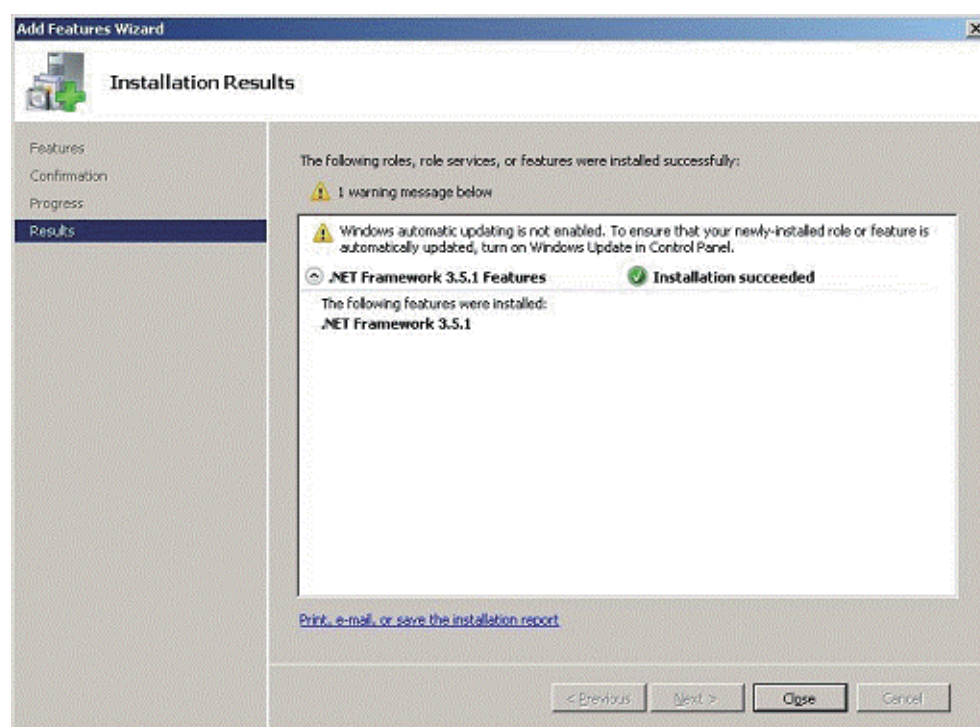


Figure B3.2.3-7 Installation Results

## B3.2.4 Configuring on Windows Server 2008

Follow these procedures when you use a Windows 2008 computer.

### ■ File System

Ensure that the file system is in the NTFS format. If it is already formatted in the FAT format, reinstall the operating system and reformat partitions into NTFS. Partitions not installed with OS should also be formatted into NTFS.

### ■ System Performance

Follow these steps to configure the system performance setting:

1. Log on as an administrative user.
2. From the Start menu, select [Control Panel] > [System and Maintenance] > [System] > [Advanced system settings].  
The System Properties dialog box appears.
3. Select the [Advanced] tab, and click [Settings] in the Performance section.  
The Performance Options dialog box appears.
4. Select the [Visual Effects] tab and select [Adjust for best performance].

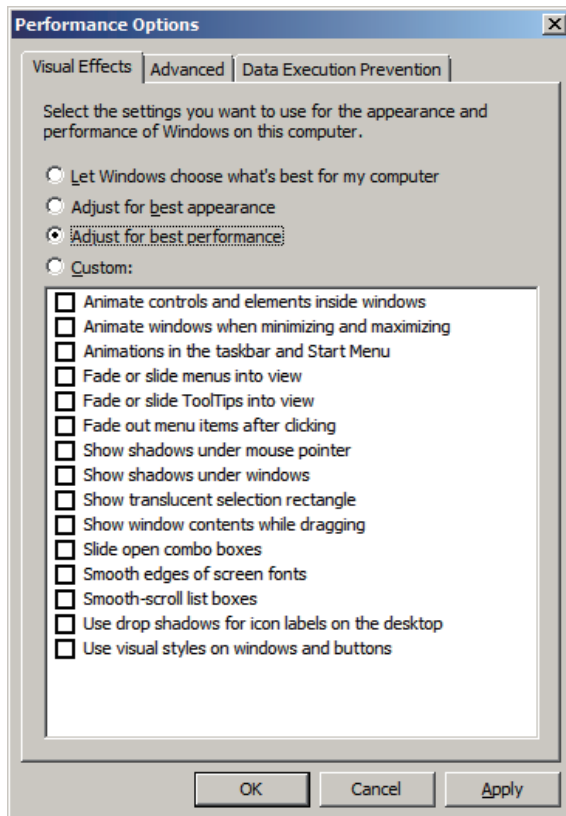


Figure B3.2.4-1 Performance Options Dialog Box (Visual Effects Tab)

5. Click [OK].

### ■ Virtual Memory

ProSafe-RS does not require virtual memory configuration. However, if the ProSafe-RS and CENTUM VP software coexist on the same computer, virtual memory should be configured according to the instruction of CENTUM VP.

## ■ Power Options

This section describes how to configure the Power Options settings. Some of the items in the explanation may not be displayed on your computer, depending on the computer's hardware configuration. If not displayed, the function of that item is not available on your computer.

1. Log on as an administrative user.
2. From the Start menu, select [Control Panel] > [Hardware and Sound] > [Power Options]. The Power Options window appears.
3. Select [High performance] under Preferred plans, and click [Change plan settings] below it. The Edit Plan Settings window appears.
4. Click [Change advanced power settings]. The Power Options dialog box appears, showing the advanced settings.

### TIP

Depending on the computer configuration, the items of unavailable functions will not be displayed in the step results hereafter.

5. Under Hard disk, set the setting for Turn off hard disk after to [Never].

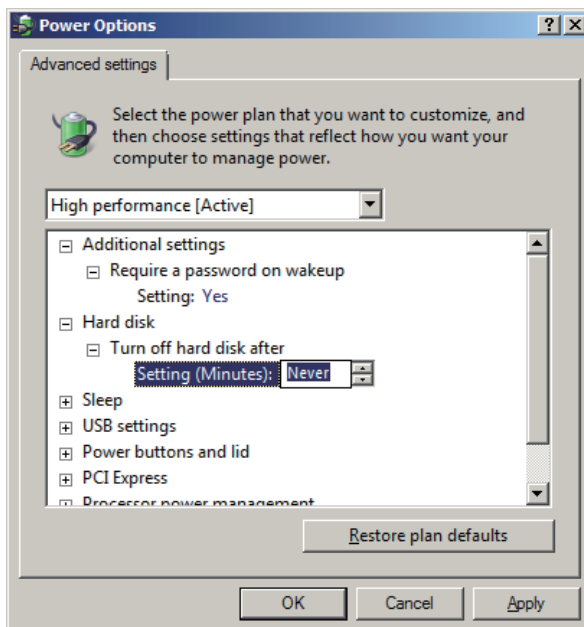


Figure B3.2.4-2 Power Options Advanced Settings

6. Configure the Sleep settings as follows:
  - [Sleep after]: Never
  - [Allow hybrid sleep]: Off
  - [Hibernate after]: Never

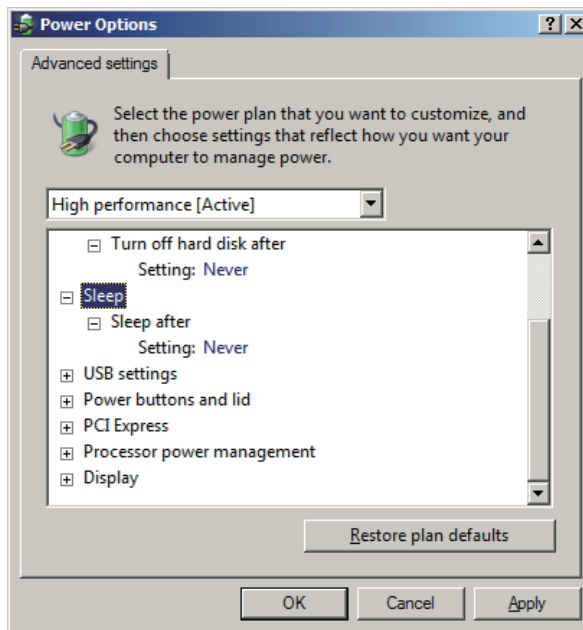


Figure B3.2.4-3 Power Options Advanced Settings

7. Configure the Power button and lid settings as follows:

- [Power button action]: Shut down
- [Start menu power button]: Shut down

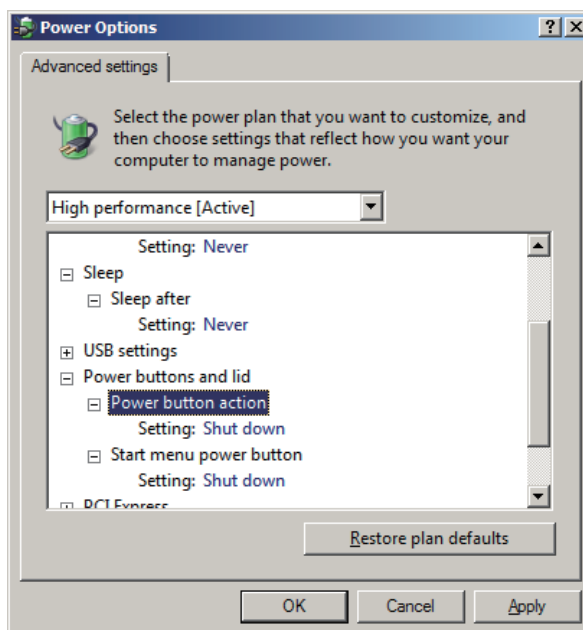
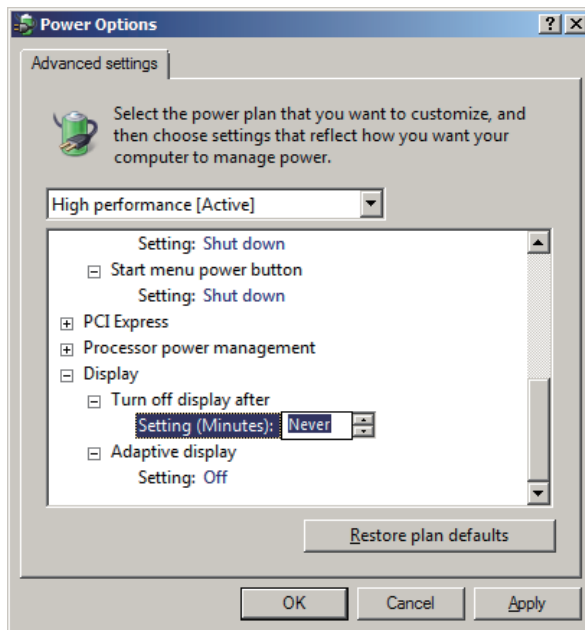


Figure B3.2.4-4 Power Options Advanced Settings

8. Under Display, set the setting for Turn off display after to [Never].



**Figure B3.2.4-5 Power Options Advanced Settings**

9. Click [OK].

#### TIP

Configure the UPS settings after installing the ProSafe-RS software.

#### SEE ALSO

For more information about setting up UPS services, refer to:

[B3.9, "Configuring the Uninterruptible Power Supply \(UPS\) Service" on page B3-83](#)

## ■ Password Setting

Because security is enhanced in Windows Server 2008, complexity may be required when you set a user password or you may not be able to set a password as intended.

In this case, do the following:

1. Log on as an administrative user.
2. From the Start menu, click [Administrative Tools] > [Local Security Policy].  
The Local security policy window appears.
3. In the left pane, select [Security Settings] > [Account Policies] > [Password Policy].  
A list of policies is displayed.
4. In the right pane, double-click [Password must meet complexity requirements].  
The properties dialog box for the policy Password must meet complexity requirements appears.
5. Select [Disabled] and click [OK].
6. Confirm that Disabled is indicated for the policy Password must meet complexity requirements.

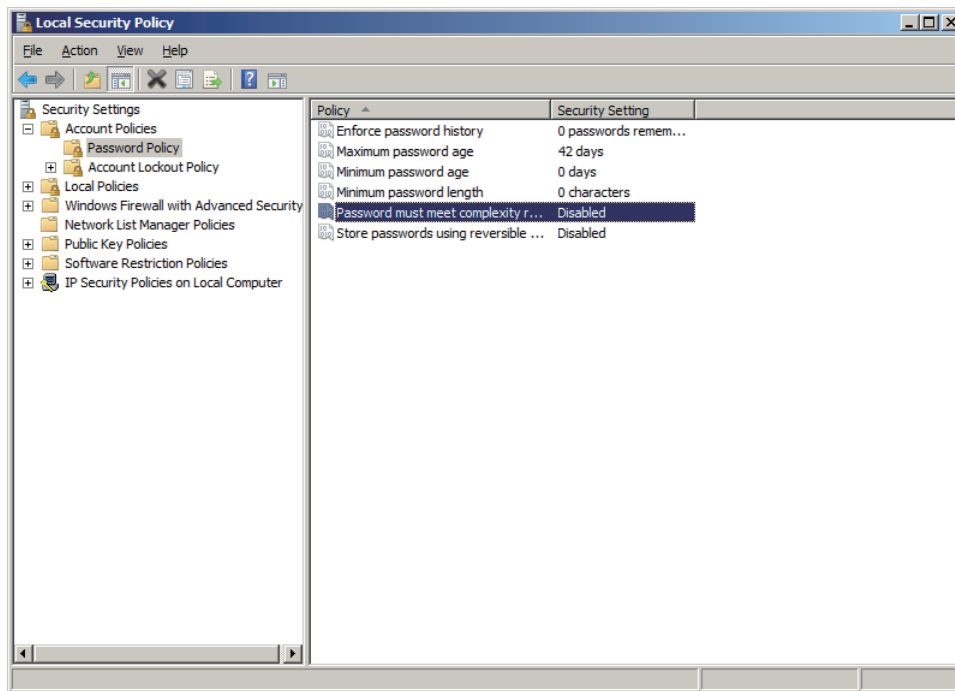


Figure B3.2.4-6 Local Security Policy Window

---

## **B3.3 Configuring Network Settings**

To use the control bus, you need to install the control bus driver. If Vnet/IP is used as the control bus, you need to install the Vnet/IP open communication driver as well.

This section describes how to install the control bus driver and the Vnet/IP open communication driver.

If you use the built-in Ethernet interface of the computer or an over-the-counter Ethernet card, read the attached instruction manual and install the proper Ethernet driver accordingly.

## B3.3.1 Installing the Control Bus Driver

This section describes the procedure for installing the control bus driver on Windows 7 as an instance.

### ■ Precautions at Installation

Mount a control bus interface card or Vnet/IP interface card in computers to be connected on a control bus network. In addition, you must install the control bus driver. Observe the following precautions when you install the control bus driver.

- Before installing the control bus driver, be sure to install a control bus interface card or Vnet/IP interface card in the computer.
- If you installed the control bus driver without installing a control bus interface card or Vnet/IP interface card by mistake, uninstall the control bus driver. Then, install a control bus interface card and install the driver again.
- If you want to change the slot in which a control bus interface card or Vnet/IP interface card is installed, uninstall the control bus driver first and then change the slot. After changing the slot, install the driver again.
- When you remove a control bus interface card or Vnet/IP interface card from the computer where the control bus driver was installed with the card installed, uninstall the driver before you remove the card from the slot.

#### TIP

- When installing the control bus driver, restarting the computer is basically not required. However, restart the computer if a dialog box indicating completion of the installation (restarting required) is displayed.
- After you install the driver, you need to configure network settings.

### ■ Notes on Using SCS Simulator

To use the SCS simulator, an environment where ProSafe-RS is integrated with CENTUM is mandatory. You can run the SCS simulator even on a computer where a control bus interface card or Vnet/IP interface is not mounted; however, you must always install the control bus driver on such computers. Observe the following precautions when you install the control bus driver on a computer where these cards are not mounted in order to use the SCS simulator.

- Install the control bus driver, and then configure Windows network settings.
- If you use the expanded test functions to run SCS simulators on multiple computers, install the control bus driver in all the computers on which you run the SCS simulator without mounting a control bus card. If mounted, you cannot launch the SCS simulator remotely.

#### TIP

- If a control bus card is not mounted when you install the control bus driver, a control bus driver of the version for use without a control bus card is installed. This driver is used when the SCS simulator is run without mounting a control bus card.
- To reuse or divert a computer installed with a without-a-control-bus-card version of control bus driver for use in actual plant operation, uninstall the control bus driver, mount a control bus card, and then install the control bus driver again.

- The control bus driver should be installed according to the procedure for installing the control bus driver.
- For the IP address for the control bus driver on each computer, set the address of control bus, "domain number (dd) .station number (ss)".  
Example: 172.16.dd.ss

Note that dd.ss must not overlap with the addresses of the other stations. In particular, it must not overlap with the "domain number.station number" used for SCS and FCS.



## ■ Installation Procedure

1. Log on as an administrative user.
2. Insert the ProSafe-RS software medium into the drive.
  - If the AutoPlay dialog box appears, click [Run Launcher.exe].
  - If the AutoPlay dialog box does not appear, use Explorer and double-click Launcher.exe in the top folder of the ProSafe-RS software medium.

The installation menu appears.

3. On the installation menu, click [Control Bus Driver].  
A dialog box appears, prompting you to confirm the setup.
4. Select [INSTALL] and click [OK].  
A dialog box appears, confirming to execute the installation.
5. Click [OK].  
A Windows Security dialog box appears, confirming installation of network protocol.
6. Make sure that the [Always trust software from “Yokogawa Electric Corporation”] check box is clear and click [Install].  
Another Windows Security dialog box appears, confirming installation of the network adapter.
7. Make sure that the [Always trust software from “Yokogawa Electric Corporation”] check box is clear and click [Install].

---

**TIP**

- Do not click [Don't Install] on the Windows Security dialog boxes. If clicked, an error occurs.
  - Do not select the [Always trust software from “Yokogawa Electric Corporation”] check box. If selected, a confirmation dialog box will not appear during the subsequent installations.
- 

8. When the message telling successful installation is displayed, click [OK].

---

**TIP**

If you have added or deleted any other devices before you install the control bus driver, a message prompting you to restart the computer may be displayed. In such a case, be sure to restart the computer.

---

## B3.3.2 Installing the Vnet/IP Open Communication Driver

When Vnet/IP is used as the control bus, the Vnet/IP open communication driver also needs to be installed. If Ethernet is also used, the installed Vnet/IP open communication driver must be disabled.

This section describes the procedure for installing the Vnet/IP open communication driver on Windows 7 as an instance.



### IMPORTANT

When the Vnet/IP interface card is mounted, always install the Vnet/IP open communication driver even if Vnet/IP open communication is not used.

### ■ Precautions at Installation

- Before installing the Vnet/IP open communication driver, be sure to install a Vnet/IP interface card in the computer. You cannot install the driver if the card is not installed.
- If you want to change the slot in which a Vnet/IP interface card is mounted, uninstall the Vnet/IP open communication driver and control bus driver and then change the slot. After changing the slot, install the drivers again.
- When removing a Vnet/IP interface card from a computer after the Vnet/IP open communication driver is installed, uninstall the driver before you remove the card from the slot.

#### TIP

- When installing the Vnet/IP open communication driver, restarting the computer is basically not required. However, restart the computer if a dialog box indicating completion of the installation (restarting required) is displayed.
- When Ethernet is also used, configure network settings after you install the Vnet/IP open communication driver and disable the driver.

When Ethernet is not used, configure network settings after you install the Vnet/IP open communication driver.

### ■ Installation Procedure

1. Log on as an administrative user.
2. Insert the ProSafe-RS software medium into the drive.
  - If the AutoPlay dialog box appears, click [Run Launcher.exe].
  - If the AutoPlay dialog box does not appear, use Explorer and double-click Launcher.exe in the top folder of the ProSafe-RS software medium.

The installation menu appears.

3. On the installation menu, click the [Vnet/IP Open com driver].  
A dialog box appears, prompting you to confirm the setup.
4. Select [INSTALL] and click [OK].  
A dialog box appears, confirming to execute the installation.
5. Click [OK].  
A Windows Security dialog box appears.
6. Make sure that the [Always trust software from “Yokogawa Electric Corporation”] check box is clear and click [Install].

**TIP**

- Do not click [Don't Install] on the Windows Security dialog box. If clicked, an error occurs.
- Do not select the [Always trust software from "Yokogawa Electric Corporation"] check box. If selected, a confirmation dialog box will not appear during the subsequent installations.

7. When the message telling successful installation is displayed, click [OK].

**TIP**

If you have added or deleted any other devices before you install the Vnet/IP open communication driver, a message prompting you to restart the computer may be displayed. In such a case, be sure to restart the computer.

### B3.3.3 Configuring Windows Network Settings

You must configure the Windows network settings after installing the network driver.

This section explains the procedures for configuring Windows network settings related to control bus, Vnet/IP open communication, and Ethernet, assuming settings are made on Windows 7/Windows Server 2008 R2. Information of other OS versions is provided as necessary as TIP.

#### ■ Cautions on Cable Wiring

When the cable is wired for network connection, the Set Network Location dialog box may appear.

**SEE  
ALSO**

For more information about the Set Network Location dialog box, refer to:

[C9.2.1, "Precaution on Network Cable Connection" on page C9-4](#)

#### ■ Checking the Network Interface Card

Check the network interface card installed in the computer.

- **When a Control Bus Interface Card is Installed**

In a system using V net, a control bus interface card is installed in computers. In this case, configure Windows network settings for control bus communications and Ethernet communications.

- **When a Vnet/IP Interface Card is Installed**

In a system using Vnet/IP, a Vnet/IP interface card is installed in computers.

In this case, a combination of either control bus communications and Ethernet communications or control bus communications and Vnet/IP open communications is used. Configure the Windows network settings according to the network configuration of the system.

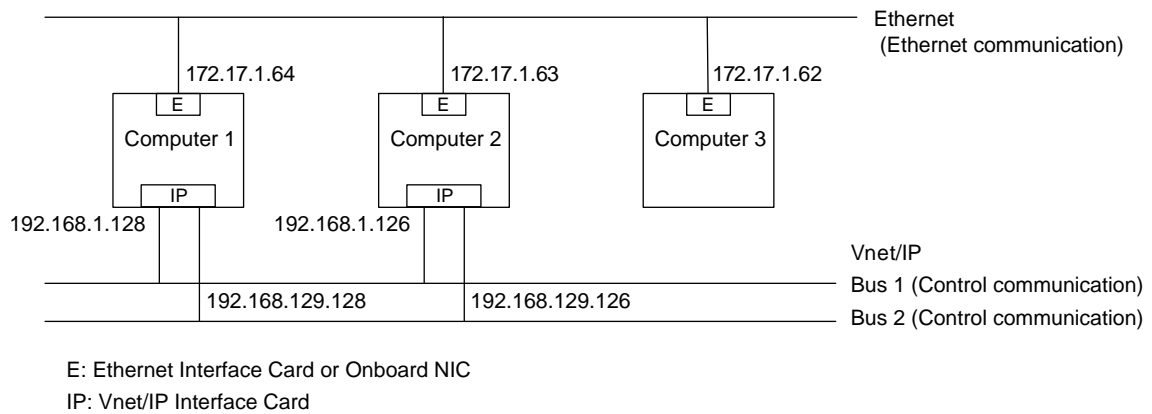
**TIP**

The Vnet/IP open communication refers to Ethernet communication performed on bus 2 of Vnet/IP.

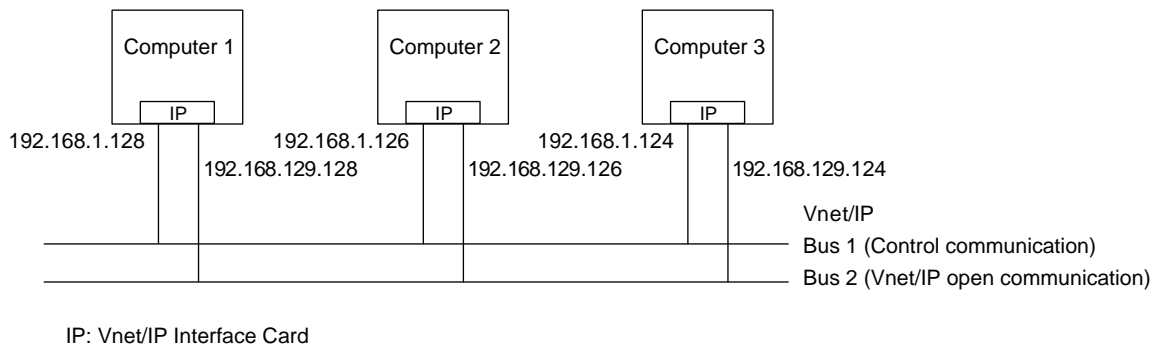
In a system using Vnet/IP open communications, bus 1 is normally used for control bus communications and bus 2 is used for Ethernet communications. If bus 1 fails, bus 2 is used for both control bus communications and Ethernet communications.

#### ■ Vnet/IP Network Configurations and Windows Network Settings

Vnet/IP network configurations and their required Windows network settings are describes as follows.



**Figure B3.3.3-1 Network Configuration and Interface (Vnet/IP and Ethernet are Installed)**



**Figure B3.3.3-2 Network Configuration and Interface (Only Vnet/IP is Installed)**

**Table B3.3.3-1 Network Configurations and Network Connections to be Set Up on Windows**

Network Configuration	Computer (Example in the figures)	Network connection to be set up on Windows
Vnet/IP + Ethernet	Connected to Vnet/IP and Ethernet (Computers 1 and 2)	Control bus, Ethernet, and Vnet/IP open communications(*1)
	Connected to Ethernet only (Computer 3)	Ethernet communications
Vnet/IP only	Connected to Vnet/IP (Ethernet communication on bus 2) (Computers 1 to 3)	Control bus, Ethernet, and Vnet/IP open communications(*2)

\*1: After installing the Vnet/IP open communication driver, you need to disable the corresponding device.

\*2: You need to disable the Ethernet device.

**SEE  
ALSO**

For more information about network construction when using Vnet/IP open communication, refer to:

Vnet/IP Network Construction Guide (Legacy Edition) (TI 30A10A10-01E)

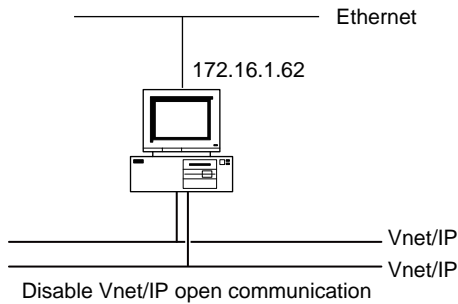
## ■ Cautions on Using Vnet/IP

On the computers connected on Vnet/IP, you need to disable the unused devices according to the network configuration.

- **When Vnet/IP and Ethernet are Installed**

**IMPORTANT**

In a system where both Vnet/IP and Ethernet are Installed, Vnet/IP open communications are not used. Even in this case, you need to install the Vnet/IP open communication driver and disable the driver on computers installed with a Vnet/IP interface card.



**Figure B3.3.3-3 Vnet/IP and Ethernet are Installed**

On a computer installed with a Vnet/IP interface card, follow these steps to disable the Vnet/IP Open communication driver:

1. Log on as an administrative user.
2. From the Start menu, select [Control Panel] > [System and Security] > [Device Manager].

**TIP**

In Windows Vista and Windows Server 2008 environment, select [Control Panel] > [System and Maintenance] > [System] > [Device Manager].

3. On Device Manager, unfold Network adapters.
4. Select [Vnet/IP Open Communication Driver (BUS2)] and then click the Disable button on the toolbar.

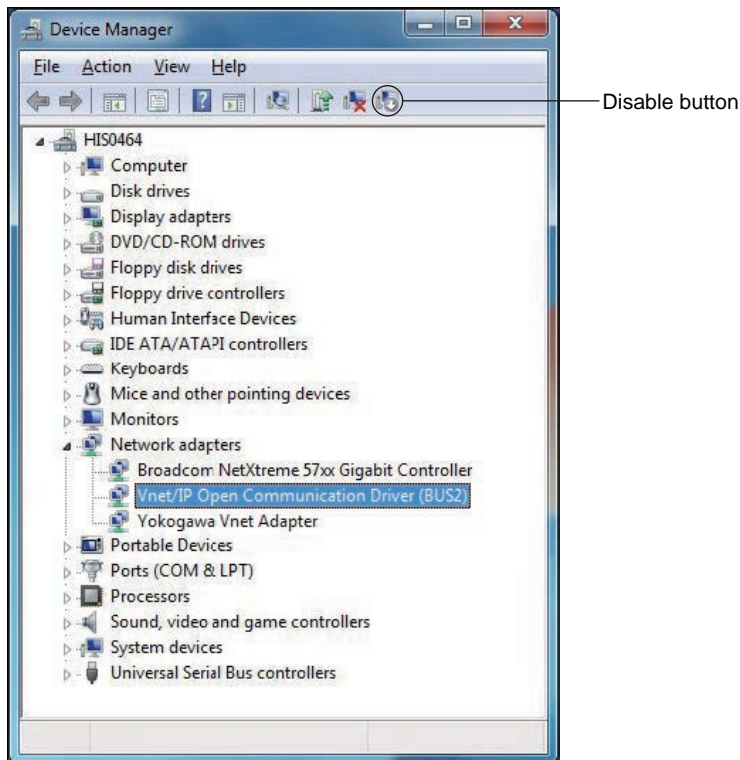


Figure B3.3.3-4 Disabling the Vnet/IP Open Communication Device

### ● When Only Vnet/IP is Installed

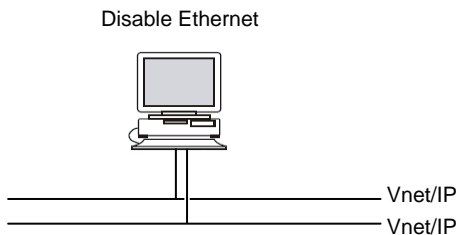


Figure B3.3.3-5 Only Vnet/IP is Installed

On a computer in a system where only Vnet/IP is installed, follow these steps to disable the Ethernet device:

1. Log on as an administrative user.
2. From the Start menu, select [Control Panel] > [System and Security] > [Device Manager].

#### TIP

In Windows Vista and Windows Server 2008 environment, select [Control Panel] > [System and Maintenance] > [System] > [Device Manager].

3. On Device Manager, unfold Network adapters.
4. Select the Ethernet device and then click the Disable button on the toolbar.

### ■ Prohibitions

Do not use the following features in ProSafe-RS.

- Internet Connection Sharing (ICS)
- Bridge Connection

- Homegroup

### ● Internet Connection Sharing (ICS)

Do not select the [Allow other network users to connect through this computer's Internet connection] check box on the Sharing tab in the properties dialog box for V net, VnetIPOpen, or Ethernet (these connection names are set in the procedures described later).

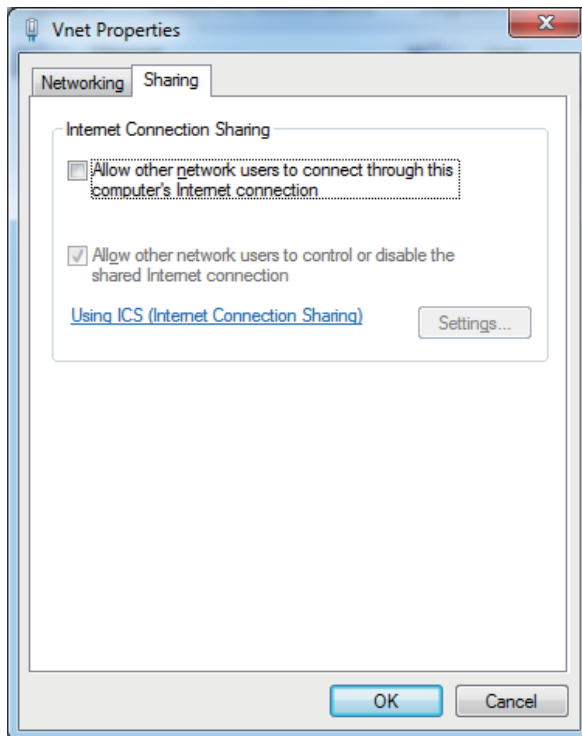


Figure B3.3.3-6 Vnet Properties (Default Setting)

#### TIP

Internet Connection Sharing (ICS) is for sharing the internet connection by the computers in a small scale office network or home network.

### ● Bridge Connection

Do not use bridge connection. If bridge connection is created in the computer, not only the control bus communication of the computer becomes abnormal, but also the communication of the whole control bus network may be jeopardized. (If the bridge connection is already created, you need to delete the bridge connection.)

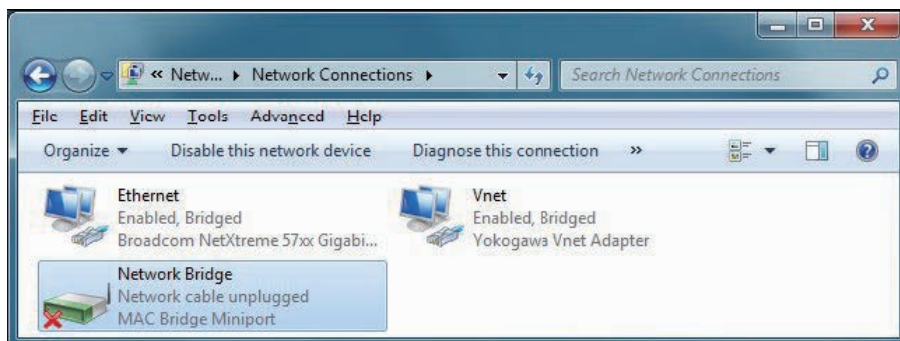


Figure B3.3.3-7 Example of Prohibited Network Setting (Bridge Connection is Enabled)



### ● Homegroup (Windows 7 Only)

In a ProSafe-RS system, folders and printers are shared using the file sharing function for the workgroup/network environment as with the earlier OS versions. Accordingly, do not select [Home Network] in the network location setting.

## ■ Procedure 1: Rename Local Area Connections

A network after the installation is named “Local Area Connection.” The network can be identified more easily if you rename the local area connection.

Rename the local area connections as necessary according to the network configuration of the system.

1. Select [Control Panel] > [Network and Internet] > [Network and Sharing Center].  
The Network and Sharing Center window appears.
2. Select [Change adapter settings].  
The Network Connections window appears.

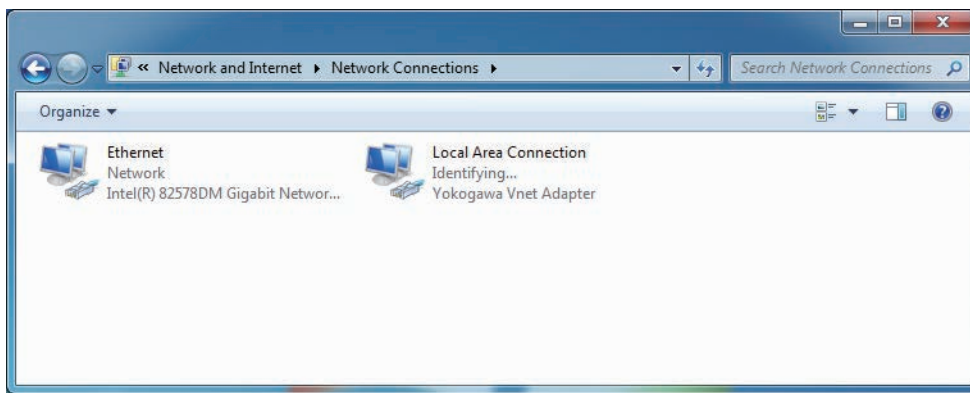


Figure B3.3.3-8 Network Connections (Before Renaming)

#### TIP

- If you are using Windows Vista or Windows Server 2008, select [Manage network connections]
- If connections are not displayed here, the corresponding installations have failed or the drivers are not working properly. Address the issues so that the connections are displayed here.

3. Right-click each of the Local Area Connection icons and select [Rename] to change the name.

Table B3.3.3-2 Renaming of Network Connections

Network type	Display on Network Connections window	Name
Ethernet	Ethernet driver names	Ethernet
Control bus	Yokogawa Vnet Adapter	Vnet
Vnet/IP open communication	Vnet/IP Open Communication Driver (BUS2)	VnetIPOpen

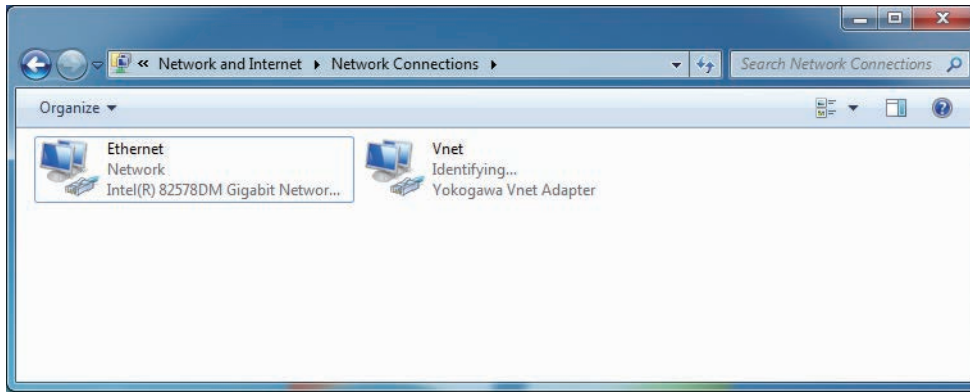


Figure B3.3.3-9 Network Connections – V net Network (After Renaming)

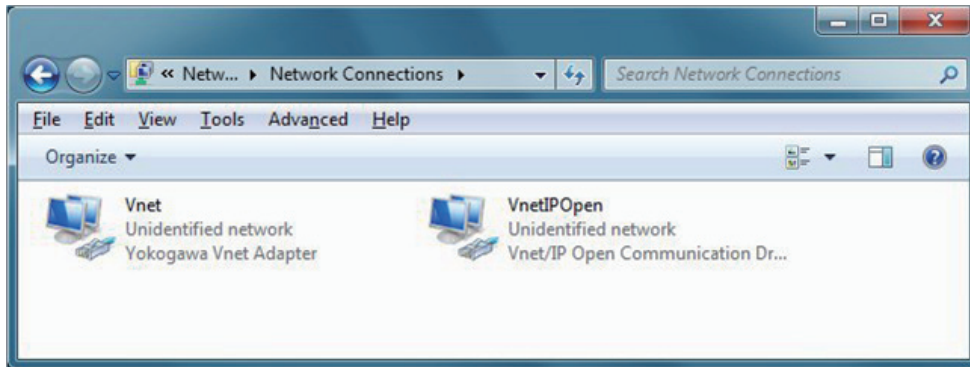


Figure B3.3.3-10 Network Connections – Vnet/IP Network (After Renaming)

**TIP**

In the instruction manuals until ProSafe-RS R2.03, it is instructed to change the name of control bus communication connection when Vnet/IP is used to “VnetIP” rather than “Vnet.”

## ■ Procedure 2: Configure Properties

In the properties of each type of network connection, you need to configure the items to be used.

Configure the properties as necessary according to the network configuration of the system.

Table B3.3.3-3 List of Items Used for Network Connections

Item	Network(*1)		
	Ethernet	VnetIPOpen	Vnet
Microsoft network client	X	X	-
QoS packet scheduler	X	X	-
Microsoft network file and printer sharing	X	X	-
Yokogawa Vnet Protocol	-	-	X
Internet protocol version 6 (TCP/IPv6)	-	-	-
Internet protocol version 4 (TCP/IPv4)	X	X	X
Link-Layer Topology Discovery Mapper I/O Driver	X	X	-
Link-Layer Topology Discovery Responder	X	X	-

\*1: X : Item used, - : Item not used

**TIP** Items in the table, except “Yokogawa Vnet Protocol,” are installed during the Windows OS installation.

### ● V net Properties

1. In the Network Connections window, right-click [Vnet] and select [Properties].  
The Vnet Properties dialog box appears.

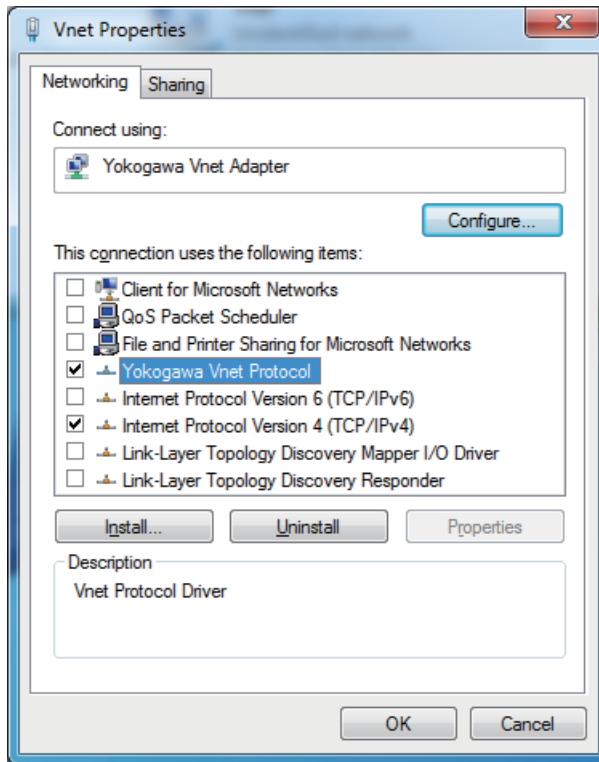


Figure B3.3.3-11 Vnet Properties Dialog Box

2. Based on “Table List of Items Used for Network Connections,” select only the check boxes for [Yokogawa Vnet Protocol] and [Internet protocol version 4 (TCP/IPv4)].
3. After the setting is complete, click [OK].

### ● VnetIPOpen Properties

1. In the Network Connections window, right-click [VnetIPOpen] and select [Properties].  
The VnetIPOpen Properties dialog box appears.

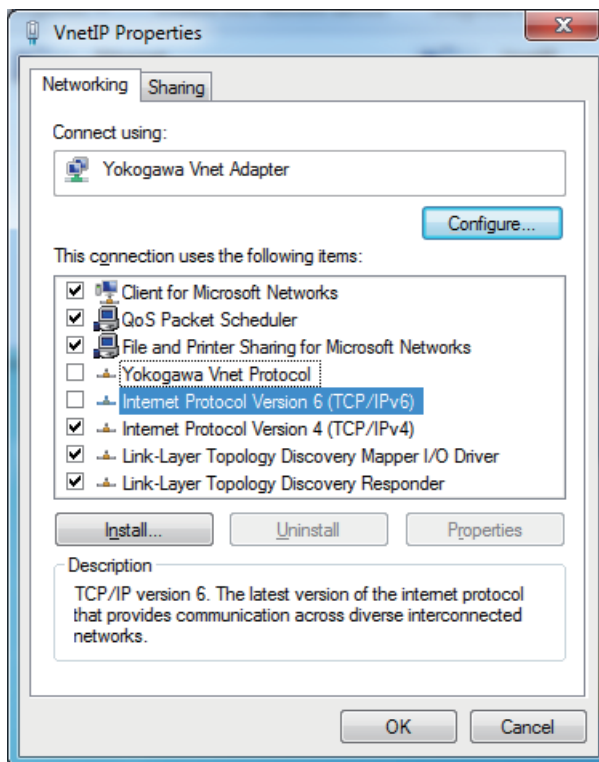


Figure B3.3.3-12 VnetIPOpen Properties Dialog Box

2. Based on “Table List of Items Used for Network Connections,” clear the check boxes for [Yokogawa Vnet Protocol] and [Internet protocol version 6 (TCP/IPv6)].
3. After the setting is complete, click [OK].

### ● Ethernet Properties

1. In the Network Connections window, right-click [Ethernet] and select [Properties]. The Ethernet Properties dialog box appears.

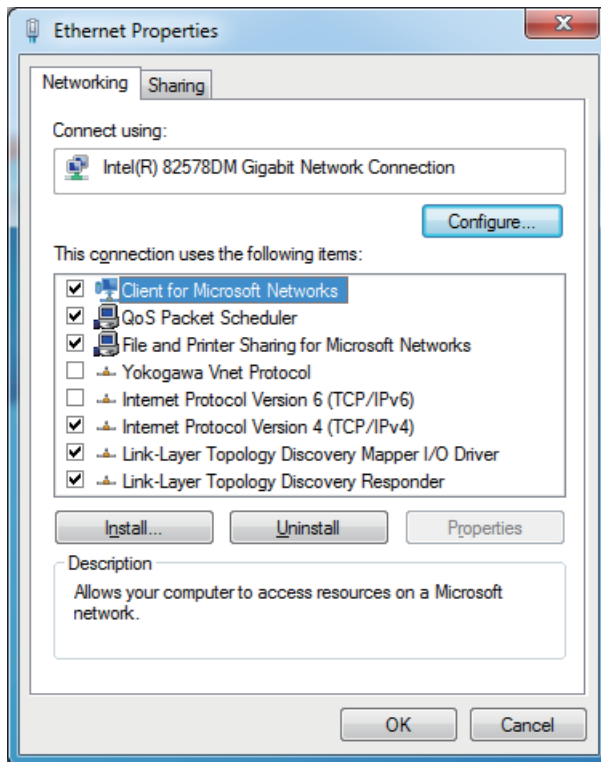


Figure B3.3.3-13 Ethernet Properties Dialog Box

2. Based on “Table List of Items Used for Network Connections,” clear the check boxes for [Yokogawa Vnet Protocol] and [Internet protocol version 6 (TCP/IPv6)].
3. After the setting is complete, click [OK].

## ■ Procedure 3: Set IP Addresses

On Windows, DHCP is enabled by default after a network driver is installed. However, since ProSafe-RS does not use DHCP, you need to set IP addresses. You need to set IP addresses also when the system is used in the domain environment. Set the IP addresses according to the network configuration of the system.

### ● Setting IP Address for Vnet

1. In the Network Connections window, right-click the Vnet icon and select [Properties]. The Vnet Properties dialog box appears.
2. Select [Internet Protocol Version 4 (TCP/IPv4)] and click [Properties]. The Internet Protocol Version 4(TCP/IPv4) Properties dialog box appears.
3. Select [Use the following IP address] and set the IP address, subnet mask, and default gateway. Set the IP address to a standard value that is determined based on the station address of the computer as long as there is no special reason.

**TIP** The standard values for Vnet are as follows:

IP address: 172.16.Domain number.Station number (\*1)

Subnet mask: 255.255.0.0

Default gateway: No setting is required.

\*1: If the network address overlaps with the network address of the existing environment, you can use an address other than 172.16.

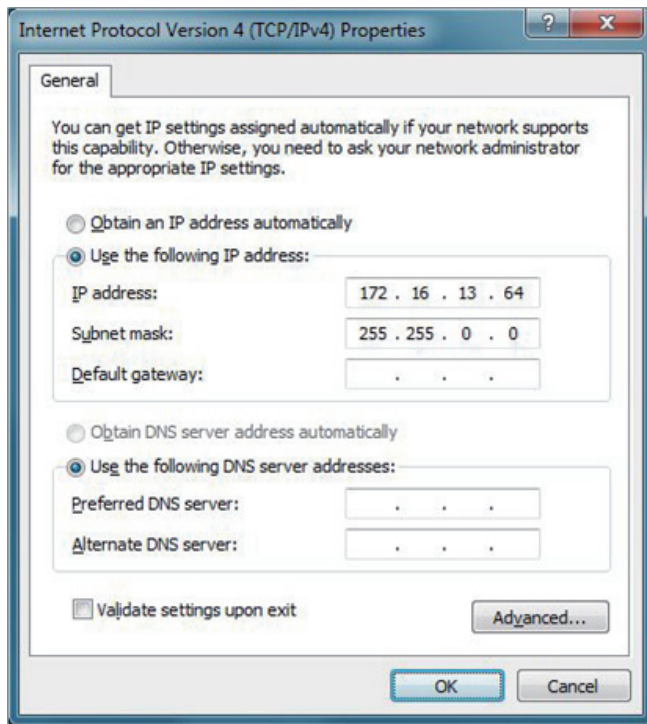


Figure B3.3.3-14 Example of IP Address Setting (Vnet)

4. After the setting is complete, click [OK]. You do not need to restart the computer.

### ● IP Address for VnetIPOpen

This setting is not required when Vnet/IP is used together with Ethernet.

1. In the Network Connections window, right-click the VnetIPOpen icon and select [Properties].  
The VnetIPOpen Properties dialog box appears.
2. Select [Internet Protocol Version 4 (TCP/IPv4)] and click the [Properties].  
The Internet Protocol Version 4 (TCP/IPv4) Properties dialog box appears.
3. Select [Use the following IP address] and specify the following values for the IP address, subnet mask, and default gateway.
  - If the computer is to be used in an existing environment, specify the values used in that network environment.
  - If the computer is to be used in a new environment, specify the standard values determined based on the station address.

#### TIP

The standard values for VnetIPOpen are as follows:

IP address: 192.168.<128 + domain number>.<129 + station number> (\*1)

Subnet mask: 255.255.255.0

Default gateway: Specify the IP address of L3SW if another Vnet/IP domain exists

\*1: Normally, use a standard value. However, you can also use other address.

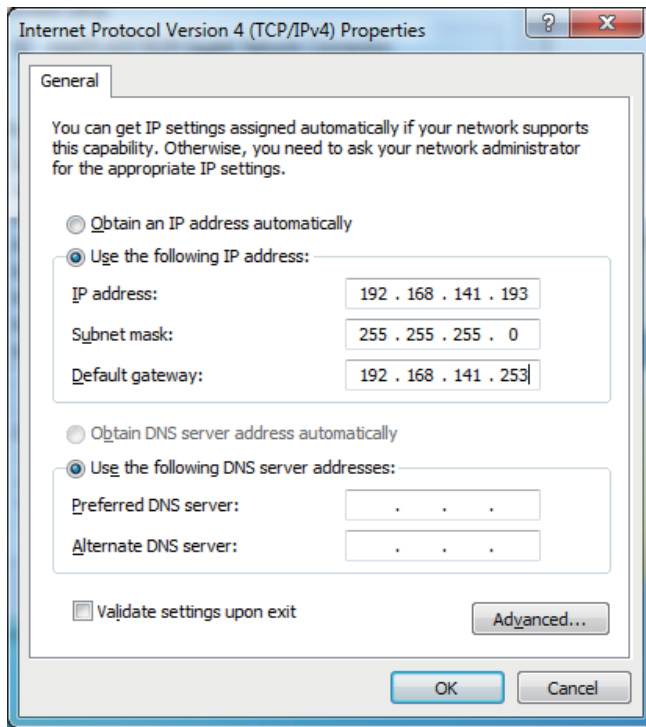


Figure B3.3.3-15 IP Address Setting Example (Vnet/IP Open Communication)

4. After the setting is complete, click [OK]. You do not need to restart the computer.

### ● Setting IP Address for Ethernet

1. In the Network Connections window, right-click the Ethernet icon and select [Properties]. The Ethernet Properties dialog box appears.
2. Select [Internet Protocol Version 4(TCP/IPv4)] and then click [Properties]. Internet Protocol Version 4 (TCP/IPv4) Properties dialog box appears.
3. Select [Use the following IP address] and set the IP address, subnet mask, and default gateway for Ethernet as follows:
  - If the computer is to be used in an existing environment, specify the values used in that network environment.
  - If the computer is to be used in a new environment, specify the standard values determined based on the station address.

#### TIP

The standard values for Ethernet are as follows:

IP address: 172.17.<Domain Number>.<Station Number> (\*1)

Subnet mask: 255.255.0.0

Default gateway: No setting is required.

\*1: Normally, use a standard value. However, you can also use other address.



## IMPORTANT

- In workgroup environment, do not change the settings for DNS server address and the settings accessed by clicking [Advanced].
- In Windows domain environment, you need to set the DNS server address according to the settings of Windows domain server.

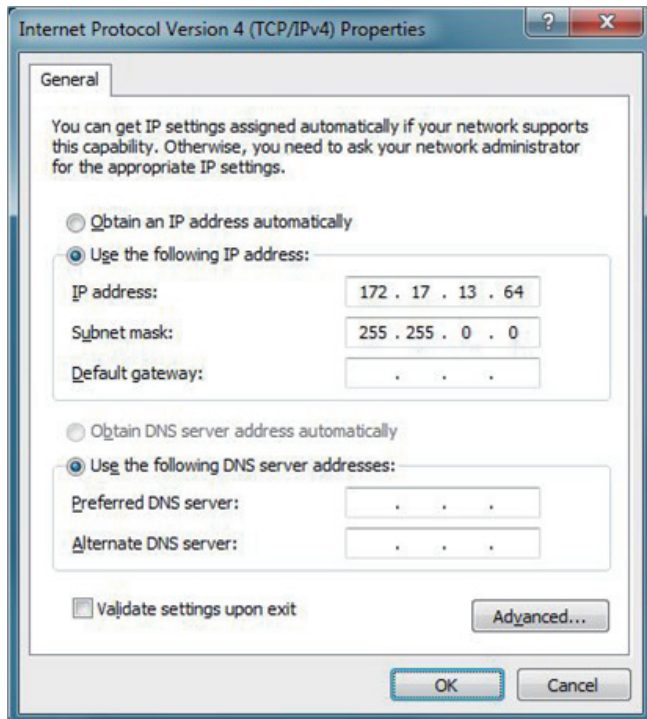


Figure B3.3.3-16 Example of IP Address Setting (Ethernet)

4. After the setting is complete, click [OK]. You do not need to restart the computer.

## ■ Procedure 4: Configure Bindings

You need to configure network bindings because ProSafe-RS uses multiple network devices: combination of Ethernet communication and control bus communication or combination of Vnet/IP open communication and control bus communication. Configure the network bindings according to the network configuration of the system.

If multiple network cards are installed, a card that is installed later has higher priority. Because of this, you need to change the binding settings so that the following priority order is ensured.

- Ethernet has higher priority than Vnet.
- If Vnet/IP open communication is used, VnetIPOpen has higher priority than Vnet.
- If both Vnet/IP open communication and Ethernet are used, the priority shall be in this order: Ethernet, VnetIPOpen, and then Vnet, where Ethernet is the highest.

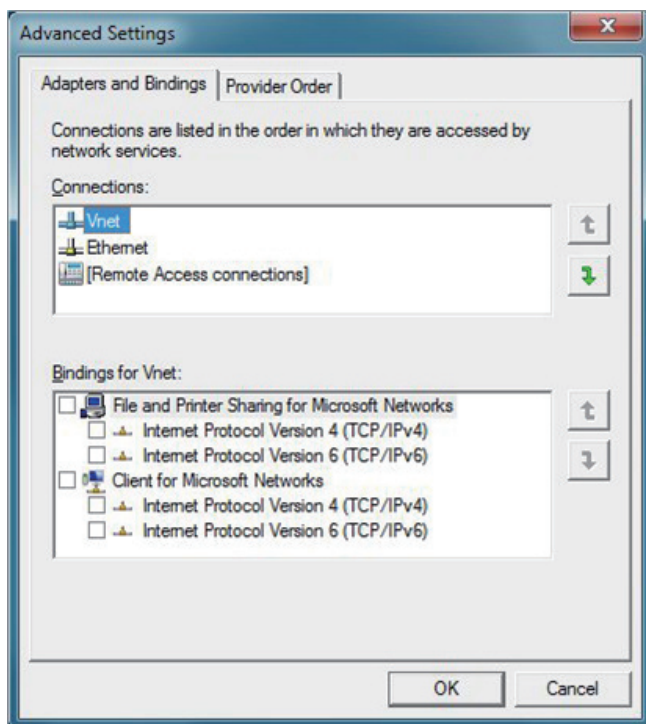
If the system uses Ethernet and Vnet, follow these steps:

1. From the Advanced menu on the Network Connections window, select [Advanced Settings].  
The Advanced Settings dialog box appears.



**TIP**

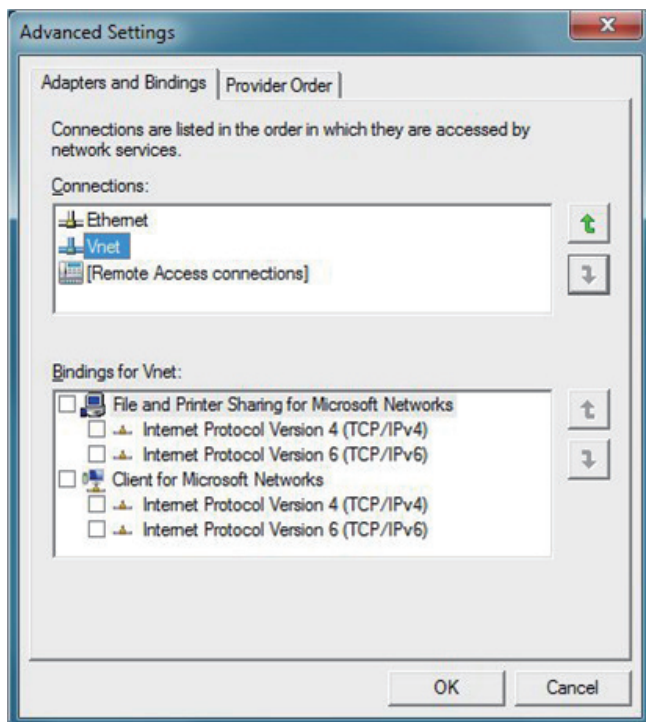
If you cannot find the Advanced menu, press the Alt key to display the menu bar.



**Figure B3.3.3-17 Advanced Settings (Network binding setting is inappropriate)**

In the above figure, the control bus has higher priority than the Ethernet because the control bus (Vnet) driver was installed later than the Ethernet driver.

2. Use the arrow buttons next to the Connections box to set the priority of Ethernet higher than Vnet.



**Figure B3.3.3-18 Advanced Settings (Network binding setting is appropriate)**

3. Click [OK].  
The setting of bindings is finished.

**TIP**

After changing the bindings, there is no need to restart the computer.

**IMPORTANT**

- Do not change the priority of Remote Access connections so as to keep it at the lowest position.
- There is no need to configure the settings on the Provider Order tab.
- Do not change the bindings for Ethernet, Vnet and VnetIPOpen that are shown in the Bindings box below the Connections box.

## ■ Setup Procedure 5: Change Computer Name

It is recommended to set the station names used in the ProSafe-RS system as the computer names.

1. Select [Control Panel] > [System and Security] > [System] > [Advanced system settings].  
The System Properties dialog box appears.
2. In the Computer Name tab, click [Change].  
The Computer Name/Domain Changes dialog box appears.
3. Enter the station name as the new computer name (case-insensitive) for the computer.

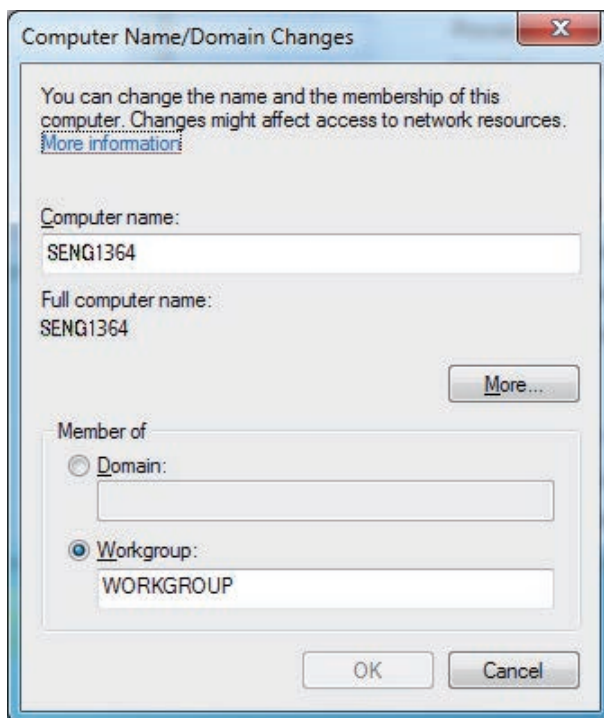


Figure B3.3.3-19 Computer Name/Domain Changes Dialog Box

4. Click [OK].  
A message box appears to prompt for restarting the computer.
5. Restart the computer.

## ■ Procedure 6: Repair TCP/IP Settings

Before you install the ProSafe-RS software, run the TCP/IP Inconsistency Detect Tool. If any inconsistency is found, use the TCP/IP Inconsistency Repair Tool and configure the TCP/IP settings again.

### TIP

On a computer where the control bus driver or Vnet/IP open communication driver had ever been uninstalled, the TCP/IPv4 network settings of IP addresses, subnet masks, and default gateway addresses may be lost every time the computer is restarted. This problem is caused by errors of the Windows OS.

### ● Running the TCP/IP Inconsistency Detect Tool

1. Use Windows Explorer to open the TOOLS directory under the following path in the Pro-Safe-RS software medium.

(Drive of ProSafe-RS software medium):\ProSafe-RS\TOOLS

### TIP

TCP/IP Inconsistency Detect Tool is installed in the following folder when you install the ProSafe-RS software:

(ProSafe-RS Installation Folder)\ProSafe-RS\YOKOGAWA\net\tool

2. Right-click [TcpipInconsistencyDetector.cmd], and select [Run as administrator] from the context menu.  
Messages are displayed according to the inconsistencies detected.
3. Click [OK] to end the tool.

If no inconsistency is detected, the computer can be connected on the network normally.

If no inconsistency is detected, the Windows system continues to work but the network connection may not. You need to use the TCP/IP Inconsistency Repair Tool and then configure the TCP/IP network settings again.

### ● Running TCP/IP Inconsistency Repair Tool



## IMPORTANT

TCP/IP Inconsistency Repair Tool resets the TCP/IP settings of all the network interface cards that are installed in the computer. Therefore, before you run the TCP/IP Inconsistency Repair Tool, you need to write down or save the current settings of the following TCP/IPv4 information for every network interface card:

- IP Address
- Subnet Mask
- Default Gateway

1. Use Windows Explorer to open the TOOLS directory under the following path in the Pro-Safe-RS software medium.

(Drive of ProSafe-RS software medium):\ProSafe-RS\TOOLS

### TIP

TCP/IP Inconsistency Repair Tool is installed in the following folder when you install the ProSafe-RS software:

(ProSafe-RS Installation Folder)\ProSafe-RS\YOKOGAWA\net\tool

2. Right-click [TcpipInconsistencyRepair.cmd], and select [Run as administrator] from the context menu.  
Messages are displayed according to the inconsistencies detected.

3. If no inconsistency is detected in the network settings, click [OK] to end the tool. The computer can be connected on the network normally.
4. If any inconsistency is detected, click [Yes]  
The network settings are reset and a message appears, prompting you to restart the computer.
5. Click [Yes] to restart the computer.
6. After the computer is restarted, re-configure the settings on the Internet Protocol Version 4 (TCP/IPv4) Properties windows for all the network interface cards.

## B3.4 Installing the ProSafe-RS Software

This section describes how to install the ProSafe-RS software.

### ■ Administrative User who Performs New Installation

When installing the ProSafe-RS software for the first time on a computer, the installation must be performed by an administrative user who belongs to the group shown in the following table.

The user who has installed the software is automatically added to the PSF\_MAINTENANCE group.

Table B3.4-1 Groups to Which the User Who Performs New Installation Belongs

Security model and user management type to be applied		
Legacy model	Standard model	
	Standalone management	Domain/Combination management
Administrators of the local computer	Administrators of the local computer	Domain Admins of the domain (*1)

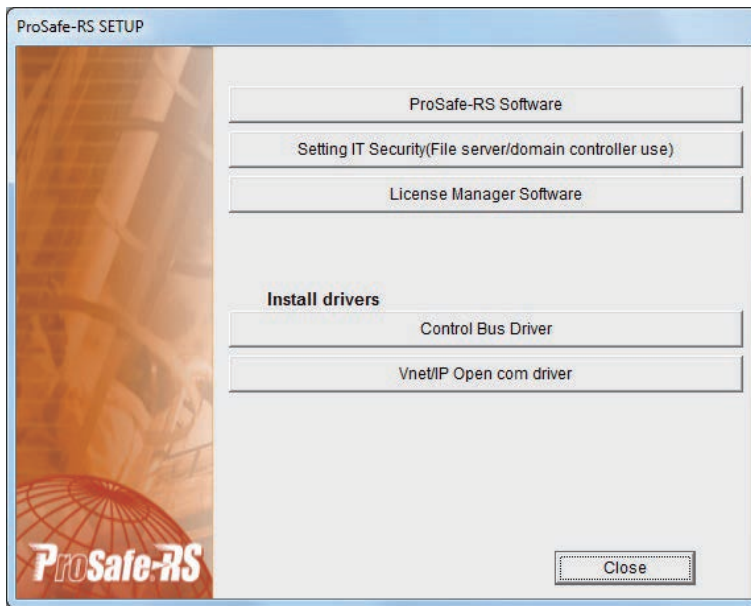
\*1: Install while the computer is connected to the domain.

### ■ Installation Procedure

Follow these steps to install the ProSafe-RS software:

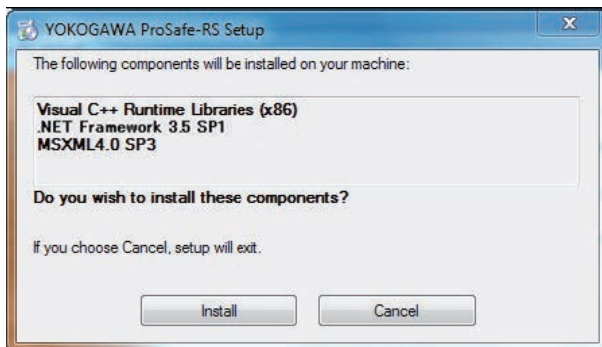
1. Log on as an administrative user.
2. Terminate all running applications, including resident programs such as anti-virus software.
3. Insert the ProSafe-RS software medium into the drive.
  - If the AutoPlay dialog box appears, click [Run Launcher.exe].
  - If the AutoPlay dialog box does not appear, use Explorer and double-click Launcher.exe in the top folder of the ProSafe-RS software medium.

The installation menu appears.



**Figure B3.4-1 Installation Menu**

4. Click [ProSafe-RS Software] in the installation menu.
5. If a dialog box appears, confirming to install Windows redistributable modules, click [Install].



**Figure B3.4-2 Dialog Box for Confirming Module Installation**

#### **TIP**

This dialog box appears when the Windows redistributable modules required to run ProSafe-RS are not already installed.

The following modules are necessary for ProSafe-RS:

- Microsoft .NET Framework 3.5 SP1
- MSXML 4.0 SP3
- Microsoft Data Access Object 3.5
- Microsoft Visual C++ 2008 redistributable package (x86)

If you click [Cancel], the installation of the ProSafe-RS software is discontinued.

Restarting the computer may be required after installing the modules. If required, restart the computer and then continue the ProSafe-RS installation.

For Windows Server 2008 R2, Microsoft .NET Framework 3.5 SP1 is included in the OS but displayed when it is disabled. If displayed, interrupt the installation and enable this module. The installation fails otherwise.

6. If the following dialog box appears, restart the computer and log on again using the same user account.

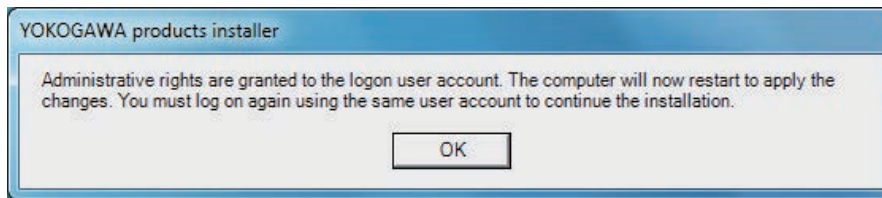


Figure B3.4-3 User Rights Setting Confirmation Dialog Box

**TIP** Restarting the computer here grants the currently logged on user the rights required to perform the subsequent installation tasks.

Installation of the ProSafe-RS software starts and the Welcome dialog box appears.

7. In the Welcome dialog box, click [Next].  
A dialog box for entering user information and the installation folder appears.

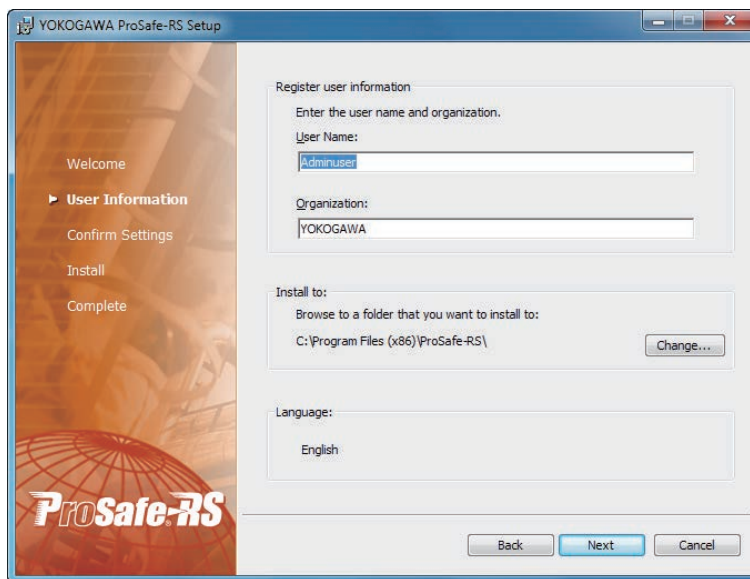


Figure B3.4-4 User Information Dialog Box

- TIP**
- If a different version of control bus driver or Vnet/IP open communication driver is already installed, a dialog box appears, prompting you to update the driver. Confirm the message and click [OK]. To update the control bus driver, uninstall the existing driver and then install the new one after you install the ProSafe-RS software. To update the Vnet/IP open communication driver, install the new driver after you install the ProSafe-RS software.
  - After updating the Vnet/IP open communication driver, disable the driver if the computer is to be connected to Ethernet.

8. Enter the user name and company name. It is recommended not to change the installation folder from the default location.

- TIP**
- If you want to change the installation folder, click [Browse] and specify a new location within 50 characters.
  - The language is determined automatically by the system language: if the system language is Japanese, the Japanese version software is installed, otherwise, the an English version is installed.

9. Click [Next].  
The installation setting confirmation dialog box appears.
10. Confirm that the installation settings are correct, and click [Install].



Installation of the ProSafe-RS software is started.

11. When the installation complete dialog box appears, perform either of the following operations.
  - If you install only ProSafe-RS, select [Yes, I want to set up IT security now.] and click [Finish]. The IT Security Tool then starts.
  - If you install another YOKOGAWA product, select [No, I want to install other software products.] and click [Finish] to complete the installation.

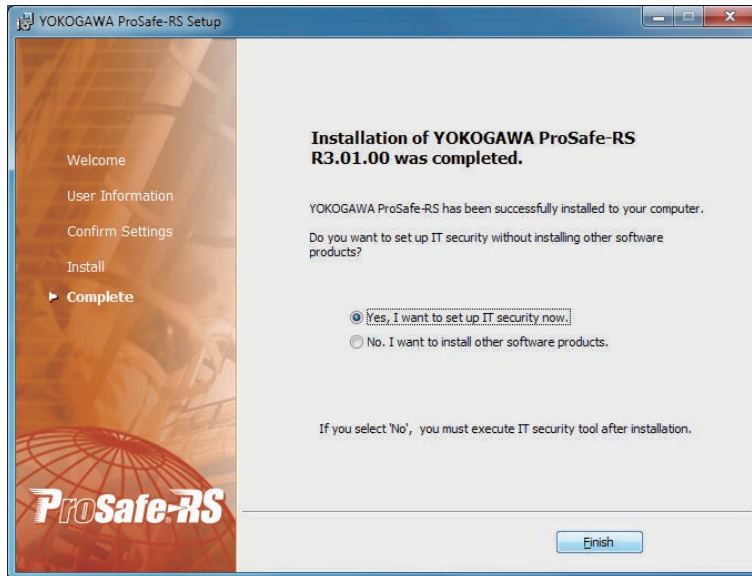


Figure B3.4-5 Installation Completed Dialog Box



## IMPORTANT

After you have installed other YOKOGAWA products, be sure to run the IT Security Tool to configure IT security settings. The IT security settings are configured for all the installed products at a time.

If you do not configure IT security settings, the products will not function properly.



## B3.5 Configuring IT Security Settings

After installing the ProSafe-RS software, you need to configure settings to strengthen Windows security.

Upon completion of the installation, exit the installer with [Yes, I want to set up IT security now.] selected. The IT Security Tool starts, allowing you to configure security settings.

This section describes how to configure security of the computer by using the IT Security Tool.



### IMPORTANT

- The security model and user management type of IT security settings must be consistent in the entire system. If you change the security model or user management type, make the changes on all computers including file server computers.
  - If you have changed any security settings from their default values, always save the security settings by using the Save function of the IT Security Tool to enable security settings to be restored at computer failure.
  - After you have activated the license of the SOE OPC Interface package (CHS2200), be sure to run the IT Security Tool from the start menu.
-

## B3.5.1 IT Security Tool

The IT Security Tool is the security configuration tool that was developed for Yokogawa system products. You need to use this tool to provide security measures on the computers installed with ProSafe-RS.

The IT Security Tool applies security settings on a computer automatically based on the selected security model and the user management type.

The functions of the IT Security Tool are shown in the following table.

**Table B3.5.1-1 Functions of the IT Security Tool**

Function	Description
Setup	Applies the Legacy model or Standard model of security settings.
Save	Saves the security settings of the OS. The security settings are encrypted with a specified password (encryption key).
Restore	Restores the security settings of the OS to the saved security settings.
Change Password (Encryption key)	Changes the password (encryption key) of the saved security settings. This function is used when you want to change the password periodically.

**SEE  
ALSO**

For more information about the functions of the IT Security Tool other than "Setup", refer to:

- C8.2, "Saving the IT Security Settings" on page C8-8
- C8.3, "Restoring the IT Security Settings" on page C8-13
- C8.4, "Changing the Security Setting File Password" on page C8-17

## ■ Security Model

You can select from the following security models according to the required security strength.

### ● Legacy Model

This model does not strengthen security. This model can be used if the priority is to be compatible with ProSafe-RS R3.01 or earlier versions, and to integrate with other YOKOGAWA products that do not support the IT Security Tool. Since this model disables Windows Firewall, you need to consider the possible impact of this model's vulnerability to information leaks, worms, and virus attacks when you select this model.

### ● Standard Model

This model enables access control by user authentication, DCOM setting, and Windows Firewall to guard against direct attacks and network attacks.

**TIP**

If you need a higher level of security than what the Standard model provide, the Strengthened model is available.

**SEE  
ALSO**

For more information about security models, refer to:

- 2., "Security Models" in ProSafe-RS Security Guide (IM 32Q01C70-31E)

## ■ User Management Types

The Standard model of security settings are applied in the following three types, according to the selected user management type. With the Legacy model, you can select only Standalone management as the user management type.

- **Domain Management**

Select this option when managing user and group accounts using the Windows domain controller. The groups must be created on the domain controller prior to configuring the security setting.

- **Standalone Management**

Select this option when managing user and group accounts for each computer without using the Windows domain controller. Although user accounts are created on each computer in this case, user groups and the user management method must match on all related computers.

- **Combination Management**

Combination management refers to a method of user management that combines the Domain management and the Standalone management. Combination management mainly manages the domain users; nevertheless, it is also designed under the assumption that the workgroups users are also managed for routine management. Unlike Domain management, however, this allows more operations to be performed with the administrative rights of a local computer, increasing security vulnerability.

## ■ Security Model and User Management within a Control Bus Domain

Within a V net domain or a Vnet/IP domain, the security model and user management type must be consistent. As the exception, however, Domain management and Combination management can be mixed. This mixed use of user management is also allowed for file server computers.

## ■ Standalone Management and Windows Domain

Even on Windows domain member computers, you can apply the "Standard model with Standalone management" type of security settings.

## ■ Security Setting Items

By running the IT Security Tool, various security setting items are configured. The tool configures a different set of security setting items, according to the selected combination of security model and user management type.

**SEE**

**ALSO** For more information about the setting items set by the IT Security Tool, refer to:

■ [Security Setting Items](#) in 6.1, "IT Security Tool" in ProSafe-RS Security Guide (IM 32Q01C70-31E)

## ■ Groups and Users Automatically Created during Security Configuration

By applying the Standard model of security settings, a specific set of users and groups are automatically created.

**SEE**

**ALSO** For more information about the users and groups that are automatically created by the tool, refer to:

2.2.3, "Users/Groups Respect to the Combination of User Management and Security Model" in ProSafe-RS Security Guide (IM 32Q01C70-31E)

## ■ User Groups and Accessible Functions

The ProSafe-RS functions that can be used by individual users are determined in user group units.

Access control is applied to the functions that are registered to the Start menu during installation of the ProSafe-RS software.

---

**SEE  
ALSO**

For more information about the functions that are accessible to each user group, refer to:

“■ Access Permissions to Programs” in 3.1.1, “Access Permissions to Files and Folders” in ProSafe-RS Security Guide (IM 32Q01C70-31E)

---

## B3.5.2 Running the IT Security Tool

This section describes the procedure for configuring the IT security settings following the completion of ProSafe-RS software installation.



### IMPORTANT

When using the IT Security Tool of ProSafe-RS R3.01 or later on a computer for the first time, any security model/user management type can be selected.

If the settings have already been configured using the IT Security Tool of the following versions of YOKOGAWA products on the computer, the security model and user management type that have been set will be selected automatically, and you cannot change them to a different security model or user management type here.

- CENTUM VP R5.01 or later
- PRM R3.10 or later
- ProSafe-RS R3.01 or later

To change the security model or user management type, first complete the IT security setting procedure with the existing settings, and then change the IT security settings by following the procedure for changing the security settings.

### ■ Running Procedure

1. When the ProSafe-RS software installation is complete, a dialog box appears. Select [Yes, I want to set up IT security now.] and click [Finish].

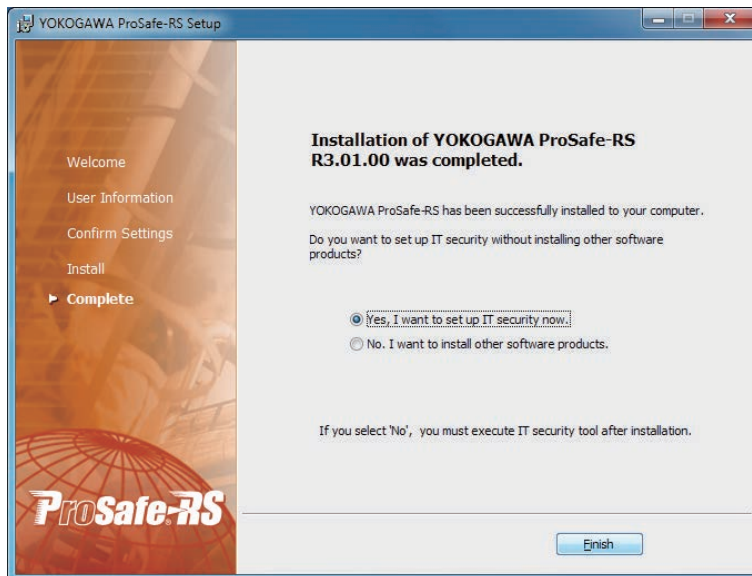
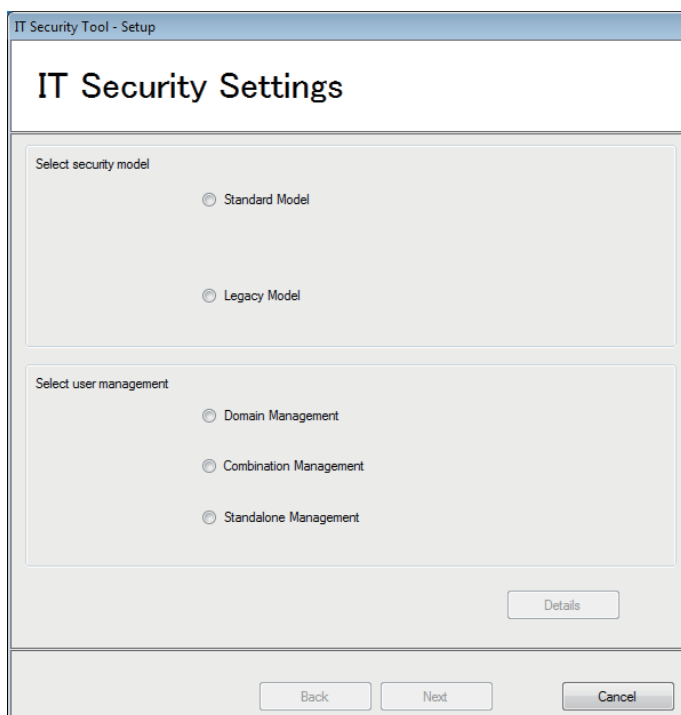


Figure B3.5.2-1 ProSafe-RS Setup Dialog Box (Completed)

The IT Security Tool starts.



**Figure B3.5.2-2 IT Security Tool — Setup**

2. On the Select security model pane, select either [Standard Model] or [Legacy Model].
3. On the Select user management pane, select [Domain Management], [Combination Management], or [Standalone Management].

**TIP**

- When you select the Legacy model, you cannot change the user management type from Standalone management.
- If you select [Standalone Management] on a Windows domain member computer, a warning message is displayed. You can go on by clicking [OK].

4. If you do not need to configure the individual setting items, click [Next] and proceed to step 7. If you want to change the setting of any individual items, click [Details]. The Select Setting Items page appears.

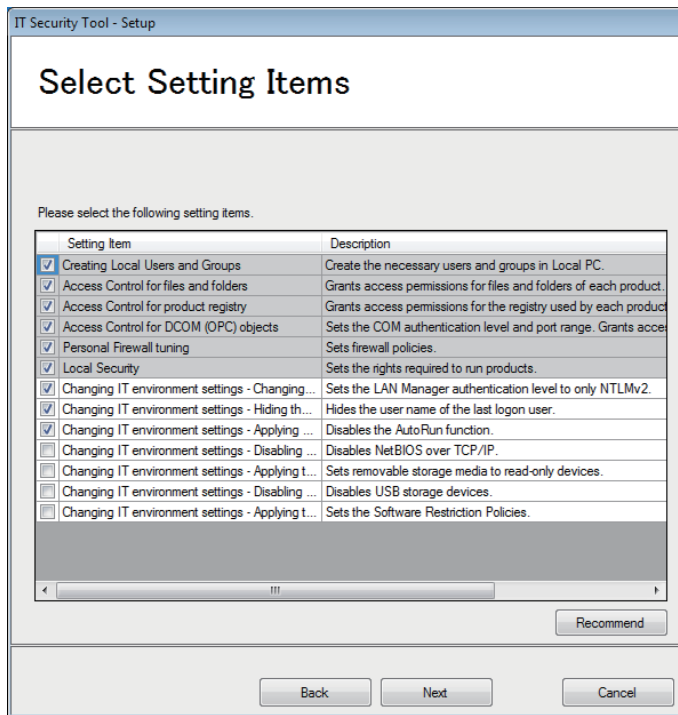


Figure B3.5.2-3 Select Setting Items Page

5. Select or clear the check boxes of the items you want to change.

**TIP**

It is recommended not to change settings when the Standard model is selected.

6. Click [Next].  
The Confirm Setting Information page appears.

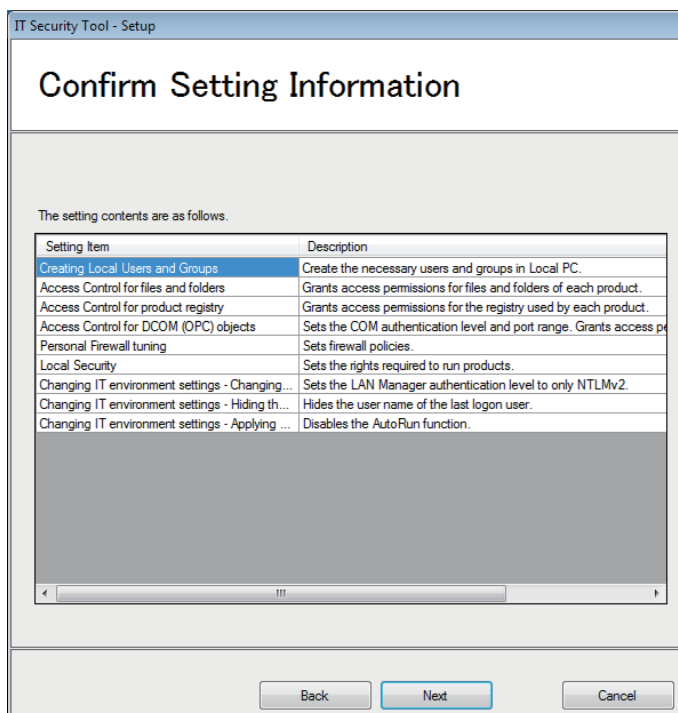


Figure B3.5.2-4 Confirm Setting Information Page

**TIP** If the settings specified are different from the default values of the security model, a warning dialog box appears.

To apply the current settings, click [Yes]. If you click [No], you will return to the Select Setting Items page.

7. Confirm the settings and click [Next].

**TIP**

- If this tool was used in the past to configure security settings without opening the Select Setting Items page, the last configured IT security settings are applied. If these settings and the default settings of the selected security model do not match, a warning dialog box appears.

To apply the current settings, click [Yes]. If you click [No], you will return to the IT Security Settings page.

When the setup is complete, the Setup Completed page appears. If there is any setting items that have failed, the failed items are displayed.

8. Select the [Restart now] check box and click [Finish].  
The IT Security Tool is exited and the computer is restarted automatically.



## IMPORTANT

If any failed setting items are displayed, contact YOKOGAWA Service.

**TIP** If you are using Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2, the Program Compatibility Assistant dialog box may appear after the security settings configuration is completed. Even this dialog box appears, the settings have been configured successfully, so click [Cancel] to close it.

**SEE ALSO** For more information about changing the IT security settings, refer to:

[C8.1, "Changing the IT Security Settings" on page C8-2](#)

### ● Notes on the Case when NetBIOS over TCP/IP is Disabled

When the Standard model is selected, you can configure to disable NetBIOS over TCP/IP. With Domain management or Combination management, NetBIOS over TCP/IP is disabled by default.

If it is disabled, you need to make the following settings for name solution.

- Standalone management  
In the LMHOSTS file of each station, set the computer names of the stations it needs to access.
- |                                     |   |
|-------------------------------------|---|
| Location of the LMHOSTS file:       | %Systemroot%\system32\drivers\etc   |
|                                     | %Systemroot% is the directory where the Windows OS is installed. Usually, it is C:\Windows. |
| Example script in the LMHOSTS file: | The following is an example of accessing HIS0124.   |
|                                     | ##### lmhosts   |
|                                     | 172.17.1.24 HIS0124 #PRE  |

**Table B3.5.2-1 LMHOSTS File Settings**

Station type	Stations to be set in the LMHOSTS file
License management station	All license-assigned stations

Continues on the next page



Table B3.5.2-1 LMHOSTS File Settings (Table continued)

Station type	Stations to be set in the LMHOSTS file
License-assigned station	<ul style="list-style-type: none"><li>• License management station</li><li>• Computer that holds project files (File server computer; if integrated with CENTUM, computer that holds CENTUM project database)</li></ul>

- Domain management/Combination management  
In the DNS server, set the license management station and all the license-assigned stations.

---

## B3.6 Distributing and Accepting Licenses

Licenses are the rights to use ProSafe-RS software packages.

To make the installed software packages available for use, you need to distribute the licenses from the license management station to license-assigned stations and accept the licenses on each license-assigned station. This process of making software packages available for use is called “activation of software packages.”

In a ProSafe-RS system, there is always one license management station and other stations are license-assigned stations. The license management station can be set up on a computer where SENG runs.

---

**SEE  
ALSO**

For more information about the procedure for distributing and activating licenses, refer to:

1., “Overview of license management” in License Management (IM 32Q01C60-31E)

---

## B3.7 Creating User Accounts

Create accounts for ProSafe-RS.

When the Standard model is selected in IT security configuration, rights to access the installation folder, registries, etc. are set by the IT Security Tool, based on the access rights granted to the ProSafe-RS user groups. Therefore, you need to register the created user as a member of the appropriate ProSafe-RS user group according to the user's role, such as engineer and maintenance personnel.

This section describes the procedures for the cases where the security settings of the Standard model with Standalone management or the Legacy model are applied.

In the case of Standard model with Domain management or Combination management, user accounts should be created in the process of setting up the domain environment.

---

**SEE  
ALSO**

For more information about creating user accounts in a Windows domain environment, refer to:

[B2.4, "Creating Domain Users" on page B2-9](#)

---

### ■ Limitation on User Account Names

- 20 characters at maximum.
- Space, tabs, and multi-byte characters such as half-width katakana and Chinese characters (kanji) cannot be used.

---

**TIP**

When the Access Control and Operation History Management Package is used and Windows authentication mode is specified, different limitations are applied.

---

---

**SEE  
ALSO**

For more information about the limitations on user account names when using Windows authentication mode of the Access Control and Operation History Management Package, refer to:

[■ Creating User Accounts in Windows Authentication Mode" on page B4-7](#)

---

## B3.7.1 When the Standard Model with Standalone Management Security Settings are Applied

When the security settings of Standard model with Standalone management are applied, user accounts should be created on each computer.

Follow these steps to create a user account:

1. Logon as an administrative user.
2. From the Start menu, choose [Control Panel] > [System and Security] > [Administrative Tools] and double-click [Computer Management].  
The Computer Management window appears.
3. On the tree view in the left pane of the window, select [System Tools] > [Local Users and Groups] > [Users].
4. Select [Action] > [New User].  
The New User dialog box appears.
5. Add a user account. (The rest of the steps shows an example of adding a new user account, OPERATOR.)

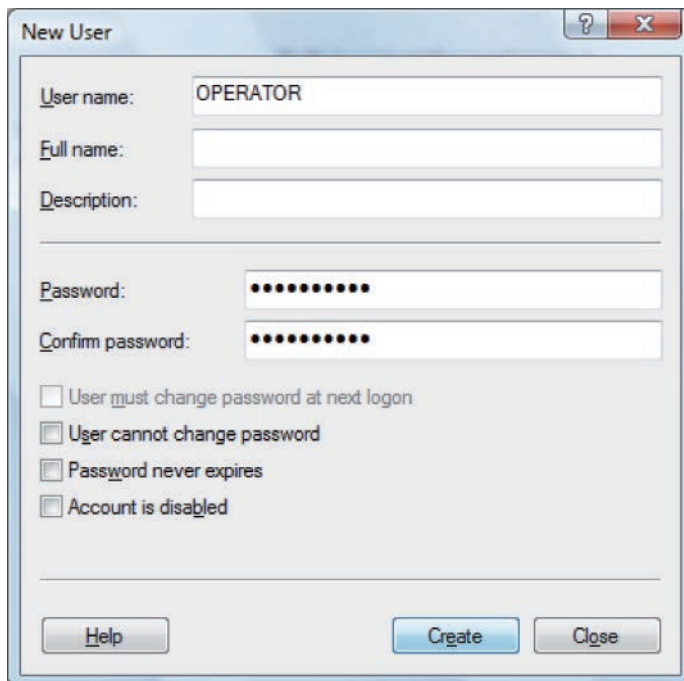
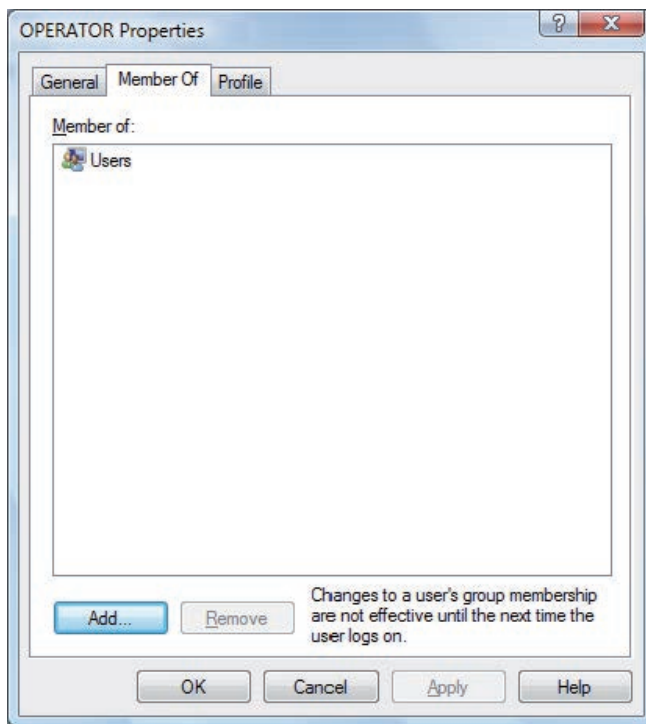
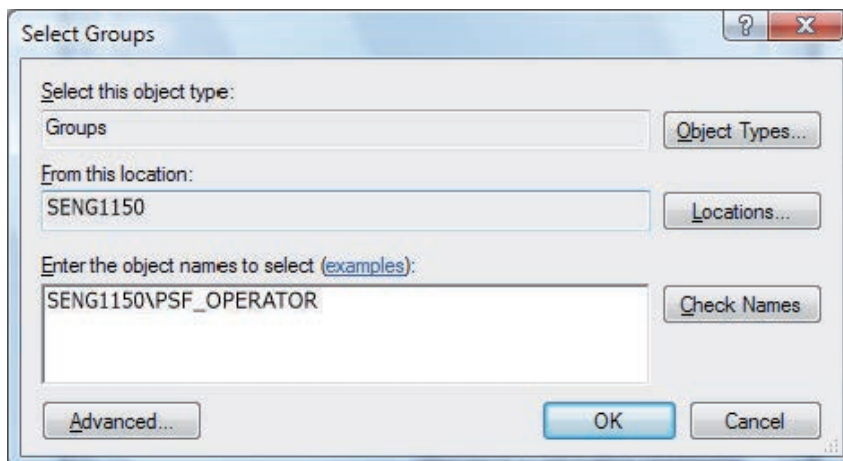


Figure B3.7.1-1 New User Dialog Box

6. Right-click the user you have created and select [Properties], and then click [Add] on the Member of tab.

**Figure B3.7.1-2 User Properties**

7. Select an appropriate user group for the created user and click [OK].

**Figure B3.7.1-3 Select Groups**

**TIP** A user who belongs to the administrative group (PSF\_MAINTENANCE) must also be a member of the Administrators group.

8. In the user properties dialog box, confirm that the group you selected has been added to the Member of list.

---

## B3.7.2 When the Legacy Model of Security Settings are Applied

The procedure for creating user accounts is the same as that for creating user accounts on a Standalone management computer. However, with the Legacy model, Windows groups PSF\_XXXX are not supported. So, there is no need to add the created users to these groups.

---

**SEE  
ALSO**

For more information about creating user accounts, refer to:

[B3.7.1, "When the Standard Model with Standalone Management Security Settings are Applied" on page B3-69](#)

---

---

## B3.8 Configuring Windows Environment Settings for Each User

After creating user accounts, configure the required Windows environment settings for each user.

## B3.8.1 Configuring on Windows 7

Follow these procedures when you use a Windows 7 computer.

### ■ Showing Icons on the Task Tray

On license-assigned stations running Windows 7, you must set so that the License Agent icon is always shown on the task tray.

1. Log on using the user account for which the License Agent icon should be displayed.
2. From the Start menu, select [Control Panel] > [Notification Area Icons].

#### TIP

If you cannot find Notification Area Icons, select [Large icons] or [Small icons] from the View by: drop-down list in the upper right of the Control Panel window.

The Notification Area Icons window appears.

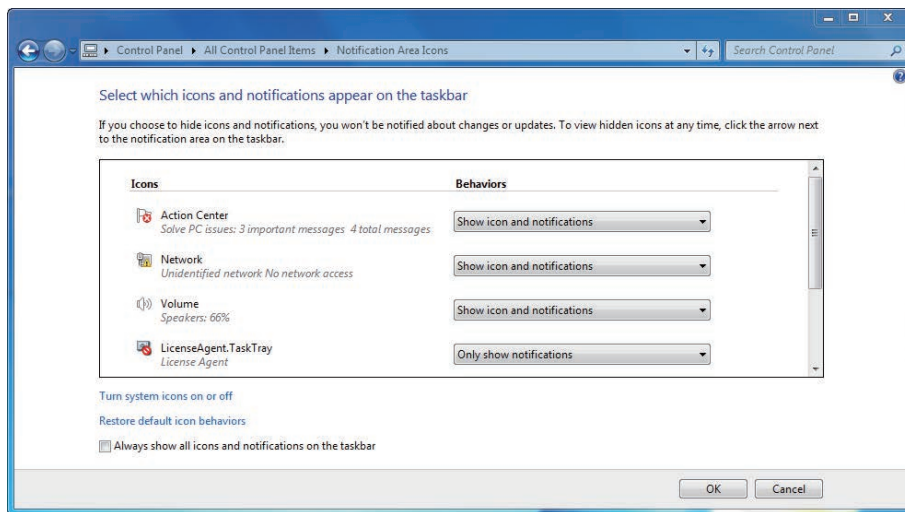


Figure B3.8.1-1 Notification Area Icons Window

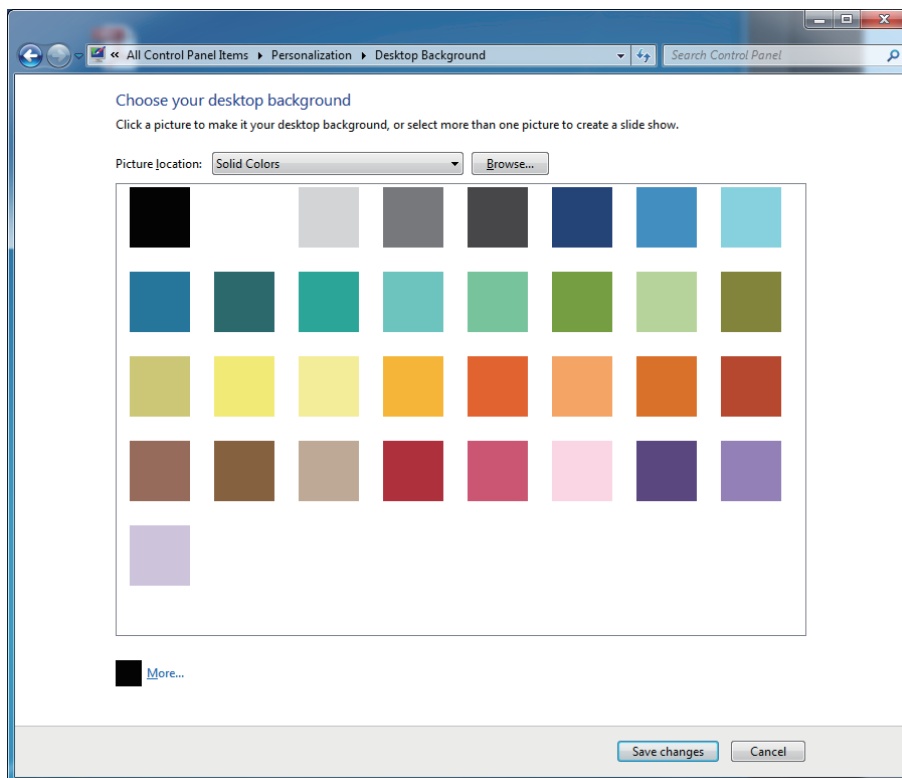
3. For License Agent.TaskTray, select [Show icon and notifications] and click [OK].

### ■ Display Properties

The procedure for setting the display properties is explained as follows.

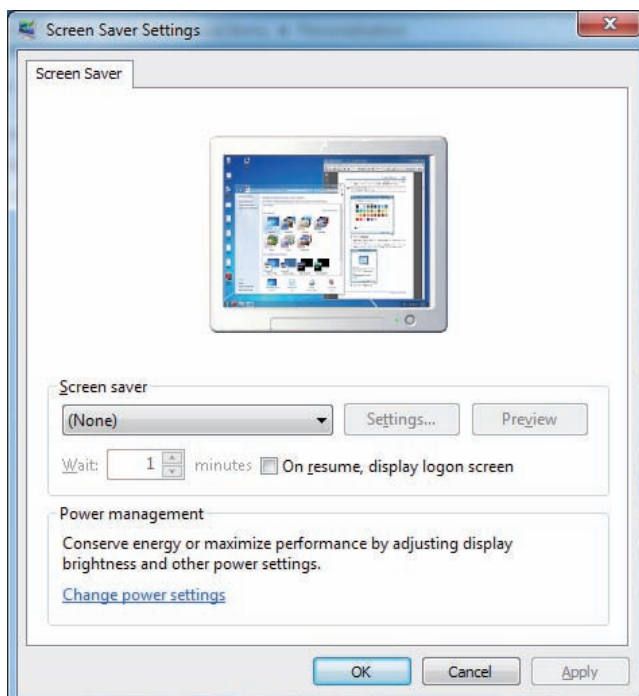
1. Log on using the user account for which to set display properties.
2. From the Start menu, select [Control Panel] > [Personalization] > [Desktop Background]. The Desktop Background window appears.





**Figure B3.8.1-2 Desktop Background Window**

3. Set [Solid Colors] for Picture Location, select the color of your choice, and then click [Save Changes].
4. Select [Screen Saver].  
The Screen Saver Settings dialog box appears.



**Figure B3.8.1-3 Screen Saver Settings Dialog Box**

5. Select [(None)] for Screen saver and then click [OK].

6. Select [Display] > [Adjust resolution] > [Advanced Settings].  
The Advanced Settings dialog box appears.

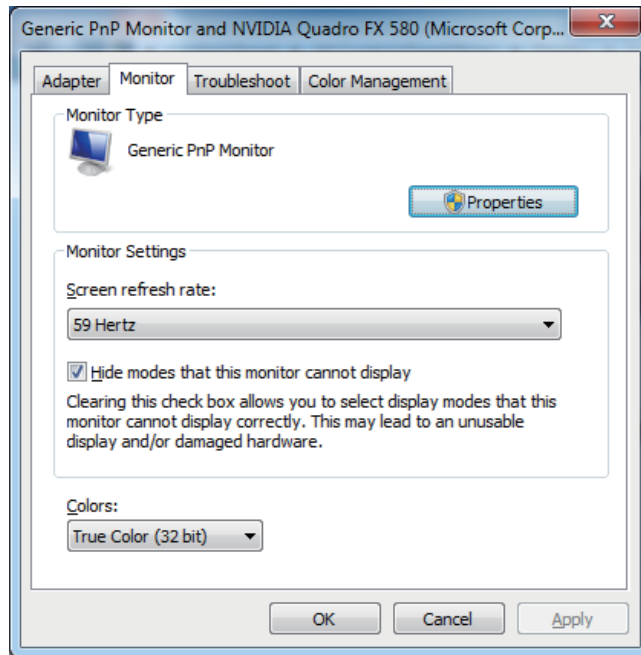


Figure B3.8.1-4 Advanced Settings Dialog Box

7. Select the [Monitor] tab, set [True Colors (32 bit)] for Colors and click [OK].

## B3.8.2 Configuring on Windows Vista

Follow these procedures when you use a Windows Vista computer.

### ■ Display Properties

The procedure for setting the display properties is explained as follows.

1. Log on using the user account for which to set display properties.
2. From the Start menu, select [Control Panel] > [Personalization] > [Desktop Background]. The Desktop Background window appears.

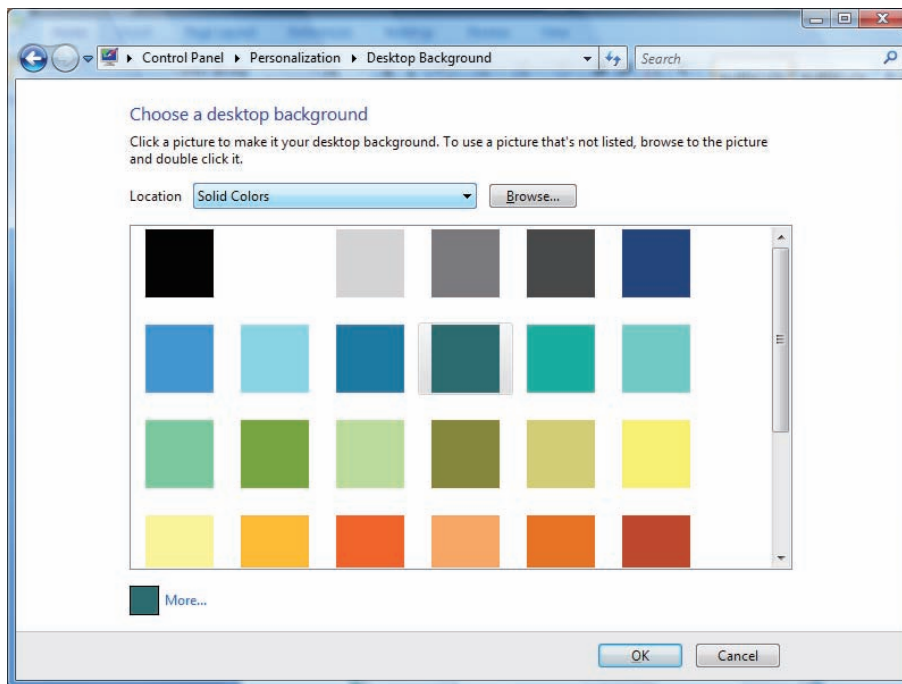


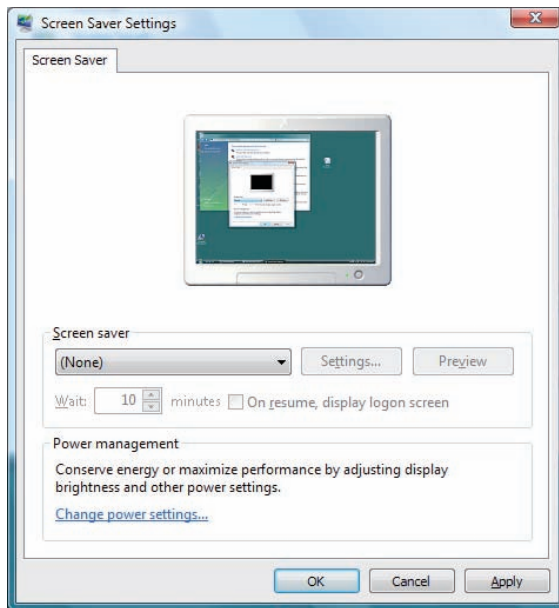
Figure B3.8.2-1 Desktop Background Window

3. Set [Solid Colors] for Location, select a color of your choice, and then click [OK].

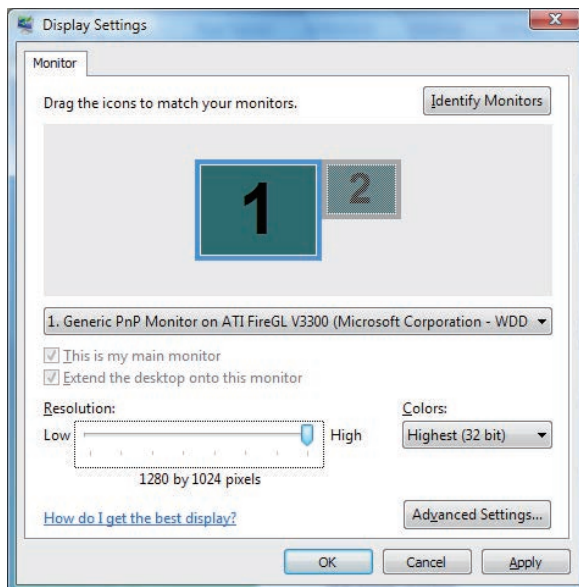
#### TIP

When the background color is defined as a solid color or another color after the first logon, the background color may revert to black at the second logon. If this problem occurs, you need to define the background color again with the same procedure.

4. Select [Screen Saver].  
The Screen Saver Settings dialog box appears.

**Figure B3.8.2-2 Screen Saver Settings**

5. Select [(None)] for Screen saver and then click [OK].
6. Select [Display Settings].  
The Display Settings dialog box appears.

**Figure B3.8.2-3 Display Settings**

7. Select [Highest (32 bit)] for Colors and then click [OK].

## B3.8.3 Configuring on Windows Server 2008 R2

Follow these procedures when you use a Windows 2008 R2 computer.

### ■ Showing Icons on the Task Tray

On license-assigned stations running Windows Server 2008 R2, you must set so that the License Agent icon is always shown on the task tray.

1. Log on using the user account for which the License Agent icon should be displayed.
2. From the Start menu, select [Control Panel] > [Notification Area Icons].

#### TIP

If you cannot find Notification Area Icons, select [Large icons] or [Small icons] from the View by: drop-down list in the upper right of the Control Panel window.

The Notification Area Icons window appears.

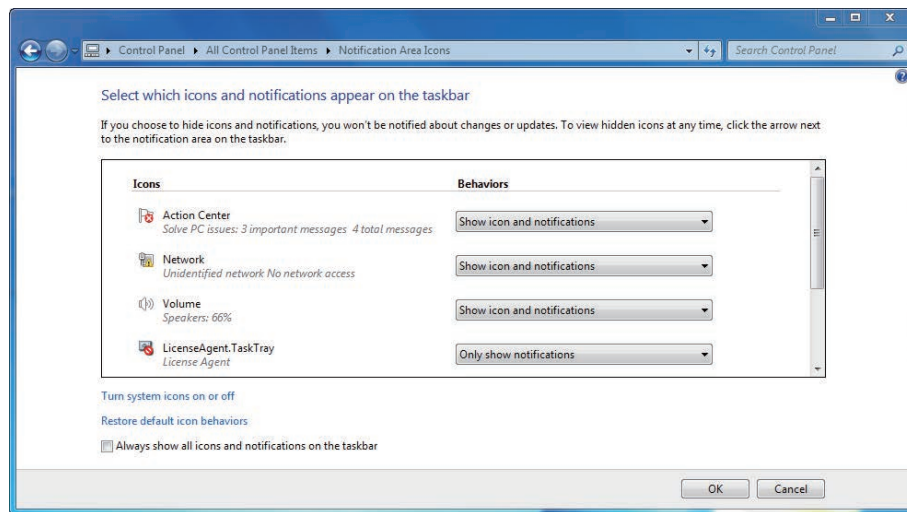


Figure B3.8.3-1 Notification Area Icons Window

3. For License Agent.TaskTray, select [Show icon and notifications] and click [OK].

### ■ Display Properties

The procedure for setting the display properties is explained as follows.

1. Log on using the user account for which to set display properties.
2. From the Start menu, select [Control Panel] > [Appearance and Personalization] > [Personalization] > [Desktop Background].  
The Desktop Background window appears.

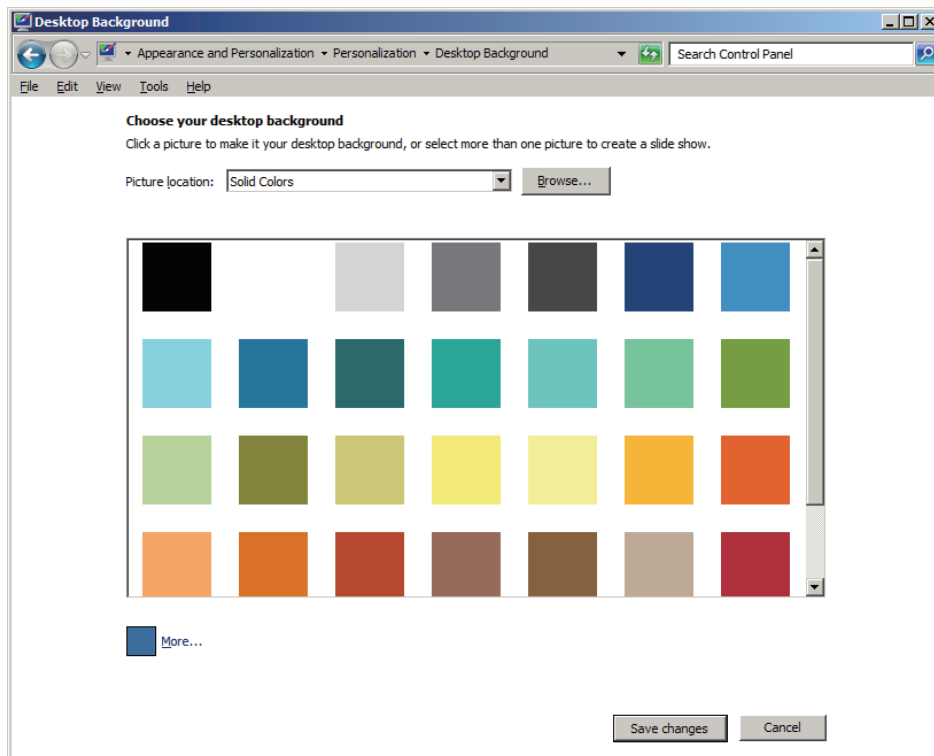


Figure B3.8.3-2 Desktop Background Window

3. Set [Solid Colors] for Picture Location, select the color of your choice, and then click [Save Changes].
4. Select [Screen Saver].  
The Screen Saver Settings dialog box appears.

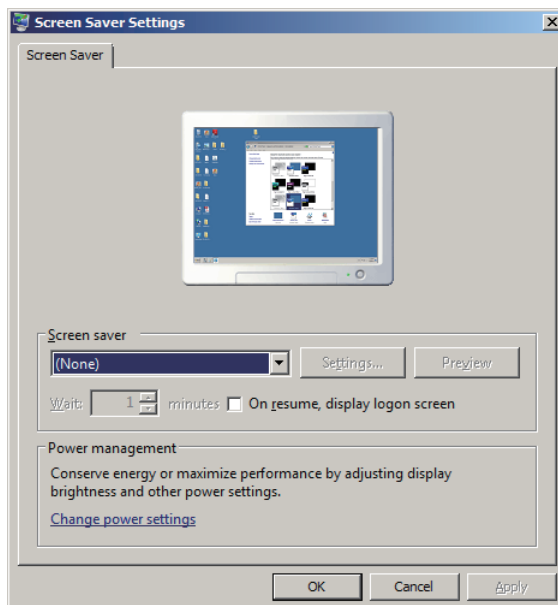
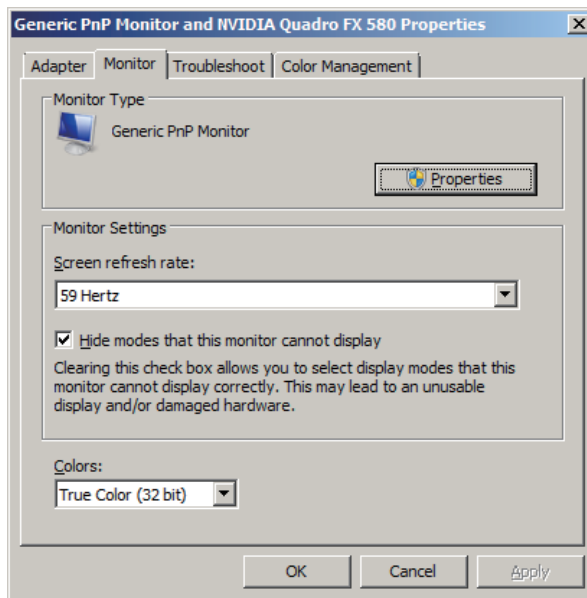


Figure B3.8.3-3 Screen Saver Settings Dialog Box

5. Select [(None)] for Screen saver and then click [OK].
6. Select [Display] > [Adjust resolution] > [Advanced Settings].  
The Advanced Settings dialog box appears.



**Figure B3.8.3-4 Advanced Settings Dialog Box**

7. Select the [Monitor] tab, set [True Colors (32 bit)] for Colors and click [OK].

## B3.8.4 Configuring on Windows Server 2008

Follow these procedures when you use a Windows 2008 computer.

### ■ Display Properties

The procedure for setting the display properties is explained as follows.

1. Log on using the user account for which to set display properties.
2. From the Start menu, select [Control Panel] > [Appearance and Personalization] > [Personalization] > [Desktop Background].  
The Desktop Background window appears.

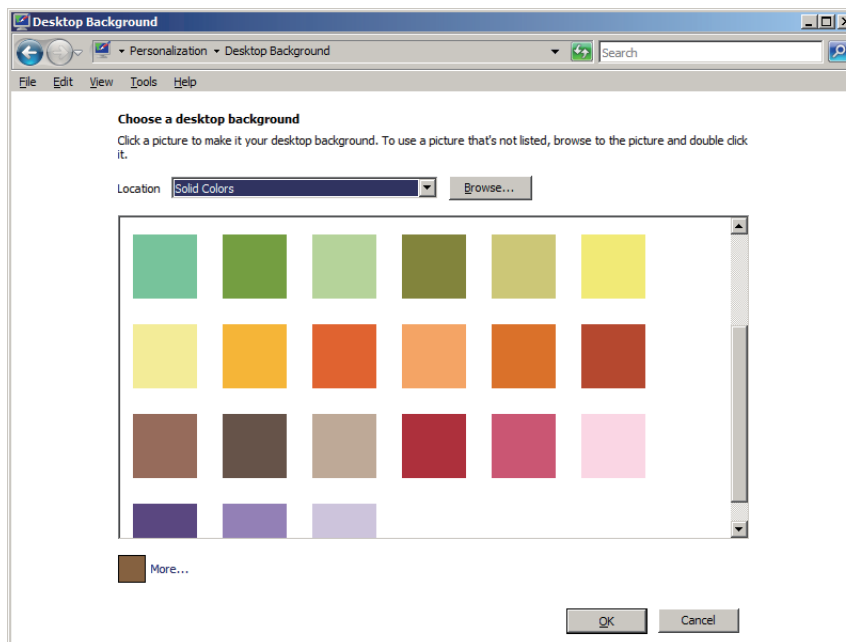


Figure B3.8.4-1 Desktop Background Window

3. Set [Solid Colors] for Location, select a color of your choice, and then click [OK].
4. Select [Screen Saver].  
The Screen Saver Settings dialog box appears.



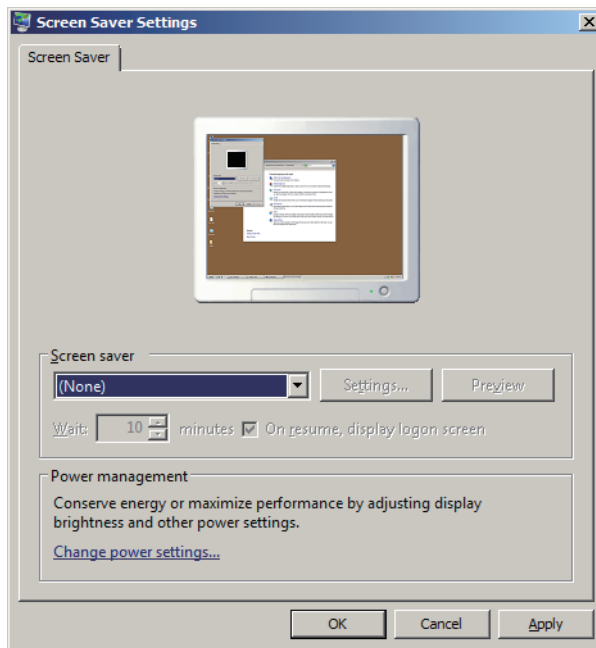


Figure B3.8.4-2 Screen Saver Settings Dialog Box

5. Select [(None)] for Screen saver and then click [OK].
6. Select [Display Settings].  
The Display Settings dialog box appears.

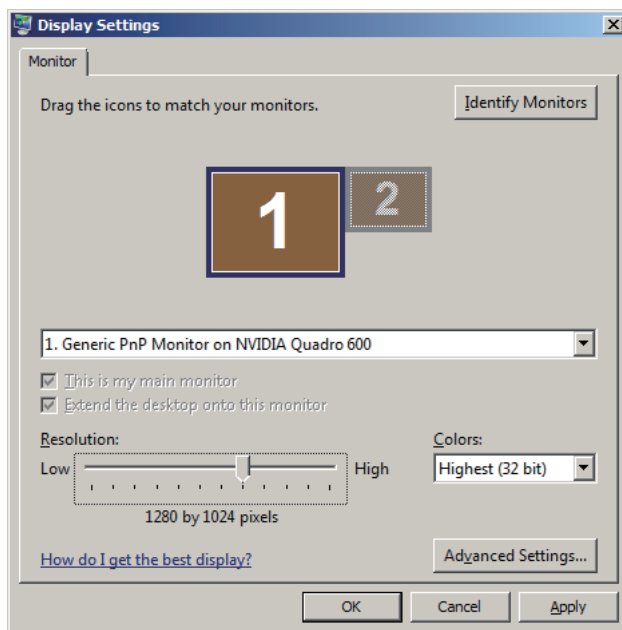


Figure B3.8.4-3 Display Settings

7. Select [Highest (32 bit)] for Colors and then click [OK].

## B3.9 Configuring the Uninterruptible Power Supply (UPS) Service

You can install uninterruptible power supply (hereinafter referred to as UPS) software and make various settings to protect data in the computer at power supply failures.

### ■ UPS Software Setting

Specify the UPS battery operation time so that the computer can continue operation with the UPS battery without shutting down even if a power supply error (for example, power interruption) occurs for a short period of time. Use several seconds as a guideline for setting the UPS battery operation time.

#### TIP

Although the UPS battery operation time can be set longer than several seconds, the computer should be shut down at a power interruption of several seconds for safety reasons.

#### SEE ALSO

For more information about the UPS software that can coexist with ProSafe-RS, refer to:

- [Software that can Coexist with ProSafe-RS](#) on page A3-4

---

## B4. Configuring Function-Specific Settings on SENG

This section describes the settings specific to functions that run on the SENG.

## B4.1 Online Manual Setting

Configure Adobe Reader to view the online manuals.

### ■ Setting of Adobe Reader

When using Adobe Reader 9.5/10.1/11.0, make sure that the [Open cross-document links in same window] check box is selected.

- The [Open cross-document links in same window] check box can be displayed by selecting [Preferences] - [Documents] from the [Edit] menu of Adobe Reader. It is necessary to do this setting for each logon user.

## B4.2 Settings of Project Database Folder

This section explains the procedure for strengthening the security of project databases.

### ■ Strengthening the Security of the Project Database on SENG PC

When ProSafe-RS software is installed, `C:\RS-Projects` folder is automatically created as the default location for saving project data. By running the IT Security Tool after the installation, share folder settings and security reinforcement are done for this default folder.

Shown below is the procedure for reinforcing security when you place the project database in a location other than the default folder on an SENG PC and have it shared with other computers.

1. Create a new folder for storing project data.
2. Log on as an administrative user belonging to the `PSF_MAINTENANCE` group and assign the share name `RS-Projects` to a folder to which the project database is to be stored.
3. Grant full control access permissions to Everyone.
4. Launch the IT Security Tool from the Start menu and configure security settings without changing the security model and user management type.

### ■ Strengthening the Security of Version Control Tool's Check-in Folder

If you place the Version Control Tool's check-in folder on an SENG PC, follow these steps to strengthen the security of the folder.

1. Create a new folder for use as the check-in folder of Version Control Tool.
2. Log on as an administrative user belonging to the `PSF_MAINTENANCE` group and assign the share name `RS-Share` to the check-in folder.
3. If the folder should be shared with other computers, grant full control access permissions to Everyone.
4. Launch the IT Security Tool from the Start menu and configure security settings without changing the security model and user management type.

---

## B4.3 Settings for Message Cache Tool

If you want to check the status of data collection by other stations using the Message Cache Tool, the following setups are required.

### ■ On Workgroup Member Computers

1. Create a user account on the station whose status of data collection shall be checked. The user account name and password should be the same as the user account of the computer that uses the Message Cache Tool.
2. Make the created user account created in step 1 belong to the PSF\_ENGINEER user group.

### ■ On Windows Domain Member Computers

Register users of the Message Cache Tool to the PSF\_ENGINEER user group.

## B4.4 Settings Required for OPC Communication

This section explains how to make settings required to perform OPC communication when the standard IT security setting model is selected on an SENG PC running the CHS2200 SOE OPC Interface Package. If the standard model of security settings is applied by the IT Security Tool after installation of ProSafe-RS, access to DCOM will be set. By this setting, only users belonging to ProSafe-RS user groups can access the SOE OPC interface.

### ■ Setting when Using Packages Performing OPC Communication with SENG PC

When you are using packages (OPC clients) that perform OPC communication with SENG PC (OPC servers), you must make the setting explained here.

#### ● In the Case of Standalone Management or When Combination Management is Applied on Some Computers

Perform the following procedure on an SENG PC performing OPC communication.

1. Create a program user of the OPC client package. Set the same user name and password as those on the client computer.
2. Make the created program user belong to the PSF\_OPC user group.

#### ● In the Case of Domain Management or When Combination Management is Applied on All Computers

- In the case of package that can join the domain
  1. Make a computer that runs the OPC client package join the domain.
  2. Register the package program user to the domain and make it belong to the PSF\_OPC user group.
- In the case of package that cannot join the domain  
Perform the following procedure on the SENG PC performing OPC communication.
  1. Create a program user of the OPC client package. Set the same user name and password as those on the computer running the package.
  2. Make the created program user belong to the PSF\_OPC\_LCL user group.

#### SEE ALSO

For more information about the settings for a computer where the SOE OPC Interface Package and CENTUM VP ExaOPC Interface Package coexist, refer to:

[D1.1.2, "CENTUM VP Standard Operation and Monitoring Function and ProSafe-RS SOE OPC Interface Package" on page D1-5](#)

For more information about the settings for using Exaquantum as an OPC client, refer to:

[D1.3.1, "ProSafe-RS SOE OPC Interface Package and Exaquantum PIMS Server" on page D1-17](#)

## B4.5 Setup when Using the Access Control and Operation History Management Package

In ProSafe-RS R3.01 and later, it is possible to manage operation histories on SENG by using the CHS5170 Access Control and Operation History Management Package. This section explains the operations required to use this package.

### SEE ALSO

For more information about the precautions to be followed when setting the access control/operation history management function, refer to:

- 2.13, “Access Control / Operation History Management Functions” in Engineering Guide (IM 32Q01C10-31E)
- 16., “Access Control/Operation History Management Function” in Engineering Reference (IM 32Q04B10-31E)

### ■ Windows User Groups to which Administrators and Engineers Belong

There are two types of personnel in a system where the access control and operation history management is applied: “administrators of access control and operation history management” (hereinafter referred to as “administrator” in this section) and “engineers.”

After creating user accounts for administrators and engineers, add them to the Windows user groups shown in the following table.

**Table B4.5-1 Windows User Groups to which Administrators and Engineers Must Belong**

Personnel	Windows user group to belong to	
	Standard or Strengthened model	Legacy model
Administrator	Either of the following: PSF_MAINTENANCE (*1) PSF_MAINTENANCE_LCL (*1)	Group with administrator privilege
Engineer	One of the following: PSF_OPERATOR PSF_ENGINEER PSF_OPERATOR_LCL PSF_ENGINEER_LCL	Any group

\*1: Users belonging to these groups must also have the Windows administrator privileges. Make them also belong to the Administrators or Domain Admins group.

### ■ Security Model and User Authentication Mode

If you select the Standard model with the IT Security Tool, you can select either ProSafe authentication mode or Windows authentication mode as the user authentication mode of the operation history management function on SENG. By default, ProSafe authentication mode is selected.

If you select the Legacy model with the IT Security Tool, only ProSafe authentication mode is available.

You can configure user authentication modes by using the operation history management setting tool included in the Access Control and Operation History Management Package.

### SEE ALSO

For more information about security models, refer to:

- 2., “Security Models” in ProSafe-RS Security Guide (IM 32Q01C70-31E)



## ■ Creating User Accounts in Windows Authentication Mode

In Windows authentication mode, Windows user names are used to log on to the SENG functions and authenticate users.



### IMPORTANT

When you use Windows authentication mode, create Windows users following the naming convention below, rather than the Windows naming convention. This naming convention is the same as the naming convention for engineers.

The naming convention for users in Windows authentication mode is as follows:

**Table B4.5-2 User Naming Convention in Windows Authentication Mode**

Number of characters	Up to 16 characters
Character type	Alphanumeric characters and the following symbols can be used: ! # \$ % ( ) - . ^ _ { } ~ Double-byte characters cannot be used.
Restriction	Upper-case characters only (*1) For the head character, alphanumeric characters and the following symbols can be used: ^ _ { } ~ Names ending with a period cannot be used.

\*1: Only upper-case characters can be used for engineer names to be registered in the Engineers' Account Builder. Although both upper-case and lower-case characters can be used on the Windows side, they are not distinguished; use upper-case characters only.

You can set passwords within 63 characters using alphanumeric characters and symbols.

- Passwords are case-sensitive.
- The following symbols and space character are allowed:  
! " # \$ % & ' ( ) \* + , - . / : ; < = > ? @ [ \ ] ^ \_ { | } ~

### SEE ALSO

For more information about how to create Windows user accounts, refer to:

[B3.7, "Creating User Accounts" on page B3-68](#)

## B4.5.1 Setup Procedure when Using Access Control and Operation History Management Functions

This section explains the setup procedure you should perform after installing the Pro-Safe-RS software when using the access control and operation history management functions. If you want to introduce the access control and operation history management functions later, use the procedure at a proper timing.

Perform the following tasks after creating administrator and engineer user accounts on Windows.

1. Add the Windows accounts for administrators and engineers to their respective appropriate user groups.
2. Configure security settings for the operation history database.
3. On a computer granted with the licenses of CHS5100 Safety System Generation and Maintenance Function Package and CHS5170 Access Control and Operation History Management Package, use the Operation History Management Setup Tool and Engineers' Account Builder to perform required setting.

---

**SEE  
ALSO**

For more information about how to create Windows user accounts, refer to:

[B3.7, "Creating User Accounts" on page B3-68](#)

For more information about the explanation of the procedure involved in making security settings for operation history management databases, refer to:

[B4.5.2, "Security Settings for the Operation History Database" on page B4-9](#)

For more information about the precautions to be followed when setting the access control/operation history management function, refer to:

[16.2, "Setting Up Access Control/Operation History Management" in Engineering Reference \(IM 32Q04B10-31E\)](#)

---

## B4.5.2 Security Settings for the Operation History Database

The administrator must specify the folder for storing the operation history database by using the operation history management setting tool. Set the security of the folder for storing the operation history database at proper timing before starting to use the operation history management function.

This section explains the procedures to configure security settings when the operation history database is placed on an SENG PC and when it is placed on a file server. After performing these procedures, the administrator and engineers can access the operation history database folder.

### ■ Setting when Operation History Databases are Placed on SENG PC

If you place an operation history database on an SENG PC, perform the following procedure to reinforce the security of the folder for storing the operation history database.

1. Create a new folder for storing the operation history database.
2. Log on to the system as an administrative user who belongs to the PSF\_MAINTENANCE group and assign the sharing name "RS-Share" to the folder for storing the operation history database.
3. If the folder needs to be shared with other computers, grant a full control permission to Everyone.
4. Launch the IT Security Tool from the Start menu and execute it again without changing the setting made the last time it was executed.

### ■ Setting when Operation History Databases are Placed on a File Server

If you place an operation history database on a computer not installed with the ProSafe-RS software and allow SENG to access the database via a network, perform the procedure to reinforce security of the file server.

#### SEE ALSO

For more information about the procedure for reinforcing the security of the file server, refer to:

[B5., "Setting Up a File Server" on page B5-1](#)

## B5. Setting Up a File Server

Provide a file server in the system, and you can access the files placed on this server computer from other computers. On a file server, you may place a project database, the check-in destination folder for Version Control Tool, and/or the operation history database of the Access Control and Operation History Management Package, allowing access to these databases via the network.

This section describes how to set up a file server computer for the following cases:

- Computer that serves only as a file server
- Computer that serves as both a file server and an SENG
- Computer that serves as both a file server and a license management station

### ■ Item to be Prepared

Have the following item at hand before you set up a file server.

- ProSafe-RS software medium (Model: CHSKM30)

### ■ File System

Ensure that the file system is in the NTFS format.

## B5.1 Setting Up a Computer that Serves Only as a File Server

This section describes how to set up a computer that is used only as a file server.

### ■ Administrative User who Performs the Setup

A file server must be set up by an administrative user who belongs to the groups shown in the following table.

**Table B5.1-1 Groups to Which the Administrative User Who Sets Up a File Server Belongs**

Security model and user management type to be applied		
Legacy model	Standard model	
	Standalone management	Domain/Combination management
Administrators of the local computer	Administrators and PSF_MAINTENANCE of the local computer	Domain Admins and PSF_MAINTENANCE of the domain (*1)

\*1: Log on to the computer when the computer is connected to the domain.

### ■ Procedure 1: Prepare to Configure IT Security Settings on a File Server

Perform one of the following procedures according to the security model to be applied.

#### ● Legacy Model

1. Log on as a member of the Administrators group.
2. Perform one of the following operations:
  - On Windows Server 2008 R2, enable .NET Framework 3.5.1.
  - On Windows Server 2008, enable .NET Framework 3.0.
3. Restart the computer.
4. Log on using the same user account as in step 1.

#### SEE ALSO

For more information about how to enable .NET Framework 3.5.1 and 3.0, refer to:

■ [Enabling .NET Framework 3.5.1](#) on page B3-25

#### ● Standard Model with Standalone Management

1. Log on as a member of the Administrators group.
2. Create the PSF\_MAINTENANCE group.
3. Add the user to be set as the administrator to the Administrators and PSF\_MAINTENANCE groups.

#### TIP

If any other YOKOGAWA product coexists in the computer, the user also needs to be a member of the MAINTENANCE group of the coexisting product. For example, if CENTUM VP coexists, also add the user to the CTM\_MAINTENANCE group.

4. Perform one of the following operations:
  - On Windows Server 2008 R2, enable .NET Framework 3.5.1.
  - On Windows Server 2008, enable .NET Framework 3.0.
5. Restart the computer.

6. Log on as the user set in step 3 above.

**SEE  
ALSO**

For more information about how to enable .NET Framework 3.5.1 and 3.0, refer to:

“■ Enabling .NET Framework 3.5.1” on page B3-25

### ● Standard Model with Domain/Combination Management

1. Log on as a user who belongs to both the Domain Admins and PSF\_MAINTENANCE groups of the domain.
2. Perform one of the following operations:
  - On Windows Server 2008 R2, enable .NET Framework 3.5.1.
  - On Windows Server 2008, enable .NET Framework 3.0.
3. Restart the computer.
4. Log on using the same user account as in step 1.

**TIP**

If any other YOKOGAWA product coexists in the computer, the user also needs to be a member of the MAINTENANCE group of the coexisting product. For example, if CENTUM VP coexists, also add the user to the CTM\_MAINTENANCE group.

**SEE  
ALSO**

For more information about how to enable .NET Framework 3.5.1 and 3.0, refer to:

“■ Enabling .NET Framework 3.5.1” on page B3-25

## ■ Procedure 2: Create and Set Up the Shared Folders

In order to reinforce the security of folders that store databases using the IT Security Tool, you must name the target folders with the following share names.

- Project database  
Share name: RS-Projects
- Operation history database and check-in destination folder of Version Control Tool  
Share name: RS-Share



### IMPORTANT

If the shared name does not match the name above, the IT Security Tool is not able to reinforce the folder security. Be sure to set the share name above using the following procedure so that you can reinforce security.

### ● Creating a New Folder

1. Start Windows Explorer and create a folder in which the project folders are to be placed.
2. On the Sharing tab in the properties of the folder that is created, click [Advanced Sharing].
3. Select [Share this folder] and set RS-Projects or RS-Share as the share name.
4. Click [Permissions] and grant full control to [Everyone] in the Share Permissions section. This access permission setting will be changed when you run the IT Security Tool.

- **When a Shared Folder is Already Created on the File Server**

Before configuring IT security settings, add a share name, “RS-Projects” or “RS-Share,” to the folder. The folder will be included in the process of IT security setting configuration and access permissions setting will be applied. Share names that were previously set up do not need to be deleted.



### **IMPORTANT**

If a folder with the share name “RS-Projects” or “RS-Share” has already been created for another purpose on an existing file server, change the existing share name to another name. Since the access permissions are granted to folders with the share name “RS-Projects” or “RS-Share” during configuration of IT security settings, unintended settings will be applied if these share names are not assigned to appropriate folders.

If IT security settings have been applied to an unintended folder, delete the permissions set during the configuration of IT security settings and set the original access permissions based on the setting of another folder, such as the C:\Windows folder.

## ■ **Procedure 3: Save the IT Security Settings on the File Server**



### **IMPORTANT**

The existing security settings before using the IT Security Tool will be required as the initial data when you change the security settings in the future. So, you must save the existing security settings here.

If the file server computer is to be added to a domain, save two sets of initial security settings before and after you add it to the domain.

If the file server computer is not to be added to a domain, you need to save only one set of initial security settings.

Follow these steps to save the security settings:

1. Log on as a user who has the rights to set up a file server.
2. Insert the ProSafe-RS software medium into the drive.
  - If the AutoPlay dialog box appears, click [Run Launcher.exe].
  - If the AutoPlay dialog box does not appear, use Explorer and double-click Launcher.exe in the top folder of the software medium.

The installation menu appears.

3. Click [Setting IT Security (File server/domain controller use)].  
The IT Security Tool starts.

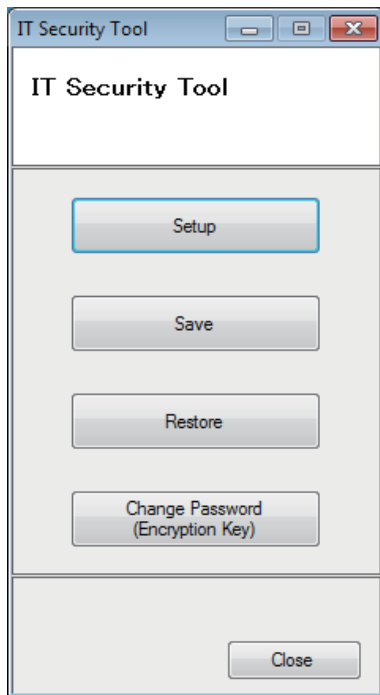


Figure B5.1-1 IT Security Tool Menu

4. Save the security settings.

**TIP**

If the file server is a member of a domain, when restoring the initial security settings on the file server, the initial data should have two types, either the initial data for a standalone computer or the initial data for a member of domain.

If you do not have the initial data for a standalone file server computer, you need to remove the file server from the domain temporarily and then save the security settings as the initial data for the standalone computer.

**SEE  
ALSO**

For more information about the subsequent operations of the IT Security Tool, refer to:

[C8.2.1, "Procedure for SENG PC" on page C8-9](#)

## ■ Procedure 4: Configure the IT Security Settings on the File Server

1. From the IT Security Tool Menu, click [Setup].  
A confirmation dialog box appears
2. If you have saved the above mentioned initial security setting data, click [OK].

**TIP**

If you have not saved the initial security setting data, click [Cancel] to return to the tool's menu and save the security settings.

The Select Security Model page appears.



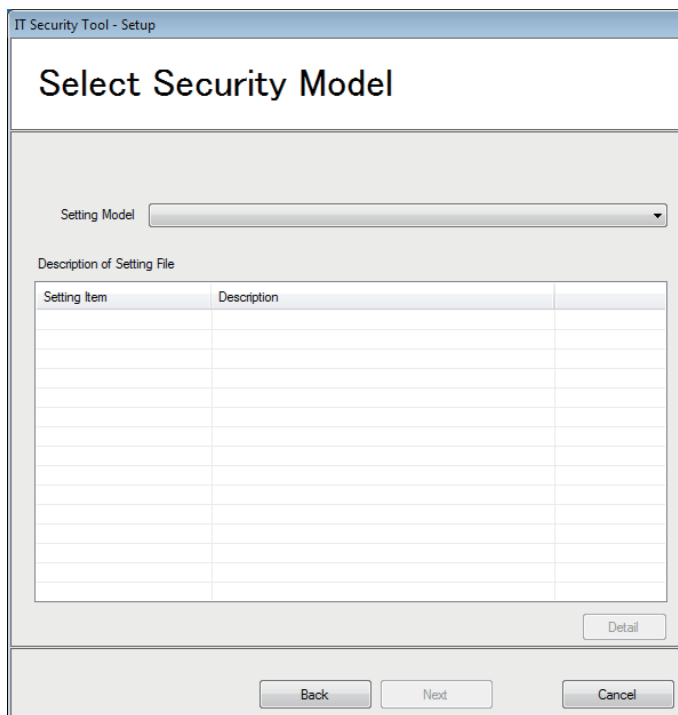


Figure B5.1-2 Select Security Model

3. From the Setting Model drop-down list, select a security model for the file server. You can select from the following four models.

Table B5.1-2 Security Models for a File Server

Model	Description
File Server Legacy Model	Select this model to apply Legacy model to the file server, regardless of the user management type.
File Server Standard Model with Standalone Management	Select this model to apply Standard model to the file server when the user management type is Stand-alone management.
File Server Standard Model with Domain Management	Select this model to apply Standard model to the file server when the user management type is Domain management.
File Server Standard Model with Combination Management	Select this model to apply Standard model to the file server when the user management type is Combination management.

4. Click [Next].  
The Confirm Setting Information page appears.

**TIP** If you click [Detail] here, the Select Setting Items page appears.

5. The subsequent steps are the same as those for the IT security setting configuration after installing the ProSafe-RS software.

**SEE ALSO** For more information about the IT security setting operations that are performed following the ProSafe-RS software installation, refer to:

B3.5.2, "Running the IT Security Tool" on page B3-62

## ■ Procedure 5: Create Accounts on the File Server for Users who Access Project Data

On the file server computer, create accounts for users who access the project data, according to the selected security model and user management type.

### ● Standard Model with Domain/Combination Management

On the domain controller, add the accounts for accessing projects. No account needs to be created if already created.

### ● Legacy/Standard Model with Standalone Management

Perform the following procedure on the file server.

1. Create a user account.  
The user name and the password must be the same as those of the SENG PCs from which the projects are accessed.
2. Register the user you have created to the same group as that on the SENG PCs which access the file server.

#### TIP

If the Standard model is applied, the following user groups have been created during the procedures so far.

- PSF\_MAINTENANCE
- PSF\_OPERATOR
- PSF\_ENGINEER
- PSF\_OPC

## ■ Procedure 6: Create the Project Folder on the File Server and Start the Operation

- Project database  
From an SENG PC, create an RS project under the shared folder “RS-Projects” created in Procedure 2.
- Check-in folder of Version Control Tool  
On an SENG PC, use the Version Control Tool to specify a folder under the shared folder “RS-Share” created in Procedure 2 as the check-in destination folder, and start project operation.
- Operation history database  
On an SENG PC, use the operation history management setting tool to specify a folder under the shared folder “RS-Share” created in Procedure 2 as the top folder of the operation history database, and start the access control and operation history management function.

## B5.2 Setting Up the File Server Function on SENG

This section describes the required settings when you use a computer that has been set up as an SENG also to be used as a file server.

**TIP**

On an SENG, the project database is created under the installation folder by default. The procedure described in this section is for the case when the project database is placed in a location other than the installation folder.

1. Set up a computer as an SENG.

**TIP**

You do not need to configure security settings during this setup.

2. On the computer, create and set up the shared folder.
3. Start the IT Security Tool from the Start menu and configure IT security settings.
4. Create a project folder in a location under the shared folder of the computer.



### IMPORTANT

On a computer used as both a file server and an SENG, do not use the [Setting IT Security (File server/domain controller use)] button on the installation menu to start the IT Security Tool.

**SEE ALSO**

For more information about how to create the project folder on the file server, refer to:

“■ Procedure 6: Create the Project Folder on the File Server and Start the Operation” on page B5-7

For more information about new setup of SENG, refer to:

B3., “Setting Up the SENG” on page B3-1

For more information about the shared folder settings, refer to:

“■ Procedure 2: Create and Set Up the Shared Folders” on page B5-3

For more information about creating accounts for users who access the project database, refer to:

“■ Procedure 5: Create Accounts on the File Server for Users who Access Project Data” on page B5-7

## B5.3 Setting Up the Computer that Serves as Both File Server and License Management Station

This section describes the setup required for the computer that serves as both a file server and a license management station.

### ■ Setup Procedure

1. Install the license management software.
2. On the dialog box that appears on completion of the installation, select [No, I want to install other software products.] and click [Finish].
3. Configure the shared folder settings required for a file server.
4. Start the IT Security Tool from the Start menu and configure IT security settings.



### IMPORTANT

On a computer used as both a file server and a license management station, do not use the [Setting IT Security (File server/domain controller use)] button on the installation menu to start the IT Security Tool.

### SEE ALSO

For more information about installing only the license management software, refer to:

[B6., "Setting Up the Computer Dedicated to License Management" on page B6-1](#)

For more information about the shared folder settings, refer to:

[■ Procedure 2: Create and Set Up the Shared Folders" on page B5-3](#)

# B6. Setting Up the Computer Dedicated to License Management

You can use a computer as the license management station by installing only the license management software on it.

This section describes the procedure for setting up the computer dedicated to license management.

## ■ Items to be Prepared

Have the following item at hand before installing the license management software.

- ProSafe-RS software medium (Model: CHSKM30)

## ■ Installation Procedure

Follow these steps to install the license management software.

1. Log on as an administrative user.
2. Insert the ProSafe-RS software medium into the drive.
  - If the AutoPlay dialog box appears, click [Run Launcher.exe].
  - If the AutoPlay dialog box does not appear, use Explorer and double-click Launcher.exe in the top folder of the ProSafe-RS software medium.

The installation menu appears.

3. Click [Install License Manager Software].  
The Welcome dialog box appears.

### TIP

- If modules required to run ProSafe-RS, such as Microsoft .NET Framework, are not already installed, a dialog box appears, prompting you to install such modules. Click [Install] .

Restarting the computer may be required after installing the modules. If required, restart the computer and then continue the ProSafe-RS installation.

For Windows Server 2008 R2, Microsoft .NET Framework 3.5 SP1 is included in the OS but displayed when it is disabled. If displayed, interrupt the installation and enable this module. The installation fails otherwise.

- A message that prompts restarting the computer may be displayed so as to grant the currently logged on user the rights required to perform the subsequent installation tasks. If prompted, restart the computer and log on using the same user account to continue the installation of the license management software.

4. Click [Next].  
The User Information dialog box appears.

### TIP

If a different version of control bus driver is already installed, a dialog box appears, prompting you to update the driver. However, you do not need to install the control bus driver on a computer dedicated to license management. Click [OK] to close the dialog box.

5. In the User Information dialog box, enter the name and company name, select the installation folder, and confirm the language for installation, and click [Next].  
The Confirm Settings dialog box appears.
6. Review the installation settings and click [Install].  
A dialog box showing the installation progress appears, and when the license management software installation is complete, the Installation Complete dialog box appears.
7. Select [Yes, I want to set up IT security now.] and click [Finish].

The IT Security Tool starts.

8. Go on to configure the security settings.

**TIP**

When deleting the ProSafe-RS function and installing only the license management software after installing ProSafe-RS, first log on using an administrative user account and uninstall ProSafe-RS, and then install the license management software.

**IMPORTANT**

If you want to manage other product's licenses on the computer dedicated to license management, you also need to install the license management software from the software medium of that product.

**SEE  
ALSO**

For more information about how to uninstall the ProSafe-RS software, refer to:

[C6.1.1, "Uninstalling the ProSafe-RS Software" on page C6-3](#)

For more information about configuring the IT security settings, refer to:

[B3.5.2, "Running the IT Security Tool" on page B3-62](#)

# B7. Configuring the Hardware of SCS and Devices for Connection between Domains

Configure the hardware of SCS and devices used for connection between domains, such as V net routers and L3 switches.

- On the processor module of SCS, set the V net or Vnet/IP address.
- If a V net router (AVR10D) is used to connect a Vnet/IP domain and a V net domain, the V net router address should be set on the CENTUM side.



## WARNING

When removing and installing the cards to set DIP switches, take measure to prevent the damages caused by static electricity.

## SEE ALSO

For more information about Antistatic measures, refer to:

[Appendix 3., "Antistatic Precautions When Handling Hardware" on page App.3-1](#)

For more information about setting up the hardware when using V net routers, bus converters, and communication gateway, refer to:

- CENTUM VP Communication Devices (IM 33K50D10-50E)
- CENTUM VP Communication Devices (IM 33M50D10-40E)
- CS 1000/CS 3000 Communication Devices (IM 33Y06H01-01E)

## B8. Installing the Functions that Operate with CENTUM VP Licenses

The test function and SOE Viewer of ProSafe-RS operate in coordination with CENTUM VP packages. You can set up a computer so as to use only these functions without using other SENG functions. First, grant the computer licenses (at least one license for the test functions) of the CENTUM VP packages that operate in coordination.

Then, install the ProSafe-RS software from the ProSafe-RS software medium. Licenses for ProSafe-RS software packages are not required.

### TIP

- If the CENTUM VP coexisting on the computer is earlier than R5.01, the CENTUM VP package that operates in coordination must be installed with the correct key code. The explanation in the subsequent sections assumes that the version of the coexisting CENTUM VP is R5.01 or later.
- When you move the CENTUM package from a computer where the function that operates with CENTUM VP licenses is used, fully install the ProSafe-RS software also on the new computer.

### ■ Installation on the Computer for Running SCS Simulator

SCS simulator is used in combination with the CENTUM packages listed in the following table. Licenses for ProSafe-RS packages are not required.

**Table B8-1 CENTUM Packages Required for SCS Simulator**

Model	CENTUM VP package name
LHS5420	Test Function Package
LHS5426	FCS Simulator Package
LHM5150	Test Function Package (for CENTUM VP Small)

With CENTUM VP R5.01 or later version, perform the following tasks on the computer where you use the SCS simulator. Either task can be performed first.

- Install CENTUM software and grant a license for any of the CENTUM packages in the table.
- Install ProSafe-RS software.

If the CENTUM VP version is earlier than R5.01, one of the following packages must be installed on the computer using the CENTUM VP key code, rather than through operation of the License Manager, before you install the ProSafe-RS software.

### SEE ALSO

For more information about installation of CENTUM VP software, refer to:

- CENTUM VP Installation (IM 33K01C10-50E)
- CENTUM VP Installation (IM 33M01A20-40E)

### ■ Installation on the Computer for Integration of CENTUM SOE Viewer

In the case of system configurations integrating CENTUM, it is possible to display SOE (Sequence of Events) of SCS on the CENTUM SOE Viewer. This is referred to as integration of CENTUM SOE Viewer. The ProSafe-RS software package licenses are not required.

With CENTUM VP R5.01 or later version, perform the following tasks on the computer where you use the SCS simulator. Either task can be performed first.

- Install CENTUM software and grant a license for the CENTUM SOE Viewer package (LPC6920).



- Install ProSafe-RS software.

If the CENTUM VP version is earlier than R5.01, the CENTUM SOE Viewer package must be installed on the computer using the CENTUM VP key code, rather than through operation of the License Manager, before you install the ProSafe-RS software.

In order to display SOE of SCS on the CENTUM SOE Viewer, it is necessary to connect the computer and SCS via V net or Vnet/IP.

---

**SEE  
ALSO**

For more information about how to grant license of CENTUM SOE Viewer Package (LPC6920), refer to:

License Management (IM 33K01C20-50E)

---

---

## C. Maintenance

This section describes the tasks required in the operation and maintenance of stations after they have been newly set up.

---

# C1. Adding Licenses and Changing License Assignments

This section describes how to add licenses, which is required to add new software packages on a station, and how to change the assignments of licenses, which is required to migrate software packages between stations.

---

## C1.1 Adding a License

The procedure for loading an additionally purchased license on the license management station is the same as the procedure for new installation.

---

**SEE  
ALSO**

For more information about how to load an additionally purchased license on the license management station, refer to:

[3.1, "Reading additional licenses on a license management station" in License Management \(IM 32Q01C60-31E\)](#)

---

---

## C1.2 Changing License Assignments

Use the License Manager on the license management station to add the license for the software package additionally required on a license-assigned station.

Also use the License Manager on the license management station to remove the license for the software package no longer required on a license-assigned station.

These operations are called “changing license assignments.”

---

**SEE  
ALSO**

For more information about changing license assignments, refer to:

[3.2, “Modifying licenses” in License Management \(IM 32Q01C60-31E\)](#)

---

## C2. Setting Up the Windows Domain Environment Later

This section describes the procedure for the case when you want to change the system that has been built as a Standalone management system to a Domain management system.

### ■ Workflow

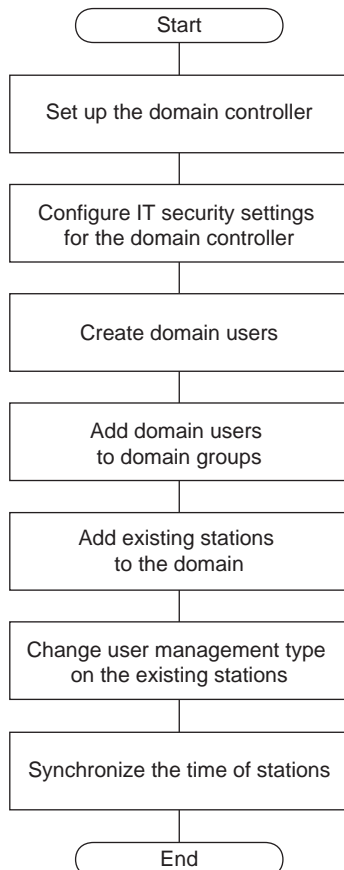


Figure C2-1 Workflow for Setting Up the Windows Domain Environment Later

### ■ Setup Procedure

1. Prepare a computer to be used as the domain controller and configure a domain controller on it.
2. Configure IT security settings.
3. Create domain users.
4. Add the domain users to domain groups.
5. Add the client computer stations to the domain.
6. On each station, change the user management type to Domain management or Combination management.
7. Synchronize the time of the stations within the domain.

**SEE  
ALSO**

For more information about configuring the domain controller, refer to:

[B2.2, "Configuring the Domain Controller \(Windows Server 2008/Windows Server 2008 R2\)" on page B2-3](#)

For more information about configuring IT security settings on the domain controller, refer to:

[B2.3, "Configuring Security Settings for the Domain Controller" on page B2-5](#)

For more information about how to create domain users and add them to domain groups, refer to:

[B2.4, "Creating Domain Users" on page B2-9](#)

For more information about how to add client computers to a domain, refer to:

[B2.5, "Adding Client Computers to the Domain" on page B2-13](#)

For more information about how to set up time synchronization within a domain, refer to:

[B2.7, "Setting Up Time Synchronization in Windows Domain Environment" on page B2-19](#)

For more information about changing the user management type, refer to:

[C8.1.2, "Procedures for a File Server or Domain Controller" on page C8-5](#)

## C3. Backing Up the System

To be prepared for system failures, it is recommended to back up the system periodically. The files in the folders listed in the following table should be regularly backed up:

**Table C3-1 Folder Backups**

Contents	Folder	Registry	When to back up
Backup of entire Windows	All hard disk	Entire registry	<ul style="list-style-type: none"> <li>When changes have been made to the system; for example, after program installation or completion of setup.</li> <li>After closing all applications</li> </ul>
ProSafe-RS engineering data	SCS project folders	-	After closing the SENG software

When you back up a system where the Standard model of IT security settings is applied, log on to Windows as an administrative user who has the right to access ProSafe-RS-related folders.

### ■ Backing Up Entire Windows

Back up Windows using a commercially available software program in preparation against disk trouble.

### ■ Creating Windows Repair Disk

Installing various application programs on a computer can cause troubles: for example, Windows does not start up, or you cannot log on to Windows. In such cases, if you have a system repair disk and boot disk, you can restore the system to the state at the time you created these disks.

To be prepared for Windows troubles, create a system repair disk and boot disk when you have changed the state of the system by installing a program, changing hardware configuration, etc.

#### SEE ALSO

For more information about how to create a repair disk, refer to:

Windows-related manual or the web site of Microsoft Corporation

### ■ Backing Up Projects

You can copy the ProSafe-RS folders to a backup medium using Windows Explorer. It is also possible to use commercially available backup software to back up the folders.

The SCS project folders should be backed up using Version Control Tool.

#### SEE ALSO

For more information about the explanation of Version Control Tool, refer to:

13., "Version Control" in Engineering Reference (IM 32Q04B10-31E)



---

## C4. Upgrading the ProSafe-RS Software

This section explains the procedure to follow when upgrading the ProSafe-RS software and tasks to be performed after upgrading.

## C4.1 Installation for Upgrading

This section explains the procedure to upgrade the ProSafe-RS software already installed on a computer to a newer version or revision.

### TIP

Upgrading the software where the number next to R is incremented by 1 or more, for example from R2.03 to R3.01, denotes version up, while the number next to R does not change, for example from R2.02 to R2.03, denotes revision up.

### ■ Items to be Prepared

Prepare the following items so that they are at hand before upgrading the ProSafe-RS software.

- ProSafe-RS software medium (Model: CHSKM30)
- ProSafe-RS license medium (Model: CHSCM30)
- ProSafe-RS license sheet (with project ID)

### ■ User Who Performs Update Installation

When update installation is performed, IT security settings are configured following the installation of the ProSafe-RS software. Update installation must be performed by a user who belongs to the groups shown in the following table.

Table C4.1-1 Groups to Which the User Who Performs Update Installation Belongs

Currently applied security model and user management type		Security model and user management type to be applied	
		Legacy model	Standard model
			Standalone type      Domain/Combination type
Legacy model		Administrators and PSF_MAINTENANCE of the local computer	Domain Admins and PSF_MAINTENANCE of the domain (*1)
Standard model	Standalone type		Administrators and PSF_MAINTENANCE of the local computer (*1) (*2)
	Domain/Combination type	Administrators and PSF_MAINTENANCE_LCL of the local computer (*1)	Domain Admins and PSF_MAINTENANCE of the domain (*1)

\*1: Log on the computer while it is connected to the domain.

\*2: While changing, the user name and password of the domain administrator are required.

### ■ Installing Latest Network Driver

Before upgrading the software, install the latest network driver (included in the new ProSafe-RS software version to be installed).

This section explains how to upgrade the control bus driver and Vnet/IP open communication driver.

#### ● Upgrading Control Bus Driver

When you upgrade the control bus driver, uninstall the current control bus driver first and then install the latest control bus driver.

### SEE ALSO

For more information about the uninstallation procedure of control bus driver, refer to:

“■ Uninstalling Control Bus Driver” on page C6-5

For more information about installing the control bus driver, refer to:

B3.3.1, “Installing the Control Bus Driver” on page B3-33

## ● Upgrading Vnet/IP Open Communication Driver

The procedure to upgrade Vnet/IP open communication driver is the same as the installation procedure of Vnet/IP open communication driver. If it is necessary to upgrade the Vnet/IP open communication driver, you can select [INSTALL] in the Setup dialog box.

Be sure to reboot the computer after upgrading the Vnet/IP open communication driver.

### SEE ALSO

For more information about installing the Vnet/IP open communication driver, refer to:

[B3.3.2, "Installing the Vnet/IP Open Communication Driver" on page B3-35](#)

## ■ Procedure for Update Installation

Follow these steps below to upgrade the ProSafe-RS software.

1. Log on as an administrative user.
2. Insert the ProSafe-RS software medium to the drive. The ProSafe-RS installation menu appears.  
If the installation menu does not appear, double-click Launcher.exe in the top folder of the software medium using Explorer.
3. Click [ProSafe-RS software].  
The Welcome dialog box appears if all the Windows redistribution modules required for ProSafe-RS have been installed. Proceed to step 6.  
The dialog box for confirming module installation appears if any of Windows redistribution modules required for ProSafe-RS have not been installed.
4. Click [Install] in the module installation confirmation dialog box. Module installation starts.
5. If the dialog box for confirming the privilege setting appears, reboot the computer and log on again.
  - a. Click [OK] and reboot the computer.
  - b. After rebooting the computer, log on again as the same user. The Welcome dialog box appears automatically.
6. Click [Next] in the welcome dialog box.  
The dialog box for confirming installation setup appears.

### TIP

- If a different version of control bus driver or Vnet/IP open communication driver is already installed, a dialog box appears, prompting you to update the driver. Confirm the message and click [OK]. To update the control bus driver, uninstall the existing driver and then install the new one after you install the ProSafe-RS software. To update the Vnet/IP open communication driver, install the new driver after you install the ProSafe-RS software.
- After updating the Vnet/IP open communication driver, disable the driver if the computer is to be connected to Ethernet.

7. Check the installation settings in the dialog box for confirming installation setup and click [Install]. The installation of ProSafe-RS starts and the dialog box showing installation progress status appears.
8. When you have completed the installation of the ProSafe-RS software, the installation complete dialog box appears.  
If there are no products to be installed subsequently, select [Yes, I want to set up IT security now.] and click [Finish].

### TIP

If you intend to continue to install other YOKOGAWA products, select [No, I want to install other software products.] and click [Finish].

**IMPORTANT**

If you select [No, I want to install other software products.] here, you must perform IT security settings when you install the last product.

**■ Additional Execution of IT Security Configuration**

If you are upgrading from R2 where the standard model of security settings are applied, you must configure IT security settings again in this way: after configuring the IT security settings following the installation of the product, reboot the computer and then start the IT Security Tool from the Start menu to configure the IT security settings.

**■ Tasks Related to Licenses**

After making IT security settings, perform the tasks related to licenses.

**SEE  
ALSO**

For more information about tasks related to licenses, refer to:

[B3.6, "Distributing and Accepting Licenses" on page B3-67](#)

## C4.2 Settings after Upgrading ProSafe-RS Software

This section explains the tasks to be performed after upgrading the SENG software.

Because the SCS databases and SCS system programs that SENG manages are basically upward compatible, there is no need to modify the engineering data created with earlier version software. However, in order to use the new features supported by the newer SCS system program, re-creation of the SCS project or offline downloading of database to SCS may be required after upgrading the SENG.



### IMPORTANT

- The SENGs in the same RS project should have the software of the same release number.
- Once opening an existing SCS project or creating a new SCS project using newer revision software in SENG, the SCS project cannot be opened using older revision software.
- The SCS system program release number of SCSs in a system should basically be the same, but mixture of different release numbers is allowed. However, the SCSs communicating with each other using the Inter-SCS safety communication function must have appropriate release numbers to be compatible.

### TIP

If Adobe Acrobat is not installed on the computer, it is recommended to upgrade the software for viewing the online manual to the Adobe Reader version recommended in this manual.

### SEE ALSO

For more information about release numbers of the SENG software and SCS system program in each software release and compatibility in inter-SCS safety communication between different revisions, refer to:

- [C5., "Upgrading to R3.02.20" on page C5-1](#)
- [Appendix 4., "Compatibility between Revisions and Cautionary Notes for Upgrading" on page App.4-1](#)

For more information about Adobe Reader settings, refer to:

[B4.1, "Online Manual Setting" on page B4-2](#)

## ■ Checking Inconsistency in TCP/IP Settings

After updating the software on the SENG, run the TCP/IP Inconsistency Detection Tool. If any inconsistencies are found in the setting, make TCP/IP settings again after executing the tool for repairing inconsistency in TCP/IP setting.

### SEE ALSO

For more information about the TCP/IP Inconsistency Detect Tool and TCP/IP Inconsistency Repair Tool, refer to:

■ [Procedure 6: Repair TCP/IP Settings" on page B3-52](#)

## ■ Settings after Upgrading Software

After upgrading the ProSafe-RS software, the following procedures need to be performed.

What procedure needs to be performed depends on what new features to be used. User needs to run the following procedures in accordance with each guideline of the revision upgrade procedure.

- Procedure A: Opening SCS Projects
- Procedure B: Master Database Offline Download
- Procedure C: Creating New SCS Project and Offline Download
- Procedure D: Setting Definition Items for New Features and Offline Download
- Procedure E: Clean Project, Build and Offline Download
- Procedure F: Setting Definition Items for New Features, Clean Project, Build, and Offline Download

Generally, only Procedure A needs to be performed after upgrading the software.



## IMPORTANT

You must perform one of the above procedures on SCS projects of all the SCSs that communicate with each other by inter-SCS safety communication. Be sure to perform "Procedure A" even for the SCSs that do not use new features. Otherwise, an error may occur during build.

## SEE ALSO

For more information about the procedures to use new features in each revision, refer to:

- C5., "Upgrading to R3.02.20" on page C5-1
- Appendix 4., "Compatibility between Revisions and Cautionary Notes for Upgrading" on page App.4-1

### ● Procedure A: Opening SCS Projects

After installing the latest revision of software in SENG, use SCS Manager to open the existing SCS projects created by the older revision software.

The SCS can continue to run. However, only the functions supported with older versions can be changed online.



## IMPORTANT

- The newer revision SCS Manager can simply open the SCS project created by the older revision SCS Manager.  
However, the project created by the older revision workbench can not be opened in the Read-Only status. It is necessary to open the SCS project in the Read-Write status.  
To open the project with password, the password needs to be entered and then open the project in the Read-Write status.
- It is necessary to use the newer revision SCS Manager at least once to open the library created by older revision SCS Manager.
- Procedure A must be done for the SCS projects of all the SCSs that communicate with each other by inter-SCS safety communication. Otherwise, an error may occur during build.

### ● Procedure B: Master Database Offline Download

For using the new features, this procedure may be necessary.

After upgrading the SENG, perform Master Database Offline Download to the SCS. Re-testing of SCS application is not required.

The outline of the procedure is as follows:

1. Run Procedure A.
2. Offline download to the SCS using Master Database Offline Download.

**SEE  
ALSO**

For more information about the procedure of Master Database Offline Download, refer to:

9.3, "Master Database Offline Download" in Engineering Reference (IM 32Q04B10-31E)

---

### ● Procedure C: Creating New SCS Project and Offline Download

For using the new features, this procedure may be necessary.

After upgrading SENG, create a new SCS project and remake the existing SCS project and then offline download the SCS project.

The procedure is the same as creating a new SCS project. And it is roughly as follows:

1. Create a new project and enter all the project settings.  
The existing SCS project can be upgraded to a later revision by using Import/Export functions. Upgrading the SENG to a newer revision and creating a new SCS project, the whole existing project data can be transferred to the new SCS project.

**TIP**

If the new SCS project uses a library, the library must be opened by a new-revision SCS Manager. However, if the library POU uses FB/FU supported only by a new revision, create a new library.

When you have upgraded an SENG, you must ensure that all SCS projects and library are of the same revision as the upgraded SENG.

Follow these steps to upgrade the revision of SCS and library:

1. Open each original library projects to upgrade. Then, copy the library to the predetermined folder, LIBRARIES, of the SCS project that uses the library.
2. Open each SCS project to upgrade.

If a project-level password is set for the SCS project or library, you have to enter the password and open it in ReadWrite mode in order to upgrade. If you do not know the password, contact the creator of the SCS project and library.

- 
2. Run build, and check the project data using Integrity Analyzer/Cross Reference Analyzer.
  3. Offline download the project.



## IMPORTANT

The SCS project and library created by an SENG in a revision later than the currently used revision cannot be used.

- The SCS project created or opened by a new revision of SENG cannot be opened by an SENG in an earlier revision.
  - The library created or opened by a new revision of SENG cannot be added to the SCS project of an earlier revision.
-

**SEE  
ALSO**

For more information about the procedures for transferring the existing SCS project using Import/Export functions, refer to:

2.20, "Import/Export Function" in Engineering Guide (IM 32Q01C10-31E)

For more information about the procedures for migrating the existing SCS project using the Import/Export functions, refer to:

"■ Confirming a Regenerated Project" in 2.20.4, "Data Transfer Procedure During SCS Project Regeneration" in Engineering Guide (IM 32Q01C10-31E)

For more information about offline downloading, refer to:

9.1, "Offline Download" in Engineering Reference (IM 32Q04B10-31E)

---

## ● Procedure D: Setting Definition Items for New Features and Offline Download

Some new features require this procedure.

Install the new revision of SENG software, set the definition items for the new features, and offline download the project.

The procedure is as follows:

1. Using SCS Manager, open the old-revision project.
2. Set the definition items for the new features.  
The items to be set are described in the section of upgrading procedures for each software release number.
3. Run Build. Then use Integrity Analyzer and Cross Reference Analyzer for approval check.



---

## IMPORTANT

Even if all POUs are displayed in green in the result of checking by Cross Reference Analyzer, further check is required if Cross Reference Analyzer is unable to detect differences related to the definition items of the new features.

- 
4. Offline download the project.

**SEE  
ALSO**

For more information about the items that cannot be detected by Cross Reference Analyzer, refer to:

"■ Other Changes Not Detectable by Cross Reference Analyzer" in 8.2.5, "Precautions on Cross Reference Analyzer" in Engineering Reference (IM 32Q04B10-31E)

---

## ● Procedure E: Clean Project, Build, and Offline Download

Some new features require this procedure.

After upgrading the SENG, run Clean Project and Build for the existing project, and offline download the project.

The procedure is as follows:

1. Using SCS Manager, open the old-revision project.
  2. Run Clean Project.
  3. Run Build. Then use Integrity Analyzer and Cross Reference Analyzer for approval check. In the check using Cross Reference Analyzer, make sure that all POUs are displayed in green.
  4. Offline download the project.
-



- **Procedure F: Setting Definition Items for New Features, Clean Project, Build, and Offline Download**

Some new features require this procedure.

This procedure consists of "Procedure D" plus Clean Project.

The procedure is as follows:

1. Using SCS Manager, open the old-revision project.
2. Set the definition items for the new features.  
The items to be set are described in the section of upgrading procedures for each software release number.
3. Run Clean Project.
4. Run Build. Then run Integrity Analyzer and Cross Reference Analyzer for an approval check.



## IMPORTANT

Even if all POUs are displayed in green in the result of checking by Cross Reference Analyzer, further check is required if Cross Reference Analyzer is unable to detect differences related to the definition items of the new features.

- 
5. Offline download the project.

### SEE ALSO

For more information about the items that cannot be detected by Cross Reference Analyzer, refer to:

“■ Other Changes Not Detectable by Cross Reference Analyzer” in 8.2.5, “Precautions on Cross Reference Analyzer” in Engineering Reference (IM 32Q04B10-31E)

---

## C4.3 Upgrading the Computer Dedicated to License Management

This section describes how to upgrade the computer dedicated to license management.

### ■ Upgrade Procedure

1. Install only the license management software from the ProSafe-RS software medium.

#### TIP

When upgrading the computer dedicated to license management, you can install the license management software in the same way as when it is installed for the first time. However, you are not required to enter the following items because the data already set are applied.

- Name
- Company name
- Installation folder

2. Configure IT security settings.

#### SEE ALSO

For more information about configuring the IT security settings, refer to:

[B3.5.2, "Running the IT Security Tool" on page B3-62](#)

For more information about installing the license management software, refer to:

[B6., "Setting Up the Computer Dedicated to License Management" on page B6-1](#)

# C5. Upgrading to R3.02.20

This section describes the cautions that you must exercise when upgrading from R3.02.10 to R3.02.20. Before you upgrade, also read the cautionary notes for upgrading to the previous versions that were issued after the software version currently installed on your computer and perform the required tasks for each upgrade.



## IMPORTANT

We recommend that you use the R5.04.00 or a later version of CENTUM VP when integrating ProSafe-RS with CENTUM VP.

## ■ Software Revisions

The respective software release number of R3.02.20 is as follows:

Software Release R3.02.20 (\*1)

- SENG software release number: R3.02.20 (\*1)
- SCS system program release number: R3.02.20 (\*1)

\*1: The last two digits of the release number will be changed in accordance with the software revisions after the release of R3.02.20.

### ● Inter-SCS Safety Communication

The release number of the SCS system program of an SCS that performs Inter-SCS safety communication with SCS with system program version R3.02.20 must be R1.01.30 or later.

If Vnet/IP is used for route of the Inter-SCS safety communication, the system programs on the SCSs must be of R1.02 or later.

### ● Control bus Drivers

The control bus drivers that are installed on the computer should be upgraded to the version supplied in R3.02.20.

**SEE  
ALSO**

For more information about how to update the control bus driver, refer to:

“● Upgrading Control Bus Driver” on page C4-2

## ■ Basic Procedure for Upgrading

To use the features added or modified, install the ProSafe-RS software R3.02.20 or later and open the existing SCS project.

## ■ Procedure for Using New and Modified Features

The following features added and upgraded in R3.02.20 cannot be used by the basic procedure for upgrading the revision. After the SENG software has been upgraded to R3.02.20, the steps such as offline downloading to SCS are required. Follow these steps to use each function.

**SEE  
ALSO**

For more information about settings after upgrading software, refer to:

“■ Settings after Upgrading Software” on page C4-5

- **ProSafe-SLS Communication Function**

To collect ProSafe-SLS data or events in SCS by using the ProSafe-SLS communication function, you need to perform "Procedure D" on an SENG of R3.02.20 or later.

- **DNP3 Slave Function**

To start communications from a DNP3 master by using the DNP3 slave function, you need to perform "Procedure C" on an SENG of R3.02.20 or later.

---

## C6. Uninstalling the ProSafe-RS Software

This section describes how to uninstall the ProSafe-RS software and network drivers. Procedures are provided for the following two cases:

- Uninstallation on SENG
- Uninstallation on the computer dedicated to license management

Note, however, that uninstalling the ProSafe-RS software does not remove the project database, user settings, registries, and so on. If you need to remove ProSafe-RS software completely, reinstall your operating system.

---

## **C6.1 Uninstallation on SENG**

This section describes the procedures for uninstallation on SENG.

## C6.1.1 Uninstalling the ProSafe-RS Software

If you uninstall the ProSafe-RS software, the license management software is also uninstalled. However, the license management data, IT Security Tool, and project data will not be deleted.

### TIP

The IT Security Tool is also used by YOKOGAWA products other than ProSafe-RS. Therefore, even if you uninstall the ProSafe-RS software, the Start menu setting, programs and files of the IT Security Tool will not be removed. To completely uninstall the IT Security Tool, you need to uninstall all the products that use the IT Security Tool and then run the command for uninstalling the IT Security Tool.

## ■ Deleting and Deactivating the Licenses

If there are any active licenses distributed on the SENG PC, delete the licenses to deactivate the software packages before uninstalling the ProSafe-RS software.

### SEE ALSO

For more information about how to deactivate software packages on a computer, refer to:

“■ Deleting a license from a license-assigned station” in 3.2.1, “Modifying license assignments” in License Management (IM 32Q01C60-31E)

## ■ Uninstallation Procedure

After deactivating the packages (deleting the licenses), follow these steps to uninstall the ProSafe-RS software:

1. From the Start menu, select [Control Panel] > [Programs] > [Programs and Features]. The following window appears.

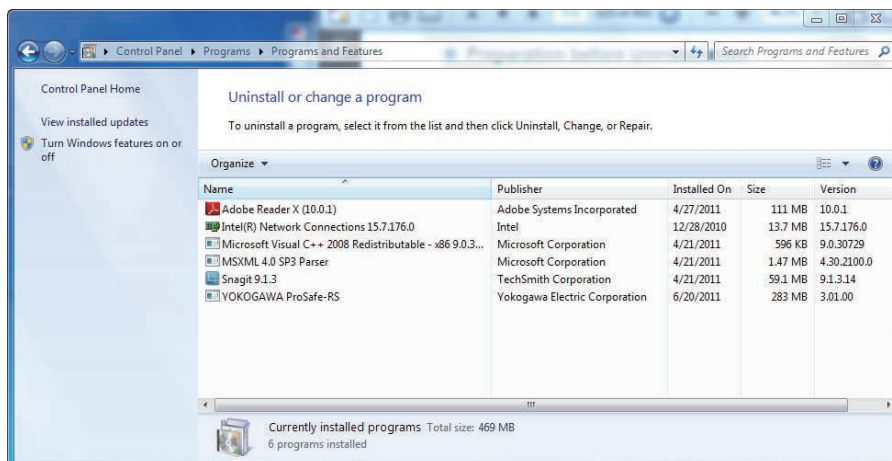


Figure C6.1.1-1 Programs and Features

2. Select [YOKOGAWA ProSafe-RS] and click [Change]. The Welcome dialog box appears.
3. Click [Next]. A dialog box for confirming the uninstallation appears.
4. Click [Remove]. Uninstallation starts and a dialog box showing the progress of uninstallation appears.

### TIP

If any active license is found, a dialog box appears confirming the continuation of the uninstallation process. Select [Yes] to continue the uninstallation. The active licenses are deactivated at this point.

However, the license information on the license management station remains unchanged. Update the license information on the license management station as necessary.

- 
5. If a User Account Control dialog box appears, click [Yes] or [Allow].

**TIP**

If you leave the User Account Control dialog box without clicking [Yes] or [Allow], the dialog box closes automatically. Then, a dialog box indicating failure of uninstallation appears, and the uninstallation is discontinued. In this case, run the uninstallation again.

---

6. In the uninstallation complete dialog box that appears upon completion of the uninstallation, do either of the following operations.:
- To restart the computer now, select [Yes, I want to restart my computer now.] and click [Finish].
  - To restart the computer later, select [No, I will restart my computer later.] and click [Finish].



## C6.1.2 Uninstalling the Network Drivers

This section describes how to uninstall the network drivers.

### ■ Uninstalling Control Bus Driver

Follow these steps to uninstall the control bus driver:

1. Log on as an administrative user.
2. Terminate all applications that are running.
3. Set the ProSafe-RS software medium in the drive.
  - If the AutoPlay dialog box appears, click [Run Launcher.exe].
  - If the AutoPlay dialog box does not appear, use Explorer and double-click Launcher.exe in the top folder of the software medium.

The installation menu appears.

4. Click [Control Bus Driver].  
The following dialog box appears.

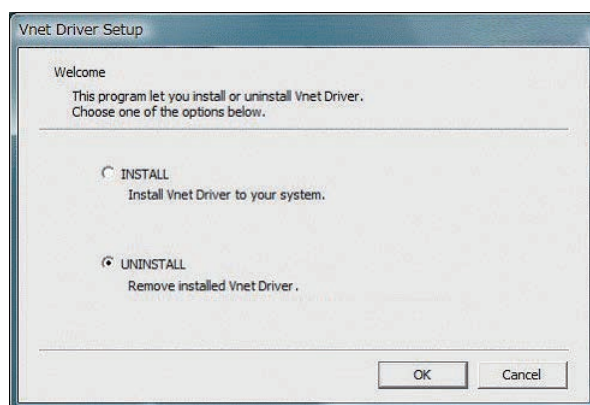


Figure C6.1.2-1 Setup Selection Dialog Box

5. Select [UNINSTALL] and then click [OK].  
A dialog box appears, confirming the uninstallation.
6. Click [OK].  
The uninstallation starts.
7. In the uninstallation complete dialog box that appears upon completion of the uninstallation, click [OK].
8. Restart the computer.



### IMPORTANT

After uninstalling the driver, run the TCP/IP Inconsistency Detection Tool.

If any inconsistency is detected, use the TCP/IP Inconsistency Repair Tool and then configure the TCP/IP settings again.

### SEE ALSO

For more information about the TCP/IP Inconsistency Detect Tool and TCP/IP Inconsistency Repair Tool, refer to:

“■ Procedure 6: Repair TCP/IP Settings” on page B3-52

## ■ Uninstalling the Vnet/IP Open Communication Driver

Follow these steps to uninstall the Vnet/IP open communication driver:

1. Log on as an administrative user.
2. Terminate all applications that are running.
3. Set the ProSafe-RS software medium in the drive.
  - If the AutoPlay dialog box appears, click [Run Launcher.exe].
  - If the AutoPlay dialog box does not appear, use Explorer and double-click Launcher.exe in the top folder of the software medium.

The installation menu appears.

4. Click [Vnet/IP Open com driver].  
The following dialog box appears.

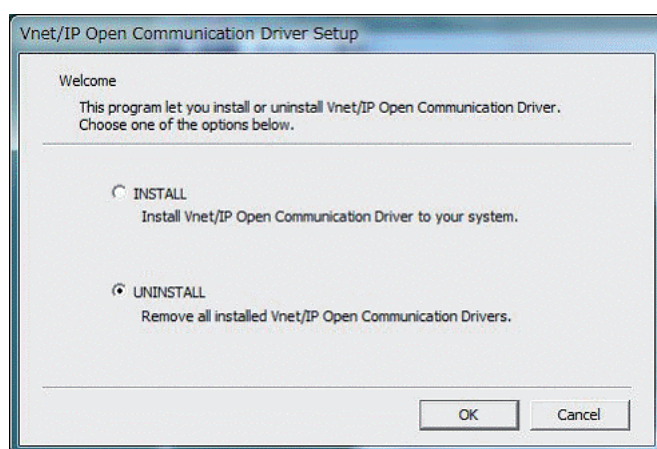


Figure C6.1.2-2 Setup Selection Dialog Box

5. Select [UNINSTALL] and then click [OK].  
A dialog box appears, confirming the uninstallation.
6. Click [OK].  
The uninstallation starts.
7. In the uninstallation complete dialog box that appears upon completion of the uninstallation, click [OK].
8. Restart the computer.



### IMPORTANT

After uninstalling the driver, run the TCP/IP Inconsistency Detection Tool.

If any inconsistency is detected, use the TCP/IP Inconsistency Repair Tool and then configure the TCP/IP settings again.

### SEE ALSO

For more information about the TCP/IP Inconsistency Detect Tool and TCP/IP Inconsistency Repair Tool, refer to:

■ [Procedure 6: Repair TCP/IP Settings](#) on page B3-52

## C6.2 Uninstallation on the computer Dedicated to License Management

This section describes the procedure for uninstalling the license management software on the computer dedicated to license management.

### ■ Running the Uninstallation

Follow these steps to uninstall the license management software:

1. Log on as an administrative user.
2. From the Start menu, select [Control Panel] > [Programs] > [Programs and Features].
3. From the program list, select [YOKOGAWA ProSafe-RS] and click [Change].  
The Welcome dialog box appears.
4. Click [Next].  
A dialog box for confirming the uninstallation appears.
5. Click [Delete].  
Uninstallation starts and a dialog box showing the progress of uninstallation appears.
6. In the uninstallation complete dialog box that appears upon completion of the uninstallation, do either of the following operations.:
  - To restart the computer now, select [Yes, I want to restart my computer now.] and click [Finish].
  - To restart the computer later, select [No, I will restart my computer later.] and click [Finish].

---

# C7. Reinstalling the ProSafe-RS Software

This section describes how to reinstall the ProSafe-RS Software. The procedures are explained for the cases when changing and not changing the computer to be used. For each case, the reinstallation procedure is explained for license-assigned stations and for the license management station.

## C7.1 When the Computer Used is the Same

This section describes the procedure for reinstalling the ProSafe-RS software to restore the software when the installed file gets damaged or deleted accidentally. The assumption is that the computer on which the software is to be installed is the same as before.

The software cannot be reinstalled by overwriting the software already installed. You must first uninstall the ProSafe-RS software and install the ProSafe-RS software again.

### ■ Reinstallation for a License-Assigned Station

This section describes the reinstallation procedure for a license-assigned station.

The flow of reinstallation is as follows.

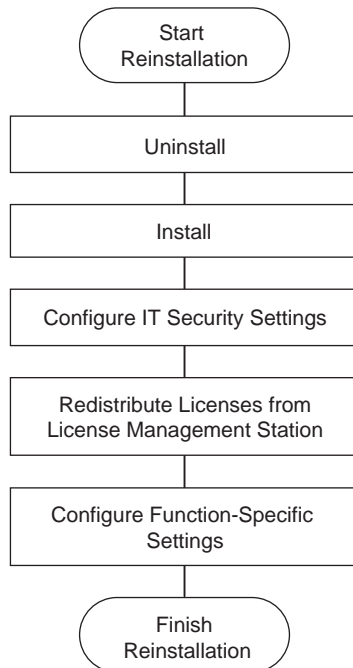


Figure C7.1-1 Flow of Reinstallation for a License-Assigned Station

#### ● Uninstall the ProSafe-RS Software

Uninstall the ProSafe-RS software.

**SEE  
ALSO**

For more information about the uninstallation procedure, refer to:

[C6.1.1, "Uninstalling the ProSafe-RS Software" on page C6-3](#)

#### ● Install the ProSafe-RS Software

Install the ProSafe-RS software.

**SEE  
ALSO**

For more information about installing the ProSafe-RS software, refer to:

[B3.4, "Installing the ProSafe-RS Software" on page B3-54](#)

#### ● Configure IT Security Settings

Configure IT security settings in the same way as that for a new installation of the ProSafe-RS software.

**SEE  
ALSO**

For more information about configuring the IT security settings, refer to:

[B3.5, "Configuring IT Security Settings" on page B3-58](#)

---

- **Redistribute Licenses from the License Management Station**

Redistribute the licenses from the license management station.

**SEE  
ALSO**

For more information about redistributing licenses from the license management station, refer to:

[3.4, "Redistributing licenses to license-assigned stations" in License Management \(IM 32Q01C60-31E\)](#)

---

- **Configure Function-Specific Settings**

Configure the settings specific to the functions that run on the SENG.

**SEE  
ALSO**

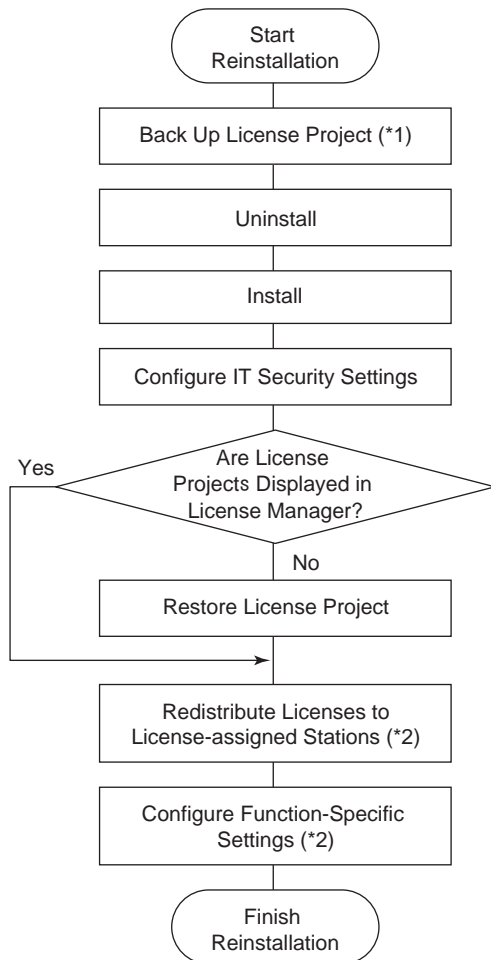
For more information about configuring the settings specific to each function of SENG, refer to:

[B4., "Configuring Function-Specific Settings on SENG" on page B4-1](#)

---

## ■ **Reinstallation for the License Management Station**

This section describes the reinstallation procedure for the license management station. The license management station can be a computer installed with the ProSafe-RS software or a computer dedicated to license management, where only the license management software is installed. You need to perform reinstallation according to the type of the license management station.



\*1: If the license project backup is already created, this task is not required.

\*2: These tasks are not required for the computer dedicated to license management.

**Figure C7.1-2 Flow of Reinstallation for the License Management Station**

### ● Back Up the License Projects

Back up the license projects managed on the computer.

#### SEE ALSO

For more information about the procedure for backing up the license project, refer to:

[3.6, "Backing up and restoring a license project" in License Management \(IM 32Q01C60-31E\)](#)

### ● Uninstall the ProSafe-RS Software

Uninstall the ProSafe-RS software. For a computer dedicated to license management, uninstall the license management software.

#### SEE ALSO

For more information about the procedure for uninstallation on an SENG PC, refer to:

[C6.1, "Uninstallation on SENG" on page C6-2](#)

For more information about the procedure for uninstallation on the computer dedicated to license management, refer to:

[C6.2, "Uninstallation on the computer Dedicated to License Management" on page C6-7](#)

---

- **Install the ProSafe-RS Software**

Install the ProSafe-RS software. For a computer dedicated to license management, install the license management software.

**SEE  
ALSO**

For more information about installing the ProSafe-RS software, refer to:

[B3.4, "Installing the ProSafe-RS Software" on page B3-54](#)

For more information about how to install the license management software, refer to:

[B6., "Setting Up the Computer Dedicated to License Management" on page B6-1](#)

---

- **Configure IT Security Settings**

Configure IT security settings in the same way as that for a new installation of the ProSafe-RS software.

**SEE  
ALSO**

For more information about configuring the IT security settings, refer to:

[B3.5, "Configuring IT Security Settings" on page B3-58](#)

---

- **Restore the License Projects**

Start the License Manager and then check if license projects are displayed. If not displayed, you need to restore the license projects from the backup.

**SEE  
ALSO**

For more information about the procedure for restoring a license project, refer to:

["■ Restoring a license project in another license management station" in 3.6, "Backing up and restoring a license project" in License Management \(IM 32Q01C60-31E\)](#)

---

- **Redistribute Licenses to License-Assigned Stations**

Redistribute the licenses to the license-assigned stations.

**SEE  
ALSO**

For more information about redistributing licenses from the license management station, refer to:

[3.4, "Redistributing licenses to license-assigned stations" in License Management \(IM 32Q01C60-31E\)](#)

---

- **Configure Function-Specific Settings**

Configure the settings specific to the functions that run on the SENG.

**SEE  
ALSO**

For more information about configuring the settings specific to each function of SENG, refer to:

[B4., "Configuring Function-Specific Settings on SENG" on page B4-1](#)

---



## C7.2 When the Computer Used is Not the Same

This section describes the procedure for reinstallation on a different computer when the computer installed with the ProSafe-RS software can no longer be used due to damage or other reasons.

### ■ Reinstallation for a License-Assigned Station

This section describes the reinstallation procedure for a license-assigned station.

The procedure is the same as that for a new setup of SENG except that you need to restore the data that were backed up.

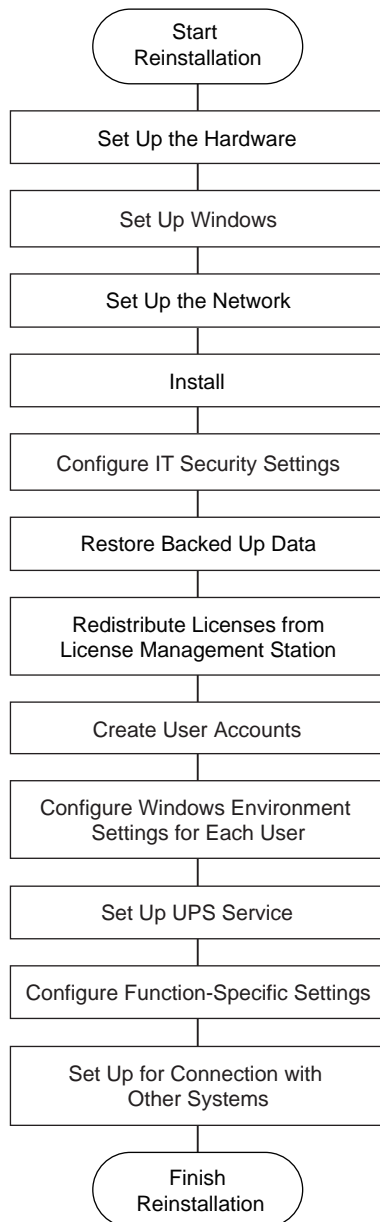


Figure C7.2-1 Flow of Reinstallation for a License-Assigned Station

**IMPORTANT**

For the station name of the new computer, specify the same name as that set on the previous computer.

**SEE  
ALSO**

For more information about the procedures for a new setup of SENG, refer to:

- B3., "Setting Up the SENG" on page B3-1
- B4., "Configuring Function-Specific Settings on SENG" on page B4-1
- D1., "Connecting YOKOGAWA products" on page D1-1

**● Restore the Backed Up Data**

Restore the backed up data on the new computer.

**SEE  
ALSO**

For more information about the backed up data, refer to:

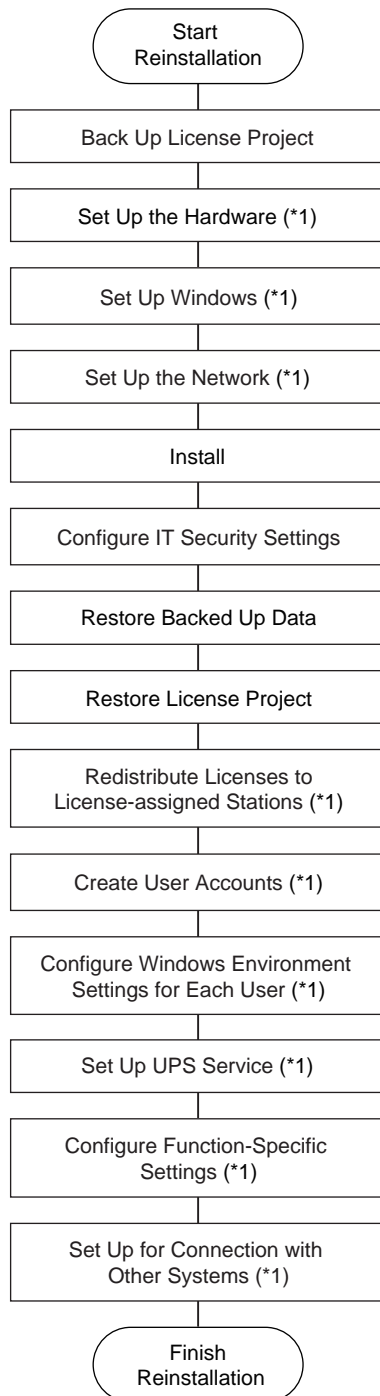
C3., "Backing Up the System" on page C3-1

**■ Reinstallation for the License Management Station**

The license management station can be a computer installed with the ProSafe-RS software or a computer dedicated to license management. You need to perform reinstallation according to the type of the license management station.

The procedure is the same as that for a new setup except that the following tasks are involved:

- Back up license projects
- Restore the backed up data
- Restore the license projects
- Redistribute licenses to the license-assigned stations



\*1: For the computer dedicated to license management, these tasks are not required or may be omitted according to the circumstances.

**Figure C7.2-2 Flow of Reinstallation for the License Management Station**



## IMPORTANT

For the station name of the new computer, specify the same name as that set on the previous computer.

**SEE  
ALSO**

For more information about the procedures for a new setup of SENG, refer to:

- B3., "Setting Up the SENG" on page B3-1
- B4., "Configuring Function-Specific Settings on SENG" on page B4-1
- D1., "Connecting YOKOGAWA products" on page D1-1

For more information about the procedure for a new setup of a computer dedicated to license management, refer to:

B6., "Setting Up the Computer Dedicated to License Management" on page B6-1

---

- **Back Up the License Projects**

Back up the license projects managed on the previous computer.

**SEE  
ALSO**

For more information about the procedure for backing up the license projects, refer to:

3.6, "Backing up and restoring a license project" in License Management (IM 32Q01C60-31E)

---

- **Restore the Backed Up Data**

Restore the backed up data on the new computer.

**SEE  
ALSO**

For more information about the backed up data, refer to:

C3., "Backing Up the System" on page C3-1

---

- **Restore the License Projects**

Restore the license projects from the backup.

**SEE  
ALSO**

For more information about the procedure for restoring the license projects, refer to:

■ Restoring a license project in another license management station" in 3.6, "Backing up and restoring a license project" in License Management (IM 32Q01C60-31E)

---

- **Redistribute Licenses to License-Assigned Stations**

Redistribute licenses to the license-assigned stations.

**SEE  
ALSO**

For more information about redistributing licenses from the license management station, refer to:

3.4, "Redistributing licenses to license-assigned stations" in License Management (IM 32Q01C60-31E)

---

## C8. Maintenance Tasks Related to IT Security

This section describes the tasks related to IT security settings that are performed apart from new or upgrade installation of the ProSafe-RS software.

## C8.1 Changing the IT Security Settings

This section describes how to change the security settings that have been applied.

Changing the security settings may do the following:

- Change the security model
- Change the user management type
- Change Individual setting items



### IMPORTANT

Before you change the IT security settings, take a backup of the current security settings.

---

#### SEE ALSO

For more information about the explanation of how to back up security settings, refer to:

[C8.2, “Saving the IT Security Settings” on page C8-8](#)

---

### ■ Confirming the Applied Security Model and User Management Type

You can confirm the currently applied security model and user management type.

#### SEE ALSO

For more information about how to check the currently set security model and user management type, refer to:

“■ Find Out the Applied Security Model and User Management Type” in 6.1, “IT Security Tool” in Pro-Safe-RS Security Guide (IM 32Q01C70-31E)

---

## C8.1.1 Procedures for SENG PC

This section describes the procedures for changing the security settings on an SENG PC.

### ■ Precautionary Notes

Precautionary notes on changing IT security settings on a computer installed with ProSafe-RS software are as follows:

#### ● Note on Changing the Security Model to Legacy Model

When you have changed to the Legacy model for a system using Windows authentication, which is a user authentication mode available with the access control and operation history management functions, you must configure the settings for using ProSafe authentication.

#### SEE ALSO

For more information about required settings for ProSafe authentication mode, refer to:

- “■ Specifying the User Authentication Mode” in 16.2.1, “Settings for Access Control” in Engineering Reference (IM 32Q04B10-31E)
- “■ Settings Required When ProSafe Authentication Mode is Selected” in 16.2.1, “Settings for Access Control” in Engineering Reference (IM 32Q04B10-31E)
- “■ Tasks Required after Changing User Authentication Mode” in 16.3.2, “Operations Performed by Administrators” in Engineering Reference (IM 32Q04B10-31E)

#### ● Notes on Changing the User Management Type

- When you change from Standalone management to Domain/Combination management, create user groups and user accounts in advance using the domain controller.
- When you change from Standalone management to Domain/Combination management, add the computer to the domain before applying the IT security settings.
- When you change from Domain/Combination management to Standalone management, you may remove the computer from the domain either before or after applying the IT security settings.

For a system using Windows authentication, which is a user authentication mode available with the access control/operation history management function, you need to perform the following tasks:

- When you have changed from Standalone management to Domain/Combination management or vice versa, you need to set up the users who uses SENG again. If you created a new Windows user of SENG, register the user in the Engineers' Account Builder.

#### SEE ALSO

For more information about the tasks on the domain controller and how to add computers to a domain, refer to:

B2., “Setting Up the Windows Domain Environment” on page B2-1

For more information about the explanation of how to register engineers, refer to:

“■ Registering an Engineer's Account” in 16.2.3, “Registering Engineers” in Engineering Reference (IM 32Q04B10-31E)

## ■ User Who Changes IT Security Settings

Table C8.1.1-1 Groups to Which the User Who Changes IT Security Settings Belongs

Currently applied security model and user management type		Security model and user management type to be applied	
		Legacy model	Standard model
			Domain/Combination type
Legacy model		Domain Admins and PSF_MAINTENANCE of the domain (*1)	
Standard model	Standalone type	Administrators and PSF_MAINTENANCE of the local computer	
	Domain/Combination type	Administrators and PSF_MAINTENANCE of the local computer (*1) (*2)	
		Domain Admins and PSF_MAINTENANCE_LCL of the local computer (*1)	
		Domain Admins and PSF_MAINTENANCE of the domain (*1)	

\*1: Log on to the computer while it is connected to the domain.

\*2: While changing, the user name and password of the domain administrator are required.

## ■ Changing Procedure

1. Log on to the computer as the user who changes the security settings.
2. From the Start menu, click [YOKOGAWA Security] > [IT Security Tool].  
The IT Security Tool starts.
3. Click [Setup].
4. Select the security model and user management type you want to change to.  
The rest of the procedure is the same as that for the normal setups.

### SEE ALSO

For more information about running the IT Security Tool, refer to:

[B3.5.2, "Running the IT Security Tool" on page B3-62](#)

## ■ Changing the Security Model when CENTUM VP R4.01 to R4.03 is Coexisting on the Computer

If CENTUM VP of a version from R4.01 to R4.03 is coexisting on the computer, the security model should be changed by a user who belongs to both the PSF\_MAINTENANCE and CTM\_MAINTENANCE groups.

In this case, change the security model for CENTUM VP first, and then change the security model for ProSafe-RS.



## C8.1.2 Procedures for a File Server or Domain Controller

This section describes the procedures for changing the security settings on a computer that serves only as a file server or a domain controller computer.



### IMPORTANT

When you change the IT security settings on a file server or domain controller computer, prepare the initial security settings that were saved before using the IT Security Tool.

### ■ User Who Changes IT Security Settings on a File Server

Table C8.1.2-1 Groups to Which the User Who Changes the Security Settings Belongs

Currently applied security model and user management type		Security model and user management type to be applied	
		Legacy model	Standard model
			Standalone type      Domain/Combination type
Legacy model		Administrators of the local computer	Administrators and PSF_MAINTENANCE of Local Group (*1)      Domain Admins and PSF_MAINTENANCE of the domain (*1) (*2)
Standard model	Standalone type	Administrators and PSF_MAINTENANCE of the local computer (*1)	Administrators and PSF_MAINTENANCE of the local computer (*1) (*3)
	Domain/Combination type	Administrators and PSF_MAINTENANCE_LCL of the local computer (*1) (*2)	Domain Admins and PSF_MAINTENANCE of the domain (*1) (*2)

\*1: If any other YOKOGAWA product coexists in the computer, the user also needs to be a member of the MAINTENANCE group of the coexisting product. For example, if CENTUM VP coexists, also add the user to the CTM\_MAINTENANCE group.

\*2: Log on to the computer while it is connected to the domain.

\*3: Until you reset the security settings to the initial status, log on the computer while it is standalone. Subsequently, when you log on the computer to apply security settings, the computer should be connected to the domain.

### ■ User Who Changes IT Security Settings on the Domain Controller

When changing the IT security settings on the domain controller computer, log on the computer as a user who belongs to the Domain Admins and PSF\_MAINTENANCE groups of the domain.

### ■ Changing Procedure

The following three procedures are described here.

- Basic procedure
- Procedure to change from Standard model (Standalone management) to Standard model (Domain/Combination management) on a file server
- Procedure to change from Standard model (Domain/Combination management) to Standard model (Standalone management) on a file server

#### ● Basic Procedure for Changing Security Settings

1. Log on as the user who changes the security settings.
2. Start the installation menu from the ProSafe-RS software medium and click [Setting IT Security (File server/domain controller use)] to start the IT Security Tool.
3. Click [Restore].
4. Select a file that the previous security settings are saved prior to running the IT Security Setting Tool so as to restore the securities.

For a file server, if it is not a domain member now, use the file holding the initial security settings that were saved while it was standalone. If it is a domain member now, use the file holding the initial security settings that were saved after it joined the domain.

5. After restoring is completed, restart the computer.
6. For a file server, if its domain membership is to be changed, add to or remove from the domain.
7. Start the installation menu again and click [Setting IT Security (File server/domain controller use)] to start the IT Security Tool.
8. Click [Setup].
9. Select the security model and the user management type you want to change to. The rest of steps are the same as the procedure for the first time setup.

**SEE  
ALSO**

For more information about how to start the installation menu, refer to:

[B3.4, "Installing the ProSafe-RS Software" on page B3-54](#)

For more information about first time setup of IT security settings on a file server, refer to:

[B5.1, "Setting Up a Computer that Serves Only as a File Server" on page B5-2](#)

For more information about first time setup of IT security settings on the domain controller, refer to:

[B2.3, "Configuring Security Settings for the Domain Controller" on page B2-5](#)

For more information about restoring the IT security settings on the file server or domain controller, refer to:

[C8.3.2, "Procedure for a File Server or Domain Controller" on page C8-16](#)

### ● **When Changing from Standard Model (Standalone Management) to Standard Model (Domain/Combination Management) on a File Server**

For this change, you need to save the security settings after the file server computer joined a domain because the security settings are changed by joining the domain. Follow these steps to make the change:

1. Log on as an administrative user who belongs to the Administrators and PSF\_MAINTENANCE groups of the local computer.
2. Start the installation menu from the ProSafe-RS software medium.
3. Click [Setting IT Security (File server/domain controller use)] to start the IT Security Tool.
4. Restore the initial security settings saved (while the computer is not a member of a domain) before you first time used the IT Security Tool to setup security.
5. After restarting, add the computer to the domain.
6. Log on as the same administrative user you previously logged on in step 1.
7. Start the installation menu and click [Setting IT Security (File server/domain controller use)].  
The IT Security Tool starts.
8. Click [Save].
9. Save the security settings as the initial settings right after it joined a domain.
10. On the IT Security Tool's menu, click [Setup].
11. Select the security model and user management type for the file server, and run the setup.
12. After applying the security settings, restart the computer.

- **When Changing from Standard Model (Domain/Combination Management) to Standard Model (Standalone Management) on a File Server**

For this change, the timing of removal from the domain is different from the basic procedure.

1. Log on as an administrative user who belongs to the Administrators and PSF\_MAINTENANCE\_CTL groups of the local computer.
2. Start the installation menu from the ProSafe-RS software medium.
3. Click [Setting IT Security (File server/domain controller use)] to start the IT Security Tool.
4. Click [Restore] to restore the initial security settings that were saved (right after the computer joined a domain) before the IT Security Tool was first used to setup security.
5. Restart the computer.
6. Log on as the same administrative user you previously logged on in step 1.
7. Start the installation menu from the ProSafe-RS software medium.
8. Click [Setting IT Security (File server/domain controller use)] to start the IT Security Tool.
9. Click [Setup], select Standard model and Standalone management for the file server, and run the setup.
10. After applying the security settings, restart the computer.
11. Remove the computer from the domain.

## C8.2 Saving the IT Security Settings

You can save the security settings on the local computer using the Save function.

The saved IT security settings can be restored by using the Restore function of the IT Security Tool as necessary.

### ■ User Who Performs Saving

When performing saving, log on as a user who belongs to the groups shown in the following table.

**Table C8.2-1 Groups to Which the User Who Saves the Security Settings Belongs**

Currently applied security model and user management type		
Legacy model	Standard model	
	Standalone type	Domain/Combination type
Administrators of the local computer	Administrators and PSF_MAINTENANCE of the local computer	Administrators and PSF_MAINTENANCE_LCL of the local computer
		Domain Admins and PSF_MAINTENANCE of the domain

### ■ Regarding the Files that Hold the Saved Security Settings

Saving the security settings creates two files with extensions of .hed and .csf.

When restoring the saved security settings, both files are required.

## C8.2.1 Procedure for SENG PC

This section describes the procedure for saving the security settings on an SENG PC.

### ■ Saving Procedure

1. From the Start menu, click [YOKOGAWA Security] > [IT Security Tool].  
The IT Security Tool starts.
2. Click [Save].  
The Specify destination page appears.

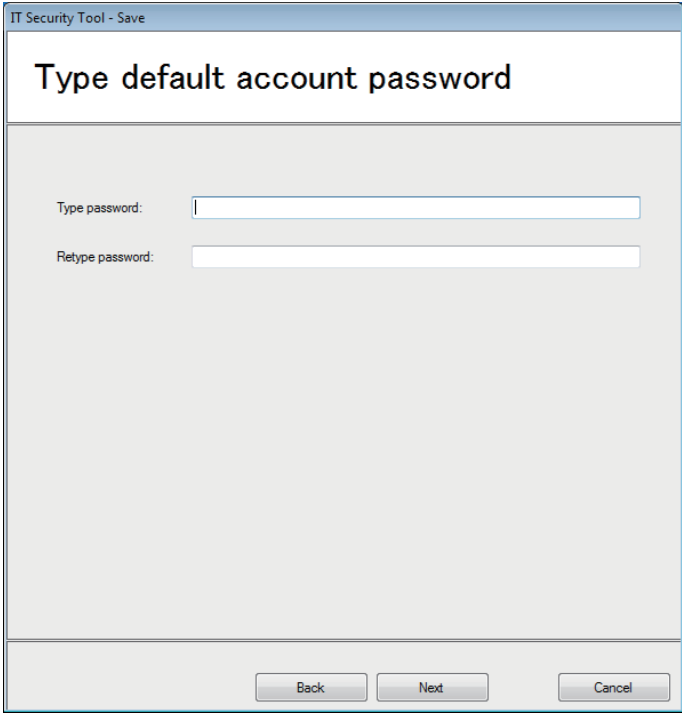
The screenshot shows a window titled "IT Security Tool - Save". The main heading is "Specify destination". Below this, there are several input fields and a list:

- Destination:** A text box followed by a small blue square icon with a magnifying glass.
- Distinguished Name:** A text box.
- Support Product:** A text box.
- Support OS:** A list box containing the following items:
  - ☐ Windows 7
  - ☐ Windows Server 2008 R2
  - ☐ Windows Server 2008
  - ☐ Windows Vista
  - ☐ Windows Server 2003 R2
  - ☐ Windows Server 2003
  - ☐ Windows XP
- File Version:** A text box.

At the bottom of the window, there are three buttons: "Back", "Next", and "Cancel".

**Figure C8.2.1-1 Specify Destination**

3. Specify the destination folder and enter other required settings.  
The Distinguished Name and File Version are omissible.
4. Click [Next].  
The Type default account password page appears.



The screenshot shows a window titled "IT Security Tool - Save". Inside the window, the title "Type default account password" is displayed at the top. Below the title, there are two text input fields. The first field is labeled "Type password:" and the second field is labeled "Retype password:". At the bottom of the window, there are three buttons: "Back", "Next", and "Cancel".

**Figure C8.2.1-2 Type Default Account Password**

5. Enter the password for use as the initial account password and click [Next].

**TIP**

This password will be used to recover the saved accounts. If the saved accounts are not found on the computer when you recover the accounts, new accounts are created. All the created accounts will be assigned with a same password.

If password policy is set and the account password does not meet the password policy, an error will occur when recovering an account.

You will be prompted to change the password when log on this account next time.

The page for entering the password for use as the encryption key of the saved data appears.

**Figure C8.2.1-3 Type Password (Encryption Key)**

6. Enter the Encryption Key and then click [Next].  
Saving of the security settings starts.



## IMPORTANT

- If this password (encryption key) is lost, the saved security settings cannot be restored. The password (encryption key) must be carefully kept by the customer.
- The password (encryption key) must be at least one character.
- The password can consist of upper-case and lower-case alphanumeric characters and the following symbols: ` ~ ! @ # \$ % ^ & \* ( ) \_ + - = { } | \ : " ' < > ? , . /  
Double-byte characters cannot be used.

7. When the saving is completed, click [Finish].  
If the saving failed, the details of the failure are displayed.
8. On the IT Security Tool menu, click [Close].



## IMPORTANT

If any save failures are displayed, contact YOKOGAWA Service.

---

## C8.2.2 Procedure for a File Server or Domain Controller

To save the IT security settings on a computer that serves only as a file server or a domain controller computer, start the installation menu from the ProSafe-RS software medium and click [Setting IT Security (File server/domain controller use)] to start the IT Security Tool. The rest of steps are the same as the procedure for an SENG PC.

---

**SEE  
ALSO**

For more information about how to start the installation menu, refer to:

[B3.4, "Installing the ProSafe-RS Software" on page B3-54](#)

---



## C8.3 Restoring the IT Security Settings

You can restore the security settings of a local computer that were saved by using the Save function.

### ■ Preparation for Restoration

According to the user management type of the security settings to be restored, the computer may be required to join a domain or removed from a domain. To restore to the Legacy mode or Standard model with Standalone management, the computer needs to be removed from a domain. To restore to the Standard model with Domain or Combination management, the computer needs to join a domain.

### ■ User Who Performs Restoring

Log on as a user who belongs to the groups shown in the following table.

**Table C8.3-1 Groups to Which the User Who Restores the Security Settings Belongs**

Security model and user management type to be restored to		
Legacy model	Standard model	
	Standalone type	Domain/Combination type
Administrators of the local computer	Administrators and PSF_MAINTENANCE of the local computer	Administrators and PSF_MAINTENANCE_LCL of the local computer (*1)
		Domain Admins and PSF_MAINTENANCE of the domain

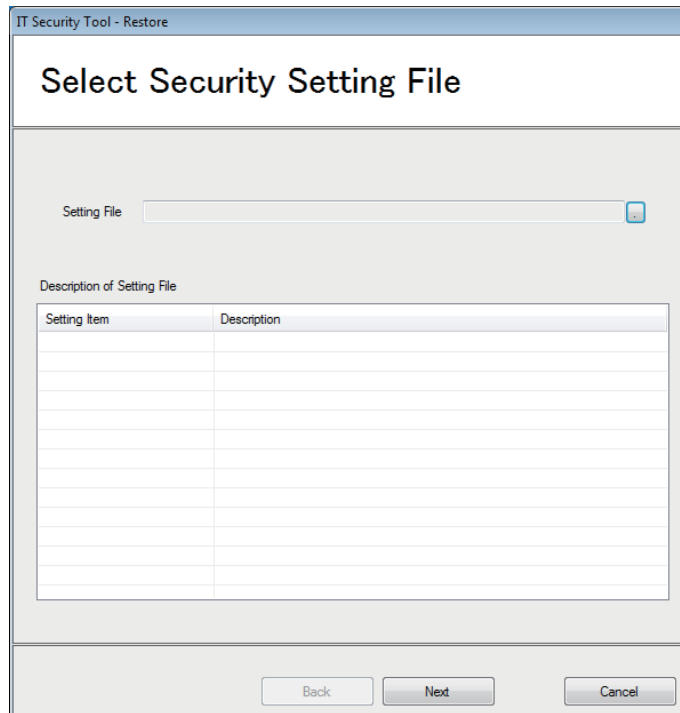
\*1: Log on as a user who belongs to these groups when the PSF\_MAINTENANCE\_LCL group does not exist on the local computer (that is, when the security model and user management type set before restoration is Legacy model or Standard model with Standalone management ).

## C8.3.1 Procedure for SENG PC

This section describes the procedure for restoring the security settings on an SENG PC.

### ■ Restoring Procedure

1. Click [YOKOGAWA Security] > [IT Security Tool] from the Windows Start menu.  
The IT Security Tool starts.
2. Click [Restore].  
The Select Security Setting File page appears.



**Figure C8.3.1-1 Select Security Setting File**

3. Click [...] next to the Setting File box.  
The Open dialog box appears.
4. Select the file you want to use for restoration and then click [Open].

#### TIP

Of the files that were created when the security settings were saved, select the file with .hed extension.

A dialog box appears, prompting you to enter the password (encryption key) for reading the selected file.

5. Enter the password (encryption key) that was set when the file was saved and click [OK].  
If the selected file is restorable, the details are displayed in the Select Security Setting File page.
6. Click [Next].  
The Confirm Setting Information page appears.

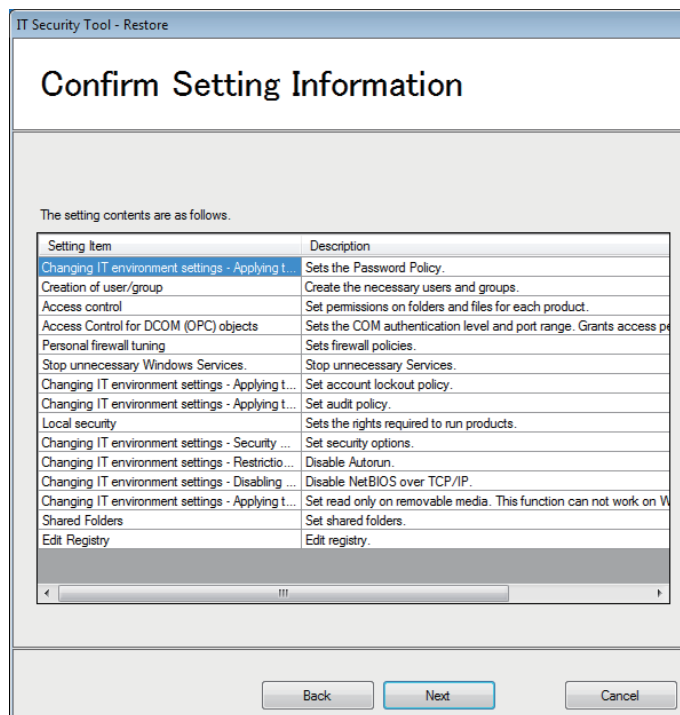


Figure C8.3.1-2 Confirm Setting Information

**TIP**

Items displayed in the Confirm Setting Information page represent the items accessed when restoring the saved security settings. Although the descriptions of these items are affirmative sentences, it doesn't mean that all of these settings will be applied. Note that the status of whether each item is set to be applied or not is not displayed on the screen.

7. Confirm the settings and click [Next].  
When the setup process is complete, the Setup Completed page appears.

**TIP**

If there are any items that failed to be set, a list of failed items is displayed.

8. Select the check box for [Restart Now] and click [Finish].
9. Click [Close] to end the IT Security Tool.

**IMPORTANT**

If any setup failures are displayed, contact YOKOGAWA Service.

---

## C8.3.2 Procedure for a File Server or Domain Controller

To restore the IT security settings on a computer that serves only as a file server or a domain controller computer, start the installation menu from the ProSafe-RS software medium and click [Setting IT Security (File server/domain controller use)] to start the IT Security Tool. The rest of steps are the same as the procedure for an SENG PC.

---

**SEE  
ALSO**

For more information about how to start the installation menu, refer to:

[B3.4, "Installing the ProSafe-RS Software" on page B3-54](#)

---

---

## C8.4 Changing the Security Setting File Password

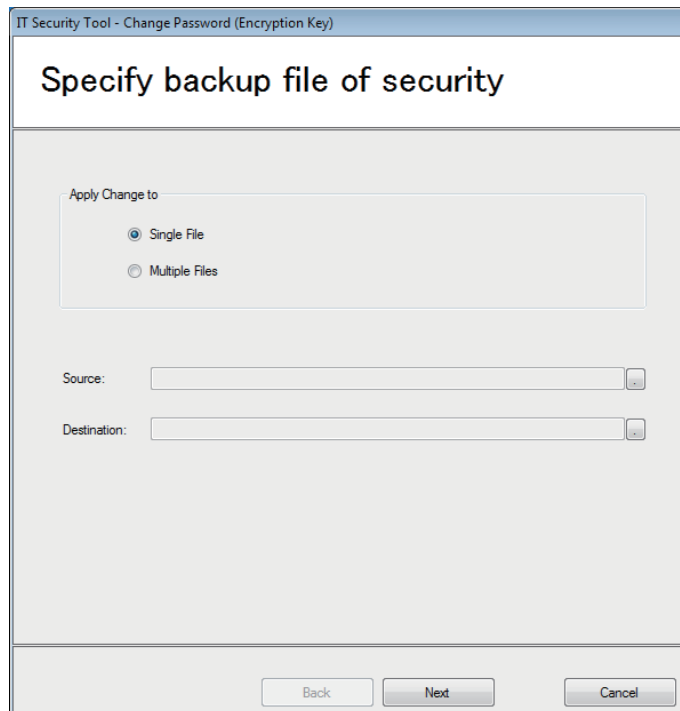
You can change the password (encryption key) for security setting files used by the IT Security Tool.

## C8.4.1 Procedures for SENG PC

This section describes the procedure for changing the password (encryption key) for security setting files on an SENG PC.

### ■ Changing Procedure

1. Log on as a member of the PSF\_MAINTENANCE group (or as an administrative user when the Legacy model is applied), and click [YOKOGAWA Security] > [IT Security Tool] from the Start menu.  
The IT Security Tool starts.
2. Click [Change Password (Encryption Key)].  
The Specify backup file of security page appears.



**Figure C8.4.1-1 Specify backup file of security**

3. Select either of the Apply Change to options and set as follows:
  - If you just want to change the encryption key of one file, select [Single File], and then specify the source file and the name of the folder to which the file after conversion is to be saved.
  - If you want to change the encryption key of multiple files in a folder, select [Multiple Files], and then specify the source file folder and the folder to which the files after conversion are to be saved.

#### TIP

- The encryption key for a pair of saved files (with .hed and .csf extensions) should be changed to the same encryption key.
- When [Single File] is selected, you can change only one file at a time. So, you need to do the operation twice to change for both .hed file and .csf files.
- When [Multiple Files] is selected, all the files in the specified source folder are changed together.
- The files generated in the destination folder will have the same file names as those in the source folder.
- Ensure that all the files in a folder have the same encryption key.

4. Click [Next].  
The Change Password (Encryption Key) page appears.



The screenshot shows a dialog box titled "IT Security Tool - Change Password (Encryption Key)". The main heading inside the dialog is "Change Password (Encryption Key)". Below the heading, there are three text input fields with labels: "Type old password (Encryption Key):", "Type new password (Encryption Key):", and "Retype new password (Encryption Key):". At the bottom of the dialog, there are three buttons: "Back", "Next", and "Cancel".

**Figure C8.4.1-2 Change Password (Encryption Key)**

5. Enter the old and the new encryption keys and click [Next].  
When the changing process is completed, the Changed Password (Encryption Key) page appears.
6. Click [Finish].
7. Click [Close] on the IT Security Tool menu.

## C8.4.2 Procedure for a File Server or Domain Controller

This section describes the procedure for changing the password (encryption key) for security setting files on a computer that serves only as a file server or a domain controller computer.

### ■ Changing Procedure

1. Log on as a member of the PSF\_MAINTENANCE group (or as an administrative user when the Legacy model is applied).
2. Start the installation menu from the ProSafe-RS software medium, and click [Setting IT Security (File server/domain controller use)] to start the IT Security Tool.  
The rest of steps are the same as the procedure for an SENG PC.

---

**SEE  
ALSO**

For more information about how to start the installation menu, refer to:

[B3.4, "Installing the ProSafe-RS Software" on page B3-54](#)

---



---

# C9. Troubleshooting

This section describes the causes of and remedies for problems that may occur.

## C9.1 Windows Related Troubleshooting

This section describes how to handle problems related to Windows.

### ■ Note on User Account Control

If you log on as a non-administrative user and try to start the installer, the following dialog box appears. Click [No] and log on again as an administrative user, and then start the installer again.

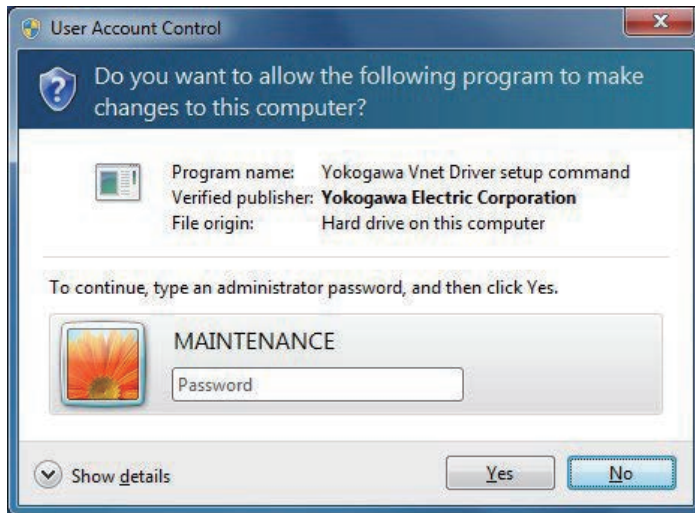


Figure C9.1-1 User Account Control Dialog Box (When Logged on as a Non-administrative User)

### ■ The System Locks Up

Contact YOKOGAWA service.

### ■ Computer Operation Becomes Unstable

If the operation of the computer that was working normally has become unstable, do the task described below.

- **Cause**

Incompatible software was installed.

- **Remedy**

Uninstall the incompatible software you have installed.

**SEE  
ALSO**

For more information about software that can coexist with ProSafe-RS, refer to:

“● Software that can Coexist with ProSafe-RS” on page A3-4

---

## C9.2 Troubleshooting Related to Network

This section describes how to handle problems related to the network.

## C9.2.1 Precaution on Network Cable Connection

On Windows 7 or Windows Server 2008 R2, the Set Network Location dialog box may appear when you connect the cables for network connection. If the dialog box appears, select [Public network].

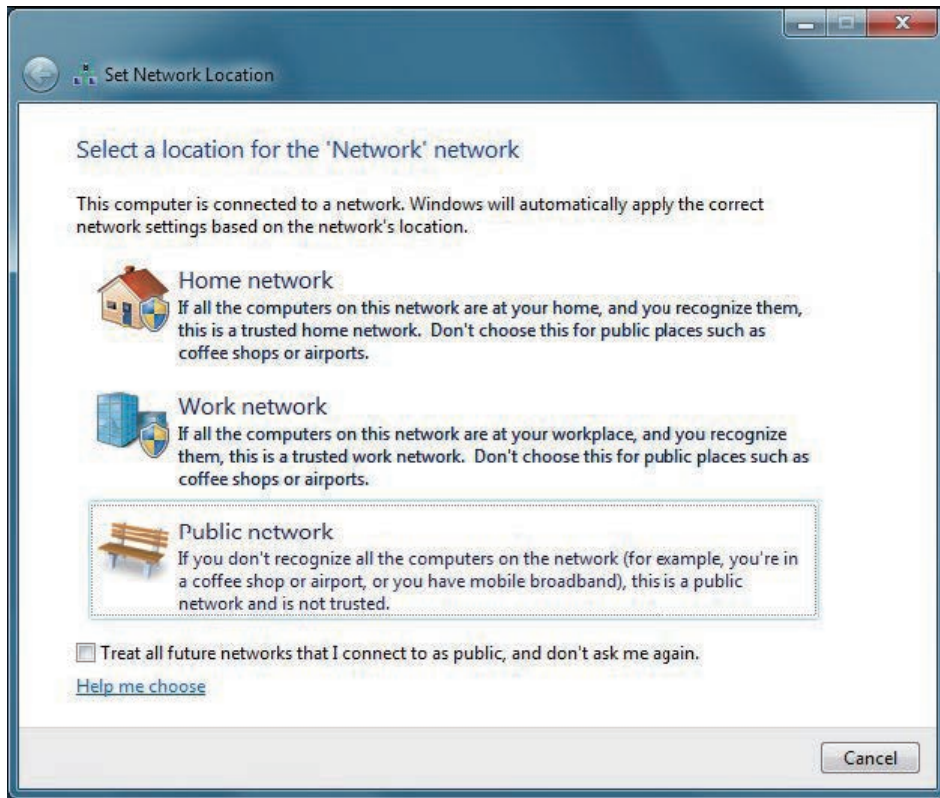


Figure C9.2.1-1 Set Network Location Dialog Box

**TIP** On Windows Vista or Windows Server 2008, select [Public location].

## C9.2.2 Problems Related to Installation and Deletion of Drivers

This section provides troubleshooting related to the installation and deletion of network drivers.



### IMPORTANT

Some operations require administrative rights, and a User Account Control dialog box may appear when you try to do such operations. You can continue the operation by clicking [Continue] as long as you have logged on as a user with administrative rights.

### ■ Confirming Installation Result

Check if the network driver is properly installed. If the driver does not appear on Device Manager, you need to install the driver again.

#### ● Control Bus Driver

When the driver is added, “Yokogawa Vnet Adapter” appears under Network Adapters on Device Manager.

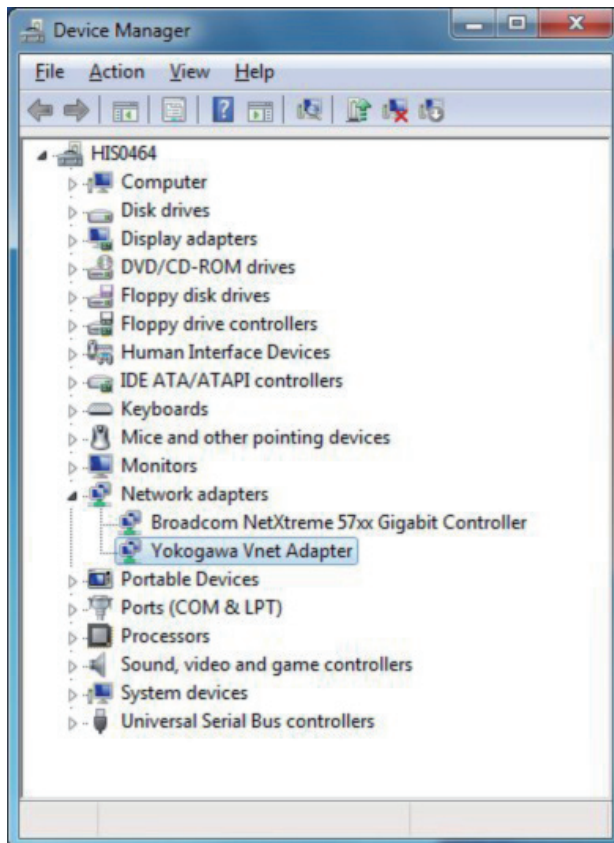
If the driver does not start successfully, the “!” symbol appears next to the network adapter icon.

Follow these steps to display Device Manager:

1. Log on as an administrative user.
2. From the Start menu, select [Control Panel] > [System and Security] > [Device Manager].

#### TIP

If you are using Windows Vista or Windows Server 2008, select [Control Panel] > [System and Maintenance] > [System] > [Device Manager].



**Figure C9.2.2-1 Adapter Driver Added Properly**

You can check whether the protocol driver is installed properly in this way: from the [View] menu of Device Manager, enable [Show hidden devices] to display “Yokogawa Vnet Protocol” driver under Non-Plug and Play Drivers. If the driver is not working properly, the “!” symbol appears next to the Non-Plug and Play Drivers icon.

**TIP**

If the “Yokogawa Vnet Protocol” driver is not displayed immediately after it is installed, perform the following.

- For Windows 7 or Windows Server 2008 R2  
Restart the computer.
- For Windows Vista or Windows Server 2008  
From the [Action] menu, select [Scan for hardware changes].

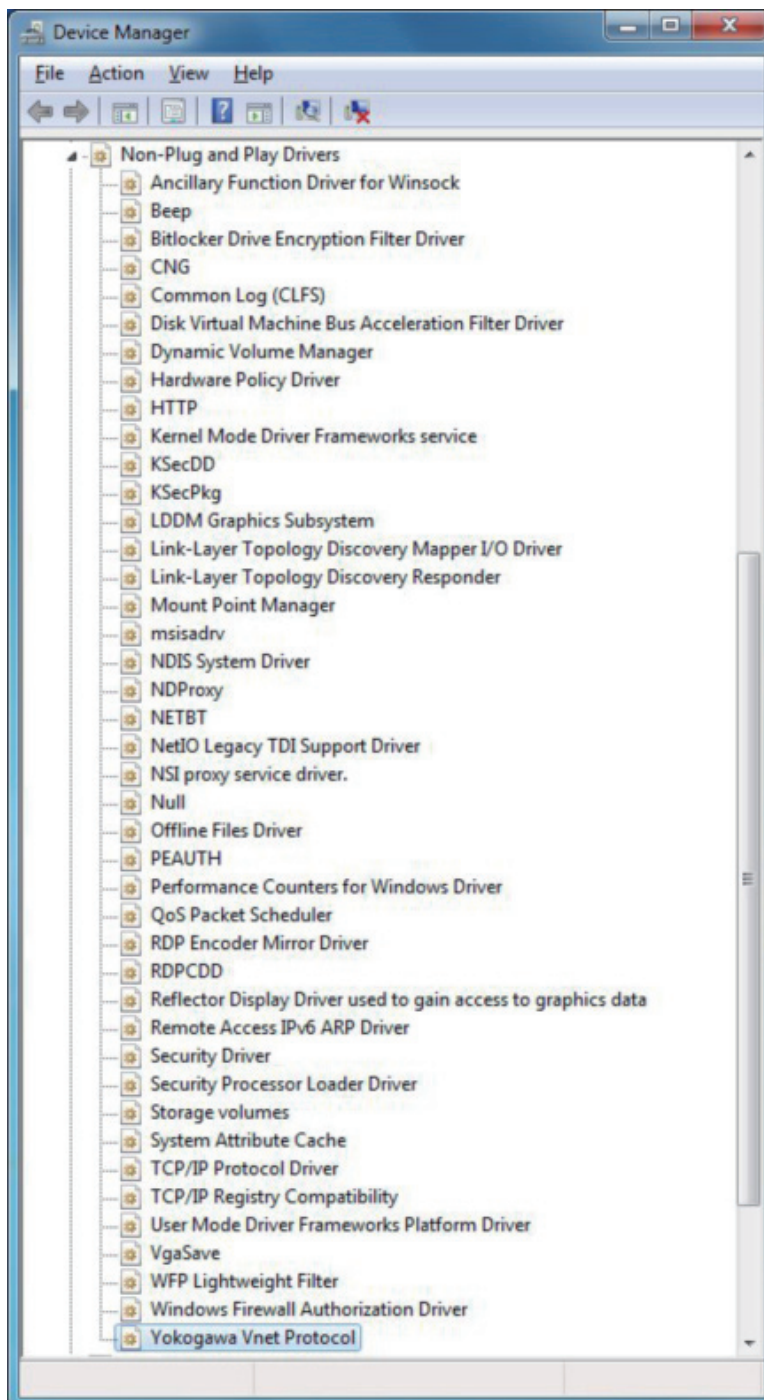


Figure C9.2.2-2 Protocol Driver Added Properly

### ● Vnet/IP Open Communication Driver

When the driver is added, “Vnet/IP Open Communication Driver (BUS2)” appears in Network Adapters in Device Manager.

If the driver does not start successfully, the “!” symbol appears next to the network adapter icon.

Follow these steps to display Device Manager:

1. Log on as an administrative user.
2. From the Start menu, select [Control Panel] > [System and Security] > [Device Manager].

**TIP**

If you are using Windows Vista or Windows Server 2008, select [Control Panel] > [System and Maintenance] > [System] > [Device Manager].

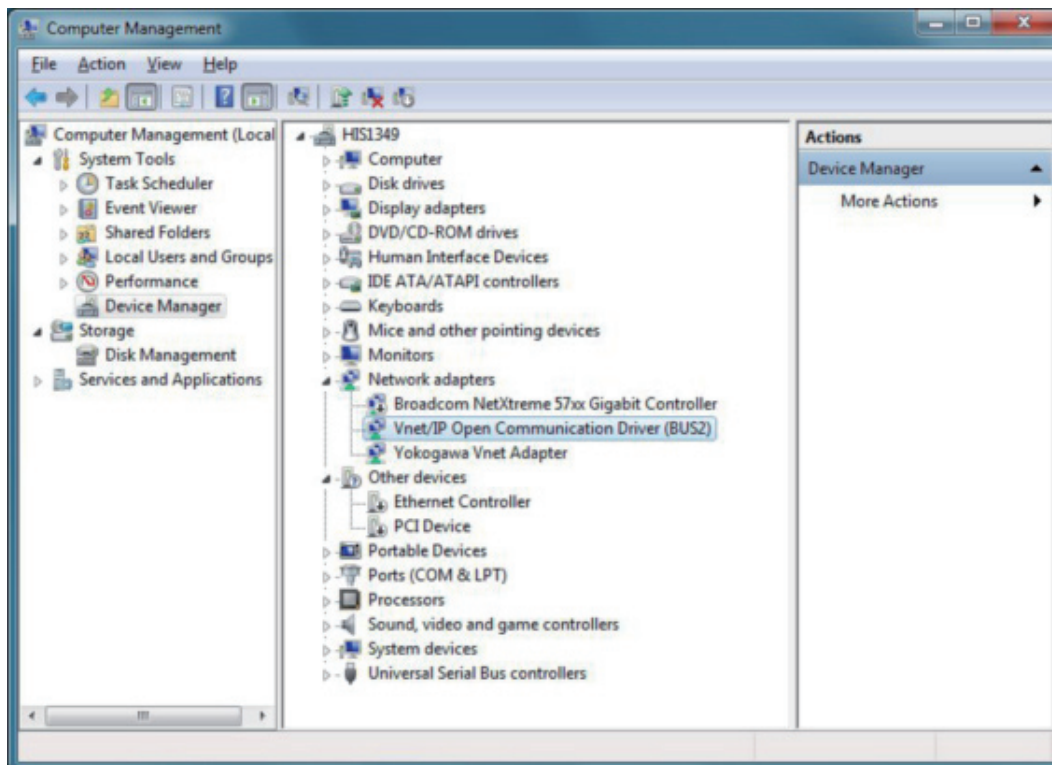


Figure C9.2.2-3 Adapter Driver Added Properly

## ■ Control Bus Driver is Successfully Installed but Does Not Start

The control bus driver may not start normally due to wrong connection of the bus cables or mistakes in address setting. In this case, VLNIC errors are recorded in the System log of Event Viewer.



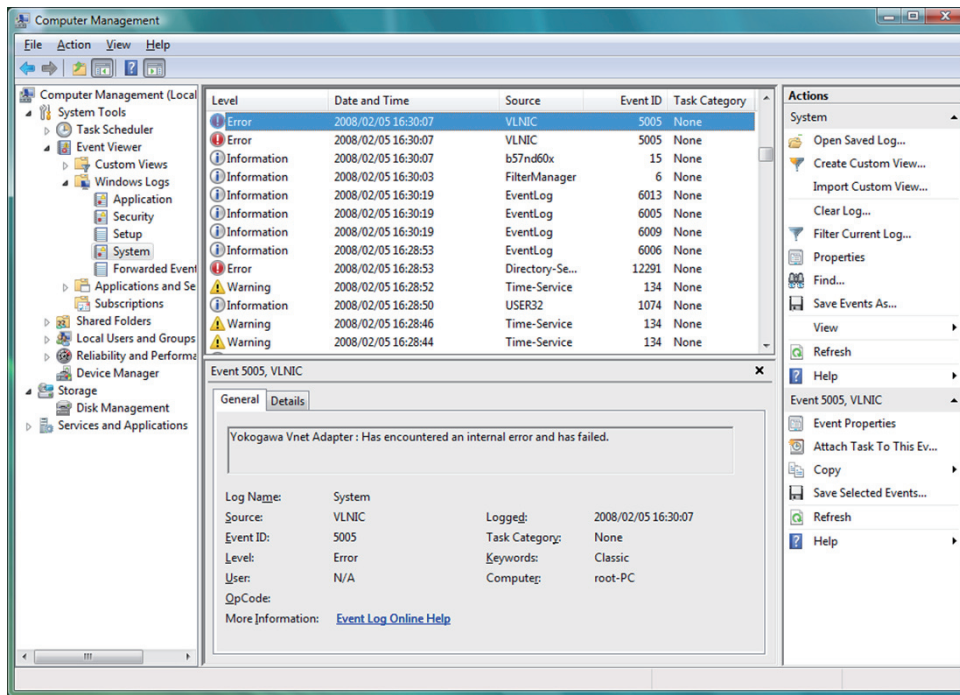


Figure C9.2.2-4 Event Viewer Recording VLNIC Errors (System)

1. Double-click a VLNIC error.  
The Event Properties dialog box appears.

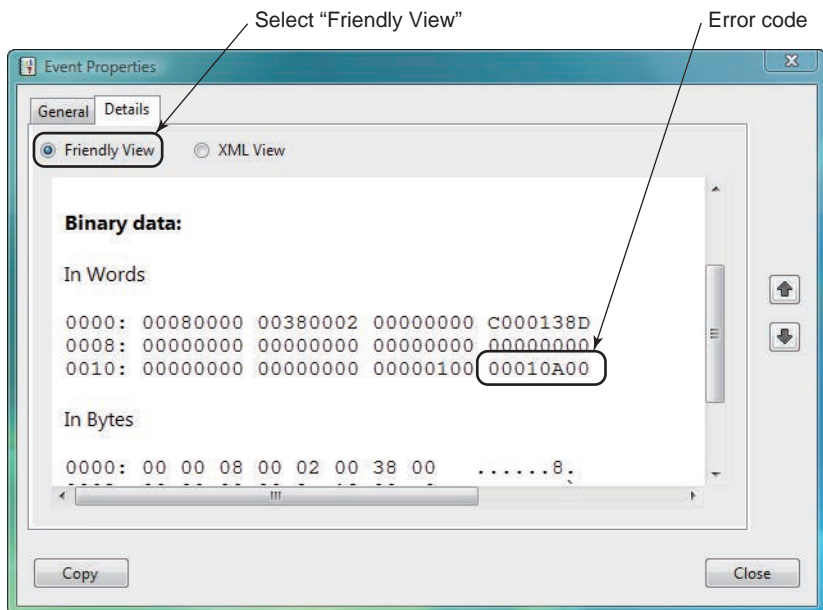


Figure C9.2.2-5 Event Properties

2. Look up the error code in the following table. If the problem is caused by the bus configuration and/or address setting, make sure that the settings are correctly made and shut down the computer. Then start up the computer again.

Table C9.2.2-1 Error Codes Generated when Starting the Driver

Code (*1)	Meaning
000101**	RAM parity error (failure of VF702/VF701/VI702/VI701 card)

Continues on the next page

Table C9.2.2-1 Error Codes Generated when Starting the Driver (Table continued)

Code (*1)	Meaning
000102**	RAM read/write error (failure of VF702/VF701/VI702/VI701 card)
000109**	Address overlap error
00010a**	Bus configuration error (wrong bus connector connection)
00010b**	Dip switch station number parity error
00010c**	Dip switch domain number parity error
00010d**	Inappropriate dip switch station number setting
00020013	Illegal station number (may be detected in the case of bus connector connection mistakes)

\*1: In the code, a 2-digit number 00 is displayed at the position of \*\* for VF702/VF701 while others for VI702/VI701.

If the driver still does not start, other possible causes may be a failure of the control bus interface card or Vnet/IP interface card, or conflicts with other devices.

Replace the control bus interface card or Vnet/IP interface card, or remove the other devices from the computer.

## ■ Duplicate Instances of the Installer

You cannot start two instances of the installer. If you start a second instance, a warning message appears. Click [OK] and terminate the installer you started later.

The processing of the installer started first continues.

## ■ Error Message is Displayed during Network Driver Installation – 1

If an error message is displayed when you click [Don't Install] in the Windows Security dialog box that appears during installation of a network driver, perform the following tasks.

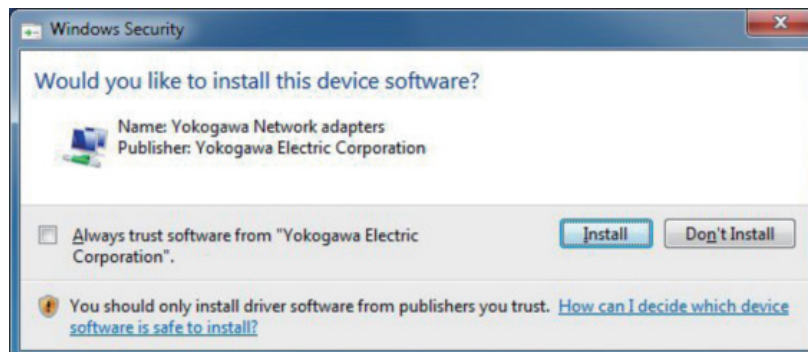


Figure C9.2.2-6 Windows Security Dialog Box (for Network Adapter)

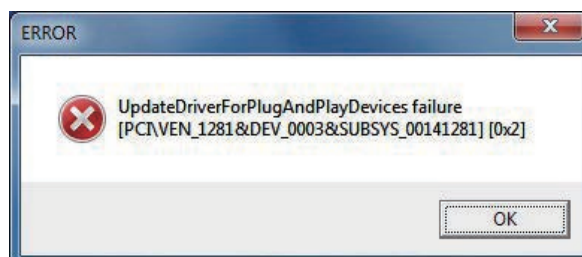


Figure C9.2.2-7 Error Message (for Network Adapter)

- **Control Bus Driver**

1. After restarting the computer, click [Control Bus Driver] on the installation menu.
2. If the control bus driver can be deleted, delete it and then restart the computer.
3. Install the control bus driver again.

- **Vnet/IP Open Communication Driver**

Start the installer again.

## ■ Error Message is Displayed during Network Driver Installation – 2

If an error message is displayed when you did not click [Do not install] in the Windows Security dialog box (for confirming installation of the network protocol or network adapter) that appears during installation of a network driver, perform the following tasks.

- **Control Bus Driver**

1. After restarting the computer, click [Control Bus Driver] on the installation menu.
2. Perform either of the following operations:
  - If the control bus driver can be deleted, delete it and then install the driver again.
  - If the control bus driver cannot be deleted, restart the computer and install the driver again.

- **Vnet/IP Open Communication Driver**

1. Start the installation menu again and click [Vnet/IP Open Communication Driver].
2. Perform either of the following operations:
  - If the driver can be deleted, delete it and restart the computer. Then, install the driver again.
  - If the driver cannot be deleted, restart the computer and install the driver again.

## ■ Error Message is Displayed during Network Driver Installation – 3

Previously functioning Ethernet communications may fail, generating an error message.

- **Cause**

- Hardware, such as the Ethernet adapter card and Ethernet cable, is not connected properly.
- The network binding is not correctly set.
- The TCP/IP communication settings are not correct (IP address, subnet mask, etc.)

- **Remedy**

- Check the hardware, Ethernet adapter card, and the Ethernet cable.
- In Control Panel, check the “Network and Dial-up Connections” settings.

## ■ Restarted the Computer After Deleting the Driver without Removing the Control Bus Interface Card or Vnet/IP Open Interface Card from the Computer

The actions you should take are described for the control bus driver and for the Vnet/IP open communication driver.

### ● Control Bus Driver

If you restart the computer after deleting the control bus driver without removing the control bus interface card from the computer, Windows judges that the control bus interface card is a newly added device and displays the following dialog box.

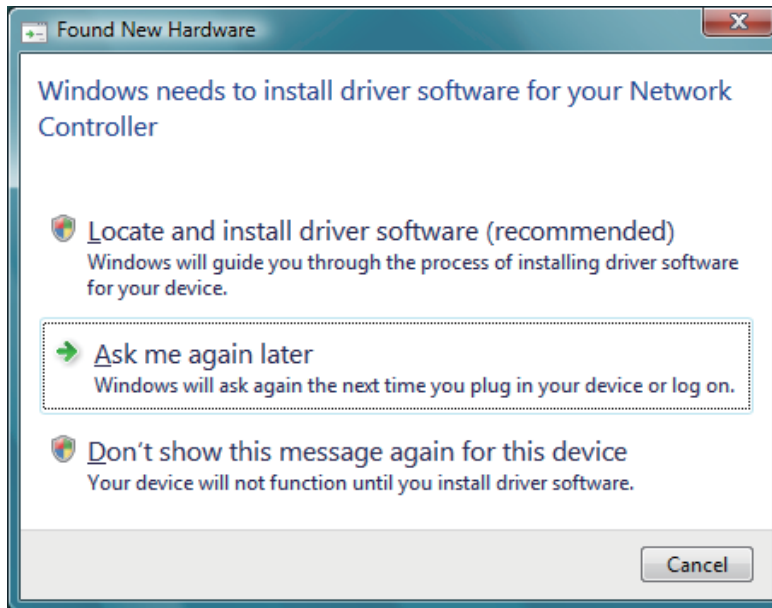


Figure C9.2.2-8 Found New Hardware Dialog Box

Click [Ask me again later] here. Then, if you do not install the control bus driver, shut down the computer and remove the control bus interface card.

### ● Vnet/IP Open Communication Driver

If you restart the computer after deleting the Vnet/IP open communication driver without removing the Vnet/IP interface card from the computer, Windows judges that the Vnet/IP interface card is a newly added device and prompts you to install the driver for it.

In this case, ignore the prompting message and do not install the driver.

---

## D. Connection with Other Products

ProSafe-RS can be connected with YOKOGAWA products, such as CENTUM VP, PRM, and Exaquantum.

When connecting to these products, you may need to change the IT security settings.

This section describes the information and procedures on how to connect various products after installation.

# D1. Connecting YOKOGAWA products

This section describes the settings that are required to connect YOKOGAWA products.

For each connection case, an integration code is assigned. You must perform the tasks that are required for the corresponding integration code of your connection case.



## IMPORTANT

- Ensure that the security model and the user management type of the products that you are connecting are the same.
- If the Strengthened model is applied to the products that you want to connect, contact YOKOGAWA.

## SEE ALSO

For more information about security models, user management types, users and groups, and security settings, refer to:

1., "Overview" in ProSafe-RS Security Guide (IM 32Q01C70-31E)

## ■ Integration code

The format of the integration code is as follows:

(Package code 1) - (Package code 2) - (Integration type) - (Revision number)

The following table describes the elements of an integration code.

Table D1-1 Integration code elements

Element	Description
Package code	The code that is assigned to a software package that can be installed independently on a computer. First package code is the package code of product 1, and Second package code is the package code of product 2.
Integration type	The connection setup of various products. The possible values are: <ul style="list-style-type: none"> <li>• 01: When products are installed and operated on the same computer, and they cannot communicate or share files with each other.</li> <li>• 02: When products are installed and operated on separate computers, and they can communicate or share files with each other.</li> <li>• 03: When products are installed and operated either on the same computer or on separate computers, and they can function together by communicating or sharing files with each other.</li> </ul>
Revision number	The version or revision number of the products that you want to connect. When the required connection procedures change on release of new versions or revisions, this revision number is incremented. The revision number can be from 01 to 99.

## TIP

You cannot install two products that have integration type 02 on the same computer.



## IMPORTANT

In the user's manuals of a product, the settings that are required to connect with other products are explained. However, information about the settings for connection that is provided in the user's manuals may be inconsistent between the connected products. The reason is that different products are released at different timings. To get the latest information, refer to the user's manuals of both products to check the product version number and the revision number of the integration code for their combination, and use the most recent setting procedure.

### ● Package codes

The following table describes the package codes of various YOKOGAWA products.

Table D1-2 Package codes

Package code	Product	Package
0101	CENTUM VP	CENTUM VP Standard Operation and Monitoring Function (*1)
0102	CENTUM VP	System Builder Function
0108	CENTUM VP	Report Package
0153	CENTUM VP	SOE Viewer Package
0196	CENTUM VP	Project Database
0201	ProSafe-RS	Safety System Generation and Maintenance Function Package
0202	ProSafe-RS	SOE OPC Interface Package
0203	ProSafe-RS	CENTUM VP/CS 3000 Integration Engineering Package
0204	ProSafe-RS	FAST/TOOLS Integration Engineering Package
0251	ProSafe-RS	SOE Viewer Package
0301	PRM	Plant Resource Manager Field Communications Server
0302	PRM	Plant Resource Manager Server
0351	PRM	Plant Resource Manager DeviceViewer
0401	Exaopc	Exaopc OPC Interface Package
0801	Exaquantum	PIMS Server
0851	Exaquantum	Explorer Client
1202	STARDOM	STARDOM FCN/FCJ OPC Server

\*1: As an optional function for this package, Exaopc OPC Interface Package (for HIS) is available. Consolidated Alarm Management Function (CAMS for HIS) is included in Standard Operation and Monitoring Function.

---

## **D1.1 CENTUM VP and ProSafe-RS**

This section describes the settings when connecting CENTUM VP and ProSafe-RS.



## D1.1.1 CENTUM VP Standard Operation and Monitoring Function and ProSafe-RS Safety System Generation and Maintenance Function Package

Connecting CENTUM VP Standard Operation and Monitoring Function and ProSafe-RS Safety System Generation and Maintenance Function Package or SOE Viewer Package enables historical information of CENTUM VP HIS to be viewed on ProSafe-RS SOE Viewer.

### ■ Viewing Historical Information of CENTUM VP on ProSafe-RS SOE Viewer

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

#### TIP

You can also use the same procedures to view the SOE event messages of ProSafe-RS on the CENTUM SOE Viewer.

**Table D1.1.1-1 Connection information**

Integration code	0101-0201-03-02 0101-0251-03-02 0153-0201-03-02		
Product 1	Standard Operation and Monitoring Function of CENTUM VP R5.03 SOE Viewer Package of CENTUM VP R5.03		
Product 2	Safety System Generation and Maintenance Function Package of ProSafe-RS R3.01 or later SOE Viewer Package of ProSafe-RS R3.01 or later		
Security model	Legacy model	Standard model	
User management type	-	Standalone management	Domain/Combination management
Required procedures	None	Refer to "● When the Standard model is applied."	

#### ● When the Standard model is applied

Add the user account for using ProSafe-RS SOE Viewer to the CTM\_OPERATOR and PSF\_OPERATOR groups.

For Standalone management, perform this setting on the computer where ProSafe-RS SOE Viewer is used. For Domain or Combination management, perform this setting on the domain controller.

#### SEE ALSO

For more information about how to create user accounts and add them to groups in Domain or Combination management, refer to:

[B2.4, "Creating Domain Users" on page B2-9](#)

For more information about how to create user accounts and add them to groups in Standalone management, refer to:

[B3.7.1, "When the Standard Model with Standalone Management Security Settings are Applied" on page B3-69](#)

## D1.1.2 CENTUM VP Standard Operation and Monitoring Function and ProSafe-RS SOE OPC Interface Package

This section explains the required settings when Exaopc OPC Interface Package (for HIS) (LHS2411) of CENTUM VP and SOE OPC Interface Package (CHS2200) of ProSafe-RS are installed on the same computer.

If the computer installed with both LHS2411 and CHS2200 comes under either of the following cases, perform all the procedures explained for each case.

- The computer installed with LHS2411 and CHS2200 is designated as the OPC server for OPC communication.
- The computer installed with LHS2411 and CHS2200 uses OPC client services.
- In a Domain management or Combination management system, the computer installed with LHS2411 and CHS2200 is designated as the OPC server on an OPC client computer that is not a member of the domain.

### ■ When the computer installed with LHS2411 and CHS2200 is designated as the OPC server to communicate with

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

**Table D1.1.2-1 Connection information**

Integration code	0101-0202-01-01		
Product 1	Standard Operation and Monitoring Function of CENTUM VP R5.03		
Product 2	SOE OPC Interface Package of ProSafe-RS R3.01 or later		
Security model	Legacy model	Standard model	
User management type	-	Standalone management	Domain/Combination management
Required procedures	None	Refer to "● When the Standard model is applied."	

#### ● When the Standard model is applied

On the OPC server computer, add the user account for using OPC client services on OPC client computers to the CTM\_OPC and PSF\_OPC groups.

For Domain or Combination management, perform this setting on the domain controller. For Standalone management, create on the OPC server computer a user account with the same name as the local user who uses OPC client services on the OPC client computer and then add the user account to the CTM\_OPC and PSF\_OPC groups.

#### SEE ALSO

For more information about how to create user accounts and add them to groups in Domain or Combination management, refer to:

[B2.4, "Creating Domain Users" on page B2-9](#)

For more information about how to create user accounts and add them to groups in Standalone management, refer to:

[B3.7.1, "When the Standard Model with Standalone Management Security Settings are Applied" on page B3-69](#)

#### ● Users who use OPC client services

The following table shows the users who use OPC client services:

Table D1.1.2-2 Users who use OPC client services

OPC client service	User
Report Package (LHS6530)	User who logged on to Windows
Access Administrator Package (FDA:21 CFR Part 11 compliant) (LHS5170)	User who logged on to Windows
OPC client other than CENTUM VP product (*1)	Users who use OPC client services

\*1: Functions created using CENTUM Data Access Library (LHS2412) are also included.

## ■ When the computer installed with LHS2411 and CHS2200 uses OPC client services

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

Table D1.1.2-3 Connection information

Integration code	0101-0202-01-01		
Product 1	Standard Operation and Monitoring Function of CENTUM VP R5.03		
Product 2	SOE OPC Interface Package of ProSafe-RS R3.01 or later		
Security model	Legacy model	Standard model	
User management type	-	Standalone management	Domain/Combination management
Required procedures	None	Refer to "● When the Standard model is applied."	

### ● When the Standard model is applied

Add the user account for using OPC client services to the CTM\_OPC and PSF\_OPC groups.

For Standalone management, perform this setting on OPC client computers. For Domain or Combination management, perform this setting on the domain controller.

#### SEE ALSO

For more information about how to create user accounts and add them to groups in Domain or Combination management, refer to:

[B2.4, "Creating Domain Users" on page B2-9](#)

For more information about how to create user accounts and add them to groups in Standalone management, refer to:

[B3.7.1, "When the Standard Model with Standalone Management Security Settings are Applied" on page B3-69](#)

### ● Users who use OPC client services

The following table shows the users who use OPC client services:

Table D1.1.2-4 Users who use OPC client services

OPC client service	User
Report Package (LHS6530)	User who logged on to Windows
Access Administrator Package (FDA:21 CFR Part 11 compliant) (LHS5170)	User who logged on to Windows
FCS Data Setting/Acquisition Package (PICOT) (LHS6710)	User who logged on to Windows

Continues on the next page

Table D1.1.2-4 Users who use OPC client services (Table continued)

OPC client service	User
Consolidated Alarm Management Function (CAMS for HIS)	User that was specified when setting up the OPC A&E server connection
OPC client other than CENTUM VP product (*1)	Users Who Use OPC Client Service

\*1: Functions created using CENTUM Data Access Library (LHS2412) are also included.

### ● When FCS Data Setting/Acquisition Package (PICOT) is used

If FCS Data Setting/Acquisition Package (PICOT) (LHS6710) and HIS type single sign on are used, also perform the following setting:

For Standalone management: On the computer running the package, add OFFUSER to the PSF\_OPC group.

For Domain or Combination management: On the computer running the package, add OFFUSER to the PSF\_OPC\_LCL group.

### ■ When the computer installed with LHS2411 and CHS2200 is designated as the OPC server to communicate with on the OPC client computer that is not a member of the domain

The following table shows the connection information for the case where Domain or Combination management is applied and the computer installed with LHS2411 and CHS2200 is designated as the OPC server on the OPC client computer that is not a member of the domain. For required procedures for connection, read the descriptions that follow the table.

Table D1.1.2-5 Connection information

Integration code	0101-0202-03-02
Product 1	Standard Operation and Monitoring Function of CENTUM VP R5.03
Product 2	SOE OPC Interface Package of ProSafe-RS R3.01 or later
Security model	Standard model
User management type	Domain/Combination management
Required procedures	Refer to "● Required procedures for connection."

### ● Required procedures for connection

On the OPC server computer, create a user account with the same name as the local user who performs OPC communication on the OPC client computer, and then add the user account to the CTM\_OPC\_LCL and PSF\_OPC\_LCL groups.

#### SEE ALSO

For more information about how to create user accounts and add them to groups in Standalone management, refer to:

[B3.7.1, "When the Standard Model with Standalone Management Security Settings are Applied" on page B3-69](#)

For more information about how to create user accounts and add them to groups in Domain or Combination management, refer to:

[B2.4, "Creating Domain Users" on page B2-9](#)

### ● Local Users Who Use OPC Client Service

The following table shows the local users who use OPC client services:

Table D1.1.2-6 Local Users Who Use OPC Client Service

OPC client service	User
Report Package (LHS6530)	User who logged on to Windows
OPC client other than CENTUM VP product (*1)	Users Who Use OPC Client Service

\*1: Functions created using CENTUM Data Access Library (LHS2412) are also included.

## D1.1.3 CENTUM VP System Builder Function and ProSafe-RS CENTUM VP/CS 3000 Integration Engineering Package

By using ProSafe-RS CENTUM VP/CS 3000 Integration Engineering Package, you can build an integrated system of CENTUM VP and ProSafe-RS.

### ■ Building a system by integrating CENTUM VP and ProSafe-RS

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

**Table D1.1.3-1 Connection information**

Integration code	0102-0203-03-02 0196-0203-03-02		
Product 1	System Builder Function of CENTUM VP R5.03 Project Database of CENTUM VP R5.03		
Product 2	CENTUM VP/CS 3000 Integration Engineering Package of ProSafe-RS R3.01 or later		
Security model	Legacy model	Standard model	
User management type	-	Standalone management	Domain/Combination management
Required procedures	None	Refer to "● When the Standard model is applied."	

#### ● When the Standard model is applied

- When CENTUM VP project is placed on a computer where SCS Manager is used:  
Add the user account for using SCS Manager of ProSafe-RS to the CTM\_ENGINEER and PSF\_ENGINEER groups.  
For Standalone management, perform this setting on the computer where SCS Manager is used. For Domain or Combination management, perform this setting on the domain controller.
- When CENTUM VP project is placed on a computer where SCS Manager is not used:  
For Standalone management, create a user account with the same name as the user who uses SCS Manager on the computer where the CENTUM VP project is placed and then add the user account to the CTM\_ENGINEER group.  
For Domain or Combination management, add the user account for using SCS Manager to the CTM\_ENGINEER group on the domain controller.

#### SEE ALSO

For more information about how to create user accounts and add them to groups in Domain or Combination management, refer to:

[B2.4, "Creating Domain Users" on page B2-9](#)

For more information about how to create user accounts and add them to groups in Standalone management, refer to:

[B3.7.1, "When the Standard Model with Standalone Management Security Settings are Applied" on page B3-69](#)

## D1.1.4 CENTUM VP System Builder Function and ProSafe-RS Safety System Generation and Maintenance Function Package

By connecting CENTUM VP System Builder Function and ProSafe-RS Safety System Generation and Maintenance Function Package, you can perform simulation tests of SCS using SCS simulator of ProSafe-RS.

### ■ Enabling SCS simulation tests using SCS simulator

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

**Table D1.1.4-1 Connection information**

Integration code	0102-0201-03-02		
Product 1	System Builder Function of CENTUM VP R5.03		
Product 2	Safety System Generation and Maintenance Function Package of ProSafe-RS R3.01 or later		
Security model	Legacy model	Standard model	
User management type	-	Standalone management	Domain/Combination management
Required procedures	None	Refer to "● When the Standard model is applied."	

#### ● When the Standard model is applied

Add all the user accounts for using SCS Manager of ProSafe-RS or System View of CENTUM VP to the CTM\_ENGINEER and PSF\_ENGINEER groups.

For Standalone management, perform this setting on the computer where SCS Manager of ProSafe-RS and System View are used. For Domain or Combination management, perform this setting on the domain controller.

#### SEE ALSO

For more information about how to create user accounts and add them to groups in Domain or Combination management, refer to:

[B2.4, "Creating Domain Users" on page B2-9](#)

For more information about how to create user accounts and add them to groups in Standalone management, refer to:

[B3.7.1, "When the Standard Model with Standalone Management Security Settings are Applied" on page B3-69](#)

## D1.1.5 Required Settings when Integrating with CENTUM VP R4.01 to R4.03

The same settings are required as those for integrating with CENTUM VP 5.01 or later. However, the security configuration must be done separately: use the Security Setting Utility for CENTUM VP and the IT Security Tool for ProSafe-RS. If ProSafe-RS is installed on the same computer where CENTUM VP is installed, use the Security Setting Utility first and then use the IT Security Tool of ProSafe-RS to configure security settings. Next, change the authentication level of COM from "Connect" to "None." Then, make the following settings on ProSafe-RS and CENTUM.

**SEE  
ALSO**

For more information about how to change the authentication level of COM, refer to:

“● DCOM setting procedure” in “■ Settings for the legacy model” in A3.2, “Settings of the OPC client” in Open Interfaces (IM 32Q05B10-31E)

### ■ Settings on ProSafe-RS

Make the same settings as when integrating ProSafe-RS with CENTUM VP 5.01.

### ■ Settings on CENTUM

Make the same settings as when integrating ProSafe-RS with CENTUM VP 5.01.

### ■ Settings on a File Server

If you place project data and operation history management databases of ProSafe-RS on a file server computer storing CENTUM VP project data, set the share name for the ProSafe-RS database folder on the file server computer, and then run the IT Security Tool of ProSafe-RS.

### ■ Coexisting with Exaopc OPC Interface Package (for HIS)

When CENTUM VP and ProSafe-RS are operating in a domain environment, set as follows:

- Add the CTM\_PROCESS user to the PSF\_OPC\_LCL group.
- If the security model is the Standard model, add the PSF\_PROCESS user to the CTM\_OPC\_LCL group. If the security model is the Legacy model, add the EXAUSER user to the CTM\_OPC\_LCL group.

When CENTUM VP and ProSafe-RS are operating in a workgroup environment, set as follows:

- Add the CTM\_PROCESS user to the PSF\_OPC group.
- If the security model is the Standard model, add the PSF\_PROCESS user to the CTM\_OPC group. If the security model is the Legacy model, add the EXAUSER user to the CTM\_OPC group.

**SEE  
ALSO**

For more information about the share name of the ProSafe-RS database folder, refer to:

“■ Procedure 2: Create and Set Up the Shared Folders” on page B5-3



---

## **D1.1.6 Required Settings when Integrating with CS 3000 R3.06 to R3.09**

If you integrate ProSafe-RS with CS 3000, computer security cannot be reinforced. You cannot install both CENTUM and ProSafe-RS on the same computer either. Make the following settings.

- Select the Legacy model when you run the IT Security Tool.
- Create a CENTUM user account (account name: CENTUM) on ProSafe-RS and set the same password as the CENTUM account on the CENTUM side.

---

## D1.2 ProSafe-RS and PRM

This section describes the settings when connecting ProSafe-RS and PRM.

**TIP**

PRM client and ProSafe-RS software can be installed on the same computer; however, special setting is not required because they do not work in collaboration.

---

## D1.2.1 SOE OPC Interface Package and PRM Server

Connecting ProSafe-RS and the PRM Server enables PRM to retrieve messages from ProSafe-RS. To perform OPC communication with PRM, the SOE OPC Interface Package (CHS2200) is required. No setting is required on the PRM Server.

### TIP

PRM server and ProSafe-RS cannot be installed on the same computer.

## ■ Enabling PRM to retrieve messages from ProSafe-RS

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

**Table D1.2.1-1 Connection information**

Integration code	0202-0302-02-02		
Product 1	SOE OPC Interface Package of ProSafe-RS R3.01 or later		
Product 2	Plant Resource Manager Server of PRM R3.10 or later		
Security model	Legacy model	Standard model	
User management type	-	Standalone management	Domain/Combination management
Required procedures	Refer to "● When the Legacy model is applied."	Refer to "● Setting the logon type with Standard model", "● Granting remote access permission with Standard model", "● Creating PRM-related internal user accounts with Standard model".	

### ● When the Legacy model is applied

1. Log on by using a user account with administrative rights.
2. From the Start menu, select [All Programs] > [YOKOGAWA ProSafe] > [SOE OPC Parameter Setting].  
The SOE OPC Interface Settings dialog box appears.
3. In the OPC Security Settings section, click [Edit].  
The Select Logon Type dialog box appears.
4. Select [Automatically logon the designated user for connecting OPC server.] and select [Default user of R2.03 and earlier versions], and then click [OK].

### ● Setting the logon type with Standard model

1. Log on to the SENG as a member of the PSF\_ENGINEER or PSF\_ENGINEER\_LCL group.
2. From the Start menu, select [All Programs] > [YOKOGAWA ProSafe] > [SOE OPC Parameter Setting].  
The SOE OPC Interface Settings dialog box appears.
3. In the OPC Security Settings section, click [Edit].  
The Select Logon Type dialog box appears.
4. Select [Automatically logon the designated user for connecting OPC server.] and select [Default user of R2.03 and earlier versions], and then click [OK].

### ● Granting remote access permission with Standard model

1. Log on to the SENG as a user with administrative rights.
2. In the search box displayed at the bottom of the Start menu, enter "dcomcnfg.exe" and hit the [Enter] key.

**TIP**

If a User Account Control dialog box appears, click [Yes].  
On Windows Vista or Windows Server 2008, click [Continue].

The component service window appears.

3. Double-click the [Computer] icon; then right-click the [My Computer] icon that appears, and select [Properties].
4. In the Properties dialog box of My Computer, click the COM Security tab, and then click [Edit Limits] in the Access Permission section.
5. Grant the remote access permission to ANONYMOUS LOGON, and click [OK].

- **Creating PRM-related internal user accounts with Standard model**

1. Log on to the SENG as a user with administrative rights.
2. To run the PRM internal account creation tool, double-click the following file in the PRM software medium:  
(DVD drive):\PRM\SecuritySettingUtility\CreateInternalUserAccount.exe  
Two user accounts, PRM\_PROCESS and PRM\_PROCESS2, are created.
3. Confirm that the created users are members of the following user group:  
PSF\_OPC when Standalone management is applied.  
PSF\_OPC\_LCL when Domain management is applied.  
PSF\_OPC or PSF\_OPC\_LCL when Combination management is applied.

## ■ Collaborating with a PRM Server of R3.03 to R3.05

To enable collaboration with a PRM server when the security model is the Standard model, perform the same procedures as those for connection with PRM R3.10 or later.

## ■ Collaborating with a PRM Server of R3.02

To enable collaboration with a PRM server when the security model is the Standard model, perform the following procedure. Then, set the logon type and grant remote access permission by using the same procedures as those for connection with PRM R3.10 or later.

- **Procedure For Standalone Management**

1. On the SENG running the SOE OPC Interface package, create the program user of PRM. The user name and password should be as follows.  
User name: PRMUSER  
Password: PRMUSER
2. Add the program user you have created to the PSF\_OPC group.

- **Procedure For Domain Management or Combination Management**

1. On the SENG running the SOE OPC Interface package, create the program user of PRM. The user name and password should be as follows.  
User name: PRMUSER  
Password: PRMUSER
2. Add the program user you have created to the PSF\_OPC\_LCL group.

---

## D1.3 ProSafe-RS and Exaquantum

This section describes the settings when connecting ProSafe-RS and Exaquantum.

## D1.3.1 ProSafe-RS SOE OPC Interface Package and Exaquantum PIMS Server

Connecting the CHS2200 SOE OPC Interface Package and Exaquantum PIMS Server enables the Exaquantum PIMS Server to collect SOE data from SCS through the OPC interface.

### ■ Enabling Exaquantum to collect SOE data from SCS

To use Exaquantum PIMS Server as an OPC client and perform OPC communication with an SENG running the SOE OPC Interface Package, you need to perform the settings described below.

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table. The logon type setting on the SENG and the setting to use Exaquantum as an OPC client are mandatory in all cases.



### IMPORTANT

As a basic rule, the security model and user management type must be consistent in the products to be connected. However, ProSafe-RS and Exaquantum can be connected even if different security model or user management type is applied.

**Table D1.3.1-1 Connection information: ProSafe-RS SOE OPC Interface Package and Exaquantum R2.60 or later**

Integration code	0202-0801-02-01		
Product 1	SOE OPC Interface Package of ProSafe-RS R3.01 or later		
Product 2	PIMS server of Exaquantum R2.60 or later		
Security model	Legacy model	Standard model	
User management type	-	Standalone management	Domain/Combination management
Required procedures	Refer to "● Setting the logon type" and "● When the Legacy model is applied to both products."	Refer to "● Setting the logon type" and "● When the Standard model is applied to both products."	

**Table D1.3.1-2 Connection information: Different security model - Case 1**

Integration code	0202-0801-02-01	
Product 1	SOE OPC Interface Package of ProSafe-RS R3.01 or later	
Product 2	PIMS server of Exaquantum R2.60 or later	
Security model	Standard model (ProSafe-RS) Legacy model (Exaquantum)	
User management type of Pro-Safe-RS	Standalone management	Domain/Combination management
Required procedures	Refer to "● Setting the logon type" and "● When the Standard model is applied to Pro-Safe-RS and the Legacy model to Exaquantum."	

**Table D1.3.1-3 Connection information: Different security model - Case 2**

Integration code	0202-0801-02-01		
Product 1	SOE OPC Interface Package of ProSafe-RS R3.01 or later		

Continues on the next page

**Table D1.3.1-3 Connection information: Different security model - Case 2** (Table continued)

Product 2	PIMS server of Exaquantum R2.60 or later	
Security model	Legacy model (ProSafe-RS) Standard model (Exaquantum)	
User management type of Exaquantum	Standalone management	Domain/Combination management
Required procedures	Refer to "● Setting the logon type" and "● When the Legacy model is applied to ProSafe-RS and the Standard model to Exaquantum."	

**Table D1.3.1-4 Connection information: Legacy model applied ProSafe-RS and Exaquantum version earlier than R2.60**

Integration code	0202-0801-02-02	
Product 1	SOE OPC Interface Package of ProSafe-RS R3.01 or later	
Product 2	PIMS server of Exaquantum R2.20 or later but earlier than R2.60	
Security model	Legacy model (ProSafe-RS) - (Exaquantum)	
User management type	-	
Required procedures	Refer to "● Setting the logon type" and "● When the Legacy model is applied to both products."	

**Table D1.3.1-5 Connection information: Standard model applied ProSafe-RS and Exaquantum version earlier than R2.60**

Integration code	0202-0801-02-02	
Product 1	SOE OPC Interface Package of ProSafe-RS R3.01 or later	
Product 2	PIMS server of Exaquantum R2.20 or later but earlier than R2.60	
Security model	Standard model (ProSafe-RS) - (Exaquantum)	
User management type of ProSafe-RS	Standalone management	Domain/Combination management
Required procedures	Refer to "● Setting the logon type" and "● When the Standard model is applied to ProSafe-RS and the Legacy model to Exaquantum."	

**SEE  
ALSO**

For more information about the details on setting up an OPC client, refer to:

[A3., "Setup for using the OPC client" in Open Interfaces \(IM 32Q05B10-31E\)](#)

## ● Setting the Logon Type

To connect Exaquantum with an SENG (OPC server) running the SOE OPC interface package of ProSafe-RS R3.01.00 or later, you need to set the logon type on the SENG beforehand. After performing this setting, perform the required setting on Exaquantum.

1. Log in to the system as a user belonging to PSF\_ENGINEER or PSF\_ENGINEER\_LCL.
2. From the Start menu, select [All Programs] > [YOKOGAWA ProSafe] > [SOE OPC Parameter Setting].  
The SOE OPC Interface Settings dialog box appears.
3. Click the [Edit] in [OPC Security Settings].  
A dialog box where you can select a type of logon to the OPC server appears.

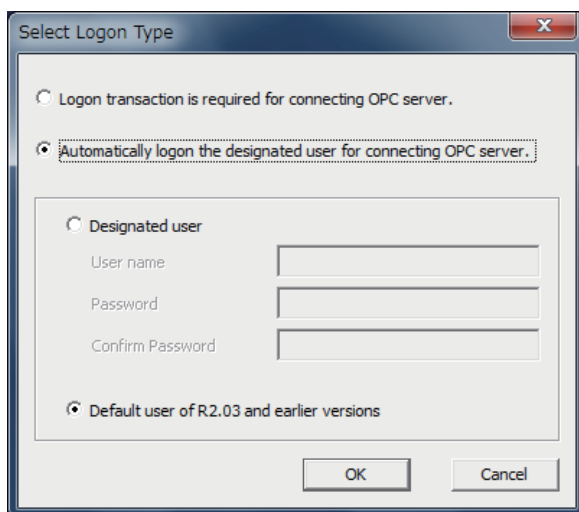


Figure D1.3.1-1 Select Logon Dialog Box

4. Select [Automatically logon the designated user for connecting OPC server.] and then [Default user of R2.03 and earlier versions], and click [OK].

- **When the Legacy model is applied to both products**

1. Set the logon type on the SENG.
2. Add an Exaquantum program user on the SENG.

**TIP**

The name and the password of the Exaquantum program user should be as follows:

User name: Quantumuser (default user name, changeable with a supplied tool)

Password: quantumuser (default password, changeable with a supplied tool)

3. On the SENG, create the same user account as the logon user account for running Exaquantum.
4. On the SENG and the computer installed with Exaquantum, perform the setting for using Exaquantum as an OPC client.

- **When the Standard model is applied to both products**

1. Set the logon type on the SENG.
2. Configure the DCOM settings on the SENG. Refer to the user's manual "Open Interfaces" for the procedure.
3. On the SENG, create QTM\_PROCESS, which is the Exaquantum program user account.
  - a. Insert the Exaquantum software medium and start the command prompt window, then move to the following folder.  
(Drive):\Tools
  - b. Run the following command.  
`CreateQTMProcess.exe`  
The QTM\_PROCESS user account is created.
4. Add the QTM\_PROCESS user you have created to the following user group on the SENG.
  - In the case of standalone management or when combination management is applied on some computers: PSF\_OPC
  - In the case of domain management or when combination management is applied on all computers: PSF\_OPC\_LCL



5. On the SENG, create the same user account as the logon user account for running Exaquantum and add the created user account to the PSF\_OPC group.
6. On the computer installed with Exaquantum, create the PSF\_PROCESS user account.
  - a. Insert the ProSafe-RS software medium and start the command prompt window, then move to the following folder.  
(Drive):\\ProSafe-RS\\SECURITY
  - b. Run the following command.  
`ProSafe.Security.CreateProSafeProcess.exe`  
The PSF\_PROCESS user account is created.
7. Add the PSF\_PROCESS user you have created to the following user group on the computer installed with Exaquantum.
  - In the case of standalone management or when combination management is applied on some computers: QTM\_OPC
  - In the case of domain management or when combination management is applied on all computers: QTM\_OPC\_LCL
8. On the SENG and the computer installed with Exaquantum, perform the setting for using Exaquantum as an OPC client.

**SEE  
ALSO**

For more information about configuring the DCOM settings, refer to:

■ [DCOM settings](#) in A2.2, [“Overview of product security settings” in Open Interfaces \(IM 32Q05B10-31E\)](#)

### ● **When the Standard model is applied to ProSafe-RS and the Legacy model to Exaquantum**

1. Set the logon type on the SENG.
2. Configure the DCOM settings on the SENG. Refer to the user's manual "Open Interfaces" for the procedure.
3. Add an Exaquantum program user on the SENG.

**TIP**

The name and the password of the Exaquantum program user should be as follows:

User name: Quantumuser (default user name, changeable with a supplied tool)

Password: quantumuser (default password, changeable with a supplied tool)

4. Add the Quantumuser user you have created to the following user group on the SENG.
  - In the case of standalone management or when combination management is applied on some computers: PSF\_OPC
  - In the case of domain management or when combination management is applied on all computers: PSF\_OPC\_LCL
5. On the SENG, create the same user account as the logon user account for running Exaquantum and add the created user account to the PSF\_OPC group.
6. On the computer installed with Exaquantum, create the PSF\_PROCESS user account.
  - a. Insert the ProSafe-RS software medium and start the command prompt window, then move to the following folder.  
(Drive):\\ProSafe-RS\\SECURITY
  - b. Run the following command.  
`ProSafe.Security.CreateProSafeProcess.exe`  
The PSF\_PROCESS user account is created.

7. On the SENG and the computer installed with Exaquantum, perform the setting for using Exaquantum as an OPC client.

**SEE  
ALSO**

For more information about configuring the DCOM settings, refer to:

“■ DCOM settings” in A2.2, “Overview of product security settings” in Open Interfaces (IM 32Q05B10-31E)

- **When the Legacy model is applied to ProSafe-RS and the Standard model to Exaquantum**

1. Set the logon type on the SENG.
2. On the SENG, create QTM\_PROCESS, which is the Exaquantum program user account.
  - a. Insert the Exaquantum software medium and start the command prompt window, then move to the following folder.  
(Drive):\Tools
  - b. Run the following command.  
`CreateQTMProcess.exe`  
The QTM\_PROCESS user account is created.
3. On the SENG, create the same user account as the logon user account for running Exaquantum.
4. On the computer installed with Exaquantum, create the EXAUSER user account. The password should also be EXAUSER.
5. Add the EXAUSER user you have created to the following user group on the computer installed with Exaquantum.
  - In the case of standalone management or when combination management is applied on some computers: QTM\_OPC
  - In the case of domain management or when combination management is applied on all computers: QTM\_OPC\_LCL
6. On the SENG and the computer installed with Exaquantum, perform the setting for using Exaquantum as an OPC client.

# Appendix 1. Setting Switches

You can set the domain number and station number by configuring the setting switches on the printed circuit board of the control bus interface card and Vnet/IP interface card.

## ■ Domain Numbers and DIP Switch Positions

The following table lists the domain numbers and corresponding setting switch positions for the control bus interface card and Vnet/IP interface card. Set the DIP switches as shown in the table to adjust to the required domain number.

Table Appendix 1-1 Domain Numbers and DIP Switch Positions

Domain number	DIP switch bit number							
	1	2	3	4	5	6	7	8
1	0	0	0	0	0	0	0	1
2	0	0	0	0	0	0	1	0
3	1	0	0	0	0	0	1	1
4	0	0	0	0	0	1	0	0
5	1	0	0	0	0	1	0	1
6	1	0	0	0	0	1	1	0
7	0	0	0	0	0	1	1	1
8	0	0	0	0	1	0	0	0
9	1	0	0	0	1	0	0	1
10	1	0	0	0	1	0	1	0
11	0	0	0	0	1	0	1	1
12	1	0	0	0	1	1	0	0
13	0	0	0	0	1	1	0	1
14	0	0	0	0	1	1	1	0
15	1	0	0	0	1	1	1	1
16	0	0	0	1	0	0	0	0
17	1	0	0	1	0	0	0	1
18	1	0	0	1	0	0	1	0
19	0	0	0	1	0	0	1	1
20	1	0	0	1	0	1	0	0
21	0	0	0	1	0	1	0	1
22	0	0	0	1	0	1	1	0
23	1	0	0	1	0	1	1	1
24	1	0	0	1	1	0	0	0
25	0	0	0	1	1	0	0	1
26	0	0	0	1	1	0	1	0
27	1	0	0	1	1	0	1	1
28	0	0	0	1	1	1	0	0
29	1	0	0	1	1	1	0	1
30	1	0	0	1	1	1	1	0
31	0	0	0	1	1	1	1	1

## ■ Station Numbers and DIP Switch Positions

The following table lists the station numbers and corresponding setting switch positions for the control bus interface card and Vnet/IP interface card. Set the DIP switches as shown in the table to adjust to the required station number.

**Table Appendix 1-2 Station Numbers and DIP Switch Positions**

Station number	DIP switch bit number							
	1	2	3	4	5	6	7	8
1	0	0	0	0	0	0	0	1
2	0	0	0	0	0	0	1	0
3	1	0	0	0	0	0	1	1
4	0	0	0	0	0	1	0	0
5	1	0	0	0	0	1	0	1
6	1	0	0	0	0	1	1	0
7	0	0	0	0	0	1	1	1
8	0	0	0	0	1	0	0	0
9	1	0	0	0	1	0	0	1
10	1	0	0	0	1	0	1	0
11	0	0	0	0	1	0	1	1
12	1	0	0	0	1	1	0	0
13	0	0	0	0	1	1	0	1
14	0	0	0	0	1	1	1	0
15	1	0	0	0	1	1	1	1
16	0	0	0	1	0	0	0	0
17	1	0	0	1	0	0	0	1
18	1	0	0	1	0	0	1	0
19	0	0	0	1	0	0	1	1
20	1	0	0	1	0	1	0	0
21	0	0	0	1	0	1	0	1
22	0	0	0	1	0	1	1	0
23	1	0	0	1	0	1	1	1
24	1	0	0	1	1	0	0	0
25	0	0	0	1	1	0	0	1
26	0	0	0	1	1	0	1	0
27	1	0	0	1	1	0	1	1
28	0	0	0	1	1	1	0	0
29	1	0	0	1	1	1	0	1
30	1	0	0	1	1	1	1	0
31	0	0	0	1	1	1	1	1
32	0	0	1	0	0	0	0	0
33	1	0	1	0	0	0	0	1

Continues on the next page

**Table Appendix 1-2 Station Numbers and DIP Switch Positions** (Table continued)

Station number	DIP switch bit number							
	1	2	3	4	5	6	7	8
.	.							
.	.							
.	.							
60	1	0	1	1	1	1	0	0
61	0	0	1	1	1	1	0	1
62	0	0	1	1	1	1	1	0
63	1	0	1	1	1	1	1	1
64	0	1	0	0	0	0	0	0

# Appendix 2. Procedure for Erasing VI702 Internal Settings

If you intend to use a VI702 card used in another system for a system configured with Pro-Safe-RS only, delete the settings within the card using the following procedure.

1. Turn off the power of the computer. For safety, remove the power plug from the outlet.
2. Set the DIP switches (SW1) for the domain number on the VI702 as follows:

**Table Appendix 2-1 Setting of DIP Switches for Domain Number Setting (SW1)**

Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7	Bit 8
1	1	0	0	0	0	0	1
Parity			MSB				LSB

3. Set the DIP switches (SW2) for the station number on the VI702 as follows:

**Table Appendix 2-2 Setting of DIP Switches for Station Number Setting (SW2)**

Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7	Bit 8
0	0	0	0	0	0	0	1
Parity	MSB						LSB

4. Check that Bit 1 through Bit 4 of the DIP switches (SW4) for the Action Mode are all set to the off position on the VI702.
5. Remove the cover of the computer.
6. Insert the VI702 in the corresponding slot and fix the card.
7. Put back the cover of the computer.
8. Do not connect the cable to either BUS1 or BUS2.
9. Put back the power cord of the computer.
10. Start the computer, and then go to BIOS setting panel instead of starting Windows. If the Windows started, it is necessary to shutdown and switch off the computer, and start the computer for BIOS setting again.
11. Wait for about a minute after BIOS setting panel appears.
12. Turn off the power of the computer. For safety, remove the power plug from the outlet.
13. Remove the VI702 from the slot.

## SEE ALSO

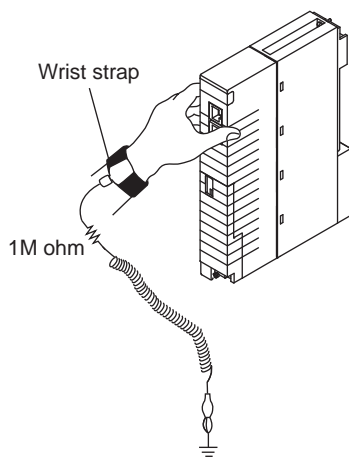
For more information about how to display the BIOS setting window, refer to:

The manual of the computer

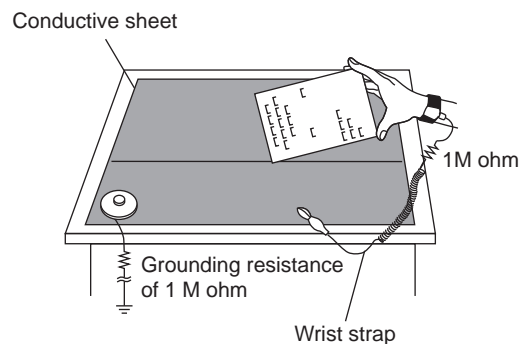
# Appendix 3. Antistatic Precautions When Handling Hardware

When doing maintenance work, take the following precautions to avoid electrostatic problems.

- When storing or carrying parts for maintenance, put them in an antistatic bag. (When shipped, they are placed in an antistatic bag labeled with cautions against electrostatic problems.)
- Wear a wrist strap with a 1M ohm grounding resistor then ground the wrist strap.
- When working on the bench, place the parts on a conductive sheet grounded via a 1 M ohm resistor and wear wrist strap. Keep static-chargeable plastic materials away from the parts.
- Never touch the parts with bare hands, without using a wrist strap and a conductive sheet.



Connect the wrist strap to the grounding terminal or unpainted part of the frame (grounded).



When working with a product with battery on a conductive sheet, set the battery ON/OFF switch to the OFF position or remove the battery.

**Figure Appendix 3-1 Using a Wrist Strap**

The wrist strap and conductive sheet are available from YOKOGAWA sales agents.

# Appendix 4. Compatibility between Revisions and Cautionary Notes for Upgrading



## IMPORTANT

- It is necessary to contact Yokogawa service agent before performing any operation explained in this chapter.
- Be sure to take a backup of the whole project before upgrading ProSafe-RS.

This section provides the compatibility information for earlier versions of ProSafe-RS software released in the past and the cautionary notes for upgrading that were published at the time of each release. The purpose of this section is to enable users to confirm the procedures for using the new features supported in each release. This section provides important descriptions of SCS specifications as compatibility information, enabling users to confirm the specifications in earlier versions.

When you upgrade ProSafe-RS, install only the software of the release number you want to use. However, for the required procedures after the installation, read the cautionary notes for upgrading for all release numbers between the release number of the software currently installed on your computer and the release number of the software you want to use.

Information on the following upgrading is provided:

- Upgrading the software with a release number older than R1.01.30 to R1.01.30.
- Upgrading the software of R1.01.30 to R1.01.40/R1.01.50.
- Upgrading the software of R1.01.30/R1.01.40/R1.01.50 to R1.02.
- Upgrading the software of R1.02 to R1.03
- Upgrading the software of R1.03 to R2.01
- Upgrading the software of R2.01 to R2.02
- Upgrading the software of R2.02 to R2.03
- Upgrading the software of R2.03 to R3.01
- Upgrading the software of R3.01 to R3.02
- Upgrading the software of R3.02.00 to R3.02.10



## Appendix 4.1 Upgrading to R1.01.30

The cautionary notes for upgrading the ProSafe-RS from an earlier version to R1.01.30 will be explained below.



### IMPORTANT

When subsystem communication or SYS\_SEC\_CTL FB are applied while ProSafe-RS R1.01.30 is integrated with CS 3000, the release number of CS 3000 software must be R3.07 or later.

- V net Driver  
Install the V net driver included in the CD-ROM of ProSafe-RS software. However, for the HIS with the CS 3000 software R3.07 environment, installation of the driver is not needed.

### ■ Software Revisions

Software revision information in release R1.01.30 and in the earlier releases is as follows:

Software Release R1.01.00

- SENG software release number: R1.01.00
- SCS system program release number: R1.01.00

Software Release R1.01.10

- SENG software release number: R1.01.10
- SCS system program release number: R1.01.00

Software Release R1.01.30

- SENG software release number: R1.01.30
- SCS system program release number: R1.01.30

### ● Inter-SCS Safety Communication

The release numbers of the SCS system programs on SCSs communicating with each other using the Inter-SCS safety communication function must be the same.

### ■ Procedures for Upgrading

When using the added and upgraded features of R1.01.30, install the ProSafe-RS R1.01.30 or later version of software to SENG and open existing SCS projects. Then the following new features of R1.01.30 are applicable.

- SCS information Dialog box
- Saves and downloads the operation marks
- Locks user-defined FB parameters

**SEE  
ALSO**

For more information about cautionary notes for opening existing SCS projects, refer to:

“● Procedure A: Opening SCS Projects” on page C4-6

## ■ Cautions on Using Added and Upgraded Features

In order to use the added and upgraded features of R1.01.30, it may be required to perform offline downloading to the SCS. The related procedures are as follows.

### SEE ALSO

For more information about detailed procedures after the upgrade, refer to:

- “● Procedure B: Master Database Offline Download” on page C4-6
- “● Procedure C: Creating New SCS Project and Offline Download” on page C4-7

### ● Subsystem Communication (Modbus Communication Package)

When performing the engineering works to apply the Modbus communication package (for ALR111, ALR121) on SCS, “Procedure C” should be performed on R1.01.30 or later version SENG. On the SCS State Management Window of SCS maintenance Support Tool and on the SCS Status view of the CENTUM HIS that has been integrated with ProSafe-RS, the status of “Comm. I/O Lock” will be displayed with [No] until the offline download is completed.

### ● Using the FU/FB Added in R1.01.30

In order to use the added FU/FB of R1.01.30 such as SYS\_SEC\_CTL (for changing SCS security level), “Procedure C” should be performed on R1.01.30 or later version SENG.

### ● Forcing (SCS Security Level 0)

From R1.01.30, when SCS security level is 0, the values of internal variables and FB parameters can be changed without locking the variable or parameter. However, this change is not valid if Procedure B is not performed on R1.01.30 or later version SENG.

### ● I/O Lock Window

In R1.01.30 version, the process of getting data from SCS and displaying them on I/O Lock window is changed. This change will become valid after Procedure B is performed on R1.01.30 or later version SENG.

### ● Inter-SCS Safety Communication



## WARNING

After upgrading SENG to R1.01.30 or later version, for the first time offline download to an SCS is performed while the SCS is running inter-SCS communication with other SCSs, the Procedure B needs to be performed on R1.01.30 or later version SENG for all the communicated SCSs. When offline download to the SCS that is running inter-SCS communication with other SCSs, it is necessary to take measures on the other SCSs so as not to cause a nuisance tripping.

### ● SCS Start Action when Applied with IRIG-B

In R1.01.30 version, the SCS start action is changed under the circumstance that the SCS is applied with IRIG-B but the IRIG-B receiver is not connected. This change will become valid after Procedure B is performed on R1.01.30 or later version SENG.

### ● Handling Messages during SCS Start

In R1.01.30 version, how the SCS during start handles the SOE data and diagnostic messages occurred before SCS stopped is changed. This change will become valid after Procedure B is performed on R1.01.30 or later version SENG.



## IMPORTANT

When the SCS is restarted by Master Database Offline Download, the Diagnostic Information Window should be closed. If the window is not closed during offline download, it is necessary to click [Update] button when the SCS start action is completed so as to display the diagnostic information properly.

## ■ Cautionary Notes for Executing Build after Upgrading SENG

If a user-defined FU satisfying the following conditions is created by an SENG in an earlier version than R1.01.30 and the SENG is upgraded to R1.01.30 or later, the first Build execution after the upgrade will cause a Build Error message.

This is because the specification change made in the R1.01.30 to prevent the creation of the user-defined FUs satisfied the following conditions.

### ● Conditions that Cause a Build Error

- FB(s) is used in a user-defined FU.
- Variable(s) of global attributes is used in a user-defined FU.

### ● Workaround

If an FB or global variable(s) is used in a user-defined FU, change the user-defined FU to a user-defined FB. An offline download is required after this change.

## ■ Notes on Running Cross Reference Analyzer after Upgrading SENG

If a user-defined FU satisfying the following condition is created by an SENG in an earlier version than R1.01.30 and the SENG is upgraded to R1.01.30 or later, the message “Instruction Modified” appears at the execution of Cross Reference Analyzer after the initial Build execution.

### ● Condition for an “Instruction Modified” Notification

If local variable(s) is used in a user-defined FU.

### ● Background

The following specification change was made in R1.01.30.

**Table Appendix 4.1-1 Specification Change**

Before	If local variable(s) is used in a user-defined FU, local variable(s) is not initialized every time the user-defined FU is called.
After	If local variable(s) is used in a user-defined FU, local variable(s) is initialized every time the user-defined FU is called. The value used for initialization is the initial value defined in Dictionary. If initial value is not defined in the Dictionary, value will be initialized using the following: DINT type: 0 REAL type: 0.0 BOOL type: FALSE TIME type: t#0s
Notes	Local variables in a user-defined FU are initialized every time the user-defined FU is called. If local variables are used in a user-defined FU, set values to local variables in advance.

- **Workaround**

Check if the “Instruction Modified” message was caused by the specification change, and modify the application logic if necessary.

- **Cautions on Online Change Downloading after Upgrading SENG**

After upgrading SENG from R1.01.10 to R1.01.30 or later version, the first time online download will download all POUs to SCS. Therefore, when running build, a warning message for locking all the outputs will be prompted.

For the later Online Change Download, it will download only the modified POU to SCS.

It is recommended to run offline download or online change download right after the upgrading. Thus, the Online Change Download for the later modifications can download only the modified POU to SCS.

Follow the procedures below to perform either offline downloading or online change download right after upgrading.

- **Offline Download**

1. Choose [Clean Project/Library] from [Project] menu.
2. Start [Build].
3. Run offline downloading.

- **Online Change Download**

1. Choose [Edit Project Description] from [Tools] menu and then click [OK] on the displayed Project description dialog box.
2. Save the project.
3. Start [Build] (a warning message for locking all the outputs will be prompted).
4. Run Online Change Download.

## Appendix 4.2 Upgrading to R1.01.40/R1.01.50

In this section, the cautionary notes for upgrading to R1.01.40/R1.01.50 will be explained. Moreover, for upgrading from a release older than R1.01.30 to R1.01.40/R1.01.50, it is necessary to read the cautionary notes for upgrading to R1.01.30 together with this section.

### ■ Software Revisions

Software revision information in release R1.01.40 is as follows:

- SENG software release number: R1.01.40
- SCS system program release number: R1.01.30

Software revision information in release R1.01.50 is as follows:

- SENG software release number: R1.01.50
- SCS system program release number: R1.01.30

#### ● Inter-SCS Safety Communication

The release numbers of the SCS system programs on SCSs communicating with each other using the Inter-SCS safety communication function must be the same.

### ■ Procedures for Upgrading

For upgrading from R1.01.30 to a newer version, the ProSafe-RS software needs to be installed into SENG. However, no specific operation is needed for applying the revised and added features after the installation.

The SCS project and library created or edited in R1.01.30 will be unconditionally converted to R1.01.40/R1.01.50 when they are first time opened after upgrading to R1.01.40/R1.01.50. There will be no confirmation dialog box prompts for the conversion.



### IMPORTANT

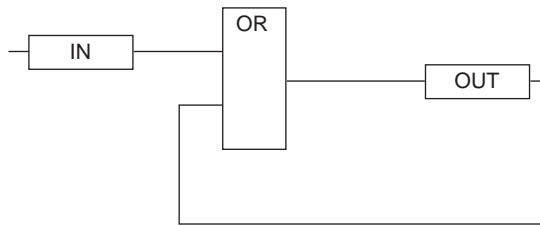
When upgrading from a release older than R1.01.30 to R1.01.40/R1.01.50, the cautionary notes for upgrading an earlier release to R1.01.30 should be referenced. It is necessary to read all the cautionary notes and then perform the required operations accordingly.

### ■ Note on Upgrading to R1.01.50

If a user-defined FB satisfying the following condition is created by an SENG in an earlier version than R1.01.50 and if the SENG is upgraded to R1.01.50 or later and a Build is performed without modification of the project data, there are cases where an offline download is required.

#### ● Condition

With POU (program or user-defined FU /FB) created by FBD, if the output of an FU/FB is looped back to its own input parameter, a variable must be placed in the loop.



**Figure Appendix 4.2-1 Example of Correct Loopback**

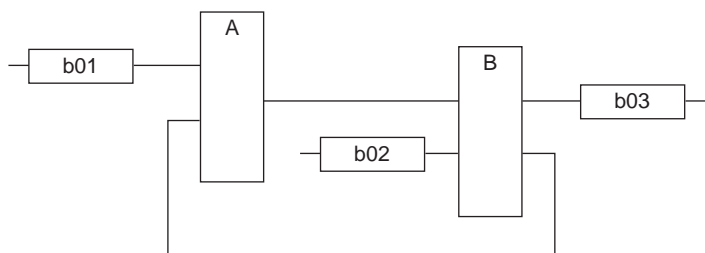
If a user-defined FB ignoring this rule meets one of the following conditions, an offline download is required.

(Condition 1)

If the “Generate symbols monitoring information” for the user-defined FB is OFF.

(Condition 2)

If the input of the loopback is the output from the FB. (B is FB in the following figure)



**Figure Appendix 4.2-2 Example of Loopback Requiring an Offline Download**

## ● Background

With an SENG in an earlier version than R1.01.50, there are cases where no warning message is output at a Build execution for a POU that does not follow the loopback rule.

With an SENG in R1.01.50 or later, the following warning message is always output at a Build execution for a POU that does not follow the loopback rule.

“WARNING: Used of loop is not recommended.”

If this message appears for a POU after the SENG is upgraded to R1.01.50 or later, place a variable in the loop.

## Appendix 4.3 Upgrading to R1.02

In this section, the cautionary notes for upgrading from R1.01.30, R1.01.40, or R1.01.50 to R1.02 will be explained. Moreover, for upgrading from a release older than R1.01.30 to R1.02, it is necessary to read the cautionary notes for upgrading to R1.01.30 together with this section.



### IMPORTANT

In order to use the new features when the ProSafe-RS R1.02 is integrated with CS 3000, the release number of the CS 3000 software must be R3.08 or later.

## ■ Software Revisions

Software revision information in release R1.02 is as follows:

Software Release R1.02.xx (\*1)

- SENG software release number: R1.02.xx (\*1)
- SCS system program release number: R1.02.xx (\*1)

\*1: xx varies in accordance with the last two digits of the release number for the software released between R1.02.00 and R1.03.00.

### ● Inter-SCS Safety Communication

The release number of the SCS system program on the Inter-SCS safety communication with an “SCS in R1.02” must be R1.01.30 or later.

If Vnet/IP is used for route of the Inter-SCS safety communication, the system programs on the SCSs must be in R1.02.

## ■ Procedures for Upgrading

In order to use the added or modified features in the R1.02, install the R1.02 or later software and open the existing “SCS Project”. This will allow you to use the following added/modified features in R1.02.

- Alarm Off
- Modified Online Change Download

**SEE  
ALSO**

For more information about cautionary notes for opening existing SCS projects, refer to:

“● Procedure A: Opening SCS Projects” on page C4-6

### ● Cautionary Notes for Online Change Download after Upgrading the SENG to R1.02 or Later

After upgrading an SENG to R1.02 or later and if you use the SENG for engineering the project data created by an SENG in an earlier version than R1.02, execute “Build” first without changing any parameter, then perform an online change download.

If you skip executing operation above and do the following, there are cases where unchanged POU (Program Organization Units) are downloaded to SCS in the online change download.

- From the Dictionary View window of the SCS Manager, Add, Delete, Sort the named global instances of FB used by POU.
- Add or Delete an existing FU to/from POU.

- In the Link Architecture View window of the SCS Manager, Change the order of the user-defined FU/FB.

**TIP**

The following warning message appears in the first “Build” execution after the SENG is upgraded to R1.02.

“WARNING: POU indexes are modified for next on line change. Online change may download others POU in addition of the modified ones.”

## ■ Cautionary Notes on Using New Features

Some steps are required before using the new features in the R1.02. The steps and cautionary notes for each feature are as follows.

**SEE ALSO**

For more information about detailed procedures after the upgrade, refer to:

- “● Procedure B: Master Database Offline Download” on page C4-6
- “● Procedure C: Creating New SCS Project and Offline Download” on page C4-7
- “● Procedure D: Setting Definition Items for New Features and Offline Download” on page C4-8

### ● Support for Vnet/IP

For engineering the SCS connected with Vnet/IP, follow the “Procedure C” on SENG in R1.02 or later.

### ● Optical ESB Bus Repeater

For extending the ESB bus using an Optical ESB Bus Repeater, follow the “Procedure D” on SENG in R1.02 or later. Set the parameters from the SCS tab on the SCS Constants Builder.

### ● Using the New FBs in the R1.02

Before using the new FBs in the R1.02, follow the “Procedure C” on SENG in R1.02 or later.

### ● Outputting Process Alarm Messages when AOF is Released

From the SCS Constants Builder window, you can specify to (or not to) output the suppressed process alarm messages when the AOF is released.

This setting is applicable when the ProSafe-RS is integrated with CENTUM.

Follow the “Procedure D” on SENG in R1.02 or later.

### ● Plant Hierarchy

For specifying Plant Hierarchy to the tag data operated and monitored on HIS when the ProSafe-RS is integrated with CENTUM, follow the “Procedure B” on SENG in R1.02 or later.

### ● Expansion of Alarm Processing Levels

When the ProSafe-RS is integrated with CENTUM, you can set the Alarm Processing Levels (5 to 16) to the tag data operated and monitored on HIS.

Follow the “Procedure D” on SENG in R1.02 or later.

**SEE ALSO**

For more information about detailed procedures, refer to:

- 2.1, “Engineering on the SENG side” in Integration with CENTUM VP/CS 3000 (IM 32Q01E10-31E)



- **Newly Supported I/O Modules (SAI143-H, SAI533, SDV541)**

In order to use the I/O Modules newly supported by the R1.02, you must follow the “Procedure C” on SENG in R1.02 or later.

## Appendix 4.4 Upgrading to R1.03

In this section, the cautionary notes for upgrading from R1.02 to R1.03 will be explained. Before you upgrade, read also the cautionary notes for the previous revisions issued after the software version currently installed on your computer.



### IMPORTANT

In order to use the new features when the ProSafe-RS R1.03 is integrated with CS 3000, the release number of the CENTUM CS 3000 software must be R3.08.50 or later.

## ■ Software Revisions

Software revision information in release R1.03 is as follows:

Software Release R1.03.xx (\*1)

- SENG software release number: R1.03.xx (\*1)
- SCS system program release number: R1.03.xx (\*1)

\*1: xx varies in accordance with the last two digits of the release number for the software which will be released after R1.03.00.

### ● Inter-SCS Safety Communication

The release number of the SCS system program to perform Inter-SCS safety communication with an “SCS in R1.03” must be R1.01.30 or later.

If Vnet/IP is used for route of the Inter-SCS safety communication, the system programs on the SCSs must be in R1.02 or later.

## ■ Procedures for Upgrading

In order to use the added or modified features in the R1.03, install the R1.03 or later software and open the existing “SCS Project”.

**SEE  
ALSO**

For more information about cautionary notes for opening existing SCS projects, refer to:

- [Procedure A: Opening SCS Projects](#) on page C4-6

## ■ Cautionary Notes on Using New and Modified Features

Some steps such as an offline download to SCS may be required before using the new features in the R1.03 after the SENG software is upgraded to R1.03. The steps and cautionary notes for each feature are the followings.

**SEE  
ALSO**

For more information about detailed procedures after the upgrade, refer to:

- ● [Procedure B: Master Database Offline Download](#) on page C4-6
- ● [Procedure C: Creating New SCS Project and Offline Download](#) on page C4-7
- ● [Procedure D: Setting Definition Items for New Features and Offline Download](#) on page C4-8

### ● Test Function (i.e. SCS Simulator that Runs on a Computer) and Interface for Plant Training

Before using the Test function (i.e. SCS simulator), you need to complete the “Procedure C.” You cannot download the project created for SCS simulation tests to an actual SCS.

CS 3000 system must be upgraded to R3.08.50 or later.

- **New Input/Output Modules (SDV521, SDV531-L)**

Before using the Input/Output modules newly supported by R1.03, you need to complete the “Procedure C.”

- **New Optical ESB Bus Repeater Modules (SNT411/SNT511)**

Before using the Optical ESB Bus Repeater Modules newly supported by R1.03, you need to complete the “Procedure D.” You need to set parameters using the SCS Constants Builder and I/O Parameter Builder.

---

**TIP**

For using SNT411/SNT511, SCP451 (processor module) which supports the SNT411/SNT511 needs to be prepared. For further information, please contact our sales office.

---

**SEE  
ALSO**

For more information about setting parameters for Optical ESB Bus Repeater Modules, refer to:

- “■ SCS Tab” in 3.1.3, “SCS Constants Builder” in Engineering Reference (IM 32Q04B10-31E)
  - “■ Items Set for Nodes” in 4.4, “I/O Parameter Builder” in Engineering Reference (IM 32Q04B10-31E)
- 

- **Using the New FBs in the R1.03**

Before using the new FBs in the R1.03, follow the “Procedure C” on SENG in R1.03 or later.

- **For Using the Online Change Function for Input/Output Module Channels**

Before using the Online change function for Input/Output module channels, you need to complete the “Procedure B.”

- **SCS Link Transmission**

Before using the SCS Link Transmission, you need to complete the “Procedure C.”

CS 3000 system must be upgraded to R3.08.50 or later.

---

**TIP**

If you use SCS Link Transmission on SCS-IP, you need to have the SCP451 which supports SCS Link Transmission. If you use SCS Global Switch Communication via Vnet/IP, you may need to update the CPU module of the FCS of CENTUM. For further information, please contact our sales office.

---

- **Grouping Override FB**

Before using the Grouping override FB, you need to complete the “Procedure C.”

CS 3000 system must be upgraded to R3.08.50 or later.

- **Structured Text (ST)**

For using the ST language in ProSafe-RS, you need to complete the “Procedure D. Use the Multi-Language Editor to create application in ST.

- **Password FB**

Before using the upgraded Password FB in R1.03, you need to complete the “Procedure B.”

CS 3000 system must be upgraded to R3.08.50 or later.

- **Enhanced CENTUM Integration for ANLG\_S**

Before using the enhanced CENTUM Integration in R1.03 for the ANLG\_S block, you need to complete the “Procedure C.”

CS 3000 system must be upgraded to R3.08.50 or later.

---

## ■ Notes on Upgrading SCS Project in R1.02 to R1.03 or Later

With the SCS project created in R1.02, no data status is attached to the PV of the mapping block S\_ANLG\_S for ANLG\_S. But in R1.03 or later, a data status is attached to the PV of the mapping block S\_ANLG\_S.

In R1.03 or later, if the status of IN terminal of ANLG\_S FB for the mapping block S\_ANLG\_S turns BAD, the data status of PV for S\_ANLG\_S turns BAD (0x8000 0000). (Default in the SCS Constants Builder)

Therefore, if the PV of S\_ANLG\_S is referred via FCS or OPC, the behavior may change between the SCS project created newly in R1.03 or later and the SCS project created in R1.02.

If you want the same behavior as that in R1.02, set [PV Status of S\_ANLG\_S] in the SCS Constants Builder to [NO].

## ■ Notes on Enhanced Integrity Analyzer

### ● Stricter Check of Recursive Call in POU

Before R1.03, there are cases where a POU containing recursively called FB and FU can be downloaded to SCS. In R1.03 or later, an error is raised for a POU with recursive calls to prevent its download to SCS.

The error detection depends on how the recursive call is implemented: during generation or by Integrity Analyzer.

When upgrading to R1.03 or later, make sure that no recursive call is included in POU. If any, change the logic to exclude the recursive call from the POU.

#### TIP

Before R1.03, this does not cause an error during Generation. Even if a Warning is displayed by Integrity Analyzer, a download to SCS is allowed after the Warning is acknowledged.

### ● Notes on Comparison Operation (=, <>) on Floating-point Data

There are cases where comparison operation using "=" (equal) or "<>" (not equal) on floating-point data does not produce expected results because a round-off error may result from repeated arithmetic operations.

In R1.03 or later, if accurate comparison operation (=, <>) on floating-point data is detected, Integrity Analyzer displays a warning.

After upgrading to R1.03 or later, if accurate comparison operation (=, <>) on floating-point data is detected, a warning is displayed after the upgrade.

If a warning appears, check if the program needs to be enhanced using "smaller than (<)" or "greater than (>)." If the result of the check is "no need to change program", acknowledge the warning that Integrity Analyzer displayed. This will enable a download of the program to SCS.

## ■ Notes on Changed Password FB

If a wrong password for the Password FB is entered from HIS, the behavior in R1.03 or later is as follows:

Table Appendix 4.4-1 Change made to Password FB

Version	Change in behavior if a wrong password is entered for Password FB
Before R1.03	In the operation to change MV in the Password FB, if user enters a wrong password, a system alarm is raised, and user has to undo the 'change MV' to the previous value. If a wrong password is entered, a diagnostic information message is displayed to notify it. Here, the changed MV value remains as is and an ANS+ or ANS- process alarm is raised.
R1.03 or later	If a wrong password is entered, an error message for the wrong password is displayed in the dialog box on HIS, and the MV value remains unchanged.

## ■ Notice on the Variables Begin with Underscore Characters

From R1.03, the variable and the Defined Words begin with underscore character will be handled differently by the system.

### ● Specification Prior to R1.03

Prior to R1.03, to start the variable or the Defined Words with underscore character is prohibited, however, if you started the variable or the Defined Words with underscore character, no error would be indicated.

### ● Specification for R1.03 or Later

Since R1.03, the variable or Defined Words begin with underscore character can be used, however, if they are identical with system reserved words, an error will be indicated. The system reserved words are as follows.

- System Reserved Words:  
\_AND, \_CALL, \_CALL\_IEC\_SFC\_FB, \_END, \_GOTO, \_IF, \_NOT, \_PUSH\_PAR, \_OR,  
\_POP\_CSTK, \_PUSH\_CSTK, \_RET, \_STEP, \_XOR

## Appendix 4.5 Upgrading to R2.01

The notices on version upgrading from R1.03 to R2.01 (R2.01.10 or later) will be explained in this section. Before upgrading installation, the documents regarding the currently installed ProSafe-RS software as well as the release notes for the previous upgrading installations should be read first.

In this section, the procedure for upgrading from R2.01.00 to R2.01.10 will also be explained. If R2.01.00 is installed in your computer, you need to upgrade the software to R2.01.10.



### IMPORTANT

- When integrating ProSafe-RS and CENTUM VP, the new features added to ProSafe-RS R2.01 are supported only in CENTUM VP R4.01 and later versions.
- If you plan to manage ProSafe-RS computers in Windows domain environment, the Windows domain environment settings should be performed before performing the installation.

## ■ Software Revisions

Software revision information in release R2.01 is as follows:

Software Release: R2.01.xx (\*1)

- SENG software release number: R2.01.xx (\*2)
- SCS system program release number: R2.01.xx (\*2)

\*1: xx stands for the revisions after releasing R2.01.00

\*2: For R2.01.10, xx stands for 00

### ● Inter-SCS Safety Communication

The earlier version of SCS can perform inter-SCS safety communication with the SCS that has R2.01 system program must be a version of R1.01.30 or later.

If the inter-SCS safety communication is routing Vnet/IP, the two version of system programs in the SCSs should be standardized to R1.02 or a later version.

### ● Control bus Drivers

The control bus drivers installed on the computer should be upgraded to the version supplied at R2.01 (R2.01.10).

The ProSafe-RS R2.01 control bus drivers are compatible with the control bus drivers provided in CENTUM VP R4.01.

## ■ Basic Procedure of Upgrading Installation

When using the added or changed software features, the installation should be performed and opening the existing SCS projects with the installed ProSafe-RS software of R2.01 or later version.

**SEE  
ALSO**

For more information about cautionary notes for opening existing SCS projects, refer to:

“● Procedure A: Opening SCS Projects” on page C4-6

## ■ Procedure for Upgrading from R2.01.00 to R2.01.10

Carry out the following procedure to upgrade your system:

1. For a Windows Vista computer with no CENTUM VP software, install the Windows hotfix program provided in the CD-ROM of R2.01.10.
2. Update the control bus drivers using the ProSafe-RS software CD-ROM of R2.01.10.
3. Without using the key code FD, carry out installation to upgrade from R2.01.00 to R2.01.10. This installation should be done by following the procedure for revision upgrading (without package addition).



### **IMPORTANT**

If any software package should be added, install it only after you have upgraded the system from R2.01.00 to R2.01.10.

---

## Appendix 4.6 Upgrading to R2.02

In this section, the cautionary notes for upgrading from R2.01 to R2.02 will be explained. Before you upgrade, read also the cautionary notes for the previous revisions issued after the software version currently installed on your computer.



### IMPORTANT

- When integrating ProSafe-RS and CENTUM VP, the new features added to ProSafe-RS R2.01 are supported only in CENTUM VP R4.02 and later versions.
- If you plan to manage ProSafe-RS computers in Windows domain environment, the Windows domain environment settings should be performed before performing the installation.

## ■ Software Revisions

Software revision information in release R2.02 is as follows:

Software Release R2.02.xx (\*1)

- SENG software release number: R2.02.xx (\*1)
- SCS system program release number: R2.02.xx (\*1)

\*1: xx varies in accordance with the last two digits of the release number for the software which will be released after R2.02.00.

### ● Inter-SCS Safety Communication

The release number of the SCS system program to perform Inter-SCS safety communication with an “SCS in R2.02” must be R1.01.30 or later.

If Vnet/IP is used for route of the Inter-SCS safety communication, the system programs on the SCSs must be in R1.02 or later.

### ● Control Bus Drivers

The control bus drivers installed on the computer should be upgraded to the version supplied at R2.02.

## ■ Procedures for Upgrading

In order to use the features added or modified in R2.02, install the R2.02 or later software and open the existing “SCS Project”.

**SEE  
ALSO**

For more information about cautionary notes for opening existing SCS projects, refer to:

- [Procedure A: Opening SCS Projects” on page C4-6](#)



## Appendix 4.6.1 Cautionary Notes for Upgrading

### ■ Procedure for Using New and Modified Features

After the SENG software has been upgraded to R2.02, some of the features added or modified in the R2.02 require further steps, such as offline downloading to SCS, before they can be used. In the following, the steps are explained for each feature.

**SEE  
ALSO**

For more information about “Procedure B” and “Procedure C” that appear in this section, refer to:

- “● Procedure B: Master Database Offline Download” on page C4-6
- “● Procedure C: Creating New SCS Project and Offline Download” on page C4-7

#### ● New I/O Module (SDV526)

To use the I/O module SDV526 newly supported in R2.02, you must perform “Procedure C.”

#### ● Behavior of AIO/DIO modules at Online Change Download

To enable online change downloading with the target AIO/DIO module kept running when you have changed any settings of I/O Parameter Builder that require downloading to the AIO/DIO module (IOM download), you must perform “Procedure B.” If not, the target AIO/DIO module will be stopped as before.

**SEE  
ALSO**

For more information about the behaviors of AIO/DIO modules during online downloading with software before R2.02, refer to:

- “■ Behavior of AIO/DIO Modules at Online Change Download” on page App.4-20

#### ● Showing the Results of the Last Analysis on Cross Reference Analyzer

To enable the function to show the results of the last analysis after you have upgraded SENG to R2.02, you must once acknowledge the analysis results in Cross Reference Analyzer and perform downloading to SCS.

### ■ Notes on Online Change Download after Upgrading SENG

In R2.02, the problem that the FB for which you have specified a minus value for a label in a CASE statement does not run properly (\*1) has been fixed. Because of this, the behavior of online change downloading after you have upgraded the SENG to R2.02 will be as follows.

After you have upgraded the SENG to R2.02, if you perform a build for a project created in a version before R2.02 and execute online change downloading, all the FBs containing any CASE statement in the ST language will be downloaded (\*2) even if no changes have been made to the logic. Once you rebuild a project of a version earlier than R2.02 on a R2.02 system and execute online change downloading, FBs with no logic change will not be downloaded in the subsequent online change downloading.

You can use the Database Validity Check Tool, as necessary, to find out which FBs will be downloaded before you execute online change downloading.

In a revision before R2.02, FBs containing any CASE statement in which a minus value is specified for a label do not run correctly, so they can be spotted and removed in the system test. Therefore, no such FBs should exist in a project. However, if such FBs do exist, the FBs may start to run normally after downloading.

To avoid such unexpected change in behavior, you should check the project to see if there are any FBs containing a CASE statement in which a minus value is specified for a label.

- If any FBs using a minus value for a label of CASE statement are found, make sure that the change in behavior does not cause any adverse effects on the system. (\*3) (\*4)

- If FBs using a minus value for a label of CASE statement are not found, all the FBs using CASE statements will be downloaded but the system behavior remains the same; so you do not need to perform tests again.
- \*1: If you specify a minus value for a label in a CASE statement in ST, an incorrect database which causes unexpected behavior may be generated. In the following example, if variable1 is neither "1" nor "2", "3" is always assigned to aaa.
- ```

CASE variable1 OF
1: aaa := 1;
2: aaa := 2;
-1: aaa := 3; (* When the variable1 is neither 1 nor 2, this line is always executed.*)
-2: aaa := 4;
ELSE aaa := 5;
END_CASE;

```
- \*2: In this case, Cross Reference Analyzer does not detect the difference of the FBs using CASE statements.
- \*3: In this case, Cross Reference Analyzer does not detect the difference of the FBs using a minus value for a label of CASE statement.
- \*4: To find the locations where CASE statements are used, open multiple STs in Multi-Language Editor and search for "CASE".

## ■ Enhanced Checking by Integrity Analyzer

### ● Checking for Multiple Writing to the Same Variable

Multiple writing to the same variable can reduce the program readability and end up downloading of programs that cause unintended behavior. Integrity Analyzer in R2.02 detects multiple writing to the same variable and displays a warning message.

This warning message is not output with the revisions before R2.02, but it will be displayed after you have upgraded to R2.02 when the program contains any multiple writing to the same variable. If this warning message is displayed, examine the program to find out if you can eliminate the multiple writing.

If you find that the multiple writing is necessary, acknowledge the results of analysis in Integrity Analyzer and you can download the program to SCS without change. In this case, the program can be used as a function allowed for safety application after verifying its validity in user tests.

### ● Checking for Multiple Calls to the Same FB Instance

Multiple calls to the same function block (FB) instance can lead to an unexpected state in the system and the program may not behave as intended. Integrity Analyzer in R2.02 detects multiple calls to the same FB instance and displays a warning message.

This warning message is not output with the revisions before R2.02, but it will be displayed after you have upgraded to R2.02 when the program contains multiple calls to the same FB instance. If this warning message is displayed, examine the program to find out if you can eliminate the multiple calls. If you find that the multiple calls are necessary, acknowledge the results of analysis in Integrity Analyzer and you can download the program to SCS without change. In this case, the program can be used as a function allowed for safety application after verifying its validity in user tests.

### ● Checking for Writing to Output Variable Status

I/O variable statuses (.status) are the data that reflect the actual statuses (normal/abnormal) of I/O channels. Therefore, they should not be changed by user logic. Integrity Analyzer in R2.02 detects writing to output variable statuses and raises an error.

In revisions before R2.02, no such error is raised. But this error will be raised after you have upgraded to R2.02 when there is any program that writes to any output variable status. If an error message is displayed, change the program to eliminate the writing to output variable statuses.

## Appendix 4.6.2 Compatibility with Earlier Revisions

### ■ Behavior of AIO/DIO Modules at Online Change Download

When online change downloading is performed after you have changed any settings of I/O Parameter Builder that require downloading to I/O modules (IOM download), the target AIO/DIO modules continue operation if the SCS system program revision is R2.02 or later while the AIO/DIO modules are stopped with revisions earlier than R2.02.

This section explains the behaviors of AIO/DIO modules when the SCS system program revision is earlier than R2.02.

#### SEE ALSO

For more information about the setting items in I/O Parameter Builder that require IOM download, refer to:

- A4.4, “Items set for analog inputs” in Safety Control Station Reference (IM 32Q03B10-31E)
- A4.5, “Items set for analog outputs” in Safety Control Station Reference (IM 32Q03B10-31E)
- A4.6, “Items set for discrete inputs” in Safety Control Station Reference (IM 32Q03B10-31E)
- A4.7, “Items set for discrete outputs” in Safety Control Station Reference (IM 32Q03B10-31E)

### ● Behavior of Input Modules

- At the time of online change, the data status of all channels of the target module become BAD, and the diagnostic information message “IOM Fail” appears. The input signals of all channels of the module are processed according to the [Input Processing at Fault] settings.
- If on-demand HART communication with PRM is performed, the HART communication is discontinued during the “IOM Fail” status.
- On completion of online change download, the channels’ data automatically return to the values input to the channels and all data statuses become GOOD.
- A diagnostic information message indicating that the input module has recovered to normal is output.
- For dual-redundantly configured I/O modules, the odd-numbered module takes the control right.

#### TIP

If any setting items that require IOM download and the setting of [Input Processing at Fault] or [Input Value at Fault] are changed online simultaneously, the input value will conform to the changed settings of [Input Processing at Fault] and [Input Value at Fault].

### ● Behavior of Output Modules

- At the time of online change, the data status of all channels of the target module become BAD, and the diagnostic information message “IOM Fail” appears. The output values on all channels change to 0 if the target module is a discrete output module, and change to the tight-shut output values (\*1) if the target module is an analog output module.
- If on-demand HART communication with PRM is performed, the HART communication is discontinued during the “IOM Fail” status.
- On completion of online change download, the data status of all channels become GOOD, while the output values still remain 0 with a discrete output module or remain the tight-shut output values with an analog output module.
- A diagnostic information message indicating that the output module has recovered to normal is output.

- For dual-redundantly configured output modules, the odd-numbered module takes the control right.
- If the user performs the output enable operation, outputs of the application logic are output from the output module.

\*1: A tight-shut output value can be set for each channel using the I/O Parameter Builder.

## ■ Changes in Multi-Language Editor Specifications

### ● Font and Font Color are Set for Each Project

In revisions earlier than R2.02, the font and font color shown in the function block diagram (FBD) window of Multi-Language Editor are retained for each user of the computer.

From R2.02, the font and font color settings for FBD windows are retained for each project. When a project is first opened in R2.02, the font and font color settings used by the user who opened the project will be retained in the project.

### ● FBD Guidelines are Set for Each Project

In revisions earlier than R2.02, the guideline setting for the FBD window of Multi-Language Editor is retained for each computer.

From R2.02, the guideline setting is retained for each project. The guideline setting when the project is first opened in R2.02 will be retained in the project.

## Appendix 4.7 Upgrading to R2.03

In this section, the cautionary notes for upgrading from R2.02 to R2.03 are explained. Before you upgrade, also read the cautionary notes for the previous revisions issued after the software version currently installed on your computer.



### IMPORTANT

- In the case of system configuration integrating ProSafe-RS and CENTUM VP, it is possible to perform operation and monitoring of the newly added features of ProSafe-RS R2.03 correctly by using CENTUM VP or R4.02 or later versions.
- Install the ProSafe-RS software version R2.03.00 after upgrading the control bus driver of SENG using the CD-ROM of ProSafe-RS R2.03.59.
- Be sure to use the CD-ROM of R2.03.59 to install the software immediately after the installation of the R2.03.00 software.
- After the installation of R2.03.59 is complete, follow the precautions given in this section and perform the tasks of upgrading the project data.

### TIP

R2.03.80 includes the features of all minor release versions of R2.03.

### SEE ALSO

For more information about the behaviors of CENTUM that are related to the new features of ProSafe-RS R2.03 when ProSafe-RS is integrated with CENTUM VP earlier than R4.02 or CS 3000, refer to:

[Appendix 1., "Differences in limitations and specifications among software release numbers of CENTUM" in Integration with CENTUM VP/CS 3000 \(IM 32Q01E10-31E\)](#)

## ■ Software Revisions

Software revision information in release R2.03 is as follows:

Software Release R2.03.xx (\*1)

- SENG software release number: R2.03.xx (\*1)
- SCS system program release number: R2.03.xx (\*1)

\*1: xx varies in accordance with the last two digits of the release number for the software which will be released after R2.03.00.

### ● Inter-SCS Safety Communication

The release number of the SCS system program to perform Inter-SCS safety communication with an "SCS in R2.03" must be R1.01.30 or later.

If Vnet/IP is used for route of the Inter-SCS safety communication, the system programs on the SCSs must be in R1.02 or later.

### ● Control Bus Drivers

Install the enhanced control bus driver that is included in the R2.03.59 CD-ROM.

## ■ Procedures for Upgrading

In order to use the features added or modified in R2.03, install the R2.03 or later software and open the existing SCS project.

---

**SEE  
ALSO**

For more information about cautionary notes for opening existing SCS projects, refer to:

- [Procedure A: Opening SCS Projects](#) on page C4-6
-

## Appendix 4.7.1 Cautionary Notes for Upgrading

### ■ Inconsistency Check of TCP/IP Settings

On a computer running Windows Vista SP2 or Windows Server 2008 SP2, run the TCP/IP Inconsistency Detect Tool after you have upgraded the SENG software to R2.03. If any inconsistency is detected in TCP/IP settings, run the TCP/IP Inconsistency Repair Tool and then configure the TCP/IP settings again.

#### SEE ALSO

For more information about The tools for detecting and repairing inconsistency in TCP/IP setting TCP/IP, refer to:

“■ Procedure 6: Repair TCP/IP Settings” on page B3-52

### ■ Procedure for Using New and Modified Features

After the SENG software has been upgraded to R2.03, some of the features added or modified in the R2.03 require further steps, such as offline downloading to SCS, before they can be used. In the following, the steps are explained for each feature.

#### SEE ALSO

For more information about “Procedure B” through “Procedure F” that appear in this section, refer to:

- “● Procedure B: Master Database Offline Download” on page C4-6
- “● Procedure C: Creating New SCS Project and Offline Download” on page C4-7
- “● Procedure E: Clean Project, Build, and Offline Download” on page C4-8
- “● Procedure F: Setting Definition Items for New Features, Clean Project, Build, and Offline Download” on page C4-9

#### ● New I/O Module (SDV53A)

To use the I/O module SDV53A newly supported in R2.03, you need to perform “Procedure C.”

#### ● New Function Blocks in R2.03

To use the new FBs in R2.03, such as SYS\_SCANEXT (scan period extension indicator), you need to perform “Procedure C” on an SENG of R2.03 or later.

#### ● Online Change Download

From R2.03, the following changes can be made by online change download.

- Change the scan period
- Add or delete input/output modules
- Rename POU's
- Change the type and attributes of FB instances
- Change the definitions on SCS Constants Builder

To download these changes online, you need to perform “Procedure E” on an SENG of R2.03 or later.

#### SEE ALSO

For more information about online changes to SCS with R2.02 or earlier system program, refer to:

“■ Online Changeable Information” on page App.4-26

- **Inter-SCS Safety Communication Locking Functions**

To use the functions for locking inter-SCS safety communication, you need to perform “Procedure E” on an SENG of R2.03 or later. However, if you also want to use the new system FB of SYS\_FORCE\_EB (inter-SCS safety communication forcing status management), you need to perform “Procedure C.”

- **Automatic IOM Download**

To use automatic IOM download, you need to perform “Procedure F” on an SENG of R2.03 or later. Use the SCS Constants Builder and set so as to enable the automatic IOM download.

- **Automatic Scan Period Extension under High CPU Load**

To use automatic scan period extension, you need to perform “Procedure F” on an SENG of R2.03 or later. Use the SCS Constants Builder and set [Extend scan period automatically] to “Yes”. However, if you also want to use the new system FB of SYS\_SCANEXT (scan period extension indicator), you need to perform “Procedure C.”



## **IMPORTANT**

If you use automatic scan period extension in a system that does not include SCS Maintenance Support Tool on SENG or CENTUM HIS, you must perform “Procedure C” on an SENG of R2.03 or later. This is because, in such a system, you need to use the SYS\_SCANEXT FB (scan period extension indicator) to detect whether the SCS is running with an automatically-extended scan period.

---

- **Specifying Behavior at Abnormal Calculation**

To enable specification of the SCS behavior at abnormal calculation, you need to perform “Procedure F” on an SENG of R2.03 or later. Use the SCS Constants Builder and specify the behavior of the SCS at abnormal calculation. However, if you also want to use the new system FB of SYS\_CERR (computation error indicator), you need to perform “Procedure C.”

---



## **IMPORTANT**

If you want to specify the behavior of the SCS at abnormal calculation in a system that does not include SCS Maintenance Support Tool on SENG or CENTUM HIS, you must perform “Procedure C” on an SENG of R2.03 or later. This is because, in such a system, you need to use the SYS\_CERR FB (computation error indicator) to detect that the SCS is running even after abnormal calculation has occurred.

---

- **Improvement in SCS Software Performance**

To improve the software performance of SCSP1 or SCSV, you need to perform “Procedure B” on an SENG of R2.03 or later.

## ■ **Cautionary Note on Offline Download after Upgrading to R2.03.59**

If you try to offline download an existing project immediately after upgrading the ProSafe-RS software to R2.03, an error occurs. You need to run Clean Project and Build before offline downloading the project.



## Appendix 4.7.2 Compatibility with Earlier Revisions

This section describes the specifications and cautionary notes of SCS with a system program before R2.03 that are critical to safety as the information on compatibility. Read this section when you use SCS with a system program before R2.03.

### SEE ALSO

For more information about compatibility of software version R2.03.51 and earlier and SCS, refer to:

“■ Specification Changes Made in SCS System Program Release Number R2.03.51” on page App.4-31

### ■ Inter-SCS Safety Communication

The Inter-SCS Communication Lock Window is not available.

For testing of inter-SCS safety communication and maintenance, internal variables should be connected to the OUT of consumer inter-SCS safety communication FBs and the application should read the values of these internal variables. During testing and maintenance, you need to lock the connected variables as necessary.

### ■ Online Changeable Information

The online changeable information in SCS with a system program before R2.03 is as follows.

#### ● POU Information that is Changeable Online

Table Appendix 4.7.2-1 POU Information

| Modification                                                                              | Online Change (*1) |                 |                 |
|-------------------------------------------------------------------------------------------|--------------------|-----------------|-----------------|
|                                                                                           | Program            | User-Defined FB | User-Defined FU |
| Adding/deleting variables                                                                 | Yes                | Yes (*2)        | Yes (*3)        |
| Adding a variable to be named the same as that of a deleted variable                      | No                 | No              | No              |
| Changing attributes of variables                                                          | No                 | No              | No              |
| Adding/deleting I/O variables                                                             | Yes                | -               | -               |
| Adding/deleting FU                                                                        | Yes                | Yes             | Yes             |
| Adding/deleting user-defined FU (*4)                                                      | Yes                | Yes             | Yes             |
| Adding/deleting FB instances                                                              | Yes                | No              | -               |
| Adding/deleting user-defined FB (*4)                                                      | Yes                | No              | -               |
| Adding a FB to be named the same Instance as that of a deleted FB                         | No                 | -               | -               |
| Changing logic                                                                            | Yes                | Yes (*2)        | Yes (*2)        |
| Creating/deleting programs Changing program names                                         | No (*5)            |                 |                 |
| Creating/deleting user-defined Function Blocks Changing user-defined Function Block names | No (*5)            |                 |                 |
| Creating/deleting user-defined Functions Changing user-defined Function names             | No (*5)            |                 |                 |

\*1: Yes: Changeable by online change download.  
No: Offline download is required.

\*2: It is not allowed to increase/decrease parameter values or change attributes. They cause an error when the database is downloaded.

\*3: An error occurs during downloading.

\*4: When user-defined FU/FB are added, they need to be tested. Pre-validated user-defined FU/FB do not need to be tested.

\*5: Online change is only possible for local variables.

## ● I/O Module Information that is Changeable Online

Table Appendix 4.7.2-2 I/O Module Information

| Modification                                                     | Online Change (*1) |
|------------------------------------------------------------------|--------------------|
| Adding nodes                                                     | No                 |
| Deleting nodes                                                   | No                 |
| Changing parameters of nodes                                     | Yes                |
| Adding I/O modules                                               | No                 |
| Deleting I/O modules                                             | No                 |
| Changing redundant I/O modules                                   | No                 |
| Changing parameters of I/O modules                               | Yes                |
| Changing parameters of channels                                  | Yes                |
| Changing subsystem communication definitions                     | Yes                |
| Defining link between a variable and an idle channel             | Yes                |
| Deleting link between a channel and a variable                   | Yes                |
| Changing link between a channel and a variable                   | Yes                |
| Adding, changing or deleting subsystem communication definitions | Yes                |
| Changing wiring of communication input/output FBs                | Yes                |

\*1: Yes: Changeable by online change download.  
No: Offline download is required.

## ● Constants and Network Information that are Changeable Online

Table Appendix 4.7.2-3 Constants and Network

| Classification            | Modification                                   | Online Change (*1) |
|---------------------------|------------------------------------------------|--------------------|
| Configuration             | Name                                           | No                 |
|                           | Password                                       | No (*2)            |
| Resource                  | Name                                           | No                 |
|                           | Resource Number                                | No                 |
|                           | Scan period                                    | No                 |
|                           | Number of variables permitted for online       | No                 |
|                           | Size of temporary variables and constants area | No                 |
| Network                   | IP address                                     | No                 |
|                           | Station address                                | No                 |
|                           | Inter-SCS safety Communication (Binding)       | No                 |
| Optional ESB BUS Repeater | Optional ESB BUS Repeater                      | No                 |
|                           | Max. extension distance                        | No                 |

\*1: No: Offline download is required.

\*2: Setting and changing passwords is ignored.

## ● Builder Definitions that are Changeable Online

The following table shows whether online change downloading is possible after you have changed definitions using builders.

Table Appendix 4.7.2-4 Online Change Download

| Builders                       | Online Change (*1) |
|--------------------------------|--------------------|
| SCS Constants Builder          | No                 |
| I/O Parameter Builder          | Yes                |
| Communication I/O Builder      | Yes                |
| SCS Link Transmission Builder  | Yes                |
| Modbus Address Builder         | Yes                |
| Tag Name Builder               | Yes                |
| Alarm Priority Builder         | No                 |
| Alarm Processing Table Builder | No                 |

\*1: Yes: Changeable by online change download.  
No: Offline download is required.

## ■ Behaviors at Abnormal Calculation in Application Logic

If abnormal calculation occurs in the application logic of an SCS with a system program before R2.03, the SCS stops.

### ● About Behaviors of SCS at Abnormal Calculation

- If an overflow or division by zero occurs in operations with REAL-type variables, or division by zero in operations with integer-type variables, SCS stops.
- When floating-point data is converted to a DINT number by the ANY\_TO\_DINT function, if the resultant number exceeds the maximum or falls below the minimum integer values (i.e. overflow occurs), the SCS stops.
- For the input to ANY\_TO\_TIME, use a DINT type value in the range from 0 to 86400000. If a value beyond this range is used, it cannot return a proper time. Note that when a real number value greater than 4294967295 (the maximum number of the unsigned 32-bit integer) or smaller than -2147483648 (the minimum number of the signed 32-bit integer) is used, the SCS stops.
- If access to the outside of an array occurs, the SCS stops.

## Appendix 4.8 Upgrading to Version R3.01

This section provides precautions to be made when upgrading the software version from R2.03 to R3.01. Please read precautions at upgrading revision of the software release number currently installed on the computer or earlier as well before starting the tasks of version upgrading to perform tasks required to upgrade each revision.



### IMPORTANT

In the case of system configuration integrating ProSafe-RS and CENTUM VP, it is possible to perform operation and monitoring of the newly added features of ProSafe-RS R3.01 correctly using CENTUM VP of R5.01 or later versions.

### SEE ALSO

For more information about the operations related to the functions newly added in the ProSafe-RS software version R3.01 when ProSafe-RS is integrated with CENTUM VP or CS 3000 of R5.01 or earlier revisions, refer to:

Appendix 1., "Differences in limitations and specifications among software release numbers of CENTUM" in Integration with CENTUM VP/CS 3000 (IM 32Q01E10-31E)

## ■ Software Revisions

The respective software release number of R3.01 is as follows:

Software Release R3.01.xx (\*1)

- SENG software release number: R3.01.xx (\*1)
- SCS system program release number: R3.01.xx (\*1)

\*1: xx will be changed in accordance with the software revisions after the release of R3.01.00.

### ● Inter-SCS Safety Communication

The release number of the SCS system program of an SCS that performs Inter-SCS safety communication with an SCS with system program version R2.0 must be of R1.01.30 or later.

If Vnet/IP is used for route of the Inter-SCS safety communication, the system programs on the SCSs must be of R1.02 or later.

### ● Control Bus Drivers

The control bus drivers installed on the computer should be upgraded to the version supplied in R3.01.

The control bus driver of ProSafe-RS R3.01 is compatible with the control bus driver supplied with CENTUM VP R5.01.

## ■ Basic Procedure of Revision Upgrading

In order to use the features added or modified, install the ProSafe-RS software R3.01 or later and open the existing SCS project.

### SEE ALSO

For more information about cautionary notes for opening existing SCS projects, refer to:

“● Procedure A: Opening SCS Projects” on page C4-6

## Appendix 4.8.1 Cautionary Notes for Upgrading

### ■ Procedure for Using New and Modified Features

After the SENG software has been upgraded to R3.01, some of the features added or modified in the R3.01 require performing further tasks, such as offline downloading to SCS, before they can be used. In the following, the steps are explained for each feature.

**SEE  
ALSO**

For more information about "Procedure B" and "Procedure C" that appear in this section, refer to:

- "● Procedure B: Master Database Offline Download" on page C4-6
- "● Procedure C: Creating New SCS Project and Offline Download" on page C4-7

#### ● New I/O Modules (SAT145 and SAR145)

To use the Input Modules that are supported by the R3.01, you must follow the "Procedure C" on SENG in R3.01 or later.

#### ● Support for Real Value Entry to ANLG1002D/ANLGVOTER

In order to enter real values to ANLG1002D/ANLGVOTER, you need to perform "Procedure B" on an SENG R3.01 or later.

## Appendix 4.8.2 Compatibility with Earlier Revisions

This section describes the specifications and precautions of SCS with a system program before R3.01 that are critical to safety as the information on compatibility. Please read this section if you use SCS with a system program before R3.01.

### ■ Function Block Parameters

The function block operation specifications have been changed in the SCS system program release number R3.01.

#### ● Support for Analog Input Modules for Thermocouple/RTD

In revisions earlier than R3.01, the following function blocks were able to handle normalization data from 0 to 100% only with their parameters.

Table Appendix 4.8.2-1 Function Blocks whose Parameters were Changed in R3.01

| Function block | Parameter                    |
|----------------|------------------------------|
| ANLG1002D      | IN1, IN2, DEL, VAL, OUT      |
| ANLGVOTER      | IN1, IN2, IN3, DEL, VAL, OUT |
| ANLG_S         | IN, HYS                      |
| ANLGI          | IN, HYS                      |
| VEL            | IN, VL, HYS                  |

#### ● ANLG1002D

Due to the specification changes of ANLG1002D parameters, the operations of VAL on SCS are changed as shown in the following table.

Table Appendix 4.8.2-2 Specification of VAL

| Earlier than R3.01                                                                                                                                      | R3.01 or later                                                       |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| -25 to 125%. If you specify a value smaller than -25.0%, it is processed as -25.0%. If you specify a value greater than 125%, it is processed as 125 %. | Specify as % or engineering units (no restrictions on range in VAL). |

#### ● ANLGVOTER

Due to the specification changes of ANLGVOTER parameters, the operations of VAL on SCS are changed as shown in the following table.

Table Appendix 4.8.2-3 Specification of VAL

| Earlier than R3.01                                                                                                                                      | R3.01 or later                                                       |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| -25 to 125%. If you specify a value smaller than -25.0%, it is processed as -25.0%. If you specify a value greater than 125%, it is processed as 125 %. | Specify as % or engineering units (no restrictions on range in VAL). |

### ■ Specification Changes Made in SCS System Program Release Number R2.03.51

#### ● Overview of Specification Changes

After the SCS system program release number R2.03.51, information on system time is no longer used to diagnose delay in inter-SCS safety communication and SCS link transmission safety communication. Specifically, there is no need to consider the gap in the system times of related SCSs when determining the DLYT value.



## IMPORTANT

In order to operate inter-SCS safety communication and SCS link transmission safety communication with the specification of R2.03.51 or later, upgrade the revision of all SCS system programs that communicate each other to R2.03.51 or later. If either the revision of the transmission or reception side has not been upgraded, the system operates with the method before the change, which uses the system time for diagnosis of delay. If the communication is performed with the method before the change, take the gap in the system times among involved SCSs as the DLYT value as in the past.

### ● Calculation Method of DLYT in Inter- SCS Safety Communication

How to calculate DLYT in inter-SCS safety communication in case of revisions earlier than R2.03.51 is explained below.

Reception interval timeout value (OUTT) and inter-FB transmission delay timeout value (DLYT) are used to set the timeout monitoring time of inter-SCS safety communication.

Temporary transmission delay errors can be detected by monitoring the communication with OUTT. In addition, you can set DLYT to detect constant transmission delay errors.

DLYT detects not only transmission delay but also time gap among SCSs. For this reason, determine the set value of DLYT taking generation of erroneous trips due to time gap into consideration as well.

- Reception interval timeout value (OUTT)  
An FB for communication on the consumer side (CONS\_\*) checks the interval of data reception. If the data reception interval exceeds the reception interval timeout value (OUTT), a communication error occurs and a failsafe value (VAL) is output.
- Transmission delay timeout value (DLYT)  
DLYT checks the time from the time an FB for communication on the producer side (PROD\_\*) transmits data to the time an FB for communication on the consumer side (CONS\_\*) receives the data. This time interval is called inter-FB transmission delay time. If the status where this interval exceeds the inter-FB transmission delay timeout value (DLYT) of CONS\_\* continues for the time indicated by OUTT, a communication error occurs and a failsafe value (VAL) is output.

The guidelines of timeout value settings are given in the following.

- Setting of Reception Interval Timeout Value (OUTT)

$OUTT = (\text{select the longer scan period of either the producer or the consumer}) \times 8 + (\text{Additional Delay})$

Additional Delay

V net Delay

No BCV/CGW used: 0 s

Via BCV/CGW: the number of BCV used  $\times$  1 s +  
the number of pairs of CGWs used  $\times$  2 s

Vnet/IP Delay

Within a Vnet/IP domain: 0 s

Between Vnet/IP domains (No wide area network):  
0 s (Regardless of the number of L3SWes)

Between Vnet/IP domains (Wide area network):  
1 s (Regardless of the number of L3SWes)

Vnet/IP – V net: V net delay + Vnet/IP delay + V net router delay (1 s)

V net(1) – Vnet/IP – V net(2): V net(1) delay + Vnet/IP delay + V net(2) delay +  
Two V net routers' delay (2 s)

Set 3 seconds to OUTT when the calculated OUTT is shorter than 3 seconds.

- Setting of the Transmission Delay Timeout Value (DLYT)

1. In cases of Inter-SCS safety communications between:

- SCSs in the same domain
- SCSs synchronized with GPS time
- SCSPs synchronized with a Vnet/IP network time
- An SCSP synchronized with SNTP server and an SCSV synchronized with GPS time:

$DLYT = (\text{scan period of the producer}) + (\text{scan period of the consumer}) + (\text{Additional Delay})$

Additional Delay

V net Delay

No BCV/CGW used: 300 ms

Via BCV/CGW: the number of BCV used  $\times$  1.3 s +  
the number of pairs of CGWs used  $\times$  2.3 s

Vnet/IP Delay

Within a Vnet/IP domain: 300 ms

Between Vnet/IP domains (No wide area network):  
300 ms (Regardless of the number of L3SWes)

Between Vnet/IP domains (Wide area network):  
1.3 s (Regardless of the number of L3SWes)

Vnet/IP – V net: V net delay + Vnet/IP delay + V net router delay (1.3 s)

V net(1) – Vnet/IP – V net(2): V net(1) delay + Vnet/IP delay + V net(2) delay +  
Two V net routers' delay (2.6 s)

Set 3 seconds to DLYT when the calculated DLYT is shorter than 3 seconds.

2. In case of Inter-SCS safety communications between SCSs synchronized with V net time in SCS in different domains:

$DLYT = (\text{the number of BCV used}) \times 5 \text{ s}$

3. If there are V net routers between SCSs synchronized with V net time in the Inter-SCS safety communications,

$DLYT = (\text{BCV/number of V net router layers}) \times 5 \text{ s}$





## IMPORTANT

If you set 0 seconds to DLYT and bypass inter-FB transmission check, it is not possible to use reception data of the given inter-SCS safety communication for the safety purpose.

- In both cases, set the value of OUTT as the DLYT value if OUTT is smaller than DLYT.
- The timeout value is used for calculating system reaction time.

### ● Precautions when Setting DLYT for Inter- SCS Safety Communication

Precautions to be followed when setting DLYT for inter-SCS safety communication in software versions R2.03.51 or earlier are given below.

- If IRIG-B time synchronization method is selected, be sure to take the time gap due to failure of GPS and IRIG-B interface into consideration.
- In the case of SCSs connected to Vnet/IP, time gap due to the SNTP server must be taken into consideration.
- Unify the time synchronization method among SCSs that perform inter- SCS safety communication and determine the setting value such that erroneous trips do not occur due to time gap among SCSs.

If you set DLYT among SCSs over multiple domains, the following points must also be taken into consideration.

- If V net time synchronization method is selected, delay of up to 5 seconds in the first level of BCV-V and 10 seconds in the second level may occur. It is recommended to select IRIG-B time synchronization if it is found that the gap is outside the allowable range.
- If domains are connected via a gateway for broadband connection, it is recommended to synchronize V net time of each domain within the allowable range or select IRIG-B time synchronization.

### ● Precautions when Setting DLYT for SCS Link Transmission Safety Communication

How to calculate DLYT of SCS link transmission safety communication for revisions R2.03.51 or earlier is explained below.

Reception interval timeout value (reception timeout, hereinafter referred to as OUTT) and inter-SCS transmission delay timeout value (transmission timeout, hereinafter referred to as DLYT) are used to set the timeout monitoring time of SCS link transmission safety communication.

Temporary transmission delay errors can be detected by monitoring the communication with OUTT. In addition, you can set DLYT to detect constant transmission delay errors.

DLYT detects not only transmission delay but also time gap among SCSs. For this reason, determine the set value of DLYT taking generation of erroneous trips due to time gap into consideration as well.

- Reception interval timeout value (OUTT)  
It is valid only when the station on the transmission side is an SCS.

The reception interval refers to the time interval of receiving data by an SCS. Specify the reception interval timeout value (OUTT) for each communication target. If normal data cannot be received within the reception interval timeout value (OUTT), a communication error occurs and a failsafe value is output.

- Inter-SCS transmission delay timeout value (DLYT)  
It is valid only when the station on the transmission side is an SCS.

Inter-SCS transmission delay time is the time duration from the time an SCS on the transmission side sends data to the time an SCS on the reception side receives the data. If the inter-SCS transmission delay timeout value exceeds the DLYT timeout value and the status continues for the time specified by OUTT or longer, a communication error occurs and a failsafe value is output.

The guidelines of timeout value settings are given in the following.

- Setting of reception interval timeout value (OUTT)  
 $\text{OUTT} = (\text{Scan frequency on the transmission or reception side, whichever longer}) \times 8$   
If OUTT is 3 seconds or less, set 3 seconds.
- Guidelines of setting value of transmission delay timeout value (DLYT)  
If the time synchronization method employed is V net time synchronization or Vnet/IP time synchronization, set 3 seconds for DLYT.

In the case of IRIG-B time synchronization, determine DLYT as follows:

$\text{DLYT} = (\text{Scan frequency on transmission side}) + (\text{Scan frequency on the reception side}) + (\text{Delay addition}) + (\text{Time gap addition})$

Delay addition: 100 ms

Time gap addition: Determine the setting value so that erroneous trips do not occur due to time gap.

If DLYT is 3 seconds or less, set 3 seconds.

If 0 seconds are set for DLYT, checking of transmission delay by DLYT is bypassed.

## Appendix 4.9 Upgrading to Version R3.02.00

This section provides cautionary notes for upgrading from R3.01 to R3.02.00. Before you upgrade, also read the cautionary notes for upgrading to the previous versions that were issued after the software version currently installed on your computer and perform the required tasks for each upgrade.



### IMPORTANT

When integrating ProSafe-RS with CENTUM VP, it is recommended that the version of CENTUM VP is R5.02.00 or later.

## ■ Software Revisions

The respective software release number of R3.02 is as follows:

Software Release R3.02.xx (\*1)

- SENG software release number: R3.02.xx (\*1)
- SCS system program release number: R3.02.xx (\*1)

\*1: xx will be changed in accordance with the software revisions after the release of R3.02.00.

### ● Inter-SCS Safety Communication

The release number of the SCS system program of an SCS that performs Inter-SCS safety communication with SCS with system program version R3.02 must be R1.01.30 or later.

If Vnet/IP is used for route of the Inter-SCS safety communication, the system programs on the SCSs must be of R1.02 or later.

### ● Control Bus Driver

You do not need to update the control bus driver if the control bus driver provided in R3.01 is installed on the computer.

The control bus driver of ProSafe-RS R3.01 is compatible with the control bus driver provided in CENTUM VP R5.01 and R5.02.

## ■ Basic Procedure of Revision Upgrading

In order to use the features added or modified, install the ProSafe-RS software R3.02 or later and open the existing SCS project.

When you open a password-protected SCS project, the security of the password is strengthened.

### SEE ALSO

For more information about cautionary notes for opening existing SCS projects, refer to:

- “● Procedure A: Opening SCS Projects” on page C4-6

## Appendix 4.9.1 Cautionary Notes for Upgrading

### ■ Procedure for Using New and Modified Features

After the SENG software has been upgraded to R3.02.00, some of the features added or modified in R3.02.00 require performing further tasks, such as offline downloading to SCS, before they can be used. In the following, the steps are explained for each feature.

**SEE  
ALSO**

For more information about "Procedure B," "Procedure C," and "Procedure D" that appear in this section, refer to:

- "● Procedure B: Master Database Offline Download" on page C4-6
- "● Procedure C: Creating New SCS Project and Offline Download" on page C4-7
- "● Procedure D: Setting Definition Items for New Features and Offline Download" on page C4-8

#### ● Ethernet Communication Module (ALE111) and Modbus TCP Slave Communication

To use the Ethernet communication module (ALE111) newly supported in R3.02 to perform Modbus slave communication over the Modbus TCP protocol, you need to perform "Procedure C" on an SENG of R3.02.00 or later.

#### ● Writing to a Single Holding Register by Modbus Slave Communication

To enable writing to a single holding register in SCS, which is a Modbus slave, from a Modbus master, you need to perform "Procedure D" on an SENG of R3.02.00 or later.

#### ● IOM Reset Function

To use the IOM reset function, you need to perform "Procedure B" on an SENG of R3.02.00 or later.

### ■ Cautionary Note on Upgrading the OS from Windows XP/Windows Server 2003

Note the following point if your upgrading of the ProSafe-RS software involves upgrading the OS from Windows XP/Windows Server 2003 to a later version OS:

If any of the values comprising an IP address of SCS is set to a value where 0 is in the upper digit and 8 or 9 is contained in the lower digits, for example, 08 and 09, on the Connection Properties dialog box in Workbench of the SENG software, the SENG can communicate with the SCS properly as long as the SENG is running on Windows XP/Windows Server 2003. With a later version OS, an error will occur in the following operations:

- Online change download
- Starting the I/O lock window
- Starting the debug mode
- Checking by the Database Validity Check Tool

To enable proper operation, delete 0 in the upper digit and perform an offline download.

### ■ Cautionary Notes on Upgrading the SCS SOE OPC Server

When the Standard model of IT security settings are applied, the authentication level of COM is set to "Connect" during upgrading to R3.02. Because of this, some client programs may become unable to connect to the SCS SOE OPC server.

---

If any client program has become unable to establish connection after the upgrading, set the authentication level of COM to "None" on the SCS SOE OPC server to enable connection.

**TIP**

If any other YOKOGAWA product coexists on the same computer, the authentication level of COM may be set to "None" according to the operational specifications of the other product.

---

**SEE  
ALSO**

For more information about how to set the authentication level of COM on the SCS SOE OPC server, refer to:

“■ DCOM settings” in A2.2, “Overview of product security settings” in Open Interfaces (IM 32Q05B10-31E)

---

## Appendix 4.10 Upgrading to R3.02.10

This section provides cautionary notes for upgrading from R3.02.00 to R3.02.10. Before you upgrade, also read the cautionary notes for upgrading to the previous versions that were issued after the software version currently installed on your computer and perform the required tasks for each upgrade.



### IMPORTANT

When integrating ProSafe-RS with CENTUM VP, the recommended version of CENTUM VP is R5.03.00 or later.

## ■ Software Revisions

The respective software release number of R3.02 is as follows:

Software Release R3.02.10 (\*1)

- SENG software release number: R3.02.10 (\*1)
- SCS system program release number: R3.02.10 (\*1)

\*1: The last two digits of the release number will be changed in accordance with the software revisions after the release of R3.02.10.

### ● Inter-SCS Safety Communication

The release number of the SCS system program of an SCS that performs Inter-SCS safety communication with SCS with system program version R3.02.10 must be R1.01.30 or later.

If Vnet/IP is used for route of the Inter-SCS safety communication, the system programs on the SCSs must be of R1.02 or later.

### ● Control Bus Driver

The control bus drivers installed on the computer should be upgraded to the version supplied in R3.02.10. In particular, the control bus driver must be upgraded when ProSafe-RS is integrated with FAST/TOOLS and used in the Narrowband mode of Vnet/IP-Upstream.

## ■ Basic Procedure for Upgrading

In order to use the features added or modified, install the ProSafe-RS software R3.02.10 or later and open the existing SCS project. For the features that require further procedures, the procedures are described in the following section.

## Appendix 4.10.1 Cautionary Notes for Upgrading

### ■ Procedure for Using New and Modified Features

After the SENG software has been upgraded to R3.02.10, some of the features added or modified in R3.02.10 require further steps, such as offline downloading to SCS, before they can be used. In the following, the steps are explained for each feature.

#### ● New Station (SSC57)

To use the SSC57 station, which is newly added in R3.02.10, you need to perform "Procedure C" on an SENG of R3.02.10 or later. With SSC57, the Narrowband mode of Vnet/IP-Upstream, gas flow rate calculation, data buffering, etc. are available.

#### ● Calculation Functions and Time Synchronization Function Block

To use the calculation functions (LOGE and POWE) and time synchronization function block (SYS\_SETTIME) newly added in R3.02.10, you need to perform "Procedure C" on an SENG of R3.02.10 or later.

#### ● Change in the Specification of SCS Behavior at Both Bus Failure of Vnet/IP

To enable the revised SCS behavior at both bus failure of Vnet/IP, you need to perform "Procedure D" on an SENG of R3.02.10 or later.

#### ● 16-bit Modbus Master Support Mode

To read and write data in 16-bit units in Modbus slave communication, you need to perform "Procedure D" on an SENG of R3.02.10 or later.

## Appendix 4.10.2 Compatibility with Earlier Revisions

This section describes the specifications and precautions of SCS with a system program before R3.02.10 that are critical to safety as the information on compatibility. Please read this section if you use SCS with a system program before R3.02.10.

### ■ Specification of SCS Constant "Writing to a Single Holding Register" has been Changed in R3.02.10

"Writing to a Single Holding Register" is a setting item of SCS Constants Builder that was added in R3.02.00. In R3.02.10, the specification of this setting item has been changed as follows:

- The item name has been changed from "Writing to a Single Holding Register" to "16-bit Modbus master support mode".
- When "16-bit Modbus master support mode" is set to Disable, there is no difference in the behavior between R3.02.00 and R3.02.10.
- The following table describes the behaviors when the SCS system program release number is R3.02.00 and when the SCS system program release number is R3.02.10 with "16-bit Modbus master support mode" set to Enable. There is no difference in writing to a Preset Single Register between R3.02.00 and R3.02.10.

**Table Appendix 4.10.2-1 SCS System Program Release Number and the Behavior when "16-bit Modbus master support mode" is Set to "Enable"**

| SCS system program release number | Behavior when "16-bit Modbus master support mode" is set to "Enable"                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| R3.02.00 (*1)                     | <ul style="list-style-type: none"> <li>• Preset Single Register (function code 06) is available.</li> <li>• If a multiple-register read/write command (function code 03, 04, or 16) is used specifying an even number for the beginning reference number or an odd number for the size of data, the error code 10 or 11 (hex.) is returned.</li> </ul>                                                                                                                                                      |
| R3.02.10                          | <ul style="list-style-type: none"> <li>• Preset Single Register (function code 06) is available.</li> <li>• Data access is possible by using multiple-register read/write commands (function codes 03, 04, and 16) specifying an even number for the beginning reference number and/or an odd number for the size of data. Error code 10 or 11 (hex.) is not returned even if an even number is specified for the beginning reference number or an odd number is specified for the size of data.</li> </ul> |

\*1: This means the case when the version of SENG is R3.02.00 and the case when SENG is upgraded to R3.02.10 but offline downloading to SCS is not yet performed.



# Revision information

Title : Installation  
Manual No. : IM 32Q01C50-31E

## Jan. 2015/4th Edition/R3.02.20 or later\*

\*: Denotes the release number of the Software Product corresponding to the contents of this Manual. The revised contents are valid until the next edition is issued.

- |              |                                                                                                                                     |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Introduction | ProSafe-RS document map has been removed, descriptions of "Safety, Protection, and Modification of the Product" have been modified. |
| A3           | Software version has been changed, use of Exaquantum has been added.                                                                |
| A3, C4.2     | Descriptions of Windows Server 2003 and Windows Server 2003 R2 have been deleted.                                                   |
| A3, C8.1.1   | Contents have been restructured.                                                                                                    |
| B2.3         | Descriptions of Windows Server 2008 have been changed.                                                                              |
| B5.1         | Descriptions of Windows Server 2003 have been deleted, and descriptions of Windows Server 2008 have been changed.                   |
| C5           | Descriptions of updating to R3.02.20 have been added.                                                                               |
| D1           | Descriptions of connection with other products, and the integration code have been changed.                                         |

## Oct. 2013/3rd Edition/R3.02.10 or later

- |              |                                                                                          |
|--------------|------------------------------------------------------------------------------------------|
| Introduction | Description of station types has been changed.                                           |
| A3           | Version numbers of the software products that can coexist have been changed.             |
| B1           | Descriptions of connection with other products have been added.                          |
| B3.2, B3.8   | Descriptions for different OSs have been arranged into separate subsections for each OS. |
| C4.2         | Descriptions of the procedures after updating the software have been changed.            |
| C5           | Descriptions of updating to R3.02.10 have been added.                                    |
| D            | Descriptions of connection with other products have been entirely revised.               |

## Dec. 2013/2nd Edition/R3.02 or later

The entire manual has been revised.

## Aug. 2011/1st Edition/R3.01 or later

Newly published

---

■ For Questions and More Information

Online Query: A query form is available on the following URL for online query.

<http://www.yokogawa.com/iss>

■ Written by Yokogawa Electric Corporation

■ Published by Yokogawa Electric Corporation  
2-9-32 Nakacho, Musashino-shi, Tokyo 180-8750, JAPAN

---