



CENTUM VP

Installation

IM 33J01C10-01EN

IM 33J01C10-01EN
9th Edition

Introduction

This manual provides the procedures for setting up CENTUM VP.

This manual consists of the following parts:

- PART-A Overview
This part provides the overview of CENTUM VP setup.
- PART-B New Setup
This part describes the procedure for a new setup of the CENTUM VP.
- PART-C Maintenance
This part describes the tasks to be done while CENTUM VP system is used.
- PART-D Connection with Other Products
This part describes how to connect the other YOKOGAWA products and cautionary notes for it .

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.
- Be sure to confirm the specifications and required settings of the devices that are used in combination with the Product by referring to the instruction manual or other documents of the devices.
- 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. This symbol for the Product indicates the possibility of dangers such as electric shock on personnel and equipment, and also indicates that the user must refer to the User's Manuals for necessary actions. In the User's Manuals, this symbol is used together with a word "CAUTION" or "WARNING" at the locations where precautions for avoiding dangers are described.

<French> Signale qu'il faut faire preuve de prudence. Ce symbole pour le produit signale la possibilité d'un danger pour le personnel et l'équipement comme un choc électrique, et signale également que l'utilisateur doit se référer au Manuel de l'utilisateur afin de prendre les mesures nécessaires. Dans le Manuel de l'utilisateur, ce symbole est utilisé conjointement avec la mention «CAUTION» ou «WARNING» aux endroits où sont décrites les précautions pour éviter les dangers.



Indicates that caution is required for hot surface. Note that the devices with this symbol become hot. The risk of burn injury or some damages exists if the devices are touched or contacted.

<French> Signale qu'il faut faire preuve de prudence avec la surface brûlante. Les appareils sur lesquels est apposé ce symbole risquent de devenir brûlants. Tout contact physique ou matériel avec ces appareils risque de provoquer des brûlures ou des dommages.



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 that a component such as a power supply switch is turned ON.
 - Indicates that a component such as a power supply switch is turned OFF.

■ 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.



WARNING

Indicates precautions to avoid a danger that may lead to death or severe injury.



CAUTION

Indicates precautions to avoid a danger that may lead to minor or moderate injury or property damage.

IMPORTANT

Indicates important information required to understand operations or functions.

TIP

Indicates additional information.

SEE ALSO

Indicates 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**

- Character string to be entered

The characters that must be entered are shown in monospace font as follows:

Example:

FIC100.SV=50.0

- ▼ Mark

This symbol indicates the description for an item for which you should make a setting in the product's engineering window.

While operating an engineering window, the help information for the selected item can be accessed from "Builder Definition Items" in the Help menu. Listing more than one definition item after this symbol implies that the paragraph on the page describes more than one definition items.

Example:

▼ Tag Name, Station Name

- Δ Mark

Indicates that a space must be entered between character strings.

Example:

.AIΔPIC010Δ-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 key on the operation 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 Used in Command Syntax or Program Statements

The following conventions are used within a command syntax or program statement format:

- Characters enclosed by angle brackets < >

Indicate character strings that user can specify freely according to certain guidelines.

Example:

```
#define <Identifier> <Character string>
```

- "..."

Indicates previous command or argument that may be repeated.

Example:

```
lmax (arg1, arg2, ...)
```

- Characters enclosed by brackets []

Indicate character strings that may be omitted.

Example:

```
sysalarm <format character string> [, <output value>...]
```

- Characters enclosed by separators ||

Indicates character strings that can be selected from more than one option.

Example:

opeguide	<format character string> [, <output value>...]	
	OG, <element number>	

■ 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.

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 Acknowledgements

- CENTUM, ProSafe, Vnet/IP, PRM, Exaopc, Exapilot, Exaquantum, Exasmoc, Exarqe, Multivariable Optimizing Control/Robust Quality Estimation, StoryVIEW and FieldMate Validator are the registered trademarks or trademarks of Yokogawa Electric Corporation.
- The names of corporations, organizations, products and logos herein are either registered trademarks or trademarks of Yokogawa Electric Corporation and their respective holders.

CENTUM VP Installation

IM 33J01C10-01EN 9th 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 CENTUM VP System.....	A2-4
A2.2.2 Setup Procedure for a Virtualization Platform-based CENTUM VP System.....	A2-6
A2.2.3 Setup Procedure for HIS.....	A2-8
A2.2.4 Setup Procedure for APCS.....	A2-9
A2.2.5 Setup Procedure for SIOS.....	A2-10
A2.2.6 Setup Procedure for GSGW.....	A2-11
A2.2.7 Setup Procedure for a Computer Installed with Only System Builders.....	A2-12
A2.2.8 Setup Procedure for a Computer Installed with Only AD Server.....	A2-13
A2.2.9 Setup Procedure for HIS-TSE.....	A2-14
A2.2.10 Setup Procedure for a File Server.....	A2-15
A2.2.11 Setup Procedure for a Computer Dedicated to License Management	A2-16
A2.2.12 Setup Procedure for Computer Switchover Type UGS.....	A2-17
A2.2.13 Setup Procedure for a UACS station.....	A2-19
A2.3 Explanation for Maintenance.....	A2-20
A3. Requirements for Operation.....	A3-1

Blank Page

CENTUM VP Installation

IM 33J01C10-01EN 9th Edition

CONTENTS

PART-B New Setup.....	B-1
B1. Preparing for the Setup.....	B1-1
B2. Setting Up the Windows Domain Environment.....	B2-1
B2.1 Overview of Setting Up the Domain Environment.....	B2-2
B2.2 Configuring the Domain Controller (Windows Server 2016/Windows Server 2012 R2).....	B2-5
B2.3 Configuring the Domain Controller (Windows Server 2008 R2/Windows Server 2008).....	B2-7
B2.4 Configuring Security Settings for the Domain Controller.....	B2-9
B2.5 Creating Domain Users.....	B2-16
B2.6 Adding Client Computers to the Domain.....	B2-21
B2.7 Setting Up Redundant Domain Controllers.....	B2-27
B2.8 Setting Up Time Synchronization in Windows Domain Environment.....	B2-28
B2.8.1 Implementing Time Synchronization Considering Security.....	B2-29
B2.8.2 Implementing Time Synchronization with Lower Introduction Cost.....	B2-31
B3. Setting Up the Hardware of FCS/Bus Converter/V net Router/CGW/WAC Router.....	B3-1
B3.1 Configurations for FCS.....	B3-2
B3.2 Configurations for Bus Converters.....	B3-5
B3.3 Configurations for V net Routers.....	B3-11
B3.4 Configurations for the Communication Gateway Unit.....	B3-13
B3.5 Configurations for Wide Area Communication Routers.....	B3-15
B3.6 Configurations for N-IO Node Interface Unit.....	B3-17
B3.6.1 Specifying the node number by using Node Number Setting Tool.....	B3-18
B3.6.2 Switching enabled/disabled of the maintenance port.....	B3-22
B4. Setting Up CENTUM Stations or Computers.....	B4-1
B4.1 Setting Up the Hardware.....	B4-2
B4.2 Setting Up Windows.....	B4-7
B4.2.1 Configuring on Windows 10.....	B4-8
B4.2.2 Configuring on Windows 7.....	B4-15
B4.2.3 Configuring on Windows Server 2016.....	B4-24

B4.2.4	Configuring on Windows Server 2012 R2.....	B4-30
B4.2.5	Configuring on Windows Server 2008 R2.....	B4-36
B4.3	Configuring Network Settings.....	B4-43
B4.3.1	Installing the Control Bus Driver.....	B4-44
B4.3.2	Installing the Vnet/IP Open Communication Driver.....	B4-46
B4.3.3	Installing the Vnet/IP Interface Package on a Virtual Machine.....	B4-48
B4.3.4	Configuring Windows Network Settings.....	B4-51
B4.3.5	Usage Notes for CENTUM VP Entry Class.....	B4-71
B4.3.6	Usage Notes for Computer Switchover Type UGS.....	B4-73
B4.3.7	Notes on Using a Virtual Machine.....	B4-75
B4.4	Installing the USB Driver for the Operation Keyboard.....	B4-77
B4.5	Tasks Required for Setting Up the Console Type HIS.....	B4-79
B4.6	Installing the CENTUM VP Software.....	B4-85
B4.7	Configuring IT Security Settings.....	B4-94
B4.8	Distributing and Accepting Licenses.....	B4-101
B4.9	Creating User Accounts.....	B4-102
B4.9.1	When the Standard Model with Standalone Management Security Settings are Applied.....	B4-103
B4.9.2	When the Legacy Model of Security Settings are Applied.....	B4-105
B4.10	Configuring Windows Environment Settings for Each User.....	B4-107
B4.10.1	Configuring on Windows 10.....	B4-108
B4.10.2	Configuring on Windows 7.....	B4-116
B4.10.3	Configuring on Windows Server 2016.....	B4-121
B4.10.4	Configuring on Windows Server 2012 R2.....	B4-128
B4.10.5	Configuring on Windows Server 2008 R2.....	B4-130
B4.11	Setting Up for User Authentication Modes.....	B4-135
B4.11.1	Setting CENTUM Authentication Mode.....	B4-137
B4.11.2	Setting Windows Authentication Mode.....	B4-139
B4.11.3	Notes for User Authentication Mode.....	B4-148
B4.12	Setting Up the Uninterruptible Power Supply (UPS) Service.....	B4-149
B5.	Setting Up the Remote Operation and Monitoring Function.....	B5-1
B5.1	Setting Up the HIS-TSE Server.....	B5-4
B5.1.1	Configuring on Windows Server 2016.....	B5-5
B5.1.2	Configuring on Windows Server 2008 R2.....	B5-20
B5.2	Setting Up HIS-TSE Clients.....	B5-45
B6.	Setting Up a File Server.....	B6-1
B6.1	Setting Up a Computer that Serves Only as a File Server.....	B6-3
B6.2	Setting Up the File Server Function on an HIS, a Computer with Only System Builders or a Computer with Only AD Server.....	B6-11
B6.3	Setting Up the Computer that Serves as Both File Server and License Management Station.....	B6-12

B7.	Setting Up the Computer Dedicated to License Management.....	B7-1
B8.	Setting Up a Virtualization Environment.....	B8-1
B8.1	SIOS.....	B8-2
B8.2	HIS.....	B8-3
B8.2.1	Settings for Using USB Devices.....	B8-4
B8.2.2	Settings for Limiting Maximum Number of Connections.....	B8-9
B8.2.3	Settings for Limiting Sessions Per User.....	B8-10
B8.2.4	Enabling Beep.....	B8-11
B8.2.5	Settings for Buzzer.....	B8-12
B8.3	HIS-TSE.....	B8-13
B8.3.1	Settings for Using USB Devices.....	B8-14
B8.3.2	Settings in the Guest OS on the Virtual Machine.....	B8-15
B8.3.3	Settings for Limiting Maximum Number of Connections.....	B8-18
B8.3.4	Settings for Limiting Sessions Per User.....	B8-19
B8.3.5	Settings for Application and Working Directory.....	B8-20
B8.3.6	Uninstalling HIS-TSE.....	B8-21
B8.4	SOE.....	B8-22
B8.4.1	Settings for Bandwidth.....	B8-23
B8.4.2	Settings for Limiting Maximum Number of Connections.....	B8-24
B8.4.3	Settings for Limiting Sessions Per User.....	B8-25
B8.4.4	Settings for Windows Network.....	B8-26

Blank Page

CENTUM VP Installation

IM 33J01C10-01EN 9th Edition

CONTENTS

PART-C Maintenance.....	C-1
C1. Adding Licenses and Changing License Assignments.....	C1-1
C1.1 Adding a License.....	C1-2
C1.2 Changing License Assignments.....	C1-3
C2. Changing the Location of Engineering Data for Reference.....	C2-1
C3. Setting Up the Windows Domain Environment Later.....	C3-1
C4. Changing from CENTUM Authentication Mode to Windows Authentication Mode.....	C4-1
C5. Backing Up the System.....	C5-1
C5.1 Backing Up the Entire Windows.....	C5-2
C5.2 Backing Up VP Projects.....	C5-3
C5.3 Backing Up the Customized Menu File.....	C5-4
C5.4 Backing Up the Database of CENTUM VP Operation and Monitoring Function.....	C5-5
C5.4.1 Backing Up Reports.....	C5-6
C5.4.2 Backing Up PICOT.....	C5-7
C5.5 Backing Up the Engineering Data Defined on CAMS for HIS Configurator.....	C5-8
C6. Upgrading the System.....	C6-1
C6.1 Upgrading from CENTUM CS 3000 to CENTUM VP R6.....	C6-2
C6.1.1 Procedures for the Upgrade.....	C6-3
C6.1.2 Backing up and Restoring CS 3000 Package Data.....	C6-8
C6.1.3 Backing up and restoring the CAMS for HIS data.....	C6-14
C6.2 Upgrading from CENTUM CS 1000 to CENTUM VP R6.....	C6-18
C6.2.1 Procedures for the Upgrade.....	C6-19
C6.2.2 Backing up and Restoring CS 1000 Package Data.....	C6-25
C6.3 Upgrading CENTUM VP R4/R5 to R6.....	C6-30
C6.4 Upgrading CENTUM R6 to a Later Revision.....	C6-40
C6.5 Upgrading the Computer Dedicated to License Management.....	C6-50
C6.6 Replacing the Operation Keyboard.....	C6-52
C6.7 Replacing the Card for Control Bus.....	C6-53
C7. Uninstalling the CENTUM VP Software.....	C7-1
C7.1 Uninstallation on the CENTUM Stations or Computers.....	C7-2

C7.1.1	Disabling the CENTUM Desktop Environment Settings.....	C7-3
C7.1.2	Restoring Various Windows Settings.....	C7-5
C7.1.3	Uninstalling the CENTUM VP Software.....	C7-10
C7.1.4	Uninstalling the Device Drivers.....	C7-13
C7.2	Uninstallation on the computer Dedicated to License Management.....	C7-20
C8.	Reinstalling the CENTUM VP Software.....	C8-1
C8.1	When the Computer Used is the Same.....	C8-2
C8.2	When the Computer Used is Not the Same.....	C8-5
C9.	Cases that Require Attention in IT Security Setting.....	C9-1
C9.1	Including CENTUM CS 3000 R3 HIS in a VP Project of CENTUM VP Standard Model.....	C9-2
C9.2	Including CENTUM VP HIS of Legacy Model in a VP Project of CENTUM VP Standard Model.....	C9-4
C9.3	Connecting Multiple Projects.....	C9-7
C9.3.1	Connecting CENTUM VP Project of Standard Model and CENTUM VP Project of Legacy Model.....	C9-8
C9.3.2	Connecting CENTUM VP Project and CENTUM CS 1000/CS 3000 R3 Project.....	C9-12
C9.3.3	Connecting CENTUM VP Project and CENTUM CS Project.....	C9-16
C9.4	Using a File Server or Domain Controller where IT Security Settings Were Configured on CENTUM VP R4.....	C9-17
C10.	Troubleshooting.....	C10-1
C10.1	Windows Related Troubleshooting.....	C10-2
C10.1.1	Note on User Account Control.....	C10-3
C10.1.2	Error Occurs when Server Manager is Started.....	C10-4
C10.1.3	Cannot Manage User Accounts in the User Accounts Dialog Box of Control Panel.....	C10-6
C10.1.4	Installed Update Programs are Not Displayed in the Programs and Features Window of Control Panel.....	C10-7
C10.1.5	Cannot Install Microsoft Updates.....	C10-8
C10.1.6	Failing to install .NET Framework.....	C10-9
C10.1.7	The System Locks Up.....	C10-10
C10.1.8	Computer Operation Becomes Unstable.....	C10-11
C10.1.9	Print Order Does Not Match the Spooled Order.....	C10-12
C10.2	Troubleshooting Related to Network.....	C10-13
C10.2.1	Precaution on Network Cable Connection.....	C10-14
C10.2.2	Problems Related to Installation and Deletion of Drivers.....	C10-15
C10.3	Troubleshooting Related to CENTUM Products.....	C10-23
C10.3.1	An Error Occurs when Downloading to an HIS after Changing Its IP Address.....	C10-24
C10.3.2	Failure to Connect to the Remote Operation and Monitoring Server..	C10-25

C10.3.3	AIP262 (AUX Board with USB Interface) USB Cable Disconnected from the Computer when Operation and Monitoring Function is Running.....	C10-26
C10.3.4	Shortcut to AD Organizer Disappeared from the Start Menu.....	C10-27
C11.	Cautionary Notes for Upgrading.....	C11-1
C11.1	Upgrading to R4.01.33.....	C11-2
C11.1.1	Setups After Installation.....	C11-7
C11.1.2	Setting Registry for R4.01.00 Compatibility.....	C11-9
C11.2	Upgrading to R4.01.60.....	C11-10
C11.2.1	Cautions Regarding Object Blinking on Graphic View.....	C11-11
C11.2.2	Selecting Actions of Graphic Objects.....	C11-12
C11.2.3	Number of Operation Windows.....	C11-13
C11.2.4	If Multiple-Monitor Support Package is used.....	C11-14
C11.2.5	Refresh Period of Views.....	C11-16
C11.2.6	Frame Color of Graphic Tag Objects.....	C11-17
C11.2.7	Operation Disabled Frame Color of Graphic Push Button and Softkey.....	C11-18
C11.2.8	Notice on Control Actions of Graphic View.....	C11-19
C11.3	Upgrading to R4.02.00.....	C11-20
C11.4	Upgrading to R4.02.30.....	C11-24
C11.5	Upgrading to R4.03.00.....	C11-25
C11.6	Upgrading to R5.01.00.....	C11-27
C11.7	Upgrading to R5.01.10.....	C11-32
C11.8	Upgrading to R5.02.00.....	C11-33
C11.9	Upgrading to R5.03.00.....	C11-34
C11.10	Upgrading to R5.03.20.....	C11-38
C11.11	Upgrading to R5.04.00.....	C11-40
C11.12	Upgrading to R5.04.20.....	C11-41
C11.13	Upgrading to R6.01.00.....	C11-42
C11.14	Upgrading to R6.01.10.....	C11-43
C11.15	Upgrading to R6.02.00.....	C11-44
C11.16	Upgrading to R6.03.00.....	C11-47
C11.17	Upgrading to R6.03.10.....	C11-50
C11.18	Upgrading to R6.04.00.....	C11-51
C11.19	Upgrading to R6.05.00.....	C11-57
C11.20	Upgrading to R6.06.00.....	C11-61
C11.21	Upgrading to R6.07.00.....	C11-63

Blank Page

CENTUM VP Installation

IM 33J01C10-01EN 9th 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 SOE Viewer 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 Integration Package.....	D1-8
D1.1.4	CENTUM VP System Builder Function and ProSafe-RS Safety System Engineering and Maintenance Function.....	D1-9
D1.1.5	CENTUM VP Engineering Server Function and ProSafe-RS Safety System Engineering and Maintenance Function.....	D1-10
D1.1.6	CENTUM VP System Builder Function and ProSafe-RS Engineering Server Function.....	D1-11
D1.2	CENTUM VP and PRM.....	D1-12
D1.2.1	CENTUM VP Standard Operation and Monitoring Function and PRM Server.....	D1-13
D1.2.2	PRM Server and CENTUM VP Standard Operation and Monitoring Function.....	D1-15
D1.3	CENTUM VP and Exaopc.....	D1-17
D1.3.1	CENTUM VP Standard Operation and Monitoring Function and Exaopc Server.....	D1-18
D1.3.2	CENTUM VP System Builder Function and Exaopc Server.....	D1-19
D1.4	CENTUM VP and Exapilot.....	D1-20
D1.4.1	CENTUM VP Standard Operation and Monitoring Function and Exapilot Server.....	D1-21
D1.4.2	CENTUM VP Standard Operation and Monitoring Funciton and Exapilot Client.....	D1-25
D1.4.3	CENTUM VP System Builder Function and Exapilot Client.....	D1-28
D1.5	CENTUM VP and Exaplog.....	D1-29
D1.5.1	CENTUM VP Standard Operation and Monitoring Function and Exaplog Event Analysis Package Server.....	D1-30
D1.6	CENTUM VP and Exaquantum.....	D1-33
D1.6.1	CENTUM VP Standard Operation and Monitoring Function and Exaquantum PIMS Server.....	D1-34

D1.6.2	CENTUM VP Standard Operation and Monitoring Function and Exaquantum Explorer Client.....	D1-37
D1.7	Multivariable Optimizing Control/R robust Quality Estimation and CENTUM VP.....	D1-39
D1.7.1	CENTUM VP Standard Operation and Monitoring Function and APC Client.....	D1-40
D1.8	CENTUM VP and Exasmoc.....	D1-42
D1.8.1	CENTUM VP Standard Operation and Monitoring Function and Exasmoc Client.....	D1-43
D1.9	CENTUM VP and Exasrqe.....	D1-45
D1.9.1	CENTUM VP Standard Operation and Monitoring Function and Exarqe Client.....	D1-46

CENTUM VP Installation

IM 33J01C10-01EN 9th Edition

CONTENTS

Appendix

Appendix 1. Setting Switches.....	App.1-1
Appendix 2. Vnet/IP Interface Management Tool.....	App.2-1
Appendix 3. Customization at Installation of Windows 10.....	App.3-1

Blank Page

A. Overview

This section explains how to read this document, types of CENTUM VP setup tasks and their workflows, and system requirements.

Blank Page

A1. How to Read This Document

This document explains the setup procedures for the CENTUM VP 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 each station, licenses must be distributed to and activated on the station by using a program called License Manager. Procedures for the tasks performed using License Manager are 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:

1.1.3, "Overview of license management process" in License Management (IM 33J01C20-01EN)

For more information about system security, refer to:

1., "Overview" in CENTUM VP Security Guide (IM 33J01C30-01EN)

■ 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 CENTUM VP 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 CENTUM VP with other YOKOGAWA products, such as ProSafe-RS, PRM, and Exaopc.

■ 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.

Blank Page

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 CENTUM VP software and licensing for it.

■ Installation and Licensing of Software Packages

In order to use CENTUM VP software packages, it is necessary to install the CENTUM VP 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 CENTUM VP 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.

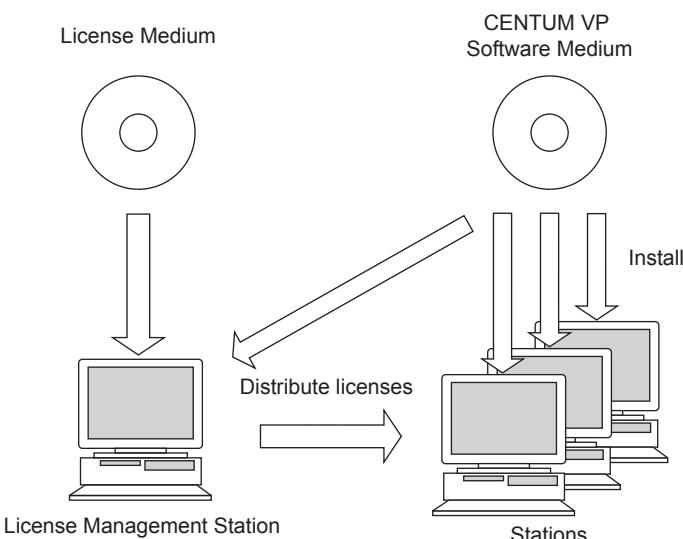


Figure A2.1-1 License Distribution

SEE ALSO

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

1.1.3, "Overview of license management process" in License Management (IM 33J01C20-01EN)

A2.2 Procedures for New Setup

This section describes the overall procedures for setting up a CENTUM VP 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.

- Human Interface Station (HIS)
- APCS
- System Integration OPC Station (SIOS)
- Generic Subsystem Gateway (GSGW)
- Computer installed with only system builders
- Computer installed with only Automation Design Server (AD Server)
- HIS with Server for Remote Operation and Monitoring Function (HIS-TSE)
- File server
- Computer dedicated to license management
- Computer switchover type UGS
- UACS station
- CENTUM VP station and computer on the virtualization platform

SEE ALSO

For more information about the procedure for setting up the network switchover type redundant UGS, refer to:

D2., "Building and maintaining a network switchover type UGS system" in Unified Gateway Station Reference (IM 33J20C10-01EN)

For more information about the virtualization platform, refer to:

A., "Overview" in Virtualization Platform Setup (IM 30A05B20-01EN)

■ Tasks to be performed after New Setup

The following works are required as the preparation for starting engineering.

- Creating an Automation Design project (AD project)
- Creating a VP project
- Registering the VP project in the AD project

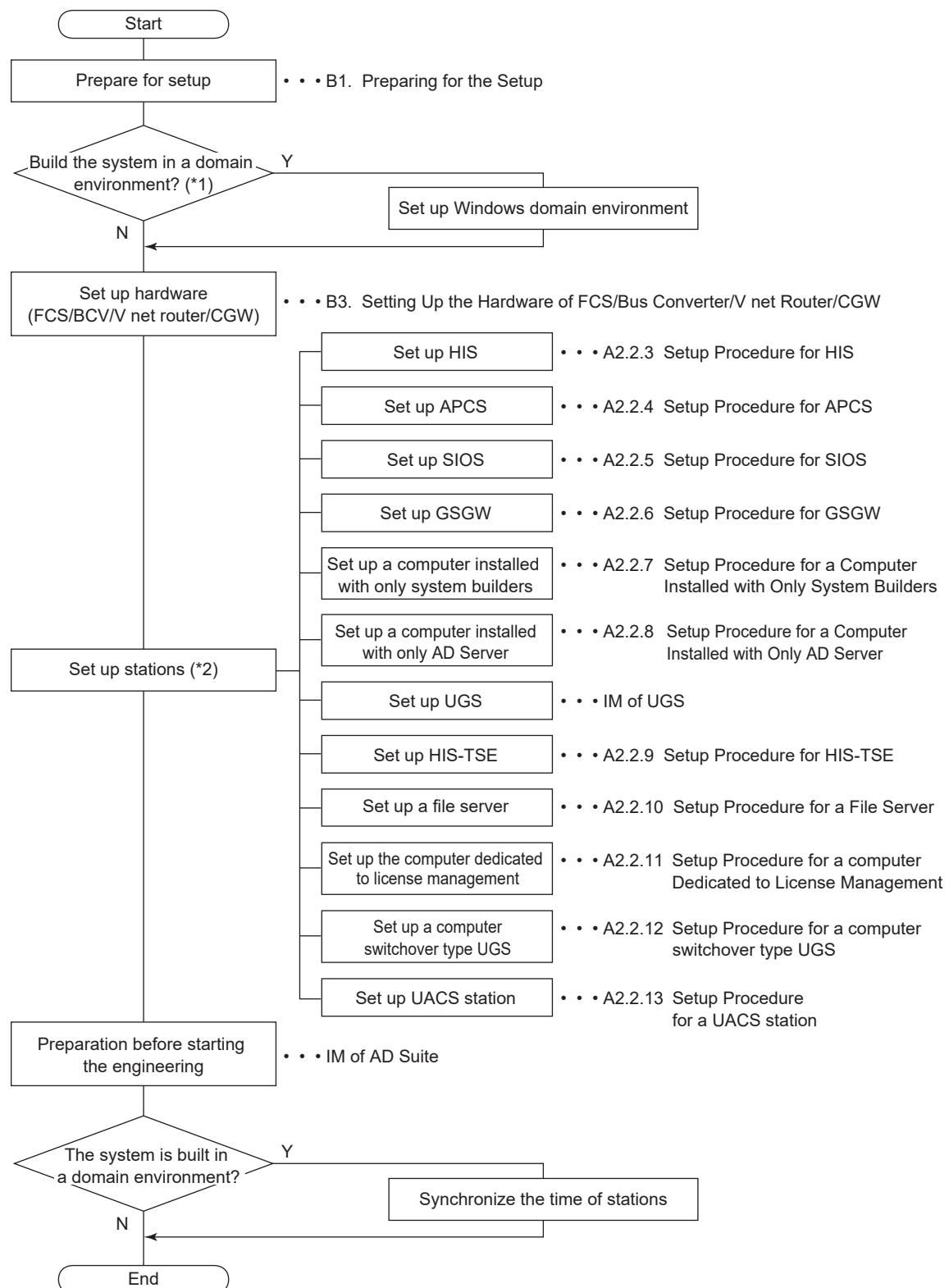
SEE ALSO

For more information about the preparation for starting engineering, refer to:

B., "Starting engineering" in Automation Design Suite Basics (IM 33J10A10-01EN)

A2.2.1 Setup Procedure for a CENTUM VP System

The following figure shows the overall procedure for setting up a CENTUM VP 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 CENTUM VP System

■ The Order of Stations to Set Up

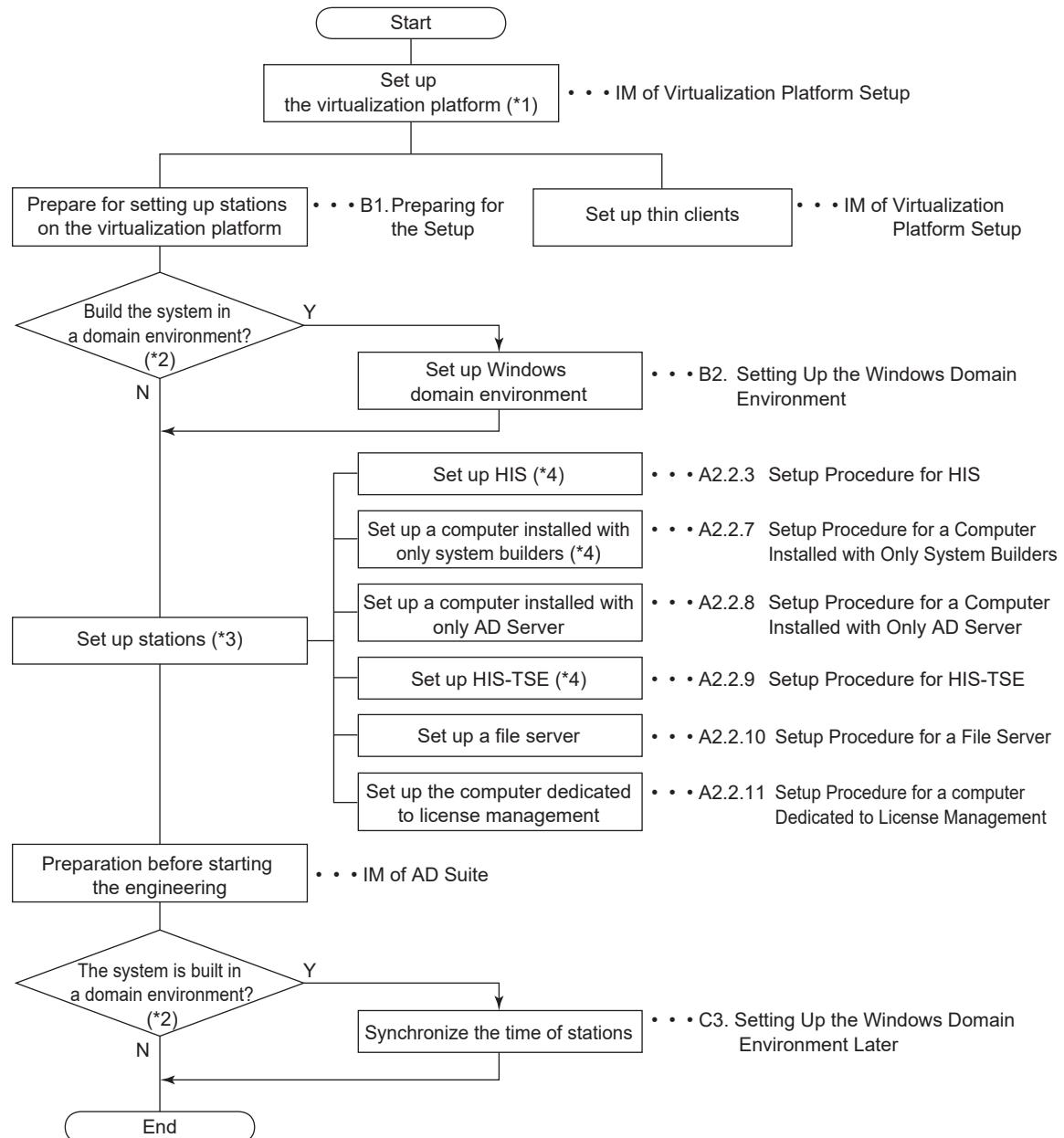
In order to use CENTUM VP software packages, it is necessary to install the CENTUM VP software on a computer and then grant licenses to the computer to enable the use of the software packages.

Because of this, you need to decide the computer to be used for granting licenses, which is called "license management station," and set up this station first.

On other stations, licenses are distributed from the license management station after software packages are installed and IT security settings are configured; the software packages then become ready for use by accepting the distributed licenses.

A2.2.2 Setup Procedure for a Virtualization Platform-based CENTUM VP System

The following figure shows the overall procedure for setting up a virtualization platform-based CENTUM VP system.



*1: Prepare a computer for virtualization host, and install the virtualization platform.

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

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

*4: You do not need to set up a Vnet/IP interface card. Also note that UPS cannot be used on the virtualization platform.

Figure A2.2.2-1 Setup Procedure for a Virtualization Platform-based CENTUM VP System

SEE

ALSO For more information about the procedure to build a file server, refer to:

A2.2.10, "Setup Procedure for a File Server" on page A2-15

For more information about how to add in a virtualization environment, refer to:

B8., "Setting Up a Virtualization Environment" on page B8-1

For more information about the installation procedure for virtualization platform, refer to:

Virtualization Platform Setup (IM 30A05B20-01EN)

■ Domain Environment

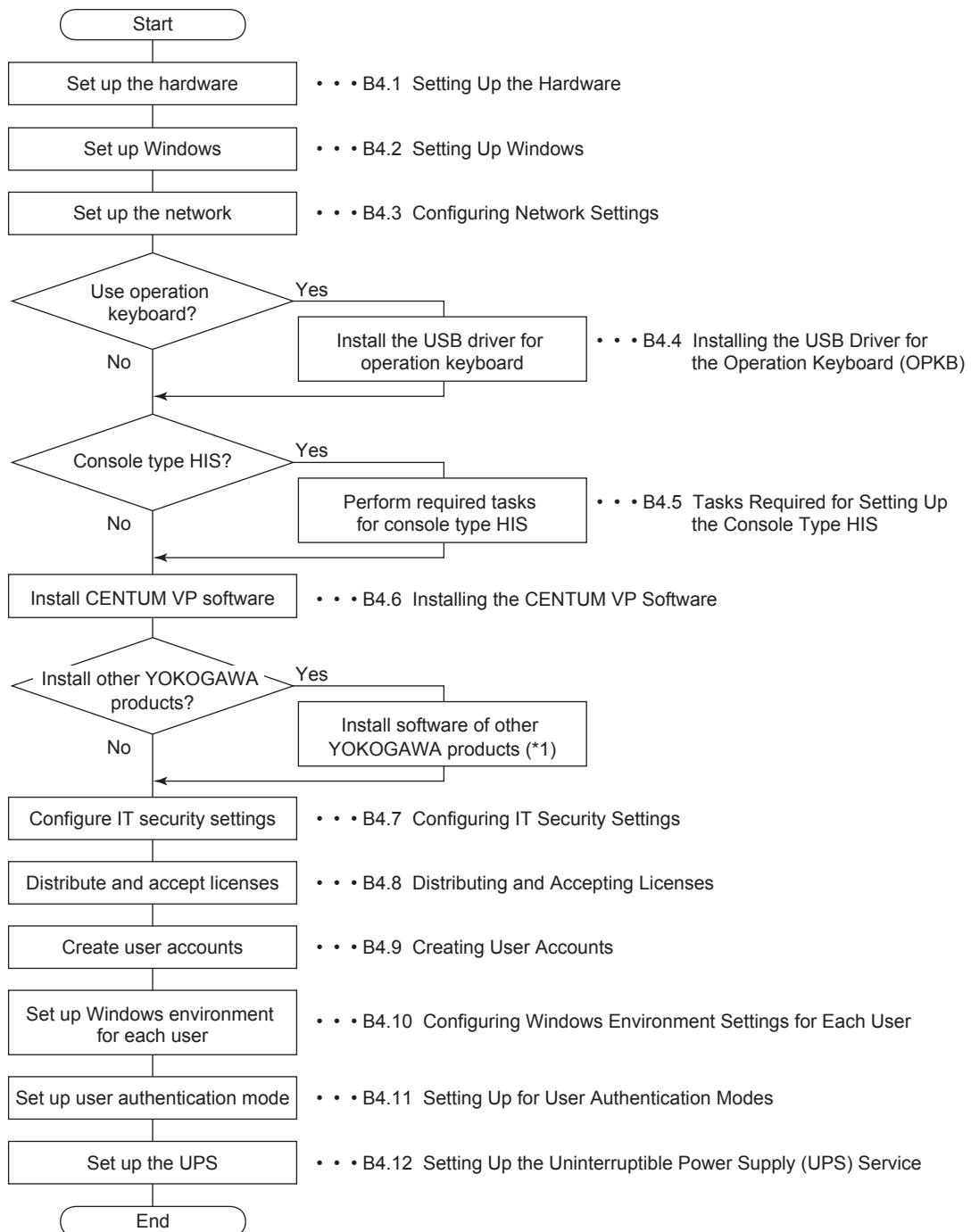
You can use a computer in the existing physical environment as the domain controller, or you can build the domain controller on the virtualization platform.

■ License Management Computer

You can use a computer in the existing physical environment as the license management computer, or you can build the license management computer on the virtualization platform.

A2.2.3 Setup Procedure for HIS

The following figure shows the setup procedure for an HIS.



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

Figure A2.2.3-1 Setup Procedure for HIS

A2.2.4 Setup Procedure for APCS

The following figure shows the setup procedure for APCS.

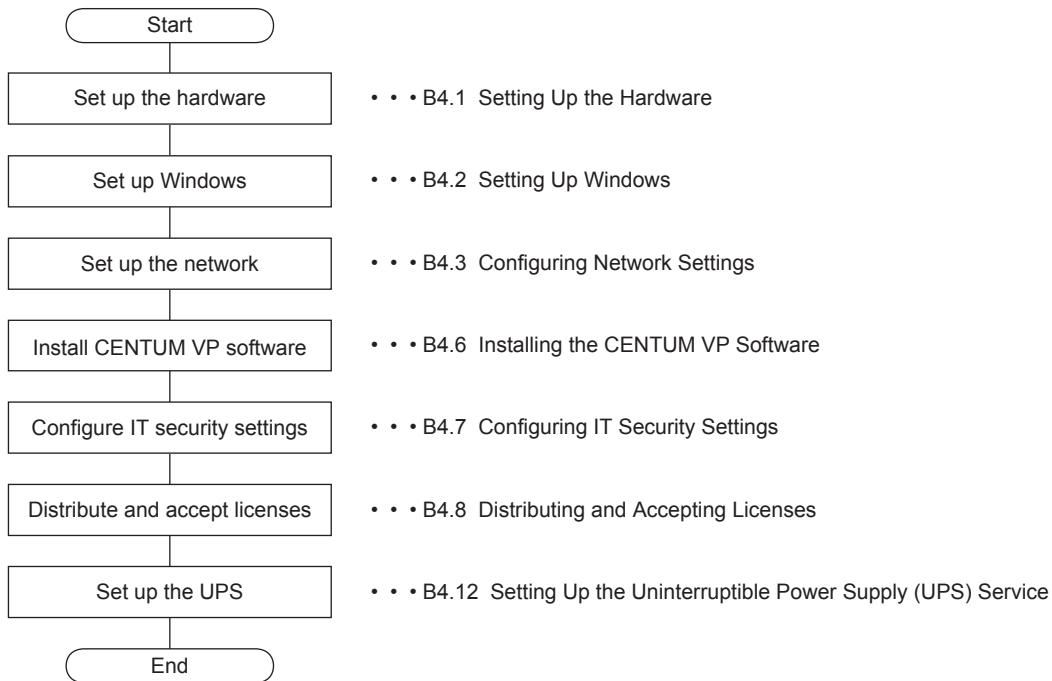


Figure A2.2.4-1 Setup Procedure for APCS

A2.2.5 Setup Procedure for SIOS

The following figure shows the setup procedure for SIOS.

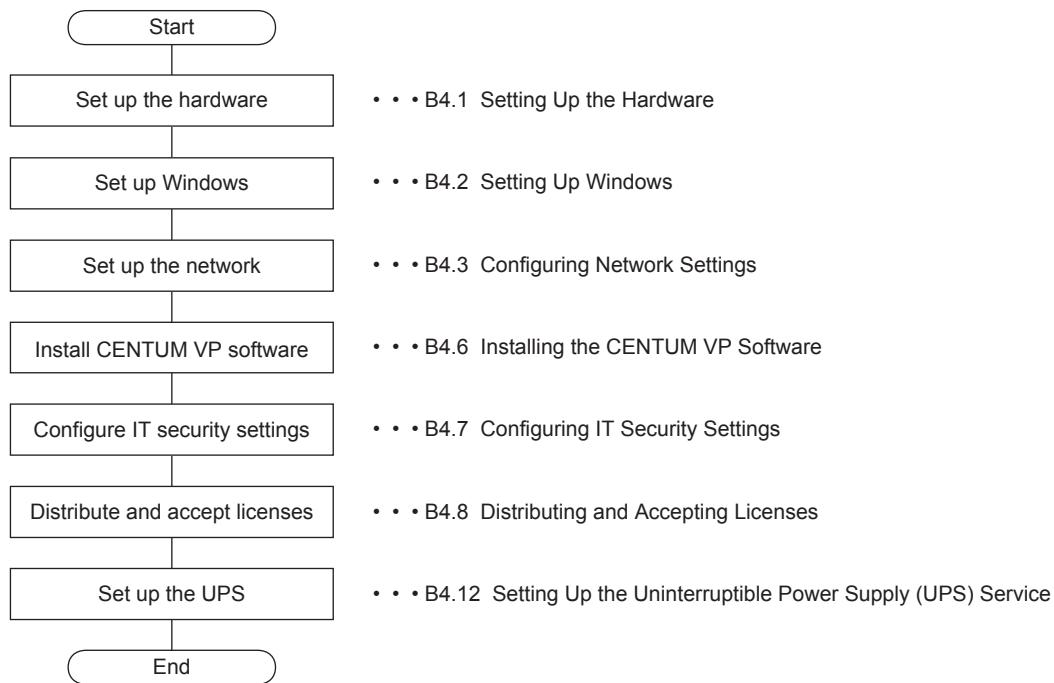


Figure A2.2.5-1 Setup Procedure for SIOS

A2.2.6 Setup Procedure for GSGW

The following figure shows the setup procedure for GSGW.

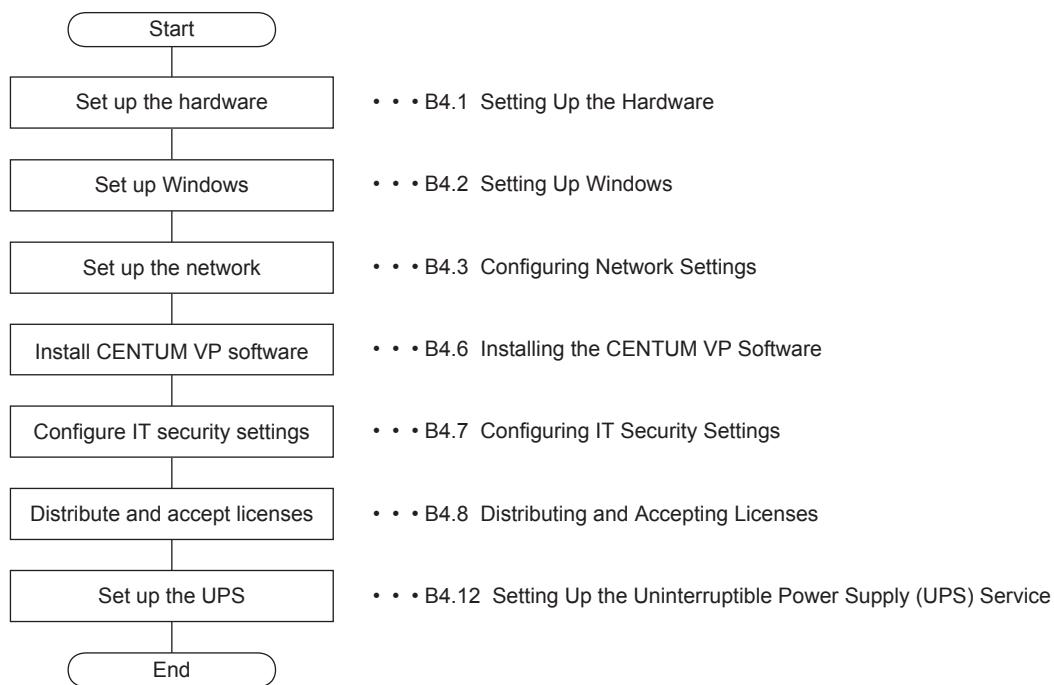
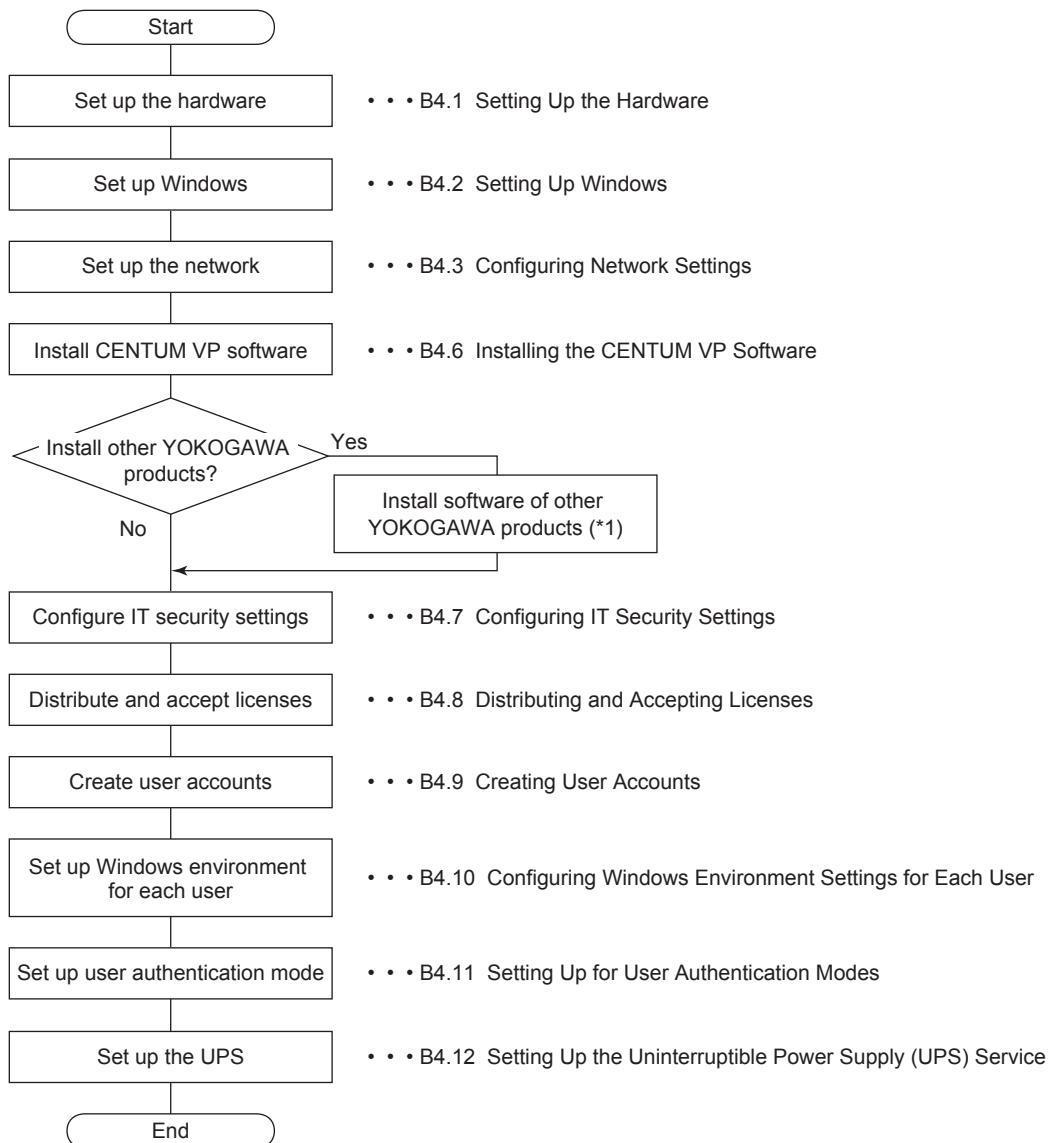


Figure A2.2.6-1 Setup Procedure for GSGW

A2.2.7 Setup Procedure for a Computer Installed with Only System Builders

The following figure shows the setup procedure for a computer installed with only system builders.

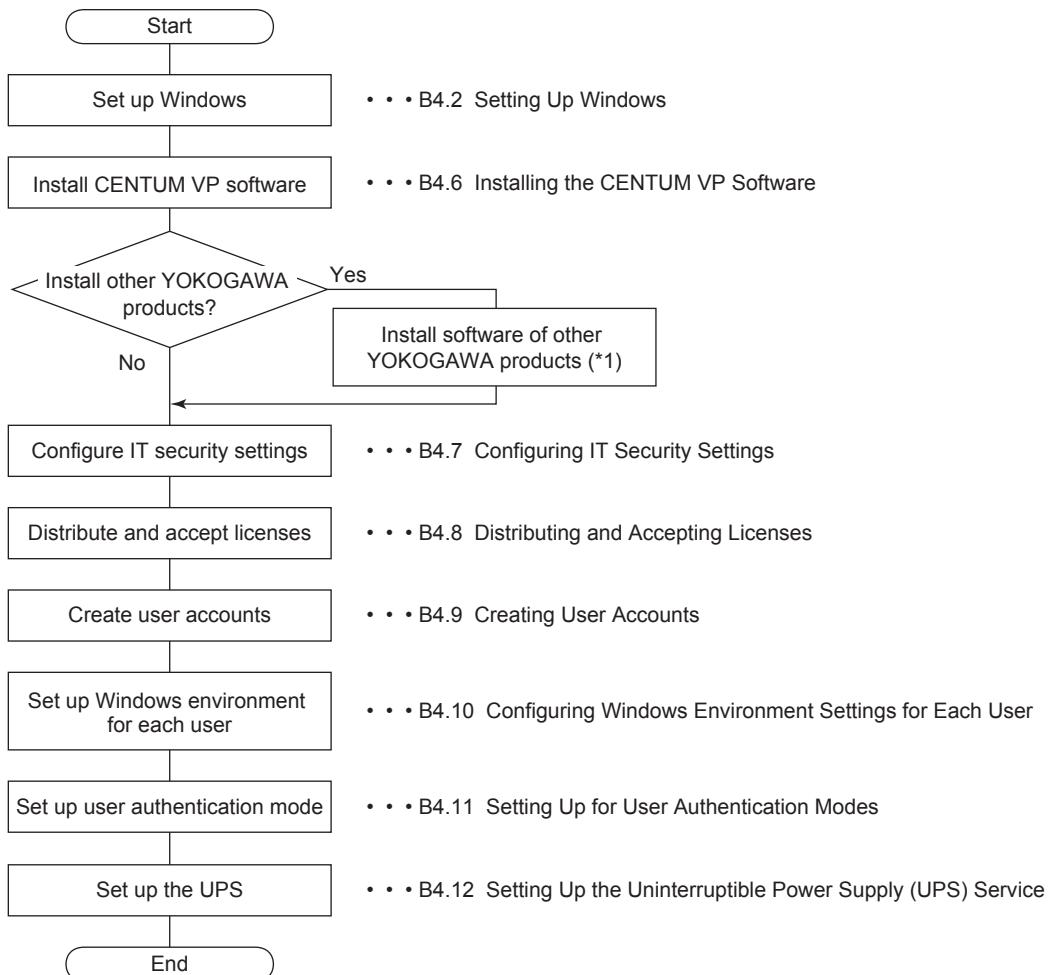


*1: You may install other products later. If you install later, you need to configure IT security settings again.

Figure A2.2.7-1 Setup Procedure for a Computer Installed with Only System Builders

A2.2.8 Setup Procedure for a Computer Installed with Only AD Server

The following figure shows the setup procedure for a computer installed with only AD Server.

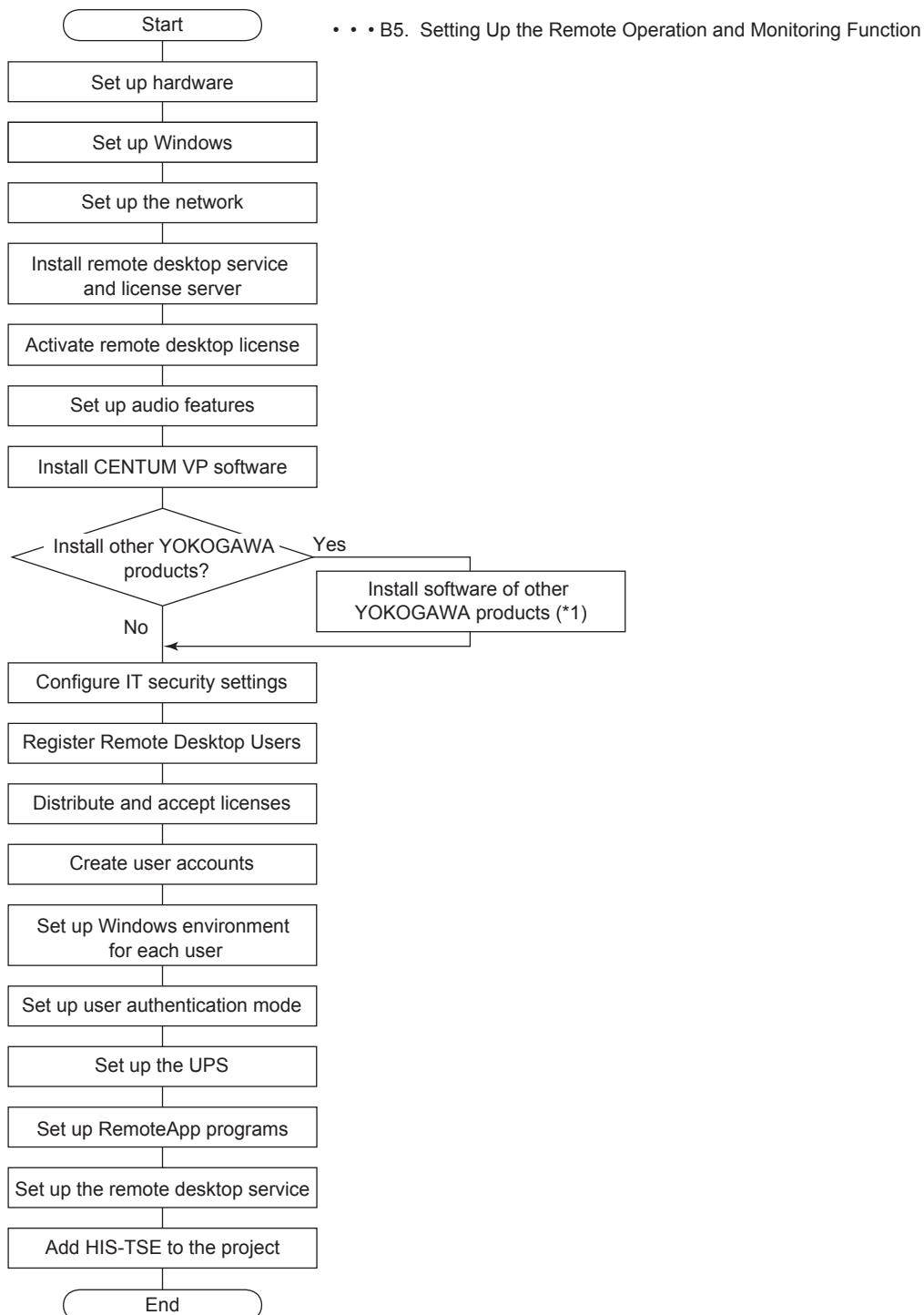


*1: You may install other products later. If you install later, you need to configure IT security settings again.

Figure A2.2.8-1 Setup Procedure for a Computer Installed with Only AD Server

A2.2.9 Setup Procedure for HIS-TSE

The following figure shows the setup procedure for HIS-TSE.



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

Figure A2.2.9-1 Setup Procedure for HIS-TSE

A2.2.10 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

The flow chart shown here illustrates the procedure for setting up a computer that serves only as a file server.

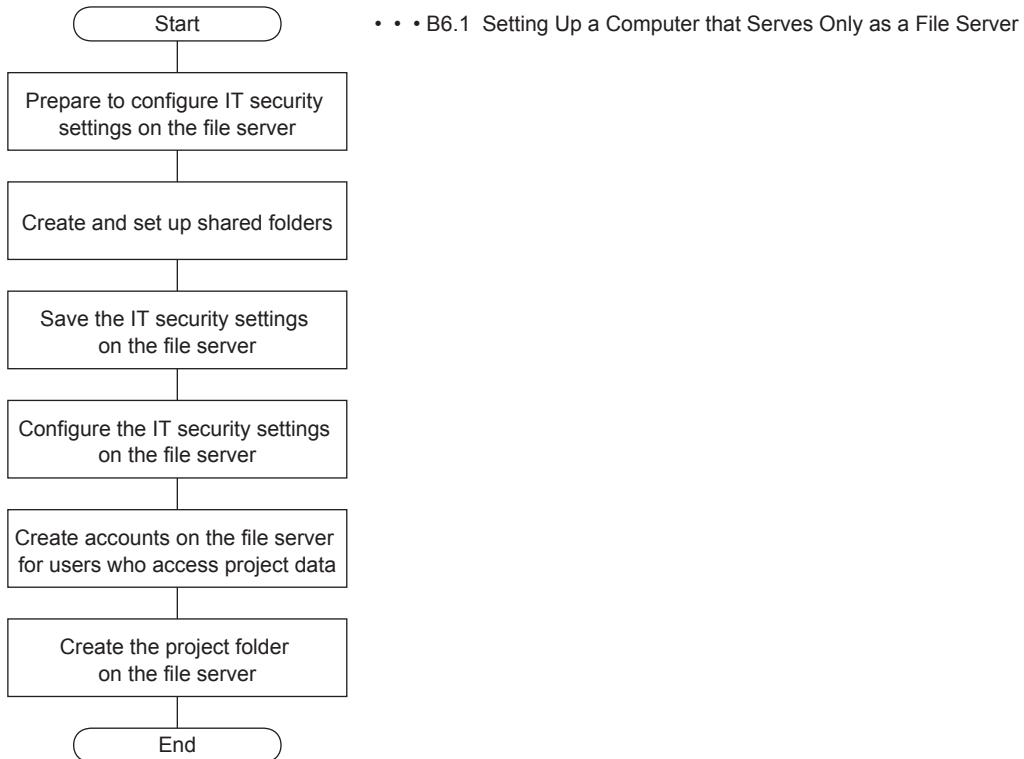


Figure A2.2.10-1 Setup Procedure for a Computer that Serves Only as a File Server

SEE ALSO

For more information about setting up the file server function on HIS or a computer installed with only system builders, refer to:

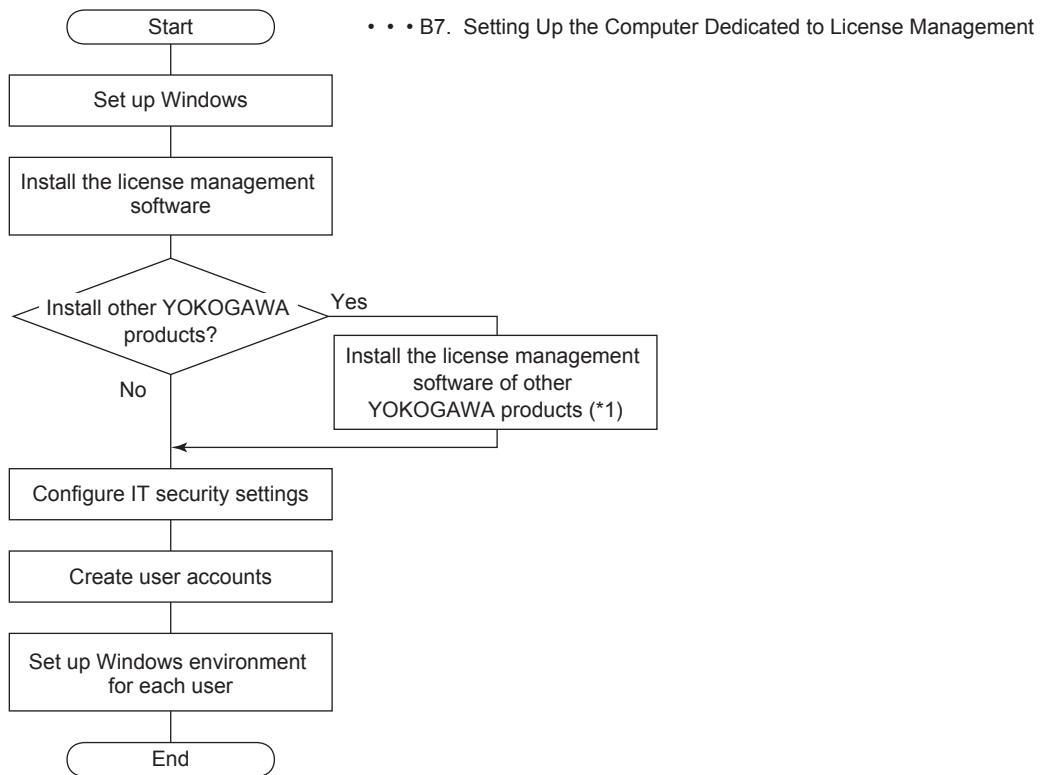
B6.2, "Setting Up the File Server Function on an HIS, a Computer with Only System Builders or a Computer with Only AD Server" on page B6-11

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

B6.3, "Setting Up the Computer that Serves as Both File Server and License Management Station" on page B6-12

A2.2.11 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.



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

Figure A2.2.11-1 Setup Procedure for a Computer Dedicated to License Management

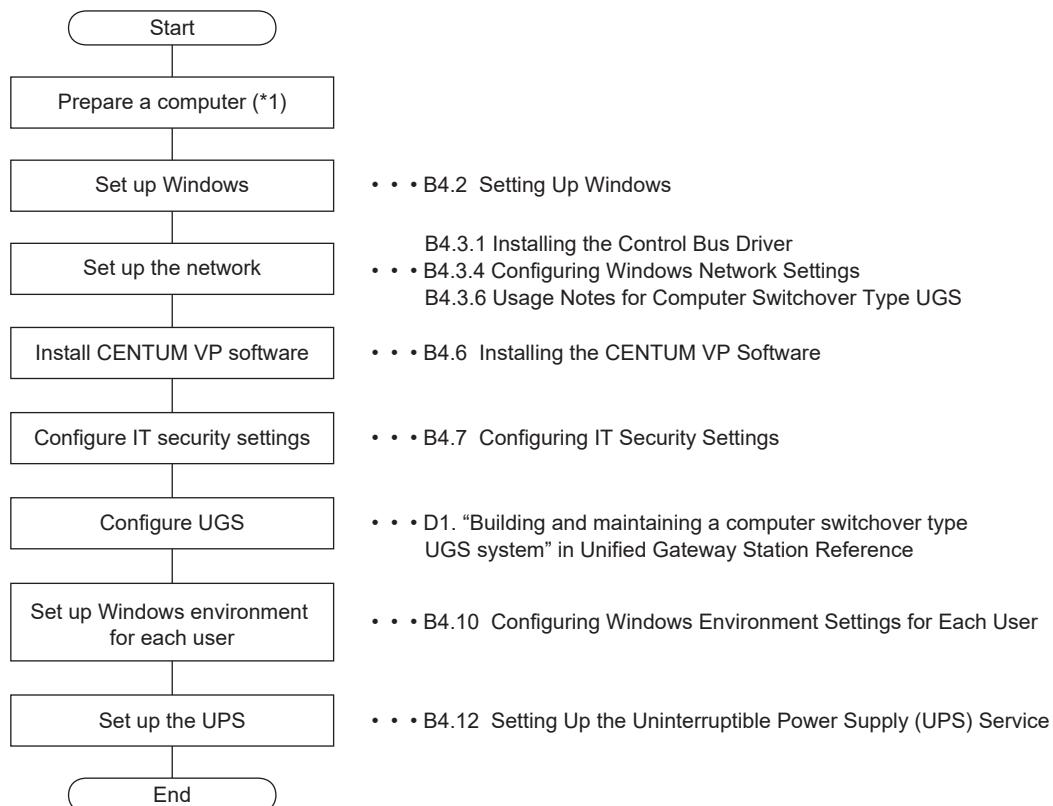
A2.2.12 Setup Procedure for Computer Switchover Type UGS

IMPORTANT

You must observe the following precautions regarding setup tasks for a computer switchover type UGS:

- When you set up a computer switchover type UGS, do not add the computer to a Windows domain before you install the CENTUM VP software on it.
- In the IT security setting configuration that is performed following the CENTUM VP software installation, set the Legacy model or the Standard model applying Standalone management temporarily.
- After you add the computer to the Windows domain, change to the Standard model applying Domain management or Combination management.
- When you use a computer switchover type UGS in a domain environment, you must configure Windows domain settings on the Windows Guest OS and on the Dual-redundant Platform for Computer.

The following figure shows the setup procedure for computer switchover type UGS.



*1: Prepare a computer to be used dedicatedly as a computer switchover type UGS, and install the Dual-redundant Platform for Computer. When you set up the UGS in a redundant configuration, prepare two computers and install the Dual-redundant Platform for Computer on each computer.

Figure A2.2.12-1 Setup Procedure for Computer Switchover Type UGS

TIP

- For information about the computer dedicated for use as a computer switchover type UGS, contact YOKOGAWA.
- When you set up the UGS in a redundant configuration, install the Dual-redundant Platform for Computer on the two computers dedicated for use as the computer switchover type UGS during the step of “Prepare a computer.” Carry out “Set up Windows” and the subsequent steps only on the first computer, which will operate as the active UGS. During the step of “Configure UGS,” the second computer, which will operate as the standby UGS, is connected to the active-side computer and equalization is performed.

A2.2.13 Setup Procedure for a UACS station

The following figure shows the setup procedure for a UACS station.

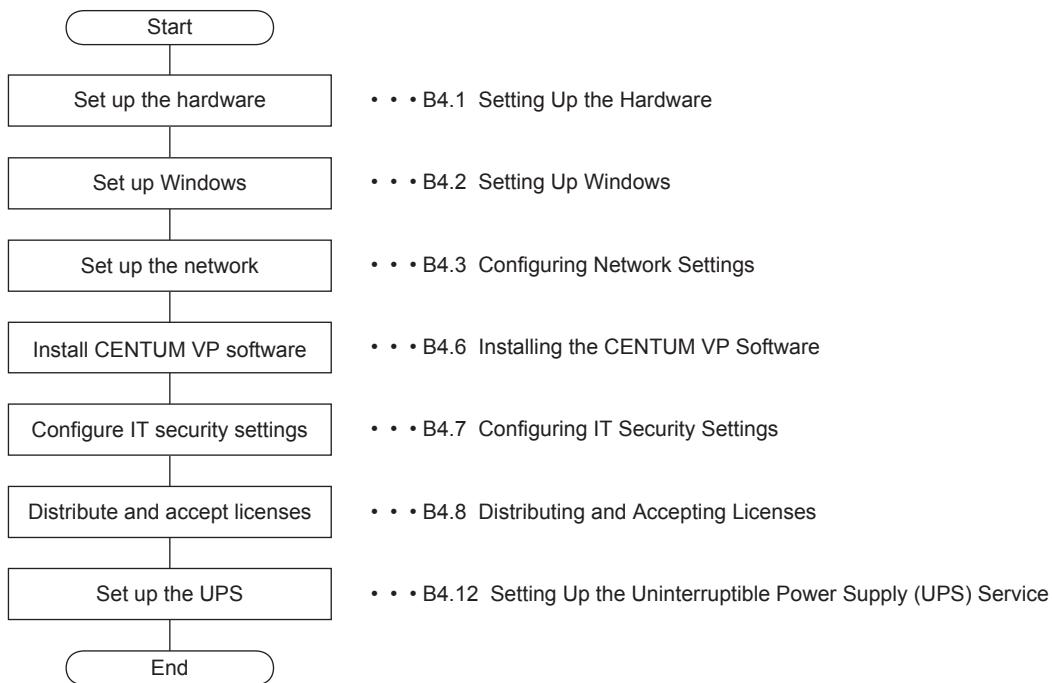


Figure A2.2.13-1 Setup Procedure for a UACS station

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 system
- Uninstall the CENTUM VP software
- Reinstall the CENTUM VP software
- Cautionary notes for upgrading

A3. Requirements for Operation

This section explains the hardware and software requirements for CENTUM VP.

■ Hardware Requirements

For information about the hardware requirements for CENTUM stations, see the related GS documents.

**SEE
ALSO**

For more information about hardware requirements of HIS, refer to:

VP6H1100 Standard Operation and Monitoring Function (GS 33J05D10-01EN)

For more information about hardware requirements of GSGW, refer to:

Model VP6B1250 GSGW Generic Subsystem Gateway Package (GS 33J20F10-01EN)

For more information about hardware requirements of SIOS, refer to:

VP6B2100 System Integration OPC Client Package (GS 33J20D10-01EN)

For more information about hardware requirements of APCS, refer to:

VP6F1200 APCS Control Functions (GS 33J15U10-01EN)

For more information about the hardware requirements for a computer installed with only system builders, refer to:

VP6E5000 Engineering Server Function VP6E5100 Standard Engineering Function (GS 33J10D10-01EN)

For more information about the hardware requirements for a computer installed with only AD Server, refer to:

VP6E5000 Engineering Server Function VP6E5100 Standard Engineering Function (GS 33J10D10-01EN)

For more information about the hardware requirements for file server computers, refer to:

“■ OS and Hardware Requirements for a File Server” on page B6-1

For more information about hardware requirements of UGS, refer to:

- VP6B1500 Unified Gateway Station Standard Function (GS 33J20C10-01EN)
- VP6B1600 Unified Gateway Station (UGS2) Standard Function (GS 33J20C20-01EN)

■ Software Requirements

This section describes the software requirements.

● Supported OS

- Windows 10 Enterprise 2016 LTSB (64-bit) (*1)
- Windows 10 IoT Enterprise 2016 LTSB (64-bit) (*1)
- Windows 10 Pro Semi-Annual Channel (64-bit, 32-bit) (*2)
- Windows 7 Professional SP1 (64-bit)
- Windows 7 Professional SP1 (32-bit) (*2)
- Windows Server 2016 Standard (64-bit)
- Windows Server 2012 R2 Standard (64-bit) (*3)
- Windows Server 2008 R2 SP1 Standard (64-bit)

*1: For the LTSB model, whose functions are not updated, only security patches and hotfixes are provided. Exercise caution because Windows 10 Enterprise LTSB is functionally different from other Windows 10 models. LTSBs are sold only with volume licenses.

- *2: This OS can be used when OPC client application is run on a general-purpose computer not running the HIS function.
 *3: This OS is supported only for use on computer switchover type UGS. It can also be used as a domain controller or file server not running CENTUM software.

TIP

Windows Server 2008 SP2 Standard Edition can be used as a domain controller or file server not running CENTUM software.

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 CENTUM VP but also can disturb its operations. It is thus recommended to reinstall the Windows OS.
- This document describes the procedure for setting up a PC 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 IM.
- It is assumed that security patches are applied according to the customer's security policy. YOKOGAWA recommends to apply security patches to CENTUM VP 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.
- When using Windows 10 Enterprise LTSB computers, customize the Windows settings during installation of Windows 10.

SEE ALSO

For more information about the procedure for customization at Installation of Windows 10 Enterprise LTSB, refer to:

Appendix 3., "Customization at Installation of Windows 10" on page App.3-1

For more information about the hardware where you run the virtualization platform and YOKOGAWA system products that run on a virtual machine on the virtualization platform, refer to:

IA System Products Virtualization Platform (GS 30A05B10-01EN)

- Software that can Coexist with CENTUM VP**

CENTUM VP can coexist with the software programs listed in the following table.

If you install software other than those listed in this table, CENTUM VP may not operate properly.

Table A3-1 Software that can coexist with CENTUM VP

Classification	Software name	Version (*1)	Remarks
Spreadsheet	Microsoft Excel (32-bit) (*2)	2010 SP2, 2013 SP1, 2016	Used with the report package, FCS Data Setting/Acquisition Package(PICOT) , and Turbomachinery I/O Module Logic Builder Package. (*3)
Word-processing software	Microsoft Word (32-bit) (*2)	2010 SP2, 2013 SP1, 2016	Module-based Engineering Package of AD suite requires 2013 SP1 or 2016.
Software development	Microsoft Visual Studio	2017(*4)	

Continues on the next page

Table A3-1 Software that can coexist with CENTUM VP (Table continued)

Classification	Software name	Version (*1)	Remarks
Web browser	Microsoft Internet Explorer	11	Used for the online manuals, self-documentation, CAMS for HIS, UACS, and Dependency Analyzer of AD suite.
Application development	.NET Framework (*5) (*6)	4.6.2 (*7), 4.7.1(*8)	
UPS software	APC PowerChute Business Edition	8.0.1, 9.0.1, 9.1.1, 9.2.1, 9.5	
	APC PowerChute Network Shutdown (*9)	v4.1.0, v4.2.0	
Security	Yokogawa standard antivirus software(*10)		
	Whitelisting Software for Endpoint Security (*11)		Model: SS1WL1C, SS1WL1S
Document reader	Adobe Acrobat Reader	DC, 2017	Pro, Standard
	Adobe Acrobat	DC, 2017	

*1: SP stands for service pack.

*2: You must install Visual Basic for Applications and Digital Certificate for VBA projects of Office Shared Features.

*3: When using Microsoft Excel, security settings must be changed.

*4: Microsoft Visual Studio 2017 does not run on Windows 10 Enterprise 2016 LTSB and Windows 10 IoT Enterprise 2016 LTSB.

*5: To create .NET components, install .NET Framework 4.6.2 Developer Pack in advance on the computer where a user program development environment is implemented. Then, specify .NET Framework 4.6.2 when you create .NET components. If a version other than NET Framework 4.6.2 is specified, .NET components will not work in graphic views.

*6: If SQL Server 2014/2012 is used for the SEM function, you need to install .Net Framework 3.5 separately.

*7: .NET Framework 4.6.2 is applicable for the software except for Windows 10 Pro.

*8: .NET Framework 4.7.1 is pre-installed in Windows 10 Pro.

*9: Only computer switcher type UGS can coexist.

*10: This anti-virus software is based on the anti-virus software product from McAfee Inc. and customized for YOKOGAWA control systems.

*11: This whitelisting software is based on the application control technology from McAfee Inc. and customized for YOKOGAWA control systems. It does not run on Windows Server 2016.

TIP

- In the CENTUM VP manuals, Adobe Reader and Adobe Acrobat Reader are collectively referred to as "Adobe Reader" except when the two must be differentiated from each other.
- After installing software programs that can coexist, perform license authentication and license agreement.

SEE ALSO

For more information about changing the security settings of Microsoft Excel with the Report Package, refer to:

2.1, "Settings for Report Package" in Optional Functions Reference (IM 33J05H10-01EN)

For more information about changing the security settings of Microsoft Excel with the FCS Data Setting/Acquisition Package (PICOT), refer to:

"■ Items to Note when Using the PICOT" in 3.1, "Overview of PICOT" in Optional Functions Reference (IM 33J05H10-01EN)

For more information about the SEM function, refer to:

9., "SEM (Sequence of Events Manager) Function" in Optional Functions Reference (IM 33J05H10-01EN)

● Report Package and Version Numbers of Microsoft Excel

When using the Report package, the functions of the Report package may be affected by the variation in the versions of Microsoft Office.

When generating reports on multiple computers, the version numbers of Microsoft Excel should be the same on all computers.

**SEE
ALSO**

For more information about the procedure of using the report files generated in the old version of Microsoft Excel in the new version of Microsoft Excel, refer to:

“■ Defining a Report” in 2.3, “Flow of Report Creation” in Optional Functions Reference (IM 33J05H10-01EN)

B. New Setup

This section explains the procedures for setting up CENTUM VP stations.

Blank Page

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.

TIP

Although a computer switchover type redundant UGS consists of two computers, the two computers are defined as one station.

● 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 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 CENTUM VP system.

Examples: HISddss (HIS or computer installed with only system builders)

BCVOddss (SIOS)

FCSddss (GSGW or APCS)

BCVUddss (UGS)

STNddss (Computer)

UACSddss (UACS station)

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

IMPORTANT

Make sure to match the computer name and the station name on all stations. If they do not match, we cannot guarantee the proper performance of the CENTUM VP system.

● 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.

When using UACS dedicated Ethernet, also determine the IP addresses of the stations connected to UACS dedicated Ethernet.

● 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.

When using UACS dedicated Ethernet, also determine the subnet masks of UACS dedicated Ethernet.

● **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.
 - If you select the Legacy model, restrictions related to Windows are in effect in some environments. For that reason, we recommend you select the Standard model.
-

SEE ALSO

For more information about security, refer to:

2., “Security Models” in CENTUM VP Security Guide (IM 33J01C30-01EN)

● **User Authentication Mode**

For HIS and the computer installed with only system builders to which the Standard model of security settings are to be applied, determine which user authentication mode to use for the CENTUM project that includes the computer you are going to set up.

SEE ALSO

For more information about the user authentication mode, refer to:

2.2.2, “CENTUM VP User Authentication Modes” in CENTUM VP Security Guide (IM 33J01C30-01EN)

● **License Assignment**

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

IMPORTANT

In a CENTUM 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 a station such as HIS runs.

Among stations of the system, you must set up the license management station first. Then, set up other stations. The software packages installed on each station become available for use after you distribute the licenses from the license management station and accept them.

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:

- 1.1, "License management" in License Management (IM 33J01C20-01EN)

■ Precautions for Setup

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

● Confirm Free Space in Disk Drive

CENTUM VP software is installed in the following folder in a disk drive.

Confirm that the disk drive has enough space for installing the software.

- Installation folder that is specified on the installer (by default, it is <system drive>:\CENTUMVP\)

● Changes in Windows Settings

Installing the CENTUM VP 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.
Windows Automatic Updates	Disable (*1) (*2)	To prevent rebooting the computer by Windows automatic updates, because the components running CENTUM VP Software are expected to run continuously.

*1: For Windows 10 and Windows Server 2016, Windows automatic update will not be disabled automatically. You must disable it manually before installing the CENTUM VP software.

*2: To use Windows Server Update Service (WSUS), install the CENTUM VP software first, manually enable Windows automatic updates, and then set the WSUS.

SEE ALSO

For more information about the procedure for manually enabling Windows automatic updates, refer to:

- Enabling Windows Update" on page C7-7

● When a Project Contains Different Revisions

If a project contains different revisions of CENTUM HIS and FCS software, computers installed with system builders and the license management station should be upgraded to the software that is the newest among the different revisions.

● 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."

● Downloading the Windows Update Programs (Windows 10)

Conditions for downloading Windows update programs are as follows:

- The OS of the computer is Windows 10 Enterprise 2016 LTSB.

- The computer will be used as an HIS with system builders or a computer with system builders.

Download and apply the following Windows update programs. If you do not apply them, table of contents may not be printed when you perform the Self-Document Printing.

- Servicing stack updates in February 2019
- Updates in March 2019

TIP

- This information is current as of March 2019. The latest information is provided as Endpoint Security Service. For information about the Endpoint Security Service, contact YOKOGAWA.
- If the updates are already applied, an error may occur at installation. In that case, ignore the error.

- **Downloading the Windows Update Programs (Windows Server 2012 R2)**

Download and apply the following Windows update programs. If you do not apply these updates, an error occurs when you access the share folders and files on Windows Server 2012 R2, and you cannot access them.

- Servicing stack update for Windows Server 2012 R2 in December 2016
- Windows Server 2012 R2 Update in April 2014
- Security Update for Windows Server 2012 in November 2014

TIP

This information is current as of March 2019. The latest information is provided as Endpoint Security Service. For information about the Endpoint Security Service, contact YOKOGAWA.

- **Downloading the Windows Update Program (Windows 7 or Windows Server 2008 R2)**

Download and apply the following Windows update program. If you do not apply it, the operation and monitoring function may not be started.

- Monthly Rollup in December 2018

TIP

This information is current as of March 2019. The latest information is provided as Endpoint Security Service. For information about the Endpoint Security Service, contact YOKOGAWA.

- **Downloading .NET Framework Developer Pack**

To create .NET components, you need to download .NET Framework 4.6.2 Developer Pack in advance onto the computer where a user program development environment is implemented.

From the Microsoft Download Center, perform a search using a keyword “developer pack” and obtain it.

- **When Connecting with Other Products**

When connecting CENTUM VP to other YOKOGAWA products, configuration of IT security settings or other tasks may be required.

SEE ALSO

For more information about the procedure to connect with other products, refer to:

D.., “Connection with Other Products” on page D-1

- **Notes on initial data of IT security settings**

On a file server or domain controller, it is necessary to save the state before applying IT security settings as initial data.

When changing the user management type or IT security setting items, use the saved initial data to restore the state before applying the IT security settings, and then apply the IT security settings again.

About a file server, when changing the security settings, the following saved data of IT security settings must be required depending on the user management type.

- When the user management type is Standalone management in Standard model:
Data saved before the first application of IT security settings in the standalone state
 - When the user management type is Domain management or Combination management in Standard model:
Data saved before applying IT security settings after adding to the domain
-

SEE

ALSO For more information about saving of IT security settings of the computer that serves only as a file server, refer to:

“■ Procedure 6: Save the IT Security Settings on the File Server” on page B6-6

For more information about the procedure for reapplying IT security, refer to:

6.3.2, “Procedures for a File Server or Domain Controller” in CENTUM VP Security Guide (IM 33J01C30-01EN)

Blank Page

B2. Setting Up the Windows Domain Environment

This section describes the required settings when CENTUM VP 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 how to set up the Windows domain environment later, refer to:
C3., "Setting Up the Windows Domain Environment Later" on page C3-1

■ Consolidated Management of IT Security Settings Using the Domain Controller

CENTUM VP allows for consolidated management of IT security settings using the domain controller.

To perform consolidated management of IT security settings, set IT securities on all clients first, and then use the domain controller to set consolidated management of IT security settings.

SEE ALSO

For more information about the procedure for setting IT security on a client, refer to:
B4.7, "Configuring IT Security Settings" on page B4-94
For more information about setting up consolidated management of IT security settings, refer to:
6.9, "Active Directory-Based Consolidated Management of IT Security Settings" in CENTUM VP Security Guide (IM 33J01C30-01EN)

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.

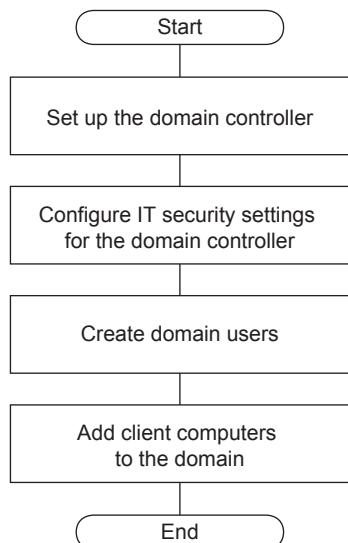


Figure B2.1-1 Flow of setting up the Windows domain environment

■ Items to be Determined in Advance

- Domain name
- IP Address of the domain controller

■ Items to be Prepared

- Computer for the domain controller
- CENTUM VP software medium
This is required for IT security configuration.

■ Items to be Set to the Domain Controller in Advance

- IP address
- Password for the Administrator account

■ Forest and Domain Function Level Settings

To configure the domain controller, the forest function level and domain function level must be set. The function level to be set varies depending on whether a new forest and domain will be configured or the domain controller will be added to an existing forest and domain.

- Function Level to Be Set When Configuring a New Forest and Domain**

Set the lowest function level that can be commonly set on all domain controller server OSs supported by CENTUM VP.

If the following domain controller server OSs are supported by CENTUM VP, for example, the lowest function level is Windows Server 2008:

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016

TIP

Set the lowest function level, considering the possibility that a server OS of low function level may be added as a domain controller.

- Functional Level to Be Set When Adding a Domain Controller to an Existing Forest and Domain**

In this case, the functional level of the existing forest and domain is set. Accordingly, which server OS can be used for the domain controller is limited by the functional level of the existing forest and domain.

The following table shows a list server OSs that can be selected for different functional levels of the existing forest and domain.

Table B2.1-1 Functional Levels of Existing Forest and Server OSs Selectable for CENTUM VP

Functional level of existing forest	Server OS selectable for CENTUM VP
Windows Server 2003	Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 R2 Windows Server 2016
Windows Server 2008	Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 R2 Windows Server 2016
Windows Server 2008 R2	Windows Server 2008 R2 Windows Server 2012 R2 Windows Server 2016
Windows Server 2012 R2	Windows Server 2012 R2 Windows Server 2016
Windows Server 2016	Windows Server 2016

Table B2.1-2 Functional Levels of Existing Domain and Server OSs Selectable for CENTUM VP

Functional level of existing forest	Server OS selectable for CENTUM VP
Windows Server 2003	Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 R2 Windows Server 2016
Windows Server 2008	Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 R2 Windows Server 2016
Windows Server 2008 R2	Windows Server 2008 R2 Windows Server 2012 R2 Windows Server 2016

Continues on the next page

Table B2.1-2 Functional Levels of Existing Domain and Server OSs Selectable for CENTUM VP (Table continued)

Functional level of existing forest	Server OS selectable for CENTUM VP
Windows Server 2012 R2	Windows Server 2012 R2 Windows Server 2016
Windows Server 2016	Windows Server 2016

For example, when the functional level of the existing forest is Windows Server 2003 and the functional level of the domain is Windows Server 2008 R2, Windows Server 2008 R2, Windows Server 2012 R2, or Windows Server 2016 can be selected as server OS for CENTUM VP.

B2.2 Configuring the Domain Controller (Windows Server 2016/Windows Server 2012 R2)

This section describes the procedure for configuring the domain controller on Windows Server 2016 or Windows Server 2012 R2.

■ Setup Procedure

1. Start the Server Manager.
2. In the left pane, click [Dashboard], in the right pane, click [QUICK START], and then click [Add roles and features].
The Add Roles and Features Wizard appears.
3. Click [Next].
The Select installation type page appears.
4. Select [Role-based or feature-based installation] and click [Next].
The Select destination server page appears.
5. Select [Select a server from the server pool], select your computer from Server Pool list, and then click [Next].
The Select server roles page appears.
6. Select [Active Directory Domain Services].
A dialog box appears, asking you to confirm adding the features.
7. Click [Add Features].
You return to the Select server roles page.
8. Click [Next].
The Select features page appears.
9. Confirm the contents and click [Next].
The Active Directory Domain Services page appears.
10. Confirm the contents and click [Next].
The Confirm installation selections page appears.
11. Confirm the contents and click [Install].
Installation starts. After the installation is complete, the results of installation appears.
12. Click [Promote this server to a domain controller].
Active Directory Domain Services Configuration Wizard appears.
13. Set as follows, and then click [Next].
 - Select [Add a new forest].
 - In the Root domain name box, type the predetermined domain name in the format "Domain name + .local."
The Domain Controller Options page appears.
14. Set as follows, and then click [Next].
 - In the Forest function level drop-down list, select [Windows Server 2008].
 - In the Domain function level drop-down list box, select [Windows Server 2008].
 - Confirm that the [Domain Name System (DNS) server] is selected.
 - Enter the password of the Directory Services Restore Mode.
The DNS Options page appears.

-
15. Click [Next].

TIP

Even when a warning message starting with "A delegation for this DNS server cannot be create" appears in the window, click [Next].

The Additional Options page appears.

16. Check the NetBIOS domain name that has been entered automatically, and click [Next].
The Paths page appears.

17. When the default paths to the following folders appear, make changes as necessary, and then click [Next]:

- Database folder
- Log files folder
- SYSVOL folder

The Review Options page appears.

18. Review the content and click [Next].

The Prerequisites Check page appears.

19. Confirm that the prerequisites are met, and then click [Install].

The installation starts. After the installation is complete, the computer automatically re-starts.

B2.3 Configuring the Domain Controller (Windows Server 2008 R2/Windows Server 2008)

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

■ Setup Procedure

1. Start the Server Manager.
2. Select [Server Manager] > [Roles], and click [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].
The Active Directory Domain Services page appears.

TIP

On Windows Server 2008 R2, the Add Roles Wizard appears before the Active Directory Domain Services page is displayed. Click [Add Required Features].

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.
8. Click [Next].
The Operating System Compatibility page appears.
9. Review the content and 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 2008] 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.

TIP

If a dialog box appears, asking you to confirm continuation, click [Yes].

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 page 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. Review the content and click [Next].
The setup 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].

B2.4 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.

TIP

If you do not run the IT Security Tool on the domain controller because of the security policy of the user environment, manually create a domain user group.

SEE**ALSO**

For more information about domain user groups required by CENTUM VP, refer to:

- “● Type 3: Standard Model/Strengthened Model - Domain Management” in “■ Combination of User Management and Security Model for Windows” in 2.2.3, “User/Group Management” in CENTUM VP Security Guide (IM 33J01C30-01EN)
- “● Type 4: Standard Model/Strengthened Model - Combination Management” in “■ Combination of User Management and Security Model for Windows” in 2.2.3, “User/Group Management” in CENTUM VP Security Guide (IM 33J01C30-01EN)

■ Installation of Microsoft Visual C++ 2017 Redistributable Package

Before you can run the IT Security Tool, you must install the Microsoft Visual C++ 2017 redistributable package.

Follow these steps to install the Microsoft Visual C++ 2017 redistributable package:

1. Log on to the domain controller as an administrative user.
2. Insert the CENTUM VP software medium into the drive.
3. Using Explorer, double-click <DVD drive>:\CENTUM\INSTALL\vcredist_x86_2017\VC_redist.x86.exe.
4. Agree to the license terms and perform the installation.

■ Application of the Root Certificate

Before you install .NET Framework 4.6.2 in Windows Server 2008 R2, you must apply the root certificate.

TIP

This operation is not required for Windows Server 2016, Windows Server 2012 R2 and Windows Server 2008.

SEE**ALSO**

For more information about the procedure for applying the root certificate, refer to:

- Applying the root certificate” on page B4-41

■ Installation of .NET Framework

Before the IT Security Tool can be run, .NET Framework of the following version must be installed:

- Windows Server 2008 R2: .NET Framework 4.6.2
- Windows Server 2008: .NET Framework 4.5.2

TIP

This operation is not required for Windows Server 2016 and Windows Server 2012 R2.

Follow these steps to install .NET Framework:

1. Log on to the domain controller as an administrative user.
2. Insert the CENTUM VP software medium into the drive.
3. Use Explorer and double-click the following file:
 - Windows Server 2008 R2: <DVD Drive>:\CENTUM\INSTALL\DotNetFX462\NDP462-KB3151800-x86-x64-Al10S-ENU.exe
 - Windows Server 2008: <DVD Drive>:\Microsoft\Runtime\DotNetFX452\NDP452-KB3026376-x86-x64-Al10S-ENU.exe
4. Agree to the license terms and perform the installation.

■ Preparing for Running the IT Security Tool

1. Log on to the domain controller as an administrative user.
2. Open Control Panel.
3. Select [System and Security] > [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.

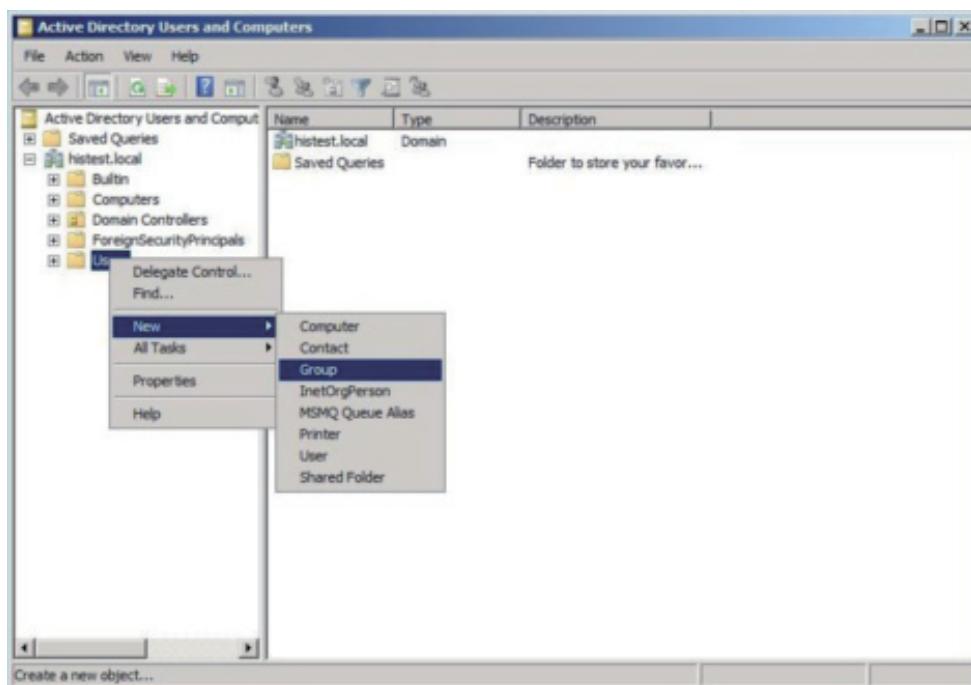
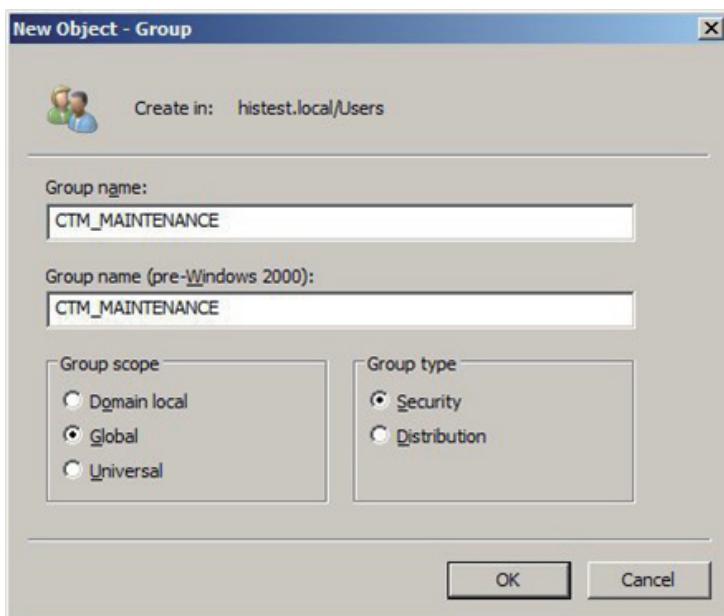
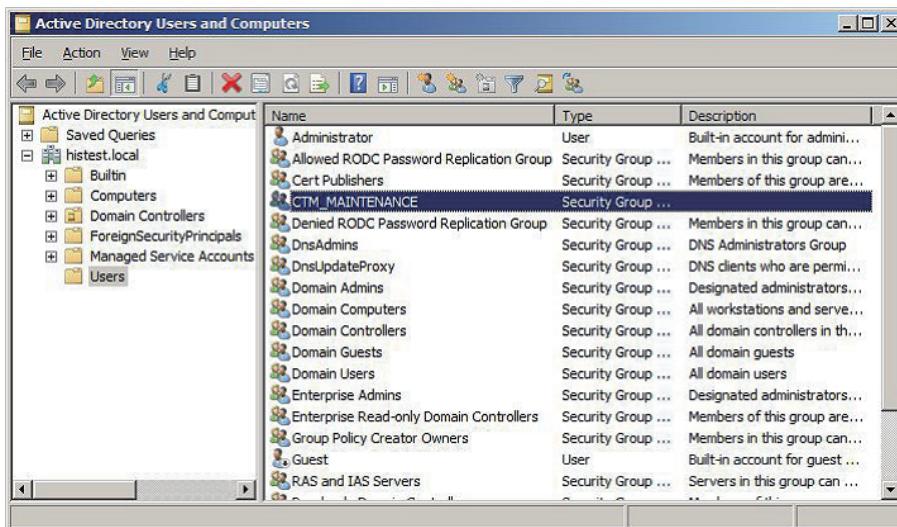


Figure B2.4-1 Active Directory Users and Computers

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

**Figure B2.4-2 New Object - Group**

- Check the right pane to confirm that the CTM_MAINTENANCE group has been created in Users.

**Figure B2.4-3 Active Directory Users and Computers (after creating a new group)**

- Add the logged on user to the CTM_MAINTENANCE and Domain Admins groups.

SEE ALSO

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

["■ Adding Domain Users to Domain Groups" on page B2-17](#)

■ Saving the Initial IT Security Settings

IMPORTANT

- When changing the IT security setting items, use the saved initial data to restore the state before applying the IT security settings, and then apply the IT security settings again. Before you run 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.
- When configuring the security settings for the second time onward, basically the security settings need not be saved. In the following cases, however, save the initial security setting data again:
 - Configure the security settings by using the IT Security Tool of R5.01 to R6.03, and then change the IT security version to 2.0 by using the IT Security Tool of R6.04 or later.
 - Configure the security settings by using the IT Security Tool earlier than R4.03, and then change the IT security version, security model or selected condition of any setting item, by using the IT Security Tool of R5.01 or later.
- To save the initial security setting data again, restore the security settings that were saved before by using the IT Security Tool. Then, perform this procedure to save the security settings. From then on, the data you have saved again will be used when the security settings are initialized; accordingly, keep the saved data in a safe place.

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

1. Log on to the computer as the user who belongs to the Domain Admins and CTM_MAINTENANCE groups.
2. Insert the CENTUM VP 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.

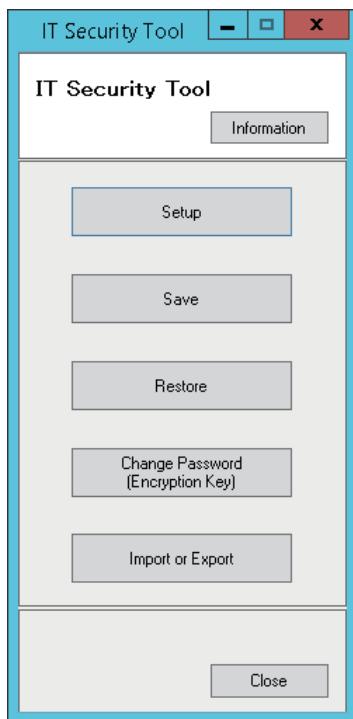


Figure B2.4-4 IT Security Tool menu

4. Click [Save].
The Specify destination page appears.
5. Specify the destination folder and enter following setting items.
 - Distinguished Name
 - Support Product
 - Support OS
 - File Version

TIP

The [Distinguished Name] and [File Version] are ommissible.

6. Click [Next].
The Type default account password page appears.
7. Enter the password for use as the initial account password and click [Next].
The Type password (Encryption Key) page appears.

TIP

This initial password will be set when the account saved with this tool is recovered. If the saved accounts are not found on the computer when you recover the accounts, new accounts are created. This password will be set as the initial password for the newly created account.

Even when multiple accounts have been created, the same initial password is assigned to all.

If the set password does not meet the password policy in the environment where the account is to be recovered, an error will occur when recovering an account.

This password is set as the initial password for the account. Accordingly, you will be prompted to change the password when you log on for the first time using this account.

8. Enter the password for encrypting the saved data, and 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.

-
9. When the saving is completed, click [Finish].
If the saving failed, the details of the failure are displayed.
 10. On the IT Security Tool menu, click [Close].

TIP

If any save failures are displayed, contact YOKOGAWA Service.

■ 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 B2.4-5 Select Security Model

3. From the Select IT security version drop-down list, select the IT security version.
4. From the Setting Model drop-down list, select [Domain Controller Standard Model Domain/Combination Management].

5. Click [Next].
The Confirm Setting Information page appears.

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

6. For the rest of steps, perform the same operations as when the IT Security Tool is run immediately after installing the CENTUM VP software.

**SEE
ALSO**

For more information about the procedure for importing the IT security settings, refer to:

6.7, "Importing/Exporting the IT Security Setting File" in CENTUM VP Security Guide (IM 33J01C30-01EN)

For more information about the IT security setting operations that are performed following the CENTUM VP software installation, refer to:

B4.7, "Configuring IT Security Settings" on page B4-94

B2.5 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. Open Control Panel.
2. Select [System and Security] > [Administrative Tools] > [Active Directory Users and Computers].
The Active Directory Users and Computers window appears.
3. In the left pane, right-click the [Users] folder and then select [New] > [User].

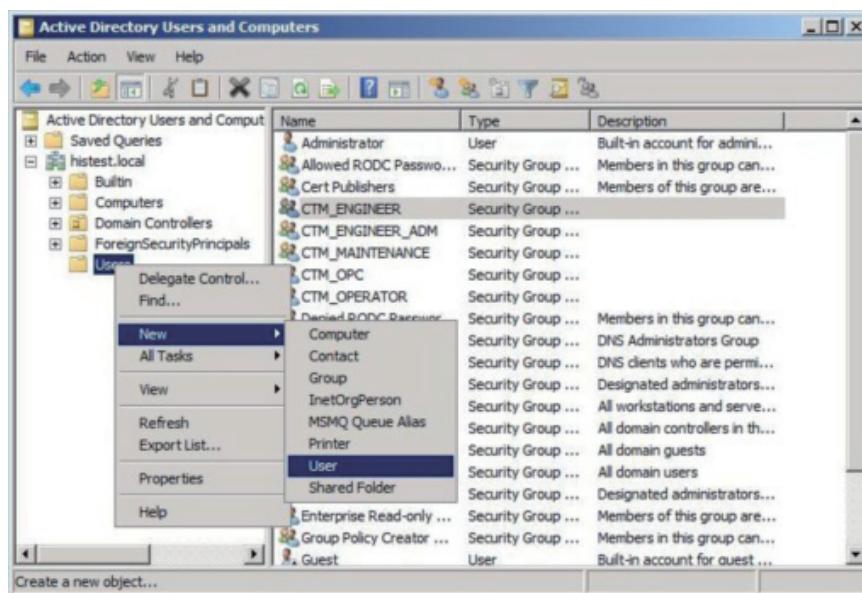


Figure B2.5-1 Active Directory Users and Computers

4. 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.

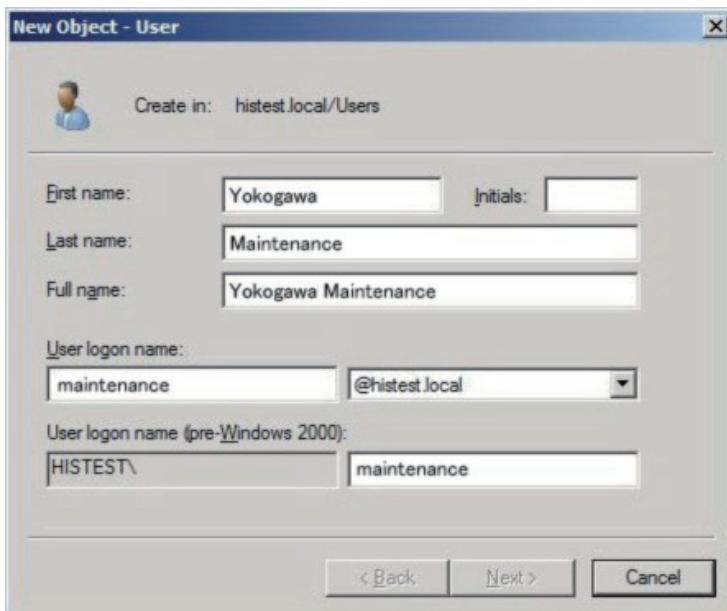


Figure B2.5-2 New Object-User

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

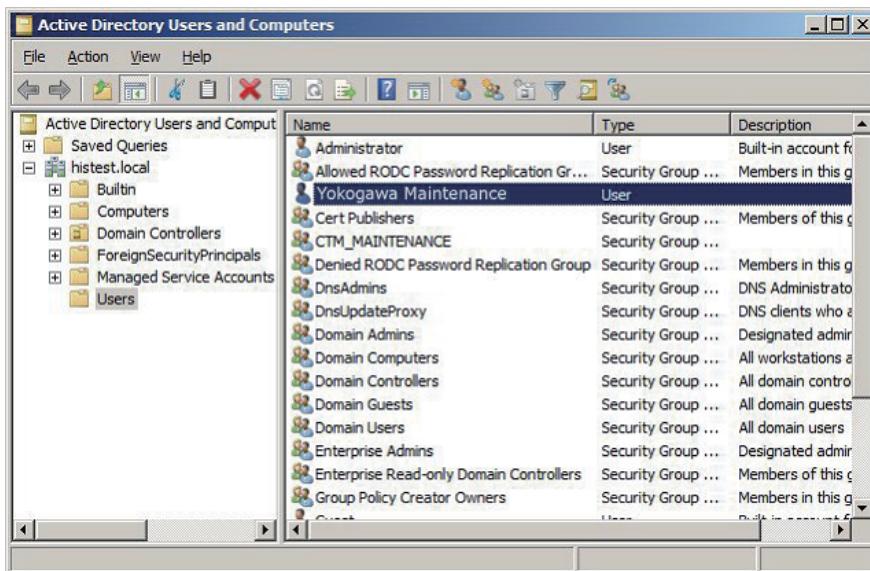


Figure B2.5-3 Active Directory Users and Computers (confirmation of newly created user)

■ 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 CENTUM VP domain groups have been created.

- CTM_OPERATOR
- CTM_ENGINEER
- CTM_OPC
- CTM_ENGINEER_ADM
- ADS_MANAGER

TIP

The CTM_MAINTENANCE group has already been created manually if you have followed the procedures so far.

● Adding a Domain User to a Domain Group

This section describes an example of adding a domain user (the user "operator") to the CTM_OPERATOR group.

This procedure is for a user for whom administrative rights are not required.

TIP

For domain users who belong to a domain group which requires administrative rights, you also need to perform the procedure in 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] to display the list of available groups. Select the CTM_OPERATOR group and click [OK].

TIP

On Windows Server 2008, click [Find Now] to display the groups.

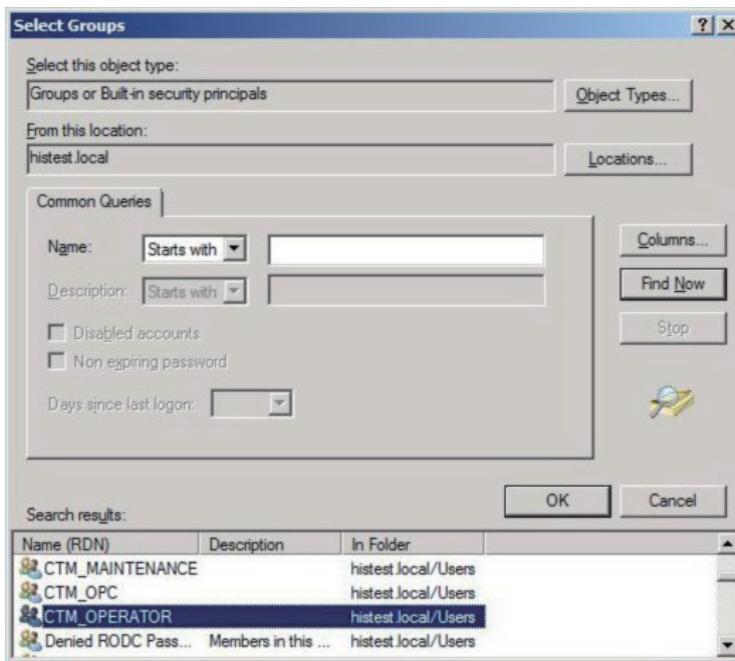


Figure B2.5-4 Select Groups dialog box - Search results

5. In the Select Groups dialog box, ensure that CTM_OPERATOR appears and click [OK].
6. In the CENTUM Operator Properties dialog box, confirm that CTM_OPERATOR is displayed in the Member of list.

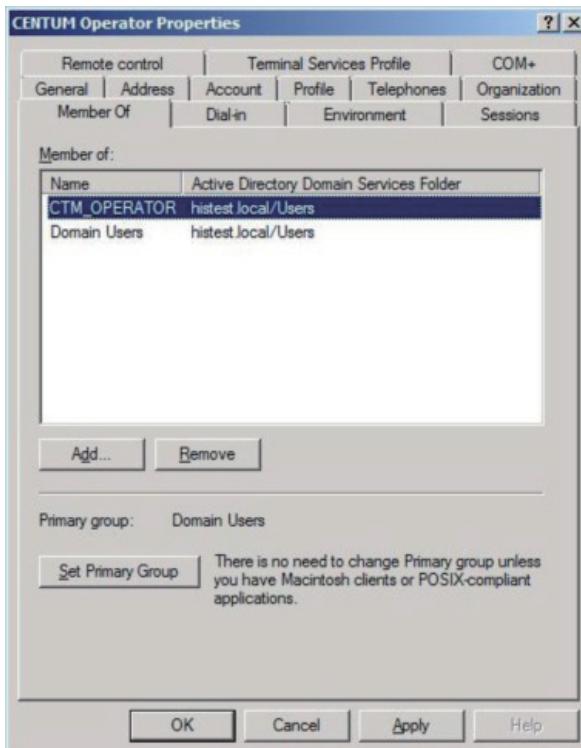


Figure B2.5-5 List of user groups assigned to the user

● 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].

B2.6 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 Regarding Setup Tasks for Client Computers

- When CENTUM VP is used in a domain environment, add the client computer to the domain before you install the CENTUM VP software. In the IT security setting configuration that is performed following the CENTUM VP 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 CENTUM VP software installation. Then, add the computer to the domain and change to the Standard model applying Domain management or Combination management.
- If a user who belongs to a domain group is used to install the CENTUM VP software on a computer added to the domain, an administrative user for installing the CENTUM VP software on the domain controller must be created in advance. Add the administrative user to the Domain Admins and CTM_MAINTENANCE user groups in advance.
- After installing the CENTUM VP software, add the administrative user of the client computer to the CTM_MAINTENANCE_LCL group.

SEE

ALSO For more information about how to change the security model, refer to:

6.3, "Changing the IT Security Settings" in CENTUM VP Security Guide (IM 33J01C30-01EN)

■ Precautions Regarding Setup Tasks for Computer Switchover Type UGS

- When you set up a computer switchover type UGS, do not add the computer to the domain before you install the CENTUM VP software.
- Set the Legacy model or the Standard model applying Standalone management temporarily in the IT security setting configuration that is performed following the CENTUM VP software installation.
- Then, add the computer to the domain and change to the Standard model applying Domain management or Combination management.
- When you use a computer switchover type UGS in a domain environment, you must configure Windows domain settings on the Windows Guest OS and on the Dual-redundant Platform for Computer.

■ Configuration on the Domain Controller

1. Open Control Panel.

2. Select [System and Security] > [Administrative Tools] > [Active Directory Users and Computers].
The Active Directory Users and Computers window is displayed.
3. In the left pane, right-click the Computers folder, and select [New] > [Computers].
The New Object - Computer dialog box appears.

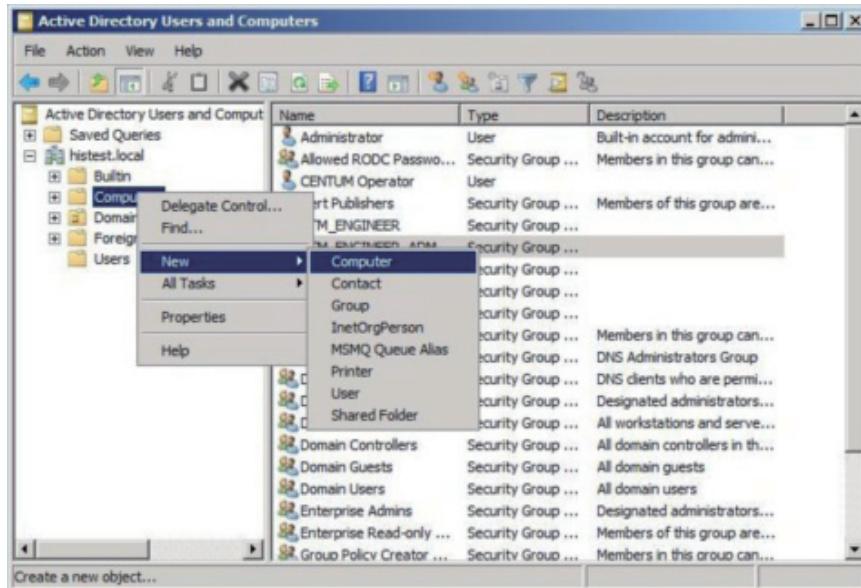


Figure B2.6-1 Active Directory Users and Computers (Create new-Computers)

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

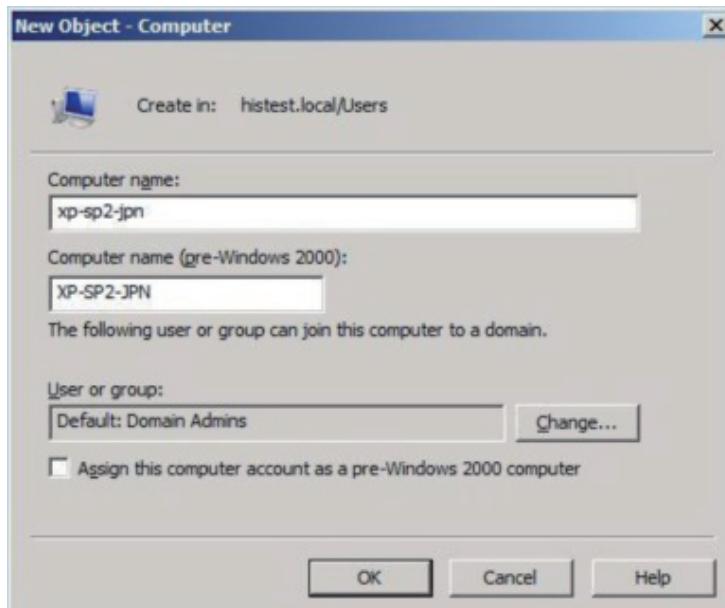


Figure B2.6-2 New Object-Computer (Input of Computer Name)

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

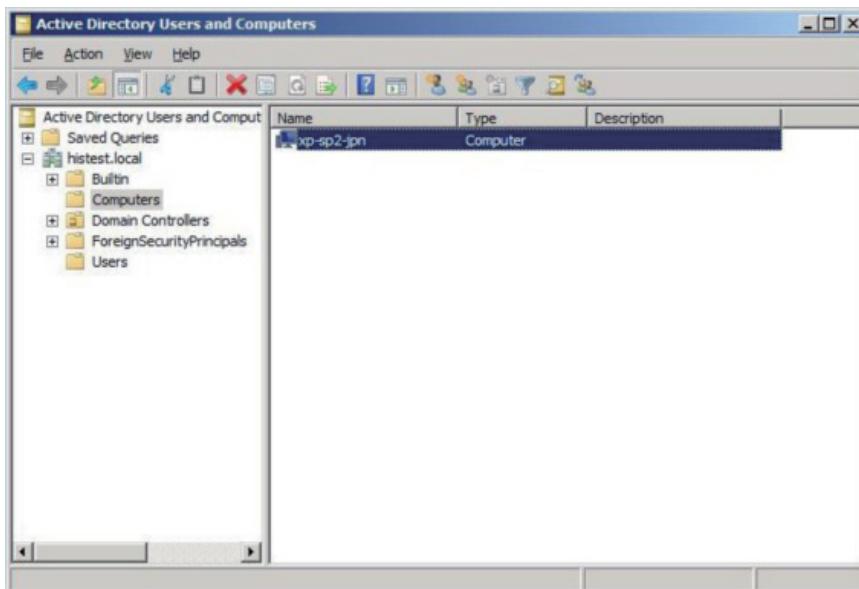


Figure B2.6-3 Active Directory Users and Computers (confirmation of newly added computers)

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

SEE ALSO

For more information about the important notes when adding a computer switchover type UGS to a domain, refer to:

“■ Required domain controller settings” in B8.4, “Key points to note when building a computer switchover type UGS” in Unified Gateway Station Reference (IM 33J20C10-01EN)

■ Configuration on a Client Computer (Windows 10)

Follow these steps to add a Windows 10 computer to the domain:

1. Open Control Panel.
2. Select [System and Security] > [System].
The System window appears.
3. Click [Change Settings].
The System Properties dialog box appears.
4. In the [Computer Name] tab, click [Change].
The Computer Name/Domain Changes dialog box appears.
5. In the Computer Name/Domain Changes dialog box, select [Domain], enter the domain name, and click [OK].
The Windows Security dialog box appears.
6. Enter the user name and password of the administrative user of the domain and click [OK].

TIP

An error message box may appear, informing you that the domain name cannot be changed. Even if this message appears, the computer has joined the domain successfully; so click [OK] to proceed.

7. In 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 7)

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

1. Open Control Panel.
2. Select [System and Security] > [System] > [Advanced system settings].
The System Properties dialog box appears.
3. Select the [Computer Name] tab and click [Change].
The Computer Name/Domain Changes dialog box appears.
4. On the Computer Name/Domain Changes dialog box, select [Domain], enter the domain name, and click [OK].

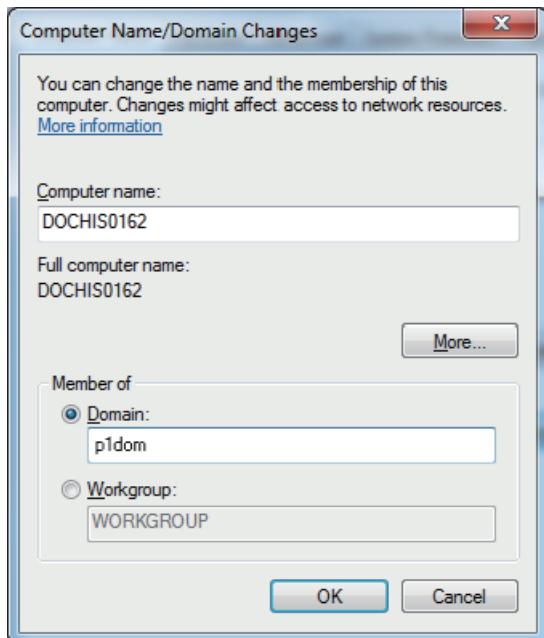


Figure B2.6-4 Computer Name/Domain Changes Dialog Box

5. 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 box may appear, informing you that the domain name cannot be changed. Even if this message appears, the computer has joined the domain successfully; so click [OK] to proceed.

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

■ Configuration on a Client Computer (Windows Server 2016)

Follow these steps to add a Windows Server 2016 computer to the domain:

1. Open Control Panel.
2. Select [System and Security] > [System].
The System window appears.
3. Click [Change settings].
The System Properties dialog box appears.

4. In the [Computer Name] tab, click [Change].
The Computer Name/Domain Changes dialog box appears.
5. In the Computer Name/Domain Changes dialog box, select [Domain], enter the domain name, and click [OK].
The Windows Security dialog box appears.
6. 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. Even if this message appears, the computer has joined the domain successfully; so click [OK] to proceed.

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

■ Configuration on a Client Computer (on Windows Server 2012 R2)

Follow these steps to add a Windows 2012 R2 computer to the domain:

1. Open Control Panel.
2. Click [System and Security].
3. Click [System].
4. In the left pane, click [Advanced system settings].
The System Properties dialog box appears.
5. In the System Properties dialog box, select the [Computer Name] tab and click [Change].
The Computer Name/Domain Changes dialog box appears.
6. In the Computer Name/Domain Changes dialog box, select [Domain], enter the domain name, and click [OK].
7. When the dialog box appears, 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. Even if this message appears, the computer has joined the domain successfully; so click [OK] to proceed.

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

■ Configuration on a Client Computer (Windows Server 2008 R2)

Follow these steps to add a Windows Server 2008 R2 computer to the domain:

1. Open Control Panel.
2. Select [System and Security] > [System] > [Advanced system settings].
The System Properties dialog box appears.
3. Select the [Computer Name] tab and click [Change].
The Computer Name/Domain Changes dialog box appears.
4. In the Computer Name/Domain Changes dialog box, select [Domain], enter the domain name, and click [OK].
5. In the dialog box that appears, 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. Even if this message appears, the computer has joined the domain successfully; so click [OK] to proceed.

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

B2.7 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:

B2.4, “Configuring Security Settings for the Domain Controller” on page B2-9

B2.8 Setting Up Time Synchronization in Windows Domain Environment

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

Because the time synchronization service of a CENTUM VP 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.

Time synchronization can be implemented in various ways; this section describes the approaches recommended for CENTUM VP, showing example cases.

■ Cautionary Note on Time Synchronization

A computer installed with the CENTUM VP 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.

B2.8.1 Implementing Time Synchronization Considering Security

This section describes approaches to implement time synchronization where a firewall or L3 switch is used to enhance security.

■ Overview of the Setup

- Introduce an SNTP server and configure so that the domain controller and the Vnet/IP system reference the time of the same SNTP server.
- For security, ensure that the SNTP server referenced by the domain controller and the Vnet/IP system is connected via a firewall (FW) or an L3 switch (L3SW).
- On the computers connected on Vnet/IP, configure so as not to perform time synchronization using the Windows W32Time service with the time on the domain controller as the time master.
- After connecting the devices, configure the domain properties.

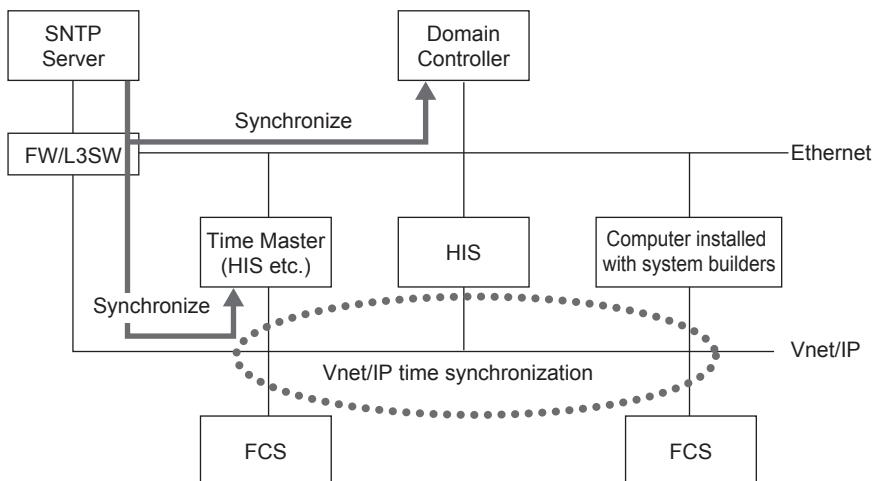


Figure B2.8.1-1 Implementing Time Synchronization Considering Security (Vnet/IP)

● Configuring Domain Properties

1. On the computer installed with system builders, start System View.
2. Select the folder of any station that is a member of the Windows domain you want to set up time synchronization, and select [File] > [Domain Properties] from the context menu. The properties dialog box for the Vnet/IP domain including the selected station appears.
3. Configure the time group settings.

TIP If 0 is specified as the time group number, time synchronization between Vnet/IP domains is not performed.

4. Set the IP address of the SNTP server.

TIP In the Connect Bus 1 text box, specify the IP address of the SNTP server that is to be connected on bus 1. If you left it blank, the system takes that "192.168.<domain number>.254" has been specified.

In the Connect Bus 2 text box, specify the IP address of the SNTP server that is to be connected on bus 2. If you left it blank, the system takes that "192.168.<128 + domain number>.254" has been specified.

5. Click [OK].

- When Both Vnet/IP and V net Are Used

When both Vnet/IP and V net are used in the system, first set up time synchronization within the Vnet/IP domain, and then perform the following configuration as well.

- Configure the properties of the V net router so that the Vnet/IP domain is placed upstream in the time system.
- If multiple V net domains exist, configure the properties of the relaying devices, such as bus converters, so that the V net domain to which the V net router is connected is placed upstream in the time system.

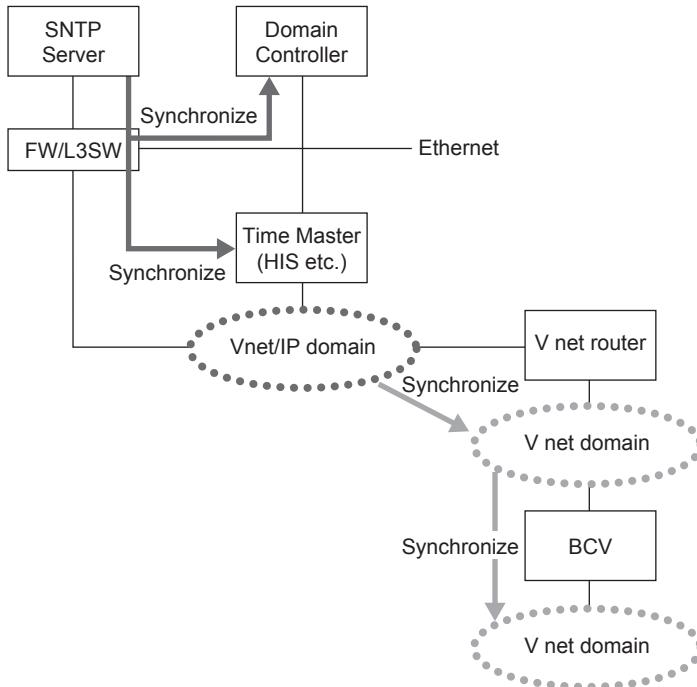


Figure B2.8.1-2 Implementing Time Synchronization Considering Security (Combination of Vnet/IP and V net)

SEE ALSO

For more information about how to set up time synchronization for Vnet/IP domains, refer to:

- “● Configuring Domain Properties” on page B2-29

B2.8.2 Implementing Time Synchronization with Lower Introduction Cost

This section describes the introduction cost-cutting approaches to implement time synchronization without using a firewall or L3 switch.

The approaches are described 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.
- If multiple V net domains exist, configure the properties of the relaying devices, such as bus converters, so that the V net domain containing the HIS that is referenced by the domain controller is placed upstream in the time system.

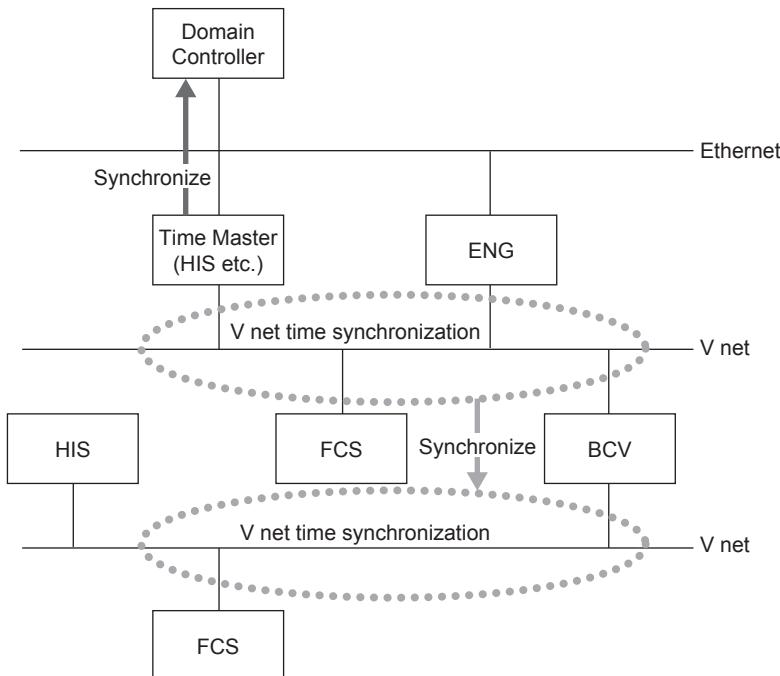


Figure B2.8.2-1 Implementing Time Synchronization with Lower Introduction Cost (V net — Not Synchronize to UTC)

● Setting a Station as the SNTP Server

1. Log on to the station you want to set as the SNTP server as an administrative user.
2. Right click on the following command, select [Run as Administrator].
`<Drive of CENTUM VP software medium>:\CENTUM\TOOLS\BeNtpServer.cmd`

TIP

If the IT security settings have been configured to apply software restriction policies, right click on the Command Prompt, select [Run as Administrator] and run the program from the command prompt window.

3. In the window that appears, enter "y" following "Enable NTP Server? (y/n/quit)."

■ 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.

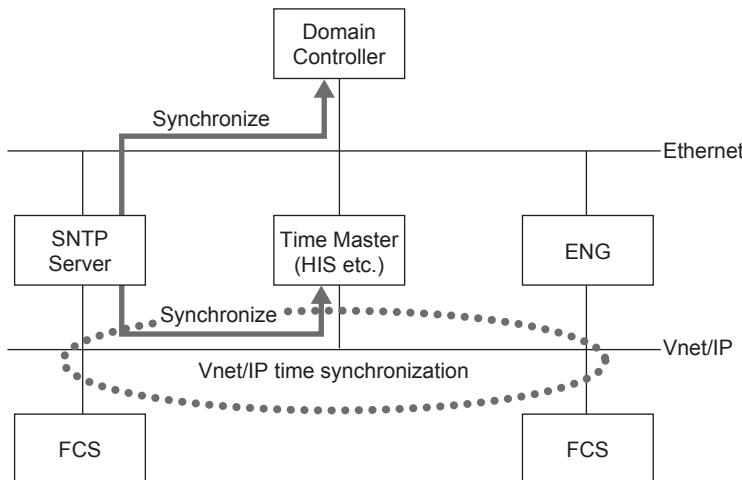


Figure B2.8.2-2 Implementing Time Synchronization with Lower Introduction Cost (Vnet/IP — Synchronize to UTC)

SEE ALSO

For more information about how to set up time synchronization for Vnet/IP domains, refer to:

- “● Configuring Domain Properties” on page B2-29

■ 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.

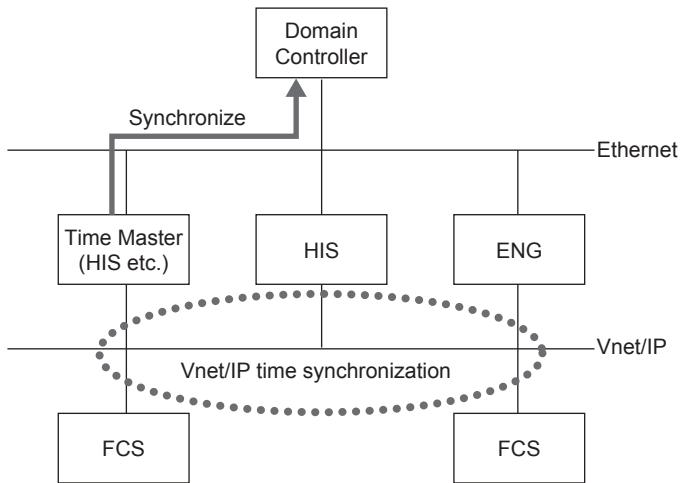


Figure B2.8.2-3 Implementing Time Synchronization with Lower Introduction Cost (Vnet/IP — Not Synchronize to UTC)

● Setting a Station as the SNTP Server

1. Log on to the station you want to set as the SNTP server as an administrative user.
2. Right click on the following command, select [Run as Administrator].
 <Drive of CENTUM VP software medium>:\CENTUM\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, right click on the Command Prompt, select [Run as Administrator] and then run the command from the command prompt window.

3. Enter **y**, and then press the [Enter] key.

Blank Page

B3. Setting Up the Hardware of FCS/Bus Converter/V net Router/CGW/WAC Router

This section describes the hardware setup for FCS, bus converter, V net router, communication gateway unit (CGW), and wide area communication router (WAC router). You may also perform the setups described here after you have set up the related stations.



CAUTION

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 prevention of static electricity, refer to:

A6.1, "Precautions against Static Electricity" in Peripherals (IM 33J50B10-01EN)

B3.1 Configurations for FCS

This section describes the hardware setups required for FCS.

■ Setting Up the Processor Unit

The processor unit is installed in a field control station and used for control computation.

The following types of processor unit are available:

- CP471
- CP461
- CP451
- CP401
- CP345
- CP703
- CP701

All of these cards have DIP switches for setting a domain number and a station number, which determine a station address.

This section describes how to set these DIP switches.

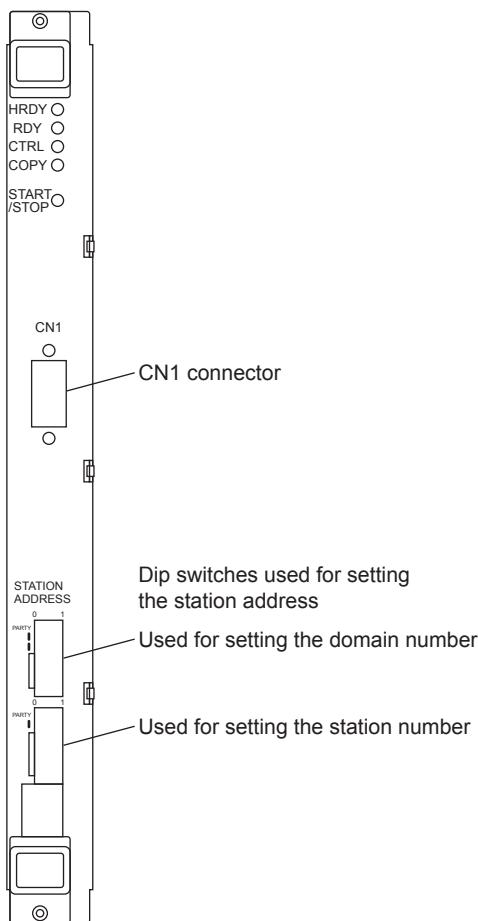


Figure B3.1-1 Locations of DIP Switches (CP345/CP703/CP701)

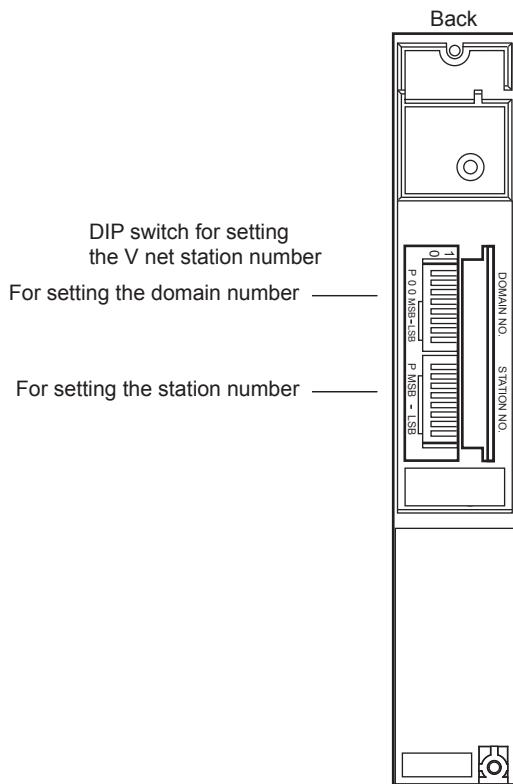
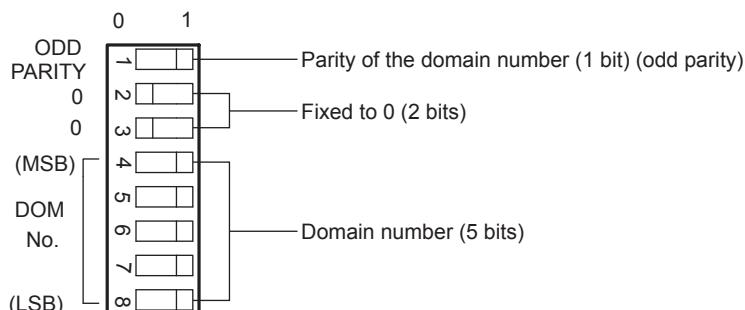


Figure B3.1-2 Locations of DIP switches (CP471/CP461/CP451/CP401)

● 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 16. For a system consisting of one domain, always set the domain number to 1.



MSB : Most Significant Bit

LSB : Least Significant Bit

Figure B3.1-3 Domain Number Setting DIP Switches (CP401)

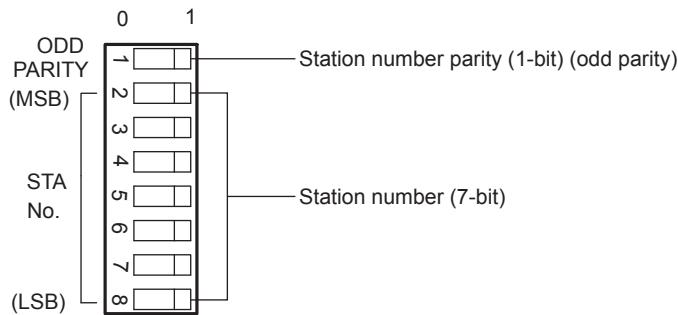
SEE ALSO

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

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

● Setting the Station Number

Set a station number from 1 to 64.



MSB : Most Significant Bit
LSB : Least Significant Bit

Figure B3.1-4 Station Number Setting DIP Switches

**SEE
ALSO**

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

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

B3.2 Configurations for Bus Converters

This section describes the hardware setups required for bus converters (ABC11S, ABC11D).

You need to set up the following hardware components in a bus converter:

- Processor card
- HF Bus/RL Bus interface card
- V net interface card

■ Setting Up the Processor Card

The processor card has DIP switches for setting a domain number and a station number, which determine a station address.

This section describes how to set these DIP switches.

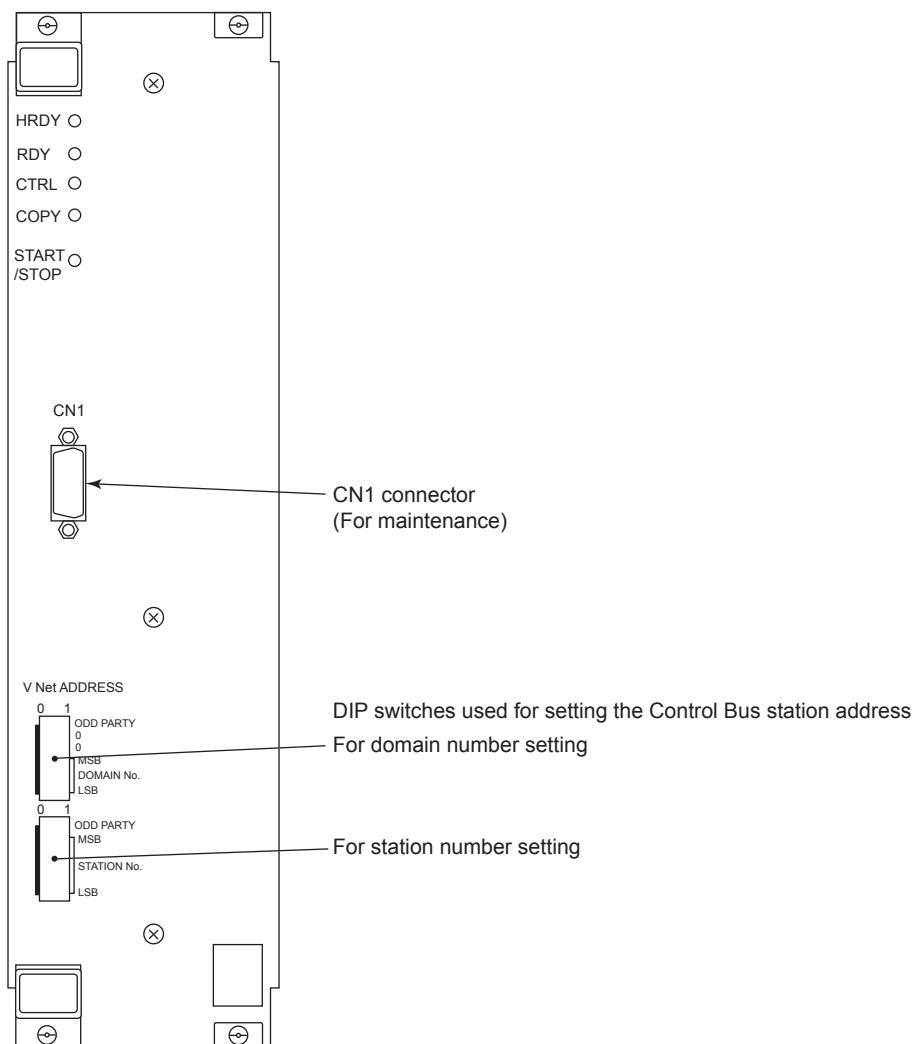
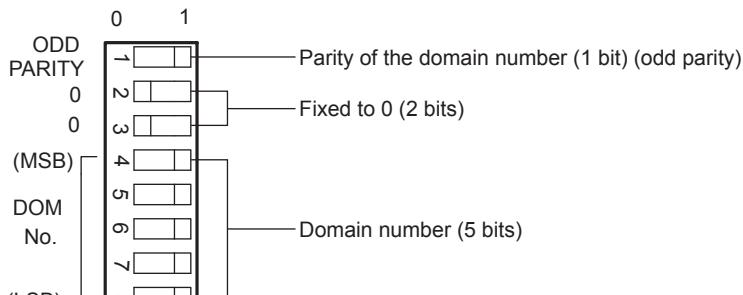


Figure B3.2-1 Locations of DIP Switches

● 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 16. For a system consisting of one domain, always set the domain number to 1.



MSB : Most Significant Bit
 LSB : Least Significant Bit

Figure B3.2-2 Domain Number Setting DIP Switches

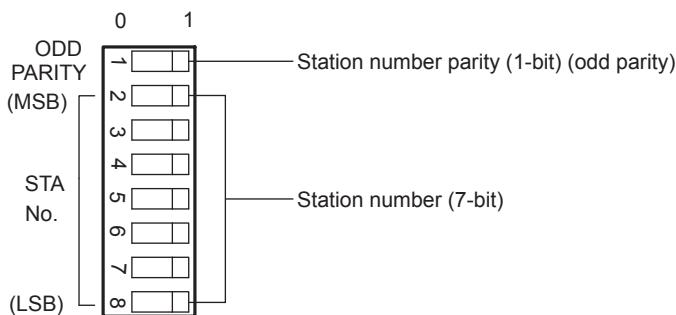
SEE ALSO

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

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

● **Setting the Station Number**

Set a station number from 1 to 64.



MSB : Most Significant Bit
 LSB : Least Significant Bit

Figure B3.2-3 Station Number Setting DIP Switches

SEE ALSO

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

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

■ **Setting Up the HF Bus/RL Bus Interface Card**

The HF Bus/RL Bus interface card has DIP switches for setting a station number or a unit number of the lower system.

This section describes how to set these DIP switches.

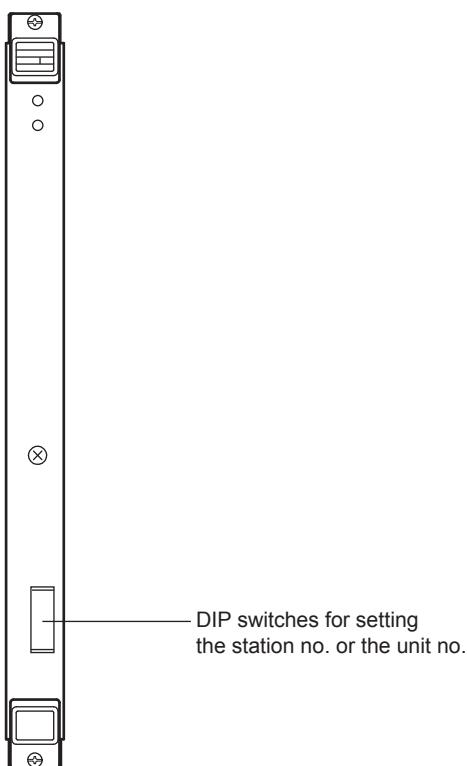
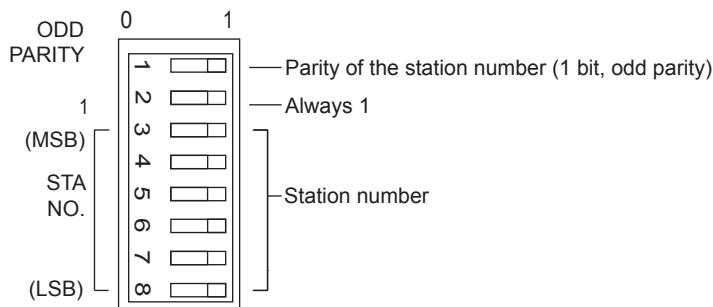


Figure B3.2-4 Location of the DIP Switches

● Setting the Station Number

Set the station number on the HF bus in the range of 1 to 32.

Set the DIP switches as shown in the following table to set the necessary station number.



MSB : Most Significant Bit

LSB : Least Significant Bit

Figure B3.2-5 DIP Switches for Station Number Setting

- DIP switch settings
 - 0: Means flipping the DIP switch to the left when looking at the module as shown in the figure above.
 - 1: Means flipping the DIP switch to the right when looking at the module as shown in the figure above.

Table B3.2-1 Station Numbers and Switch Positions

Station number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bit 1	1	1	0	1	0	0	1	1	0	0	1	0	1	1	0	1
Bit 2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Continues on the next page

Table B3.2-1 Station Numbers and Switch Positions (Table continued)

Station number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bit 3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bit 4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Bit 5	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0
Bit 6	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0
Bit 7	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0
Bit 8	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0

Station number	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Bit 1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	1	1
Bit 2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Bit 3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Bit 4	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0
Bit 5	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0
Bit 6	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0
Bit 7	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0
Bit 8	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0

● Setting the Unit Number

Set the unit number on the RL bus in the range of 1 to 21. The DIP switch positions and the corresponding unit numbers are the same as those for the station number setting on the HF bus interface card.

■ Setting Up the V net Interface Card

The V net interface card is used to perform communication between the following systems:

- CENTUM VP V net and another CENTUM VP V net
- CENTUM VP V net and a CS 3000 V net
- CENTUM VP V net and a CENTUM CS V net
- CENTUM VP V net and a CS 1000 VL net

The V net interface card has DIP switches for setting a domain number and a station number.

This section describes how to set these DIP switches.

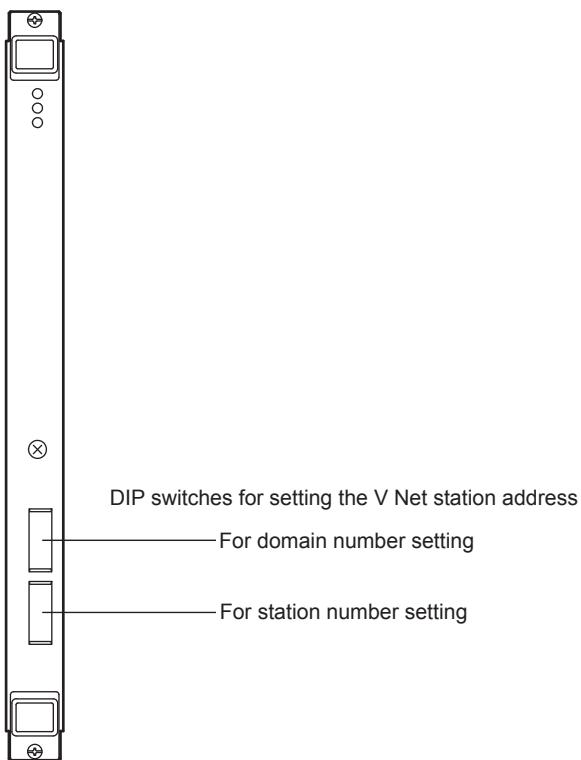
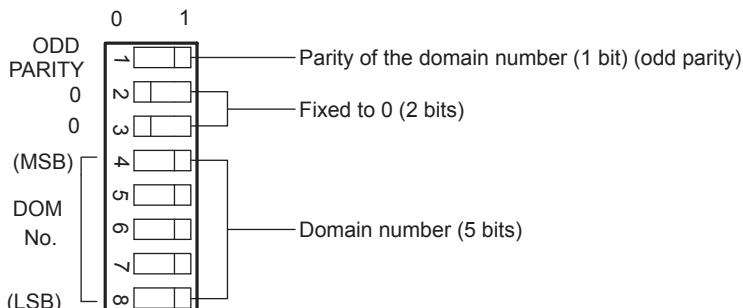


Figure B3.2-6 Locations of DIP Switches

- **Setting the Domain Number**

Set the domain number of the lower system in the range from 1 to 16.

If the system consists of one domain, set the domain number to 1.



MSB : Most Significant Bit

LSB : Least Significant Bit

Figure B3.2-7 Domain Number Setting DIP Switches

SEE ALSO

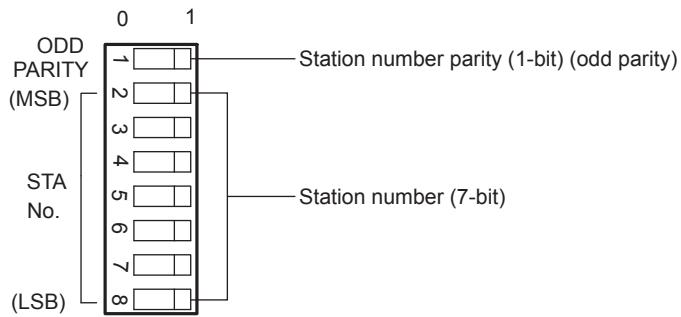
For more information about domain numbers and the corresponding DIP switch positions, refer to:

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

- **Setting the Station Number**

Set the station number of the lower system in the range from 1 to 64.

If the lower system is CS 1000, set a station number from 1 to 24.



MSB : Most Significant Bit
LSB : Least Significant Bit

Figure B3.2-8 Station Number Setting DIP Switches

**SEE
ALSO**

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

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

B3.3 Configurations for V net Routers

This section describes the hardware setups required for a V net router (AVR10D).

■ Setting Up the Communication Module of the V net Router

The communication module of the V net router has DIP switches for setting a domain number and a station number, which determine a station address.

This section describes how to set these DIP switches.

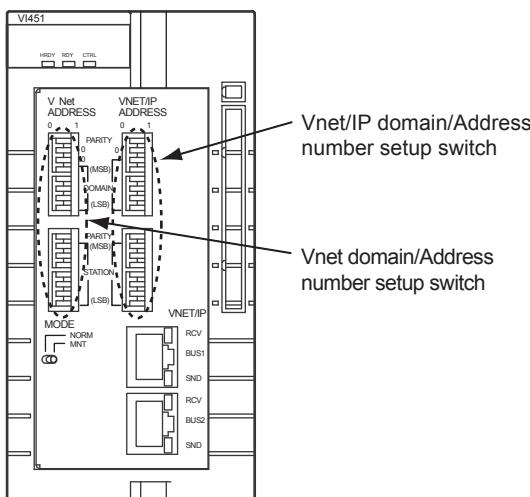
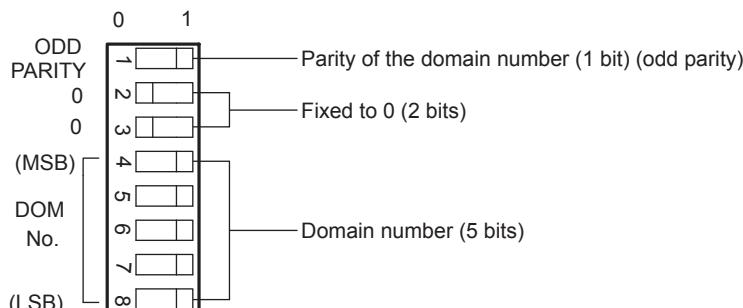


Figure B3.3-1 Locations of the DIP Switches

● 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 16. For a system consisting of one domain, always set the domain number to 1.



MSB : Most Significant Bit
LSB : Least Significant Bit

Figure B3.3-2 Domain Number Setting DIP Switches

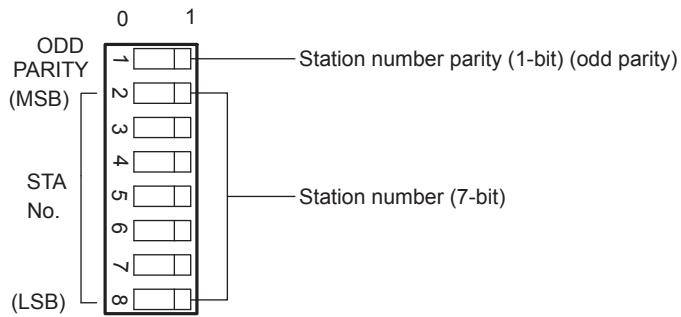
SEE ALSO

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

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

● Setting the Station Number

Set a station number from 1 to 64.



MSB : Most Significant Bit
LSB : Least Significant Bit

Figure B3.3-3 Station Number Setting DIP Switches

**SEE
ALSO**

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

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

B3.4 Configurations for the Communication Gateway Unit

This section describes the hardware setups required for the communication gateway unit.

■ Setting Up the Communication Gateway Unit

The communication gateway unit has DIP switches for setting a domain number and a station number, which determine a station address.

This section describes how to set these DIP switches.

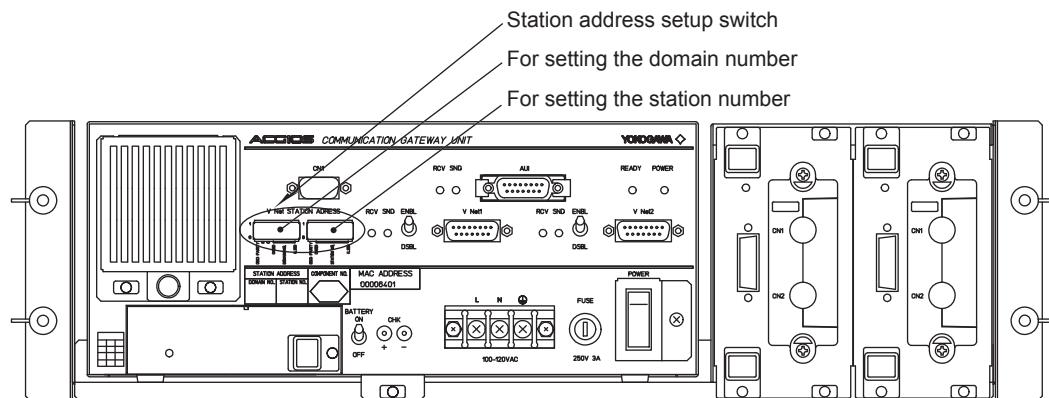
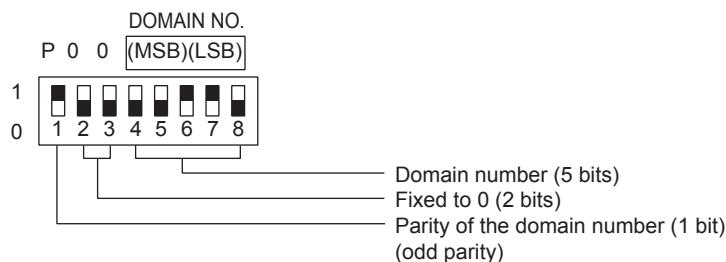


Figure B3.4-1 Locations of the DIP Switches

● 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 16. For a system consisting of one domain, always set the domain number to 1.



P (odd parity): Set in such a way that, of the 8 dip switches, the sum of those switches set to 1 becomes an odd number.

MSB: Most Significant Bit

LSB : Least Significant Bit

Figure B3.4-2 Domain Number Setting DIP Switches

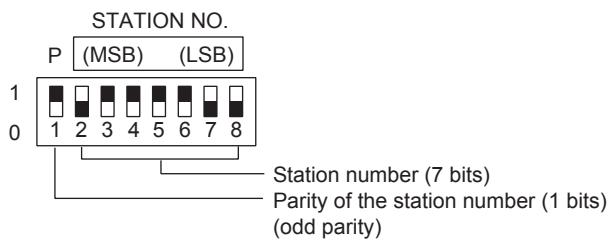
SEE ALSO

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

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

● Setting the Station Number

Set a station number in the range from 1 to 64.



P (odd parity): Set in such a way that, of the 8 dip switches, the sum of those switches set to 1 becomes an odd number.

MSB: Most Significant Bit

LSB: Least Significant Bit

Figure B3.4-3 Station Number Setting DIP Switches

**SEE
ALSO**

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

"■ Station Numbers and DIP Switch Positions" on page App.1-1

B3.5 Configurations for Wide Area Communication Routers

This section describes the hardware setups required for a wide area communication router (AW810D).

■ Setting Up the Communication Module of the Wide Area Communication Router

The communication module of the wide area communication router has DIP switches for setting a domain number and a station number, which determine a station address.

This section describes how to set these DIP switches.

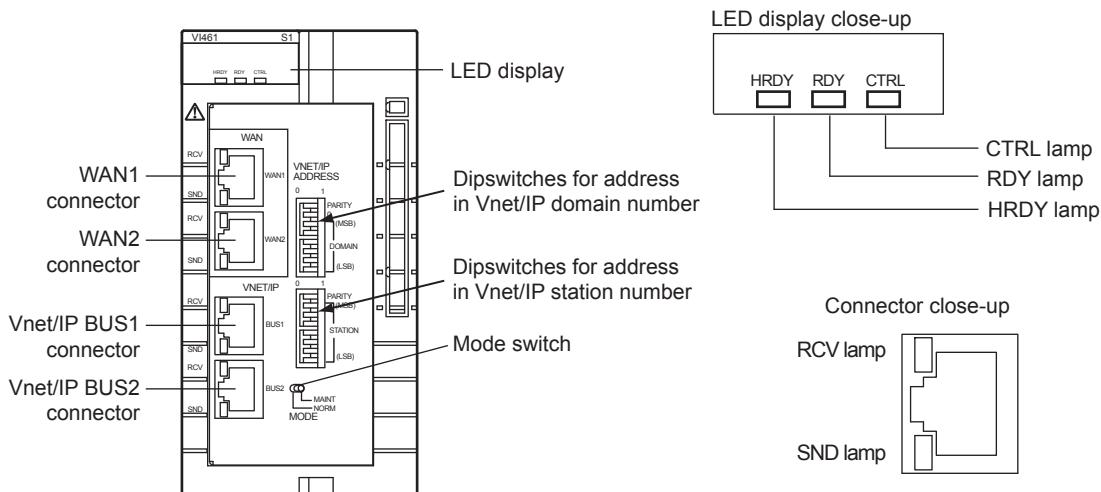


Figure B3.5-1 Locations of the DIP Switches

● 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 16. For a system consisting of one domain, always set the domain number to 1.

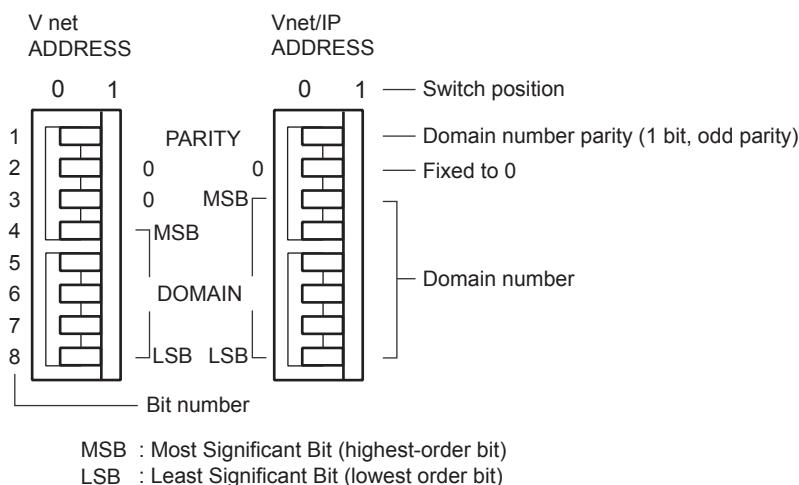


Figure B3.5-2 Domain Number Setting DIP Switches

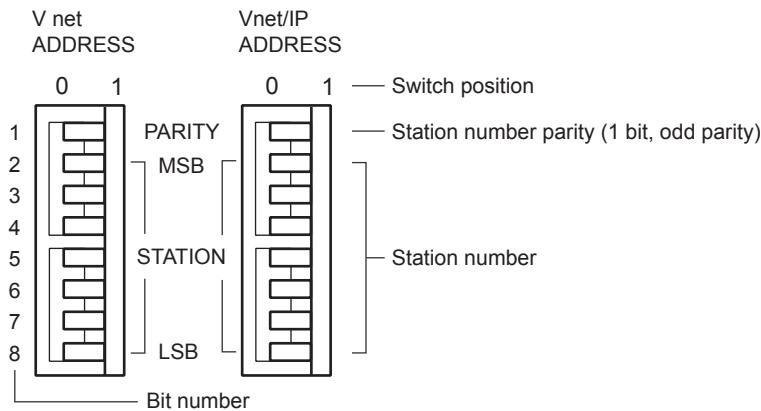
SEE ALSO

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

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

● Setting the Station Number

Set a station number from 1 to 64.



MSB : Most Significant Bit (highest-order bit)

LSB : Least Significant Bit (lowest-order bit)

Figure B3.5-3 Station Number Setting DIP Switches

SEE ALSO

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

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

B3.6 Configurations for N-IO Node Interface Unit

To use N-IO Node Interface Unit, you connect the maintenance port of the node interface unit to a computer, and specify the node number by using the software on the computer. This section describes the tool that is used for specifying the node number, and the tool that is used for switching enabled/disabled of the maintenance port.

B3.6.1 Specifying the node number by using Node Number Setting Tool

You can specify the node number by using Node Number Setting Tool. This section describes Node Number Setting Tool.

■ Summary for specifying the node number

With factory default settings, N-ESB bus module that is installed in the node interface unit of N-IO Node does not have a node number. Specifying a node number is necessary before you connect the N-ESB bus module to the FCU.

You connect the maintenance port of the N-ESB bus module to a computer, and specify the node number by using the software on the computer.

The software for specifying the node number is included in the installation medium of CENTUM VP.

■ Items to be Prepared

The following item is required to specify the node number.

- **CENTUM VP software medium**

The medium includes the USB driver and Node Number Setting Tool that are necessary to specify the node number. You install the software on the computer that you use to specify the node number.

- **Computer**

A computer that matches the following specification is required.

- **Hardware**
Needs to be conformed to the Windows 10, Windows 8.1 or Windows 7.
- **Software**
Windows 10 Pro (64bit)
Windows 8.1 Professional (64-bit, 32-bit)
Windows 7 Professional SP1 (64-bit, 32-bit)

- **USB cable**

The connector of N-ESB bus module end must be MicroUSB Micro-B.

■ Preparing the computer for specifying the node number

Install the necessary software on the computer that you use to specify the node number.

- **Installing the USB Driver**

1. Insert the CENTUM VP installation medium into the drive of the computer.
2. By using Windows Explorer or File Explorer, navigate to the following folder in the CENTUM VP installation medium.
<CENTUM VP Software Medium drive>:CENTUM\NIO_TOOLS
3. Double-click `Setup.exe` in the folder.
The User Account Control dialog box appears.
4. Click [Yes].
A dialog box appears, asking you to confirm the contents of the setup.

5. Select [INSTALL] and click [OK].
A dialog box appears, asking you to confirm to start the installation.
6. Click [OK].
7. When a Windows Security dialog box appears, Click [Install].
8. When a dialog box appears, indicating the completion of the installation, click [OK].

TIP

- If a dialog box that prompts you to restart the computer appears, click [OK] and restart the computer.
- You can install the USB driver after you connect N-ESB bus module to the computer.

● Copying Node Number Setting Tool

1. Insert the CENTUM VP installation medium into the drive of the computer.
2. By using Windows Explorer or File Explorer, navigate to the following folder in the CENTUM VP installation medium.
<CENTUM VP Software Medium drive>:CENTUM\NIO_TOOLS
3. Copy `NodeNumSetting.exe` in the folder to an optional folder.

■ Procedure for specifying the node number

This section describes the procedure for specifying the node number.

● Verification before the procedure

Before you start working on the procedure, ensure that the STAT lamp of N-ESB bus module is lit.

Unplug all cables from the two parts of N-ESB bus module to disable communications.

● Dismounting N-ESB bus module

If a node number is already specified to the N-ESB bus module, dismount one of the two parts of the module from the node interface unit. Either of two can be dismounted.

If no node number is specified to the N-ESB bus module (if ADRS lamp is not lit), you do not need to dismount the module.

● Connecting N-ESB bus module to the computer

With the USB cable, connect the USB port on the computer that you use for specifying the node number to the maintenance port on the N-ESB bus module in which power is supplied on the node interface unit.

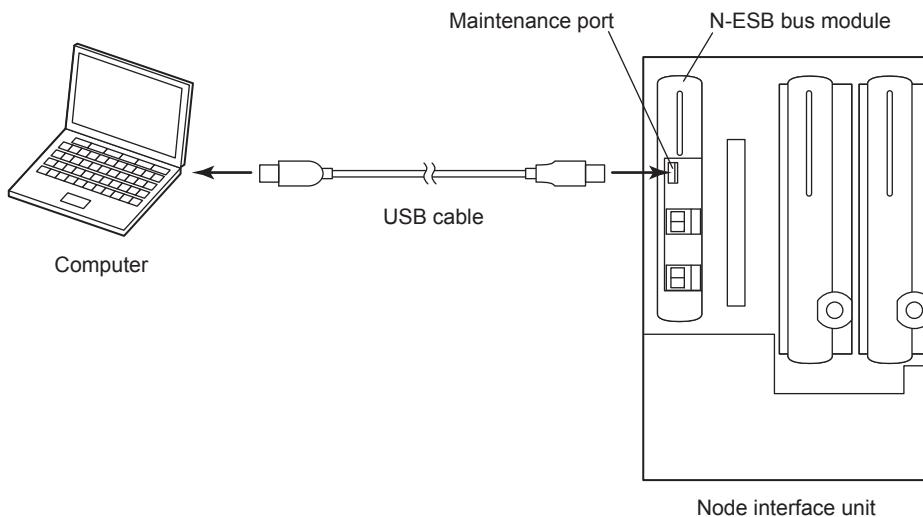


Figure B3.6.1-1 Connecting N-ESB bus module to the computer

● Operating the tool

1. Double-click to start `NodeNumSetting.exe` on the computer.
The dialog box of the Node Number Setting Tool appears.

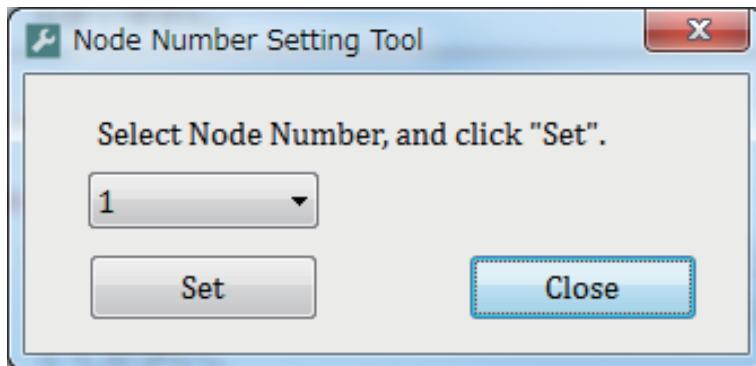


Figure B3.6.1-2 Node number Setting tool

2. Select the node number and click [Set].
A confirmation dialog box that shows the current node number and the node number that you are about to specify appears.
3. Click [Yes].
The node number is specified to the N-ESB bus module. A dialog box that notifies the completion appears.
4. Verify the node number by using the ADRS lamp on the N-ESB bus module.

SEE ALSO

For more information about the position of ADRS lamp and how to identify the node number, refer to:

“■ Structure and parts of the N-ESB bus module” in 2.4, “N-ESB bus module” in Input & Output Modules Vol.2 (IM 33J62F10-01EN)

● Specifying the node number for the remaining part of the module

If you dismounted one of the two parts of the module, perform the following procedures for the dismounted part. If you dismounted neither part of the module, proceed to the next procedure.

1. Mount the dismounted part of the module on the node interface unit.
The node number is copied from the other part of the module that has been mounted.

2. Verify the node number by using the ADRS lamp on the N-ESB bus module.

● **Procedures after specifying the node number**

1. Exit Node Number Setting Tool.
2. Unplug the USB cable from the device.
3. Plug all cables to the both parts of N-ESB bus module to enable communications.

TIP

The maintenance port of the N-ESB bus module is enabled before shipping. Before starting operation, disable the port by using N-IO Node Security Tool on HIS.

SEE

ALSO For more information about N-IO node security tool, refer to:

B3.6.2, “Switching enabled/disabled of the maintenance port” on page B3-22

B3.6.2 Switching enabled/disabled of the maintenance port

The maintenance port of the N-ESB bus module is enabled before shipping. However, from the viewpoint of security, disable the port while the system is running. If you use FieldMate Validator, enable the port while using them and disable the port after using them. This section describes the tool that is used for switching enabled/disabled of the maintenance port.

■ Overview

You can switch enabled/disabled of the maintenance port by using N-IO Node Security Tool that runs on a computer installed with system builders. N-IO Node Security Tool has following functions.

- Retrieves the status of enabled/disabled of the maintenance port.
- Switches enabled/disabled of the maintenance port on the redundant N-ESB bus modules collectively.

■ Operating the tool

This section describes how to operate the tool.

● Run permissions of the tool

The following table shows the users that can run the tool.

Table B3.6.2-1 Users that can run the tool

Security model	Users that can run the tool
Standard model	Users that belong to the following groups <ul style="list-style-type: none"> • CTM_ENGINEER, CTM_ENGINEER_LCL • CTM_ENGINEER_ADMIN, CTM_ENGINEER_ADMIN_LCL • CTM_MAINTENANCE, CTM_MAINTENANCE_LCL
Legacy model	CENTUM user

● Starting the tool

The N-IO Node Security Tool should be started on a computer installed with system builders. The following list describes the procedure to start the tool.

1. Log on to the computer installed with system builders as a user with run permissions for the tool.
2. Start the N-IO Node Security Tool.
Command Prompt appears, asking you to type the domain and station numbers.
3. Type the domain and station numbers.
The command prompt proceeds to waiting for subcommand input.

● Subcommand

After specifying the domain and station numbers, run subcommands according to the following format.

<subcommand>Δ [<node number>]

The following table shows subcommands.

Table B3.6.2-2 Subcommand

Subcommand	Description
disable [Δ <node number>]	Disables the maintenance port. If you omit the node number, the command works on all the N-IO Nodes that are specified on the station. In this case, the confirmation message appears, asking if you want to disable the ports.
enable [Δ <node number>]	Enables the maintenance port. You cannot omit the node number.
disp [Δ <node number>]	Displays the status of the port. If you omit the node number, the command works on all the N-IO Nodes that are specified on the station.
change	Changes the target station for operation by specifying the domain and station numbers.
lo [Δ <file name>]	Starts logging the results of running commands. If you specify an existing file name, the running results are added at the end of the file. If you omit the file name, the running results are output to the following file. <My Documents folder>\NioNodeSecurityLog\NioNodeSecurity_YYYYMMDD_hmmss.log YYYYMMDD: Year, month, and date hhmmss: Hour, minute, and second
lc	Stops logging the result of running commands.
help	Displays help.
quit or q	Exits the command.

● Displaying running results

When you run subcommands disp, enable, or disable, conditions are displayed according to the following table.

Table B3.6.2-3 Displaying running results

Displayed text	Meaning
DISABLED	The maintenance port is disabled.
ENABLED	The maintenance port is enabled.
MAINTENANCE	The port is in the maintenance mode.
FAIL	The N-ESB bus module does not respond.

● Displaying errors

When errors occur, error messages are displayed according to the following table.

Table B3.6.2-4 Error messages when errors occur

Message	Meaning
VHF Communication Error : v_sts 0x34 (error code)	Communication error of control bus
Invalid Domain Number (specified domain number)	The domain number is invalid.
Invalid Station Number (specified station number)	The station number is invalid.
Invalid Node Address (specified node address)	The node number is invalid.
NIU Access Error : Node1 Left code = 0x3b1c (error code)	NIU communication error

■ Command examples

This section describes examples.

● Example of starting command

The following example shows an example specifying the domain number 2 and station number 8 right after starting the command.

```
C:\> NioNodeSecurityTool
Domain? 2
Station? 8
[02-08]001:
```

- **Example of disabling the N-IO Node number**

Disables the maintenance port of node 2.

```
[02-08]002: disable
Node02 : DISABLED (Left : DISABLED Right : DISABLED)
```

- **Example of disabling all the N-IO Nodes**

Disables maintenance ports of all the specified N-IO Nodes by using the subcommand after starting the main command.

```
[02-08]003: disable
Disable All Nodes? y
Node01 : DISABLED (Left : DISABLED Right : DISABLED)
Node02 : DISABLED (Left : DISABLED Right : FAIL)
Node05 : DISABLED (Left : DISABLED Right : DISABLED)
Node06 : MAINTENANCE (Left : MAINTENANCE Right : MAINTENANCE)
```

- **Example of displaying status of maintenance ports of all specified N-IO Nodes**

Displays status of maintenance ports of all the specified N-IO Nodes by using the subcommand after starting the main command.

```
[02-08]001: disp
Node01 : ENABLED (Left : ENABLED Right : ENABLED)
Node02 : ENABLED (Left : ENABLED Right : FAIL)
Node05 : ENABLED (Left : ENABLED Right : ENABLED)
Node06 : MAINTENANCE (Left : MAINTENANCE Right : MAINTENANCE)
```

- **Example of changing the target station**

Changes the target station to domain number 3 and station number 9.

```
[02-08]004: change
Domain? 3
Station? 9
[03-09]005:
```

■ Verifying the running results

You can also verify the enabled/disabled of the maintenance port by using Status Display Panel or system alarm messages.

- **Verifying the results on Status Display Panel**

As for N-IO Node, you can verify enabled/disabled of the maintenance port by using Status Display Panel or system alarm messages.

**SEE
ALSO**

For more information about N-IO node on Status Display Panel, refer to:

4.10, "FFCS-C Status Display View" in Human Interface Stations Reference Vol.1 (IM 33J05A10-01EN)

- **Generating messages**

When any one of the maintenance ports becomes enabled where all the maintenance ports in the FCS are disabled, a message that indicates the maintenance ports are enabled is generated.

When all the maintenance ports in the FCS become disabled, a message that indicates the maintenance ports are disabled is generated.

**SEE
ALSO**

For more information about the detail of the message, refer to:

2.5, "Control Station Status Change Related Messages (Message Nos. 0400 to 0496)" in Operating Messages (IM 33J05A30-01EN)

Blank Page

B4. Setting Up CENTUM Stations or Computers

This section describes the tasks required for the new setup of CENTUM stations or computers that should be performed following the setup tasks described so far.

Related stations or computers are shown as follows.

- HIS
- APCS
- SIOS
- GSGW
- UGS
- Computer Installed with Only System Builders
- Computer Installed with Only AD Server
- UACS station
- Virtual machine

IMPORTANT

In a CENTUM VP 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 a CENTUM station such as HIS runs.

Among the stations of a CENTUM VP system, you must set up the license management station first. Then, set up the computers that will be used as license-assigned stations, and distribute and accept licenses from the license management station. The software packages thus become available for use on the license-assigned stations.

You can also set up the license management station as the computer dedicated to license management.

TIP

Refer to the GS and TI regarding virtualization platform for details of functions that can be virtualized by using the virtualization platform.

SEE ALSO

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

B7., “Setting Up the Computer Dedicated to License Management” on page B7-1

■ Items to be Prepared

Have the following items at hand before new installation of the CENTUM VP software.

- CENTUM VP R6 software medium
- CENTUM VP license medium (only required on the license management station when distributing licenses)

B4.1 Setting Up the Hardware

This section describes the hardware setups that are required for the main stations and computers.

However, these hardware setups are not required for a computer with only the AD server function, a computer switchover type UGS, and a virtualization host computer.



CAUTION

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 prevention of static electricity, refer to:

A6.1, "Precautions against Static Electricity" in Peripherals (IM 33J50B10-01EN)

■ 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.

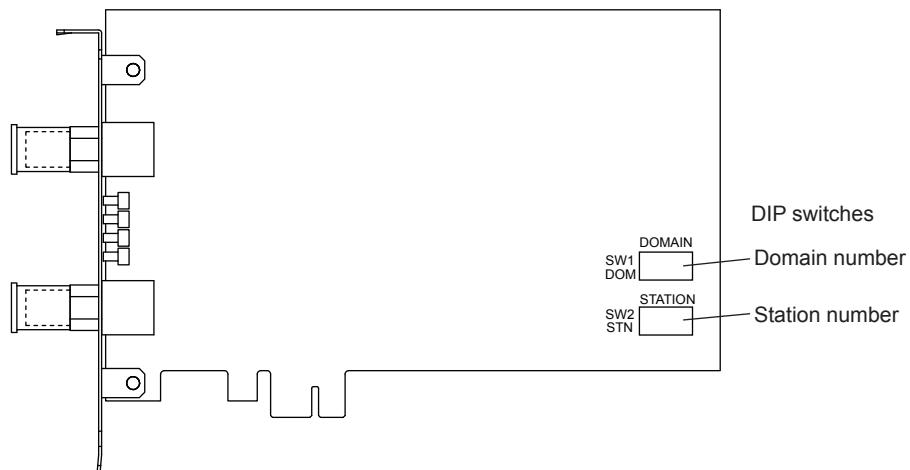
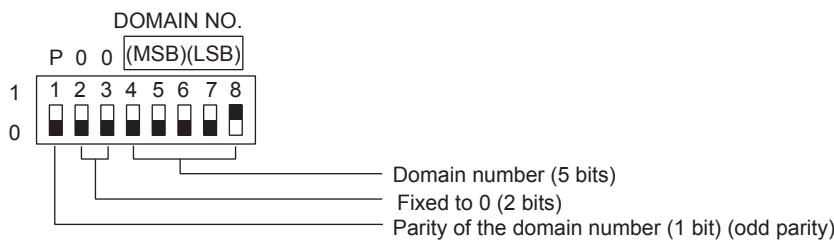


Figure B4.1-1 Location of DIP Switches

● 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 16.



MSB : Most Significant Bit
LSB : Least Significant Bit

Figure B4.1-2 Domain Number Setting DIP Switches

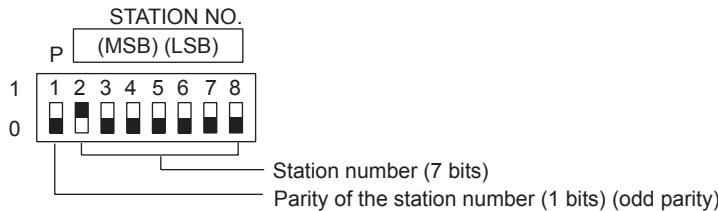
SEE ALSO

For more information about domain numbers and the 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 B4.1-3 Station Number Setting DIP Switches

SEE ALSO

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

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

● **Precautions When 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.

● **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:

- Turn off the power of the computer. For safety, remove the power plug from the outlet.
- Remove the cover of the computer.
- Unscrew the screws fixing the slot cover and remove the slot cover.
- Insert the VF702/VF701 card in the corresponding slot and fix it to the slot.
- 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 bus. 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 properly before configuring network settings.

This section describes how to set the DIP switches.

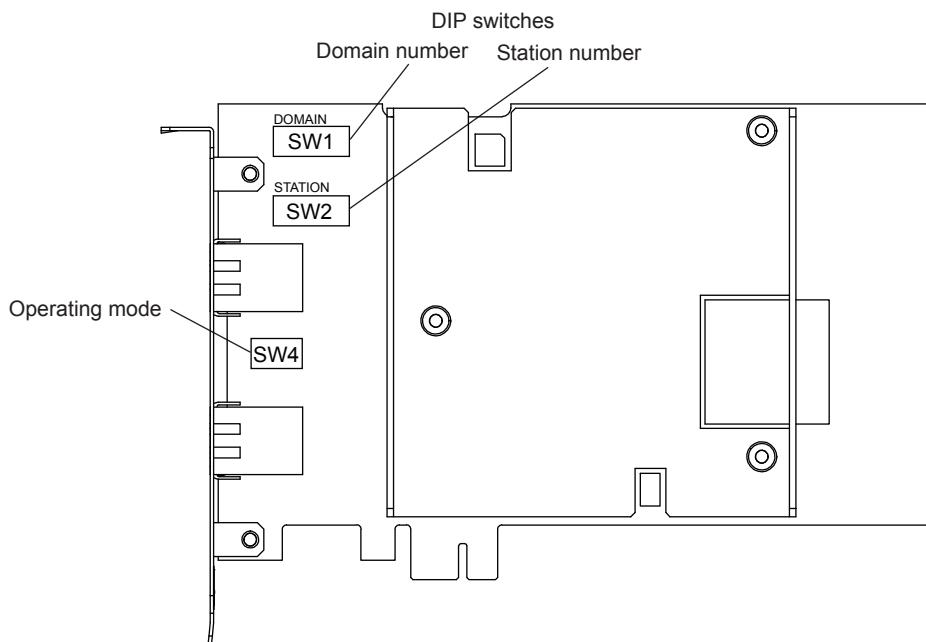
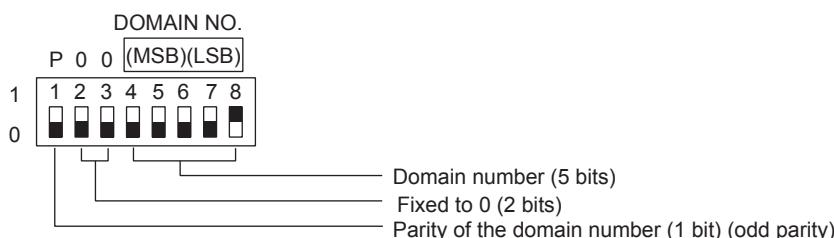


Figure B4.1-4 Locations of the DIP Switches

● 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 16.



MSB : Most Significant Bit
LSB : Least Significant Bit

Figure B4.1-5 Domain Number Setting DIP Switches

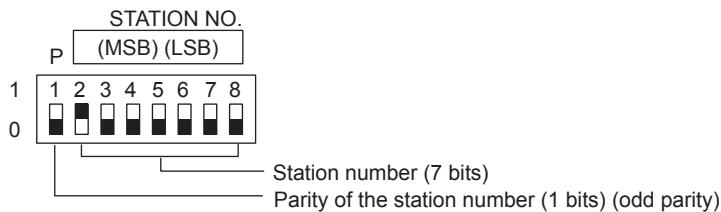
SEE ALSO

For more information about domain numbers and the 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 B4.1-6 Station Number Setting DIP Switches

SEE ALSO

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

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

● 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:

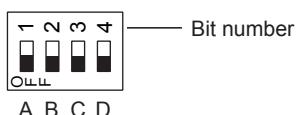


Figure B4.1-7 Action Mode Switch

Table B4.1-1 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 When Installing the Vnet/IP Interface Card

- Install a Vnet/IP interface card in the computer after setting up Windows but before configuring the network settings.
- Install network drivers when you restart the computer after installing the Vnet/IP interface card. Follow the procedure in this manual to install the drivers.

- **Installing the Vnet/IP Interface Card**

After you have set the station address and action mode on the Vnet/IP interface 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 Vnet/IP interface 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 the Vnet/IP interface card and Layer 2 switch. There is no need to turn off the power of the Layer 2 switch.
7. Put the power cord of the computer back to the outlet and turn on the computer.
8. Make sure that the RDY lamp on the Vnet/IP interface card is lit.
9. Write the station address on the label that comes with the Vnet/IP interface card and paste it in the front or other easy-to-see location of the computer.

B4.2 Setting Up Windows

Before installing the software for this product, 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.

■ Windows Setting Items and Required Settings on Each Station

The Windows setting items you need to configure before installing the software for this product vary, depending on the type of the station and Windows OS. Configure the required Windows settings based on the following table.

Table B4.2-1 Windows Setting Items and Whether Configuration is Required on Each Station

Windows setting item	HIS	APCS	SIOS	GSGW	UGS	UACS station	Computer installed with only system builders	Computer installed with only AD Server
File System	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Performance	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Virtual Memory	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Power Options	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Turning off fast startup (*1)	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Windows Defender(*2)	Yes	Yes	Yes	Yes	Yes (*3)	Yes	Yes	Yes
Windows Update (*4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Disk Defragmenter (*5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Password setting (*6)	Yes	Yes	No	Yes	No (*7)	Yes	Yes	Yes
Root certificate (*8)	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Windows update program	Yes (*9)	Yes (*10)	Yes (*11)	Yes (*11)	Yes (*12)	No	Yes (*13)	Yes (*11)
DCOM Settings	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

*1: Only on Windows 10

*2: Only on Windows 10, Windows 7, Windows Server 2016, and Windows Server 2008 R2

*3: "No" for computer switchover type UGS.

*4: Only on Windows 10, and Windows Server 2016

*5: Only on Windows 10, Windows 7, Windows Server 2016, and Windows Server 2012 R2

*6: Only on Windows Server 2016, Windows Server 2012 R2, and Windows Server 2008 R2

*7: "Yes" for computer switchover type UGS.

*8: Only on Windows 7 and Windows Server 2008 R2

*9: "Yes" for Windows 7 or Windows Server 2008 R2. "Yes" for HIS with system builders on Windows 10. Otherwise, "No."

*10: "Yes" for Windows Server 2008 R2. Otherwise, "No."

*11: "Yes" for Windows 7 or Windows Server 2008 R2. Otherwise, "No."

*12: "Yes" for Windows Server 2012 R2. Otherwise, "No."

*13: "Yes" for Windows 10, Windows 7, or Windows Server 2008 R2. Otherwise, "No."

B4.2.1 Configuring on Windows 10

Follow these procedures when you use a Windows 10 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. Sign in as an administrative user.
2. Open Control Panel.
3. Select [System and Security] > [System] > [Advanced system settings].
The System Properties dialog box appears.
4. Select the [Advanced] tab, and click [Settings] in the Performance section.
The Performance Options dialog box appears.
5. Click the [Visual Effects] tab and select [Let Windows choose what's best for my computer].
6. Click [OK].

■ Virtual Memory

A custom size is recommended for setting the virtual memory. Follow these steps:

1. Sign in as an administrative user.
2. Open Control Panel.
3. Select [System and Security] > [System] > [Advanced system settings].
The System Properties dialog box appears.
4. Select the [Advanced] tab, and click [Settings] in the [Performance] section.
The Performance Options dialog box appears.
5. Select the [Advanced] tab, select [Programs] under [Adjust for best performance of] and then, in the [Virtual Memory] area, click [Change].
The Virtual Memory dialog box appears.
6. Clear the [Automatically manage paging file size for all drives] check box.
7. Select [Custom size] and set the Initial size and the Maximum size to a value 1.5 times the main memory capacity.
For example, set the custom size to 9216 MB if the main memory capacity is 6 GB, or 12288 MB if 8 GB.
8. Click [Set] and then click [OK].

TIP

After setting the virtual memory, a message box for restarting the computer to validate the virtual memory may be displayed. If displayed, follow the instruction of the dialog to restart the computer.

■ 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. Sign in as an administrative user.
2. Open Control Panel.
3. Select [Hardware and Sound] > [Power Options].
The Power Options window appears.
4. Select [High performance] under Preferred plans and click [Change plan settings] on the right side.
The Edit Plan Settings window appears.

TIP

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

5. Click [Change advanced power settings].
The Power Options dialog box appears.

TIP

Some of the advanced setting items explained hereafter may not be displayed, depending on the computer configuration. If not displayed, the functions of such items are not available.

6. Under Hard disk, set the setting for Turn off hard disk after to [Never].
7. Configure the Sleep settings as follows:
 - [Sleep after]: Never
 - [Allow hybrid sleep]: Off
 - [Hibernate after]: Never
 - [Allow wake timers]: Disable
8. Set the setting for Power button action under Power buttons and lid to [Shut down].
9. Configure the Display settings as follows:
 - [Turn off display after]: Never
 - [Enable adaptive brightness]: Off
10. Click [OK].

TIP

Configure the UPS service settings after installing the software for this product.

■ Turning Off Fast Startup

You must turn off fast startup before installing the control bus driver or Vnet/IP open communication driver.

Follow these steps to turn off fast startup:

1. Sign in as an administrative user.
2. Open the Control Panel.
3. Select [Hardware and Sound] > [Power Options].
The Power Options window appears.
4. In the left pane, click [Choose what the power button does].

The System Settings window appears.

5. Click [Change settings that are currently unavailable].
6. The [Turn on fast startup (recommended)] check box appears under [Shutdown settings]. Clear the check box if it is selected.

TIP

If the [Turn on fast startup (recommended)] check box does not appear, this setting is not required.

7. Click [Save changes].
8. Restart the computer.

IMPORTANT

After turning off fast startup, you must restart the computer.

■ Windows Defender

The Windows Defender software detects and removes spy ware.

It is recommended to turn off this function because it is not used with this product.

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 the Local Group Policy Editor.

● Turning Off Windows Defender in Local Group Policy Editor

Follow these steps to turn off Windows Defender:

1. Sign in as an administrative user.
2. Open Command Prompt.
3. Enter `gpedit.msc`.
Local Group Policy Editor appears.
4. In the left pane, select [Computer Configuration] > [Administrative Templates] > [Windows Components] > [Windows Defender].
5. In the right pane, double-click [Turn off Windows Defender].
The Turn off Windows Defender dialog box appears.
6. Select [Enabled] and click [OK].

■ Windows Update

Windows Update is a feature that updates Windows.

In this product, you must disable Windows Update for the following reasons:

- With Windows Update enabled, it takes longer time to install the software for this product.
- Components running the software for this product are expected to run continuously, but the computer will restart automatically when Windows Update is enabled.

TIP

To use Windows Server Update Service (WSUS), install the software for this product first, manually enable Windows automatic updates, and then set the WSUS.

Follow these steps to disable Windows Update:

1. Sign in as an administrative user.
2. Open the Command Prompt.
3. Type gpedit.msc.
Local Group Policy Editor appears.
4. In the left pane, select [Computer Configuration] > [Administrative Templates] > [Windows Components] > [Windows Update].
5. In the right pane, double-click [Configure Automatic Updates].
The Configure Automatic Updates dialog box appears.
6. Select [Disabled] and click [OK].

SEE ALSO

For more information about the procedure for enabling Windows Update manually, refer to:

- ["Enabling Windows Update" on page C7-7](#)

■ Defragment and Optimize Drives

The Defragmenter Tool can be used to reorganize the fragmented files on computer hard disk so as to improve the computer performance. Since the performance of this product may be affected when defragmenter is running, it is recommended to disable the schedule of 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. Sign in as an administrative user.
2. Open Control Panel.
3. Select [System and Security] > [Administrative Tools] > [Defragment and Optimize Drives].
The Optimize Drives window appears.
4. Click [Change settings].
The Optimize Drives dialog box appears.
5. Clear the [Run on a schedule (recommended)] check box and click [OK].

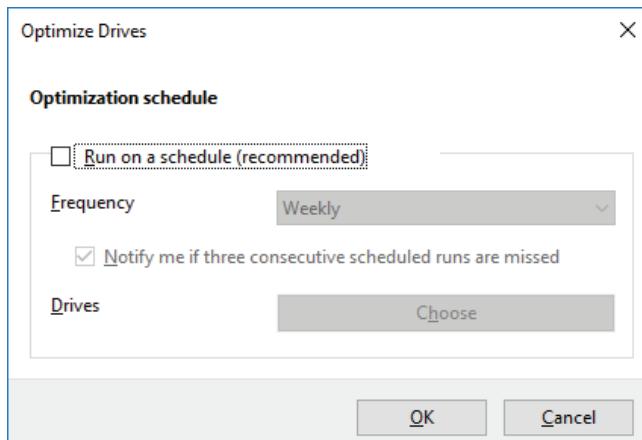


Figure B4.2.1-1 Optimize Drives dialog box

■ Disabling the Automatic Cleanup Task

A function to automatically clean up obsolete files upon application of update programs has been added.

Considering the degradation in system performance that may be caused by execution of automatic cleanup, we recommend to disable the automatic cleanup task.

Follow these steps to disable the automatic cleanup task:

1. Sign in as an administrative user.
2. Open Control Panel.
3. Select [System and Security] > [Administrative Tools] > [Task Scheduler].
The Task Scheduler window appears.
4. In the left pane, select [Task Scheduler (Local)] > [Task Scheduler Library] > [Microsoft] > [Windows] > [Servicing].
5. In the middle pane, right-click [StartComponentCleanup] and select [Disable].

■ Installing the Windows Update Programs

Download and apply the Windows update programs.

**SEE
ALSO**

For more information about downloading Windows update programs, refer to:

- “● Downloading the Windows Update Programs (Windows 10)” on page B1-3
-

■ DCOM Settings

When Default Authentication Level in DCOM settings is set to [None], installation of applications such as redistributable modules fails. When installing this product, set the Default Authentication Level to [Connect]. Follow these steps to set Default Authentication Level to [Connect]:

1. Sign in as an administrative user.
2. Open Control Panel.
3. Select [System and Security] > [Administrative Tools] > [Component Services].
The Component Services window appears.

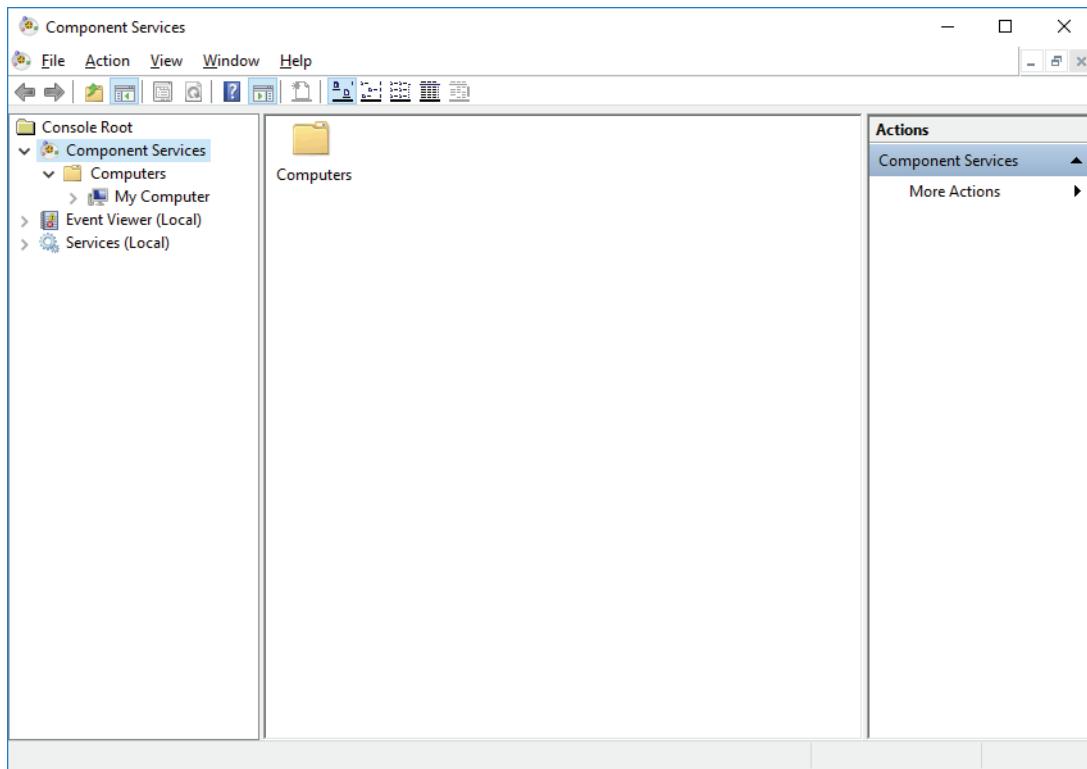


Figure B4.2.1-2 Component Services Window

4. Select [Console Root] > [Component Services] > [Computers].
5. Right-click [My Computer] and select [Properties].
The My Computer Properties dialog box appears.

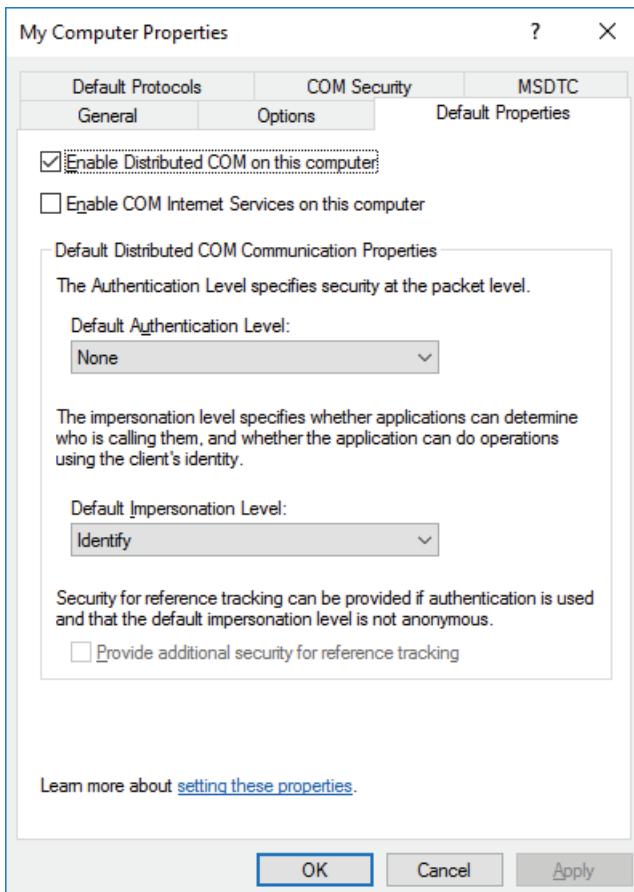


Figure B4.2.1-3 My Computer Properties Dialog Box

6. Open the Default Properties tab, from the [Default Authentication Level] drop-down list, select [Connect], and then click [OK].
7. Restart the computer.

B4.2.2 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 the partition of the operating system is already formatted in FAT, reinstall the operating system to reformat it 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. Open Control Panel.
3. Select [System and Security] > [System] > [Advanced system settings].
The System Properties dialog box appears.
4. Select the [Advanced] tab, and click [Settings] in the Performance section.
The Performance Options dialog box appears.
5. Click the [Visual Effects] tab and select [Let Windows choose what's best for my computer].

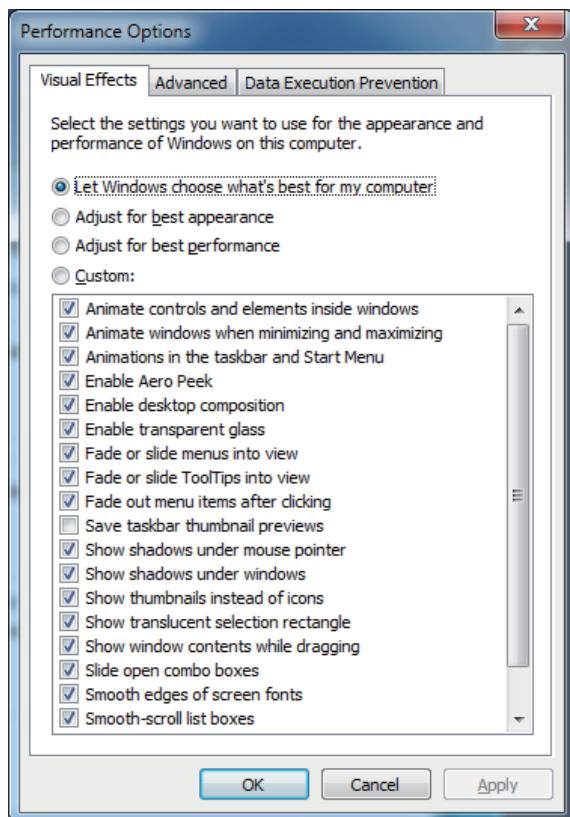


Figure B4.2.2-1 Performance Options Dialog Box (Visual Effects Tab)

6. Click [OK].

■ Virtual Memory

A custom size is recommended for setting the virtual memory. Follow these steps:

1. Log on as an administrative user.
2. Open Control Panel.
3. Select [System and Security] > [System] > [Advanced system settings].
The System Properties dialog box appears.
4. Select the [Advanced] tab, and click [Settings] in the [Performance] section.
The Performance Options dialog box appears.
5. On the [Advanced] tab, select [Programs] under [Adjust for best performance of] and then, in the [Virtual Memory] area, click [Change].
The Virtual Memory dialog box appears.
6. Clear the [Automatically manage paging file size for all drives] check box.
7. Select [Custom size] and set the Initial size and the Maximum size to a value 1.5 times the main memory capacity.
For example, set the custom size to 9216 MB if the main memory capacity is 6 GB, or 12288 MB if 8 GB.

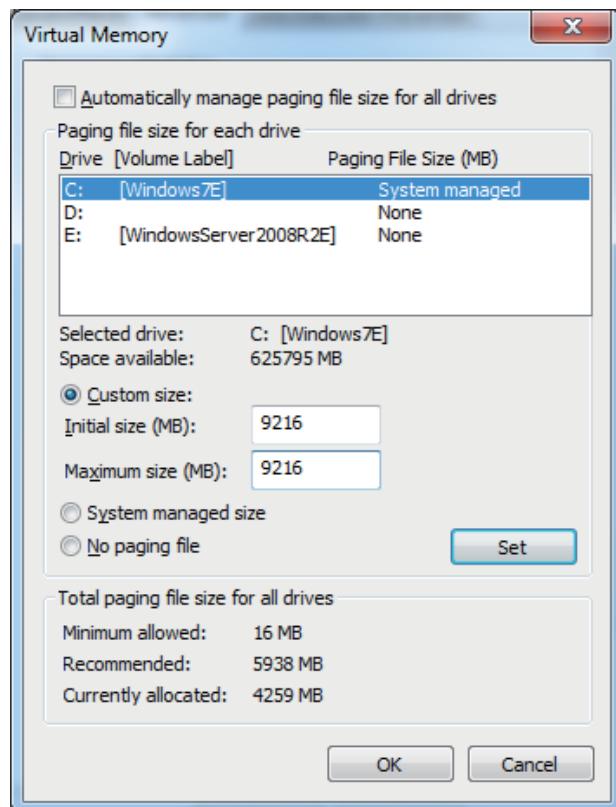


Figure B4.2.2-2 Virtual Memory Dialog Box

8. Click [Set] and then click [OK].

TIP

After setting the virtual memory, a message box for restarting the computer to validate the virtual memory may be displayed. If displayed, follow the instruction of the dialog to restart the computer.

■ 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. Open Control Panel.
3. Select [Hardware and Sound] > [Power Options].
The Power Options dialog box appears.
4. 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.

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

TIP

Some of the advanced setting items explained hereafter may not be displayed, depending on the computer configuration. If not displayed, the functions of such items are not available.

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

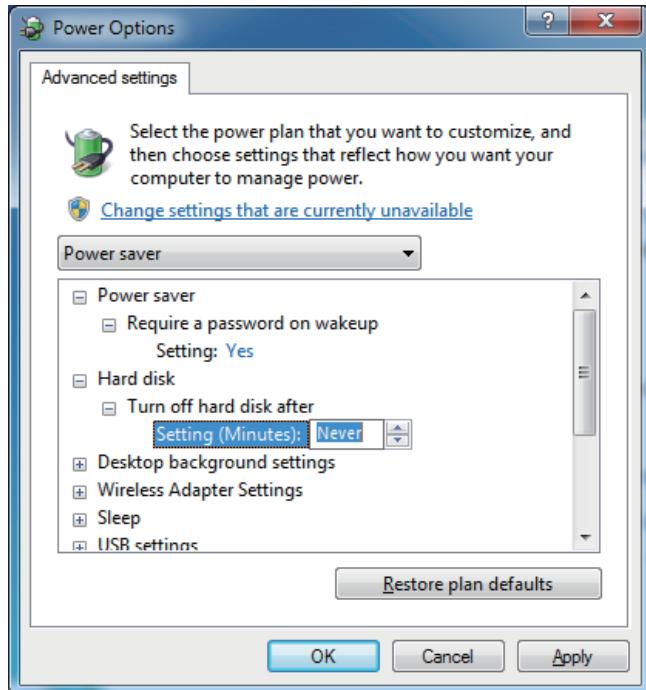


Figure B4.2.2-3 Power Options Advanced Settings

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

- [Allow wake timers]: Disable

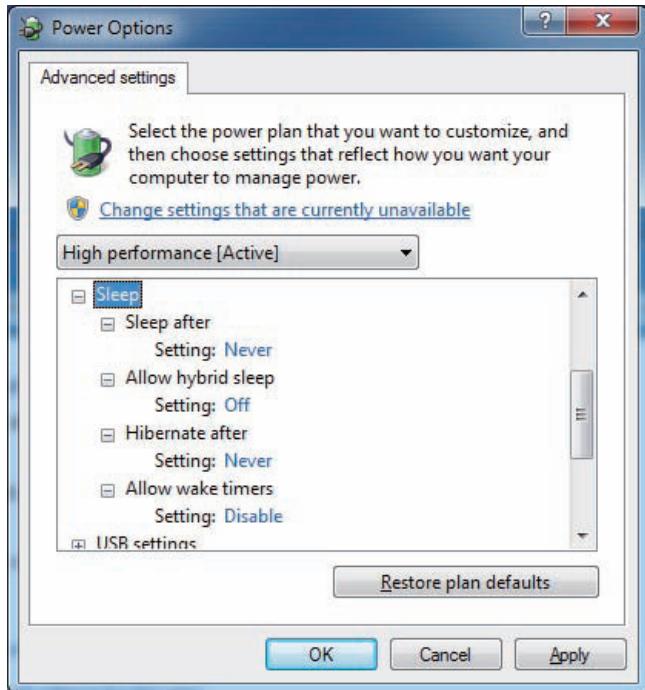


Figure B4.2.2-4 Power Options Advanced Settings

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

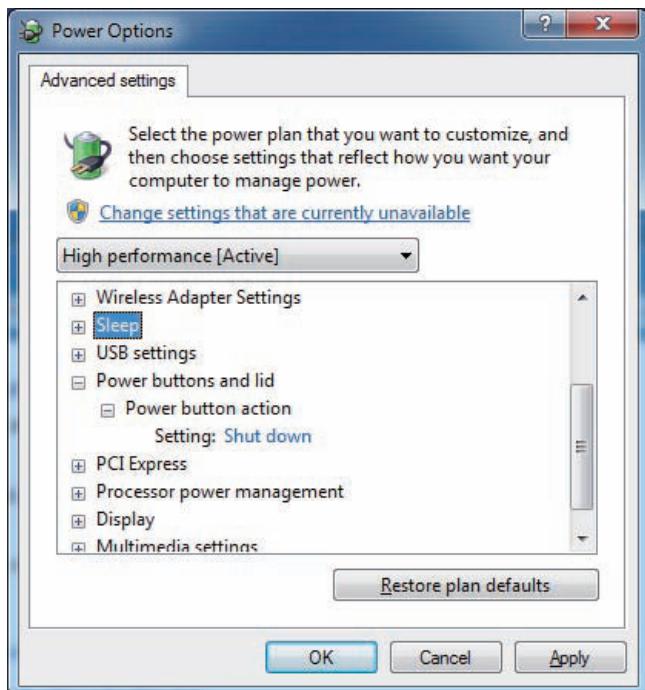


Figure B4.2.2-5 Power Options Advanced Settings

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

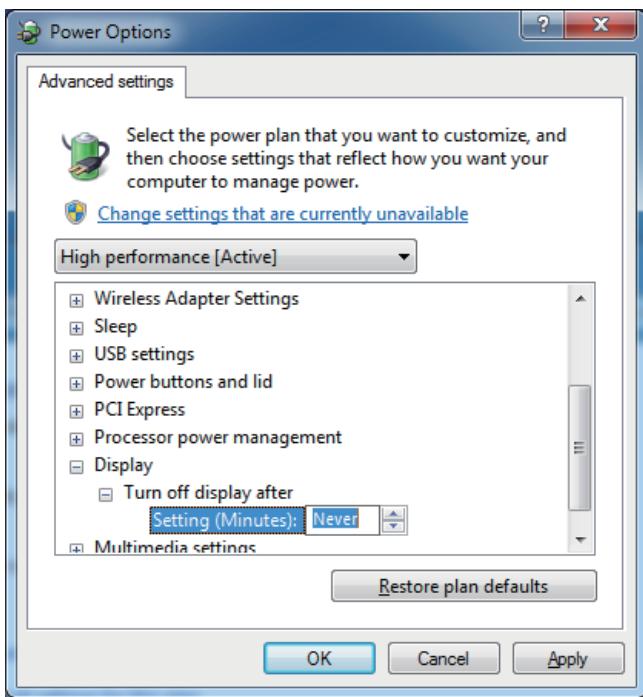


Figure B4.2.2-6 Power Options Advanced Settings

10. Click [OK].

TIP

Configure UPS service settings after installing the software for this product.

SEE ALSO

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

B4.12, "Setting Up the Uninterruptible Power Supply (UPS) Service" on page B4-149

■ Windows Defender

The Windows Defender software detects and removes spy ware.

It is recommended to turn off this function because it is not used with this product.

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. Open 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].

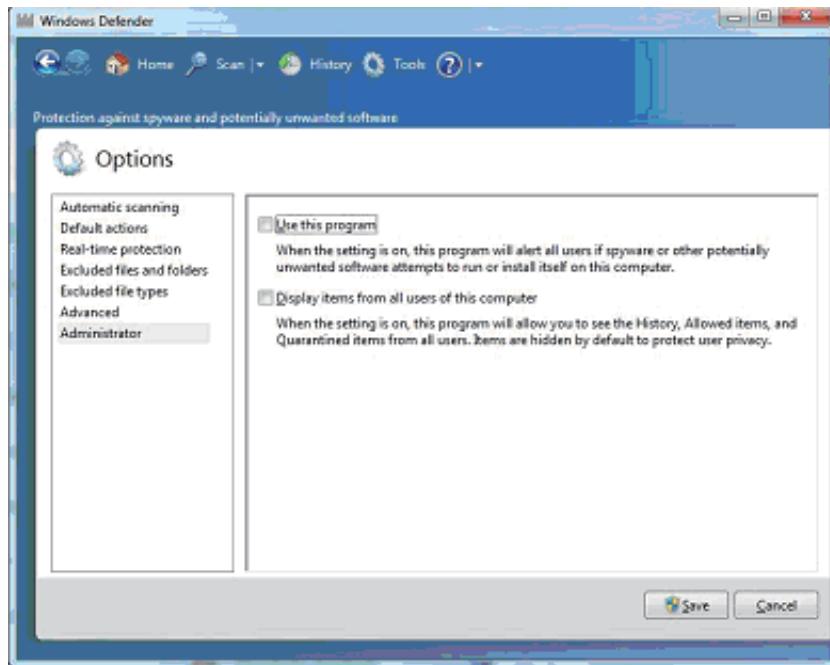


Figure B4.2.2-7 Options

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

● Turning Off Windows Defender in Local Group Policy Editor

TIP

If [Tools] of Windows Defender is disabled and cannot be selected, 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. Open Command Prompt.
3. Enter `gpedit.msc`.
Local Group Policy Editor window appears.
4. 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.
5. Select [Enabled] and click [OK].

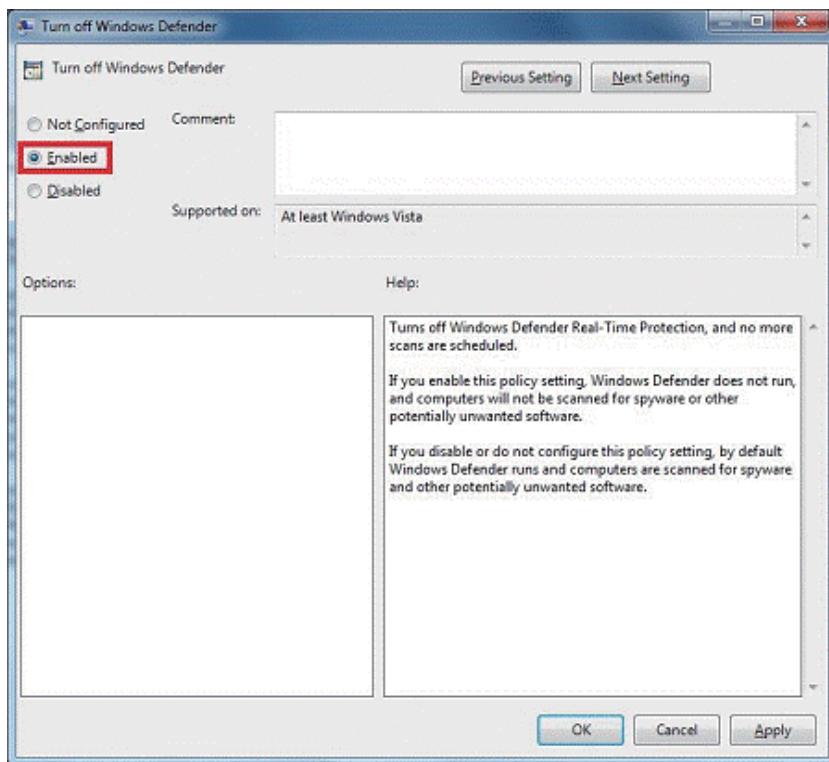


Figure B4.2.2-8 Turn Off Windows Defender Dialog Box

■ Disk Defragmenter

Disk Defragmenter 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 is scheduled to start periodically at 1:00 on Wednesday. Since the performance of this product may be affected when defragmenter is running, it is recommended to disable the schedule of 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. Start Disk Defragmenter.
3. Click [Configure schedule...].
The Modify Schedule dialog box appears.
4. Clear the [Run on a schedule (recommended)] check box and click [OK].

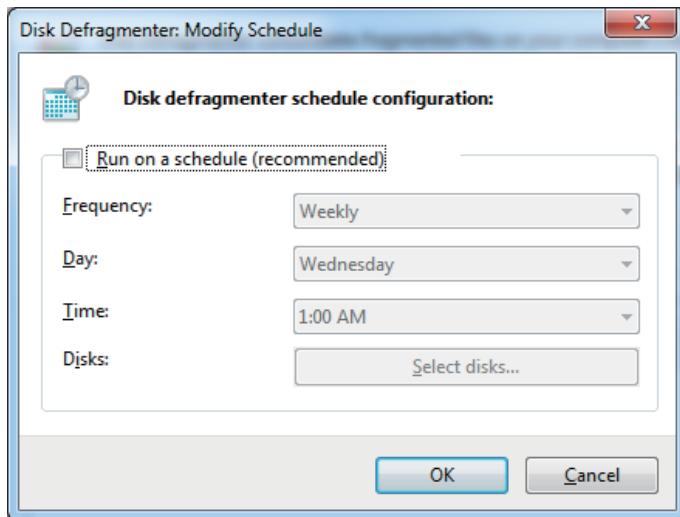


Figure B4.2.2-9 Modify Schedule Dialog Box

■ Applying the root certificate

By default, Windows 7 does not come with the root certificate needed to verify the .NET Framework 4.6.2 package certificate. Accordingly, any attempt to install .NET Framework 4.6.2 will fail in the offline environment.

The root certificate needed to install .NET Framework 4.6.2 (Microsoft Root Certificate Authority 2011) must be applied.

Follow these steps to apply the root certificate:

1. Log on as an administrative user who installs the CENTUM VP software.

IMPORTANT

This setting must be made for each user. Because .NET Framework 4.6.2 is installed during installation of the CENTUM VP software, you must log on as an administrative user who installs the CENTUM VP software, not as any other administrative user.

2. Insert the CENTUM VP software medium into the drive.
3. Open Command Prompt.
4. Enter `certmgr.msc`.
The certmgr starts.
5. In the left pane, right-click [Trusted Root Certification Authorities] and select [All Tasks] > [Import].
The Certificate Import Wizard appears.
6. Click [Next].
The File to Import page appears.
7. Click [Browse] and specify the following file.
<CENTUM VP software medium drive>:\Microsoft\Certificates\MicrosoftRootCertificateAuthority2011.cer
8. Click [Next].
The Certificate Store page appears.
9. Select [Place all certificates in the following store] and click [Next].
The Completing the Certificate Import Wizard page appears.

10. Click [Finish].
The Security Warning dialog box appears.
11. Click [Yes].
The Certificate Import Wizard dialog box appears, and the certificate import is completed.

■ Installing the Windows Update Programs

Download and apply the Windows update programs.

**SEE
ALSO**

For more information about the procedure to download the Windows update program, refer to:

- “● Downloading the Windows Update Program (Windows 7 or Windows Server 2008 R2)” on page B1-4
-

B4.2.3 Configuring on Windows Server 2016

Follow these steps when you use a Windows Server 2016 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. Sign in as an administrative user.
2. Open Control Panel.
3. Select [System and Security] > [System] > [Advanced system settings].
The System Properties dialog box appears.
4. On the [Advanced] tab, click [Settings] in the Performance section.
The Performance Options dialog box appears.
5. On the [Visual Effects] tab, select [Let Windows choose what's best for my computer].
6. Click [OK].

■ Virtual Memory

A custom size is recommended for setting the virtual memory. Follow these steps:

1. Sign in as an administrative user.
2. Open Control Panel.
3. Select [System and Security] > [System] > [Advanced system settings].
The System Properties dialog box appears.
4. On the [Advanced] tab, click [Settings] in the [Performance] section.
The Performance Options dialog box appears.
5. On the [Advanced] tab, select [Programs] under [Adjust for best performance of] and then, in the [Virtual Memory] area, click [Change].
The Virtual Memory dialog box appears.
6. Clear the [Automatically manage paging file size for all drives] check box.
7. Select [Custom size] and set the Initial size and the Maximum size to a value 1.5 times the main memory capacity.
For example, set the custom size to 9216 MB if the main memory capacity is 6 GB, or 12288 MB if 8 GB.
8. Click [Set] and then click [OK].

TIP

After setting the virtual memory, a message box for restarting the computer to validate the virtual memory may be displayed. If displayed, follow the instruction of the dialog to restart the computer.

■ 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. Sign in as an administrative user.

2. Open Control Panel.
3. Select [Hardware] > [Power Options].
The Power Options window appears.
4. Select [High performance] under Preferred plans and click [Change plan settings] on the right side.
The Edit Plan Settings window appears.

TIP

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

5. Click [Change advanced power settings].
The Power Options dialog box appears.

TIP

Some of the setting items explained hereafter may not be displayed, depending on the computer configuration. If not displayed, the functions of such items are not available.

6. Under Hard disk, set the setting for Turn off hard disk after to [Never].
7. Configure the Sleep settings as follows:
 - [Sleep after]: Never
 - [Allow hybrid sleep]: Off
 - [Hibernate after]: Never
 - [Allow wake timers]: Disable
8. Set the setting for Power button action under Power buttons and lid to [Shut down].
9. Configure the Display settings as follows:
 - [Turn off display after]: Never
 - [Enable adaptive brightness]: Off
10. Click [OK].

TIP

Configure UPS service settings after installing the software for this product.

■ Windows Defender

The Windows Defender software detects and removes spy ware.

It is recommended to turn off this function because it is not used with this product.

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 the Local Group Policy Editor.

● Turning off Windows Defender in Local Group Policy Editor

Follow these steps to turn off Windows Defender:

1. Sign in as an administrative user.
2. Open Command Prompt.
3. Enter `gpedit.msc`.
Local Group Policy Editor appears.

4. In the left pane, select [Computer Configuration] > [Administrative Templates] > [Windows Components] > [Windows Defender].
5. In the right pane, double-click [Turn off Windows Defender].
The Turn off Windows Defender dialog box appears.
6. Select [Enabled] and click [OK].

■ Windows Update

Windows Update is a feature that updates Windows.

In this product, you must disable Windows Update for the following reasons:

- With Windows Update enabled, it takes longer time to install the software for this product.
- Components running the software for this product are expected to run continuously, but the computer will restart automatically when Windows Update is enabled.

TIP

To use Windows Server Update Service (WSUS), install the software for this product first, manually enable Windows automatic updates, and then set the WSUS.

Follow these steps to disable Windows Update:

1. Sign in as an administrative user.
2. Open Command Prompt.
3. Enter gpedit.msc.
Local Group Policy Editor appears.
4. In the left pane, select [Computer Configuration] > [Administrative Templates] > [Windows Components] > [Windows Update].
5. In the right pane, double-click [Configure Automatic Updates].
The Configure Automatic Updates dialog box appears.
6. Select [Disabled] and click [OK].

SEE ALSO

For more information about the procedure for enabling Windows Update manually, refer to:

“■ Enabling Windows Update” on page C7-7

■ Defragment and Optimize Drives

The Defragmenter Tool can be used to reorganize the fragmented files on computer hard disk so as to improve the computer performance. Since the performance of this product may be affected when the defragmenter is running, it is recommended to disable the schedule of 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. Sign in as an administrative user.
2. Open Control Panel.
3. Select [System and Security] > [Administrative Tools] > [Defragment and Optimize Drives].
The Optimize Drives window appears.
4. Click [Change settings].
The Optimize Drives dialog box appears.
5. Clear the [Run on a schedule (recommended)] check box and click [OK].

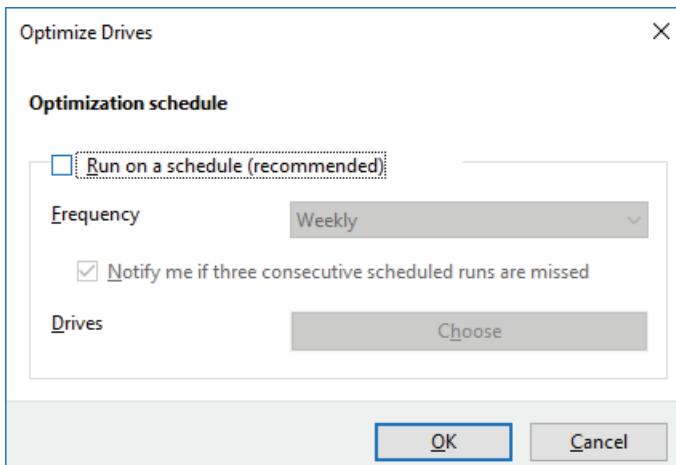


Figure B4.2.3-1 Optimize Drives Dialog Box

■ Disabling the Automatic Cleanup Task

A function to automatically clean up obsolete files upon application of update programs has been added.

Considering the degradation in system performance that may be caused by execution of automatic cleanup, we recommend to disable the automatic cleanup task.

Follow these steps to disable the automatic cleanup task:

1. Sign in as an administrative user.
2. Open Control Panel.
3. Select [System and Security] > [Administrative Tools] > [Task Scheduler].
The Task Scheduler window appears.
4. In the left pane, select [Task Scheduler (Local)] > [Task Scheduler Library] > [Microsoft] > [Windows] > [Servicing].
5. In the middle pane, right-click [StartComponentCleanup] and select [Disable].

■ Password Setting

Because security is enhanced in Windows Server 2016, 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. Sign in as an administrative user.
2. Open Control Panel.
3. Select [System and Security] > [Administrative Tools] > [Local Security Policy].
The Local security policy window appears.
4. In the left pane, select [Security Settings] > [Account Policies] > [Password Policy].
A list of policies is displayed.
5. In the right pane, double-click [Password must meet complexity requirements].
The properties dialog box for the Password must meet complexity requirements appears.
6. Select [Disabled] and click [OK].
7. Confirm that [Password must meet complexity requirements] is set to Disabled.

■ DCOM Settings

When Default Authentication Level in DCOM settings is set to [None], installation of applications such as redistributable modules fails. When installing this product, set the Default Authentication Level to [Connect]. Follow these steps to set Default Authentication Level to [Connect]:

1. Sign in as an administrative user.
2. Open Control Panel.
3. Select [System and Security] > [Administrative Tools] > [Component Services].
The Component Services window appears.

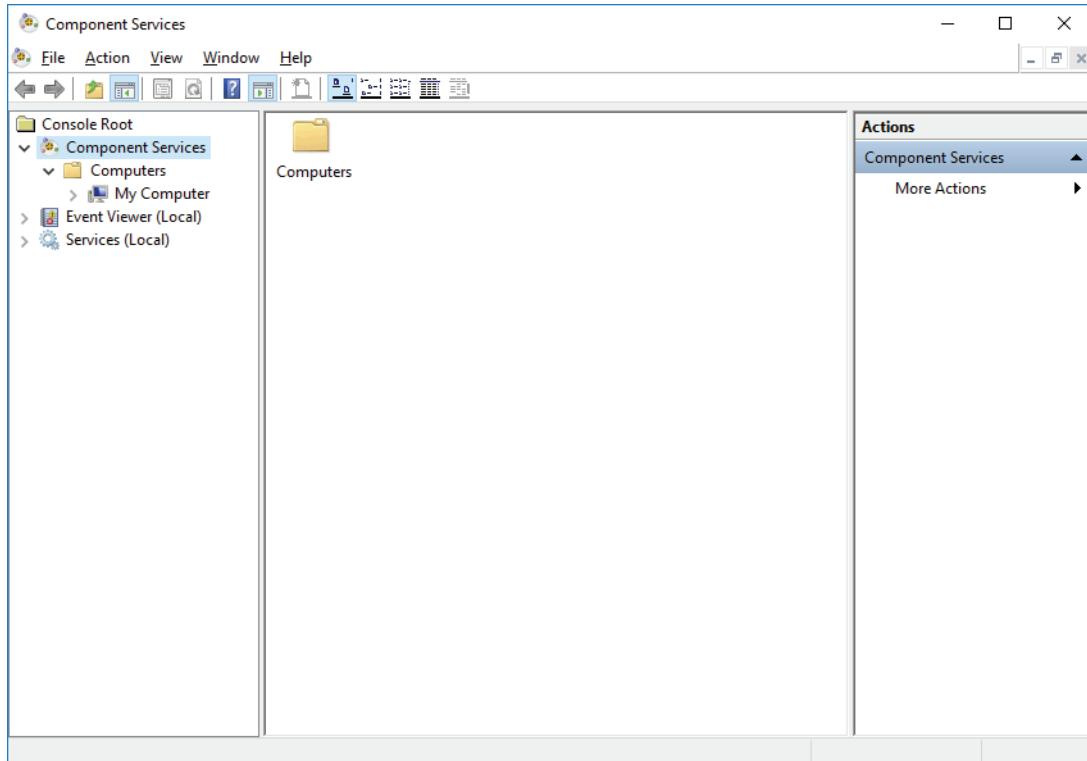


Figure B4.2.3-2 Component Services Window

4. Select [Console Root] > [Component Services] > [Computers].
5. Right-click [My Computer] and select [Properties].
The My Computer Properties dialog box appears.

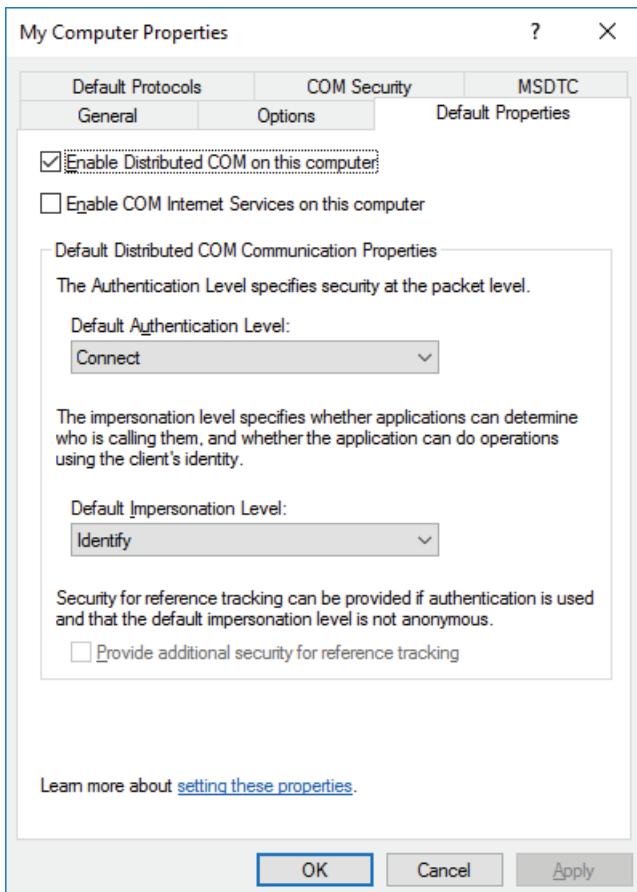


Figure B4.2.3-3 My Computer Properties Dialog Box

6. Open the Default Properties tab, from the [Default Authentication Level] drop-down list, select [Connect], and then click [OK].
7. Restart the computer.

B4.2.4 Configuring on Windows Server 2012 R2

Follow these steps when you use a Windows 2012 R2 computer.

TIP

Windows Server 2012 R2 is supported only for use on computer switchover type UGS.

■ 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. Sign in as an administrative user.
2. Open Control Panel.
3. Click [System and Security].
4. Click [System].
5. In the left pane, click [Advanced system settings].
The System Properties dialog box appears.
6. Select the [Advanced] tab, and click [Settings] in the [Performance] section.
The Performance Options dialog box appears.
7. Select the [Visual Effects] tab and select [Adjust for best performance].
8. Click [OK].

■ Virtual Memory

A custom size is recommended for setting the virtual memory. Follow these steps:

1. Sign in as an administrative user.
2. Open Control Panel.
3. Click [System and Security].
4. Click [System].
5. In the left pane, click [Advanced system settings].
The System Properties dialog box appears.
6. Select the [Advanced] tab, and click [Settings] in the [Performance] section.
The Performance Options dialog box appears.
7. On the [Advanced] tab, select [Programs] under [Adjust for best performance of] and then, in the [Virtual Memory] area, click [Change].
The Virtual Memory dialog box appears.
8. Clear the [Automatically manage paging file size for all drives] check box.
9. Select [Custom size] and set the Initial size and the Maximum size to a value 1.5 times the main memory capacity.
For example, set the custom size to 9216 MB if the main memory capacity is 6 GB, or 12288 MB if 8 GB.
10. Click [Set] and then click [OK].

TIP

After setting the virtual memory, a message box for restarting the computer to validate the virtual memory may be displayed. If displayed, follow the instruction of the dialog to restart the computer.

■ 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. Sign in as an administrative user.
2. Open Control Panel.
3. Click [Hardware].
4. Click [Power Options].
The Power Options window appears.
5. 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 plans], click [Show additional plans]. Select [High performance] and then click [Change plan settings] to the right of it.

6. Click [Change advanced power settings].
The Power Options dialog box appears.

TIP

Some of the advanced setting items explained hereafter may not be displayed, depending on the computer configuration. If not displayed, the functions of such items are not available.

7. Under [Hard disk], set the setting for [Turn off hard disk after] to [Never].
8. Configure the [Sleep] settings as follows:
 - [Sleep after]: Never
 - [Allow hybrid sleep]: Off
 - [Hibernate after]: Never
 - [Allow wake timers]: Disable
9. Set the setting for [Power button action] under [Power buttons and lid] to [Shut down].
10. Under [Display], set the setting for [Turn off display after] to [Never].
11. Click [OK].

■ Defragment and Optimize Drives

The Defragmenter Tool can be used to reorganize the fragmented files on computer hard disk so as to improve the computer performance. Since the performance of this product may be affected when defragmenter is running, it is recommended to disable the schedule of 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. Sign in as an administrative user.
2. Open Control Panel.
3. Select [System and Security] > [Administrative Tools] > [Defragment and Optimize Drives].

The Optimize Drives window appears.

4. Click [Change Settings].

The Optimize Drives dialog box appears.

5. Clear the [Run on a schedule (recommended)] check box and click [OK].

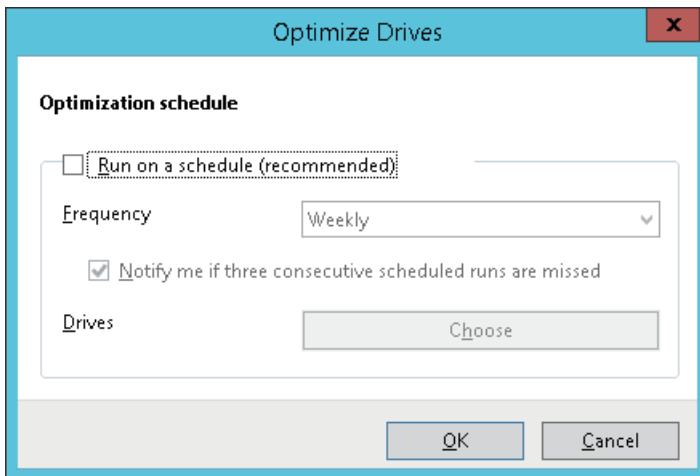


Figure B4.2.4-1 Optimize Drives dialog box

■ Disabling the Automatic Cleanup Task

A function to automatically clean up obsolete files upon application of update programs has been added.

Considering the degradation in system performance that may be caused by execution of automatic cleanup, we recommend to disable the automatic cleanup task.

Follow these steps to disable the automatic cleanup task:

1. Sign in as an administrative user.
2. Open Control Panel.
3. Select [System and Security] > [Administrative Tools] > [Task Scheduler].
The Task Scheduler window appears.
4. In the left pane, select [Task Scheduler (Local)] > [Task Scheduler Library] > [Microsoft] > [Windows] > [Servicing].
5. In the middle pane, right-click [StartComponentCleanup] and select [Disable].

■ Password Setting

Security features were enhanced in Windows Server 2012 R2. As a result, you may find the user password setting more complex or may not be able to set the password as intended.

In this case, do the following:

1. Sign in as an administrative user.
2. Open Control Panel.
3. Select [System and Security] > [Administrative Tools] > [Local Security Policy].
The Local Security Policy window appears.
4. In the left pane, select [Security Settings] > [Account Policies] > [Password Policy].
A list of policies is displayed.
5. In the right pane, double-click [Password must meet complexity requirements].

The properties dialog box for the policy Password must meet complexity requirements appears.

6. Select [Disabled] and click [OK].
7. Confirm that Disabled is indicated for the policy [Password must meet complexity requirements].

■ Installing the Windows Update Programs

Install Windows update programs according to the purpose or configuration of the computer.

● Domain Controller and File Server

Download and apply the Windows update programs.

SEE ALSO

For more information about downloading Windows update programs, refer to:

- “● Downloading the Windows Update Programs (Windows Server 2012 R2)” on page B1-4

● Computer with Dual-redundant Platform for Computer Installed

After you install the Dual-redundant Platform for Computer, download and apply the following Windows update program:

- Security Update for Windows Server 2012 in November 2014

Follow these steps to apply the Windows update program:

1. Sign in as an administrative user.
2. Insert the installation medium of Dual-redundant Platform for Computer into the drive.
3. In Explorer, open <DVD drive>:\GuestOS\Win2012EvrR2\Updates.
4. Double-click [Windows8.1-KB2919442-x64.msu].
The Windows Update Standalone Installer dialog box appears.
5. Click [Yes].
The installation starts.
6. When the installation is complete, click [Close].
7. Double-click [Windows8.1-KB2919355-x64.msu].
The Windows Update Standalone Installer dialog box appears.
8. Click [Yes].
The installation starts.
9. When the installation is complete, click [Restart now] to restart the computer.
10. Double-click [Windows8.1-KB2995730-x64.msu].
The Windows Update Standalone Installer dialog box appears.
11. Click [Yes].
The installation starts.
12. When the installation is complete, click [Restart now] to restart the computer.
13. Apply the Security Update for Windows Server 2012 in November 2014.

TIP

This information is current as of March 2019. The latest information is provided as Endpoint Security Service. For information about the Endpoint Security Service, contact YOKOGAWA.

- **Stopping the installation of .NET Framework 4.6.2**

If you install the software for this product before installing the Windows update program, the installation of the software for this product stops during the installation of .NET Framework 4.6.2. In that case, stop the .NET Framework 4.6.2 installation and install the Windows update programs.

Follow these steps to stop the installation of .NET Framework 4.6.2:

1. Start Task Manager.
2. On the [Details] tab, right-click [NDP462-KB3151800-x86-x64-AIOS-ENU.exe] and select [End Task].
The installation of .NET Framework 4.6.2 stops and the installation of the software for this product also stops.

■ DCOM Settings

When Default Authentication Level in DCOM settings is set to [None], installation of applications such as redistributable modules fails. When installing this product, set the Default Authentication Level to [Connect]. Follow these steps to set Default Authentication Level to [Connect]:

1. Sign in as an administrative user.
2. Open Control Panel.
3. Select [System and Security] > [Administrative Tools] > [Component Services].
The Component Services window appears.

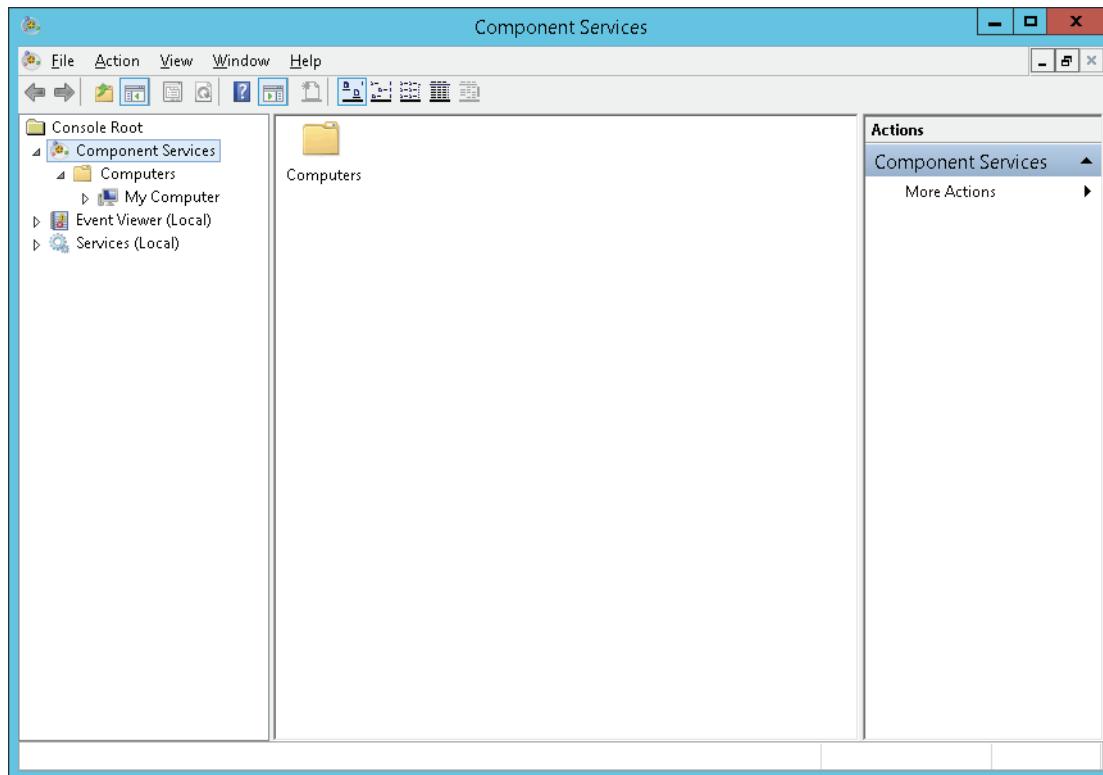


Figure B4.2.4-2 Component Services Window

4. Select [Console Root] > [Component Services] > [Computers].
5. Right-click [My Computer] and select [Properties].
The My Computer Properties dialog box appears.

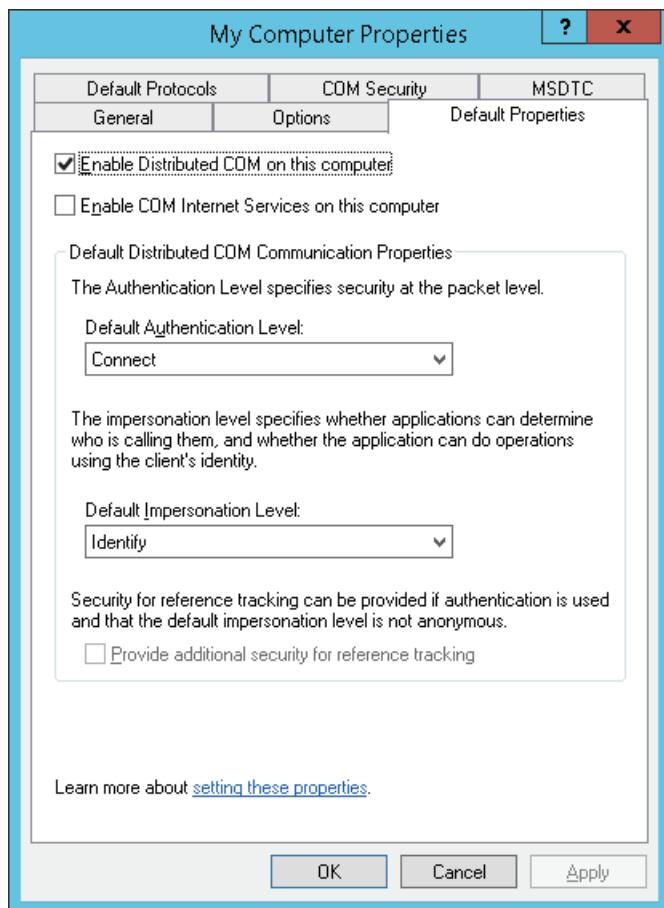


Figure B4.2.4-3 My Computer Properties Dialog Box

6. Open the Default Properties tab, from the [Default Authentication Level] drop-down list, select [Connect], and then click [OK].
7. Restart the computer.

B4.2.5 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. Open Control Panel.
3. Select [System and Security] > [System] > [Advanced system settings].
The System Properties dialog box appears.
4. Select the [Advanced] tab, and click [Settings] in the Performance section.
The Performance Options dialog box appears.
5. Select the [Visual Effects] tab and select [Adjust for best performance].

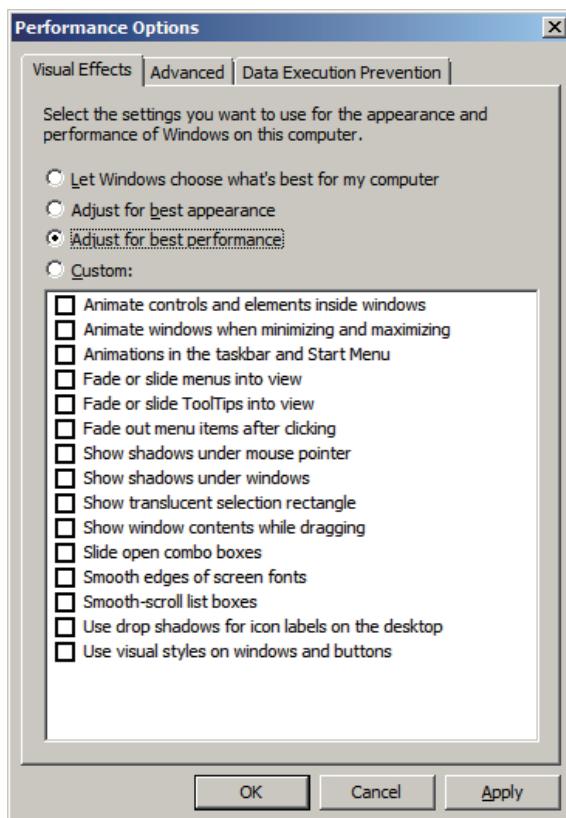


Figure B4.2.5-1 Performance Options Dialog Box (Visual Effects Tab)

6. Click [OK].

■ Virtual Memory

A custom size is recommended for setting the virtual memory. Follow these steps:

1. Log on as an administrative user.

2. Open Control Panel.
3. Select [System and Security] > [System] > [Advanced system settings].
The System Properties dialog box appears.
4. Select the [Advanced] tab, and click [Settings] in the [Performance] section.
The Performance Options dialog box appears.
5. On the [Advanced] tab, select [Programs] under [Adjust for best performance of] and then, in the [Virtual Memory] area, click [Change].
The Virtual Memory dialog box appears.
6. Clear the [Automatically manage paging file size for all drives] check box.
7. Select [Custom size] and set the Initial size and the Maximum size to a value 1.5 times the main memory capacity.
For example, set the custom size to 9216 MB if the main memory capacity is 6 GB, or 12288 MB if 8 GB.

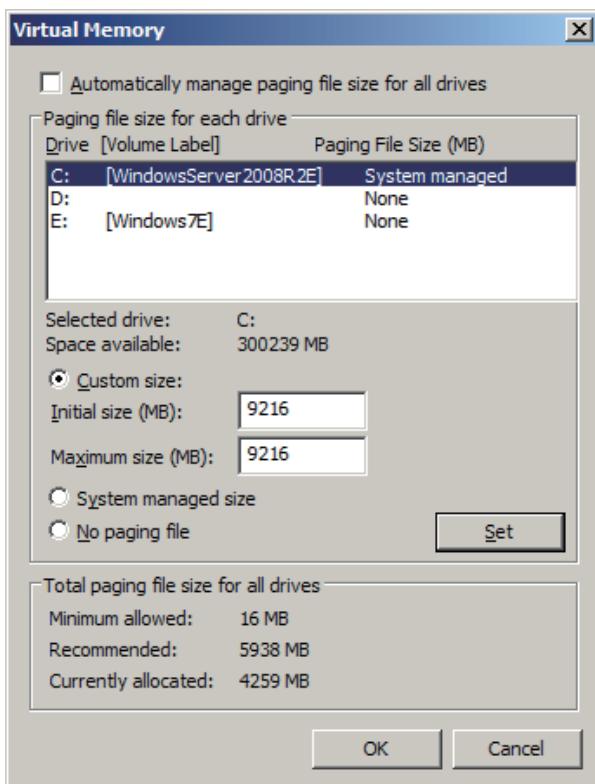


Figure B4.2.5-2 Virtual Memory Dialog Box

8. Click [Set] and then click [OK].

TIP

After setting the virtual memory, a message box for restarting the computer to validate the virtual memory may be displayed. If displayed, follow the instruction of the dialog to restart the computer.

■ 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. Open Control Panel.
3. Select [Hardware] > [Power Options].

The Power Options dialog box appears.

4. 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.

5. Click [Change advanced power settings].

The Power Options dialog box appears, showing the advanced settings.

TIP

Some of the advanced setting items explained hereafter may not be displayed, depending on the computer configuration. If not displayed, the functions of such items are not available.

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

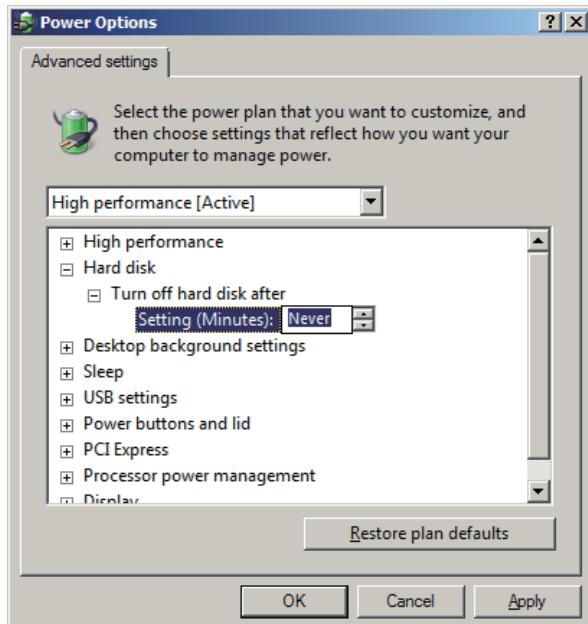


Figure B4.2.5-3 Power Options Advanced Settings

7. Configure the Sleep settings as follows:

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

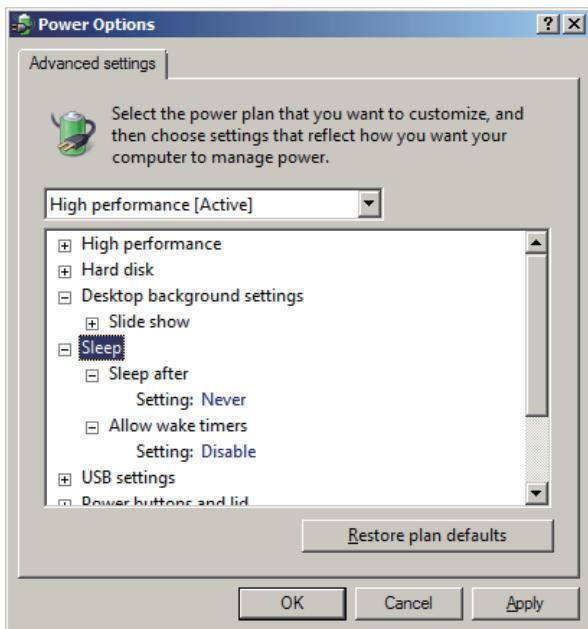


Figure B4.2.5-4 Power Options Advanced Settings

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

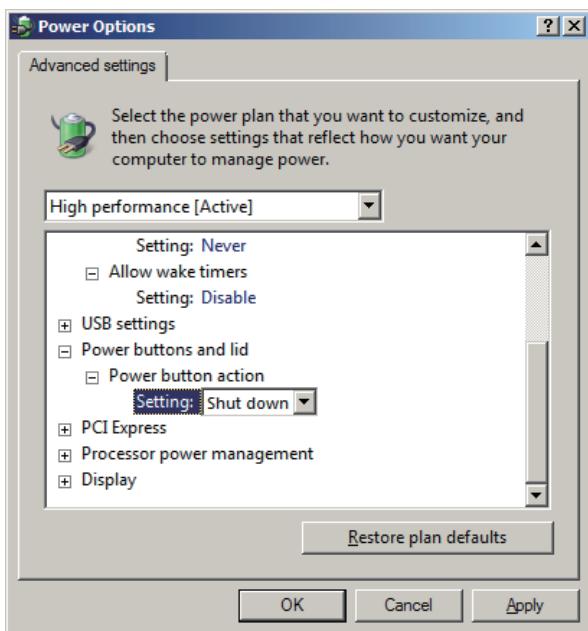


Figure B4.2.5-5 Power Options Advanced Settings

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

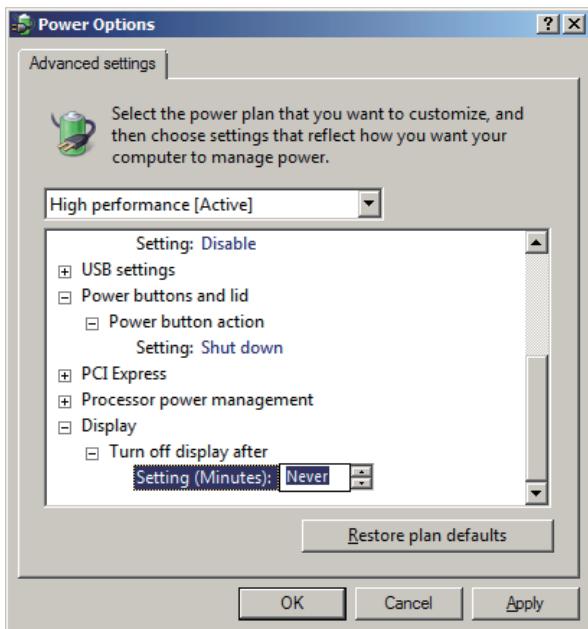


Figure B4.2.5-6 Power Options Advanced Settings

10. Click [OK].

TIP

Configure UPS service settings after installing the software for this product.

SEE ALSO

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

B4.12, “Setting Up the Uninterruptible Power Supply (UPS) Service” on page B4-149

■ Windows Defender

The Windows Defender software detects and removes spy ware.

It is recommended to turn off this function because it is not used with this product.

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 the Local Group Policy Editor.

- **Turning off Windows Defender in Local Group Policy Editor**

Follow these steps to turn off Windows Defender:

1. Log on as an administrative user.
2. Open Command Prompt.
3. Enter `gpedit.msc`.
Local Group Policy Editor appears.
4. In the left pane, select [Computer Configuration] > [Administrative Templates] > [Windows Components] > [Windows Defender].
5. In the right pane, double-click [Turn off Windows Defender].
The Turn off Windows Defender dialog box appears.
6. Select [Enabled] and click [OK].

■ Password Setting

Security features were enhanced in Windows Server 2008 R2. As a result, you may find the user password setting more complex or may not be able to set the password as intended.

In this case, do the following:

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

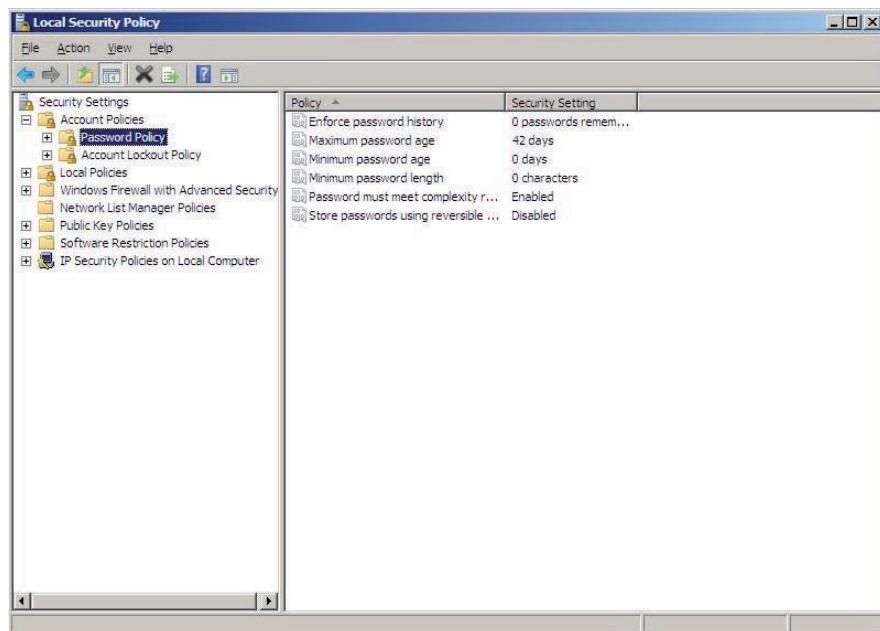


Figure B4.2.5-7 Local Security Policy Window

■ Applying the root certificate

By default, Windows Server 2008 R2 does not come with the root certificate needed to verify the .NET Framework 4.6.2 package certificate. Accordingly, any attempt to install .NET Framework 4.6.2 will fail in the offline environment.

The root certificate needed to install .NET Framework 4.6.2 (Microsoft Root Certificate Authority 2011) must be applied.

Follow these steps to apply the root certificate:

1. Log on as an administrative user who installs the CENTUM VP software.

IMPORTANT

This setting must be made for each user. Because .NET Framework 4.6.2 is installed during installation of the CENTUM VP software, you must log on as an administrative user who installs the CENTUM VP software, not as any other administrative user.

2. Insert the CENTUM VP software medium into the drive.
3. Open Command Prompt.
4. Enter `certmgr.msc`.
The certmgr starts.
5. In the left pane, right-click [Trusted Root Certification Authorities] and select [All Tasks] > [Import].
The Certificate Import Wizard appears.
6. Click [Next].
The File to Import page appears.
7. Click [Browse] and specify the following file.
`<CENTUM VP software medium drive>:\Microsoft\Certificates\MicrosoftRootCertificateAuthority2011.cer`
8. Click [Next].
The Certificate Store page appears.
9. Select [Place all certificates in the following store] and click [Next].
The Completing the Certificate Import Wizard page appears.
10. Click [Finish].
The Security Warning dialog box appears.
11. Click [Yes].
The Certificate Import Wizard dialog box appears, and the certificate import is completed.

■ Installing the Windows Update Programs

Download and apply the Windows update programs.

**SEE
ALSO**

For more information about downloading Windows update programs, refer to:

- “● Downloading the Windows Update Program (Windows 7 or Windows Server 2008 R2)” on page B1-4

B4.3 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.

In the case of virtual machines, the Vnet/IP Interface Package is installed. Also, do not install the Vnet/IP open communication driver.

B4.3.1 Installing the Control Bus Driver

The procedure for installing the control bus driver is basically the same for Windows 10, Windows 7, Windows Server 2016, Windows Server 2012 R2, and Windows Server 2008 R2. This section describes the procedure for installing the control bus driver on Windows 10 as an example.

■ 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.

However, when you use the Test Function, install the control bus driver even if the card is not installed. In this case, set the IP address for the control bus driver on each computer to the same address as the control bus address: that is, "domain number (dd) .station number (ss)". If the Expanded Test Function is used, ensure that the control bus addresses do not overlap among the connected computers.
- For Windows 10, be sure to check that fast startup is turned off before installing the control bus driver. If fast startup is not turned off, turn it off and restart 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, a dialog box indicating completion of the installation (restarting required) may be displayed though restarting the computer is basically not required. In such a case, restart the computer.
- After you install the driver, you need to configure network settings.
- If the control bus interface card or Vnet/IP interface card is not installed when the control bus driver is installed, the "no-card" type control bus driver will be installed. This driver is used to operate the FCS simulator without installing the card.
- To use in actual operation the computer in which the no-card control bus driver has been installed, uninstall the control bus driver, and then install the control bus interface card or Vnet/IP interface card, and install the control bus driver again.
- The Vnet/IP interface card is not required for computer switchover type UGS. However, you need to prepare a dedicated computer. Even in this case, you must install the control bus driver.

SEE ALSO

For more information about the procedure for turning off fast startup in Windows 10, refer to:

“■ Turning Off Fast Startup” on page B4-9

■ Installation Procedure

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.

1. Log on as an administrative user.
 2. Insert the CENTUM VP 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 CENTUM VP 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].

TIP

- If the Windows Security dialog box appears, select the [Always trust software from "Yokogawa Electric Corporation"] check box, and click [Install].
- Do not click [Don't Install] on the Windows Security dialog boxes. If clicked, an error occurs.

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

B4.3.2 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.

The procedure for installing the Vnet/IP open communication driver is basically the same for Windows 10, Windows 7, Windows Server 2016, Windows Server 2012 R2, and Windows Server 2008 R2. This section describes the procedure for installing the Vnet/IP open communication driver on Windows 10 as an example.

Do not install the Vnet/IP open communication driver on computer switchover type UGS.

IMPORTANT

When the Vnet/IP interface card is installed, Vnet/IP open communication driver should be installed even though the 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.
- For Windows 10, be sure to check that fast startup is turned off before installing the Vnet/IP open communication driver. If fast startup is not turned off, turn it off and restart the computer.
- 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.
- After you install the driver, you need to configure network settings.

SEE ALSO

For more information about the procedure for turning off fast startup in Windows 10, refer to:

“■ Turning Off Fast Startup” on page B4-9

■ Installation Procedure

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.

1. Log on as an administrative user.
2. Insert the CENTUM VP 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 CENTUM VP 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].

TIP

- If the Windows Security dialog box appears, select the [Always trust software from "Yokogawa Electric Corporation"] check box, and click [Install].
- Do not click [Don't Install] on the Windows Security dialog boxes. If clicked, an error occurs.

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

B4.3.3 Installing the Vnet/IP Interface Package on a Virtual Machine

When using the virtualization platform, you need to install the Vnet/IP Interface Package on virtual machines.

Follow these steps to install the Vnet/IP Interface Package.

IMPORTANT

- You do not need to install a Vnet/IP interface card in the virtualization host computer.
- After installing the Vnet/IP Interface Package, configure network settings on the virtual machine.

SEE ALSO

For more information about virtualization, refer to:

- Virtualization Platform Setup (IM 30A05B20-01EN)
 - Virtualization Platform: Planning and Implementation Guide (TI 30A05B10-01EN)
-

■ Precautions When Installing the Vnet/IP Interface Package

Observe the following precautions when you install the Vnet/IP Interface Package.

- **Precautions at First-time Installation**

Install the Vnet/IP Interface Package before applying IT security. If you install the Vnet/IP Interface Package for the first time on a computer after applying IT security, you must apply IT security again.

TIP

After IT security is applied, you do not need to apply IT security again when you reinstall the Vnet/IP Interface Package.

- **Precautions at Reinstallation**

Reinstalling the Vnet/IP Interface Package resets the password of the Vnet/IP Interface Package execution user. If you have changed the password, set it again.

■ Preparation

Download and apply the following Windows update program. If it is not applied, installation of Windows update is failed.

- Servicing stack updates in February 2019

In addition, download and apply the following Windows update program. If it is not applied, error log overflow occurs in system log collection in RIP Listener.

- Cumulative update in March 2019

TIP

This information is current as of March 2019. The latest information is provided as Endpoint Security Service. For information about the Endpoint Security Service, contact YOKOGAWA.

■ Procedure 1: Enable the RIP Listener Service

In Windows Server 2016, the RIP Listener service is disabled by default, so you must enable the RIP Listener service. Follow these steps to enable the RIP Listener Service:

1. Sign in to the guest OS on the virtual machine as an administrative user.
2. Right-click on the [Command Prompt], select [Run as Administrator].
3. Run the following command:
`dism /online /enable-feature /featurename:rasrip /all`
4. Confirm that the message “The operation completed successfully.” appears.
5. Check that the RIP Listener service has been enabled.
 - a. Open Control Panel.
 - b. Select [System and Security] > [Administrative Tools] > [Service].
The Services window appears.
 - c. Confirm that RIP Listener is shown and its Startup Type is [Automatic].

TIP

If the Default Authentication Level of DCOM is set to “None,” you cannot enable the RIP Listener service.

SEE ALSO

For more information about how to change the default authentication level of DCOM to “Connect”, refer to:
C10.1.2, “Error Occurs when Server Manager is Started” on page C10-4

■ Procedure 2: Install the Vnet/IP Interface Package

Follow these steps to install the Vnet/IP Interface Package.

TIP

If you have added or deleted any other devices before you install the Vnet/IP Interface Package, a message prompting you to restart the computer may be displayed. If displayed, be sure to restart the virtual machine.

1. Sign in to the host OS on the virtualization host computer as an administrative user.
2. Copy an ISO format file of the CENTUM VP software medium and paste it into a folder in the host OS on the virtualization host computer.
3. From the Start menu, select [Server Manager].
Server Manager starts.
4. From the menu bar of Server Manager, select [Tools] > [Hyper-V Manager].
Hyper-V Manager starts.
5. In the left pane of Hyper-V Manager, select the virtualization host computer. The virtual machines on the selected virtualization host computer are displayed on the middle pane. Select the virtual machine and select [Connect] in the right click menu.
The virtual machine connection window appears.

TIP

The virtual machine connection window may appear full-screen. If it appears full-screen, click [Undo] to exit full-screen.

6. From the menu bar of the virtual machine connection window, select [Media] > [DVD Drive] > [Insert Disk].
A file opening dialog box appears.
7. Specify the copied ISO format file of the CENTUM VP software medium.
The selected ISO format file is mounted on the virtual machine.

- 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 folder where the ISO file of the CENTUM VP software is stored.

The installation menu appears.

8. In the installation menu, click [Control Bus Driver].
A dialog box appears, prompting you to confirm the setup.
9. Select [INSTALL] and click [OK].
A dialog box appears, confirming to execute the installation.
10. Click [OK].

TIP

- If the Windows Security dialog box appears, select the [Always trust software from "Yokogawa Electric Corporation"] check box, and click [Install].
- Do not click [Don't Install] on the Windows Security dialog box. If clicked, an error occurs.

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

■ Procedure 3: Set the Domain Number and Station Number Managed by the Vnet/IP Interface Package

When the installation of the Vnet/IP Interface Package is complete, the Vnet/IP Interface Management Tool appears. Using this tool, set the domain number and station number that will be managed by the Vnet/IP Interface Package. Follow these steps to set the domain number and station number:

TIP

You can also set the domain number and station number managed by the Vnet/IP Interface Package later. However, you must restart the virtual machine to have the new settings to take effect.

1. Open the [Settings] tab of the Vnet/IP Interface Management Tool.
2. Set the domain number in [Domain No] and the station number in [Station No], and then click [Save].

TIP

You can set a number in the range from 1 to 31 as the domain number, and from 1 to 64 as the station number.

On a virtual machine where you run an FCS simulator that can be operated through remote connection from another HIS by installing the Expanded Test Functions and FCS Simulator Package, set both the domain number and the station number to 0.

Note that the license of Vnet/IP Interface Package is not required when using only the test function with the domain number and the station number set to 0.

3. Click [CLOSE], and restart the virtual machine.

SEE ALSO

For more information about Vnet/IP Interface Management Tool, refer to:

Appendix 2., "Vnet/IP Interface Management Tool" on page App.2-1

■ Procedure 4: Activate License of the Vnet/IP Interface Package

Before you can use the Vnet/IP Interface Package, you must activate the license for the package. After installing the CENTUM VP software, distribute and accept the license of the Vnet/IP Interface Package.

B4.3.4 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, Ethernet, and Ethernet dedicated to UACS, assuming settings are made on Windows 7/Windows Server 2008 R2. Information of other OS versions is provided as necessary as TIP.

TIP

When you set up a computer switchover type UGS, read from the section "■ Procedure 1: Rename Local Area Connections."

■ Cautions on Cable Wiring

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

TIP

In Windows 10 and Windows Server 2016, a network charm bar may appear.

SEE ALSO

For more information about the Set Network Location dialog box and network charm bar, refer to:

C10.2.1, "Precaution on Network Cable Connection" on page C10-14

■ Checking the Card for Control Bus

Check the card for control bus that is installed on 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 described as follows.

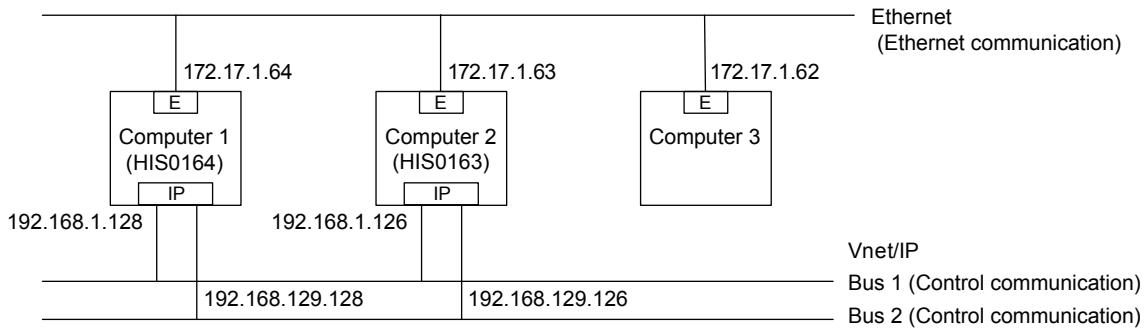


Figure B4.3.4-1 Network Configuration and Interface (Vnet/IP and Ethernet are Installed)

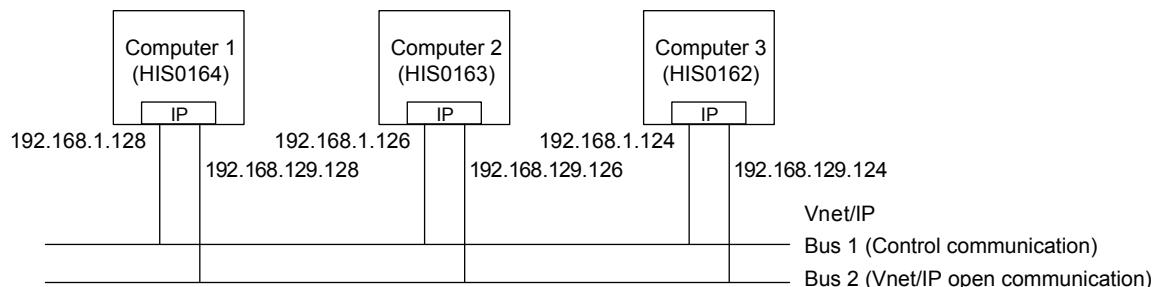


Figure B4.3.4-2 Network Configuration and Interface (Only Vnet/IP is Installed)

Table B4.3.4-1 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.

■ 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.

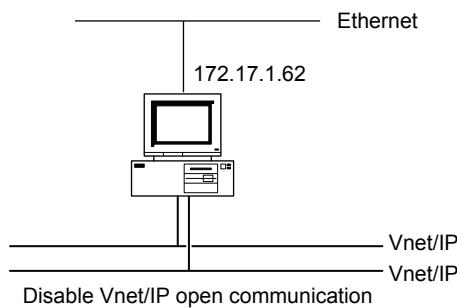


Figure B4.3.4-3 When Vnet/IP and Ethernet are Installed

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

1. Log on using an administrative user account.
2. Open Control Panel.
3. Select [System and Security] > [System] > [Device Manager]. Device Manager appears.
4. Unfold Network adapters.
5. Select [Vnet/IP Open Communication Driver (BUS2)] and then click the Disable button on the toolbar.

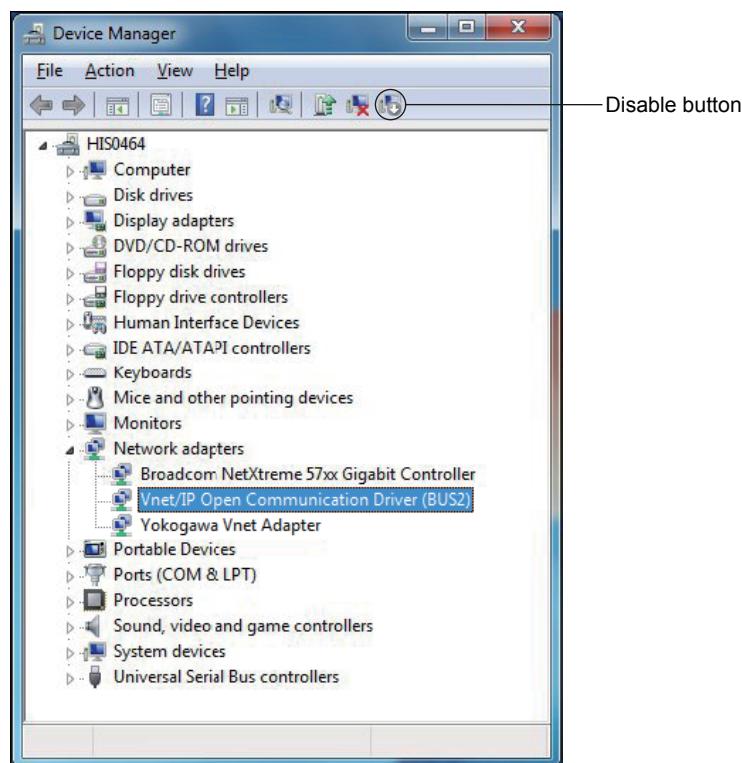


Figure B4.3.4-4 Disabling the Vnet/IP Open Communication Device

- When Only Vnet/IP is Installed

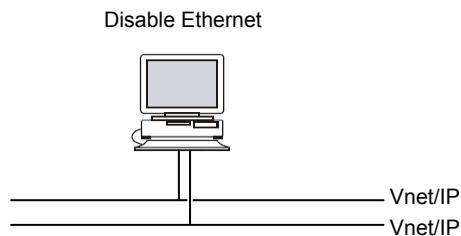


Figure B4.3.4-5 Only Vnet/IP is Installed

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

- Log on using an administrative user account.
- Open Control Panel.
- Select [System and Security] > [System] > [Device Manager]. Device Manager appears.
- Unfold Network adapters.
- Select the Ethernet device and then click the Disable button on the toolbar.

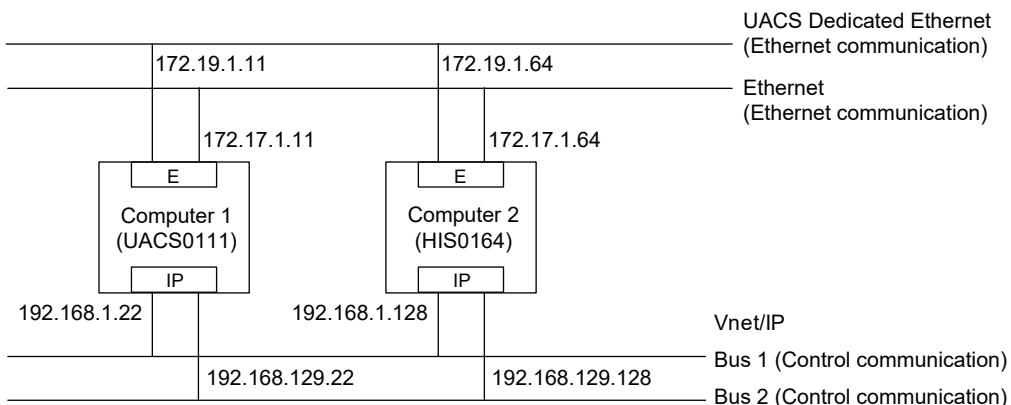
SEE ALSO

For more information about the conditions that allow Ethernet communications using Vnet/IP bus 2, refer to:

"• Ethernet" under "■ Network Specifications" in Integrated Production Control System CENTUM VP System Overview (GS 33J01A10-01EN)

■ Network Configurations and Windows Network Settings when Using UACS Dedicated Ethernet

When using UACS dedicated Ethernet, network configurations and their required Windows network settings are described as follows.



E: Ethernet Interface Card or Onboard NIC

IP: Vnet/IP Interface Card

Figure B4.3.4-6 Network Configuration and Interface

Table B4.3.4-2 Network Configurations and Network Connections to be Set Up on Windows

Computer (example in the figures)	Network connection to be set up on Windows
Connected to Vnet/IP, Ethernet, and UACS dedicated Ethernet (Computers 1 and 2)	Control bus communication, Ethernet communication, Vnet/IP open communication (*1), and UACS dedicated Ethernet

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

■ Prohibitions

Do not use the following features in CENTUM VP:

- 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).

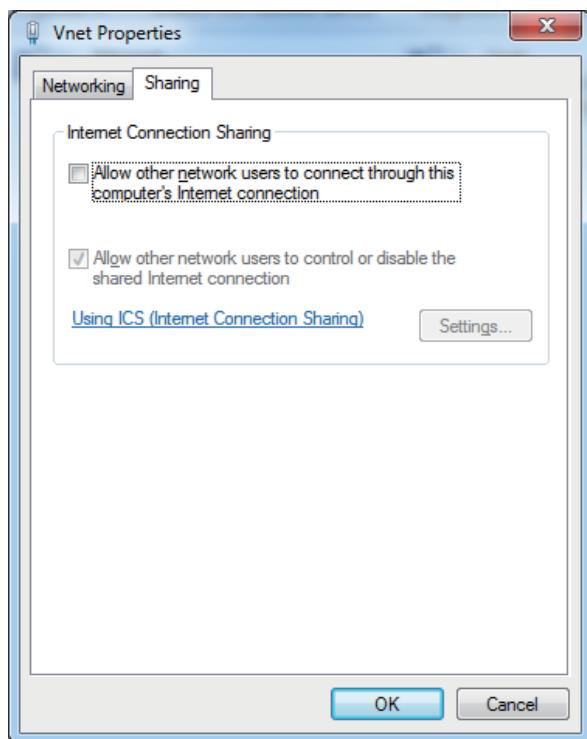


Figure B4.3.4-7 Vnet Properties (Default Setting)

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.)

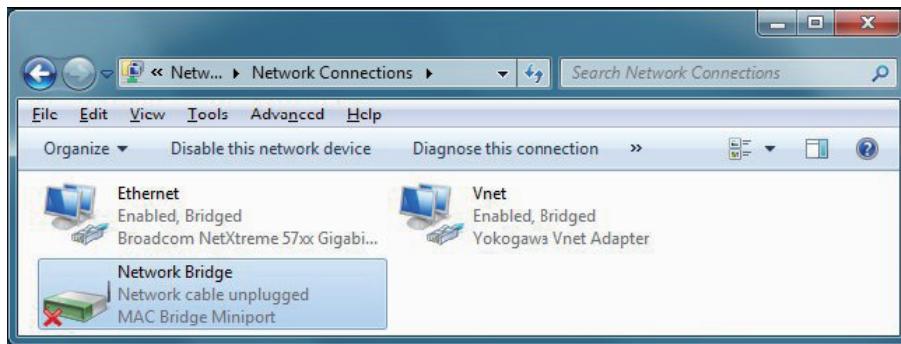


Figure B4.3.4-8 Example of Prohibited Network Setting (Bridge Connection is Enabled)

- **Homegroup (Windows 10 or Windows 7)**

In a CENTUM system, folders and printers are shared by using the file sharing function for the workgroup/network environment as with the earlier VP versions. Accordingly, in Windows 7, do not select Home network in the network location setting, but select Public network. In Windows 10, select No on the network charm bar.

SEE ALSO

For more information about the Set Network Location dialog box and network charm bar, refer to:

C10.2.1, “Precaution on Network Cable Connection” on page C10-14

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

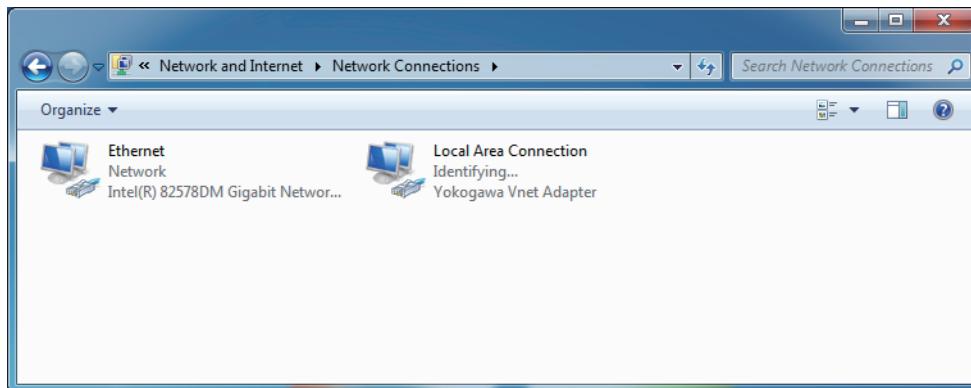


Figure B4.3.4-9 Network Connections (Before Renaming)

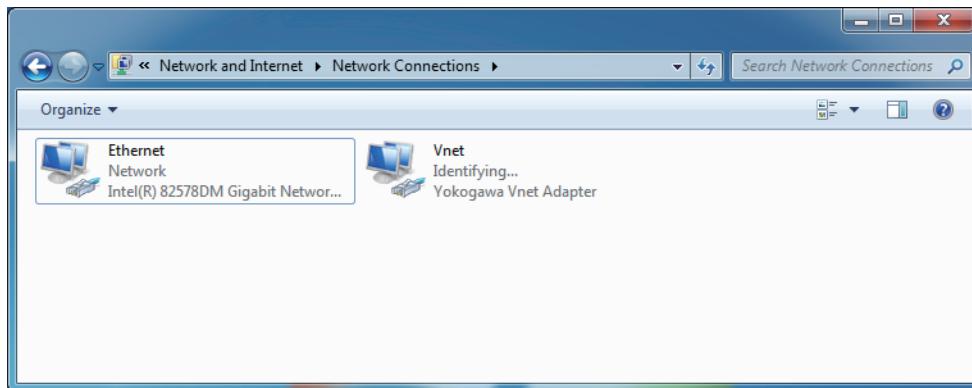
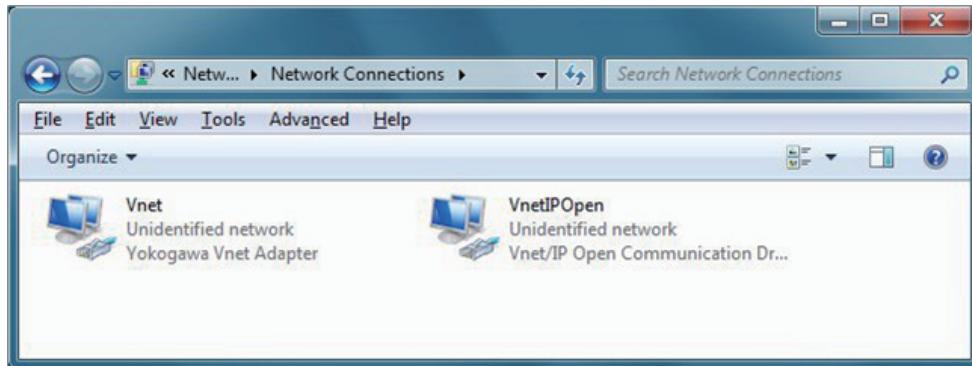
TIP

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.

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

Table B4.3.4-3 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
Ethernet dedicated to UACS	Ethernet driver names	UACSEthernet

**Figure B4.3.4-10 Network Connections – V net Network (After Renaming)****Figure B4.3.4-11 Network Connections – Vnet/IP Network (After Renaming)**

● Confirming the Network Type

Follow these steps to confirm the network type:

1. In the Network Connections window, right-click on a network and select [Properties].
2. Open the Networking tab, and click [Configure].
3. Open the Advanced tab and confirm the Value that is displayed when you select Hyper-V Network Adapter Name in Properties.
The device name that was set when the virtual machine was built is displayed.

TIP

For the Value that you confirm in the step 3, contact to the engineer who configured the virtual machine.

SEE ALSO

For more information about the network settings for a virtual machine, refer to:

B4.3.7, "Notes on Using a Virtual Machine" on page B4-75

■ 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 B4.3.4-4 List of Items Used for Network Connections

Item	Usage of the item (*1)			
	Ethernet	VnetIPOpen	Vnet	UACSE- thernet
Client for Microsoft Networks	Yes	Yes	No	No
QoS Packet Scheduler	Yes	Yes	No	No
File and Printer Sharing for Microsoft Networks	Yes	Yes	No	No
Microsoft Network Adapter Multiplexor Protocol (*2)	No	No	No	No
Microsoft LLDP Protocol Driver (*2)	Yes	Yes	No	No
Yokogawa Vnet Protocol	No	No	Yes	No
Internet protocol version 6 (TCP/IPv6)	No	No	No	No
Internet protocol version 4 (TCP/IPv4)	Yes	Yes	Yes (*3)	Yes
Link-Layer Topology Discovery Mapper I/O Driver	Yes	Yes	No	No
Link-Layer Topology Discovery Responder	Yes	Yes	No	No

*1: Yes: Select the check box
No: Clear the check box

*2: Only on Windows 10 and Windows Server 2016

*3: For computer switchover type UGS, do not select [Internet Protocol Version 4 (TCP/IPv4)].

TIP

Items in the table, except "Yokogawa Vnet Protocol," are installed during the Windows OS installation.

SEE ALSO

For more information about how to set the network adapters of the virtual machine, refer to:

B4.3.7, "Notes on Using a Virtual Machine" on page B4-75

For more information about the network settings specific to computer switchover type UGS, refer to:

"■ Network Settings Specific to Computer Switchover Type UGS" on page B4-73

● V net Properties

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

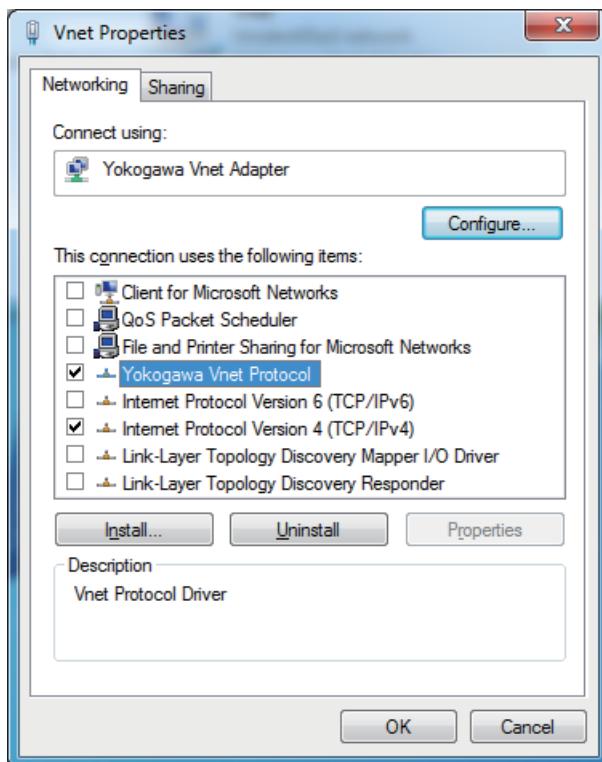


Figure B4.3.4-12 Vnet Properties Dialog Box

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)].

IMPORTANT

For computer switchover type UGS, leave the [Internet Protocol Version 4 (TCP/IPv4)] check box clear, and select only the [Yokogawa Vnet Protocol] check box.

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.

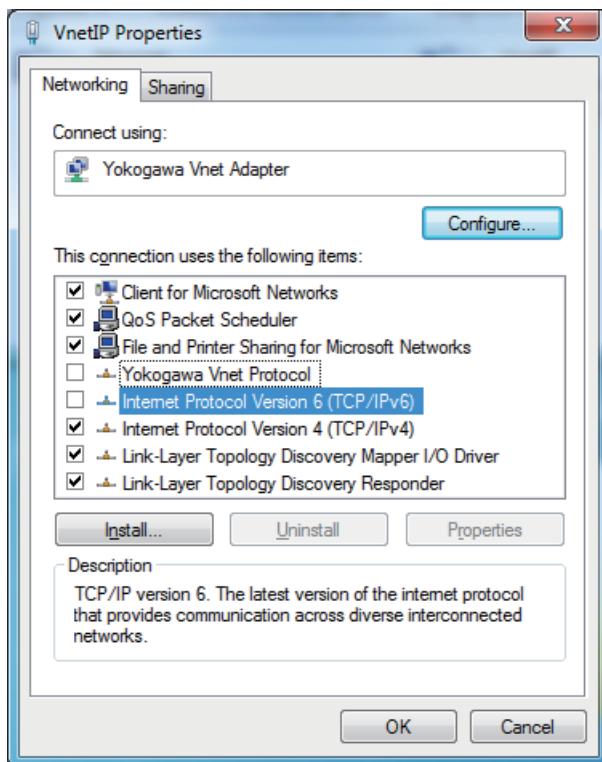


Figure B4.3.4-13 VnetIPOpen Properties Dialog Box

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.

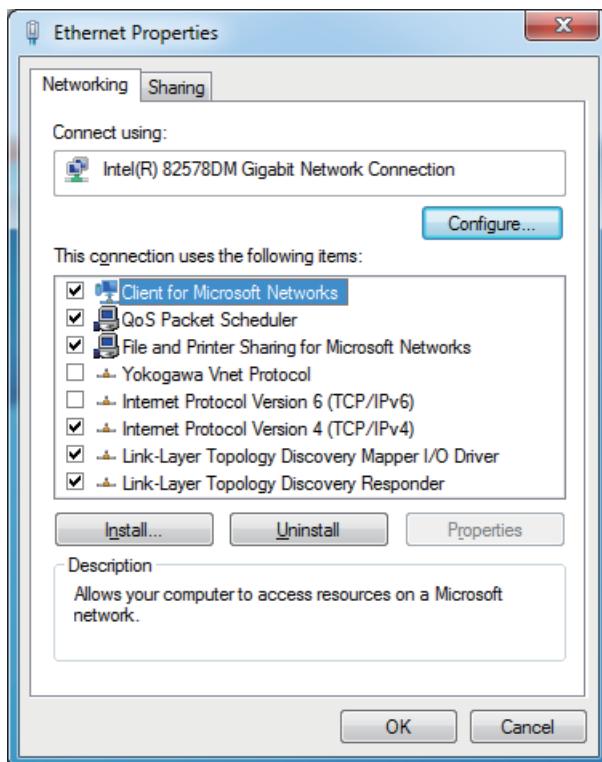


Figure B4.3.4-14 Ethernet Properties Dialog Box

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].

TIP

On a computer switchover type UGS, you must also configure the interface metric settings in the Ethernet properties.

Also when you install the System Integration OPC Station related software on a Windows 10 or Windows Server 2016 computer, you must configure the interface metric settings in the Ethernet properties.

SEE ALSO

For more information about how to configure the interface metric settings, refer to:

“■ Interface Metric Settings” on page B4-74

● **UACSEthernet Properties**

1. In the Network Connections window, right-click [UACSEthernet] and select [Properties]. The UACSEthernet Properties window appears.
2. Based on “Table List of Items Used for Network Connections,” select the check box for [Internet protocol version 4 (TCP/IPv4)], and clear the other check boxes.
3. Follow these steps to configure the interface metric settings:
 - a. Select [Internet Protocol Version 4(TCP/IPv4)] and then click [Properties]. The Internet Protocol Version 4 (TCP/IPv4) Properties dialog box appears.
 - b. Click the General tab.
 - c. Click [Advanced]. The Advanced TCP/IP Settings dialog box appears.
 - d. Click the IP Settings tab.

- e. Clear the [Automatic metric] check box and enter 9999 in the [Interface metric] box.
 - f. Click [OK].
4. Click [OK].

■ Procedure 3: Set IP Addresses

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

● Setting IP Address for Vnet

IMPORTANT

This setting is not required for computer switchover type UGS.

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 address of the existing environment, you can use a value other than 172.16 for the network address.

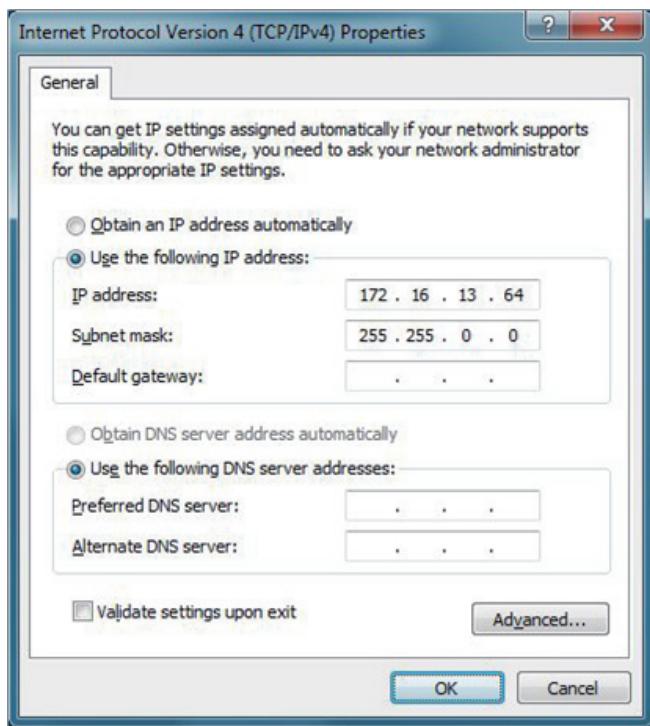


Figure B4.3.4-15 Example of IP Address Setting (Vnet)

- 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.

IMPORTANT

This setting is not required for computer switchover type UGS.

- In the Network Connections window, right-click the VnetIPOpen icon and select [Properties].
The VnetIPOpen Properties dialog box appears.
- Select [Internet Protocol Version 4 (TCP/IPv4)] and click the [Properties].
The Internet Protocol Version 4 (TCP/IPv4) Properties dialog box appears.
- 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.

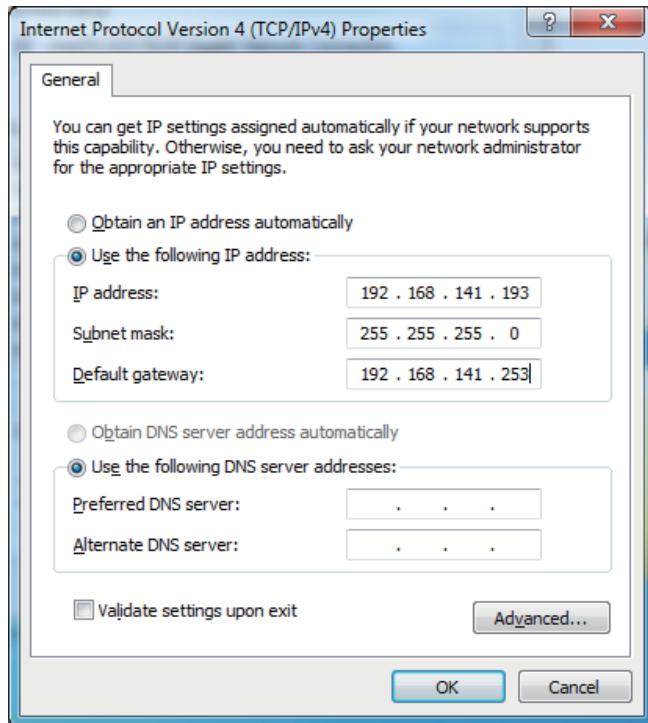


Figure B4.3.4-16 IP Address Setting Example (Vnet/IP Open Communication)

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

SEE ALSO

For more information about the network settings for a virtual machine, refer to:

B4.3.7, "Notes on Using a Virtual Machine" on page B4-75

● Setting IP Address for Ethernet

- In the Network Connections window, right-click the Ethernet icon and select [Properties]. The Ethernet Properties dialog box appears.
- Select [Internet Protocol Version 4(TCP/IPv4)] and then click [Properties]. The Internet Protocol Version 4 (TCP/IPv4) Properties dialog box appears.
- 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.
- For computer switchover type UGS, select [Obtain an IP address automatically]. Set the IP address of the DNS server as necessary.

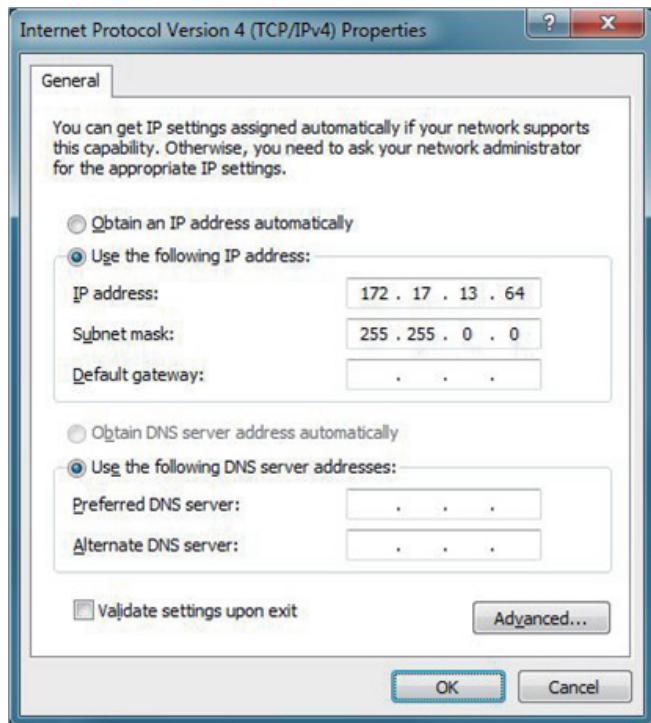


Figure B4.3.4-17 Example of IP Address Setting (Ethernet)

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

IMPORTANT

When using a computer switchover type UGS, there are limitations on the Ethernet network addresses.

SEE ALSO

For more information about the limitations on network addresses when using a computer switchover type UGS, refer to:

Dual-redundant Platform for Computer Read Me First (IM 30A01A20-01EN)

● Cautions on Setting an IP Address Other Than the Default

When setting an IP address other than the default address (172.17.dd.ss) on HIS, you need to do the following tasks after installing the CENTUM VP software but before enabling the CAMS for HIS: on System View, enter the Host Name, IP Address, and Subnet Mask that are currently set on the HIS at [Ethernet TCP/IP Settings] on the Network tab of the Properties dialog box of the HIS, and then download the Project Common Items to all HISs.

● Setting IP Address for UACSEthernet

1. In the Network Connections window, right-click the UACSEthernet icon and select [Properties].
The UACSEthernet Properties dialog box appears.
2. Select [Internet Protocol Version 4(TCP/IPv4)] and then 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 for UACSEthernet as follows:
IP address: 172.19. Domain number. Station number
Subnet mask: 255.255.0.0
Default gateway: No setting is required.
 - You do not need to set the DNS server.
 - If the network address overlaps with the network address of the existing environment, you can use a value other than 172.19 for the network address.
4. After the setting is complete, click [OK]. You do not need to restart the computer.

■ Procedure 4: Configure Bindings

IMPORTANT

This configuration is not required for Windows 10 and Windows Server 2016.

You need to configure network bindings because CENTUM VP 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.
- UACSEthernet has lower priority than Vnet.
- If Vnet/IP open communication, Ethernet, and UACSEthernet are used, the priority shall be in this order: Ethernet, VnetIPOpen, Vnet, and then UACSEthernet, 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, choose [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.

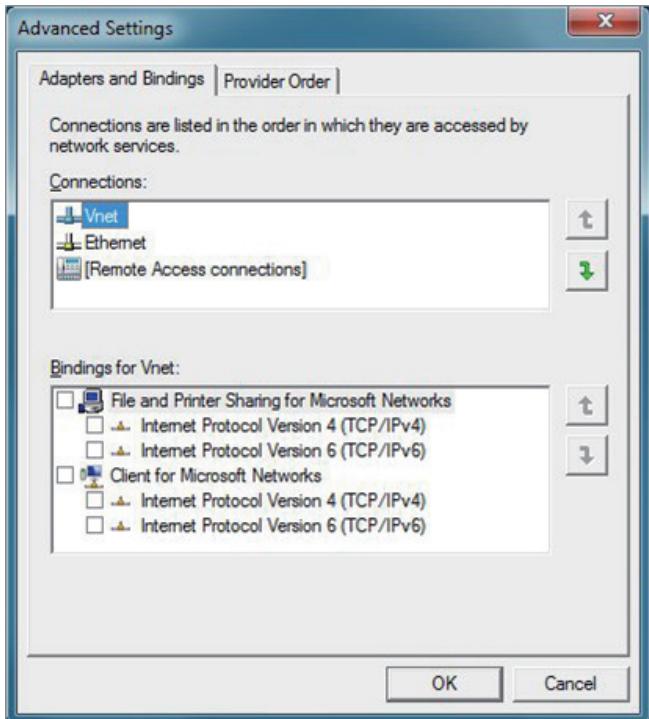


Figure B4.3.4-18 Advanced Settings (Network binding setting is inappropriate)

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.

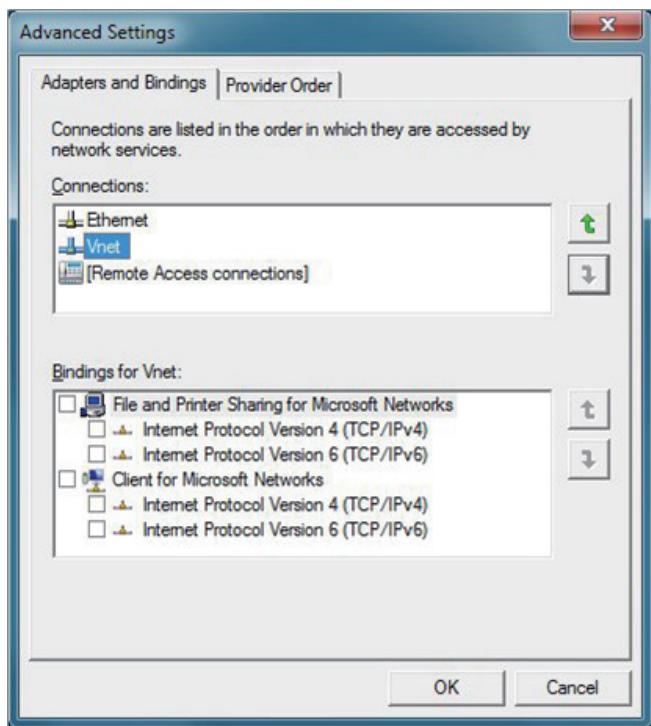


Figure B4.3.4-19 Advanced Settings (Network binding setting is appropriate)

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, VnetIPOpen, and UACSEthernet that are shown in the Bindings box below the Connections box.

SEE ALSO

For more information about the priority order of network bindings for computer switchover type UGS, refer to:

“■ Network Bindings for Computer Switchover Type UGS” on page B4-73

■ Setup Procedure 5: Change Computer Name

It is recommended to set the station names used in the CENTUM VP system as the computer names.

1. Open Control Panel.
2. Select [System and Security] > [System] > [Advanced system settings].
The System Properties dialog box appears.
3. In the Computer Name tab, click [Change].
The Computer Name/Domain Changes dialog box appears.

4. Enter the station name as the new computer name (case-insensitive) for the computer.

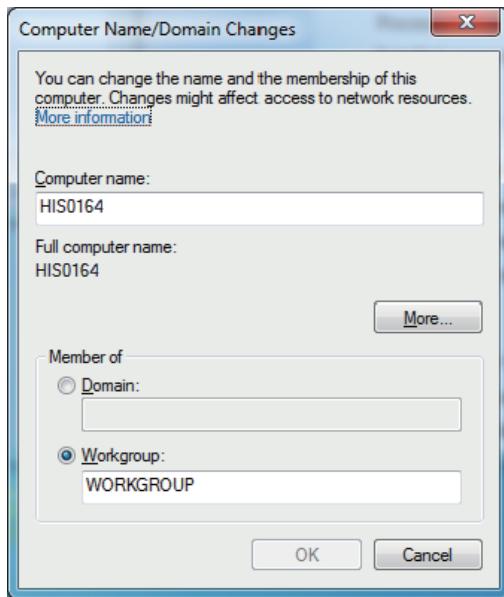


Figure B4.3.4-20 Computer Name/Domain Changes Dialog Box

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

IMPORTANT

For a computer switchover type UGS, the computer name can consists of up to 13 alphanumeric characters. Use of - (hyphen) is allowed. However, the first character must be an alphabetical character.

You must set the same computer name for the two computers of a redundant UGS.

■ Procedure 6: Repair TCP/IP Settings

Before you install the CENTUM VP 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.

IMPORTANT

This setting is not required for computer switchover type UGS.

● Running the TCP/IP Inconsistency Detect Tool

1. Use Windows Explorer to open the TOOLS directory under the following path in the CENTUM VP software medium.
<Drive of CENTUM VP software medium>:\CENTUM\TOOLS

TIP

TCP/IP Inconsistency Repair Tool is installed in the following folder when you install the CENTUM VP software:

<CENTUM VP installation folder>\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.

SEE ALSO

For more information about TCP/IP Inconsistency Repair Tool, refer to:

“● Running TCP/IP Inconsistency Repair Tool” on page B4-70

● **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 CENTUM VP software medium.
<Drive of CENTUM VP software medium>:\CENTUM\TOOLS

TIP

TCP/IP Inconsistency Repair Tool is installed in the following folder when you install the CENTUM VP software:

<CENTUM VP installation folder>\net\tool

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

B4.3.5 Usage Notes for CENTUM VP Entry Class

Note the following points when using CENTUM VP Small.

■ When Using CENTUM VP Entry Class with Non-redundant V net

On CENTUM VP Entry Class, use the following command to start a network setting tool to set the V net to [Single].

<CENTUM VP installation folder>\Tool\CS3000ToolNetwork.exe

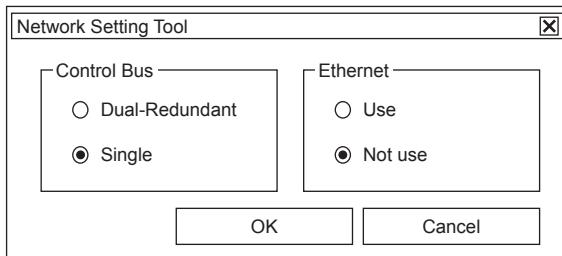


Figure B4.3.5-1 Network Setting Tool

■ When Not Using Ethernet Connections in CENTUM VP Entry Class

This setting is relevant when V net network is used for Ethernet communication.

If you are not using Ethernet connections in CENTUM VP Entry Class, set the [Ethernet] setting to [Do not use] in the Network Settings Tool described in “■ Setting the V net to Single in CENTUM VP Entry Class”.

The setting needs to be changed in the V net network properties.

The following is how to change the setting in the V net network properties.

1. Use an administrative user account to logon.

TIP

Stop all the applications (including System View and operation and monitoring applications).

2. Open Control Panel.
3. Select [Network and Internet] > [Network and Sharing Center].
The Network and Sharing Center window appears.
4. Select [Change adapter settings].
The network connections window appears.
5. On the network connection window, right-click [Vnet] and then choose [Properties].
The Vnet Properties dialog box appears.

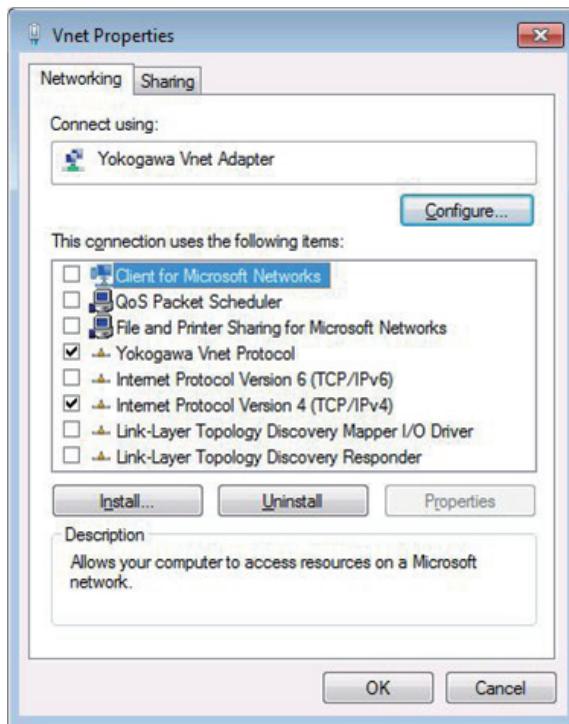


Figure B4.3.5-2 Vnet Properties Dialog Box

6. Select the following four check boxes on the Network tab.
 - Client for Microsoft networks
 - File and printer sharing for Microsoft networks
 - Link-Layer Topology Discovery Mapper I/O Driver
 - Link-Layer Topology Discovery Responder
7. Click [OK] and restart the computer.

B4.3.6 Usage Notes for Computer Switchover Type UGS

Note the following points when using computer switchover type UGS.

■ Network Bindings for Computer Switchover Type UGS

On computer switchover type UGS, set the priority order of network bindings as follows:

IMPORTANT

This configuration is not required for Windows Server 2016.

1. Ethernet and external Ethernet
2. Vnet
3. Redundancy control network

TIP

- You must determine the priority order of Ethernet and external Ethernet networks, considering the priority of subsystem communication or other communications.
- Redundancy control network is used when you use UGS in a redundant configuration.

SEE ALSO

For more information about configuring network bindings, refer to:

- Procedure 4: Configure Bindings" on page B4-66

■ Network Settings Specific to Computer Switchover Type UGS

The computer switchover type UGS uses the following specific networks:

- Redundancy control network
- External Ethernet networks 1 to 4

TIP

- External Ethernet networks 3 and 4 may not be used depending on the configuration of the computer switchover type UGS.
- Redundancy control network is used when you use UGS in a redundant configuration.

On computer switchover type UGS, you must change the setting for these networks so as not to use Yokogawa Vnet Protocol.

Follow these steps to change the network setting:

1. Sign in as an administrative user.
2. Open Control Panel.
3. Click [View network status and tasks].
The Network and Sharing Center window appears.
4. On the left pane, click [Change adapter settings].
The Network Connections window appears.
5. Right-click the icon of the network that is specific to computer switchover type UGS, and click [Properties].
The Properties dialog box appears.
6. Clear the [Yokogawa Vnet Protocol] check box.
7. Click [OK].

TIP

Perform this operation for all networks that are specific to computer switchover type UGS.

■ Interface Metric Settings

On a computer switchover type UGS, you must configure the interface metric settings in the Ethernet properties.

TIP

Also when you install the System Integration OPC Station related software on a Windows 10 or Windows Server 2016 computer, you must configure the interface metric settings in the Ethernet properties.

Follow these steps to configure the interface metric settings:

1. Sign in as an administrative user.
2. Open Control Panel.
3. Click [View network status and tasks].
The Network and Sharing Center window appears.
4. On the left pane, click [Change adapter settings].
The Network Connections window appears.
5. Right-click the Ethernet icon and select [Properties].
The Properties dialog box appears.
6. Select [Internet Protocol Version4 (TCP/IPv4)] and click [Properties].
The Internet Protocol Version 4 (TCP/IPv4) Properties dialog box appears.
7. On the [General] tab, click [Advanced].
The Advanced TCP/IP Settings dialog box appears.
8. On the [IP Settings] tab, clear the [Automatic metric] check box and enter 1 in the [Interface metric] box.

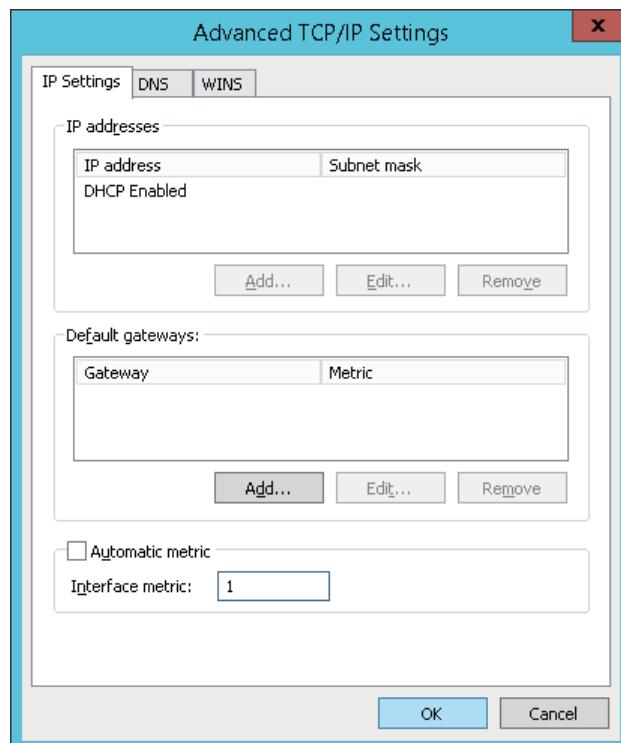


Figure B4.3.6-1 Advanced TCP/IP Settings dialog box

9. Click [OK].

B4.3.7 Notes on Using a Virtual Machine

When using a virtual machine, you need to configure control network and remote UI network settings in addition to Ethernet and V net.

■ Rename Local Area Connections

Set the names of local area connections regarding control network and remote UI network as shown below.

Table B4.3.7-1 Renaming of Network Connections

Network type	Display on Network Connections window (*1)	Name (*2)
Control network 1	Microsoft Hyper-V Network Adapter #n	VnetIPBUS1
Control network 2	Microsoft Hyper-V Network Adapter #n	VnetIPBUS2
Remote UI network	Microsoft Hyper-V Network Adapter #n	RemoteUINetwork

*1: These are the default names, where n = 1, 2, ..., which means the virtual NIC number.

*2: Be sure to set these names. The names are not case-sensitive.

● Confirming the Network Type

Follow these steps to confirm the network type:

1. In the Network Connections window, right-click on a network and select [Properties].
2. Open the Network tab, and click [Configure].
3. Open the Advanced tab and confirm the Value that is displayed when you select Hyper-V Network Adapter Name in Properties.
The device name that was set when the virtual machine was built is displayed.

TIP

For the Value that you confirm in the step 3, contact to the engineer who configured the virtual machine.

■ Configure Properties

In the properties of each type of network connection, you need to configure the items to be used. Configure the properties as shown in the following table.

Table B4.3.7-2 List of Items Used for Network Connections

Item	Usage of the item (*1)		
	Control network 1	Control network 2	Remote UI network
Client for Microsoft Networks	No	No	Yes
QoS Packet Scheduler	No	No	Yes
File and Printer Sharing for Microsoft Networks	No	No	No
Microsoft Network Adapter Multiplexor Protocol	No	No	No
Microsoft LLDP Protocol Driver	No	No	Yes
Yokogawa Vnet Protocol	No	No	No
Internet protocol version 6 (TCP/IPv6)	No	No	No
Internet protocol version 4 (TCP/IPv4)	Yes	Yes	Yes
Link-Layer Topology Discovery Mapper I/O Driver	No	No	Yes
Link-Layer Topology Discovery Responder	No	No	Yes

*1: Yes: Select the check box
No: Clear the check box

■ Set IP Addresses

You do not need to set the IP address, subnet mask, and default gateway for the control network. They will be set automatically by the Vnet/IP interface management tool based on the domain number and station number settings that are managed by the Vnet/IP Interface Package. For the remote UI network, it is recommended to set the IP address, subnet mask, and default gateway to the following values.

IP address: 172.18.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 172.18.

B4.4 Installing the USB Driver for the Operation Keyboard

If you are using an operation keyboard (hereinafter referred to as OPKB) that connects via USB, the USB driver for OPKB is required.

This section describes the procedure for installing the USB driver for OPKB using Windows 10 as an example. If the setup or window displays are different on other operating systems, an additional explanation is provided as necessary.

The USB driver for OPKB is included in the CENTUM VP software medium.

■ Installation Procedure

The USB driver for OPKB installation procedure is as follows.

1. Log on using an administrative user account.
2. Exit all applications that are running.
3. Connect the OPKB to an USB port.

TIP

If your OPKB is AIP827, also connect the power cable of the OPKB.

4. Insert the CENTUM VP 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.

5. Click [USB driver for Operation Keyboard].
A dialog box appears, prompting you to confirm the setup.
6. Select [INSTALL] and click [OK].
A dialog box appears, prompting you to confirm to start the installation.
7. Click the [OK].

TIP

- If the Windows Security dialog box appears, select the [Always trust software from "Yokogawa Electric Corporation"] check box, and click [Install].
- Do not click [Don't Install] on the Windows Security dialog boxes. If clicked, an error occurs.

8. When a dialog box appears, indicating the completion of the installation, click [OK].

TIP

If a dialog box that prompts you to restart the computer appears, be sure to restart the computer.

■ Usage Notes for the Operation Keyboard for Eight-loop Simultaneous Operation (Model: AIP831)

When using the operation keyboard for eight-loop simultaneous operation (Model: AIP831), the license for AIP831 is required.

SEE ALSO

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

B4.8, "Distributing and Accepting Licenses" on page B4-101

■ Using the Sound Speaker of AIP830/AIP831

The sound device name for these products is USB AUDIO DAC. When using the sound speaker of AIP830/AIP831, specify this device as the output destination.

However, the same device name may be displayed for the speaker that is built in the computer. If this is your case, make a sound with the computer and confirm that the sound is output from AIP830/AIP831 before use.

B4.5 Tasks Required for Setting Up the Console Type HIS

For a console type HIS, the following driver installation and settings are required in addition to the settings so far.

- RS-232C driver
- RAS driver
- Operation keyboard setup
- Touch Panel setup
- HIS automatic start and automatic logon settings

TIP

After you install the above drivers, do not reconnect the USB cable to a different port of the computer. If you change the USB port, the device connected to the AUX board with USB interface becomes unable to work.

■ Installing the RS-232C Driver

The RS-232C driver is required to use an eight-loop operation keyboard on a console type HIS.

The RS-232C driver installation procedure is as follows.

IMPORTANT

In order to install the RS-232C driver, an AUX board or an AUX board with USB interface must be connected to the computer.

- AUX board: Connected via the interface expansion card for console type HIS (model: AIP261) installed in the computer.
- AUX board with USB interface (model: AIP262) : Connected via a USB port of the computer.

1. Log on using an administrative user account.
 2. Exit all applications that are running.
 3. Insert the CENTUM VP 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.
4. Click [RS driver for Console HIS].
The PC Interface Selection dialog box appears.
 5. Select the PC interface of the driver to be installed, and click [Install].

TIP

- If an AUX board with USB interface is connected to a USB port of the computer, select "USB (AIP262)." If an AUX board is connected via the interface expansion card for console type HIS (AIP261) installed in the computer, select "PCI (AIP261)."
- In the following steps, there may be minor differences in dialog box appearances, depending on the selected PC interface. However, the procedure is the same.

Confirmation dialog box appears.

6. Select [INSTALL] and click [OK].

A dialog box for confirming the installation appears.

7. Click [OK].

TIP

If the Windows Security dialog box appears, select the [Always trust software from "Yokogawa Electric Corporation"] check box, and click [Install].

8. In the dialog box indicating successful installation that appears, click [OK].

TIP

If a dialog box that prompts you to restart the computer appears, click [OK] and restart the computer.

■ Confirming and Reconfiguring COM Port Numbers of RS-232C Drivers (Windows 10, Windows Server 2016)

If both of the following conditions are met, confirm that the RS-232C drivers are assigned to the COM port numbers properly:

- The operating system of the computer is Windows 10 or Windows Server 2016
- An AUX board with USB interface is used

If the RS-232C drivers are not assigned to the COM port numbers properly, reconfigure the COM port numbers of the RS-232C drivers.

This section describes the following procedures:

- Confirming the COM port numbers of RS-232C drivers
- Reconfiguring the COM port numbers of RS-232C drivers

● Confirming COM Port Numbers of RS-232C Drivers

Follow these steps to confirm the COM port numbers of RS-232C drivers:

1. Sign in as an administrative user.
2. Start the Device Manager.

TIP

If a User Account Control dialog box appears, click [Yes].

3. Expand [Ports (COM & LPT)] and confirm that four [USB Serial Port Device (AIP262)] drivers appear.



Figure B4.5-1 USB Serial Port Device (AIP262) Drivers

4. Confirm that (COM3) to (COM6) appear to the right of the four [USB Serial Port Device (AIP262)] drivers. If any number other than these appears, reconfigure the COM port number of the RS-232C driver.
5. Confirm that the COM port numbers are assigned to each driver properly when (COM3) to (COM6) appear to the right of the four [USB Serial Port Device (AIP262)] drivers. Perform the following steps for each [USB Serial Port Device (AIP262)] driver:
 - a. Double-click [USB Serial Port Device (AIP262)] driver.

The Properties dialog box appears.

- b. From the [Property] drop-down list on the [Details] tab, select [Hardware Ids].

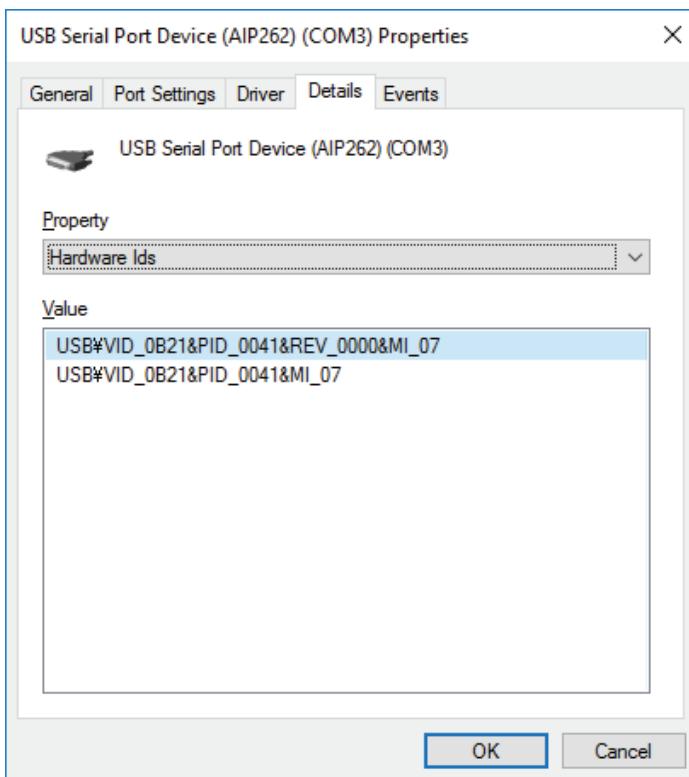


Figure B4.5-2 Hardware IDs

- c. Check the IDs listed in the top of the [Value] list to see if the COM port numbers and hardware IDs correspond as shown in the following table. Reconfigure the COM port number of the RS-232C driver if they do not correspond to the table.

Table B4.5-1 COM Port Numbers and the Corresponding Hardware IDs

COM port number	Hardware IDs
COM3	USB\VID_0B21&PID_0041&REV_0000&MI_01
COM4	USB\VID_0B21&PID_0041&REV_0000&MI_03
COM5	USB\VID_0B21&PID_0041&REV_0000&MI_05
COM6	USB\VID_0B21&PID_0041&REV_0000&MI_07

● Reconfiguring COM Port Numbers of RS-232C Drivers

Perform the following steps to reconfigure the COM port numbers of RS-232C drivers.

1. Sign in as an administrative user.
2. Start the Device Manager.

TIP

If a User Account Control dialog box appears, click [Yes].

3. Repeat the following steps to change the COM port numbers of the drivers with (COM3) to (COM6) displayed to any number other than COM3 to COM6.
 - a. Double-click the driver.
The Properties dialog box appears.
 - b. On the [Port Settings] tab, click [Advanced].

The Advanced Settings dialog box appears.

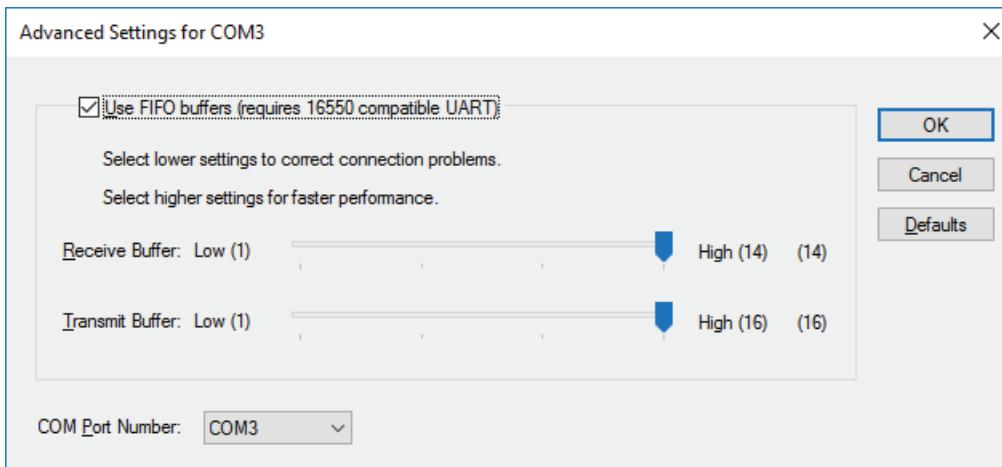


Figure B4.5-3 Advanced Settings Dialog Box

- c. From the [COM Port Number] drop-down list, select an unused COM port number other than COM3 to COM6, and then click [OK].
4. Repeat the following steps to reconfigure the COM port numbers of the four [USB Serial Port Device (AIP262)] drivers.
 - a. Double-click [USB Serial Port Device (AIP262)] driver. The Properties dialog box appears.
 - b. From the [Property] drop-down list on the [Details] tab, select [Hardware Ids].
 - c. Confirm the IDs listed in the top of the [Value] list.
 - d. On the [Port Settings] tab, click [Advanced]. The Advanced Settings dialog box appears.
 - e. From the [COM Port Number] drop-down list, select the COM port number as shown in the following table.

Table B4.5-2 COM Port Numbers to be Configured

Hardware IDs	COM port number
USB\VID_0B21&PID_0041&REV_0000&MI_01	COM3
USB\VID_0B21&PID_0041&REV_0000&MI_03	COM4
USB\VID_0B21&PID_0041&REV_0000&MI_05	COM5
USB\VID_0B21&PID_0041&REV_0000&MI_07	COM6

5. Restart the computer.

■ Installing the RAS Driver

The RAS driver is required to use an AUX board or an AUX board with USB interface for the console type HIS.

The RAS driver installation procedure is as follows.

IMPORTANT

To install the RAS driver, an AUX board or an AUX board with USB interface must be connected to the computer.

- AUX board: Connected via the interface expansion card for console type HIS (model: AIP261) installed in the computer.
- AUX board with USB interface (model: AIP262) : Connected via a USB port of the computer.

1. Log on as an administrative user.
2. Exit all running programs.
3. Insert the CENTUM VP 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.
4. Click the [RAS driver for Console HIS].
A dialog box appears, prompting you to select the Console Type and the PC Interface.
5. Select the console type and the PC interface for the driver to be installed, and click the [Install].

TIP

- If an AUX board with USB interface is connected to a USB port of the computer, select "USB."
If an AUX board is connected via the interface expansion card for console type HIS installed in the computer, select "PCI."
- In the following steps, there may be minor differences in dialog box appearances, depending on the selected PC interface. However, the procedure is the same.

6. Select [INSTALL] and click [OK].
The Installation Confirmation dialog box appears.
7. Click [OK].

TIP

If the Windows Security dialog box appears, select the [Always trust software from "Yokogawa Electric Corporation"] check box, and click [Install].

8. In the dialog box indicating successful installation that appears, click [OK].

TIP

If a dialog box that prompts you to restart the computer appears, click [OK] and restart the computer.

■ Operation Keyboard Setup

Console type HISs are automatically set to use an operation keyboard. The connecting port is COM4.

■ Touch Panel Setup

On solid style console type HISs, the Touch Panel Setup dialog box will appear during the installation of the CENTUM VP software. Select [Use/Do not use] Touch Panel in the dialog

box. If you are using two-level monitors, select [Use/Do not use] Touch Panel for both the upper and lower level monitors.

Touch Panel is not set up on open style console type HISs. Configure the setting separately based on the instruction manual provided with the hardware for Touch Panel.

■ HIS Auto Start and Automatic Logon

If an engineering keyboard is not to be connected on a console type HIS, enable the auto logon feature of the operation and monitoring function (including Windows automatic start). This is because [Ctrl] + [Alt] + [Del] and the password cannot be keyed in to display the Windows logon dialog box using an operation keyboard (OPKB).

SEE

ALSO

For more information about the auto logon feature of the operation and monitoring function (including Windows automatic start), refer to:

“■ Setting to Automatically Start the Operation and Monitoring Function” on page B4-137

B4.6 Installing the CENTUM VP Software

This section describes how to install the CENTUM VP software.

■ Administrative User who Performs the Installation

The CENTUM VP software must be installed by an administrative user shown in the following table.

Installing the CENTUM VP software creates the CTM_MAINTENANCE group and adds the user who installed the software to the CTM_MAINTENANCE group automatically.

Table B4.6-1 Administrative User Who Performs New Installation

Security model and user management type to be applied		
Legacy model	Standard model	
	Standalone management	Domain/Combination management
Local user who belongs to the Administrators local group	Local user who belongs to the Administrators local group	<ul style="list-style-type: none"> • Domain user who belongs to the Domain Admins domain group • Domain user who belongs to the Administrators local group • Local user belonging to the Administrators local group(*1)

*1: : The domain user name and password must be entered during installation.

TIP

If the user management type is Domain or Combination management, install the software after the computer is added to the domain.

SEE ALSO

For more information about registering an administrative user who belong to a domain group, refer to:

“■ Precautions Regarding Setup Tasks for Client Computers” on page B2-21

■ Installation Procedure

The procedure for installing the CENTUM VP software differs for HIS, computer installed with only system builders or computer installed with only AD Server and for APCS/SIOS/GSGW/UGS/UACS station.

- **Installing on the HIS, Computer Installed with Only System Builders or Computer Installed with only AD Server**

1. Log on as an administrative user.
2. Exit all running applications, including resident programs such as anti-virus software.
3. Insert the CENTUM VP 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.

4. Click [CENTUM VP Software] in the installation menu.
A message that prompts restarting the computer is displayed so as to grant the currently logged on user the rights required in the subsequent installation tasks.

TIP

If the Windows redistributable modules required to run CENTUM VP, such as Microsoft .NET Framework, are not already installed, a dialog box appears, prompting you to install such modules.

Click [Install] to install them. If you click [Cancel], the installation of the CENTUM VP software is discontinued.

The following modules are required for CENTUM VP.

- Microsoft .NET Framework 4.6.2
- MSXML 6.0 SP1
- Microsoft Visual C++ 2017 Redistributable Package
- OPCCOM ProxyStub

When installation of these modules is started, the display in the status field changes accordingly. Restarting the computer may be required after installing the modules. If required, restart the computer and then continue the CENTUM VP installation after the computer is restarted.

IMPORTANT

On Windows Server 2012 R2, if the installation of Microsoft .NET Framework 4.6.2 stops midway for more than 5 to 10 minutes, it may be because Windows update programs are not installed. Stop the installation of Microsoft .NET Framework 4.6.2, and install the Windows update programs.

5. Click [OK].
The computer is restarted.
6. Log on using the same user account.
Installation of the CENTUM VP software starts and the Welcome dialog box appears.
7. Click [Next].
A dialog box for entering user information and the installation folder appears.

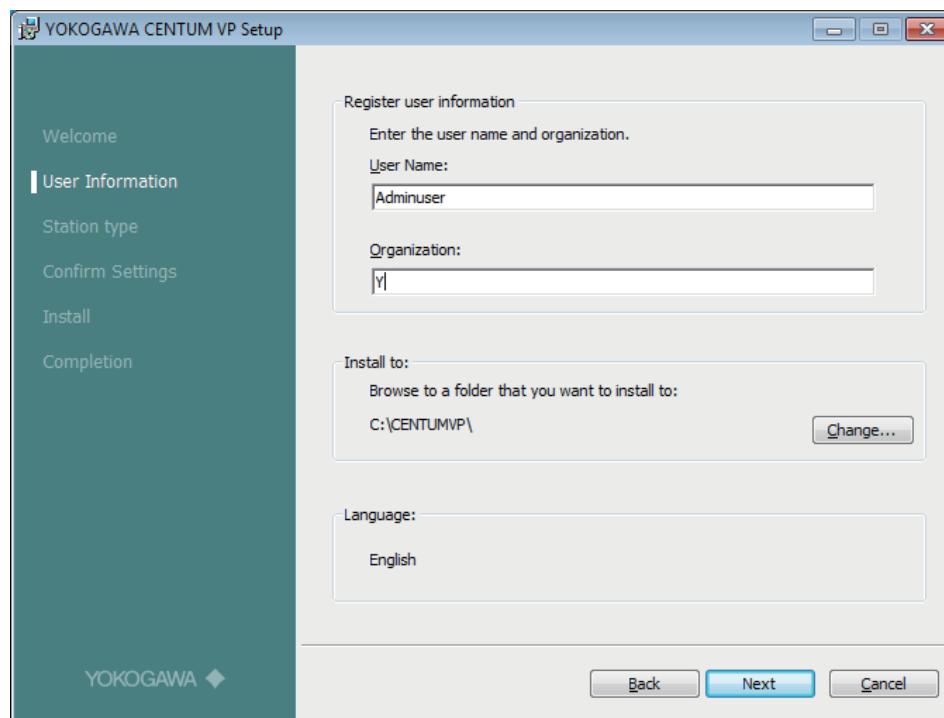


Figure B4.6-1 CENTUM VP Setup Dialog Box (User Information)

TIP

- If the driver of a different version is installed, a dialog box appears, informing you so. Confirm the information, and click [OK]. To update the driver, uninstall the existing driver and install the new one after you install the CENTUM VP software.
- When the Vnet/IP interface card is installed, you need to update the Vnet/IP open communication driver even if the Vnet/IP open communication is not used. If you connect the computer to Ethernet, update the Vnet/IP open communication driver and then disable the driver.

8. Enter the user name and company name. If you want to change the installation folder from the default location, click [Browse] and specify a new location.

TIP

- The user name and company name must be set within 100 characters.
- The default installation folder is <system drive>:\CENTUMVP\. When you change the folder, the folder path name must be set 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].

A dialog box appears, prompting you to select the station type, enter the database reference, and to select the console type of the station.

10. Select the station type.

TIP

The software that will be installed according to the selected station type is as follows:

Table B4.6-2 Installed Software and Selected Station Type

Station type	Installed software
HIS/ENG or PC (*1)	Operation and monitoring functions, System configuration functions, AD server, SOE server related software.
UGS	Unified Gateway Station (UGS) related software
GSGW General Subsystem Gateway	Generic Subsystem Gateway (GSGW) related software
SIOS System Integrated OPC Station	System Integration OPC Station (SIOS) related software
APCS Advanced Process Control Station	Advanced Process Control Station (APCS) related software

*1: Stations to be defined as HISddss or computer on SystemView. If the AD server does not coexist with operation and monitoring function or system builders, the station name is same as the computer name.

11. Enter the database reference location (the name of the computer where the project database is placed) using up to 15 characters. If the computer is installed with only system builders or AD server, this setting is not necessary.

TIP

- The name of the currently installed computer is the default setting. This setting can be changed at a later time. The changing procedure is provided in the section "Changing the Location of Engineering Data for Reference."
- If the project database is on a HIS installed with system builders or a computer installed with system builders, enter the computer name with seven characters.

12. Select the console type of the station.

If the RAS driver has been installed, the console type of the station, the console type selected during installation of the driver is set by default. In other cases, it is set to "PC" by default.

- When selecting PC for the console type

The port number is left blank by default.

When using an operation keyboard, select the number of the COM port to which the operation keyboard is to be connected.

When not using an operation keyboard, select blank for the number of the COM port to which the operation keyboard is to be connected.

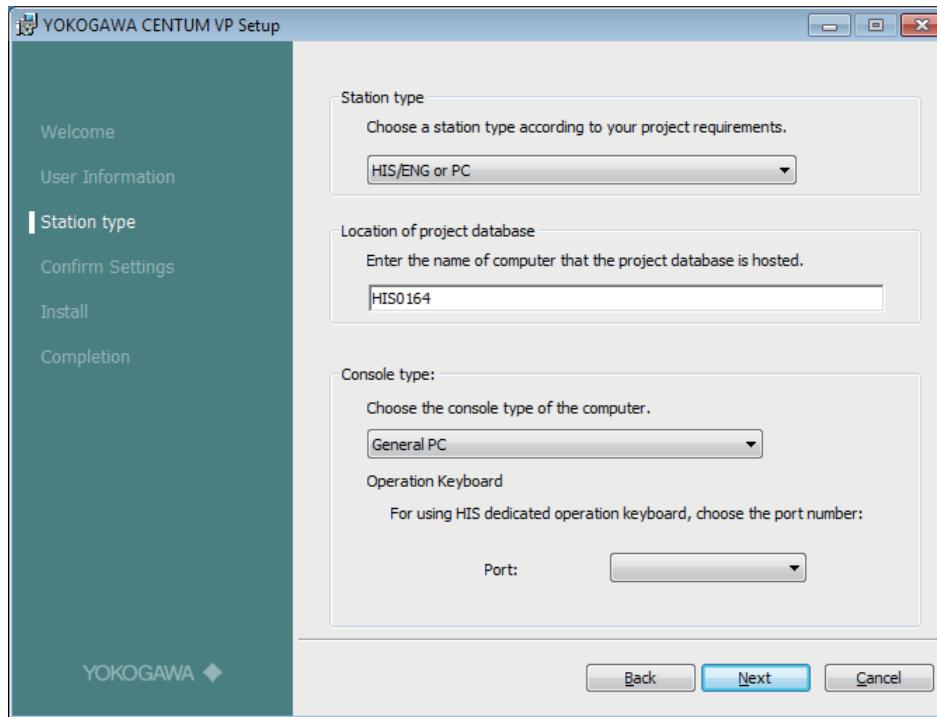


Figure B4.6-2 CENTUM VP Setup Dialog Box (PC Selected for Console Type)

- When selecting solid style console for the console type

The Touch Panel check box is not selected for both the upper and lower level monitors.

When using the Touch Panel on the upper level of two-level monitors, select the check box for [Use Touch Panel (Upper Level)].

When using the Touch panel on the lower level, select the check box for [Use Touch Panel (Lower Level)].

When using the Touch Panel on a single monitor, select the check box for [Use Touch Panel (Lower Level)]. Leave the check box for [Use Touch Panel (Upper Level)] clear.

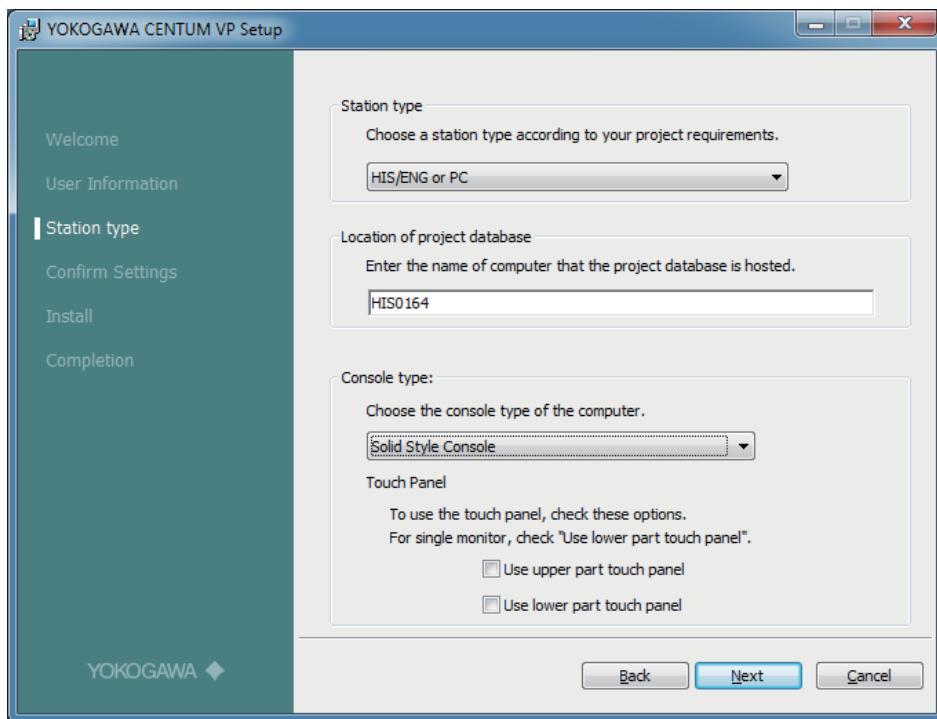


Figure B4.6-3 CENTUM VP Setup Dialog Box (Solid Style Console Selected for Console Type)

Click [Next]. If the Touch Panel is set not to be used, the following confirmation dialog box will appear. To resume the installation, click [Yes]. To return to the setting screen to reconfigure the setting, click [No].



Figure B4.6-4 Dialog Box Confirming Use of Touch Panel

- When selecting open style console for the console type
No particular setting is required.

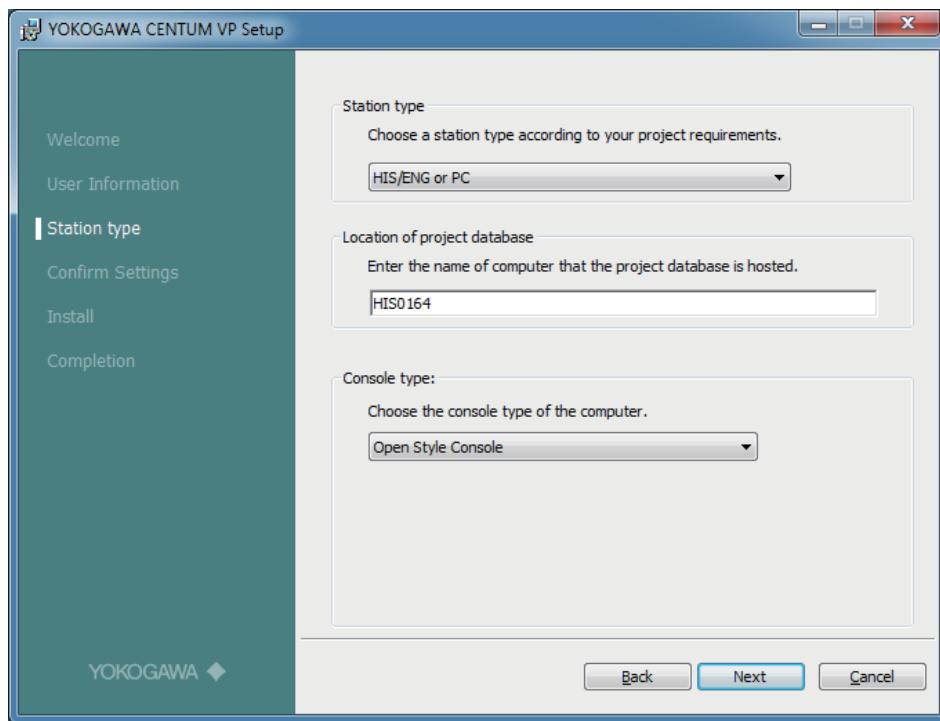


Figure B4.6-5 CENTUM VP Setup Dialog Box (Open Style Console Selected for Console Type)

13. Click [Next].
The installation setting confirmation dialog box appears.

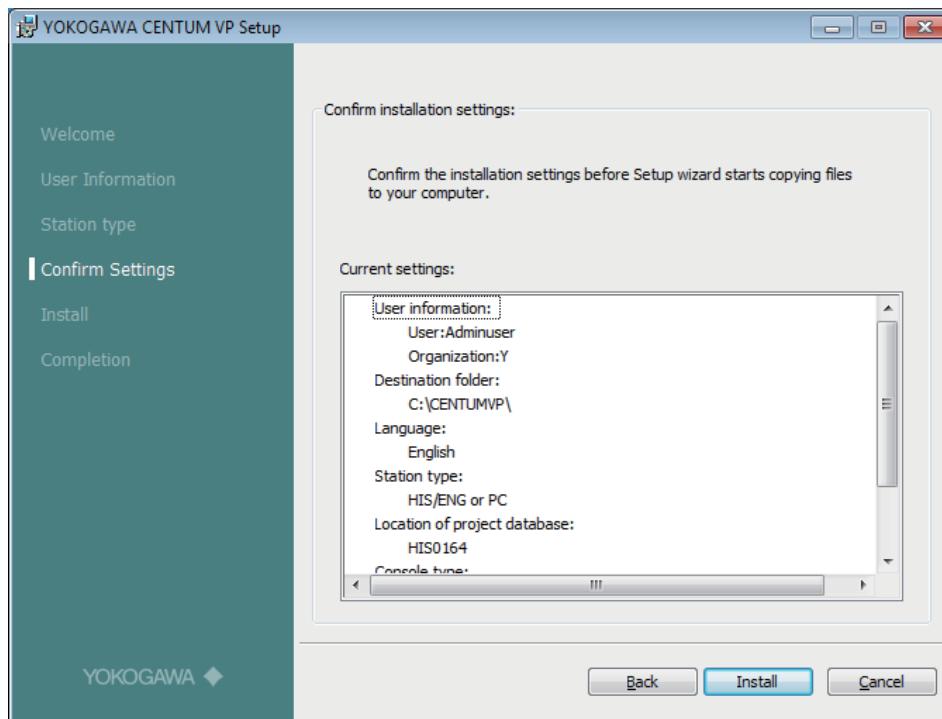


Figure B4.6-6 CENTUM VP Setup Dialog Box (Setting Confirmation)

14. Make sure that the installation settings are correct, and click [Install] to start the installation.
The CENTUM VP software installation starts.

TIP

During installation, the progress is displayed in a dialog box. It may take several minutes for the installation to be completed.

15. When the installation complete dialog box appears, perform either of the following operations.

- If you install only CENTUM VP, 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.

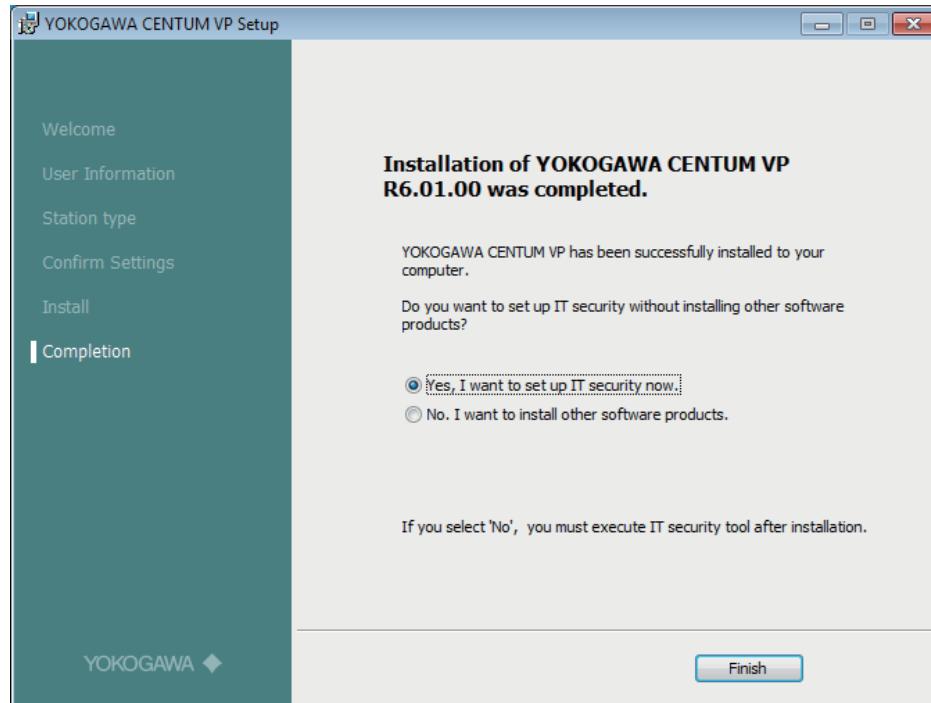


Figure B4.6-7 CENTUM VP Setup Dialog Box (Complete)

IMPORTANT

Even when you install other YOKOGAWA products, you must run the IT Security Tool after the installation of the last product. In this case, the IT Security Tool will be run for all the installed products.

If you do not run the IT Security Tool, the products may not function properly.

SEE ALSO

For more information about the procedure for stopping installation of Microsoft .NET Framework 4.6.2, refer to:

- Stopping the installation of .NET Framework 4.6.2" on page B4-34

For more information about the procedure for installing the Windows update programs on Windows Server 2012 R2, refer to:

- "Installing the Windows Update Programs" on page B4-33

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

- B4.7, "Configuring IT Security Settings" on page B4-94

● Installing on the APCS/SIOS/GSGW/UGS/UACS station

1. Perform steps 1 through 10 in the section "Installing on the HIS or Computer Installed with Only System Builders."
2. Click [Next].
The installation setting confirmation dialog box appears.
3. Make sure that the installation settings are correct, and click [Install] to start the installation.
The CENTUM VP software installation starts.

TIP

During installation, the progress is displayed in a dialog box. It may take several minutes for the installation to be completed.

4. When the installation complete dialog box appears, perform either of the following operations.
 - If you install only CENTUM VP, 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.

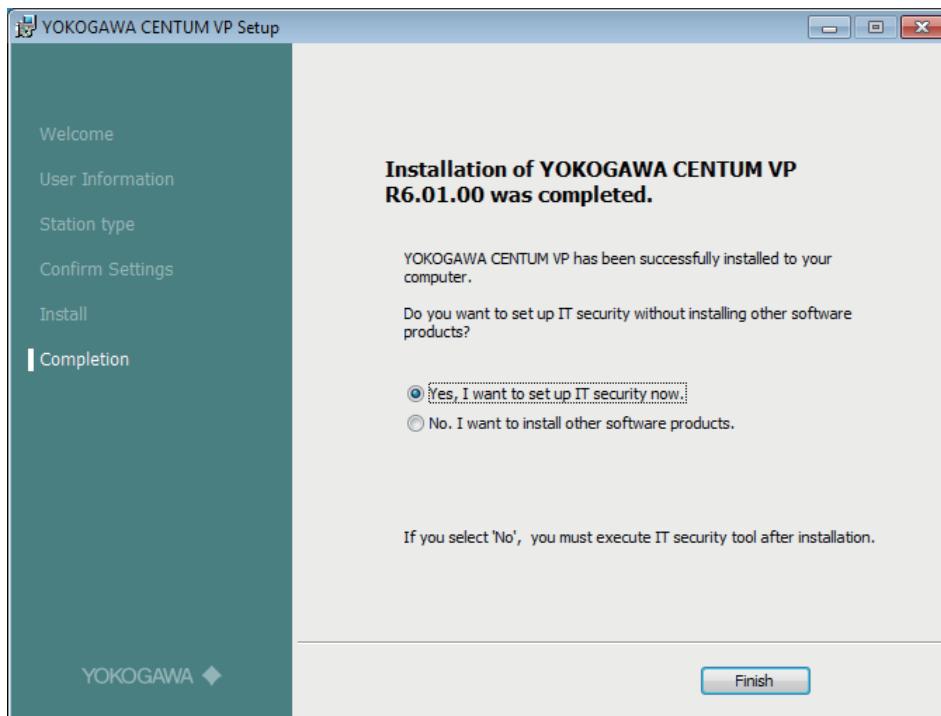


Figure B4.6-8 CENTUM VP Setup Dialog Box (Complete)

IMPORTANT

After an installation including the installation of other YOKOGAWA products, you need to start the IT Security Tool to set up securities. The settings on the IT Security Tool will be valid to all the installed products.

If the security settings are not performed by the IT security tool, the products may not be properly functioning.

**SEE
ALSO**

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

B4.7, "Configuring IT Security Settings" on page B4-94

B4.7 Configuring IT Security Settings

After installing the CENTUM VP software, you must 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 TI 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.
- If you select the Legacy model, restrictions related to Windows are in effect in some environments. For that reason, we recommend you select the Standard model.
- Security settings customized by other than the IT Security Tool are overwritten with the setting information held by the IT Security Tool when the IT Security Tool is run. If you want to use the same security settings as before running the IT Security Tool, customize them again after running the IT Security Tool.

Note that upgrading will run the IT Security Tool and overwrite the security settings.

TIP

- Even when a domain controller is used to perform consolidated management of IT security settings, be sure to set IT security on each client. After setting IT security on all clients, use the domain controller to set up consolidated management of IT security settings.
- When using a computer switchover type UGS in a Windows domain environment, do not add the UGS computer to the domain before you install the CENTUM VP software. In that case, set the Legacy model or the Standard model applying Standalone management temporarily in the IT security setting configuration that you perform following the CENTUM VP software installation.
- When using a computer switchover type UGS in a domain environment, add the UGS computer to the domain and then change the IT security settings to the Standard model applying Domain management or Combination management.

SEE ALSO

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

6.1, "IT Security Tool" in CENTUM VP Security Guide (IM 33J01C30-01EN)

For more information about the procedure for performing consolidated management of IT security settings with a domain controller, refer to:

6.9, "Active Directory-Based Consolidated Management of IT Security Settings" in CENTUM VP Security Guide (IM 33J01C30-01EN)

For more information about precautions for coexistence with other YOKOGAWA product, refer to:

"■ Precautions for Coexistence with Other Product" on page B4-99

For more information about cases that require attention in IT security setting, refer to:

C9., "Cases that Require Attention in IT Security Setting" on page C9-1

■ Running the IT Security Tool

This section describes the procedure for configuring the IT security settings following the completion of CENTUM VP software installation.

IMPORTANT

If the software of the following YOKOGAWA products has already been installed and the YOKOGAWA products do not support IT security version 2.0, the selection of IT security version 1.0 cannot be changed.

- PRM
- ProSafe-RS
- Exaopc
- Exapilot
- Exaplog

If they support IT security version 2.0, the IT security version can be kept or changed.

Follow these steps to run the IT Security Tool:

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

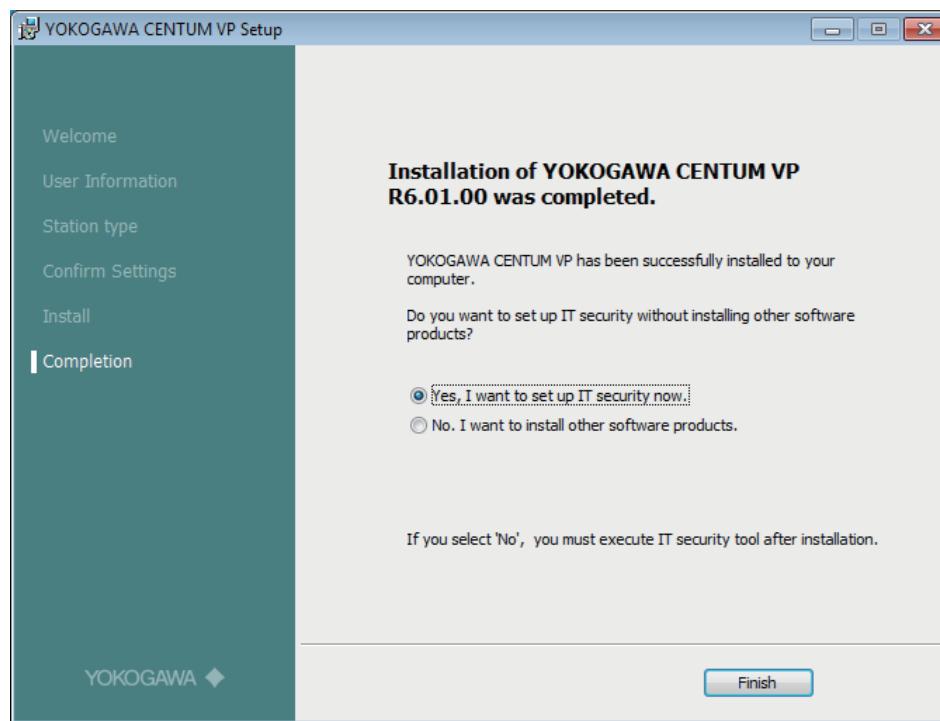


Figure B4.7-1 CENTUM VP Setup Dialog Box (Completed)

The IT Security Tool starts.

TIP

Despite not installing other products, if you select accidentally [No, I want to install other software products.] and click [Finish], start the IT Security Tool from the Start menu and click [Settings] on the menu. The IT Security Settings dialog box appears.

When installing other products, the dialog box appears after completion of the installation, and the IT Security Tool can be started, so there is no need to start from the start menu.



Figure B4.7-2 IT Security Tool (Setup)

2. From the Select IT security version drop-down list, select the IT security version.
3. In the Select security model section, select either [Standard Model] or [Legacy Model].

TIP

If you select [2.0] for Select IT security version, only the Standard model can be selected.

4. In the Select user management section, select [Domain Management], [Combination Management], or [Standalone Management].

TIP

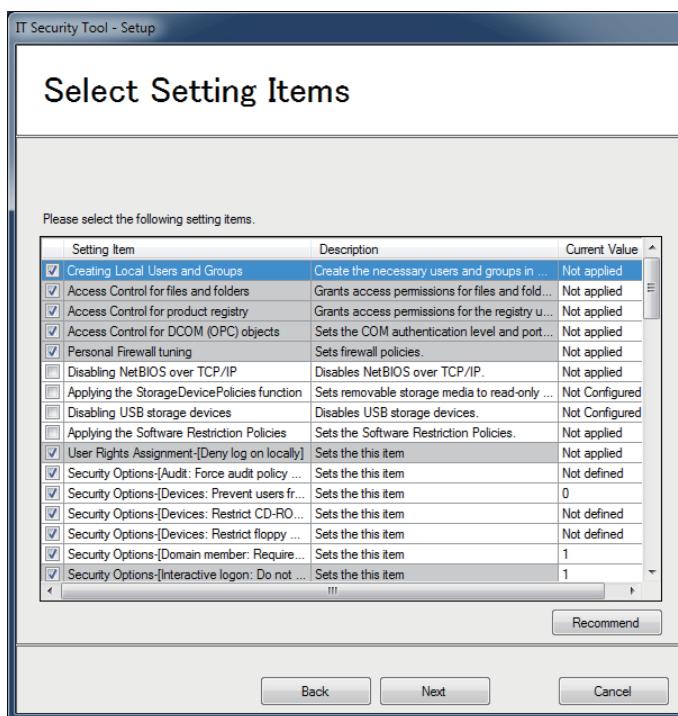
- When you select the Legacy model, you cannot change the user management type from Standalone management.
- If you select [Standalone Management] on a Windows domain member computer, a warning message is displayed. You can go on by clicking [OK].

5. To reconfigure the individual setting items, perform these steps:

TIP

- If IT security version 2.0 is selected, a confirmation dialog box appears. To apply the current settings, click [Yes]. However, when the IT Security Tool is run on the product that supports only IT security version 2.0, this confirmation dialog box does not appear.
- If you do not configure the individual setting items, click [Next]. The security settings are configured. When the setup is complete, the Setup Completed page for security information settings appears. If there is any setting items that have failed, the failed items are displayed. Next, select the [Restart now] check box and click [Finish]. The IT Security Tool is exited and the computer is restarted automatically.

- a. To reconfigure the individual setting items, click [Details]. The Select Setting Items page appears.

**Figure B4.7-3 Select Setting Items Page (When IT Security Version 2.0 Is Selected)**

- b. Select or clear the check boxes of the items you want to change.
Under Current Value, the value currently set for the applicable setting item is displayed according to the following table.

IMPORTANT

The group policy settings that were distributed from the domain controller are not displayed. The local group policy settings are displayed.

Table B4.7-1 Content displayed in Current Value

Content displayed	Description
Actual value	The value actually set is displayed. For example, Enabled, Disabled, 30, 0, etc., is displayed. (*1)
[Not defined]	This is displayed for a setting item relating to security options, for which no value is set.
[Not configured]	This is displayed for a setting item for the group policy management template, for which no value is set.
[Not applied]	This is displayed for a setting item that takes multiple values, for which IT security has never been applied.
[Applied]	This is displayed for a setting item that takes multiple values, for which IT security has been applied at least once.

*1: Even when the set value is a character string in the Security Policy window, it may be managed as a value in the OS, in which case the value is displayed.

TIP

It is recommended not to change the settings when the Standard model is selected.

- c. Click [Next].
The Confirm Setting Information page appears.

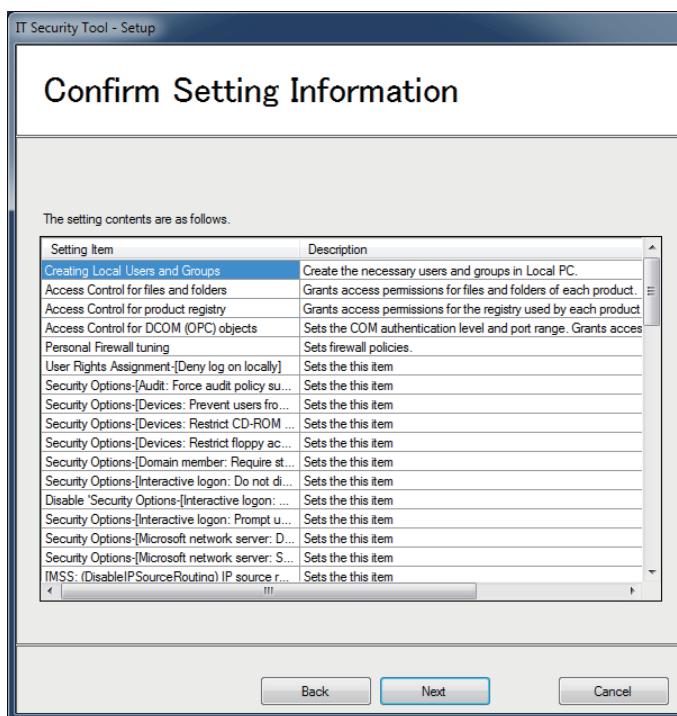


Figure B4.7-4 Confirm Setting Information Page (When IT Security Version 2.0 Is Selected)

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.

6. 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].

When the setup is complete, the Setup Completed page appears. If there is any setting items that have failed, the failed items are displayed.

7. Select the check box for [Restart now] 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

The "Program Compatibility Assistant" dialog box may appear after the security settings configuration is completed. Even when this dialog box appears, the settings have been configured successfully, so click [Cancel] to close it.

SEE ALSO

For more information about the procedure for importing the IT security settings, refer to:

6.7, "Importing/Exporting the IT Security Setting File" in CENTUM VP Security Guide (IM 33J01C30-01EN)

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

6.3, "Changing the IT Security Settings" in CENTUM VP Security Guide (IM 33J01C30-01EN)

For more information about mapping of CENTUM VP applications that can be called from the Start menu, refer to:

"CENTUM VP Applications That Can Be Called Up from the Start Menu" in Read Me First (IM 33J01A10-01EN)

● 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.

In this case, perform the following settings for name solution.

1. From System View on the engineering station, open the properties of each HIS and set the correct host name on the Network tab.
2. In the LMHOSTS file of each station on the network, make the following settings for access to other stations:
 - Location of the LMHOSTS file
PATH: %Systemroot%\system32\drivers\etc
%Systemroot% is the root directory of Windows. Usually, it is <C:\Windows>.
 - Example script in the LMHOSTS file
The following is an example of accessing the project file on HIS0124 (host name = station name).

1hosts
172.17.1.24 HIS0124 #PRE

Table B4.7-2 LMHOSTS File Settings

Station type	Stations to be set in the LMHOSTS file
License management station	All license-assigned stations
HIS	License management station and the computer that holds project files
Stations other than the above	License management station

■ Precautions for Coexistence with Other Product

Precautions to be heeded when a YOKOGAWA product that supports IT security settings co-exists on a CENTUM VP computer are explained.

● Installing the CENTUM VP Software After Installing Other Product

When installing the CENTUM VP software after installing other product that does not support IT security version 2.0, only IT security version 1.0 can be selected.

When installing the CENTUM VP software after installing other product that supports IT security version 2.0, the IT security version can be kept or changed.

- **Installing Other Product After Installing the CENTUM VP Software**

If IT security Version 2.0 is set during the installation of the CENTUM VP software and then IT security settings are configured during the installation of other product that does not support IT security version 2.0, the following warning dialog box will appear.

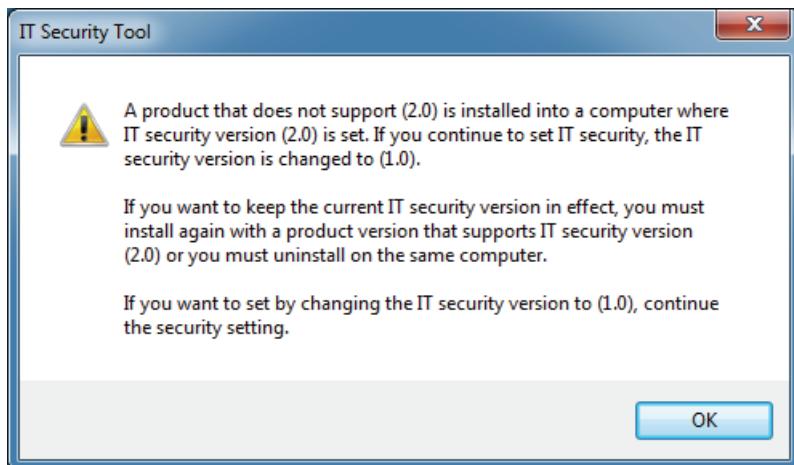


Figure B4.7-5 Warning Dialog Box

In this case, change the specification of IT security version to 1.0.

B4.8 Distributing and Accepting Licenses

Licenses are the rights to use CENTUM VP 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 CENTUM VP system, one computer is always one license management station and other computers are license-assigned stations. The license management station can be set up on a computer where a CENTUM VP station, such as HIS, runs.

**SEE
ALSO**

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

1.1.3, “Overview of license management process” in License Management (IM 33J01C20-01EN)

For more information about version up procedure of license, refer to:

4., “Upgrading the Licenses from CENTUM VP R5 to R6, or from ProSafe-RS R3 to R4” in License Management (IM 33J01C20-01EN)

B4.9 Creating User Accounts

Create accounts for CENTUM VP.

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 CENTUM VP user groups. Therefore, you need to register the created user as a member of the appropriate CENTUM VP 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:

B2.5, "Creating Domain Users" on page B2-16

■ Limitation on User Account Names in CENTUM Authentication Mode

- 20 characters at maximum.
- Space, tabs, and multi-byte characters such as half-width katakana and Chinese characters (kanji) cannot be used.

■ Limitation on User Account Names in Windows Authentication Mode

- 16 characters at maximum.
- Space, tabs, and multi-byte characters such as half-width katakana and Chinese characters (kanji) cannot be used.
- Only upper-case characters are allowed.
- Cannot end with a period.

B4.9.1 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. Open Control Panel.
3. Select [System and Security] > [Administrative Tools] > [Computer Management].
The Computer Management window appears.
4. On the tree view in the left pane of the window, select [System Tools] > [Local Users and Groups] > [Users].
5. Select [Action] > [New User].
The New User dialog box appears.
6. Add a user account. (The rest of the steps shows an example of adding a new user account, OPERATOR.)

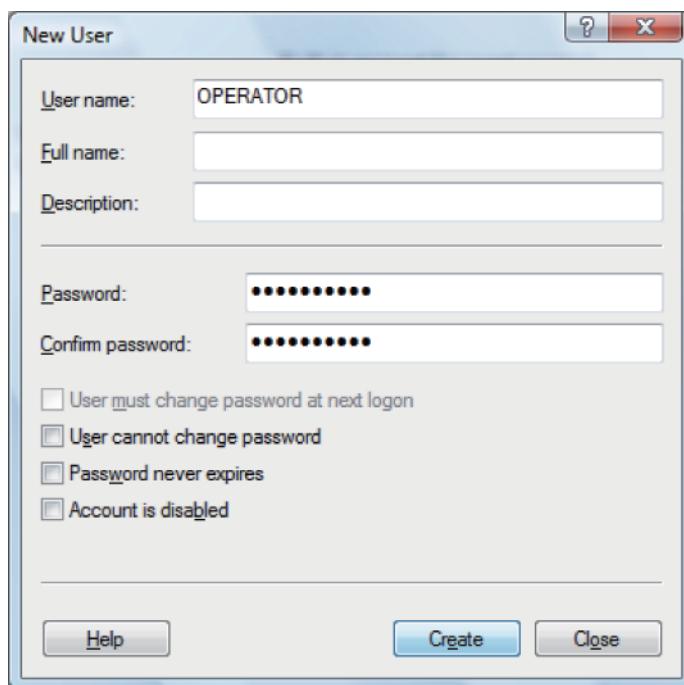


Figure B4.9.1-1 New User Dialog Box

7. Right-click the user you have created and select [Properties], and then click [Add] on the Member of tab.

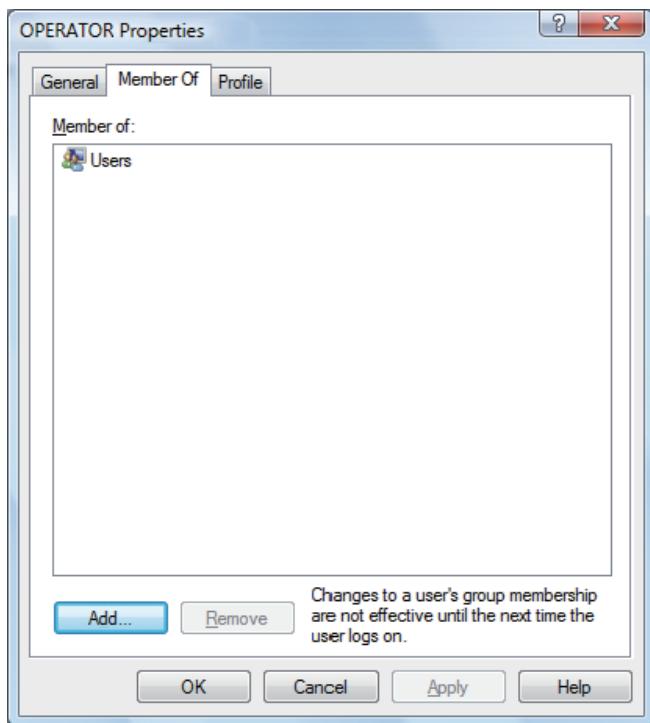


Figure B4.9.1-2 User Properties

8. Select an appropriate user group for the created user and click [OK].

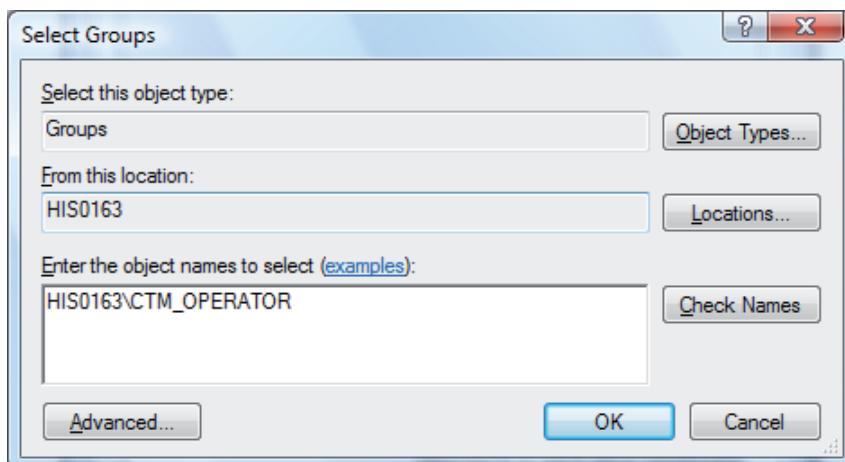


Figure B4.9.1-3 Select Groups

TIP

A user who belongs to the administrative group (CTM_MAINTENANCE, CTM_ENGINEER_ADM) must also be a member of the Administrators group.

9. In the user properties dialog box, confirm that the group you selected has been added to the Member of list.

B4.9.2 When the Legacy Model of Security Settings are Applied

A user account named CENTUM has been automatically created by the IT Security Tool. The default password for this account is "Yokogawa1." Change this password at the first logon.

You can create other user accounts for engineering purposes. The procedure for creating user accounts is the same as creating user accounts on the Standalone management computer. However, with Legacy model, a Windows user group CTM_ENGINEER is not created. There is no need to add the created user to the CTM_ENGINEER group.

SEE ALSO

For more information about creating user accounts, refer to:

B4.9.1, "When the Standard Model with Standalone Management Security Settings are Applied" on page B4-103

■ Changing the Maximum Password Age

The password for the CENTUM account, which is automatically created with Legacy security model, is defined with a limited time by default. In this case, when the password expires, the actions such as downloading to HIS, displaying sequence table status or SFC flow chart status may not function properly. It is recommended to set [Password never expires] for this password.

The procedure for setting the password age is as follows:

1. Logon as an administrative user.
2. Open Control Panel.
3. Select [System and Security] > [Administrative Tools] > [Computer Management].
The Computer Management window appears.
4. Under [System Tools], select [Local Users and Groups] > [Users].
5. Select the CENTUM user and open its properties.

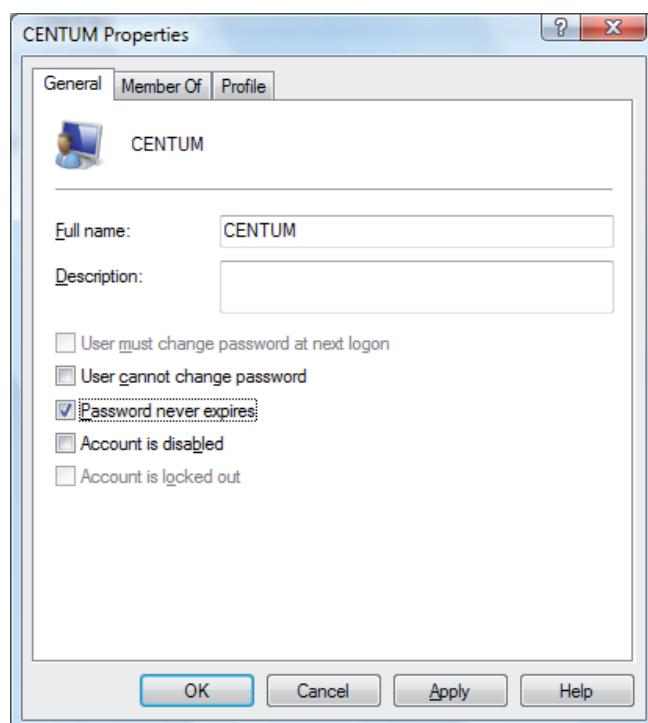


Figure B4.9.2-1 CENTUM Properties

-
6. Select the [Password never expires] check box and click [OK].

B4.10 Configuring Windows Environment Settings for Each User

After creating user accounts, configure the required Windows environment settings for each user.

■ Windows Setting Items and Required Settings on Each Station

The Windows setting items to be configured for each user vary, depending on the type of the station and Windows OS version. Configure the required Windows settings based on the following table.

Table B4.10-1 Windows Setting Items and Whether Configuration is Required on Each Station

Windows setting item	HIS	APCS	SIOS	GSGW	UGS	UACS station	Computer installed with only system builders	Computer installed with only AD Server
Windows security center/action center alerts (*1)	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Display properties (color)/appearance/screen saver/resolution	Yes	No	No	No	No	No	No	Yes
Display Scale	Yes	No	No	No	No (*2)	No	No	No
Scroll settings (*3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Virtual desktops (*3)	Yes (*4)	Yes (*5)	Yes (*4)	Yes (*4)				
Windows Firewall toast notification (*6)	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes

*1: Only on Windows 7, Server 2008 R2 and Windows Server 2012 R2

*2: "Yes" for computer switchover type UGS.

*3: Only on Windows 10 and Windows Server 2016

*4: According to whether to use virtual desktops, configure the setting for when using virtual desktops or the setting for when not using virtual desktops.

*5: Configure the setting for when not using virtual desktops.

*6: This setting is required only on Windows 10 where the legacy IT security model is applied.

B4.10.1 Configuring on Windows 10

Follow these procedures when you use a Windows 10 computer.

■ Display Properties

The procedure for setting the display properties is explained as follows.

1. Sign in using the user account for which to set display properties.
2. Open Control Panel.
3. Select [Appearance and Personalization] > [Personalization].
The Personalization window appears.

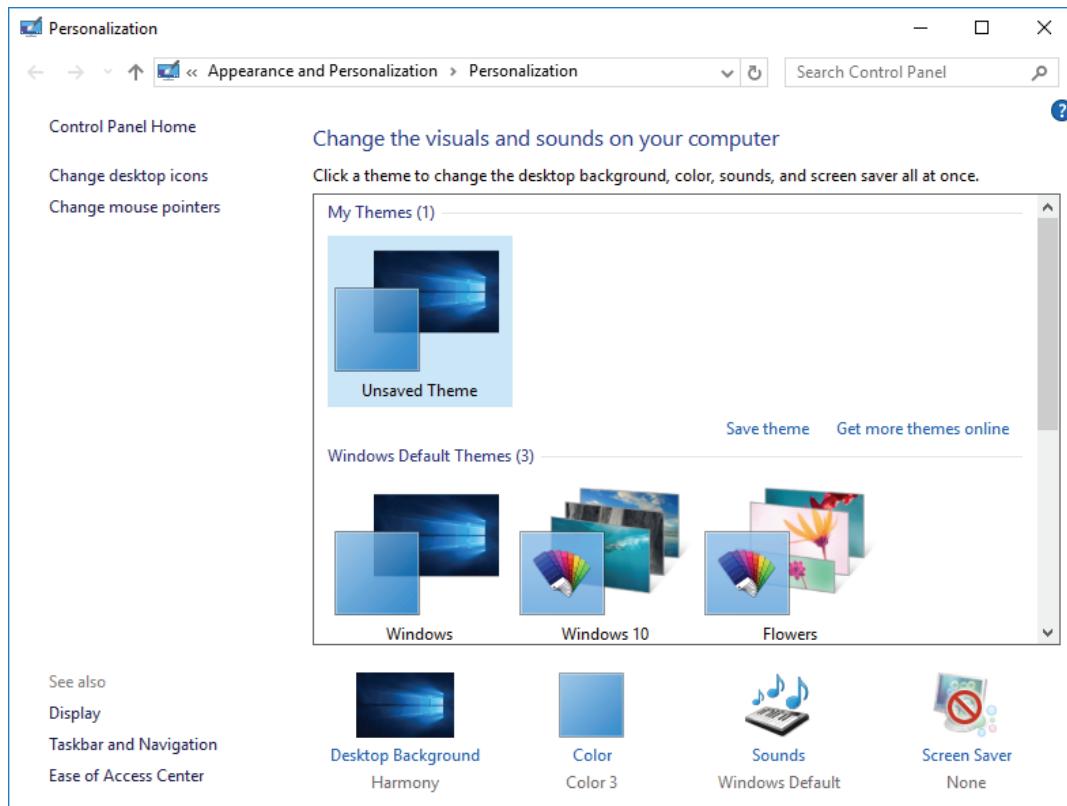


Figure B4.10.1-1 Personalization Window

4. From Windows Default Themes, select [Windows].
5. Select [Desktop Background].
The Windows Settings window appears.

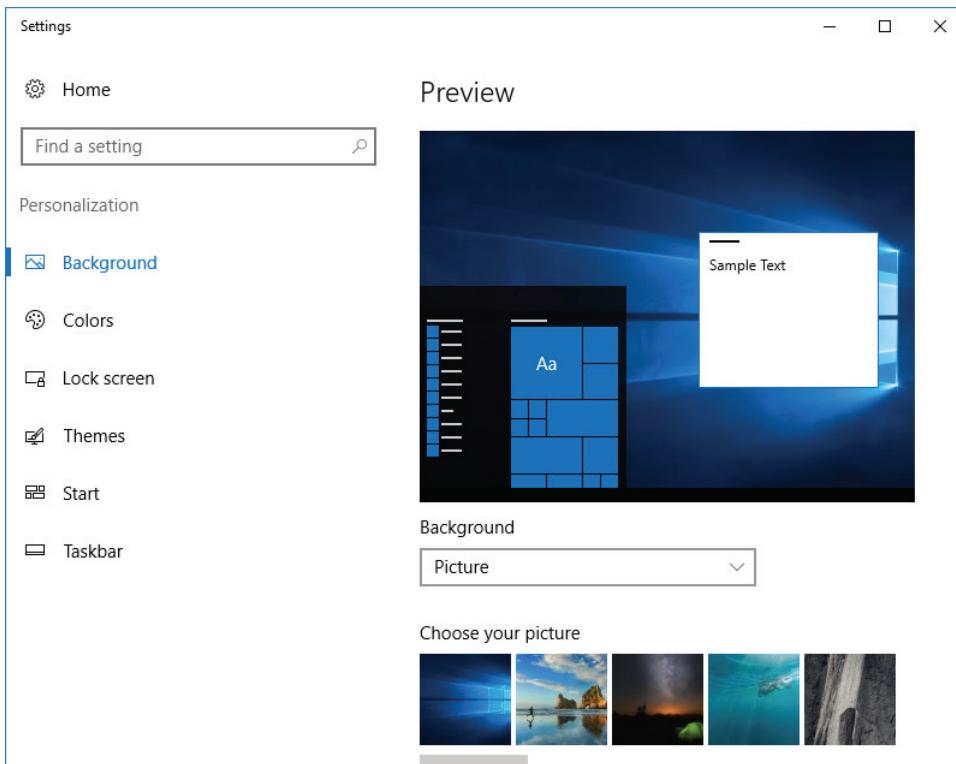


Figure B4.10.1-2 Settings Window

6. From the Background drop-down list, select [Solid Colors] and select a desired background color.
7. Click the [x] button to close the window.
Return to the Personalization window
8. Select [Screen Saver].
The Screen Saver Settings dialog box appears.

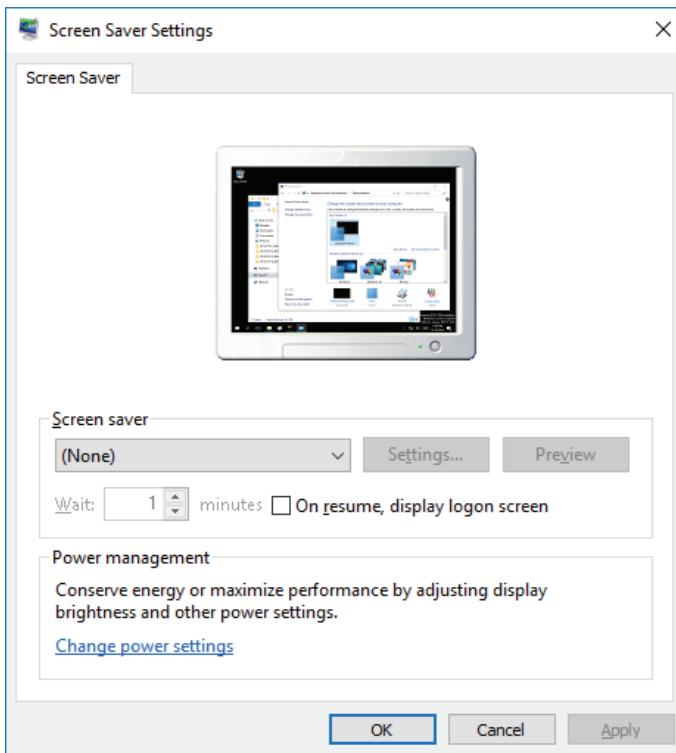


Figure B4.10.1-3 Screen Saver Settings Dialog Box

9. From the Screen Saver drop-down list, select [(None)], and then click [OK].
10. From the Start menu, start the Windows Settings window.
11. Select [System] > [Display].
12. In the right pane, click [Advanced display settings].
The Advanced display settings page appears.
13. Set the resolution to one of the following and click [Apply].
 - Normal monitor: 1280 x 1024 or 1600 x 1200
 - Wide screen monitor: 1280 x 800, 1440 x 900, 1680 x 1050, 1920 x 1080, or 1920 x 1200

■ Display Scale

The procedure for setting the display scale is explained as follows.

1. Sign in using the user account for which to set display scale.
2. Start the Windows Settings window.
3. Select [System] > [Display].
The Customize your display page appears.

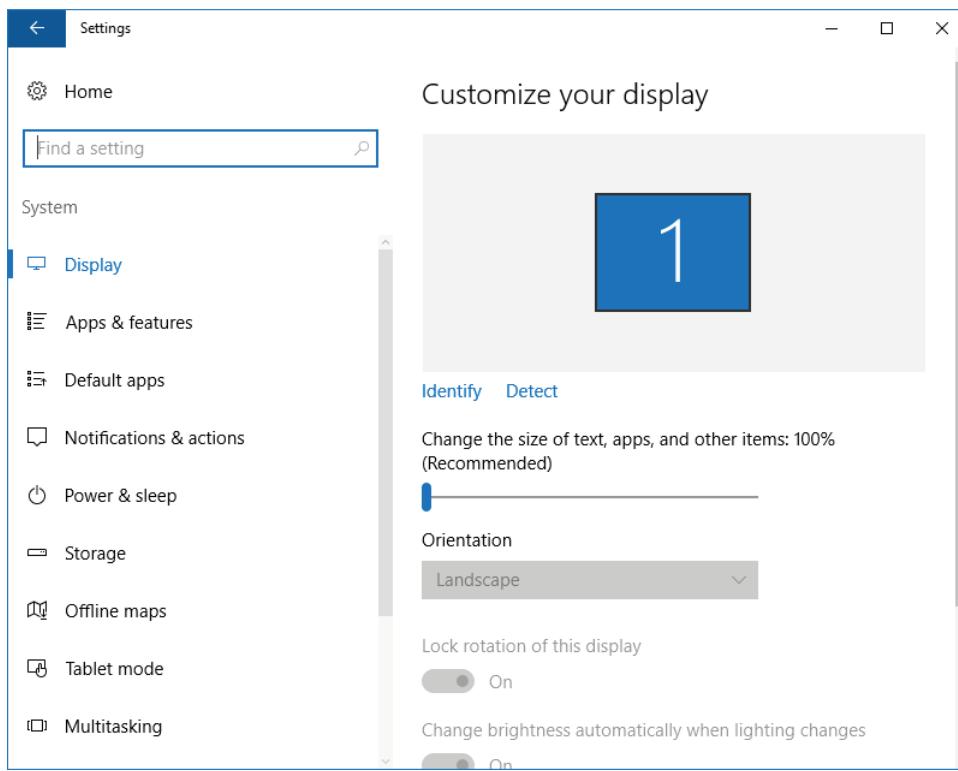


Figure B4.10.1-4 Customize Your Display Page

4. Adjust the [Change the size of text, apps, and other items] slider to 100%.
5. Click the [x] button to close the window.

■ Setting for Scrolling of Inactive Windows

In Windows 10, inactive windows can be scrolled with the mouse wheel. Stop this function because it can cause malfunction of the system.

Follow these steps to stop the inactive window scrolling function:

1. Sign in with the user account for which to disable scrolling of inactive windows.
2. Start the Windows Settings window.
3. Select [Devices].
4. In the left pane, select [Mouse & touchpad].
The Mouse page appears.

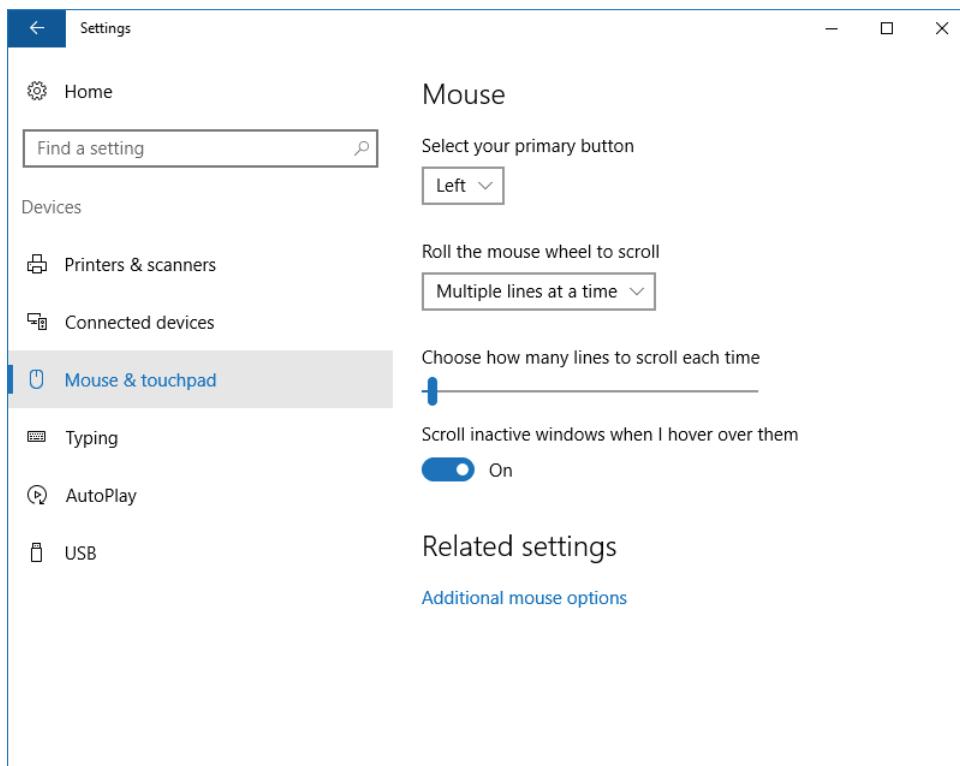


Figure B4.10.1-5 Mouse Page

5. Turn off [Scroll inactive windows when I hover over them].
6. Click the [x] button to close the window.

■ Virtual Desktops

With Windows 10, virtual desktops can be used. The virtual desktop is a function that lets you have multiple desktops virtually. You can switch among the multiple desktops to select the one you want to display.

By using the software for this product with the virtual desktop function, you can display different operation and monitoring windows on multiple desktops, or display operation and monitoring windows and other windows on different desktops.

When using the software for this product on virtual desktops, make sure all virtual desktop windows are shown on the taskbar.

If virtual desktops are not to be used, hide the task view buttons on the taskbar.

IMPORTANT

- There are precautions to be heeded when performing operation and monitoring on virtual desktops. Be sure to check those precautions.
- Do not use virtual desktops on computers that are set up as APCS, SIOS, GSGW, or UGS.
- Virtual desktops are not available when the software of Console HIS Support Package for Enclosed Display Style, Console HIS Support Package for Open Display Style, or Eight-loop Simultaneous Operation Package (for AIP831) is enabled.

SEE ALSO

For more information about the precautions for use of virtual desktops, refer to:

- Virtual Desktops in Windows 10 and Windows Server 2016" in 1., "Human Interface Station" in Human Interface Stations Reference Vol.1 (IM 33J05A10-01EN)

● Setting for When Using Virtual Desktops

When using virtual desktops, make sure all virtual desktop windows are shown on the taskbar.

Follow these steps to show all virtual desktop windows on the taskbar:

1. Sign in as a user who uses virtual desktops.
2. Start the Windows Settings window.
3. Select [System].
4. In the left pane, select [Multitasking].
5. Under Virtual desktops in the right pane, select "All Desktops" from the [On the taskbar, show windows that are open on] drop-down list.

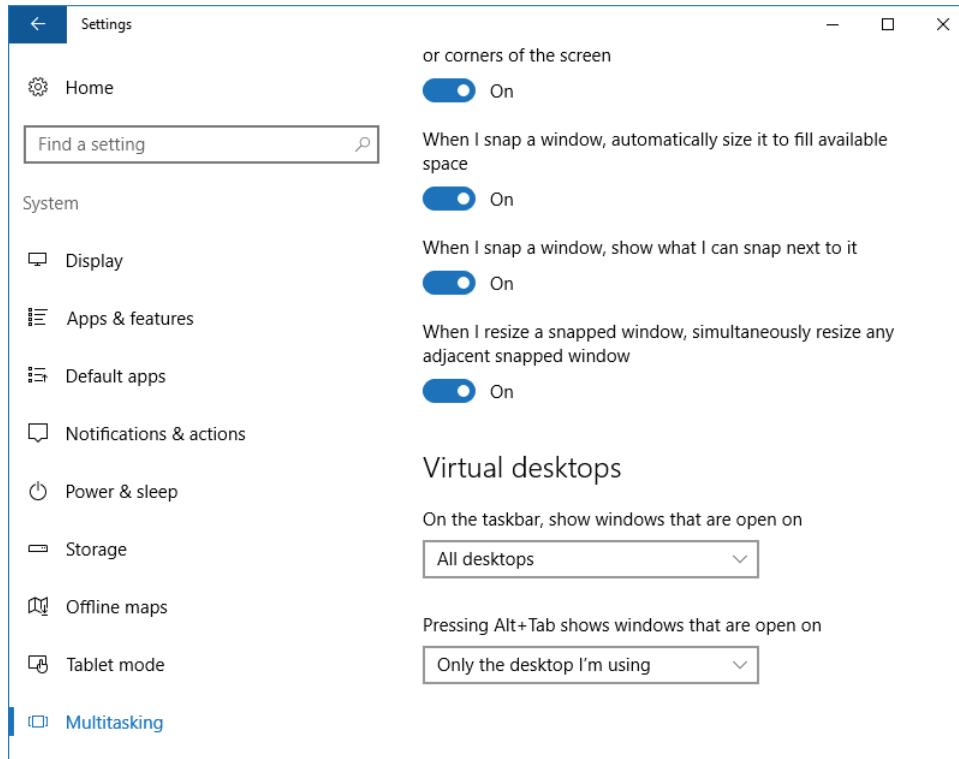


Figure B4.10.1-6 Settings Window

6. Click the [x] button to close the window.

● Setting for When Not Using Virtual Desktops

If virtual desktops are not to be used, hide the task view buttons on the taskbar.

IMPORTANT

Once this operation is performed, the virtual desktops will become inoperable. Before performing this operation, ensure that no virtual desktops have been configured for use.

Follow these steps to hide the task view buttons on the taskbar:

1. Sign in as a user who does not use virtual desktops.
2. Right-click the taskbar at the bottom of the desktop, and clear the [Show Task View Button] check box.

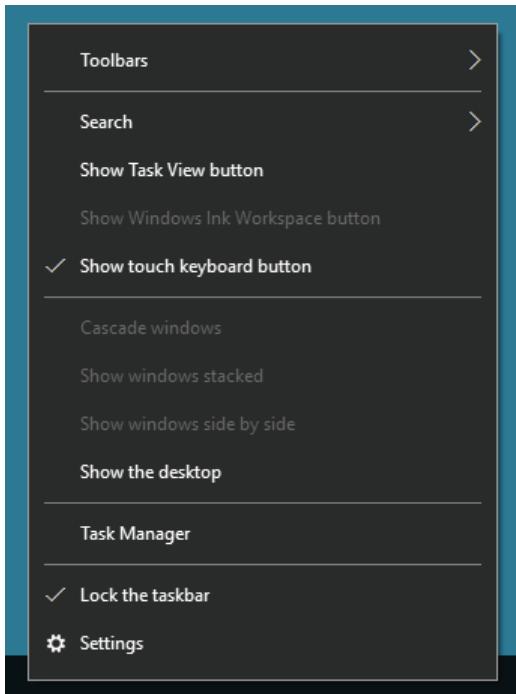


Figure B4.10.1-7 Taskbar Context Menu

■ Suppressing Toast Notifications Regarding Windows Firewall

This configuration is necessary when the legacy IT security model is applied.

Follow these steps to suppress toast notifications regarding Windows Firewall:

1. Sign in as an administrative user.
2. Open Control Panel.
3. Select [System and Security] > [Windows Firewall].
The Windows Firewall window appears.
4. In the left pane, click [Turn Windows Firewall on or off].
5. Select [Turn off Windows firewall] in the private network settings, public network settings, and domain network settings. However, you need to configure the domain network settings only in domain environments.
6. Click [OK].
7. Sign out and sign in again using the user account for which to turn off toast notifications regarding Windows Firewall.
8. Open Control Panel.
9. Select [System and Security] > [Security and Maintenance].
The Security and Maintenance window appears.
10. On the left pane, click [Change Security and Maintenance settings].
11. Clear the [Network firewall] check box under Security messages.
12. Click [OK].

TIP

- If the [Network firewall] check box is grayed out, wait for a few minutes until it is enabled.
 - With a user account for which CENTUM desktop is set up, you cannot open Control Panel. To perform this configuration, cancel the CENTUM desktop first.
 - If a toast notification [Turn on Windows firewall] appears, carry out the above procedure without clicking the toast notification.
-

B4.10.2 Configuring on Windows 7

Follow these procedures when you use a Windows 7 computer.

■ Windows Security Center/Action Center Alerts

Windows Security Center and Action Center manage all functions required for security protection of the computer.

For computers on which software for this product is to be installed, it is recommended to disable Windows automatic update. Accordingly, Windows automatic update is disabled when the software for this product is installed.

If Windows automatic update is disabled, alerts are notified from the Windows Security Center and Action Center; accordingly, the procedure for disabling these alerts is described.

IMPORTANT

To enable Windows automatic update, Windows automatic update must be manually enabled after the software for this product is installed. In such a case, this setting is not required.

TIP

Windows Security Center and Action Center are client security monitoring services.

1. Log on using the user account for which the alerts of Windows Security Center and Action Center are to be disabled.
2. Open Control Panel.
3. Set the display style of Control Panel to Small icons.
4. From the items displayed in Control Panel, select [Notification Area Icons].
The Notification Area Icons window appears.

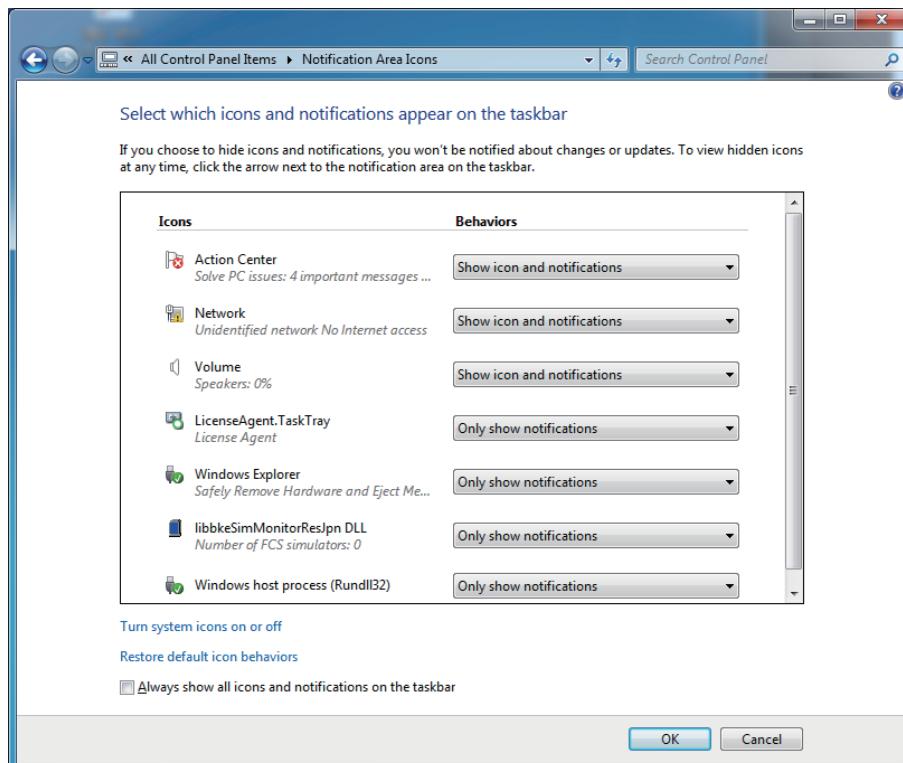


Figure B4.10.2-1 Notification Area Icons Window

TIP

If the Action Center setting is grayed out, clear the [Always show all icons and notifications on the taskbar] check box. If the setting is still grayed out after clearing this check box, wait for a few minutes until it becomes active.

If the Action Center icon does not appear in the Notification Area Icons window, click [Turn system icons on or off] and, in the window that appears, turn on the setting for [Action Center]. If this setting is grayed out when the window appears, also wait for a few minutes until it becomes active.

5. For [Action Center], select [Hide icon and notifications] and click [OK].

TIP

On license-assigned stations, select [Show icon and notifications] for [LicenseAgent.TaskTray].

SEE ALSO

For more information about the procedure for manually enabling Windows automatic updates, refer to:

- “Enabling Windows Update” on page C7-7

■ 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. Open Control Panel.
3. Select [Appearance and Personalization] > [Personalization].
The Personalization window appears.

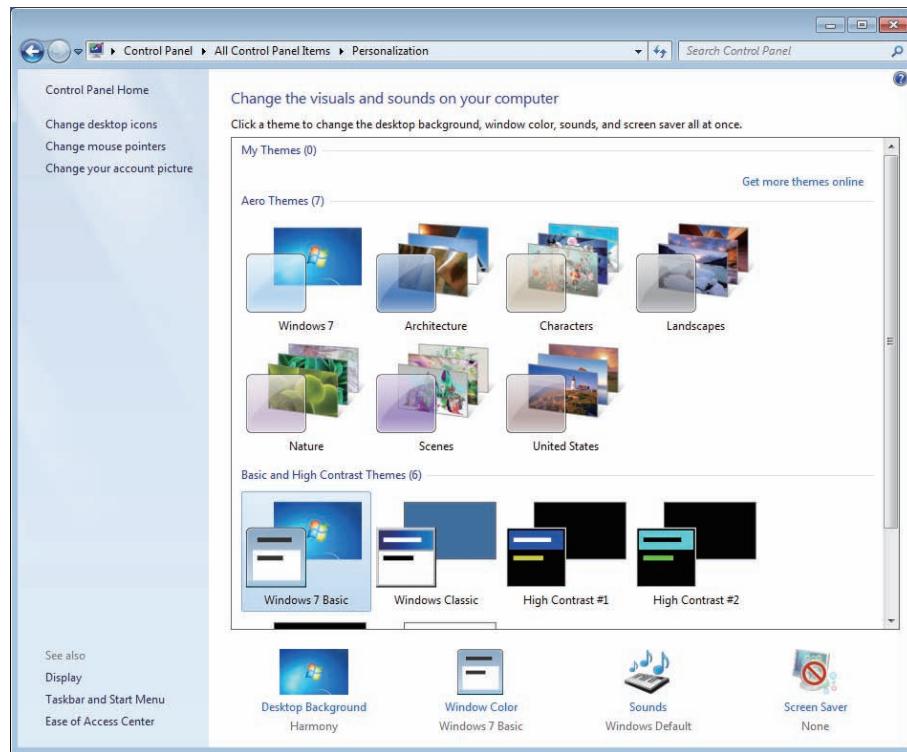


Figure B4.10.2-2 Personalization Window

4. From Aero Themes, select [Windows 7].
5. Select [Personalization] > [Desktop Background].
The Desktop Background window appears.

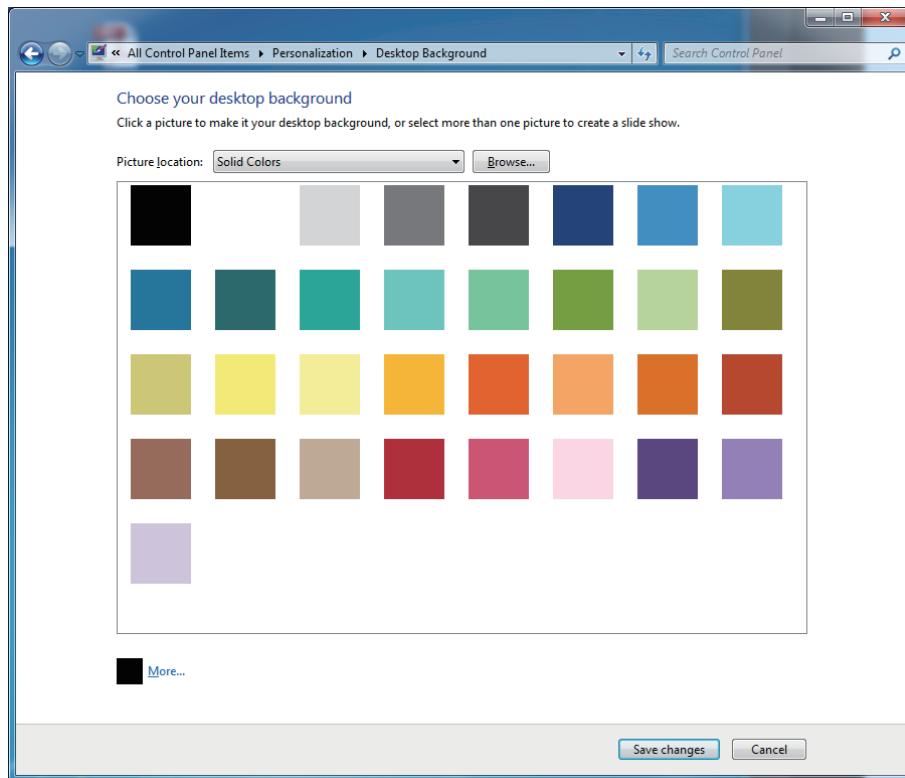


Figure B4.10.2-3 Desktop Background Window

6. Set [Solid Colors] for Picture location, select the color of your choice, and then click [Save changes].
7. Select [Screen Saver].
The Screen Saver Settings dialog box appears.



Figure B4.10.2-4 Screen Saver Settings Dialog Box

8. Select [(None)] for Screen saver and click [OK].

9. Open Control Panel.
10. Select [Appearance and Personalization] > [Display] > [Adjust resolution].
The Screen resolution window appears.
11. Set the resolution to one of the following and click [OK].
 - Normal monitor: 1280 x 1024 or 1600 x 1200
 - Wide screen monitor: 1280 x 800, 1440 x 900, 1680 x 1050, 1920 x 1080, or 1920 x 1200
12. Select [Display] > [Adjust resolution] > [Advanced Settings].
The Advanced Settings dialog box appears.

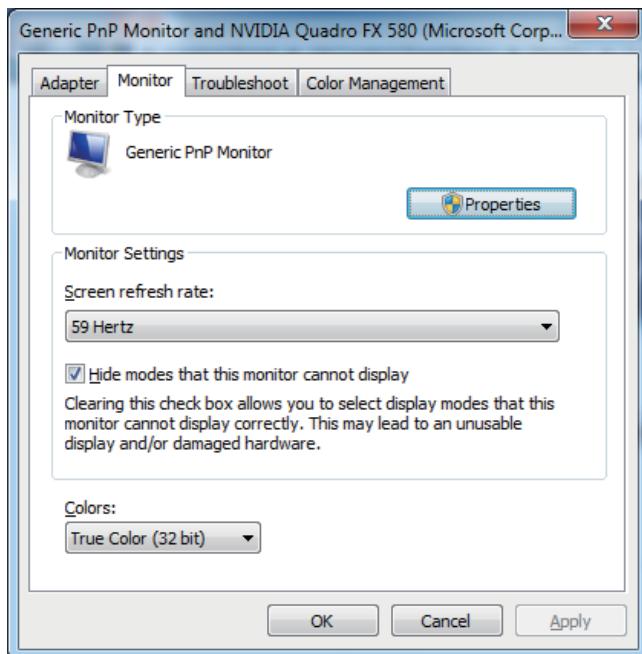


Figure B4.10.2-5 Advanced Settings Dialog Box

13. Select the [Monitor] tab, set [True Colors (32 bit)] for Colors and click [OK].

■ Display Scale

The procedure for setting the display scale is explained as follows.

1. Log on using the user account for which to set display scale.
2. Open Control Panel.
3. Select [Appearance and Personalization] > [Display].
The Display window appears.

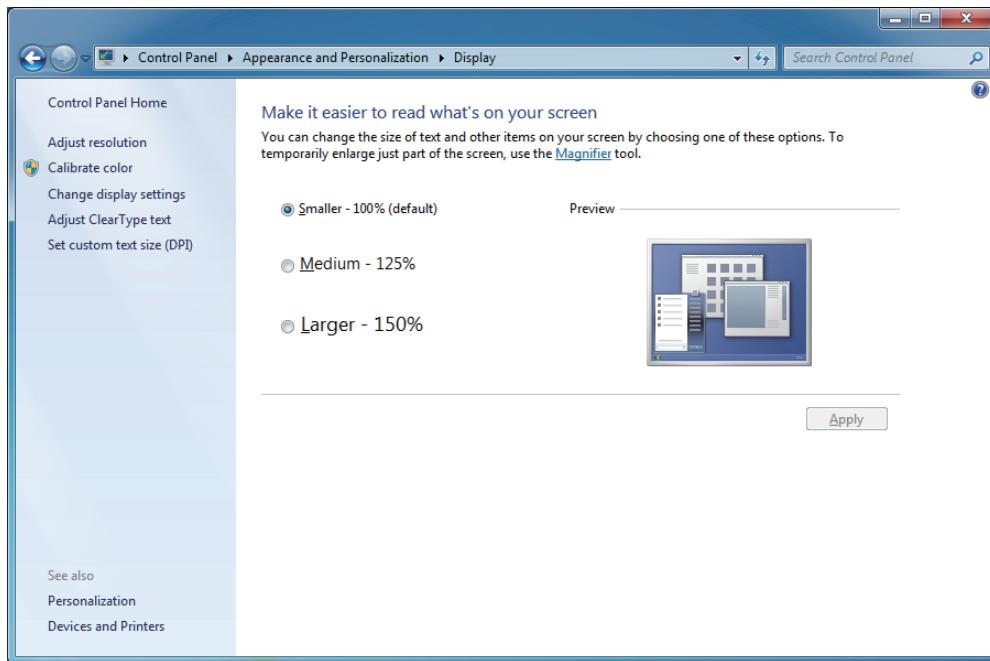


Figure B4.10.2-6 Display Window

4. Select [Smaller - 100%].

B4.10.3 Configuring on Windows Server 2016

Follow these steps when you use a Windows Server 2016 computer:

■ Display Properties

The procedure for setting the display properties is explained as follows.

1. Sign in using the user account for which to set display properties.
2. Open Control Panel.
3. Select [Appearance and Personalization] > [Personalization].
The Personalization window appears.

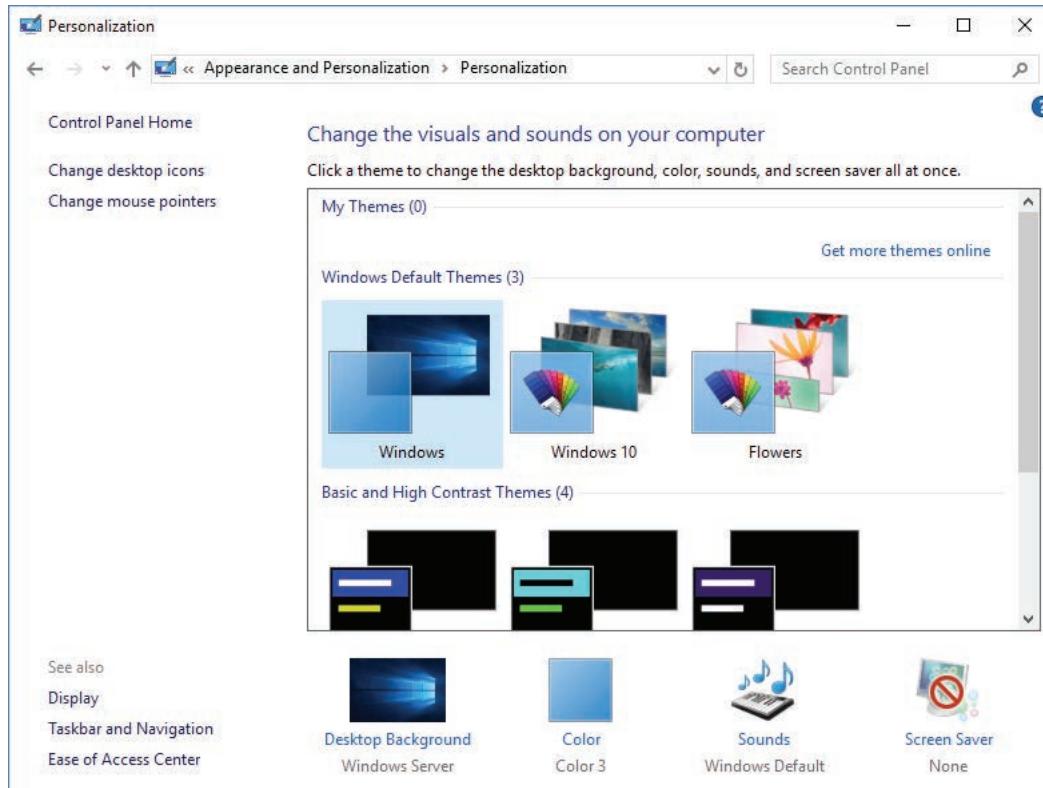


Figure B4.10.3-1 Personalization Window

4. From Windows Default Themes, select [Windows].
5. Select [Desktop Background].
The Windows Settings window appears.

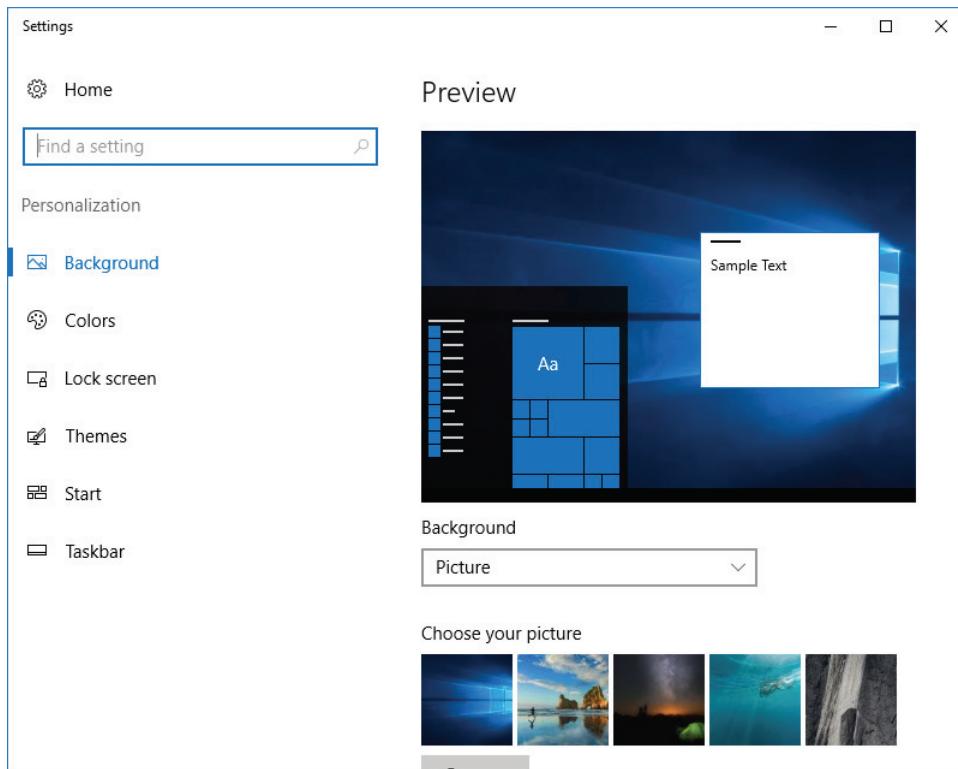


Figure B4.10.3-2 Settings Window

6. From the Background drop-down list, select [Solid Colors] and select a desired background color.
7. Click the [x] button to close the window.
The screen returns to the Personalization window.
8. Select [Screen Saver].
The Screen Saver Settings dialog box appears.

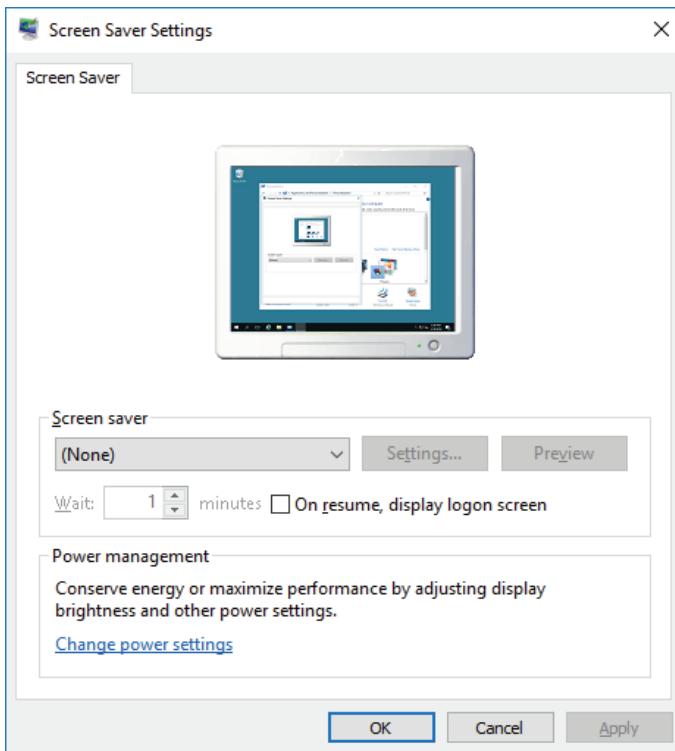


Figure B4.10.3-3 Screen Saver Settings Dialog Box

9. From the Screen Saver drop-down list, select [(None)], and then click [OK].
10. From the Start menu, start the Windows Settings window.
11. Select [System] > [Display].
12. In the right pane, click [Advanced display settings].
The Advanced display settings page appears.
13. Set the resolution to one of the following and click [Apply].
 - Normal monitor: 1280 x 1024 or 1600 x 1200
 - Wide screen monitor: 1280 x 800, 1440 x 900, 1680 x 1050, 1920 x 1080, or 1920 x 1200

■ Display Scale

The procedure for setting the display scale is explained as follows.

1. Sign in using the user account for which to set display scale.
2. Start the Windows Settings window.
3. Select [System] > [Display].
The Customize your display page appears.

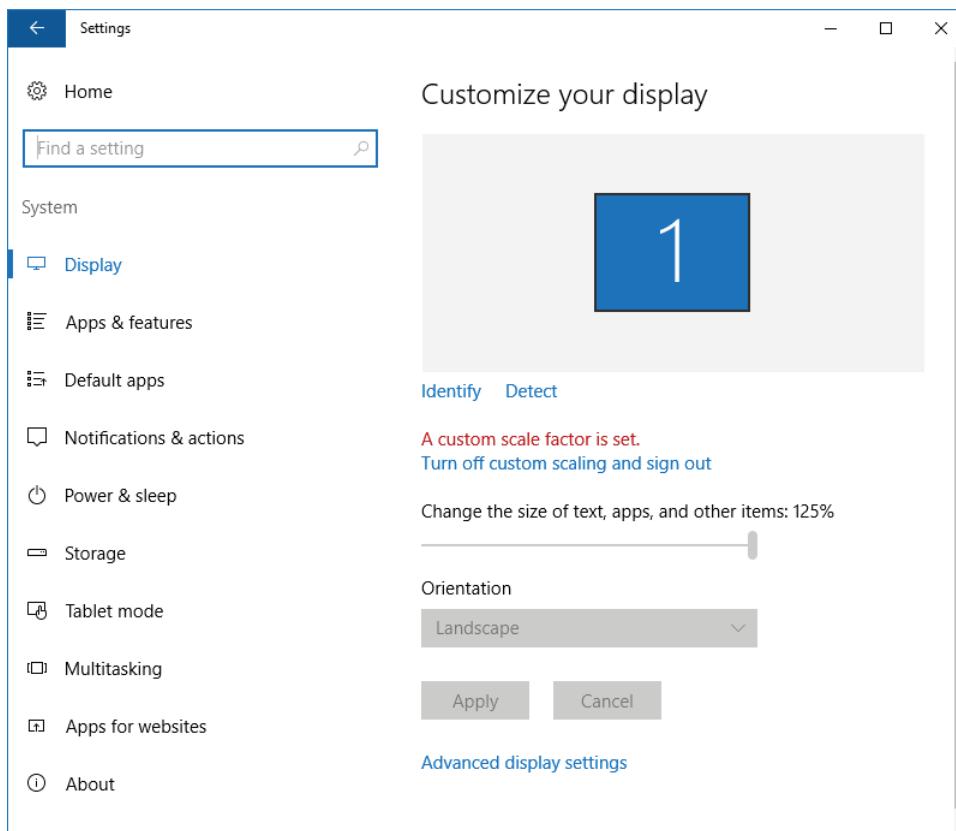


Figure B4.10.3-4 Customize Your Display Page

4. Adjust the [Change the size of text, apps, and other items] slider to 100%.
5. Click the [x] button to close the window.

■ Setting for Scrolling of Inactive Windows

In Windows Server 2016, inactive windows can be scrolled with the mouse wheel. Stop this function because it can cause malfunction of the system.

Follow these steps to stop the inactive window scrolling function:

1. Sign in with the user account for which to disable scrolling of inactive windows.
2. Start the Windows Settings window.
3. Select [Devices].
4. In the left pane, select [Mouse & touchpad].
The Mouse page appears.

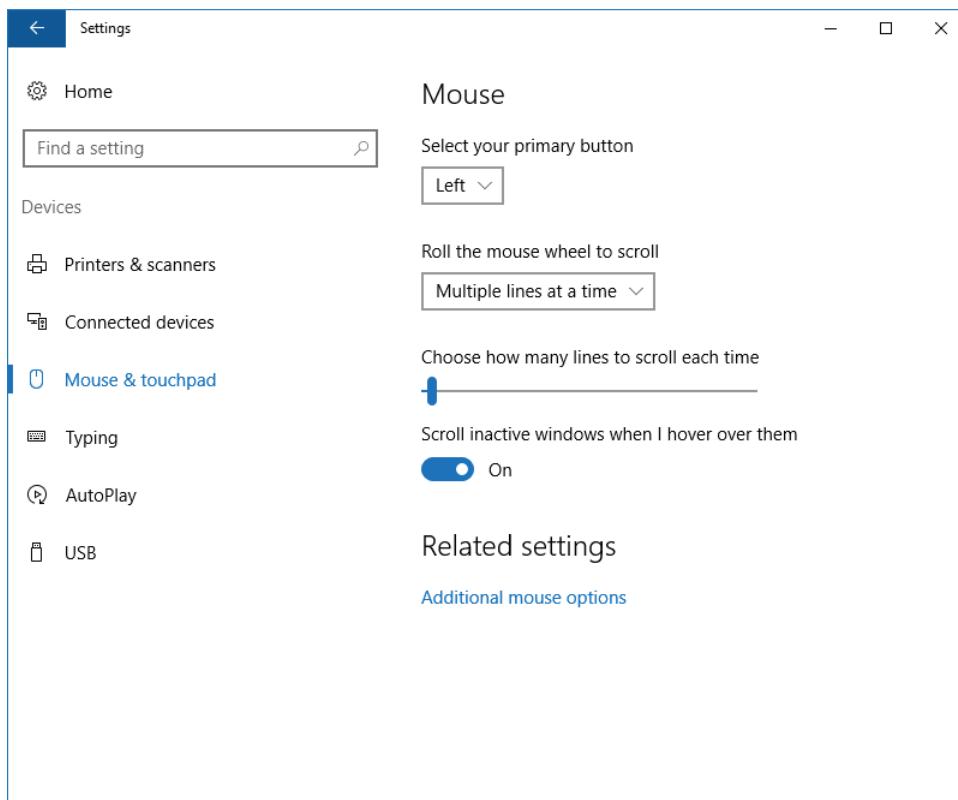


Figure B4.10.3-5 Mouse Page

5. Turn off [Scroll inactive windows when I hover over them].
6. Click the [x] button to close the window.

■ Virtual desktops

With Windows Server 2016, virtual desktops can be used. The virtual desktop is a function that lets you have multiple desktops virtually. You can switch among the multiple desktops to select the one you want to display.

By using the software for this product with the virtual desktop function, you can display different operation and monitoring windows on multiple desktops, or display operation and monitoring windows and other windows on different desktops.

When using the software for this product on virtual desktops, make sure all virtual desktop windows are shown on the taskbar.

If virtual desktops are not to be used, hide the task view buttons on the taskbar.

IMPORTANT

- There are precautions to be heeded when performing operation and monitoring on virtual desktops. Be sure to check those precautions.
- Do not use virtual desktops on computers that are set up as APCS, SIOS, GSGW, or UGS.
- Virtual desktops are not available when the software of Console HIS Support Package for Enclosed Display Style, Console HIS Support Package for Open Display Style, or Eight-loop Simultaneous Operation Package (for AIP831) is enabled.

SEE ALSO

For more information about the precautions for use of virtual desktops, refer to:

- Virtual Desktops in Windows 10 and Windows Server 2016" in 1., "Human Interface Station" in Human Interface Stations Reference Vol.1 (IM 33J05A10-01EN)

● Setting for When Using Virtual Desktops

When using virtual desktops, make sure all virtual desktop windows are shown on the taskbar.

Follow these steps to show all virtual desktop windows on the taskbar:

1. Sign in as a user who uses virtual desktops.
2. Start the Windows Settings window.
3. Select [System].
4. In the left pane, select [Multitasking].
5. At the Virtual desktops in the right pane, select "All Desktops" from the [On the taskbar, show windows that are open on] drop-down list.

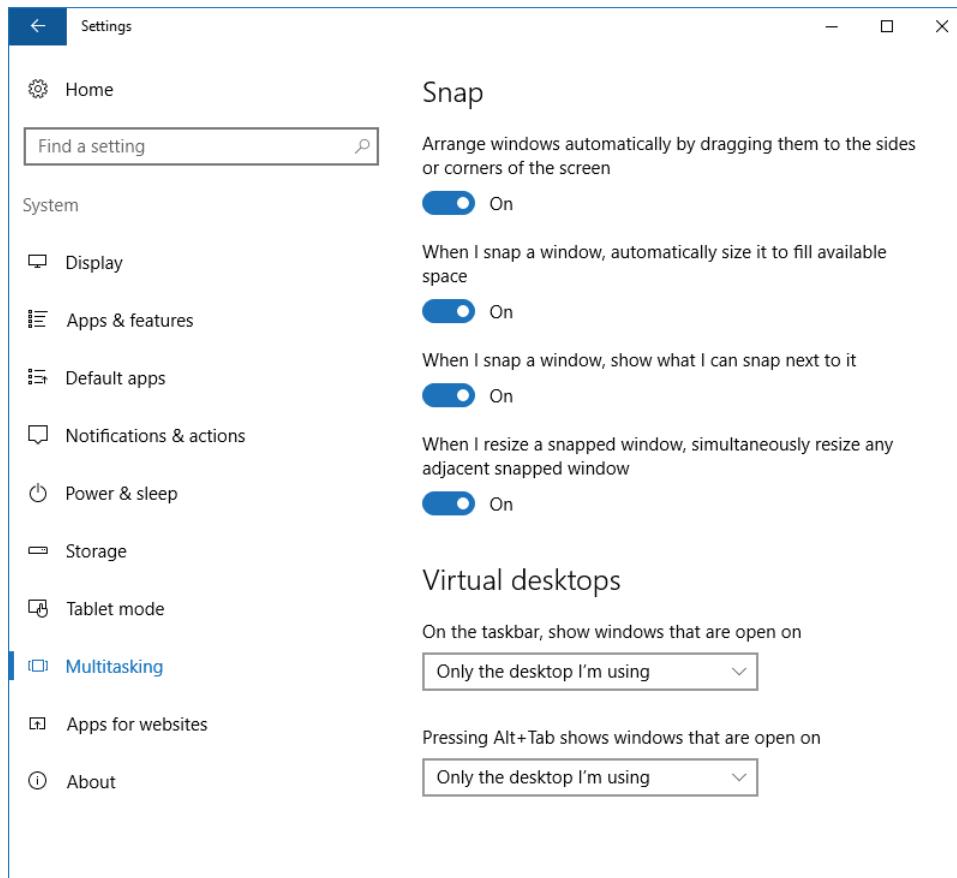


Figure B4.10.3-6 Settings Window

6. Click the [x] button to close the window.

● Setting for When Not Using Virtual Desktops

If virtual desktops are not to be used, hide the task view buttons on the taskbar.

IMPORTANT

Once this operation is performed, the virtual desktops will become inoperable. Before performing this operation, ensure that no virtual desktops have been configured for use.

Follow these steps to hide the task view buttons on the taskbar:

1. Sign in as a user who does not use virtual desktops.
2. Right-click the taskbar at the bottom of the desktop, and clear the [Show Task View Button] check box.

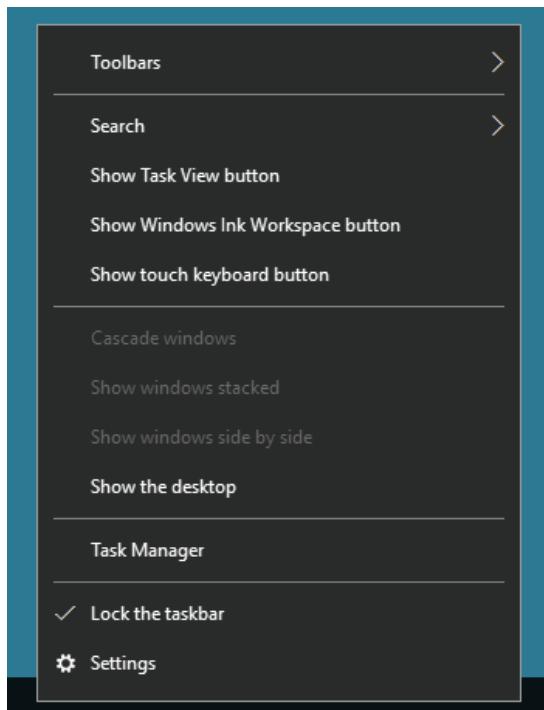


Figure B4.10.3-7 Taskbar Context Menu

B4.10.4 Configuring on Windows Server 2012 R2

Follow these steps when you use a Windows Server 2012 R2 computer.

TIP

Windows Server 2012 R2 is supported only for use on computer switchover type UGS.

■ Windows Security Center/Action Center Alerts

Windows Security Center and Action Center manage all functions required for security protection of the computer.

For computers on which software for this product is to be installed, it is recommended to disable Windows automatic update. Accordingly, Windows automatic update is disabled when the software for this product is installed.

If Windows automatic update is disabled, alerts are notified from the Windows Security Center and Action Center; accordingly, the procedure for disabling these alerts is described.

IMPORTANT

To enable Windows automatic update, Windows automatic update must be manually enabled after the software for this product is installed. In such a case, this setting is not required.

TIP

Windows Security Center and Action Center are client security monitoring services.

1. Sign in using the user account for which the alerts of Windows Security Center and Action Center are to be disabled.
2. Open Control Panel.
3. Set the display style of Control Panel to Small icons.
4. Select [Notification Area Icons] from the displayed items.
The Notification Area Icons window appears.

TIP

If the Action Center setting is grayed out, clear the [Always show all icons and notifications on the taskbar] check box. If the setting is still grayed out after clearing this check box, wait for a few minutes until it becomes active.

If the Action Center icon does not appear in the Notification Area Icons window, click [Turn system icons on or off] and, in the window that appears, turn on the setting for [Action Center]. If this setting is grayed out when the window appears, also wait for a few minutes until it becomes active.

5. For [Action Center], select [Hide icon and notifications] and click [OK].

TIP

On license-assigned stations, select [Show icon and notifications] for [LicenseAgent.TaskTray].

SEE ALSO

For more information about the procedure for manually enabling Windows automatic updates, refer to:

“■ Enabling Windows Update” on page C7-7

■ Display Properties

The procedure for setting the display properties is explained as follows.

1. Sign in using the user account for which to set display properties.
2. Open Control Panel.

3. Select [Hardware] > [Display] > [Change desktop background].
The Desktop Background window appears.
4. Set [Solid Colors] for Picture location, select the color of your choice, and then click [Save changes].
5. Select [Change screen saver].
The Screen Saver Settings dialog box appears.
6. Select [(None)] for Screen saver and click [OK].
7. In Control Panel, select [Hardware] > [Display] > [Adjust resolution].
The Screen Resolution window appears.
8. Set the resolution to 1024 x 768 and click [OK].
9. Click [Keep changes].

■ Display Scale

The procedure for setting the display scale is explained as follows.

1. Sign in using the user account for which to set display scale.
2. Open Control Panel.
3. Select [Hardware] > [Display].
The Display window appears.
4. Select the check box for [Let me choose one scaling level for all my displays], and select [Smaller - 100%].

B4.10.5 Configuring on Windows Server 2008 R2

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

■ Windows Security Center/Action Center Alerts

Windows Security Center and Action Center manage all functions required for security protection of the computer.

For computers on which software for this product is to be installed, it is recommended to disable Windows automatic update. Accordingly, Windows automatic update is disabled when the software for this product is installed.

If Windows automatic update is disabled, alerts are notified from the Windows Security Center and Action Center; accordingly, the procedure for disabling these alerts is described.

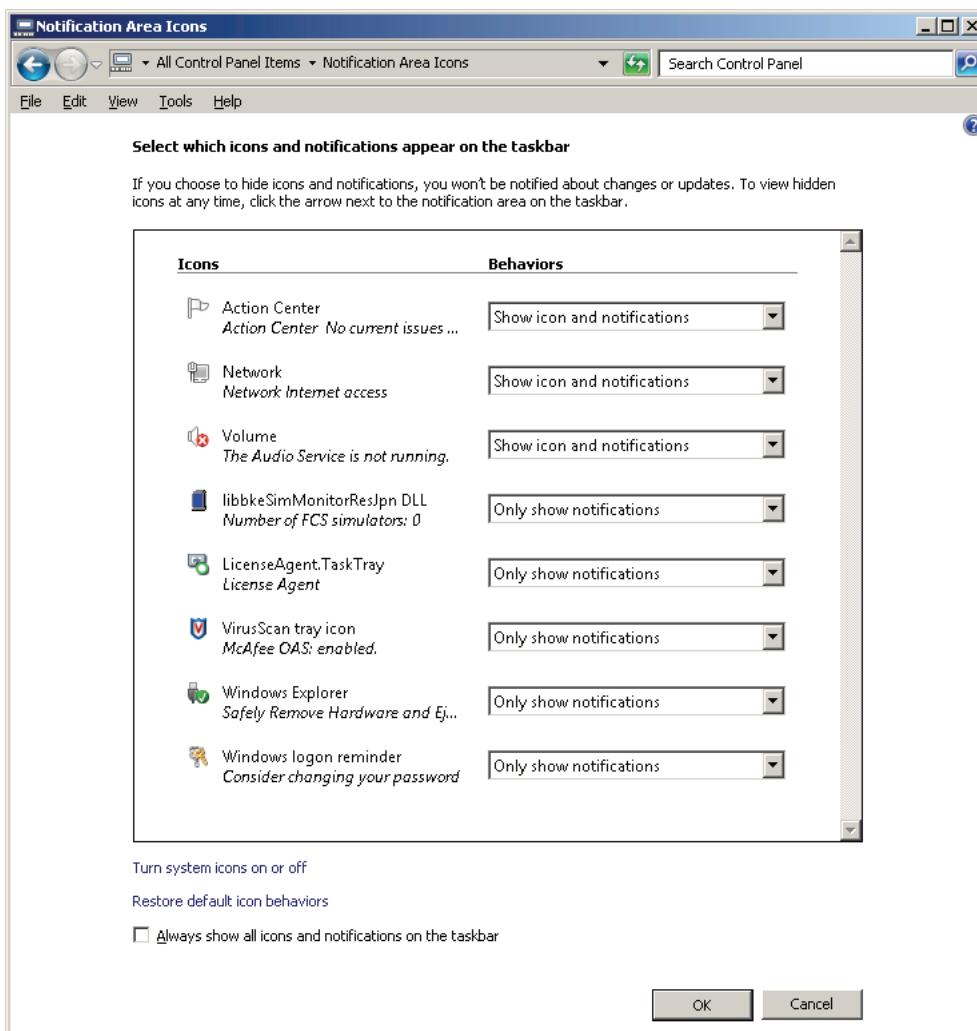
IMPORTANT

To enable Windows automatic update, Windows automatic update must be manually enabled after the software for this product is installed. In such a case, this setting is not required.

TIP

Windows Security Center and Action Center are client security monitoring services.

1. Log on using the user account for which the alerts of Windows Security Center and Action Center are to be disabled.
2. Open Control Panel.
3. Set the display style of Control Panel to Small icons.
4. From the items displayed in Control Panel, select [Notification Area Icons].
The Notification Area Icons window appears.

**Figure B4.10.5-1 Notification Area Icons Window****TIP**

If the Action Center setting is grayed out, clear the [Always show all icons and notifications on the taskbar] check box. If the setting is still grayed out after clearing this check box, wait for a few minutes until it becomes active.

If the Action Center icon does not appear in the Notification Area Icons window, click [Turn system icons on or off] and, in the window that appears, turn on the setting for [Action Center]. If this setting is grayed out when the window appears, also wait for a few minutes until it becomes active.

- For [Action Center], select [Hide icon and notifications] and click [OK].

TIP

On license-assigned stations, select [Show icon and notifications] for [LicenseAgent.TaskTray].

SEE ALSO

For more information about the procedure for manually enabling Windows automatic updates, refer to:

- "■ Enabling Windows Update" on page C7-7

■ Display Properties

The procedure for setting the display properties is explained as follows.

- Log on using the user account for which to set display properties.
- Open Control Panel.

3. Select [Hardware] > [Display] > [Change desktop background].
The Desktop Background window appears.

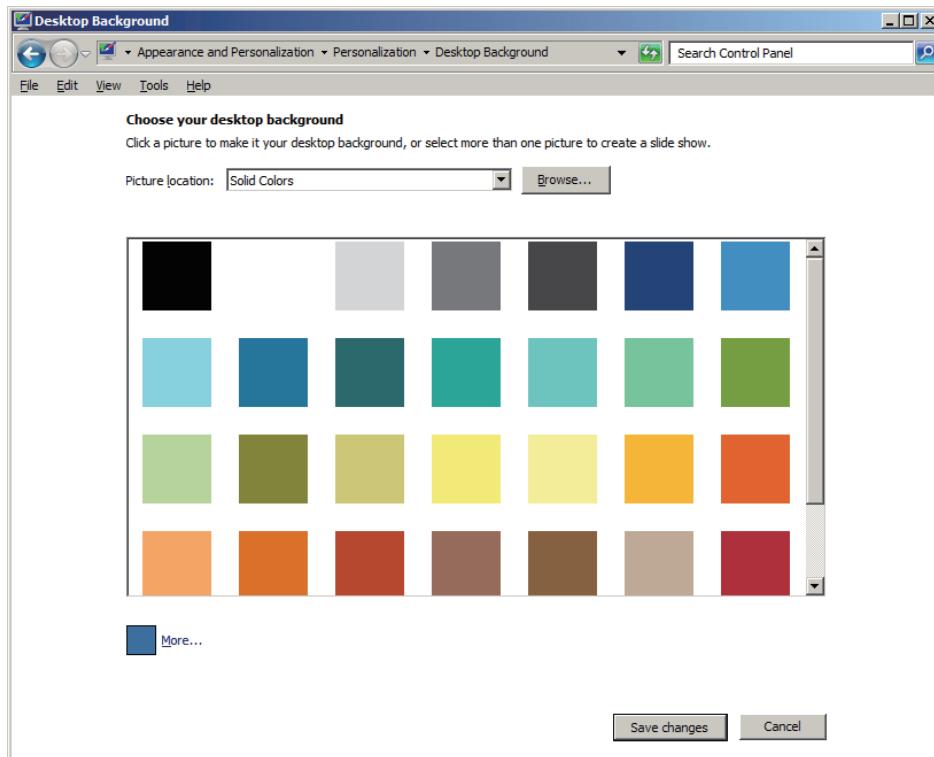


Figure B4.10.5-2 Desktop Background Window

4. Set [Solid Colors] for Picture location, select the color of your choice, and then click [Save changes].
5. Select [Screen Saver].
The Screen Saver Settings dialog box appears.

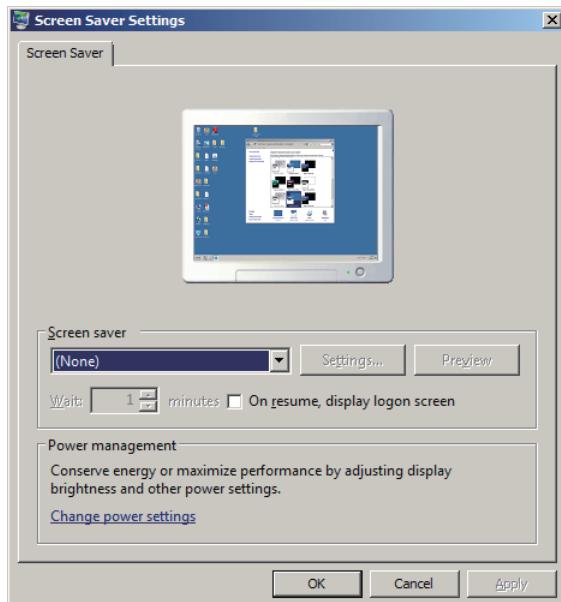


Figure B4.10.5-3 Screen Saver Settings Dialog Box

6. Select [(None)] for Screen saver and click [OK].
7. In Control Panel, select [Hardware] > [Display] > [Adjust resolution].
The Screen Resolution window appears.

8. Set the resolution to one of the following and click [OK].
 - Normal monitor: 1280 x 1024 or 1600 x 1200
 - Wide screen monitor: 1280 x 800, 1440 x 900, 1680 x 1050, 1920 x 1080, or 1920 x 1200
9. Click [Keep changes].
10. Select [Display] > [Adjust resolution] > [Advanced settings].
The Advanced Settings dialog box appears.

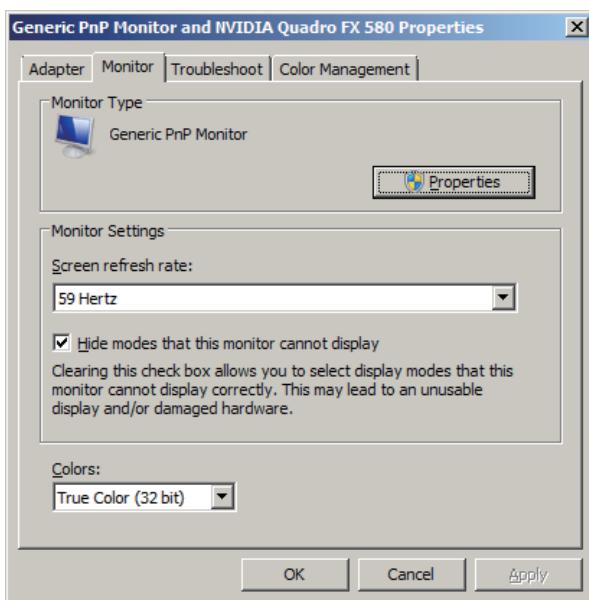


Figure B4.10.5-4 Advanced Settings Dialog Box

11. Select the [Monitor] tab, set [True Colors (32 bit)] for Colors and click [OK].

■ Display Scale

The procedure for setting the display scale is explained as follows.

1. Log on using the user account for which to set display scale.
2. Open Control Panel.
3. Select [Hardware] > [Display].
The Display window appears.

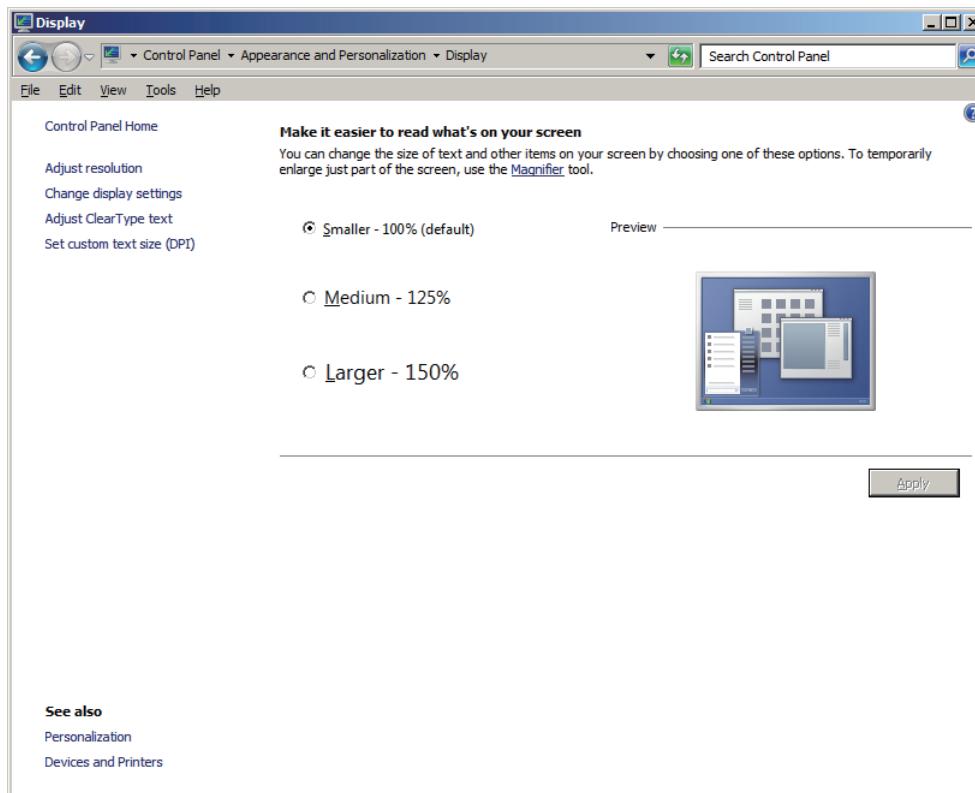


Figure B4.10.5-5 Display Window

4. Select [Smaller - 100%].

B4.11 Setting Up for User Authentication Modes

This section describes the setups for user authentication modes.

■ User Authentication Modes

When the Standard model is selected as the security model in IT security settings, the following two user authentication modes are available.

- CENTUM authentication mode
- Windows authentication mode

The default is CENTUM Authentication.

When the Legacy model is selected, the user authentication mode is fixed to CENTUM authentication.

Table B4.11-1 User Authentication-related Terms

Term	Description
Windows authentication mode	User authentication is performed using Windows standard functions.
CENTUM authentication mode	User authentication is performed using CENTUM's own method. This is the same as the user authentication of R4.02 and earlier.
HIS type single sign on	A user sign on type that is available when Windows authentication mode is selected. The user-in dialog box of HIS is used to sign on.
Windows type single sign on	A user sign on type that is available when Windows authentication mode is selected. The logon dialog box of Windows is used to sign on.
HIS group users	Users that are handled on the Security Builder and log on to/log off from the operation and monitoring functions on HIS.
ENG group users	The following users are collectively called "ENG group users" when the access control package or the FDA 21 CFR Part 11-compliant package is activated <ul style="list-style-type: none"> • System engineers who use the system builders • Recipe engineers who use the recipe builders • Users who use the reporting functions
ENG group users builders	The following builders are collectively called the "ENG group users builders" when the access control package or the FDA 21 CFR Part 11-compliant package is activated. <ul style="list-style-type: none"> • Builder for registering the system engineers • Builder for registering the recipe engineers • Builder for registering users who use the reporting functions

SEE ALSO

For more information about user authentication mode, refer to:

- 4.1, "Items to be Considered before Setting Security Functions" in CENTUM VP Security Guide (IM 33J01C30-01EN)
- 1.1, "How to Start and End HIS" in Human Interface Stations Reference Vol.1 (IM 33J05A10-01EN)

● User Management Type and Passwords

Ensure that the user management type and passwords are unified on all computers.

Pay attention to the followings:

- If a project includes computers installed with R4.02 or earlier version software:
The authentication mode of the project should be CENTUM Authentication.

TIP

A computer installed with R4.02 or earlier version software denotes the computer installed with any of the following software packages:

- Standard Operation and Monitoring Function (LHS1100/LHM1101) and optional packages that are used with this package
- Standard Builder Function (LHS5100/LHM5100) and optional packages that are used with this package
- Remote Operation and Monitoring Function (LHS1150/LHM1150)
- Report Package (LHS6530)
- CS Batch 3000 Builder Package (LHS5160)
- CS Batch 3000 Recipe Management Package (LHS5161)
- CCS Batch 3000 Process Management Package (LHS6600/LHM6600)
- Access Control Package (LHS5110)
- Access Administrator Package (FDA:21 CFR Part 11 compliant) (LHS5170)

-
- If the CENTUM with Windows authentication mode and R3.60 or earlier version Exaopc are mixed in a system:

After changing the management of the passwords for CENTUM authentication to individual management, change the authentication mode to Windows Authentication.

The passwords defined for CENTUM authentication are intact.

If a new user is added, the authentication will not check the user password.

On the computer where the project files to be referenced by Exaopc R3.60 exist, create the OPC_PROCESS user by using the CreateOPCProcess tool and register the user to the CTM_OPCT group.

- When Windows authentication mode is used:

Either Windows Domain/Combination management or Standalone management can be used but needs to be unified.

One project should not be utilized with more than one Windows domain. However, one Windows domain may be utilized with multiple projects. (Windows domain : projects = 1 : N)

B4.11.1 Setting CENTUM Authentication Mode

This section describes the settings in the CENTUM authentication mode.

■ Setup Procedure

When the Standard model is selected as the security model in IT security settings, the default authentication mode is CENTUM Authentication.

When the project is produced after the setup, confirm that the check box for [Use Windows user names as HIS user names] on the property dialog of the project is not selected.

Also, confirm that the check box for [Use Windows user names as HIS user names] on the Access Control tab of the Access Control Utility is not selected.

**SEE
ALSO**

For more information about registering HIS group users, refer to:

“● User Authentication” in “■ Project Name and Position” in 2.2, “Creating a New Project” in Engineering Reference Vol.1 (IM 33J10D10-01EN)

For more information about registering ENG group users, refer to:

4.3, “Engineers’ Account Builder” in Compliance with FDA: 21CFR Part 11 (IM 33J10D21-01EN)

■ Setting to Automatically Start the Operation and Monitoring Function

To automatically start the operation and monitoring function when a user logs on to Windows in CENTUM authentication mode, configure the following settings with the HIS Utility. The operation and monitoring function cannot be automatically started when the computer is not connected to the control bus.

1. Logon as an administrative user.
2. Start HIS Utility.
3. Select the [User] tab and click [Setting].
The User Environment Settings dialog box appears.
4. Click [Add].
The Add Users dialog box appears.

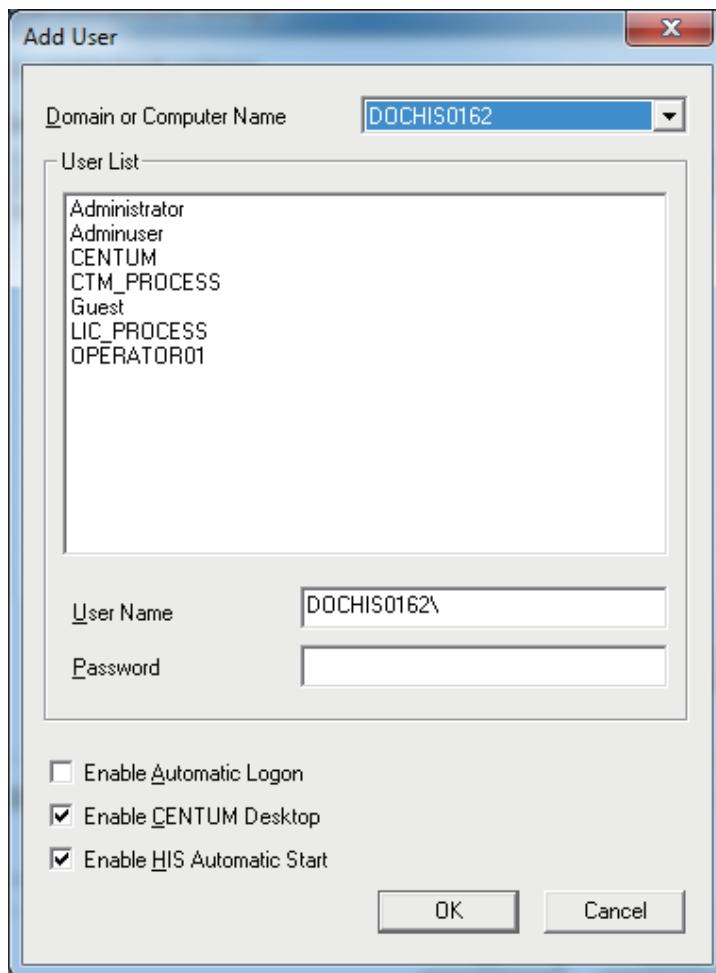


Figure B4.11.1-1 Add Users Dialog Box

5. From the Domain and Computer Name drop-down list, select a Windows domain name or the local computer name.
6. Select the target user and enter the password.
7. Select the [Enable HIS Automatic Start] check box and click [OK].

TIP

After clicking [OK], a warning message appears, informing you that it may take time to finish if you have added a user who has not ever been logged on.

8. Repeat steps 5 to 7 if you have any other users for whom to enable automatic starting of the operation and monitoring function at logon.
9. Click [OK] and end the HIS Utility.

B4.11.2 Setting Windows Authentication Mode

This section describes the settings related to Windows authentication mode.

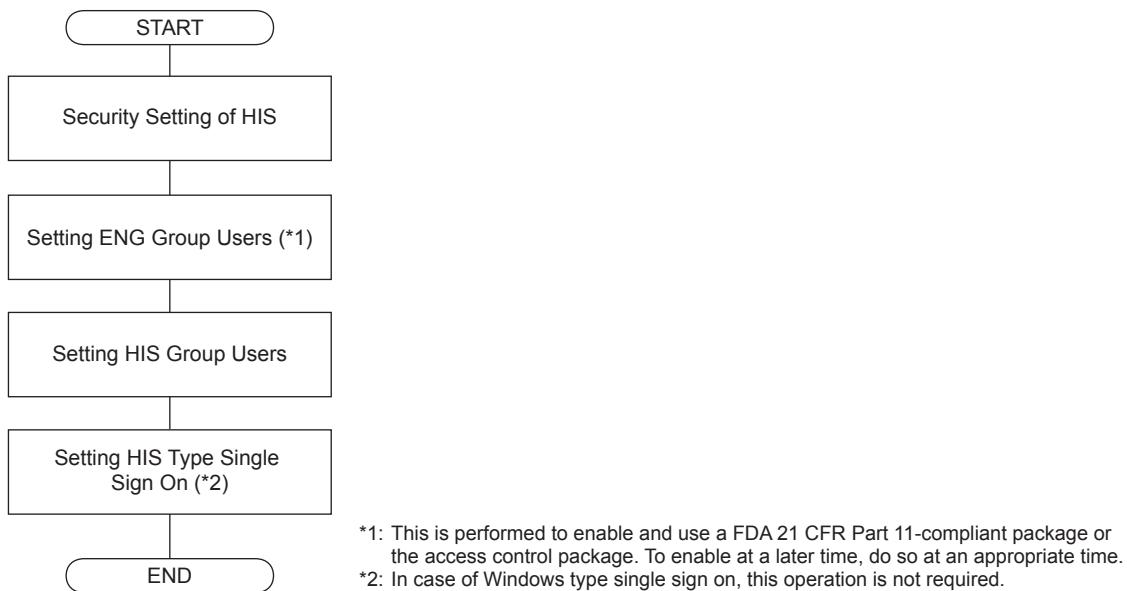


Figure B4.11.2-1 Workflow

TIP

In the case of HIS type single sign on, users' access rights to programs registered in the Start menu are the same as those granted to the OFFUSER. The rights remain the same even after user-in.

In the case of Windows type single sign on, users' access rights to the Start menu programs are according to the rights granted to the logged on user.

SEE ALSO

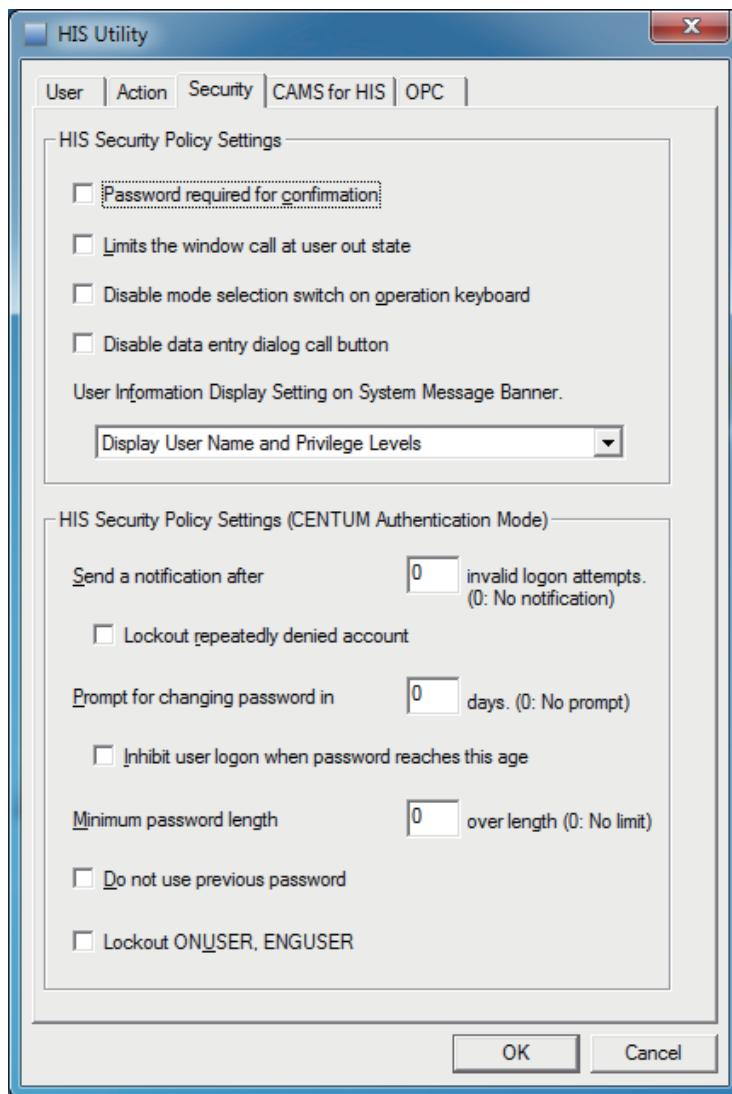
For more information about permissions to use the Start Menu, refer to:

“■ Access Permissions for Programs” in 3.1.1, “Access Permissions to Files and Folders” in CENTUM VP Security Guide (IM 33J01C30-01EN)

■ Security Setting of HIS

Configure the setting on each computer when the standard operation and monitoring function is enabled.

1. Log on using the account of a CTM_MAINTENANCE group user.
2. Start HIS Utility.

**Figure B4.11.2-2 Security Tab**

3. Based on the security policy set for HIS operations, configure the following check box settings on the Security tab.
 - [Password required for confirmation] check box
 - [Limit the window call in user out state] check box
 - [Disable mode selection switch on operation keyboard] check box
 - [Disable data entry dialog call button] check box

TIP

By the default settings of Windows authentication mode, when OFFUSER is logged on, calling windows is not permitted. In order to get permission to call windows, clear the option box of [Limits the window call at user out state].

SEE ALSO

For more information about the above mentioned check boxes, refer to:

3.1, "User" in Engineering Reference Vol.1 (IM 33J10D10-01EN)

■ Set Up ENG Group Users

Set up ENG group users.

● Setting User Environment

Perform this operation on the computers on which one or more of the standard builder function, recipe management package, or report package, as well as the FDA 21 CFR Part 11-compliant package or access control package, are activated.

1. Logon as a user of the CTM_MAINTENANCE or CTM_ENGINEER_ADM group.
2. Start Access Control Utility.
The Setting Target Selection dialog box appears, prompting you to select the target for audit trail management and access control.

TIP

If the standard builder function, recipe management package, and report package are simultaneously enabled on a computer, you can configure separate settings for the audit trail management and access control in this dialog box. This dialog box will not appear if only one of the standard builder function, recipe management package, or report package is enabled. The Access Control Utility for the package that is enabled will start.

3. To start the Access Control Utility for the system engineering builders, select [Engineering Function]. To start it for the recipe management function or reporting function, select [Recipe Function] or [Report Function], respectively.
4. Click [OK].
The Access Control Utility starts.
5. Click [Settings] on the General tab.
The User Environment Settings dialog box appears.
6. Configure the following settings for each of the ENG group users as necessary.
 - When the standard operation and monitoring function is not installed on the same computer: Automatic Logon and CENTUM Desktop settings

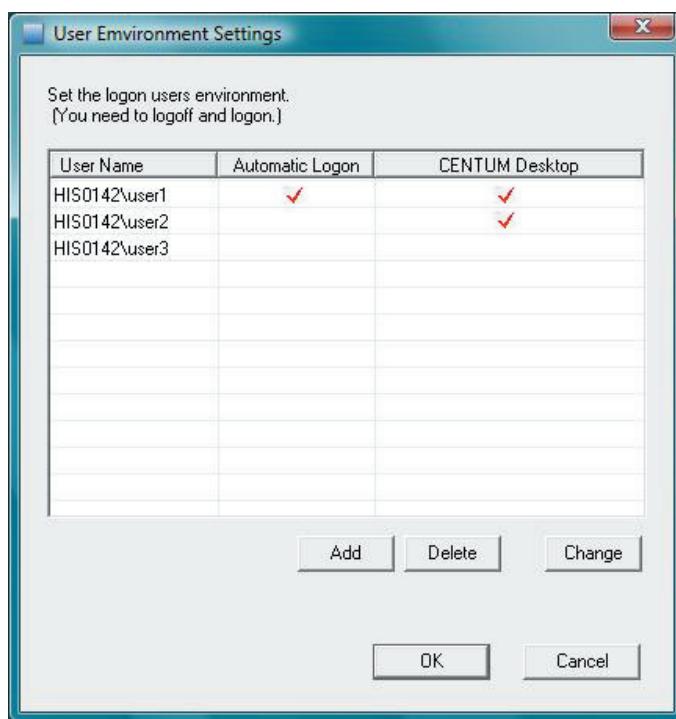


Figure B4.11.2-3 User Environment Setting Dialog Box (Example when Standard Operation and Monitoring Function is Not Installed)

- When the standard operation and monitoring function is installed on the same computer: Automatic Logon, CENTUM Desktop, and HIS Start settings

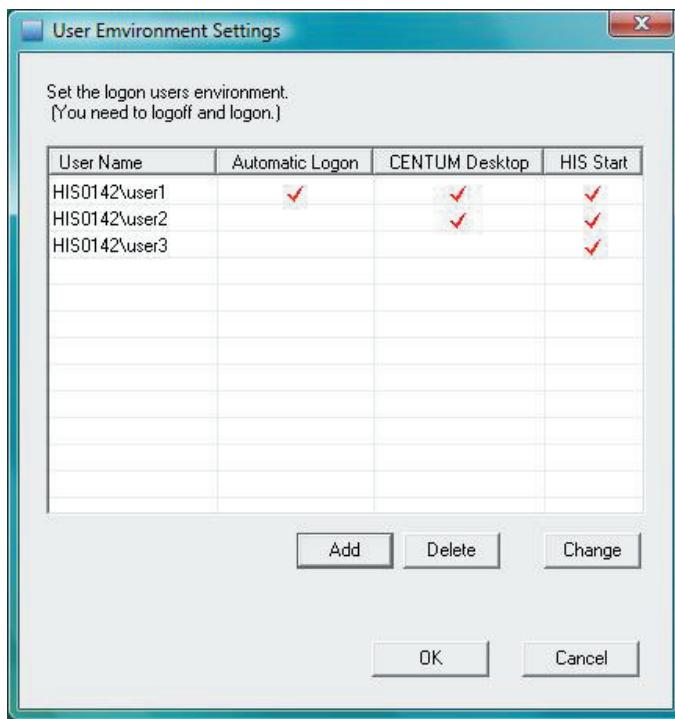


Figure B4.11.2-4 User Environment Setting Dialog Box (Example when Standard Operation and Monitoring Function is Installed)

TIP

For the HIS group users, when Windows authentication mode is selected, the following dialog box is displayed. There are two setting columns of CENTUM Desktop and HIS Start.

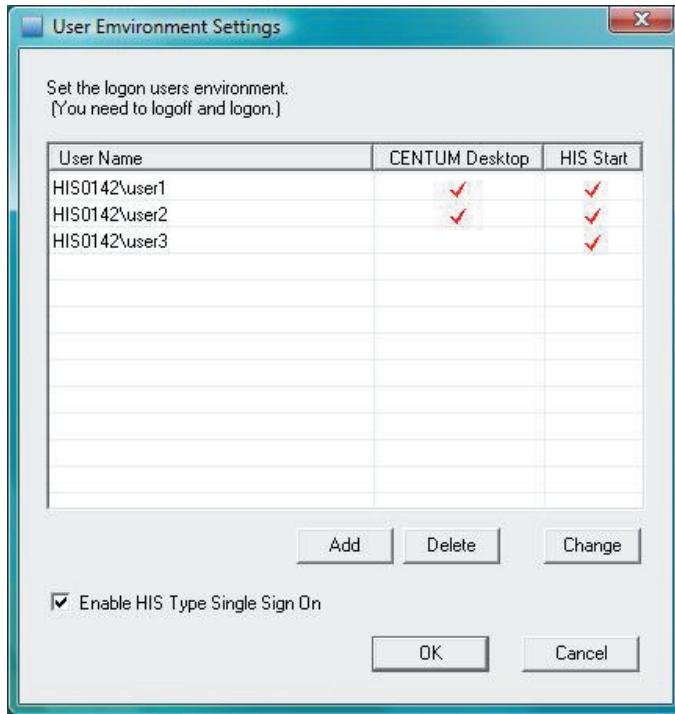


Figure B4.11.2-5 User Environment Setting Dialog Box

SEE ALSO

For more information about the Enable HIS Type Single Sign On check box, refer to:

“■ Setting HIS Type Single Sign On” on page B4-145

● Setting Windows Authentication Mode to Authenticate ENG Group Users

Perform the following procedure on the computer used for ENG group user management.

1. Display the Access Control tab of the Access Control Utility.
2. Select the check box according to the target you have selected.
 - If you selected [Engineering Function] in the Setting Target Selection dialog box, select the check box for [Use Windows user names as system engineer user names].
 - If you selected [Recipe Function], select the check box for [Use Windows user names as recipe user names].
 - If you selected [Report Function], select the check box for [Use Windows user names as report user names].

● Registering ENG Group Users

Perform the following procedure on the computer used for ENG group user management.

If you selected [Report Function] in the Setting Target Selection dialog box, take the terms “Engineers’ account file,” “Engineers’ account builder,” and “Engineer name” that appear in the following description for “Users’ account file,” “Users’ account builder,” and “User name,” respectively.

1. To create a new engineers’ account file, clear the [Choose an existing file] check box.
2. In the [Refer to:] box, specify the folder in which the created engineers’ account file is to be saved and click [OK] or [Apply].
The default engineers’ account file is created.
3. Click [Edit...] to start the Engineers’ account builder.
4. Select the [Valid Account] tab.
5. Set up the engineer names and engineering group.
6. Save the settings and end the Engineers’ account builder.
7. Click [OK] on the Access Control Utility.

SEE ALSO

For more information about the Engineers’ account builder, refer to:

4.3, “Engineers’ Account Builder” in Compliance with FDA: 21CFR Part 11 (IM 33J10D21-01EN)

■ Set Up HIS Group Users

Set up HIS group users.

● Setting User Environment

Perform this setting on the computers on which the standard operation and monitoring function is activated.

Use the HIS Utility to set the user environment for each HIS group user as necessary.

1. Logon as a user of the CTM_MAINTENANCE group.
2. Start HIS Utility.
3. On the User tab, click [Setting].
User Environment Settings dialog box appears.

**SEE
ALSO**

For more information about setting user environment, refer to:

- “● Setting User Environment” on page B4-141

● Creating a New Project

The following operations need to be performed on the computer used for creating and configuring project. System View is used for creating the new project.

1. Logon as a user of CTM_MAINTENANCE or CTM_ENGINEER_ADM group.
2. Start System View.
3. And then create a new project.

TIP

Projects can be created by a user who belongs to the CTM_ENGINEER group. Since the user authentication mode is set to Windows authentication mode later, however, log on using an account of the user who belongs to the CTM_MAINTENANCE or CTM_ENGINEER_ADM group here.

**SEE
ALSO**

For more information about using System View, refer to:

- A1.5, “Operating System View” in Engineering Tutorial (IM 33J10D20-01EN)

● Configuring Project

The following operations need to be performed on the computer used for creating and configuring project. Various engineering builders are used for configuring the project.

**SEE
ALSO**

For more information about using various engineering builders, refer to:

- A2., “Engineering for a New System” in Engineering Tutorial (IM 33J10D20-01EN)

● Setting Windows Authentication Mode to Authenticate HIS Group Users

The following operations need to be performed on the computer used for creating and configuring project.

1. If you have logged on the computer as a user of the CTM_ENGINEER group to create and configure a project, you need to log off first and then logon as a user of the CTM_MAINTENANCE or CTM_ENGINEER_ADM group.
2. Choose a project and open its properties dialog box.

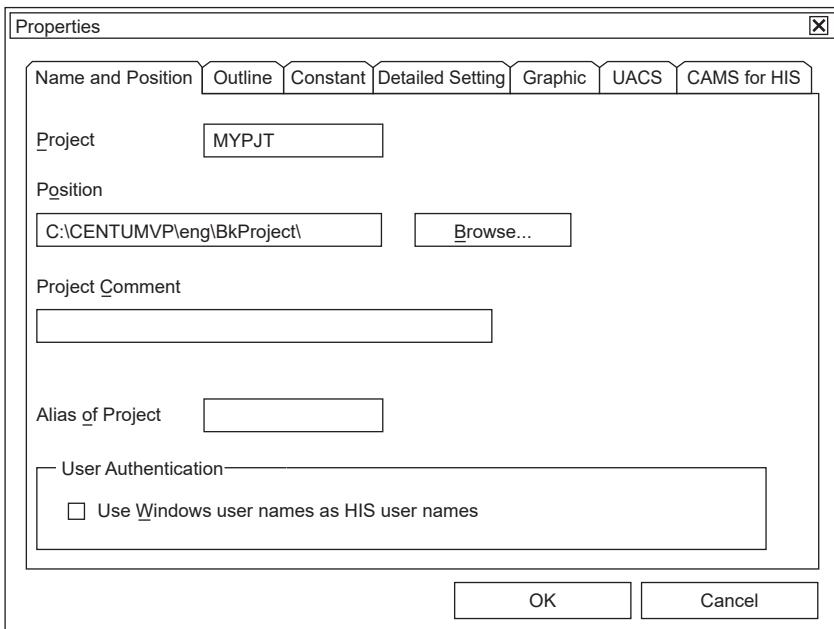


Figure B4.11.2-6 Project's Properties Dialog Box

3. Select the [Name and Position] tab.
4. Select the [Use Windows user names as HIS user names] check box.

● Registering HIS Group Users

The following operations need to be performed on the computer used for creating and configuring project.

1. Start the Security builder.
2. Select the [Valid User] tab.
3. Enter a user name.
4. Download the project common section.

SEE ALSO

For more information about the security builder, refer to:

3., “Security Policy” in Engineering Reference Vol.1 (IM 33J10D10-01EN)

● Restarting the HIS

If the project common section has not been downloaded after you created and built a project, and changed the user authentication mode on the computers on which the standard operation and monitoring function is installed, download the project common section in System View.

And then restart HIS.

■ Setting HIS Type Single Sign On

Configure these settings to use the HIS type single sign on function on the computers where the standard operation and monitoring function is enabled.

● Setting a Password for OFFUSER

Perform this procedure on the computer where HIS type single sign on is to be used.

1. Log on the computer using an administrative user account.

2. Use Windows Explorer to open the following folder. If the program is in C: driver, the location is:
C:\Program Files (x86)\YOKOGAWA\IA\iPCS\Platform\SECURITY\PROGRAM
3. Double-click Yokogawa.IA.iPCS.Platform.Security.OFFUSEREnabler.exe to run it.
The password “!centumvp123” is set for the OFFUSER.

TIP

The OFFUSER created by IT Security Tool has a default but disclosed password. The above procedure is for temporarily changing the password of the OFFUSER account in Windows environment.

● Setting Windows Operating Environment for OFFUSER

Perform this procedure on the computer where HIS type single sign on is to be used.

- Log on to Windows using the OFFUSER account, and configure Windows environment settings.
The password for OFFUSER account is “!centumvp123.”

TIP

OFFUSER is the Windows user account that is used for HIS type single sign on.

SEE ALSO

For more information about the setting of Windows operating environment, refer to:

B4.10, “Configuring Windows Environment Settings for Each User” on page B4-107

● Initializing the Password of OFFUSER

Perform this procedure on the computer where HIS type single sign on is to be used.

1. Log on the computer using an administrative user account.
2. Use Windows Explorer to open the following folder. If the program is in C: driver, the location is:
C:\Program Files (x86)\YOKOGAWA\IA\iPCS\Platform\SECURITY\PROGRAM
3. Double-click Yokogawa.IA.iPCS.Platform.Security.OFFUSERDisabler.exe to run it.
The password of OFFUSER is initialized.

TIP

For security purposes, OFFUSER's password is changed back to the secret initial password here.

● Enabling HIS Type Single Sign On

Perform this procedure on the computer where HIS type single sign on is to be used.

1. Log on as an administrative user.
2. Start HIS Utility.
3. Select the [User] tab and click [Setting].
User Environment Settings dialog box appears.
4. Select the [Enable HIS Type Single Sign On] check box.

● Changing the OFFUSER's Rights

On the computer used for creating and configuring projects, perform this procedure if you want to change the OFFUSER's rights from the default rights.

1. Use an administrative user account to logon.
2. Start the Security Builder.
3. Select the [Valid User] tab.

4. Edit the OFFUSER's rights.
5. On System View, run [Download Project Common Section].

B4.11.3 Notes for User Authentication Mode

This section describes the cautionary notes on using the user authentication mode.

■ Notes on Connecting Multiple Projects in Windows Authentication Mode

When the system is set up for HIS type single sign on in Windows authentication mode, you need to do the following setup to connect with other projects by using the multiple project connection function.

- **When Connecting with a CENTUM VP R4.03 or earlier Project with Standard Model of Security Settings**

Perform the following steps for the project to connect with.

1. Run the following program provided in the CENTUM VP software medium to create OFF-USER.
\\CENTUM\\SECURITY\\Yokogawa.IA.iPCS.Platform.Security.CreateOffuser.exe
2. In the access permissions setting for the project database folder, add the OFFUSER.

■ Notes on CENTUM Data Access Library in Windows Authentication Mode

When the system is set up for HIS type single sign on in Windows authentication mode, you need to do the following setup to access the other project on connecting multiple projects with CENTUM Data Access Library.

- **When Connecting with a CENTUM VP Project with Standard Model of Security Settings**

Perform the following steps for the project to connect with.

1. Run the following program provided in the CENTUM VP software medium to create OFF-USER. (Only when connecting with a CENTUM VP R4.03 or earlier)
\\CENTUM\\SECURITY\\Yokogawa.IA.iPCS.Platform.Security.CreateOffuser.exe
2. Do the following settings.
 - For Standalone management: Add OFFUSER to the CTM_OPC group.
 - For Domain/Combination management: Add OFFUSER to the CTM_OPC_LCL group.

B4.12 Setting Up the Uninterruptible Power Supply (UPS) Service

In order to protect data in the computer at power supply failures, you can connect an uninterruptible power supply (hereinafter referred to as UPS) to the computer and install software to configure the UPS in various ways.

On the computer running CENTUM VP software, the UPS management software can be used. The CENTUM VP standard packages do not have UPS management software; you need to use the proper software for the selected UPS.

CENTUM VP includes the following commands to be used with the UPS management software. The commands are used to alert computer power failure in a system alarm message and safely stop the software.

- System alarm message output command
- Software shutdown command

Using CENTUM VP standard package and UPS management software can have the following actions:

Table B4.12-1 Actions of Using CENTUM VP Standard Package and UPS management software

Phenomenon	Windows standard UPS management software	Third party software (such as POWERCHUTE plus)
switch-over to the battery due to power failure	No function	Outputs System Alarm Message "AC Fail"
Power recovery	No function	Outputs System Alarm Message "AC Recover"
System shutdown	Output System Alarm Message output "AC Fail Shutdown"	
System shutdown	Operation and monitoring function shutdown	
When the battery needs to be replaced	No function	Outputs System Alarm Message Output "UPS Diagnose Error"

■ Basic Idea about the Setup

The basic idea regarding UPS actions during power failure is shown as follows.

This idea, however, does not necessarily apply to all systems. Change the operations and set times of the software based on the power supply conditions and policies. Some functions cannot be used with some management software programs.

- A short-time power failure (transient power failure) should not trigger the computer shutdown, the UPS battery backup should be continuously applied.

TIP

UPS battery backup should be continued for about a minute.

To notify the computer user of the power failure, the UPS management software triggers the BKHHisAcFail.exe program. As a result, a system message "AC Fail" is generated.

- If the duration of a power failure exceeds the operating duration of the UPS battery, execute the "BKHAcFailShut.exe" command on the UPS management software. The operation and monitoring function can then be normally shutdown, preventing data from being destroyed. At this time, a system message, "AC Fail Shutdown Execute," will be generated.
- A few minutes after the operation and monitoring function is shut down in Step 2, shut down Windows via the UPS management software. By delaying to shut down Windows, you can gain time to terminate system engineering builders and applications normally.

- A few minutes after shutting down Windows, the secondary power supply of UPS will be shutdown by the UPS management software.
- Execute the “BkHHisAcRecover.exe” command on the UPS upon power recovery. A system message, “AC Recover,” will be generated as a result.

TIP

By executing “BKHUpsChk.exe” in an event such as an alert for battery replacement on the UPS side, you can generate the “UPS Diagnose Error” system alarm. This alarm will alert the user to check the UPS log file. Accordingly, if the log is maintained on the UPS management software side, it will be useful for analysis in the event of a power failure.

- **Command provided by HIS standard function**

Table B4.12-2 BKHHisAcFail.exe

Path	<CENTUM VP installation folder>\his\tool\BKHHisAcFail.exe
Argument	None
Function	Outputs the System alarm message “AC Fail”

Table B4.12-3 BkHHisAcRecover.exe

Path	<CENTUM VP installation folder>\his\tool\BkHHisAcRecover.exe
Argument	None
Function	Outputs the System alarm message “AC Recover”

Table B4.12-4 BKHAcFailShut.exe

Path	<CENTUM VP installation folder>\his\tool\BKHAcFailShut.exe
Argument	None
Function	Shuts down the operation and monitoring function after outputting the System alarm message “AC Fail Shutdown”

Table B4.12-5 BKHHisStop.exe

Path	<CENTUM VP installation folder>\his\tool\BKHHisStop.exe
Argument	None
Function	Shuts down the operation and monitoring function

Table B4.12-6 BKHUpsChk.exe

Path	<CENTUM VP installation folder>\his\tool\BKHUpsChk.exe
Argument	None
Function	Outputs the System alarm message “UPS Diagnose Error”

- **Command provided by APCS/GSGW standard function**

Table B4.12-7 BKFApcsaCFail.exe

Path	<CENTUM VP installation folder>\Fcs\tool\ BKFApcsaCFail.exe
Argument	None
Function	Outputs the System alarm message “AC Fail”

Table B4.12-8 BKFApcsaCRecover.exe

Path	<CENTUM VP installation folder>\Fcs\tool\ BKFApcsaCRecover.exe
------	--

Continues on the next page

Table B4.12-8 BKFApcsAcRecover.exe (Table continued)

Argument	None
Function	Outputs the System alarm message “AC Recover”

Table B4.12-9 BKFApcsAcFailShut.exe

Path	<CENTUM VP installation folder>\Fcs\tool\ BKFApcsAcFailShut.exe
Argument	None
Function	Shuts down the APCS/GSGW control function after outputting the System alarm message “AC Fail Shutdown”

- **Command provided by SIOS/UGS standard function**

Table B4.12-10 BKVUpsAcFail.exe

Path	<CENTUM VP installation folder>\Eng\tool\BKVUpsAcFail.exe
Argument	None
Function	Outputs the System alarm message “AC Fail”

Table B4.12-11 BKVUpsAcRecover.exe

Path	<CENTUM VP installation folder>\Eng\tool\BKVUpsAcRecover.exe
Argument	None
Function	Outputs the System alarm message “AC Recover”

Table B4.12-12 BKVUpsDiagErr.exe

Path	<CENTUM VP installation folder>\Eng\tool\BKVUpsDiagErr.exe
Argument	None
Function	Outputs the System alarm message “UPS Diagnose Error”

Blank Page

B5. Setting Up the Remote Operation and Monitoring Function

The server for remote operation and monitoring function enables you to use the operation and monitoring function of CENTUM VP even from computers on the intranet that are not installed with CENTUM VP through access to the server computer installed with CENTUM VP.

The remote operation and monitoring function uses the remote desktop service of Windows.

The remote operation and monitoring function that runs on Windows Server's remote desktop service is also referred to as HIS-TSE.

SEE ALSO

For more information about the settings of the remote desktop services, refer to:

Instruction manuals of Microsoft Windows

For more information about Server for Remote Operation and Monitoring Function, refer to:

7., "Server for Remote Operation and Monitoring Function" in Optional Functions Reference (IM 33J05H10-01EN)

■ Item to be Prepared

Have the following item at hand before you set up a file server.

- CENTUM VP software medium

■ Administrative User who Performs the Installation

The CENTUM VP software must be installed by an administrative user shown in the following table.

The user who has installed the software is automatically added to the CTM_MAINTENANCE group.

Table B5-1 Administrative User Who Performs New Installation

Security model and user management type to be applied		
Legacy model	Standard model	
	Standalone management	Domain/Combination management
Local user who belongs to the Administrators local group	Local user who belongs to the Administrators local group	<ul style="list-style-type: none"> • Domain user who belongs to the Domain Admins domain group • Domain user who belongs to the Administrators local group • Local user belonging to the Administrators local group (*1)

*1: The domain user name and password must be entered during installation.

TIP

If the user management type is Domain or Combination management, install the software after the computer is added to the domain.

■ Restrictions on Package Coexistence

If the licenses of the packages that cannot coexist with the Server for Remote Operation and Monitoring Function are distributed to the HIS-TSE server computer, errors will occur.

Table B5-2 Package Coexistence in HIS-TSE Server

Package Code	Description	Coexistence	Remarks
VP6H1100	Standard Operation and Monitoring Function	Yes	
VP6H1120	Console HIS Support Package for Enclosed Display Style	No	
VP6H1130	Console HIS Support Package for Open Display Style	No	
VP6H2411	Exaopc OPC Interface Package (for HIS)	Yes	The functions of the OPC server are different from those of the standard HIS. The operation check of the application program under the TSE environment is required.
VP6H2412	CENTUM Data Access Library	Yes	The actions need to be confirm in each created application.
VP6H4000	Million Tag Handling Package	Yes	
VP6H4100	Configured Information Reference Package	Yes	
VP6H4150	Output to External Recorder Package	No	
VP6H4190	Line Printer Support Package	No	
VP6H4200	Historical Message Integration Package (meeting FDA Regulations)	No	
VP6H4410	Control Drawing Status Display Package	Yes	
VP6H4420	Logic Chart Status Display Package	Yes	
VP6H4450	Multiple Project Connection Package	Yes	
VP6H4600	Multiple-monitor Support Package	No	
VP6H4700	Advanced Alarm Filter Package	No	
VP6H6510	Long-Term Data Archive Package	Yes	
VP6H6530	Report Package	No	A remote operation environment can be constructed by installing the Report Package on the client computer.
VP6H6660	Process Management Package	Yes	Please define the server for remote operation and monitoring as a client station in the process management configuration definition.
VP6H6710	FCS Data Setting / Acquisition Package (PI-COT)	No	
VP6E5000	Engineering Server Function	Yes	One session only.
VP6E5100	Standard Engineering Function	Yes	One session only.
VP6E5110	Access Control Package	Yes	One session only.
VP6E5150	Graphic Builder	Yes	One session only.
VP6E5165	Batch Builder	Yes	One session only.
VP6E5166	Recipe Management Package	Yes	One session only.
VP6E5170	Access Administrator Package (FDA:21 CFR Part 11 compliant)	Yes	One session only.
VP6E5210	Module-based Engineering Function	Yes	One session only.
VP6E5215	Tuning Parameter Management Package (for Module-based Engineering)	Yes	One session only.
VP6E5216	Bulk Editing Package (for Module-based Engineering)	Yes	One session only.

Continues on the next page

Table B5-2 Package Coexistence in HIS-TSE Server (Table continued)

Package Code	Description	Coexistence	Remarks
VP6E5250	Change Management Package	Yes	One session only.
VP6E5260	Dependency Analysis Package	Yes	One session only.
VP6E5420	Test Function	No	
VP6E5425	Expanded Test Functions	No	
VP6E5426	FCS Simulator Package	No	
VP6E5427	HIS Simulator Package	No	
VP6A2505	UACS Simulator Package	No	
VP6E5450	Multiple Project Connection Builder	Yes	One session only.
VP6E5490	Self-Documentation Package	Yes	One session only.
VP6C5495	Electronic Instruction Manual	Yes	Up to two instances per session. Up to eight instances per computer.
VP6P6920	SOE Viewer Package	Yes	

■ Note on Setting Up the Remote Operation and Monitoring Function

Take note of the following precautions before you start the setup of the remote operation and monitoring function.

- **Server Manager Errors**

When you start the Server Manager after you set up the remote operation and monitoring function, errors may be displayed on the Server Manager.



Figure B5-1 Server Manager Errors Dialog Box

SEE ALSO

For more information about the action to be taken when a Server Manager error occurs, refer to:

C10.1.2, "Error Occurs when Server Manager is Started" on page C10-4

B5.1 Setting Up the HIS-TSE Server

To use the server for remote operation and monitoring function, you need to set up both HIS-TSE clients and the HIS-TSE server. This section describes how to set up the HIS-TSE server.

A batch file is provided for HIS-TSE server configuration. You must observe the following precautions regarding usage of the batch file:

- If the IT security has been configured to apply software restriction policies, right-click Command Prompt (cmd.exe) from the Start menu and select [Run As Administrator]. Then, be sure to run the batch files in the Command Prompt that is opened.
- If the HIS-TSE function is implemented in a domain environment, you must log on as Administrator of the domain to run the batch file.

B5.1.1 Configuring on Windows Server 2016

Follow these steps when you use a Windows Server 2016 computer:

■ Procedure 1: Set Up the Hardware

Set up the hardware of the HIS-TSE server computer.

SEE ALSO For more information about hardware setup , refer to:

B4.1, “Setting Up the Hardware” on page B4-2

■ Procedure 2: Set Up Windows

Before you install the CENTUM VP software on the computer, configure Windows settings.

TIP Set the same virtual memory size as the size that was set when setting up the HIS.

SEE ALSO For more information about the procedures for setting up Windows, refer to:

B4.2.3, “Configuring on Windows Server 2016” on page B4-24

■ Procedure 3: Configure Network Settings

The control bus driver needs to be installed for running the CENTUM VP software. If Vnet/IP is used, the Vnet/IP open communication driver also needs to be installed.

In this step, 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.

SEE ALSO For more information about the procedures for network setting, refer to:

B4.3, “Configuring Network Settings” on page B4-43

■ Procedure 4: Install Remote Desktop Service

Follow these steps to install the Remote Desktop Service.

1. Sign in to the server computer using the Administrator account.
2. Insert the CENTUM VP installation medium into the drive.
3. Use Windows Explorer to open the following folder in the CENTUM VP installation medium.
<Drive of CENTUM VP software medium>:\CENTUM\HIS\TSE
4. Right-click “1-InstallFeature.bat” and select [Run As Administrator].
When the installation of the Remote Desktop Service is complete, the server computer restarts.

■ Procedure 5: Install License Server

Follow these steps to install a license server and configure the authentication method for Remote Desktop Session Host, Remote Desktop licensing mode, and the discovery scope for Remote Desktop licensing:

TIP

- The settings of the Configure Client Experience page are automatically set as follows:
 - [Audio and video playback]: Enable
 - [Audio recording redirection]: Enable
 - [Desktop composition (provides the user interface elements of Windows Aero)]: Disable
- If there are multiple remote desktop servers in the system and the license server is running on Windows Server 2016 as with the remote desktop server, Remote Desktop licenses can be shared.

1. Sign in to the server computer using the Administrator account.
2. Insert the CENTUM VP installation medium into the drive.
3. Use Windows Explorer to open the following folder in the CENTUM VP installation medium.
<Drive of CENTUM VP software medium>:\CENTUM\HIS\TSE
4. Right-click “2-InstallLicense.bat” and select [Run As Administrator].
5. Input for User Authentication: sets the authentication method for Remote Desktop Session Host. Enter 1 and press [Enter] key to set “Require Network Level Authentication”.
6. Input for Terminal Service Setting: sets the Remote Desktop licensing mode. Enter either of the following values, and press the [Enter] key.
 - When selecting the number of connectable devices: 2
 - When selecting the number of connectable users: 4
7. Input for Discovery Scope: sets the discovery scope for Remote Desktop licensing. Enter either of the following values, and press the [Enter] key.
 - When selecting the work group: 0
 - When selecting the domain: 1

TIP

Select domains when the server computer is used in a domain environment.

8. [Input for License Servers To Use:] sets the license server to use. Enter the computer name or IP address of the license server and press the [Enter] key. If the license server is placed in a domain environment, use “Fully Qualified Domain Name (FQDN)” for the computer name and specify the host name, the domain name and others without omission.

TIP

If the license server and the remote desktop server run in the same computer, specify the name of local computer or its IP address.

The authentication method for Remote Desktop Session Host, the Remote Desktop licensing mode, the discovery scope for Remote Desktop licensing, and the setting information of license server are displayed in the batch file screen.

9. Confirm the authentication method for Remote Desktop Session Host, the Remote Desktop licensing mode, the discovery scope for Remote Desktop licensing, and the setting information of license server and if there is no problem, enter **y** at To be continued?: and press the [Enter] key. When the setup is complete, a message “Press any key to continue...” appears. If you need to change the setting, enter **n** at To be continued?: and run 2-InstallLicense.bat to perform the setup all over again.

■ Procedure 6: Authenticate Remote Desktop Licensing Server

Follow these steps to authenticate the Remote Desktop Licensing server:

1. Sign in to the server computer using the Administrator account.
2. Open Command Prompt.

3. Enter `licmgr.exe`.
The RD Licensing Manager appears.

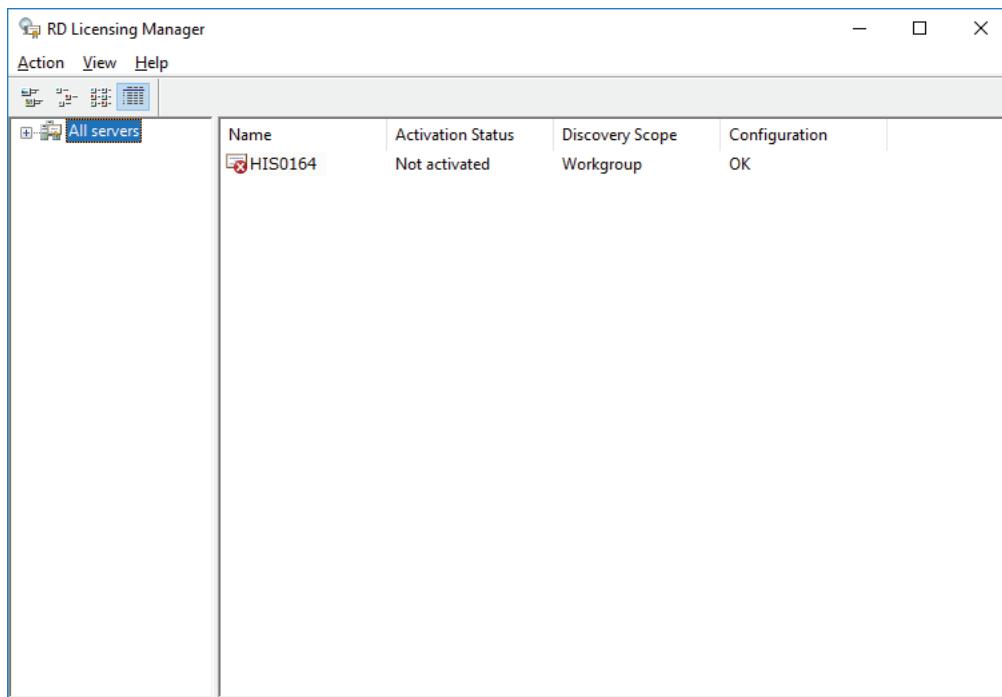


Figure B5.1.1-1 RD Licensing Manager

4. Select the computer to be authenticated, and select [Action] > [Activate Server] from the menu bar.
The Activate Server Wizard appears.
5. Follow the instructions of the Wizard and proceed the steps.

TIP

To install the Remote Desktop Services Client Access Licenses (RDS CAL), you must first authenticate the Remote Desktop Licensing server with Microsoft.

When the activation of license server is complete, install RDS CAL.

Contact Microsoft for more information about the authentication.

■ Procedure 7: Set up Audio

To make audio service available in remote desktop service environment, the system sound service need to be enabled.

- **Enabling Audio Service**

1. Open Control Panel.
2. Select [System and Security] > [Administrative Tools] > [Service].
The Services window appears.
3. Double-click [Windows Audio].
The Windows Audio Properties dialog box appears.

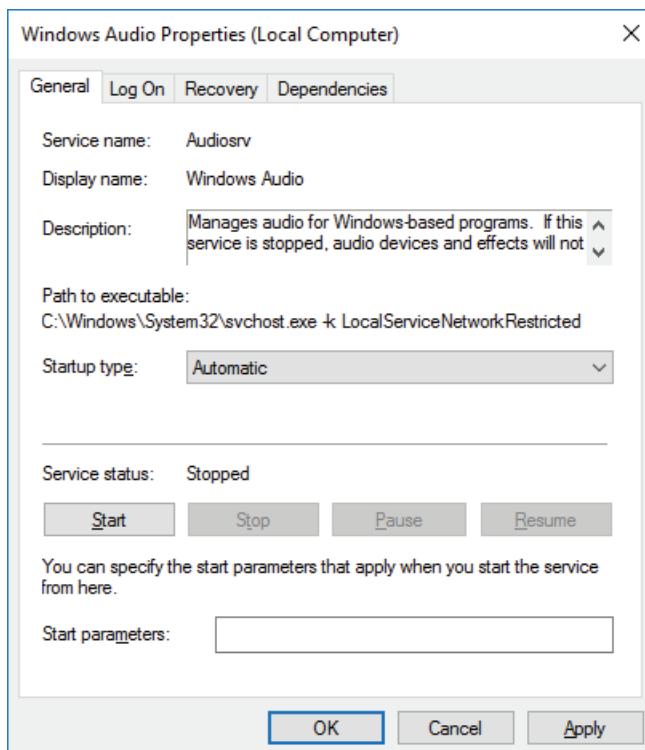


Figure B5.1.1-2 Windows Audio Properties Dialog Box

- From the Startup type drop-down list, select [Automatic] and, for Service status, select [Start]. After that, click [OK].
- On the Services window, confirm that Windows Audio service has become [Started] and its Startup Type is changed to [Automatic].

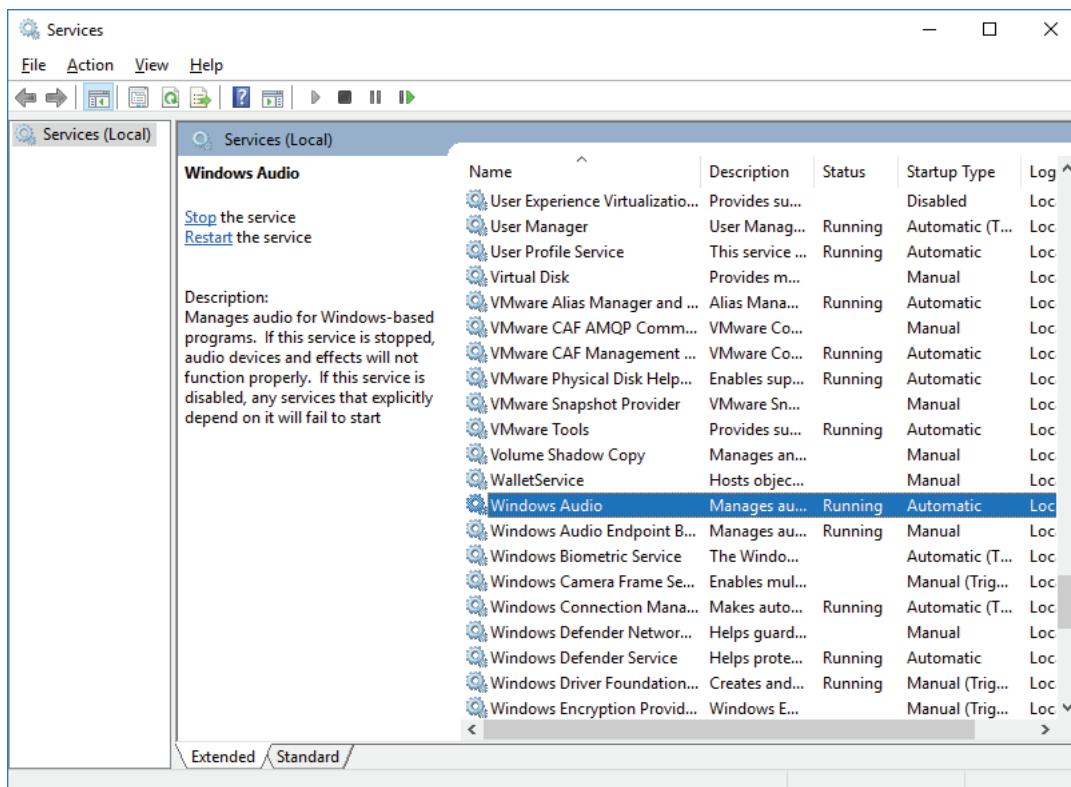


Figure B5.1.1-3 Services Window

● Run the System Sound Service

1. Open Control Panel.
2. Select [System and Security] > [Administrative Tools] > [Task Scheduler].
The Task Scheduler window appears.
3. Select [Task Scheduler Library] > [Microsoft] > [Windows] > [Multimedia].
4. Right-click [SystemSoundService] and select [Enable].

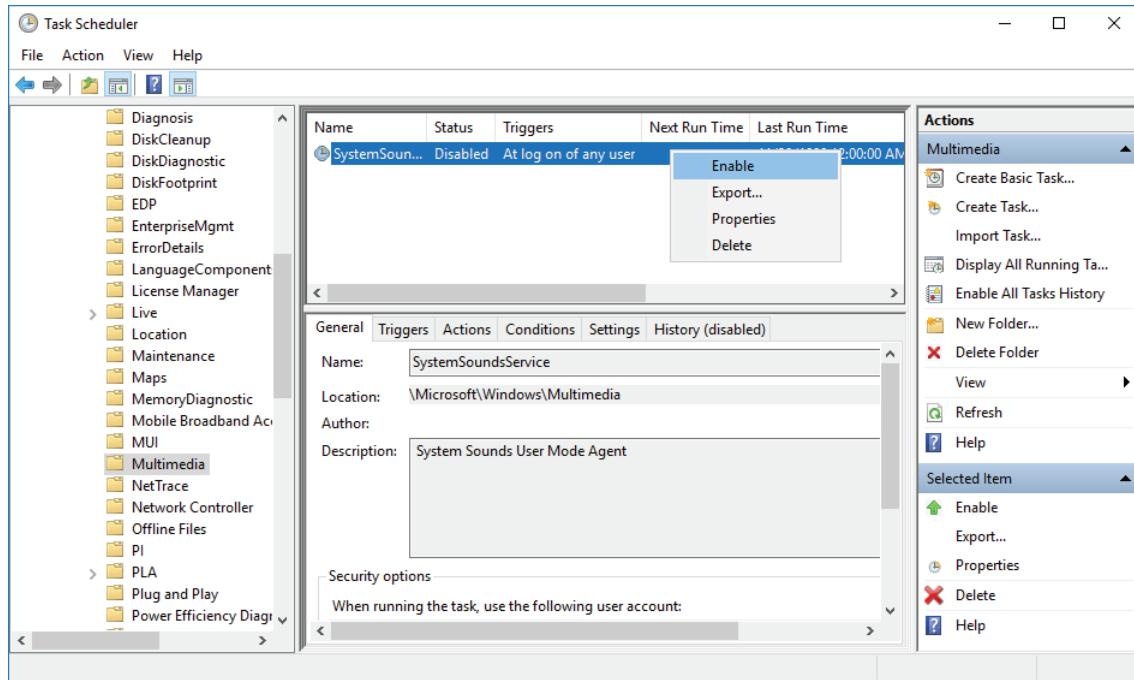


Figure B5.1.1-4 Task Scheduler Window – Enabling SystemSoundService

5. Right-click [SystemSoundService] and select [Run].

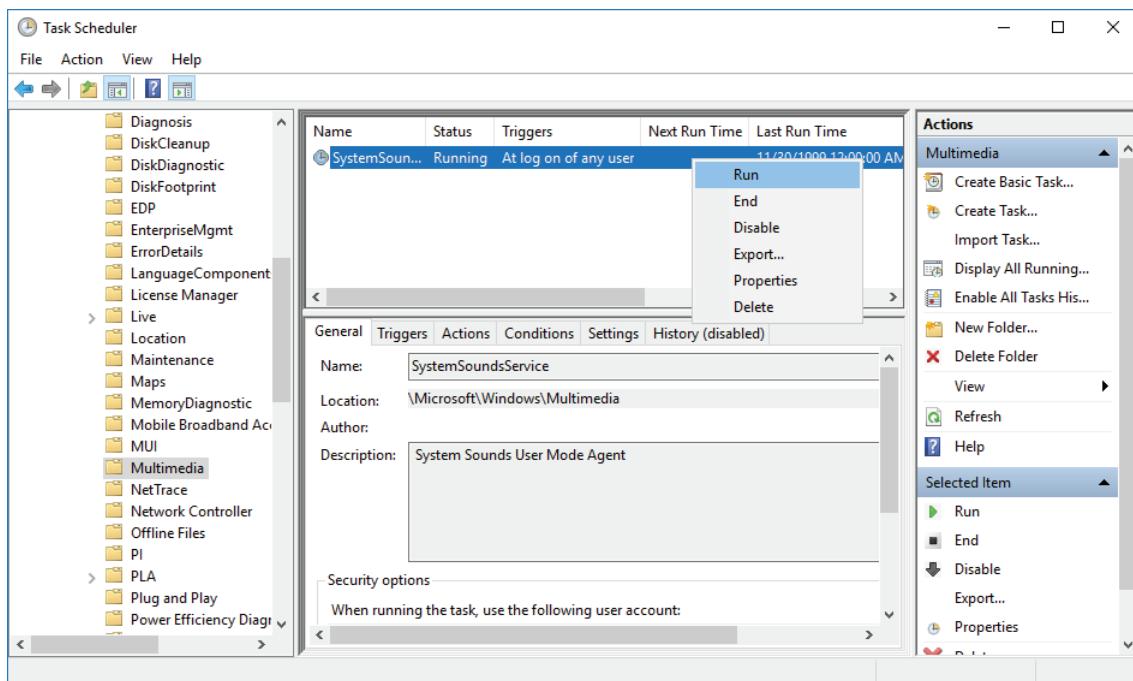


Figure B5.1.1-5 Task Scheduler Window – Running SystemSoundService

■ Procedure 8: Install the CENTUM VP Software

On the Remote Operation and Monitoring server, install the CENTUM VP software in the same way as the installation on HIS.

SEE ALSO

For more information about how to install the CENTUM VP software, refer to:

B4.6, “Installing the CENTUM VP Software” on page B4-85

■ Procedure 9: Configure IT Security Settings

After installing the CENTUM VP software, you need to configure security settings to strengthen the IT security of the computer.

SEE ALSO

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

B4.7, “Configuring IT Security Settings” on page B4-94

■ Procedure 10: Register Remote Desktop Users

After configuring the IT security settings, register the user or the user group to remotely log on to the Remote Desktop Users group. This section describes the procedure to register a RemoteCentum user to the Remote Desktop Users group.

1. Log on to the server computer using the Administrator account.
The Server Manager appears.
2. Select [Tools] > [Computer Management].
The Computer Management window appears.
3. Select [Computer Management] > [Local Users and Groups] > [Groups].
A list of groups appears.
4. Select and right-click [[Remote Desktop Users]] and select [Add to Group].

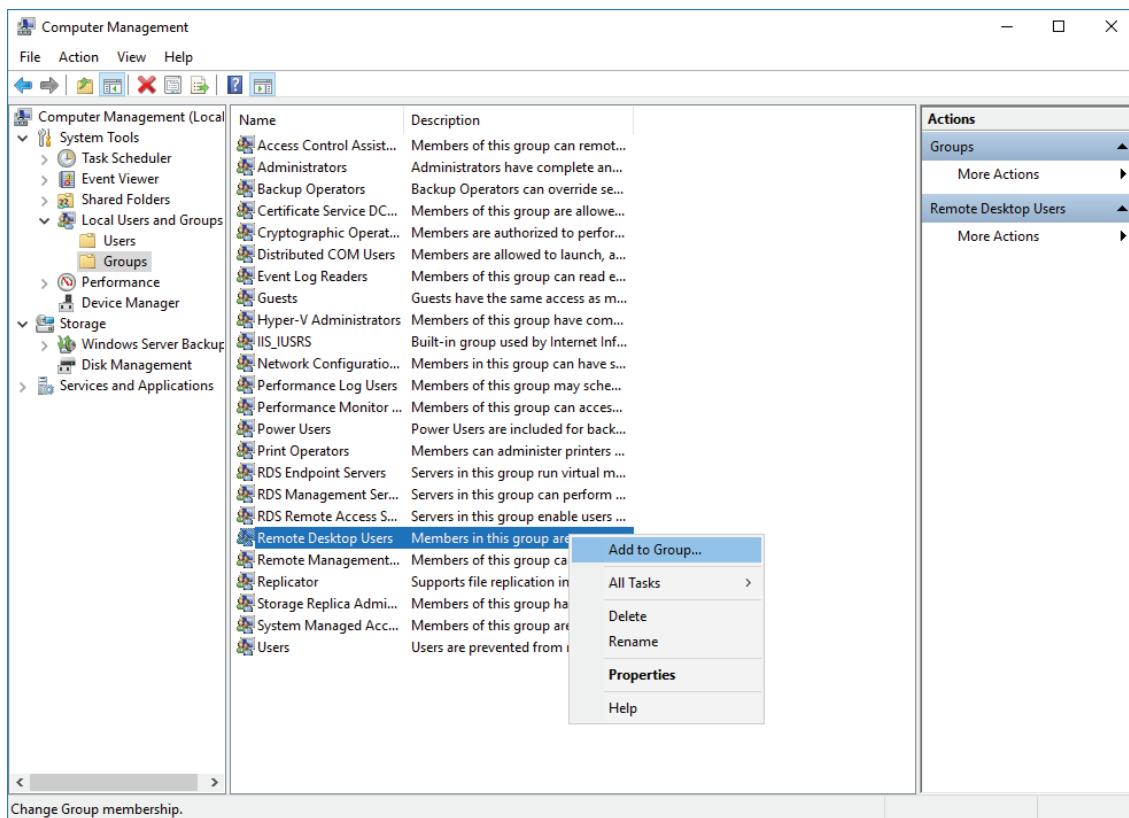


Figure B5.1.1-6 Computer Management Window

A list of Remote Desktop Users members appears.

5. On the [General] tab, click [Add].
The Choose user dialog box appears.
6. Click [Advanced].
The Advanced area appears additionally.
7. Click [Locations].
A list of locations appears.

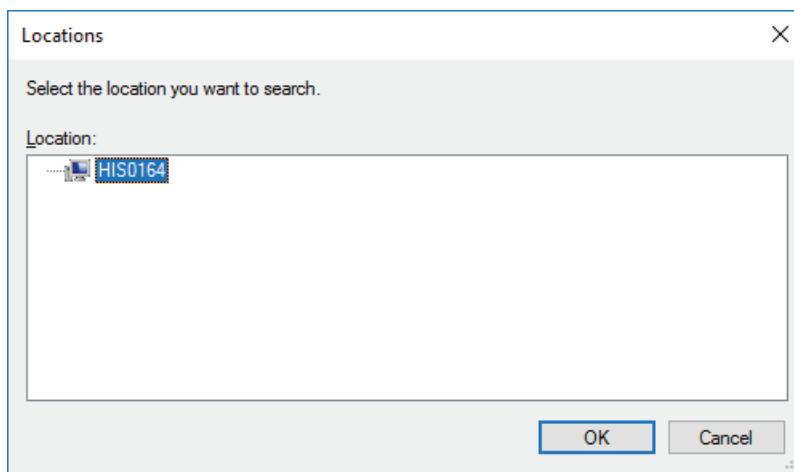


Figure B5.1.1-7 List of Locations

8. Select the name of the computer or domain to which the user you want to add belongs, and click [OK].
You are brought back to the Choose user dialog box.
9. Click [Find Now].

A list of users who belong to the selected computer or domain appears.

TIP

If you selected a domain name for the location, the list of users may not appear depending on the configuration of the domain. Also note that if the domain contains more than 10000 users, all users cannot be displayed in the list.

If this is your case, click [Cancel] to close the Advanced setting dialog box and type the user name in the [Enter the object names to select] box.

Example: When specifying a domain user: somedomain\RemoteCentum

When specifying a local user: HIS0164\RemoteCentum

10. Select the RemoteCentum user that you want to add and click [OK].
RemoteCentum is added to the Member of list.

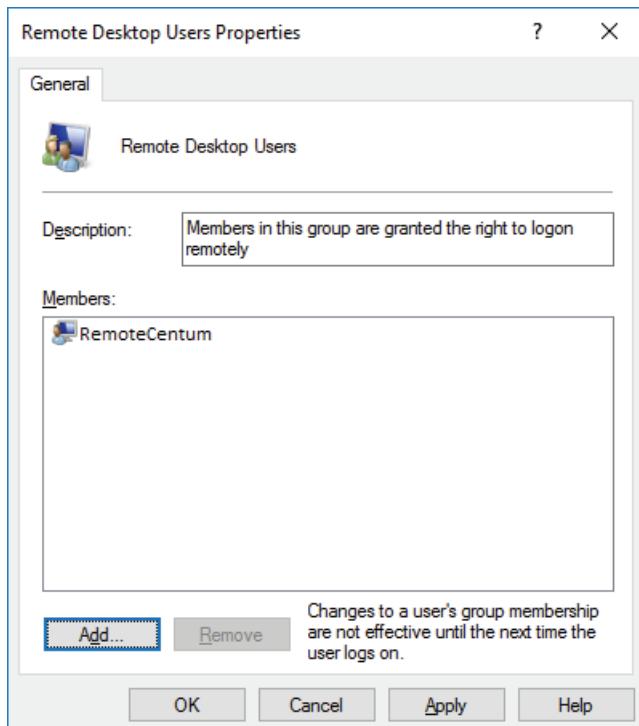


Figure B5.1.1-8 Properties of Remote Desktop Users

11. Click [OK].

■ Procedure 11: Distribute and Accept Licenses

From the license management station, distribute the licenses of the required packages in addition to the Server for Remote Operation and Monitoring Function, and accept them.

SEE ALSO

For more information about the procedure for distributing and accepting licenses, refer to:

B4.8, "Distributing and Accepting Licenses" on page B4-101

■ Procedure 12: Create User Accounts

You must create user accounts.

SEE ALSO

For more information about creating user accounts, refer to:

B4.9, "Creating User Accounts" on page B4-102

■ Procedure 13: Configure Windows Environment Settings for Each User

You need to configure the Windows operating environment settings for each user who logs on to the server.

SEE ALSO

For more information about the procedures for setting the Windows operating environment for each user, refer to:

B4.10, "Configuring Windows Environment Settings for Each User" on page B4-107

■ Procedure 14: Set User Authentication Mode

You need to configure settings for the user authentication mode.

SEE ALSO

For more information about the procedures for setting up for user authentication modes, refer to:

B4.11, "Setting Up for User Authentication Modes" on page B4-135

■ Procedure 15: Set Up the Uninterruptible Power Source (UPS)

To use an UPS, you need to configure the settings for it.

SEE ALSO

For more information about the procedure for setting up the UPS service, refer to:

B4.12, "Setting Up the Uninterruptible Power Supply (UPS) Service" on page B4-149

■ Procedure 16: Set Up RemoteApp Programs

To make the CENTUM VP operation and monitoring function available from a computer that connects remotely to the HIS-TSE server, you need to configure the remote desktop services.

● Adding StartDesktop.bat

This setup is required to use HIS-TSE in Desktop mode. Follow these steps to add StartDesktop.bat.

1. Sign in to the server computer using the Administrator account.
2. Insert the CENTUM VP installation medium into the drive.
3. Use Windows Explorer to open the following folder in the CENTUM VP installation medium.
<Drive of CENTUM VP software medium>:\CENTUM\HIS\TSE
4. Right-click "3-AddStartDesktop.bat" and select [Run As Administrator].
5. After confirming that the CENTUM VP software is installed on the computer, enter **y** at Have you installed CENTUM VP Software? and press the [Enter] key. If the CENTUM VP software is not installed, enter **n** and press the [ENTER] key. Then, install CENTUM VP and perform this setup again.

TIP

During installation of CENTUM VP, StartDesktop.bat is installed in <CENTUM VP installation folder>\program files. Because this procedure does not work if CENTUM VP is not installed on the computer, make sure that StartDesktop.bat exists in place.

● Adding BKHBos.exe

This setup is required to use HIS-TSE in Panel mode. Follow these steps to add BKHBos.exe.

1. Sign in to the server computer using the Administrator account.
2. Insert the CENTUM VP installation medium into the drive.
3. Use Windows Explorer to open the following folder in the CENTUM VP installation medium.
 <Drive of CENTUM VP software medium>:\CENTUM\HIS\TSE
4. Right-click “A1-AddBKHBos.bat” and select [Run As Administrator].
5. After confirming that the CENTUM VP software is installed on the computer, enter **y** at Have you installed CENTUM VP Software? and press the [Enter] key. If the CENTUM VP software is not installed, enter **n** and press the [ENTER] key. Then, install CENTUM VP and perform this setup again.

TIP

During installation of CENTUM VP, BKHBos.exe is installed in <CENTUM VP installation folder>\program. Because this procedure does not work if CENTUM VP is not installed on the computer, make sure that BKHBos.exe exists in place.

■ Procedure 17: Set Up the Remote Desktop Service

Follow these steps to configure session restrictions and network adapters:

TIP

The RDP-Tcp Properties items are automatically set as follows:

- General: [Allow connections only from computers running Remote Desktop with Network Level Authentication] is turned on.
- Log on Settings: [Always use the following log on information] is turned on with CENTUM set as the user.
- Remote Control: [Do not allow remote control] is turned on.
- Client Settings: [Limit Maximum Color Depth], [Audio Recording], and [Audio and video playback] are turned off.

1. Sign in to the server computer using the Administrator account.
2. Insert the CENTUM VP installation medium into the drive.
3. Use Windows Explorer to open the following folder in the CENTUM VP installation medium.
 <Drive of CENTUM VP software medium>:\CENTUM\HIS\TSE
4. Right-click “4-TerminalServiceSetting.bat” and select [Run As Administrator].
5. In Input for Single Session Per User:, configure the settings regarding restricting sessions. Enter either of the following values, and press the [Enter] key.
 - When the Legacy model of IT security settings are applied (always use the CENTUM account to sign in): 0
 - When the Standard model is selected for IT security settings and operators use their individual names to sign in: 1
6. In Select Network Adapter:, specify the network adapter to be used for communications between the HIS-TSE server and HIS-TSE clients. When the options of available network adapters appear, enter the value of applicable network adapter and press the [Enter] key.

TIP

Do not specify Yokogawa Vnet Adapter:1.

7. Confirm the session restriction and network adapter settings that you have configured and if there is no problem, enter **y** at To be continued?: and press the [Enter] key. When the setup is complete, a message “Press any key to continue...” appears. If you need to change the setting, enter **n** at To be continued?: and run 4-TerminalServiceSetting.bat to perform the setup all over again.

● Setting to Automatically Start the Operation and Monitoring Function

When using HIS-TSE in Desktop mode, if you set a batch file for the Start a program on connection policy in the Local Group Policy Editor, the operation and monitoring function can be started automatically just by connecting to the HIS-TSE server, without configuration on each HIS-TSE client. Follow these steps to set up automatic starting of the operation and monitoring function:

1. Sign in to the server computer using the Administrator account.
2. Open Command Prompt.
3. Enter `gpedit.msc`.
The Local Group Policy Editor appears.
4. In the left pane, select [Computer Configuration] > [Administrative Templates] > [Windows Components] > [Remote Desktop Services] > [Remote Desktop Session Host], and click [Remote Session Environment].
5. Double-click [Start a program on connection].
The Start a program on connection dialog box appears.

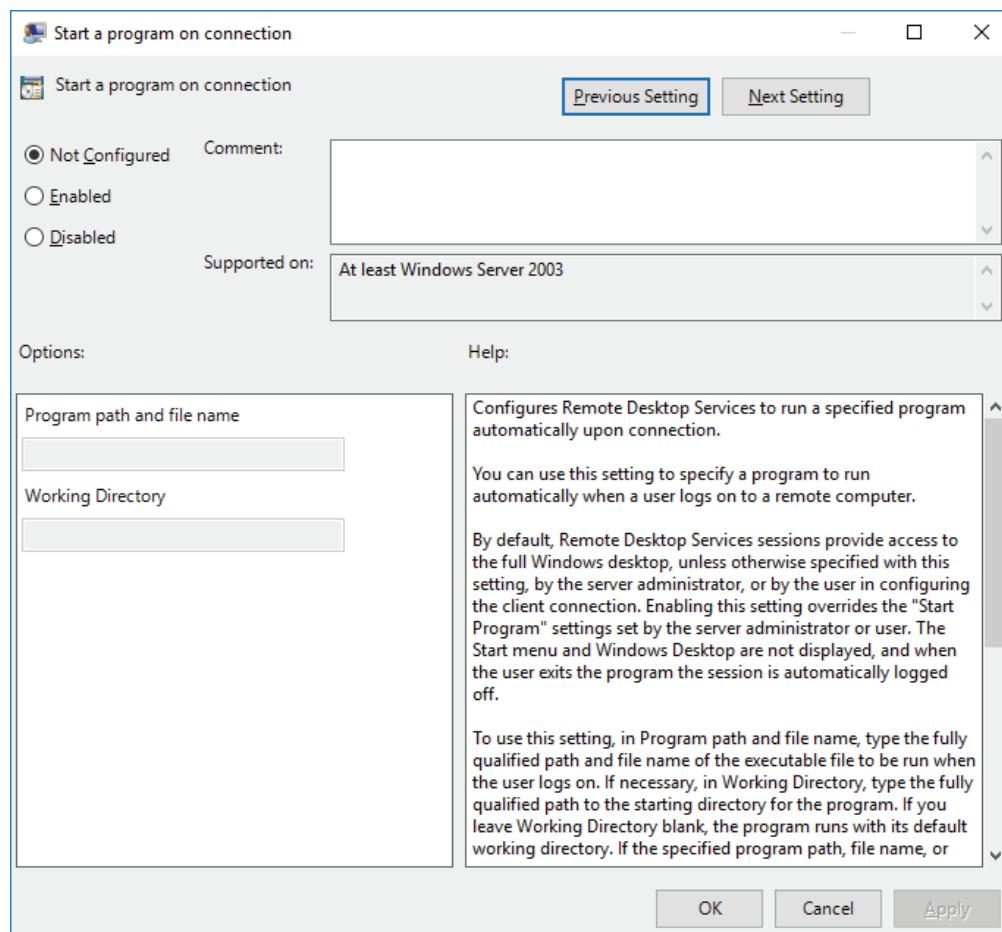


Figure B5.1.1-9 Start a program on connection Dialog Box

6. Select [Enabled].

7. In the Program path and file name box, enter the path to the following batch file.
<CENTUM VP installation drive>:\CENTUMVP\Program\StartDesktop.bat
8. In the Working Directory box, enter the following path:
<CENTUM VP installation drive>:\CENTUMVP\Program
9. Click [OK].

■ Procedure 18: Add HIS-TSE to the Project

1. On System View, open the project to which the HIS-TSE is to be added.
2. Add a station, specifying [HIS-TSE HIS with Server for Remote Operation and monitoring function] as the station type.
3. In the same procedures as those for the standard HIS, run the following download commands: [Download Project Common Section], [Download to HIS], and [Download Tag-List].
4. Restart the Remote Operation and Monitoring Server.

SEE ALSO

For more information about the builder definition items when a new HIS is created, refer to:

2.4.2, "Creating a New HIS" in Engineering Reference Vol.1 (IM 33J10D10-01EN)

■ Confirming the Settings

You can view a list of the settings that have been set by batch files in Procedures 5, 16, and 17. Follow these steps to view the settings that have been set:

1. Sign in to the server computer using the Administrator account.
2. Insert the CENTUM VP installation medium into the drive.
3. Use Windows Explorer to open the following folder in the CENTUM VP installation medium.
<Drive of CENTUM VP software medium>:\CENTUM\HIS\TSE
4. Right-click "A2-ConfirmSettings.bat" and select [Run As Administrator].
The current settings are listed in the following format:

Setting item [Expected value]: Set value
5. If there is any difference between the expected value and the set value, run the corresponding batch file to re-configure the settings.

SEE ALSO

For more information about how to run the batch files, refer to:

- "■ Procedure 5: Install License Server" on page B5-5
- "■ Procedure 16: Set Up RemoteApp Programs" on page B5-13
- "■ Procedure 17: Set Up the Remote Desktop Service" on page B5-14

● Expected Values of the Settings

The following table shows the expected values of the settings for each batch file.

Table B5.1.1-1 Expected Values of the Settings for Each Batch File

Batch file	Setting item	Expected value	Description
2-InstallLicense.bat (Procedure 5)	User Authentication	1	Specify Authentication Method for Remote Desktop Session Host: Require Network Level Authentication is set.
		0	Specify Authentication Method for Remote Desktop Session Host: Do not require Network Level Authorization is set.
	Terminal Service Setting	2	Remote Desktop licensing mode: Per Device is set.
		4	Remote Desktop licensing mode: Per User is set.
	DisableCam	0 (Fixed)	Configure Client Experience: Audio and video playback is enabled.
	DisableAudioCapture	0 (Fixed)	Configure Client Experience: Audio recording redirection is enabled.
	Allow Desktop Composition On Server	0 (Fixed)	Configure Client Experience: Desktop composition is disabled.
	Discovery Scope	0	Configure Discovery Scope for RD Licensing: This workgroup is selected.
		1	Configure Discovery Scope for RD Licensing: This domain is selected.
	License Servers To Use	The computer name or IP address of the license server	Specify the license server to use
3-AddStartDesktop.bat (Procedure 16)	StartDesktop_Command-LineSetting	0 (Fixed)	RemoteApp program specification: Command-line arguments are not allowed.
	StartDesktop_Name	StartDesktop (Fixed)	RemoteApp program specification: Batch file name
	StartDesktop_Path	<CENTUM VP installation folder>\program\StartDesktop.bat (Fixed)	RemoteApp program specification: The file pathname of the batch file for the RemoteApp program to be added is set.
	StartDesktop_ShowInTS-WA	1 (Fixed)	RemoteApp program specification: 'RemoteApp program is available through RD Web Access' is enabled.

Continues on the next page

Table B5.1.1-1 Expected Values of the Settings for Each Batch File (Table continued)

Batch file	Setting item	Expected value	Description
A1-AddBKHBos.bat (Procedure 16)	BKHBos_CommandLine-Setting	1 (Fixed)	Setting for execution in panel mode: Command-line arguments are allowed.
	BKHBos_Name	BKHBos (Fixed)	Setting for execution in panel mode: RemoteApp program name
	BKHBos_Path	<CENTUM VP installation folder>\program\BKHBos.exe (Fixed)	Setting for execution in panel mode: The file pathname of the added RemoteApp program is set.
	BKHBos_ShowInTWSA	1 (Fixed)	Setting for execution in panel mode: 'RemoteApp program is available through RD Web Access' is enabled.

Continues on the next page

Table B5.1.1-1 Expected Values of the Settings for Each Batch File (Table continued)

Batch file	Setting item	Expected value	Description
4-TerminalServiceSetting.bat (Procedure 17)	Single Session Per User	0	Terminal Service specification: 'Restrict each user to a single session' is disabled.
		1	Terminal Service specification: 'Restrict each user to a single session' is enabled.
	Inherit Auto Logon	1 (Fixed)	Terminal Service specification: 'Allow connections only from computers running Remote Desktop with Network Level Authentication' is enabled.
	Max Disconnection Time	60000 (Fixed)	Terminal Service specification: Time-out value of End a disconnected session
	Shadow	0 (Fixed)	Terminal Service remote control specification: 'Do not allow remote control' is enabled.
	Inherit Color Depth	1 (Fixed)	Terminal Service client specification: 'Limit Maximum Color Depth' is disabled.
	Max Monitors	1 (Fixed)	Terminal Service client specification: Maximum number of monitors for each session
	Network Adapter	Network adapter number	Terminal Service network adapter specification: ID number for the selected network adapter list
	Network Adapter List	List of network adapters	Terminal Service network adapter specification: List of available network adapters

B5.1.2 Configuring on Windows Server 2008 R2

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

■ Procedure 1: Set Up the Hardware

Set up the hardware of the HIS-TSE server computer.

SEE ALSO For more information about hardware setup , refer to:

B4.1, “Setting Up the Hardware” on page B4-2

■ Procedure 2: Set Up Windows

Before you install the CENTUM VP software on the computer, configure Windows settings.

TIP Set the same virtual memory size as the size that was set when setting up the HIS.

SEE ALSO For more information about the procedures for setting up Windows, refer to:

B4.2.5, “Configuring on Windows Server 2008 R2” on page B4-36

■ Procedure 3: Configure Network Settings

The control bus driver needs to be installed for running the CENTUM VP software. If Vnet/IP is used, the Vnet/IP open communication driver also needs to be installed.

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

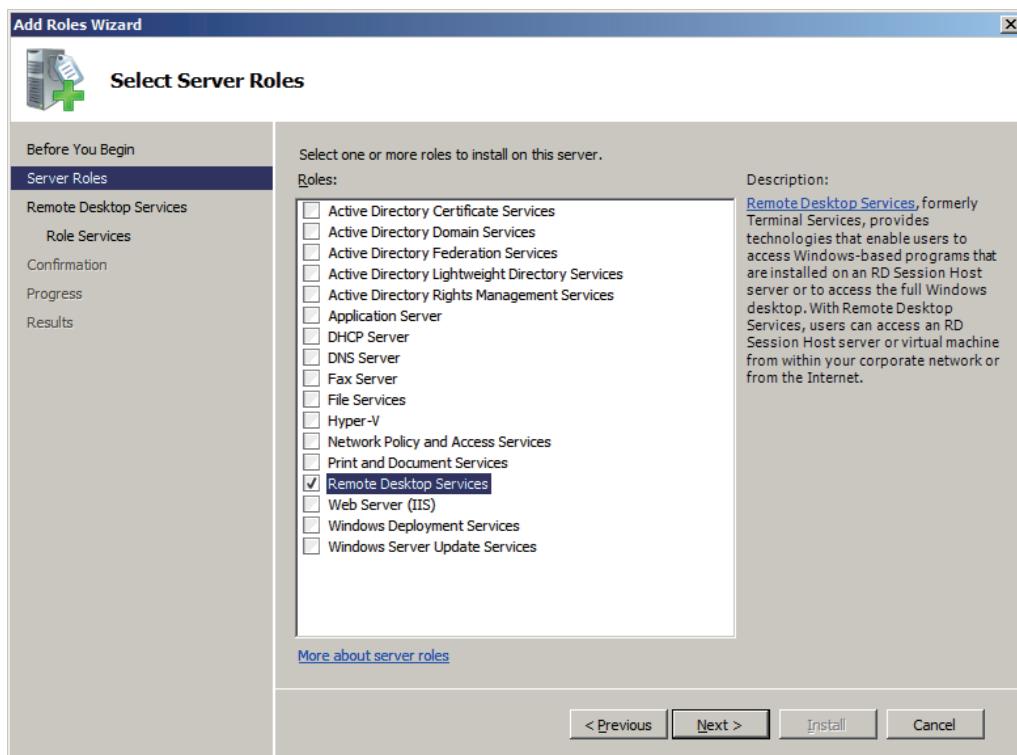
If you use the built-in Ethernet interface of the computer or an over-the-counter Ethernet card, read the attached instruction manual and install the proper Ethernet driver accordingly.

SEE ALSO For more information about the procedures for network setting, refer to:

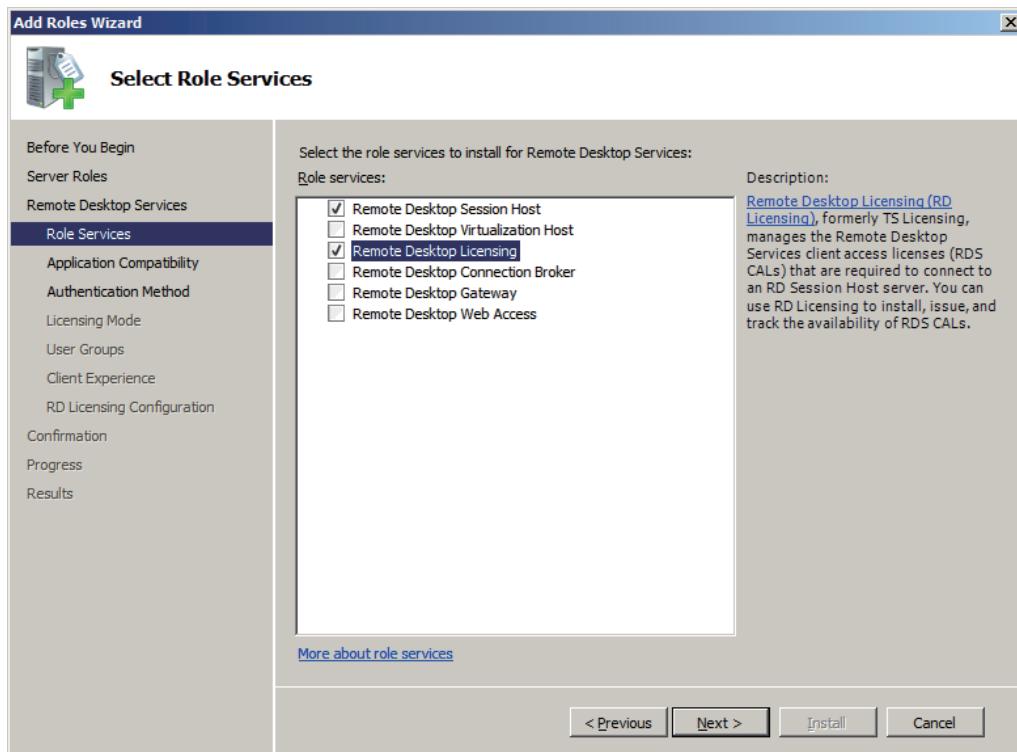
B4.3, “Configuring Network Settings” on page B4-43

■ Procedure 4: Install Remote Desktop Service and License Server

1. Log on to the server computer using the Administrator account.
The Server Manager appears.
2. Select [Roles] > [Add Roles].
The Add Roles Wizard appears.
3. Read and verify the conditions displayed on the Add Roles Wizard, and click [Next].
The following window appears.

**Figure B5.1.2-1 Add Roles Wizard - Select Server Roles**

4. Select [Remote Desktop Services] from the [Server Roles] list, and click [Next].
 5. Confirm the message displayed in the window, and click [Next].
- The Select Role Services window appears.

**Figure B5.1.2-2 Add Roles Wizard - Select Role Services**

6. Select [Remote Desktop Session Host] and [Remote Desktop Licensing] from the [Role Services] list, and click [Next].
The Uninstall and Reinstall Applications for Compatibility window appears.

TIP

Since [Remote Desktop Licensing] can be shared by multiple terminal servers, select the checkbox as necessary. When connecting to an existing license server, confirm that the license server and the remote desktop server are using the same version of operating system of Windows Server 2008 R2 or later.

7. Confirm the message displayed in the window, and click [Next].
The “Specify Authentication Method for Remote Desktop Session Host” window will be displayed.

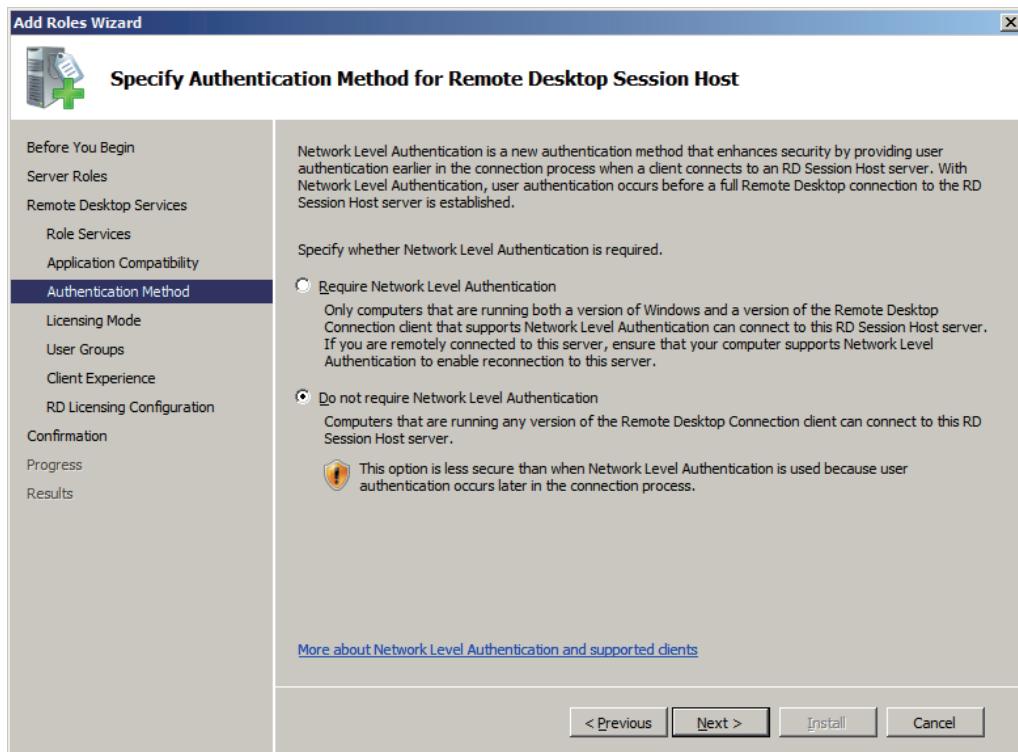


Figure B5.1.2-3 Add Roles Wizard - Specify Authentication Method for Remote Desktop Session Host

8. Select [Require Network Level Authorization].
9. Click [Next].
The Specify Licensing Mode window appears.

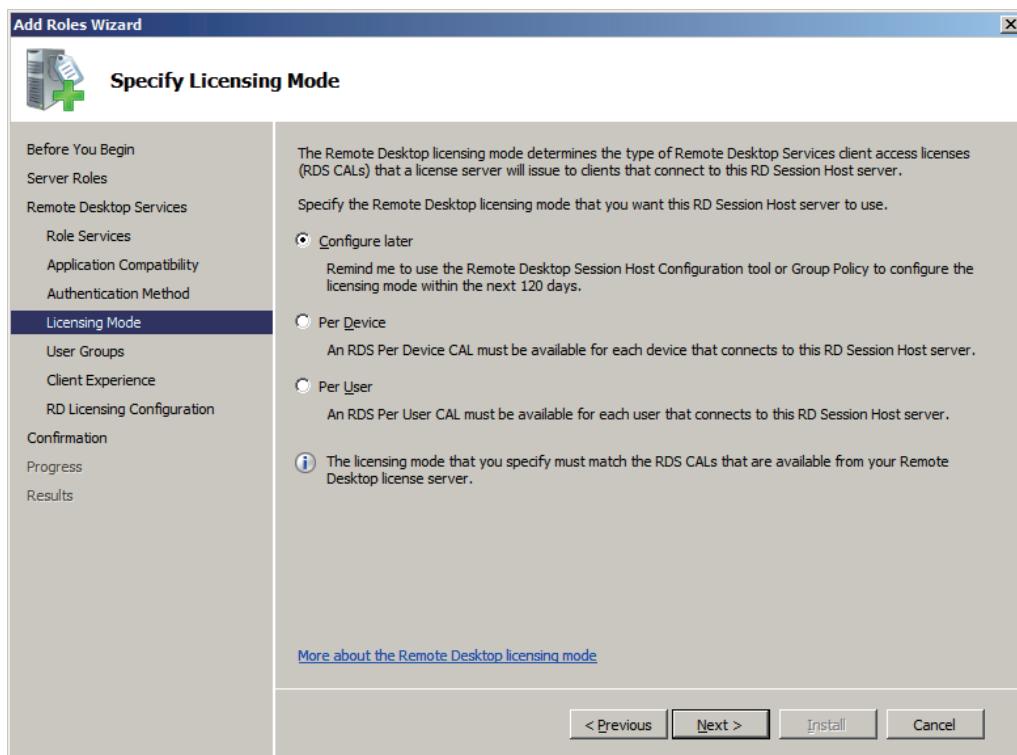


Figure B5.1.2-4 Add Roles Wizard - Specify Licensing Mode

10. Specify Remote Desktop licensing mode to be used on this remote desktop server, and click [Next].
The Select User Groups Allowed Access to This RD Session Host Server window appears.

TIP

Even if you select [Configure Later] here, the settings are still required before the next remote desktop license needs to be activated. It is recommended to configure the settings here.

11. Click [Next].
The Configure Client Experience window appears.

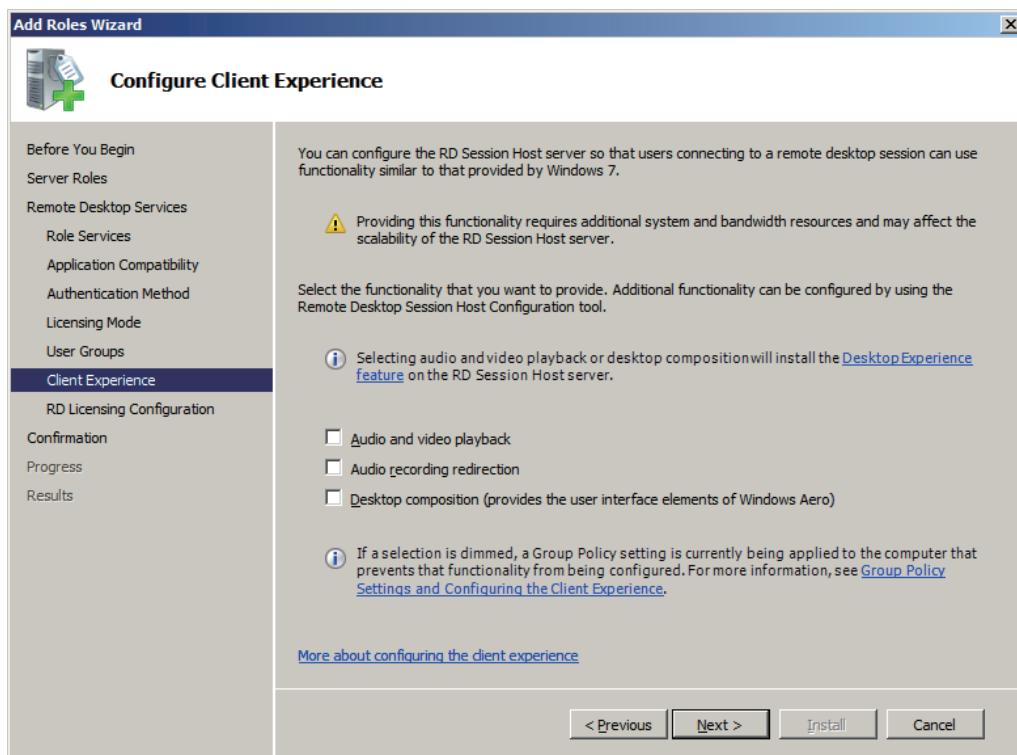


Figure B5.1.2-5 Add Roles Wizard - Configure Client Experience

TIP

When CENTUM VP has been installed, the user or the user group to remotely logon must be registered to the "Remote Desktop Users Group."

12. Clear all check boxes and click [Next].

The Configure Discovery Scope for RD Licensing window appears.

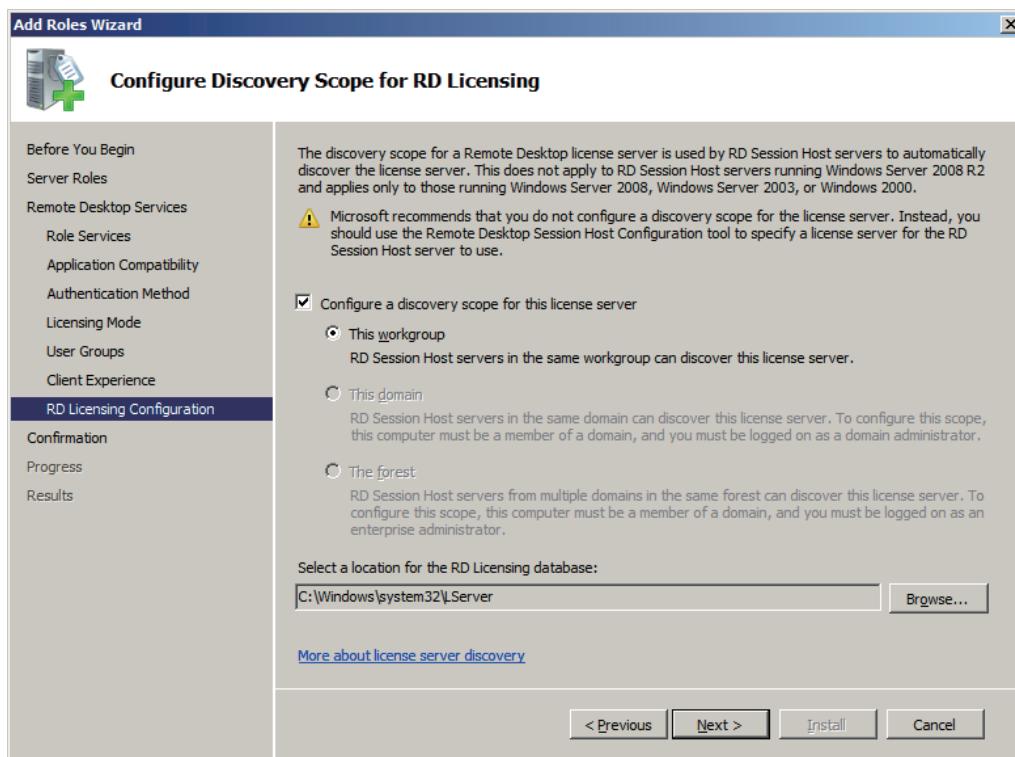


Figure B5.1.2-6 Add Roles Wizard - Configure Discovery Scope for RD Licensing

13. Select the check box for [Configure a discovery scope for this licenses server], select [This workgroup], and then click [Next] (If Domain management is used, select [This domain]).

The Confirm Installation Selections window appears.

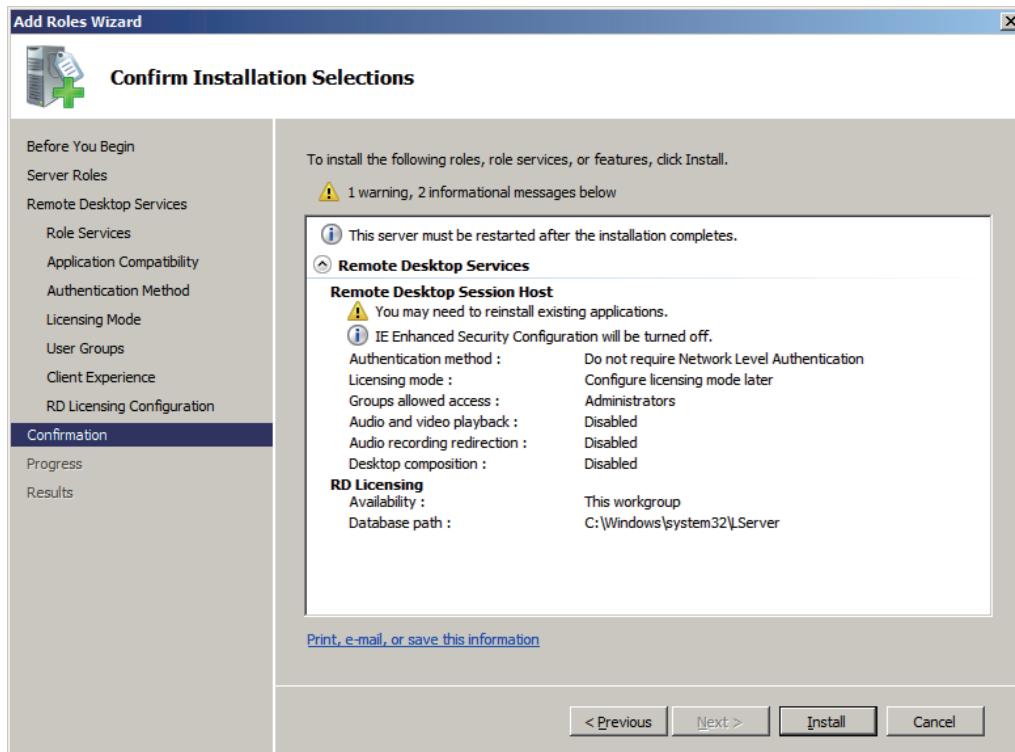


Figure B5.1.2-7 Add Roles Wizard - Confirm Installation Selections

14. Confirm the description in the window and click [Install].
The installation starts, and when the installation is complete, the Installation Results window appears.
15. Confirm the displayed results and click [Close].
A dialog box for confirming restarting of the computer appears.
16. Click [Yes] to restart the computer.
After the computer has restarted, the Installation Results window appears.
17. Confirm the displayed contents and click [Close].

■ Procedure 5: Authenticate Remote Desktop Licensing Server

Follow these steps to authenticate the Remote Desktop Licensing server:

1. Select [Server Manager] > [Roles] > [Remote Desktop Services] > [RD Session Host Configuration].
The following window appears.

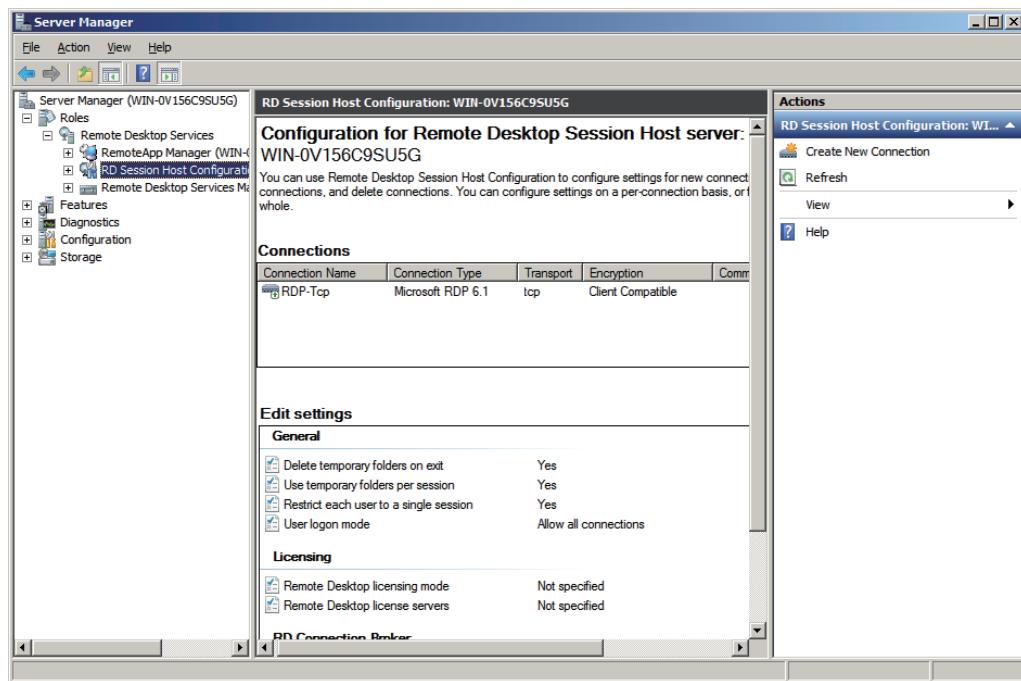


Figure B5.1.2-8 Configuration for Remote Desktop Session Host Server

2. In the Edit settings section, double-click [Remote Desktop licensing mode].
The license properties are displayed.

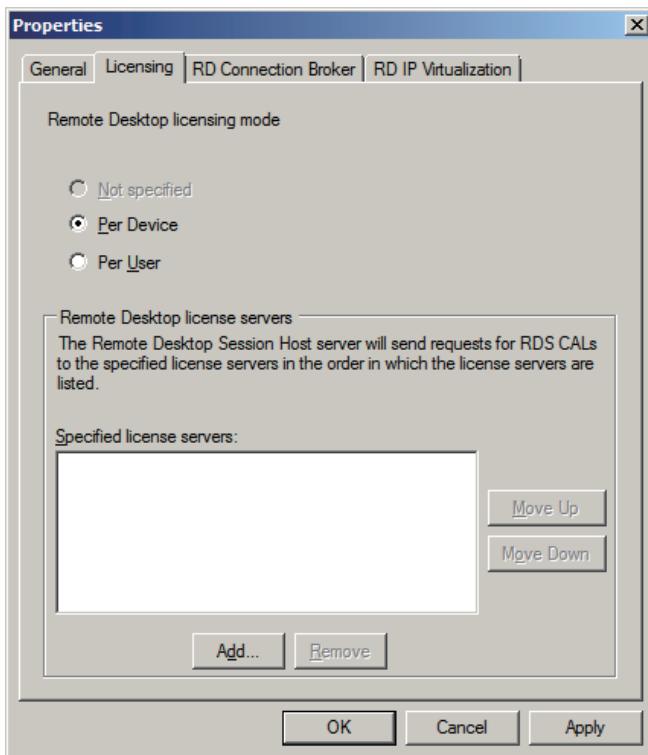


Figure B5.1.2-9 Properties Dialog Box

3. Set the properties according to your circumstances and click [OK].

TIP

In case no to set the license server, you cannot access it 120 days later.

4. Select [Server Manager] > [Roles] > [Remote Desktop Services].
The following window appears.

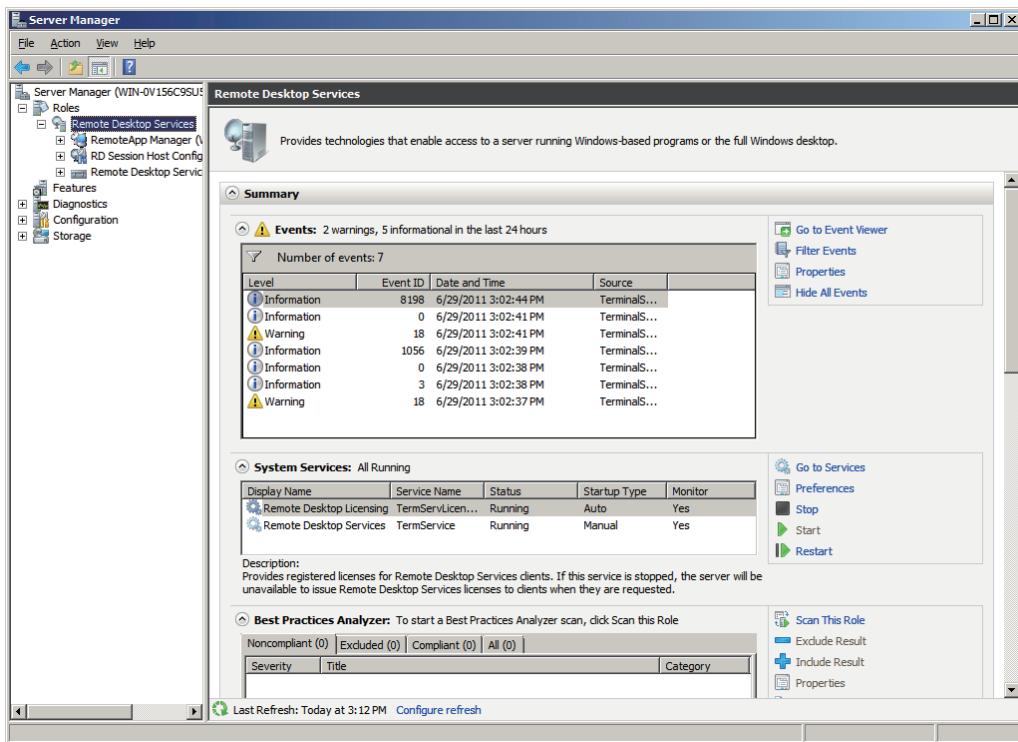


Figure B5.1.2-10 Server Manager

- Click [Remote Desktop Licensing Manager] in the [Advanced Tools] area. The RD Licensing Manager starts.

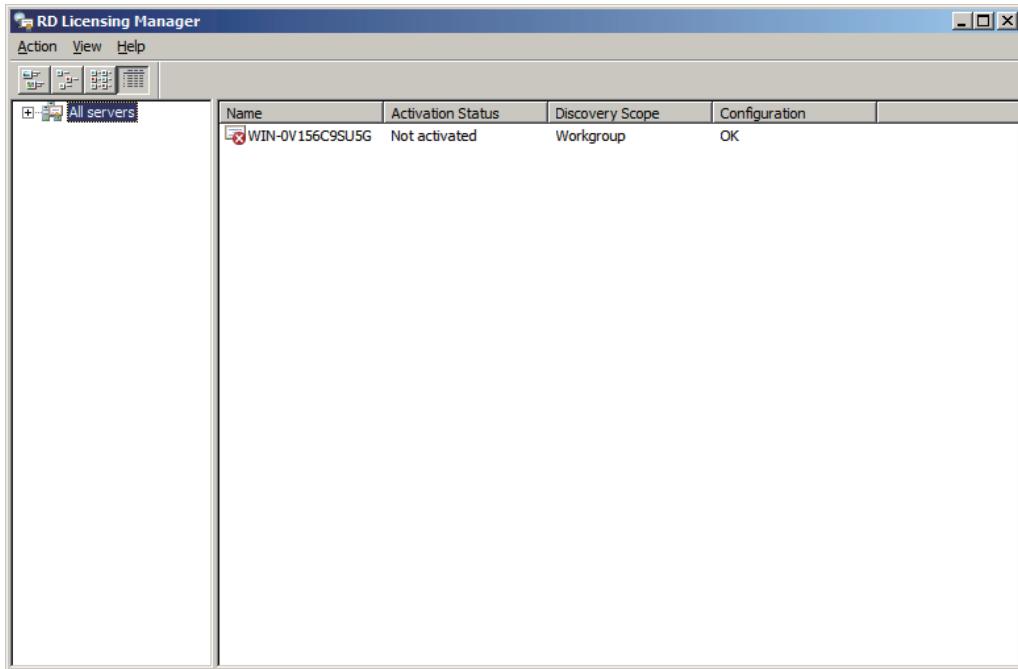


Figure B5.1.2-11 RD Licensing Manager

- Select the computer to be authenticated, and select [Action] > [Activate Server] from the menu bar.
The Activate Server Wizard appears.
- Follow the instructions of the Wizard and proceed the steps.

TIP

To install the Remote Desktop Services Client Access Licenses (RDS CAL), you must first authenticate the Remote Desktop Licensing server with Microsoft.

When the activation of license server is complete, install RDS CAL.

Contact Microsoft for more information about the authentication.

■ Procedure 6: Setup Audio

To make audio service available in remote desktop service environment, the system sound service need to be enabled.

● Enable Audio Service

1. Open Control Panel.
2. Select [System and Security] > [Administrative Tools] > [Services].
The Services window appears.
3. Double-click [Windows Audio].
The Windows Audio Properties dialog box appears.

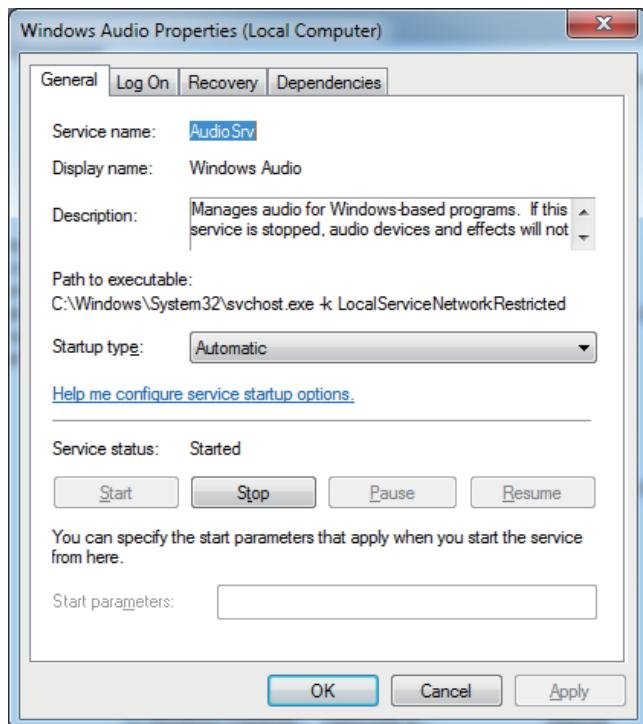


Figure B5.1.2-12 Windows Audio Properties Dialog Box

4. From the Startup type drop-down list, select [Automatic] and, for Service status, select [Start]. After that, click [OK].
5. On the Services window, confirm that Windows Audio service has become Started and its Startup Type is changed to [Automatic].

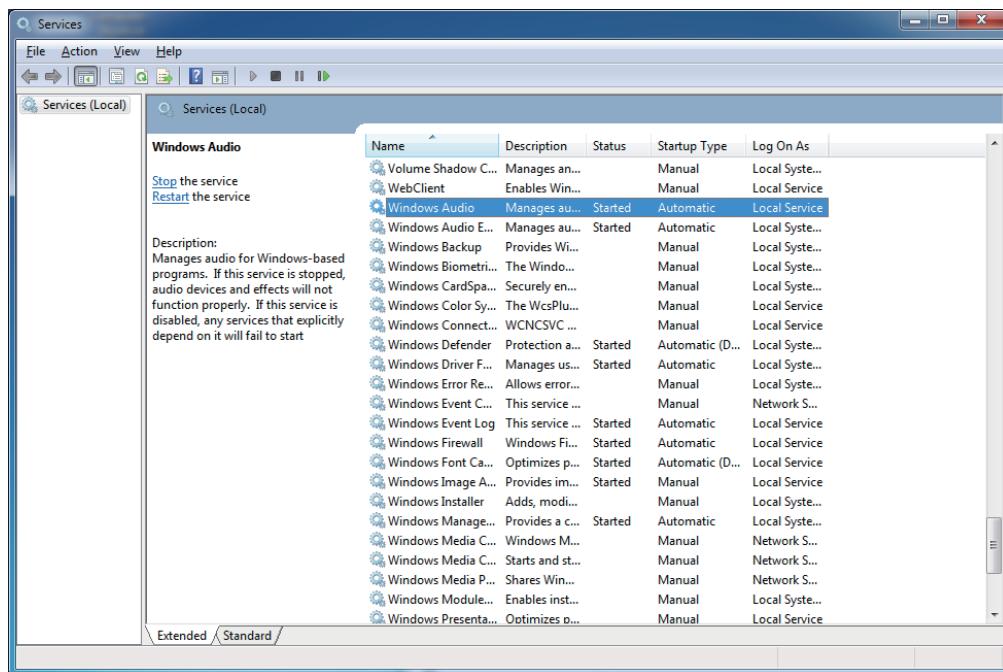


Figure B5.1.2-13 Services Window

● **Install Desktop Experience**

1. Select [Server Manager] > [Features].
The Server Manager appears.
2. Click Add Features in the [Features Summary] section.
The Add Features Wizard appears.
3. Select [Desktop Experience] check box.
A dialog box for confirming adding features appears.
4. Click [Add Required Features].
You are brought back to the Add Features Wizard.
5. Click [Next].
6. Confirm that “Ink and Handwriting Services Ink Support” and “Desktop Experience” are displayed as the items to be installed and click [Install].
Installation starts.
7. In the installation results, confirm that “Ink and Handwriting Services” and “Desktop Experience” have been added and click [Close].
The computer restarts.
8. After restarting, confirm in the Installation Results page of the wizard that “Ink and Handwriting Services” and “Desktop Experience” have been installed successfully and click [Close].

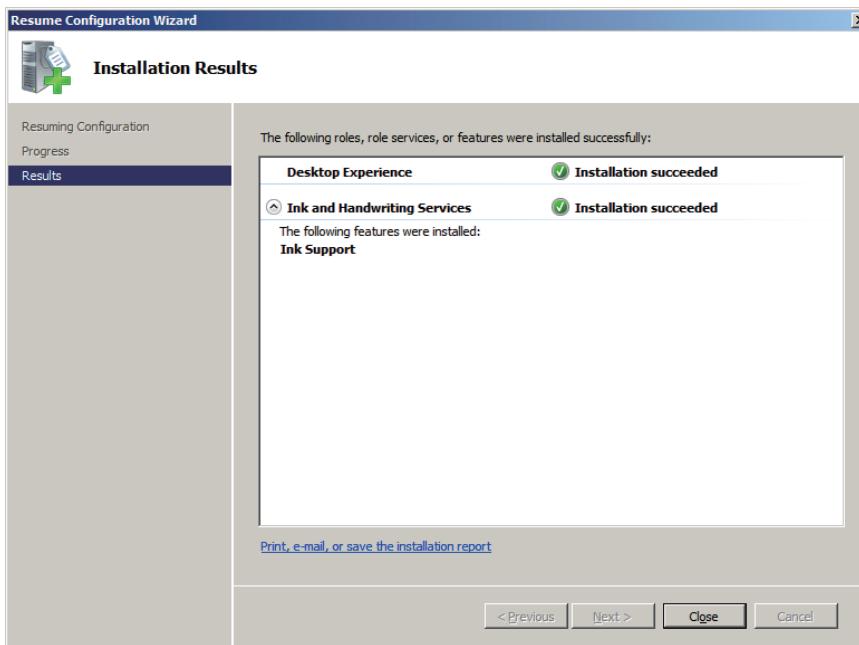


Figure B5.1.2-14 Installation Results

- **Run the System Sound Service**

1. Open Control Panel.
2. Select [System and Security] > [Administrative Tools] > [Task Scheduler]. The Task Scheduler window appears.
3. Select [Task Scheduler Library] > [Microsoft] > [Windows] > [Multimedia].
4. Right-click [SystemSoundService] and select [Enable].

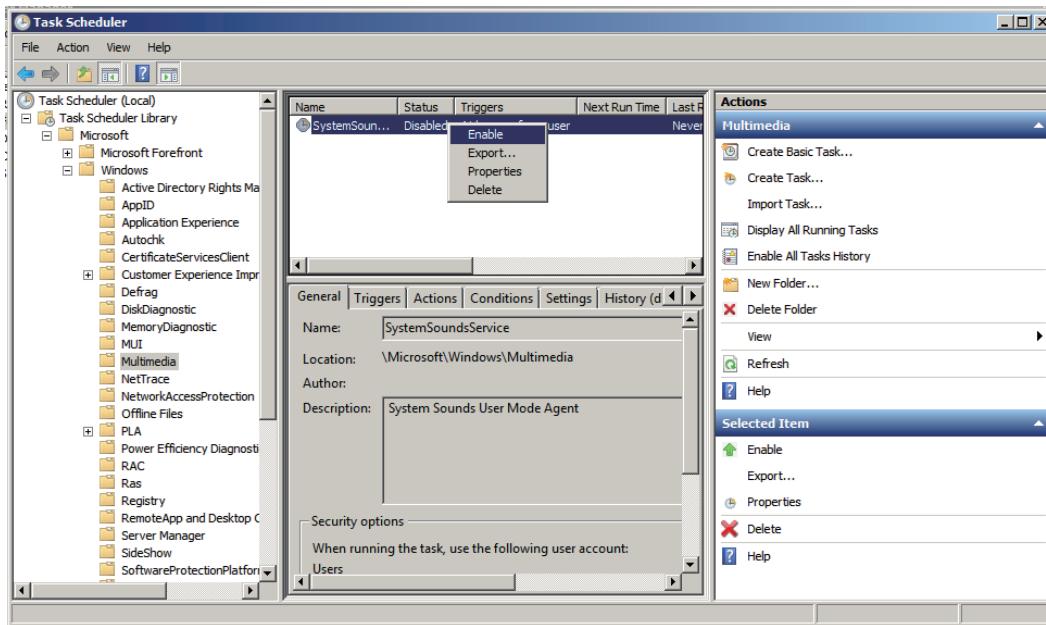


Figure B5.1.2-15 Task Scheduler Window – Enabling SystemSoundService

5. Right-click [SystemSoundService] and select [Run].

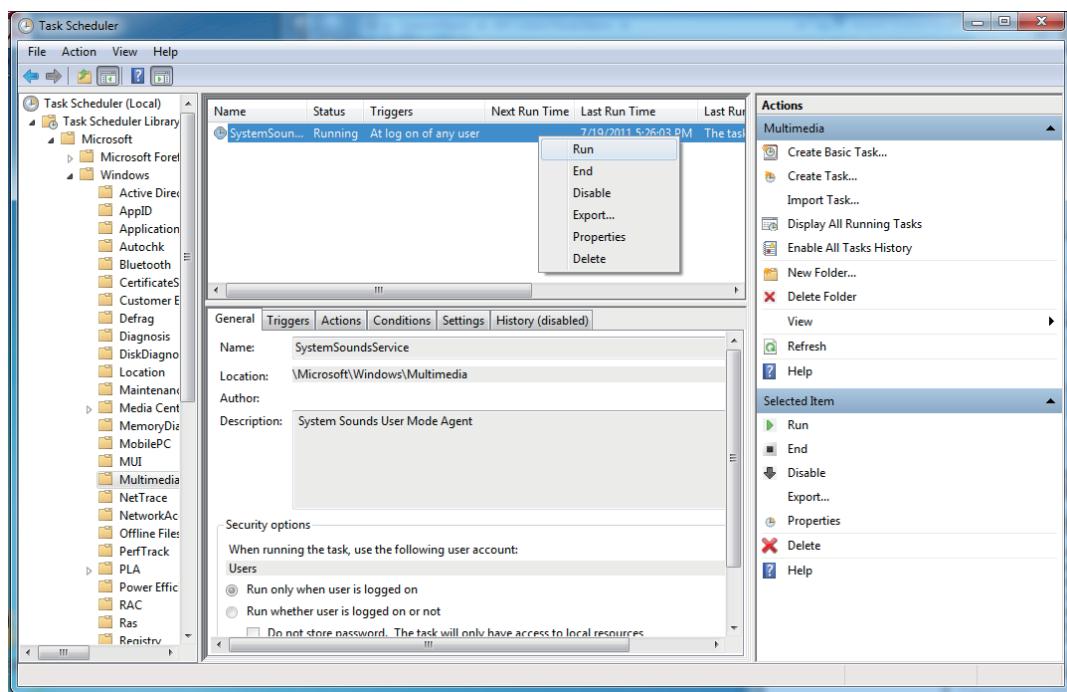


Figure B5.1.2-16 Task Scheduler Window – Running SystemSoundService

■ Procedure 7: Install the CENTUM VP Software

On the Remote Operation and Monitoring server, install the CENTUM VP software in the same way as the installation on HIS.

SEE ALSO

For more information about how to install the CENTUM VP software, refer to:

B4.6, “Installing the CENTUM VP Software” on page B4-85

■ Procedure 8: Configure IT Security Settings

After installing the CENTUM VP software, you need to configure security settings to strengthen the IT security of the computer.

SEE ALSO

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

B4.7, “Configuring IT Security Settings” on page B4-94

■ Procedure 9: Register Remote Desktop Users

After configuring the IT security settings, register the user or the user group to remotely logon to the “Remote Desktop Users” group. This section describes the procedure to register a RemoteCentum user to the “Remote Desktop Users” group.

1. Log on to the server computer using the Administrator account.
The Server Manager appears.
2. Select [Tools] > [Computer Management].
The Computer Management window appears.
3. Select [Computer Management] > [Local Users and Groups] > [Groups].
A list of groups appears.
4. Select and right-click “Remote Desktop Users” and select [Add to Group].

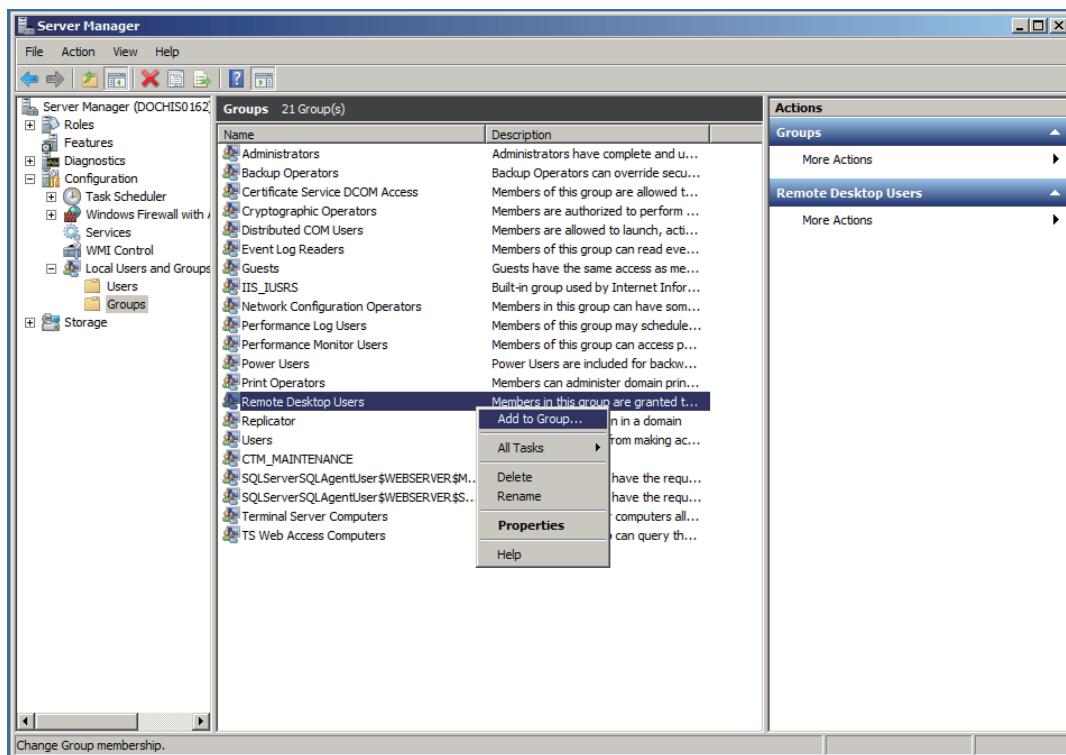


Figure B5.1.2-17 Computer Management Window

A list of Remote Desktop Users members appears.

5. On the [General] tab, click [Add].
The Choose user dialog box appears.
6. Click [Advanced].
The Advanced area appears additionally.
7. Click [Locations].
A list of locations appears.

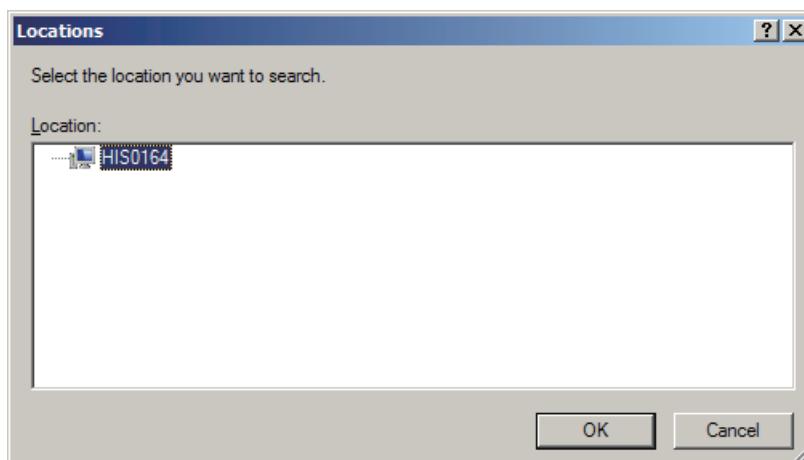


Figure B5.1.2-18 List of Locations

8. Select the name of the computer or domain to which the user you want to add belongs, and click [OK].
You are brought back to the Choose user dialog box.
9. Click [Find Now].
A list of users who belong to the selected computer or domain appears.

TIP

If you selected a domain name for the location, the list of users may not appear depending on the configuration of the domain. Also note that if the domain contains more than 10000 users, all users cannot be displayed in the list.

If this is your case, click [Cancel] to close the Advanced setting dialog box and type the user name in the [Enter the object names to select] box.

Example: When specifying a domain user: somedomain\RemoteCentum

When specifying a local user: HIS0164\RemoteCentum

10. Select the RemoteCentum user that you want to add and click [OK].
RemoteCentum is added to the Member of list.

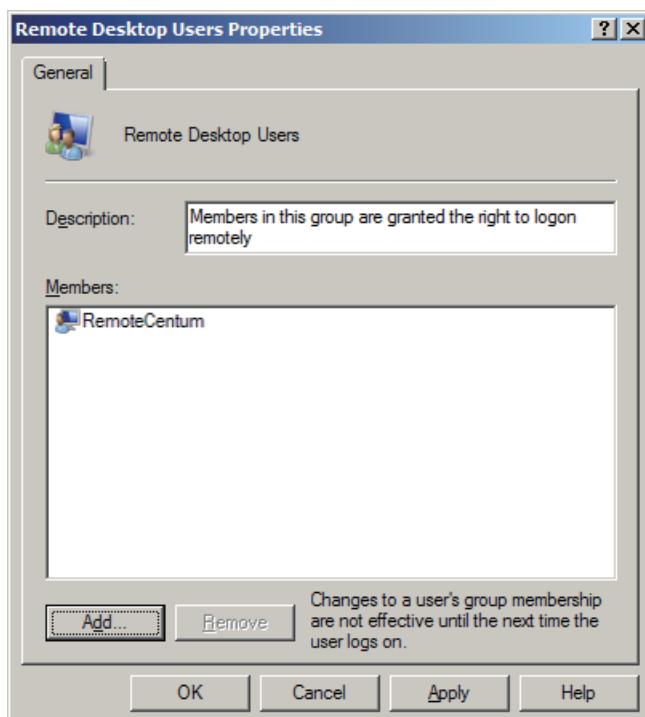


Figure B5.1.2-19 Properties of Remote Desktop Users

11. Click [OK].

■ Procedure 10: Distribute and Accept Licenses

From the license management station, distribute the licenses of the required packages in addition to the Server for Remote Operation and Monitoring Function, and accept them.

SEE

ALSO For more information about the procedure for distributing and accepting licenses, refer to:

B4.8, "Distributing and Accepting Licenses" on page B4-101

■ Procedure 11: Create User Accounts

You must create user accounts.

SEE

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

B4.9, "Creating User Accounts" on page B4-102

■ Procedure 12: Configure Windows Environment Settings for Each User

You need to configure the Windows operating environment settings for each user who logs on to the server.

SEE ALSO

For more information about the procedures for setting the Windows operating environment for each user, refer to:

B4.10, "Configuring Windows Environment Settings for Each User" on page B4-107

■ Procedure 13: Set User Authentication Mode

You need to configure settings for the user authentication mode.

SEE ALSO

For more information about the procedures for setting up for user authentication modes, refer to:

B4.11, "Setting Up for User Authentication Modes" on page B4-135

■ Procedure 14: Set Up the Uninterruptible Power Source (UPS)

To use an UPS, you need to configure the settings for it.

SEE ALSO

For more information about the procedure for setting up the UPS service, refer to:

B4.12, "Setting Up the Uninterruptible Power Supply (UPS) Service" on page B4-149

■ Procedure 15: Set Up RemoteApp Programs

To make the CENTUM VP operation and monitoring function available from a computer that connects remotely to the HIS-TSE server, you need to configure the remote desktop services.

● Adding StartDesktop.bat

1. Select [Server Manager] > [Roles] > [Remote Desktop Service] > [RemoteApp Manager].
The Server Manager appears.
2. From the Actions pane, click [Add RemoteApp Programs].
The RemoteApp Wizard starts.
3. Read the content on the wizard and click [Next].
The page for selecting programs appears.
4. Click [Browse].
The Choose a Program window appears.
5. Open StartDesktop.bat in the folder where the StartDesktop.bat file is located.
In the page for selecting programs to be added, the check box for [StartDesktop.bat] becomes selected.

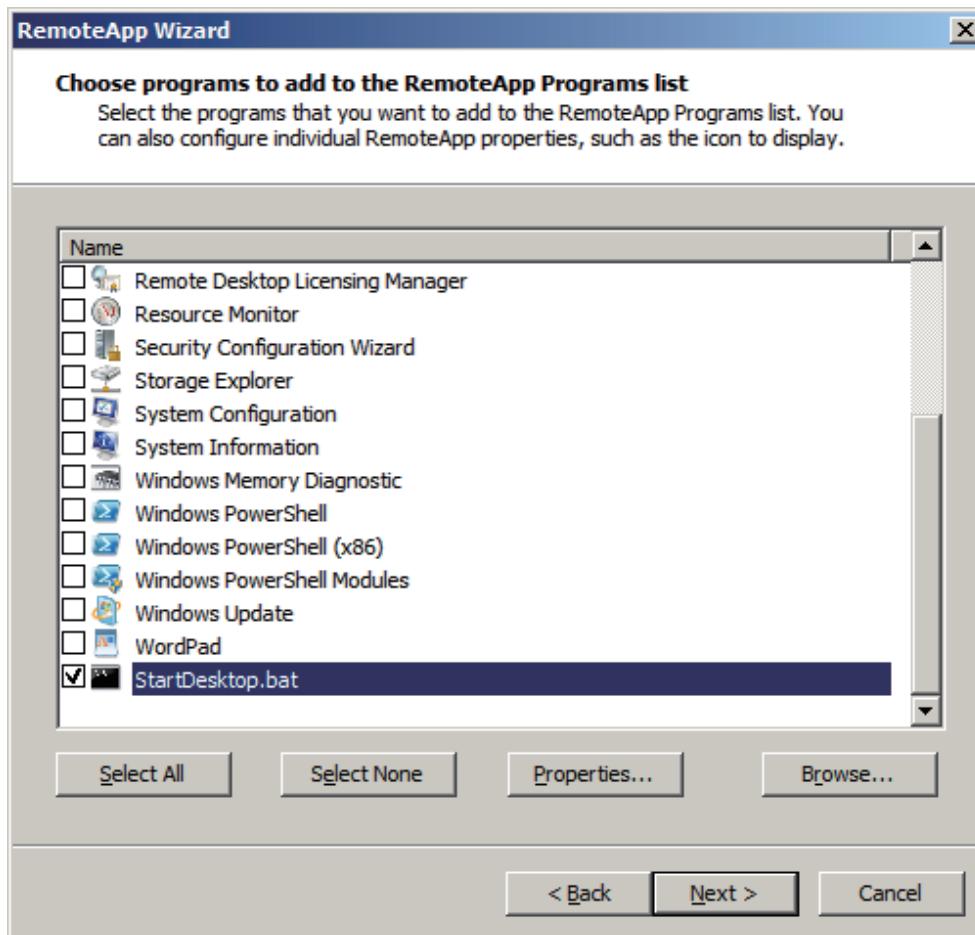


Figure B5.1.2-20 RemoteApp Wizard

TIP

If CENTUM VP is installed in C:\CENTUMVP, the StartDesktop.bat file is located in the C:\CENTUMVP\program program folder.

6. Confirm the displayed contents and click [Next].
The Review Settings page appears.

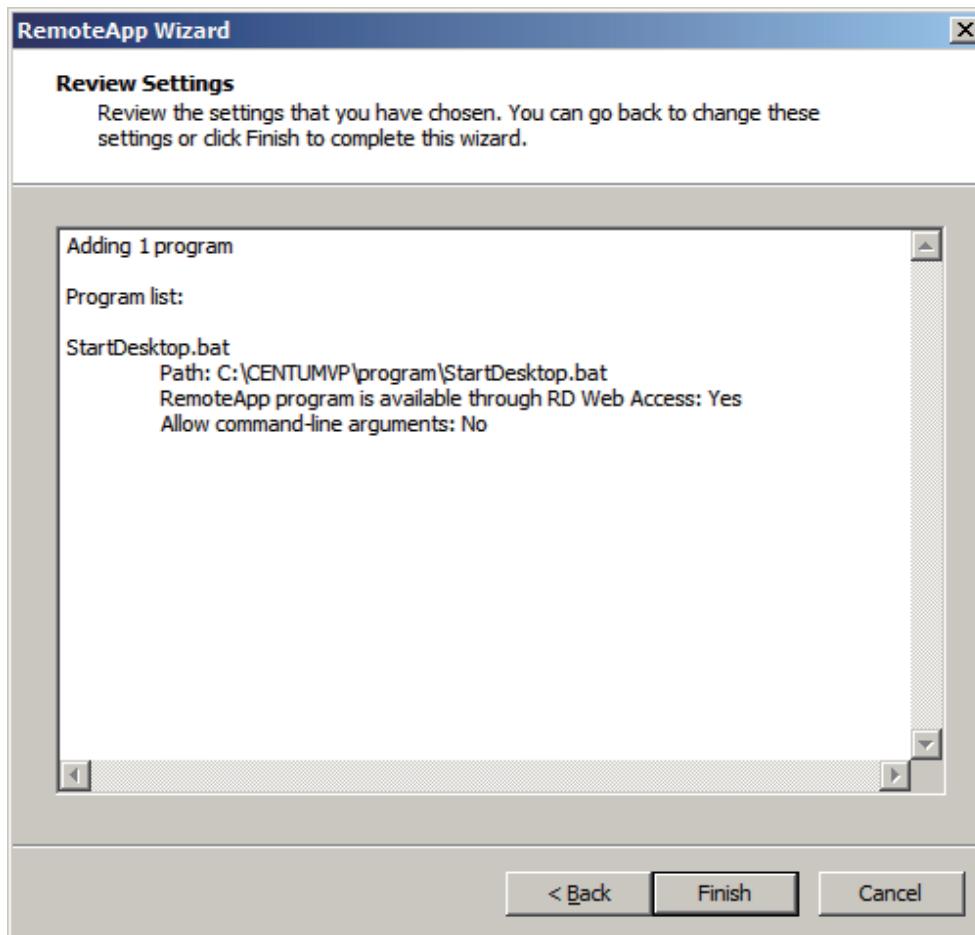


Figure B5.1.2-21 RemoteAppWizard - Review Settings

7. Confirm that the settings are the same as specified above, and click [Finish].
8. In the RemoteApp Manager pane, confirm that StartDesktop.bat has been added to the RemoteApp Programs table.

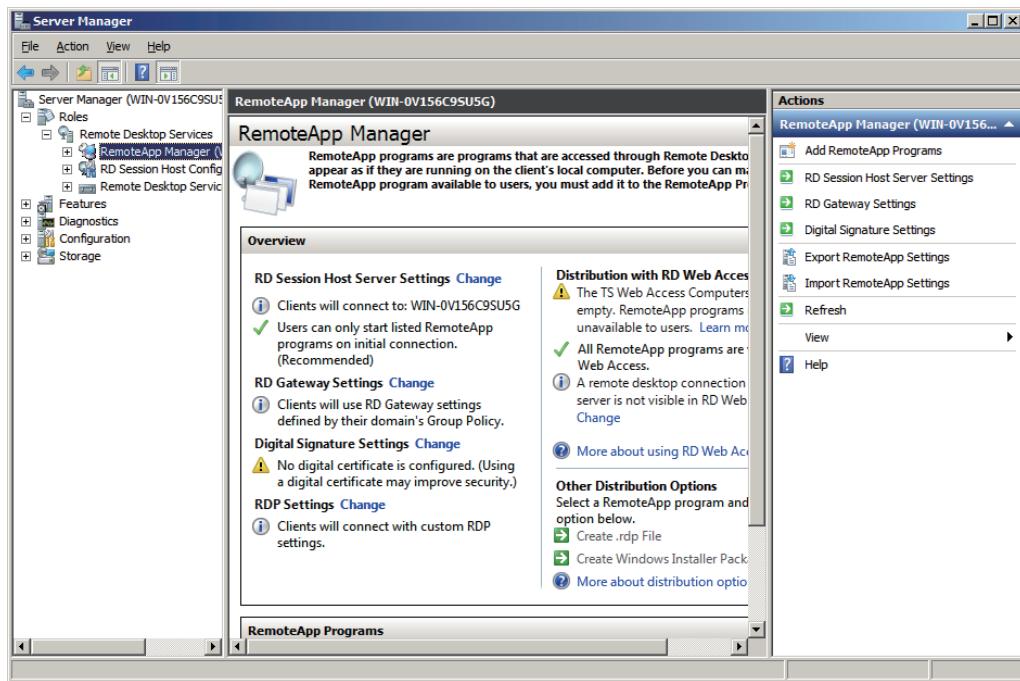


Figure B5.1.2-22 Server Manager - RemoteApp Manager

- **Add BKHBos.exe**

This setup is required only when running the Panel Mode.

1. Select [Server Manager] > [Roles] > [Remote Desktop Service] > [RemoteApp Manager]. The Server Manager appears.
2. In the Actions pane, click [Add RemoteApp Programs]. The RemoteApp Wizard starts.
3. Read the content on the wizard and click [Next]. The page for selecting programs appears.
4. Click [Browse]. The Choose a Program window appears.
5. Open BKHBos.exe in the folder where the BKHBos.exe file is located. In the page for selecting programs to be added, the check box for [BKHBos.exe] becomes selected.

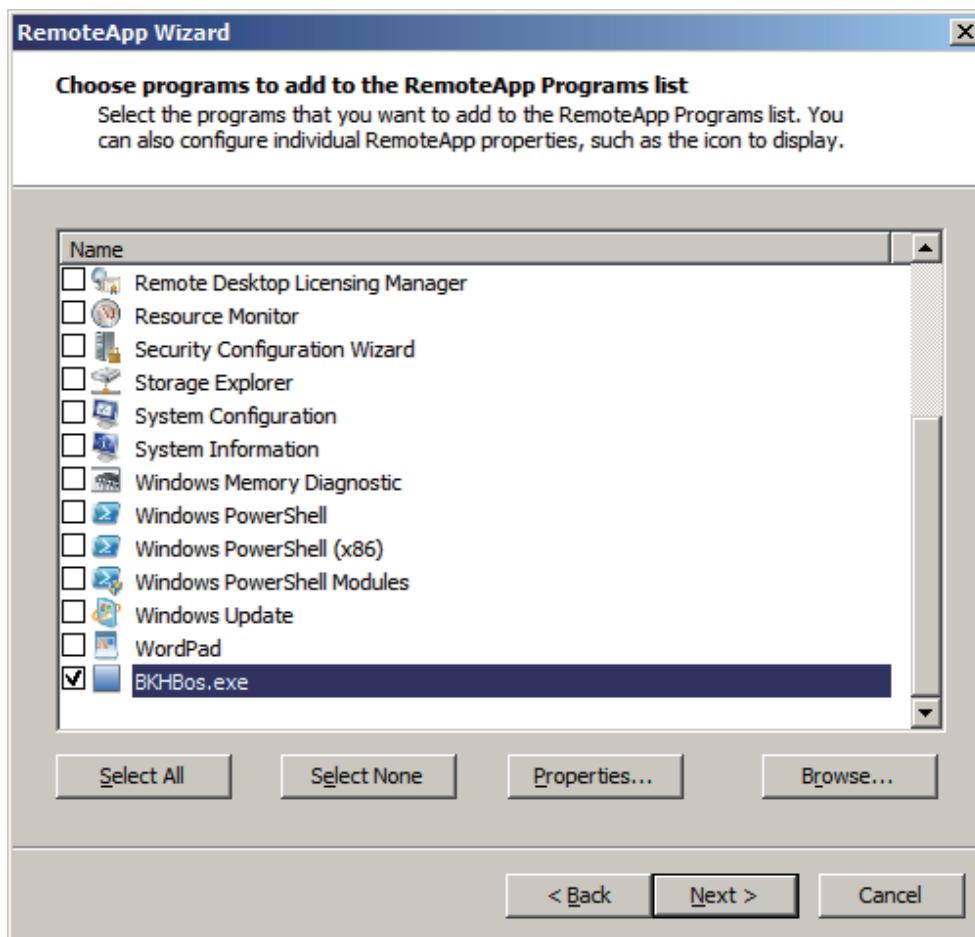


Figure B5.1.2-23 RemoteAPP Wizard

TIP

If CENTUM VP is installed on C:\CENTUMVP, the BKHBos.exe file is located in the C:\CENTUMVP program folder.

6. Upon confirming the above, click [Properties].
The BKHBOS.exe Properties dialog box appears.
7. In the Command-line Arguments section, select [Allow any command-line arguments] and click [OK].
A confirmation dialog box to continue the operation appears.
8. Click [Yes].
9. On the Remote App wizard, click [NEXT].
The page for confirming the settings appears.

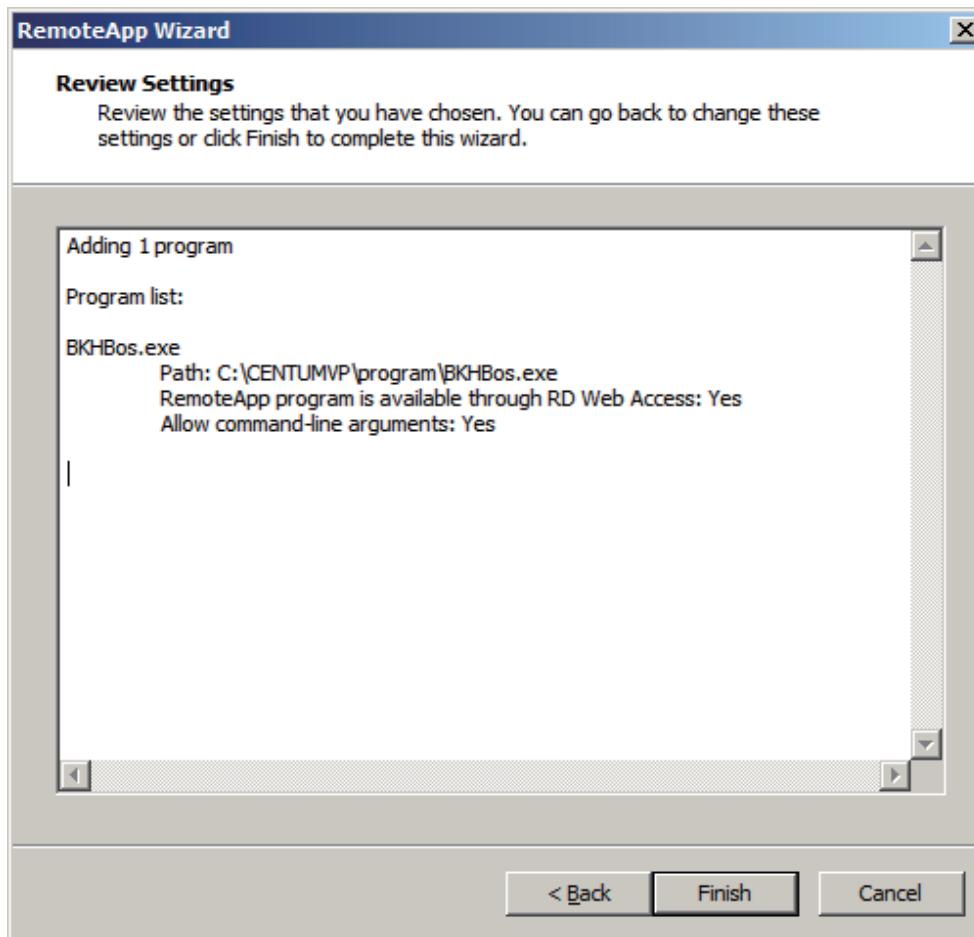


Figure B5.1.2-24 RemoteAPP Wizard - Review Settings

10. Confirm that the settings are the same as shown in the page above, and click [Finish].
11. In the RemoteApp Manager pane, confirm that BKHBOS.exe has been added to the RemoteApp program table and “Unrestricted” is indicated in the Arguments column.

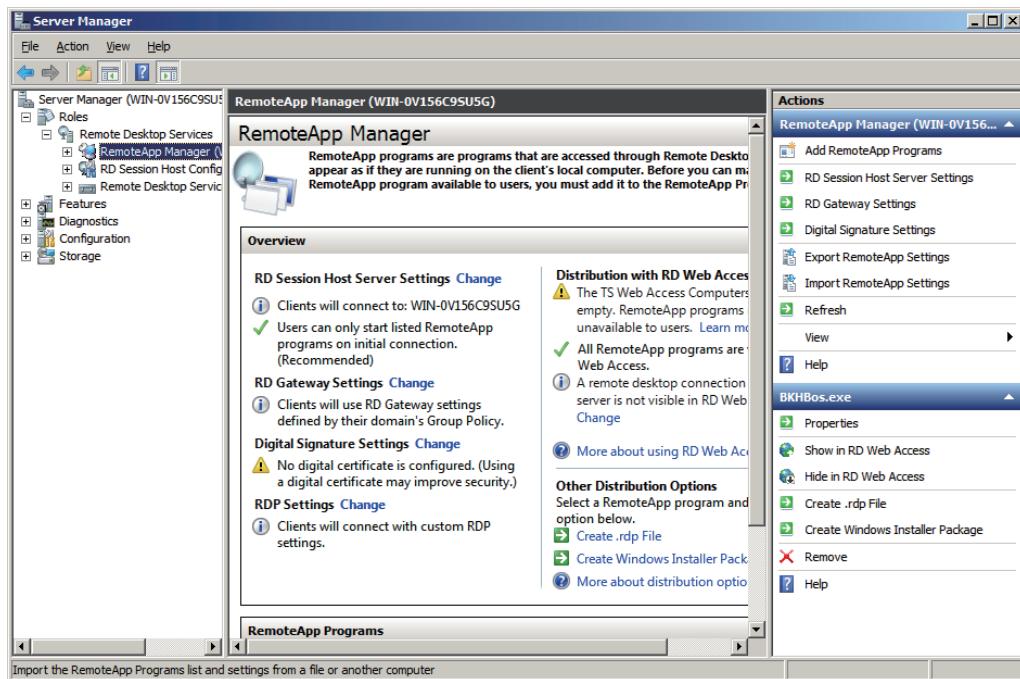


Figure B5.1.2-25 Server Manager - RemoteAPP Manager

■ Procedure 16: Set Up the Remote Desktop Service

1. Log on to the server computer using the Administrator account.
The Server Manager appears.
2. Select [Server Manager] > [Roles] > [Remote Desktop Services] > [RD Session Host Configurations].
The Server Manager appears.
3. In the Edit settings section, double-click [Restrict each user to a single session].
The Properties dialog box appears.

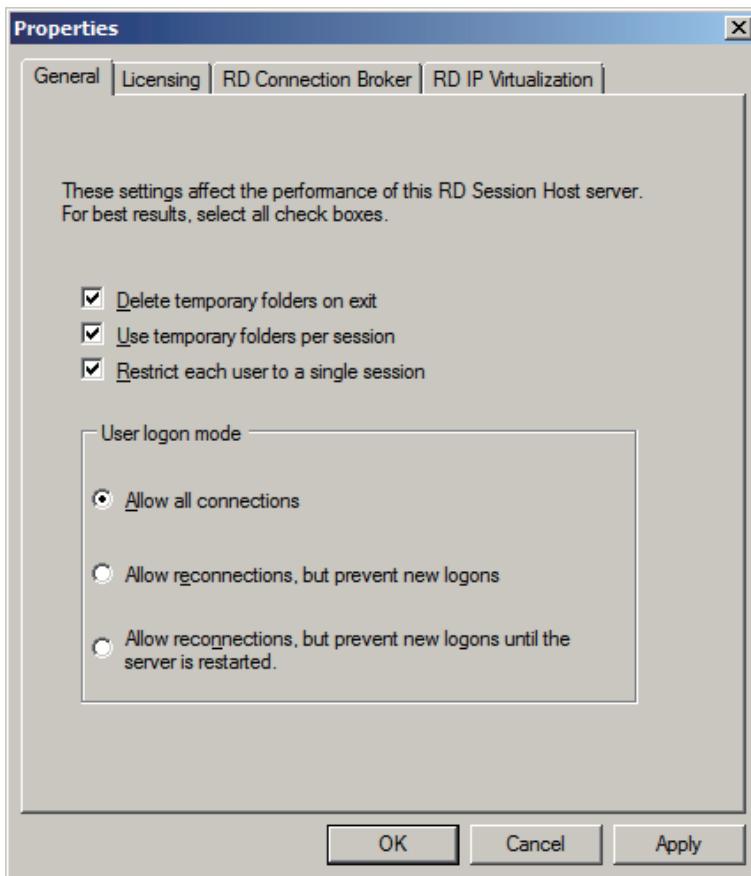


Figure B5.1.2-26 Properties Dialog Box

4. On the General tab, select or clear the check box for [Restrict each user to a single session] depending on the circumstance:
 - When the Legacy model of IT security settings are applied (always use the CENTUM account to log on), clear the check box.
 - When the Standard model of IT security settings are applied and operators log on using their individual names, select the check box.
5. On the Licensing tab, specify the remote desktop licensing mode (the number of connecting users and the number of connecting devices) based on the license usage condition.
6. Click [OK].
7. From the Connections section in the Server Manager window, right-click [RDP-Tcp] and select [Properties].
The Properties dialog box appears

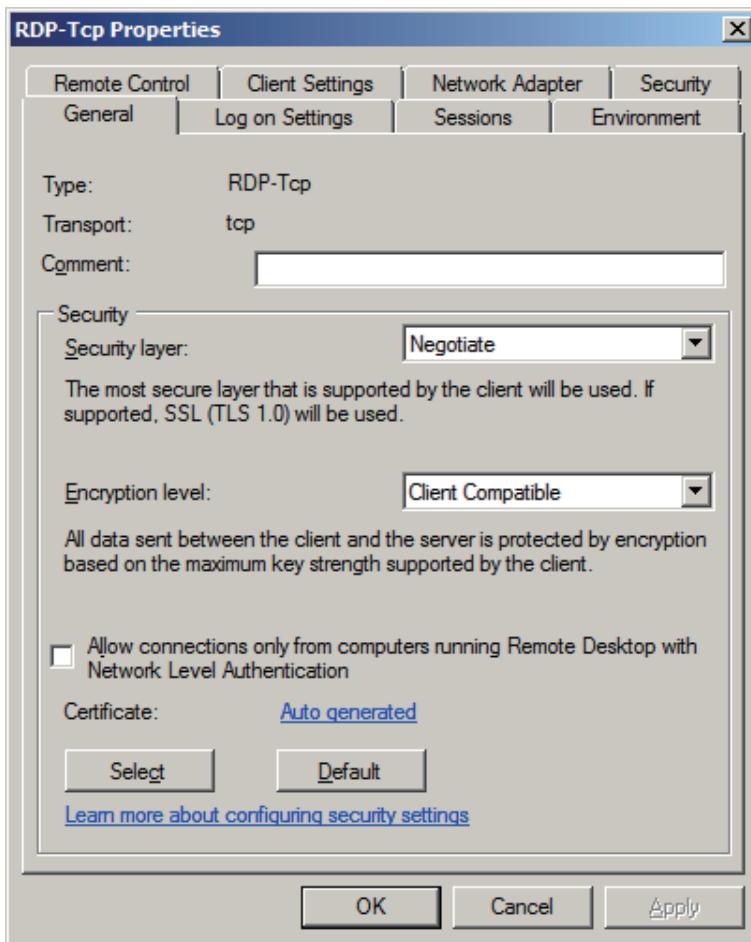


Figure B5.1.2-27 RDP-Tcp Properties Dialog Box

8. On the General tab, select the check box for [Allow connections only from computers running Remote Desktop with Network Level Authentication].

TIP

Leave the default settings for all other options unchanged.

9. On the Log on Settings tab, configure the settings based on the circumstances. Normally, you can leave it to the default setting of [Use client-provided log on information].

TIP

To restrict the account of the connecting client to a CENTUM user, select the [Always use the following log on information] check box. Enter CENTUM in [User name], and enter the password in [Password] and [Confirm password]. With this setting, the clients can only use the CENTUM account to logon. Even if the client option is set to logon using a different account, this setting will override any such setting and thus only CENTUM user can logon. When the password is not entered or the [Always prompt for password] check box is selected, the logon dialog box will be displayed when the client attempts to connect. Since the logon user name can be changed in this dialog box, the client can logon using an account other than the CENTUM account.

10. On the Sessions tab, select the check box for [Override user settings] and choose "1 minute" for [End a disconnected session].
11. On the Environment tab, configure the settings based on the circumstances. The default settings can be used.

TIP

When using the HIS TSE only in the Desktop mode, the HIS can be set to start automatically when connected to the HIS TSE server with the settings configured here.

In combination with the “Logon Settings,” the client can logon as a CENTUM user and the HIS can start automatically simply by specifying the connection target from the client program.

The setup procedure is as follows.

1. Select the check box for [Start the following program when the user log on].
2. Enter the path to the StartDesktop.bat file in the Program path and file name box.
If CENTUM VP is installed on C:\CENTUMVP, the path should be set to “C:\CENTUMVP\Program\StartDesktop.bat”.
3. In the Start in box, enter the path to the folder where the StartDesktop.bat file is located. If CENTUM VP is installed on C:\CENTUMVP, the path should be set to “C:\CENTUMVP\Program”.

As described in the dialog box, this setting will override the client setting. Therefore, if the StartDesktop.bat file is designated here, the HIS can only be started in the Desktop mode. (The StartDesktop.bat file is a batch file to be used to start the HIS in the Desktop mode.)

12. On the Remote Control tab, select [Do not allow remote control].
13. On the Client Settings tab, clear the check box for [Limit Maximum Color Depth] in the [Color Depth] section.
14. Also on the Client Settings tab, clear the check boxes for [Audio Recording] and [Audio and video playback] in the [Redirection] section.
15. On the Network Adapter tab, specify the network adapter to be used for the communications between the HIS TSE server and the client. Do not specify “Yokogawa Vnet/VLnet adapter.”
16. Click [OK].

■ Procedure 17: Add HIS-TSE to the Project

1. On the System View, open the project to which the HIS-TSE is to be added.
2. Add a station, specifying [HIS-TSE HIS with Server for Remote Operation and monitoring function] as the station type.
3. In the same procedures as those for the standard HIS, run the following download commands: [Download Project Common Section], [Download to HIS], and [Download Tag-List].
4. Restart the Remote Operation and Monitoring Server.

SEE ALSO

For more information about the builder definition items when a new HIS is created, refer to:

2.4.2, “Creating a New HIS” in Engineering Reference Vol.1 (IM 33J10D10-01EN)

B5.2 Setting Up HIS-TSE Clients

To use the server for remote operation and monitoring function, you need to set up HIS-TSE clients at the same time as the HIS-TSE server.

**SEE
ALSO**

For more information about setting up HIS-TSE clients, refer to:

7.1, "Remote Operation and Monitoring on HIS-TSE" in Optional Functions Reference (IM 33J05H10-01EN)

Blank Page

B6. 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, the project database created using system engineering builders and/or the recipe database are placed; and these databases can be accessed via the network.

TIP

For the FDA audit trail database, you need to prepare a computer dedicated for it.

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 HIS, a computer with only system builders or a computer with only AD Server
- Computer that serves as both a file server and a license management station

SEE ALSO

For more information about setting up the file server for the audit trail database, refer to:

4., “Access Control and Audit Trail Settings for Builders” in Compliance with FDA: 21CFR Part 11 (IM 33J10D21-01EN)

For more information about setting up the SOE server, refer to:

9., “SEM (Sequence of Events Manager) Function” in Optional Functions Reference (IM 33J05H10-01EN)

■ Item to be Prepared

Have the following item at hand before you set up a file server.

- CENTUM VP software medium

■ OS and Hardware Requirements for a File Server

The supported OS and the hardware requirements for a file server computer are as follows:

Table B6-1 Supported OS and Hardware Requirements for a File Server

Supported OS	Hardware requirements
Windows Server 2016 Standard Edition	CPU: 2 GHz minimum Memory: 2 GB or more Hard disk: 32 GB or more required. 50 GB or more recommended Drive: DVD-ROM Network adapter: Required Display: Super VGA (800 x 600) or higher resolution required
Windows Server 2012 R2 Standard Edition	CPU: 2 GHz minimum Memory: 2 GB or more Hard disk: 32 GB or more required. 50 GB or more recommended Drive: DVD-ROM Network adapter: Required Display: Super VGA (800 x 600) or higher resolution required

Continues on the next page

Table B6-1 Supported OS and Hardware Requirements for a File Server (Table continued)

Supported OS	Hardware requirements
Windows Server 2008 R2 Standard Edition SP1	CPU: 2 GHz minimum Memory: 2 GB or more Hard disk: 20 GB or more required. 50 GB or more recommended Drive: DVD-ROM Network adapter: Required Display: Super VGA (800 x 600) or higher resolution required
Windows Server 2008 Standard Edition SP2	CPU: 2 GHz minimum Memory: 2 GB or more Hard disk: 20 GB or more required. 50 GB or more recommended Drive: DVD-ROM Network adapter: Required Display: Super VGA (800 x 600) or higher resolution required

■ File System

Ensure that the file system is in the NTFS format.

B6.1 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 the administrative user shown in the following table.

Table B6.1-1 Administrative User Who Sets Up a File Server

Legacy Model	Security model and user management type to be applied	
	Standard Model	
	Standalone Management	Domain/Combination Management
Local user who belongs to the Administrators local group	Local user who belongs to the Administrators local group and CTM_MAINTENANCE local group	<ul style="list-style-type: none"> • Domain user who belongs to the Domain Admins domain group and CTM_MAINTENANCE domain group • Domain user who belongs to the Administrators local group and CTM_MAINTENANCE local group • Local user belonging to the Administrators local group and CTM_MAINTENANCE local group (*1)

*1: The domain user name and password must be entered during installation.

TIP

If the user management type is Domain or Combination management, perform the setup after the computer is added to the domain.

■ Procedure 1: Install Microsoft Visual C++ 2017 Redistributable Package

Before you can run the IT Security Tool, you must install the Microsoft Visual C++ 2017 redistributable package.

SEE ALSO

For more information about how to install Microsoft Visual C++ 2017 redistributable package, refer to:

“■ Installation of Microsoft Visual C++ 2017 Redistributable Package” on page B2-9

■ Procedure 2: Apply the Root Certificate

Before you install .NET Framework 4.6.2 in Windows Server 2008 R2, you must apply the root certificate.

TIP

This operation is not required for Windows Server 2016, Windows Server 2012 R2 and Windows Server 2008.

SEE ALSO

For more information about the procedure for applying the root certificate, refer to:

“■ Applying the root certificate” on page B4-41

■ Procedure 3: Install .NET Framework

Before the IT Security Tool can be run, .NET Framework of the following version must be installed:

- Windows Server 2008 R2: .NET Framework 4.6.2

- Windows Server 2008: .NET Framework 4.5.2

TIP

This operation is not required for Windows Server 2016 and Windows Server 2012 R2.

SEE ALSO

For more information about the procedure for installing the .NET Framework, refer to:

- “■ Installation of .NET Framework” on page B2-9

■ Procedure 4: Create an Administrative User

Create an administrative user according to the security model to be selected.

TIP

In the case of the Legacy model, this operation is not required because the setup can be performed by an existing user.

● Standard Model with Standalone Management

- Log on to Windows as a user with administrator rights.
- Create a CTM_MAINTENANCE group.
- Add the user to be set as the administrator to the Administrators and CTM_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 ProSafe-RS coexists, also add the user to the PSF_MAINTENANCE group.

● Standard Model with Domain/Combination Management

Follow these steps to designate a local group user as an administrator:

TIP

To use a domain group user as an administrative user, this operation is not required because the user already exists.

- Log on to Windows as a user with administrative rights.
- Create the CTM_MAINTENANCE local group.
- Add the domain user or local user to be set as the administrator to the Administrators local group and CTM_MAINTENANCE local group.

TIP

- If any other product coexists in the computer, the user also needs to be a member of the MAINTENANCE group of the coexisting product. For example, if ProSafe-RS coexists, also add the user to the PSF_MAINTENANCE group.
- After the IT Security Tool is run, the name of the CTM_MAINTENANCE group you have created will change to CTM_MAINTENANCE_LCL.

■ Procedure 5: 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:

Shared name: CTM_PJTS_DBSF

IMPORTANT

If the share 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. Log on as an administrative user.
2. Start Windows Explorer and create a folder in which the project folders are to be placed.
3. On the Sharing tab in the properties of the folder that is created, click [Advanced Sharing].
4. Select [Share this folder] and set CTM_PJTS_DBSF as the share name.
5. Click [Permissions], and grant full control to [Everyone] in the Share Permissions tab. 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, “CTM_PJTS_DBSF,” 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 “CTM_PJTS_DBSF” 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 “CTM_PJTS_DBSF” during configuration of IT security settings, unintended settings will be applied if the name “CTM_PJTS_DBSF” is not assigned to appropriate folders.

If the IT security settings are applied to an unintended folder, delete the permissions set up in the IT security settings, and specify the original access permission setting based on the setting of another folder, such as the C:\Windows folder.

■ Procedure 6: Save the IT Security Settings on the File Server

IMPORTANT

- Before you run the IT Security Tool to configure IT security settings for the first time, be sure to save the security settings on the computer.
- On a file server, when changing the IT security settings, use the initial data saved beforehand to restore the security settings, and then apply them again.

Therefore, the following saved data of IT security settings must be required.

- When the user management type is Standalone management in Standard model:
Data saved before the first application of IT security settings in the standalone state
- When the user management type is Domain management or Combination management in Standard model:
Data saved before applying IT security settings after adding to the domain
- For the second and subsequent security settings, it is basically unnecessary to save the security settings. However, save the initial data of security settings again in the following cases.
 - Configure the security settings by using the IT Security Tool of R5.01 to R6.03, and then change the IT security version to 2.0 by using the IT Security Tool of R6.04 or later.
 - Configure the security settings by using the IT Security Tool earlier than R4.03, and then change the IT security version, security model or selected condition of any setting item, by using the IT Security Tool of R5.01 or later.
- To save the initial security setting data again, restore the security settings that were saved before by using the IT Security Tool. If the file server is a member of the domain, determine which of the two sets of initial data will be recovered based on whether or not to keep the file server as the member of the domain. Then, perform this procedure to save the security settings. From then on, the data you have saved again will be used when the security settings are initialized; accordingly, keep the saved data in a safe place.

Follow these steps to save the security settings:

1. Log on as an administrative user.
2. Insert the CENTUM VP 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.

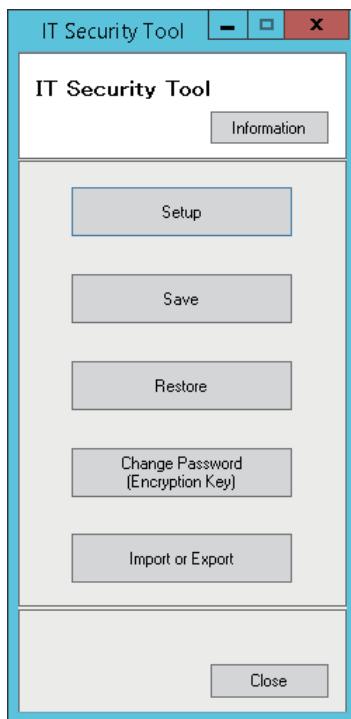


Figure B6.1-1 IT Security Tool Menu

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.

4. Click [Save].
The Specify destination page appears.
5. Specify the destination folder and enter following setting items.
 - Distinguished Name
 - Support Product
 - Support OS
 - File Version

TIP

The [Distinguished Name] and [File Version] are ommissible.

6. Click [Next].
The Type default account password page appears.
7. Enter the password for use as the initial account password and click [Next].
The Type password (Encryption Key) page appears.

TIP

This initial password will be set when the account saved with this tool is recovered. If the saved accounts are not found on the computer when you recover the accounts, new accounts are created. This password will be set as the initial password for the newly created account.

Even when multiple accounts have been created, the same initial password is assigned to all.

If the set password does not meet the password policy in the environment where the account is to be recovered, an error will occur when recovering an account.

This password is set as the initial password for the account. Accordingly, you will be prompted to change the password when you log on for the first time using this account.

8. Enter the password for encrypting the saved data, and 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.

9. When the saving is completed, click [Finish].
If the saving failed, the details of the failure are displayed.
10. On the IT Security Tool menu, click [Close].

TIP

If any save failures are displayed, contact YOKOGAWA Service.

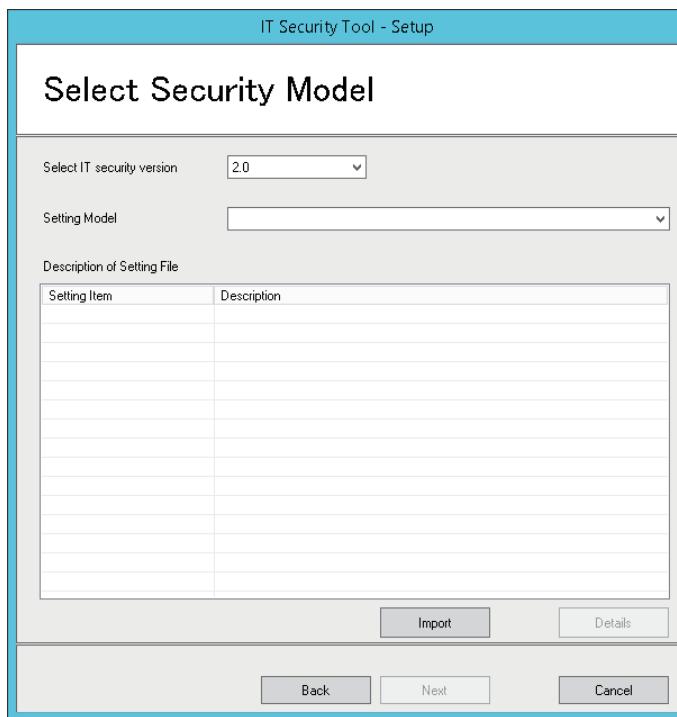
■ Procedure 7: Configure the IT Security Settings on the File Server

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 B6.1-2 Select Security Model**

3. From the Select IT security version drop-down list, select the IT security version.
4. From the Setting Model drop-down list, select a security model for the file server.
You can select from the following four models:

Table B6.1-2 Security Models for a File Server

Model	Description
File Server Legacy Model (*1)	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.

*1: If you select [2.0] for Select IT security version, you cannot select the file server legacy model.

5. Click [Next].
The Confirm Setting Information page appears.

TIP

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

6. The subsequent steps are the same as those for the IT security setting configuration after installing the CENTUM VP software.

SEE ALSO

For more information about the procedure for importing the IT security settings, refer to:

6.7, "Importing/Exporting the IT Security Setting File" in CENTUM VP Security Guide (IM 33J01C30-01EN)

For more information about the IT security setting operations that are performed following the CENTUM VP software installation, refer to:

B4.7, "Configuring IT Security Settings" on page B4-94

■ Procedure 8: 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 on the computers that access the projects.
2. Register the user you have created to the same group as that on the computers which access the file server.

TIP

If the Standard model is applied, the following user groups have been created by running the IT Security Tool in Procedure 7.

- CTM_OPERATOR
- CTM_ENGINEER
- CTM_OPC
- CTM_ENGINEER_ADM
- ADS_MANAGER

■ Procedure 9: Create the Project Folder on the File Server

1. On a computer installed with system builders, create a CENTUM project under the shared folder, "CTM_PJTS_DBSF", that was created in Procedure 5.
2. Log on to the file server using an administrative user account, and select the CENTUM project folder created in step 1.
3. On the Sharing tab in the folder's properties dialog box, click [Advanced Sharing].
4. Select the [Share this folder] check box, and add the following shared name in the Share name box:
 - CS1000PJT to share the project database
 - CTMRMNG to share the recipe builder databaseA sharing name is not required for the audit trail database.
5. Click [Permissions] to open the Permission dialog box.
6. Grant full control to [Everyone].

B6.2 Setting Up the File Server Function on an HIS, a Computer with Only System Builders or a Computer with Only AD Server

This section describes the required settings when you use a computer that has been set up as an HIS, a computer with only system builders or a computer with only AD Server.

TIP

On a computer with only system builders, the project database is created under the installation folder by default. You need to use the procedure described in this section if the project database is placed in a location other than the installation folder.

1. Set up a computer as an HIS, a computer with only system builders or a computer with only AD Server.

TIP

You do not need to configure security settings at this point.

2. On the computer, create and set up the shared folder.
3. Start the IT Security Tool 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 HIS, a computer with only system builders or a computer with only AD Server, 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 new setup of HIS, a computer installed with system builders or a computer installed with AD server, refer to:

B4., “Setting Up CENTUM Stations or Computers” on page B4-1

For more information about the shared folder settings, refer to:

“■ Procedure 5: Create and Set Up the Shared Folders” on page B6-4

For more information about creating accounts for users who access the project database, refer to:

“■ Procedure 8: Create Accounts on the File Server for Users who Access Project Data” on page B6-10

For more information about how to create the project folder on the file server, refer to:

“■ Procedure 9: Create the Project Folder on the File Server” on page B6-10

B6.3 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 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:

B7., “Setting Up the Computer Dedicated to License Management” on page B7-1

For more information about the shared folder settings, refer to:

“■ Procedure 5: Create and Set Up the Shared Folders” on page B6-4

B7. 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.

- CENTUM VP software medium

■ Administrative User who Performs the Installation

The administrative users shown in the following table should install the license management software:

Table B7-1 Administrative User Who Installs the License Management Software

Legacy Model	Security model and user management type to be applied	
	Standard Model	Standalone Management
Local user who belongs to the Administrators local group	Local user who belongs to the Administrators local group	<ul style="list-style-type: none"> • Domain user who belongs to the Domain Admins domain group • Domain user who belongs to the Administrators local group • Local user belonging to the Administrators local group (*1)

*1: The domain user name and password must be entered during installation.

TIP

If the user management type is Domain or Combination management, install the software after the computer is added to the domain.

■ Setting Up a License Management Station

This section describes the procedure for setting up a license management station.

● Set Up Windows

Configure Windows settings for the following features according to the OS version:

- File System: All Windows versions
- Power Options: All Windows versions
- Turning off fast startup Windows 10
- Windows Defender: Windows 10, Windows 7
- Windows Update: Windows 10
- Disk Defragmenter: Windows 10, Windows 7
- Root certificate: Windows 7, Windows Server 2008 R2

SEE ALSO

For more information about the procedure for configuring each Windows setting item, refer to:

B4.2, "Setting Up Windows" on page B4-7

● Install the License Management Software

Follow these steps to install the license management software.

1. Log on using an administrative user account.
2. Insert the CENTUM VP 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 CENTUM VP software medium.

The installation menu appears.

3. Click [Install License Manager Software].
The Welcome dialog box appears.

TIP

If the Windows redistributable modules required to run CENTUM VP, such as Microsoft .NET Framework, are not already installed, a dialog box appears, prompting you to install such modules.

Click [Install] to install them. If you click [Cancel], the installation of the CENTUM VP software is discontinued.

The following modules are required for CENTUM VP.

- Microsoft .NET Framework 4.6.2
- MSXML 6.0 SP1
- Microsoft Visual C++ 2017 Redistributable Package
- OPCCOM ProxyStub

When installation of these modules is started, the display in the status field changes accordingly. Restarting the computer may be required after installing the modules. If required, restart the computer and then continue the CENTUM VP installation after the computer is restarted.

4. Click [Next].
The User Information dialog box appears.
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 installation setting confirmation 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 then starts.
8. Go on to configure the security settings.

TIP

When deleting the CENTUM VP function and installing only the license management software after installing CENTUM VP, first log on using an administrative user account and uninstall CENTUM VP, 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 the settings on the User Information dialog box, refer to:

B4.6, "Installing the CENTUM VP Software" on page B4-85

For more information about IT security, refer to:

B4.7, "Configuring IT Security Settings" on page B4-94

For more information about how to uninstall the CENTUM VP software, refer to:

C7.1.3, "Uninstalling the CENTUM VP Software" on page C7-10

● **Create User Accounts**

Create accounts for the users who manage licenses.

**SEE
ALSO**

For more information about creating user accounts, refer to:

B4.9, "Creating User Accounts" on page B4-102

For more information about the user who manages licenses, refer to:

1.2.2, "User privileges in License Manager" in License Management (IM 33J01C20-01EN)

● **Configure Windows Environment Settings for Each User**

Configure Windows settings for the following features according to the OS version:

- Windows security center/action center alerts: All Windows versions
- Scrolling: Windows 10
- Virtual desktops: Windows 10

**SEE
ALSO**

For more information about the procedure for configuring each Windows setting item, refer to:

B4.10, "Configuring Windows Environment Settings for Each User" on page B4-107

Blank Page

B8. Setting Up a Virtualization Environment

This section describes the settings that are required to run CENTUM VP functions in a virtual machine.

B8.1 SIOS

Set the metric value of the network card that matches with the Ethernet IP address specified with SIOS station property definition in System View to a minimum value.

If you change the metric value of network in a virtual machine, you must set the metric value of the above network card to the minimum value.

If the plant information network is present separately from the above network card, you must set the metric value of the plant information network to the second smallest value after the above network card.

**SEE
ALSO**

For more information about how to change the metric value of the network, refer to:

- [“Changing the network metric values” in B1.4, “Configuring system products after installing” in Virtualization Platform Setup \(IM 30A05B20-01EN\)](#)
-

B8.2 HIS

This section describes the following settings.

- Settings for using USB devices
- Settings for limiting maximum number of connections
- Settings for limiting sessions per user
- Settings for enabling beep
- Settings for buzzer

B8.2.1 Settings for Using USB Devices

To use USB devices, setting works are separately required in thin client, in the virtualization host computer, in virtual machines, and in HIS on the virtual machine.

■ Configuring in a thin client running on Windows OS

This section describes settings in a thin client that runs on Windows OS.

- **Installing the USB Driver for Operation Keyboard**

If you want to use the USB operation keyboard, connect a USB DVD drive to the thin client and install the USB driver for operation keyboard.

SEE ALSO

For more information about installing the USB driver for the operation keyboard, refer to:

B4.4, “Installing the USB Driver for the Operation Keyboard” on page B4-77

For more information about uninstalling the USB driver for operation keyboard, refer to:

“■ Uninstalling the USB Driver for OPKB” on page C7-17

- **Adding settings associated with the operation keyboard to the file for connection settings**

Follow these steps to add the settings associated with the operation keyboard to the setting file for connecting to virtual machines:

1. Sign in to thin client as an administrative user.
2. Right-click the file that the settings for connecting virtual machines and select [Edit].
3. Click [Show Options].
4. Click the Local Resources tab.
5. In the Local devices and resources box, click [More].
6. Select the [Other supported RemoteFX USB devices] > [USB AUDIO DAC] check boxes.
7. Select the [Other supported RemoteFX USB devices] > [Yokogawa OPKB Device] check boxes.
8. Click the General tab.
9. In the Connection settings box, click [Save].
10. Close Remote Desktop Connection.

SEE ALSO

For more information about how to create a setting file for connecting to virtual machines, refer to:

C1.1.4, “Configuring connection settings” in Virtualization Platform Setup (IM30A05B20-01EN)

■ Settings in the Host OS on the Virtualization Host Computer

This section describes the settings in the host OS on the virtualization host computer.

- **Changing the Local Group Policy**

Follow these steps to change the local group policy:

1. Sign in to the virtualization host computer as an administrative user.
2. Open Command Prompt and type `gpedit.msc`.
Local Group Policy Editor appears.

3. In the left pane, select [Computer Configuration] > [Administrative Templates] > [Windows Components] > [Remote Desktop Services] > [Remote Desktop Connection Client], and click [RemoteFX USB Device Redirection].
4. In the right pane, double-click [Allow RDP redirection of other supported RemoteFX USB devices from this computer].
The Properties dialog box appears
5. Select [Enabled], and select [Administrators and Users] in [RemoteFX USB Redirection Access Rights].
6. Click [OK].
7. Restart the virtualization host computer.

● Configuring the Hyper-V Setting

Follow these steps to use the enhanced session mode of Hyper-V:

1. Select [Start] > [Server Manager].
Server Manager starts.
2. Select [Tools] > [Hyper-V Manager].
Hyper-V Manager starts.
3. Right-click the host computer name and select [Hyper-V Settings].
4. In the [Enhanced Session Mode Policy] section, select [Allow enhanced session mode] and click [OK].

● Installing the USB Driver for Operation Keyboard

This operation is required only when the USB driver for operation keyboard is used as an USB device.

Follow these steps to install the USB driver for operation keyboard:

1. Connect the operation keyboard to the virtualization host computer.
2. Install the USB driver for operation keyboard on the virtualization host computer.

SEE ALSO

For more information about installing the USB driver for the operation keyboard, refer to:

“Installing the USB Driver for the Operation Keyboard” on page B4-77

For more information about uninstalling the USB driver for operation keyboard, refer to:

“Uninstalling the USB Driver for OPKB” on page C7-17

■ Settings in the Guest OS on the Virtual Machine

You must configure the settings described here after you configure the settings in the host OS on the virtualization host computer.

● Installing the Remote Desktop Session Host Role Service

Follow these steps to install the Remote Desktop Session Host role service:

1. Sign in to the guest OS on the virtual machine as an administrative user.
2. Select [Start] > [Server Manager].
Server Manager starts.
3. Select [Manage] > [Add Roles and Features].
The Add Roles and Features Wizard appears.
4. Select [Installation Type] in the left pane and select [Role-based or feature-based installation] in the right pane.

5. Select [Server Selection] in the left pane, select [Select a server from the server pool] in the right pane, and select the computer to install.
6. Select [Server Roles] in the left pane and select [Remote Desktop Services] check box in the right pane.
7. Select [Remote Desktop Services] > [Role Services] in the left pane and select [Remote Desktop Session Host] check box in the right pane.
A dialog box appears.
8. Select [Include management tools (if applicable)] check box in the dialog box and click [Add Features].
9. Select [Confirmation] in the left pane and select [Install] in the right pane.
The installation of service starts.
10. When the installation is complete, click [Close].
11. Restart the virtual machine.

● **Installing Remote Desktop Licensing Role Service**

Follow these steps to install the Remote Desktop Licensing role service:

1. Sign in to the guest OS on the virtual machine as an administrative user.
2. Select [Start] > [Server Manager].
Server Manager starts.
3. Click [Manage] > [Add Roles and Features].
The Add Roles and Features Wizard appears.
4. Select [Installation Type] in the left pane and select [Role-based or feature-based installation] in the right pane.
5. Select [Server Selection] in the left pane, select [Select a server from the server pool] in the right pane, and select the computer to install.
6. Select [Server Roles] in the left pane and select [Remote Desktop Services] > [Remote Desktop Licensing] check box in the right pane.
7. If a dialog box appears, select [Include management tools (if applicable)] check box in the dialog box and click [Add Features].
8. Select [Confirmation] in the left pane and select [Install] in the right pane.
The installation of service starts.
9. When the installation is complete, click [Close].

● **Specifying the Remote Desktop Licensing Server**

Follow these steps to specify the Remote Desktop Licensing server:

1. Sign in to the guest OS on the virtual machine as an administrative user.
2. Open Command Prompt and type `gpedit.msc`.
Local Group Policy Editor appears.
3. In the left pane, select [Computer Configuration] > [Administrative Templates] > [Windows Components] > [Remote Desktop Services] > [Remote Desktop Session Host], and double-click [Licensing].
4. In the right pane, double-click [Use the specified Remote Desktop licensing servers].
The Properties dialog box appears.
5. Select [Enabled] and enter the computer name or IP address of the license server to the [License server to use].
6. Click [OK].

7. In the right pane, double-click [Settings of Remote Desktop licensing mode].
The Properties dialog box appears.
8. Select [Enabled] and select [Per Device] in the [Specify the licensing mode for the RD Session Host server].
9. Click [OK].

● **Activate Remote Desktop Licensing Server**

Follow these steps to activate the Remote Desktop Licensing server:

1. Sign in to the guest OS on the virtual machine as an administrative user.
2. Select [Start] > [Server Manager].
Server Manager starts.
3. Select [Tools] > [RD Licensing Manager].
The RD Licensing Manager starts.
4. Select the computer to be activated in the left pane, and select [Action] > [Activate Server] from the menu bar.
The Activate Server Wizard appears.
5. Follow the instructions of the Wizard and activate the server.

● **Changing the Local Group Policy**

Follow these steps to change the local group policy:

1. Sign in to the guest OS on the virtual machine as an administrative user.
2. Open Command Prompt and type `gpedit.msc`.
Local Group Policy Editor appears.
3. In the left pane, select [Computer Configuration] > [Administrative Templates] > [Windows Components] > [Remote Desktop Services] > [Remote Desktop Session Host], and click [Device and Resource Redirection].
4. In the right pane, double-click [Do not allow supported Plug and Play device redirection].
The Properties dialog box appears
5. Select [Disabled] and click [OK].
6. Restart the virtual machine.

● **Installing the USB Driver for Operation Keyboard**

This operation is required only when the USB driver for operation keyboard is used as an USB device.

Follow these steps to install the USB driver for the operation keyboard on the virtual machine:

1. Connect the operation keyboard to the virtualization host computer.
2. Select [Start] > [Server Manager].
Server Manager starts.
3. Select [Tools] > [Hyper-V Manager].
Hyper-V Manager starts.
4. In the right pane, select and right-click the virtual machine to connect and select [Connect].
The Connection dialog box appears.
5. Select [Show Options].
6. Open the Local Resources tab, click [More] in [Local devices and resources].

7. Select [Other supported RemoteFX USB devices] > [Yokogawa OPKB Device] check box of , and click [OK].
8. Click [Connect].
9. Start Device Manager of the virtual machine, and confirm that [Other device->Unknown device] is displayed.
10. Install the driver for operation keyboard.

SEE ALSO

For more information about installing the USB driver for the operation keyboard, refer to:

B4.4, “Installing the USB Driver for the Operation Keyboard” on page B4-77

For more information about uninstalling the USB driver for operation keyboard, refer to:

“■ Uninstalling the USB Driver for OPKB” on page C7-17

■ Settings in HIS on the Virtual Machine

When using operation keyboard, set Configuration Operation Keyboard on the [Action] tab to [USB] by using HIS Utility in the virtual machine.

SEE ALSO

For more information about HIS Utility, refer to:

1.2, “The Settings on HIS Utility” in Human Interface Stations Reference Vol.1 (IM 33J05A10-01EN)

B8.2.2 Settings for Limiting Maximum Number of Connections

Specify the limit of concurrent connection in the guest OS on the virtual machine.

Follow these steps to configure the limit of maximum number of connections:

1. Sign in to the guest OS on the virtual machine as an administrative user.
2. Open Command Prompt and type `gpedit.msc`.
Local Group Policy Editor appears.
3. In the left pane, select [Computer Configuration] > [Administrative Templates] > [Windows Components] > [Remote Desktop Services] > [Remote Desktop Session Host] > [Connections].
4. In the right pane, double-click [Limit number of connections].
The Properties dialog box appears.
5. Select [Enabled] and set the [RD Maximum Connections allowed] to 1.
6. Click [OK].
7. Restart the virtual machine.

B8.2.3 Settings for Limiting Sessions Per User

Specify the number of sessions per user in the guest OS on the virtual machine.

Follow these steps to configure the limit of sessions per user:

1. Sign in to the guest OS on the virtual machine as an administrative user.
2. Open Command Prompt and type `gpedit.msc`.
Local Group Policy Editor appears.
3. In the left pane, select [Computer Configuration] > [Administrative Templates] > [Windows Components] > [Remote Desktop Services] > [Remote Desktop Session Host] > [Connections].
4. In the right pane, double-click [Restrict Remote Desktop Services users to a single Remote Desktop Services session].
The Properties dialog box appears.
5. Select [Disabled] and click [OK].
6. Restart the virtual machine.

B8.2.4 Enabling Beep

Enable beep in the guest OS on the virtual machine.

■ Enabling Audio Service

**SEE
ALSO**

For more information about steps for enabling audio service, refer to:

- “■ Procedure 7: Set up Audio” on page B5-7
-

■ Run the System Sound Service

**SEE
ALSO**

For more information about steps to run the system sound service, refer to:

- “● Run the System Sound Service” on page B5-9
-

B8.2.5 Settings for Buzzer

When you use operation keyboard, set the type of [Buzzer Switching] to [Operation Keyboard] in the Buzzer tab of HIS Setup window.

When you do not use operation keyboard, set the type of [Buzzer Switching] to [Advanced Sound] in the Buzzer tab of HIS Setup window.

B8.3 HIS-TSE

This section describes the following settings.

- Settings for using USB devices
- Settings in the guest OS on the virtual machine
- Settings for limiting maximum number of connections
- Settings for limiting sessions per user
- Settings for application and working directory

Steps for uninstalling HIS-TSE in a virtualization environment are also provided.

B8.3.1 Settings for Using USB Devices

Specify these settings to use USB devices in HIS-TSE.

- Settings in thin client
- Settings in the host OS on the virtualization host computer
- Settings in the guest OS on the virtual machine

**SEE
ALSO**

For more information about steps for configuration in thin client and for configuration in the host OS on the virtualization host computer, refer to:

- “■ Configuring in a thin client running on Windows OS” on page B8-4
- “■ Settings in the Host OS on the Virtualization Host Computer” on page B8-4

B8.3.2 Settings in the Guest OS on the Virtual Machine

You must configure the settings described here after you configure the settings in the host OS on the virtualization host computer.

■ Installing the Remote Desktop Session Host Role Service

Follow these steps to install the Remote Desktop Session Host role service:

1. Sign in to the host OS of virtualization host computer as an administrative user.
2. Copy an ISO format file of the CENTUM VP software medium and paste it into a folder in the host OS on the virtualization host computer.
3. From the Start menu, select [Server Manager].
Server Manager starts.
4. From the menu bar of Server Manager, select [Tools] > [Hyper-V Manager].
Hyper-V Manager starts.
5. In the left pane of Hyper-V Manager, select the virtualization host computer. The virtual machines on the selected virtualization host computer are displayed on the middle pane. Select the virtual machine to be used as HIS-TSE server and select [Connect] in the right click menu.
The virtual machine connection window appears.

TIP

The virtual machine connection window may appear full-screen. If it appears full-screen, click [Undo] to exit full-screen.

6. From the menu bar of the virtual machine connection window, select [Media] > [DVD Drive] > [Insert Disk].
A file opening dialog box appears.
7. Specify the copied ISO format file of the CENTUM VP software medium.
The selected ISO format file is mounted on the virtual machine.
8. Use Windows Explorer to open the following folder in the mounted CENTUM VP software installation medium.
<Mounted drive>:\CENTUM\HIS\TSE
9. Right-click “1-InstallFeature.bat” and select [Run As Administrator].
The Remote Desktop Session Host role service is installed and the virtual machine re-starts after the installation is complete.

■ Installing Remote Desktop Licensing Role Service and Specifying Remote Desktop Licensing Server

Follow these steps to install Remote Desktop Licensing role service and specify Remote Desktop Licensing server:

1. Sign in to the host OS of virtualization host computer as an administrative user.
2. Copy an ISO format file of the CENTUM VP software medium and paste it into a folder in the host OS on the virtualization host computer.
3. From the Start menu, select [Server Manager].
Server Manager starts.
4. From the menu bar of Server Manager, select [Tools] > [Hyper-V Manager].
Hyper-V Manager starts.
5. In the left pane of Hyper-V Manager, select the virtualization host computer. The virtual machines on the selected virtualization host computer are displayed on the middle pane.

Select the virtual machine to be used as HIS-TSE server and select [Connect] in the right click menu.

The virtual machine connection window appears.

TIP

The virtual machine connection window may appear full-screen. If it appears full-screen, click [Undo] to exit full-screen.

6. From the menu bar of the virtual machine connection window, select [Media] > [DVD Drive] > [Insert Disk].
A file opening dialog box appears.
7. Specify the copied ISO format file of the CENTUM VP software medium.
The selected ISO format file is mounted on the virtual machine.
8. Use Windows Explorer to open the following folder in the mounted CENTUM VP software installation medium.
<Mounted drive>:\CENTUM\HIS\TSE
9. Right-click “2-InstallLicense.bat” and select [Run As Administrator].
10. [Input for User Authentication:] sets the authentication method for Remote Desktop Session Host. Enter 1 and press [Enter] key to set “Require Network Level Authentication”.
11. [Input for Terminal Service Setting:] sets the Remote Desktop licensing mode. Enter either of the following values, and press the [Enter] key.
 - When selecting the number of connectable devices: 2
 - When selecting the number of connectable users: 4
12. [Input for Discovery Scope:] sets the discovery scope for Remote Desktop licensing. Enter either of the following values, and press the [Enter] key.
 - When selecting the work group: 0
 - When selecting the domain: 1

TIP

Select domains when the server computer is used in a domain environment.

13. [Input for License Servers To Use:] sets the license server to use. Enter the computer name or IP address of the license server and press the [Enter] key. If the license server is placed in a domain environment, use “Fully Qualified Domain Name (FQDN)” for the computer name and specify the host name, the domain name and others without omission.

TIP

If the license server and the remote desktop server run in the same computer, specify the name of local computer or the IP address of local computer.

14. Confirm the authentication method for Remote Desktop Session Host, the Remote Desktop licensing mode, the discovery scope for Remote Desktop licensing, and the setting information of license server and if there is no problem, enter y at [To be continued?:] and press the [Enter] key.

When the setup is complete, a message “[Press any key to continue...]” appears.

If you need to change the setting, enter n at [To be continued?:] and run 2-InstallLicense.bat to perform the setup all over again.

TIP

If the group policy of the domain controller is specified, an error occurs at the setting of license server that is used when you run 2-InstallLicense.bat. However, you can safely use because the license server is specified in the group policy of the domain controller.

■ Activate Remote Desktop Licensing Server

Follow these steps to activate the Remote Desktop Licensing server:

1. Sign in to the guest OS on the virtual machine to be used as HIS-TSE server as an administrative user.
2. Open Command Prompt and type `licmgr.exe`.
The RD Licensing Manager appears.
3. In the left pane, select [All servers].
The server computer appears in the right pane.
4. In the right pane, select the computer to be activated, and select [Action] > [Activate Server] from the menu bar.
The Activate Server Wizard appears.
5. Follow the instructions of the Wizard and activate the server computer.

■ Changing the Local Group Policy

**SEE
ALSO**

For more information about how to change the local group policy, refer to:

- “● Changing the Local Group Policy” on page B8-4
-

B8.3.3 Settings for Limiting Maximum Number of Connections

Setting values vary depending on the activated packages of Server for Remote Operation and Monitoring Function.

Specify the limit of concurrent connection in the guest OS on the virtual machine.

Follow these steps to configure the limit of maximum number of connections:

1. Sign in to the guest OS on the virtual machine as an administrative user.
2. Open Command Prompt and type `gpedit.msc`.
Local Group Policy Editor appears.
3. In the left pane, select [Computer Configuration] > [Administrative Templates] > [Windows Components] > [Remote Desktop Services] > [Remote Desktop Session Host] > [Connections].
4. In the right pane, double-click [Limit number of connections].
The Properties dialog box appears.
5. Select [Enabled] and set [RD Maximum Connections allowed] to 4 for the package of Server for Remote Operation and Monitoring Function (Number of client PCs that can be simultaneously connected: Up to four) and set [RD Maximum Connections allowed] to 8 for the package of Server for Remote Operation and Monitoring Function (Number of client PCs that can be simultaneously connected: Up to eight).
6. Click [OK].
7. Restart the virtual machine.

B8.3.4 Settings for Limiting Sessions Per User

Specify the number of sessions per user in the guest OS on the virtual machine.

Follow these steps to configure the limit of sessions per user:

1. Sign in to the guest OS on the virtual machine as an administrative user.
2. Open Command Prompt and type `gpedit.msc`.
Local Group Policy Editor appears.
3. In the left pane, select [Computer Configuration] > [Administrative Templates] > [Windows Components] > [Remote Desktop Services] > [Remote Desktop Session Host] > [Connections].
4. In the right pane, double-click [Restrict Remote Desktop Services users to a single Remote Desktop Services session].
The Properties dialog box appears.
5. Select [Not Configured] and click [OK].
6. Restart the virtual machine.

B8.3.5 Settings for Application and Working Directory

The tasks are required only when thin client runs in thin OS.

Follow these steps to configure settings for application and working directory:

1. Start the [Connection Manager].
The Connection Manager window appears.
2. Connect to the virtual machine that you want to connect.
The remote connection dialog box appears.
3. Specify the following settings to [Application] in Logon tab.
 - To start in Desktop mode, run <the folder where the CENTUM VP software is installed>:\CENTUMVP\Program\Startdesktop.bat.
 - To start in Panel mode, specify <the folder where the CENTUM VP software is installed>:\CENTUMVP\Program\BKHBo.exe and then specify the launch argument “-P”, function string, and argument.
4. Specify <the folder where the CENTUM VP software is installed>:\CENTUMVP\Program to the [Working Directory] in Logon tab in any start mode.
5. Click [OK].

B8.3.6 Uninstalling HIS-TSE

Follow these steps if you have specified the program that runs first at the connection of Remote Desktop in Preferences:

1. Sign in to the guest OS on the virtual machine as an administrative user.
2. Open Command Prompt and type `gpedit.msc`.
Local Group Policy Editor appears.
3. In the left pane, select [Computer Configuration] > [Administrative Templates] > [Windows Components] > [Remote Desktop Services] > [Remote Desktop Session Host] > [Remote Session Environment].
4. In the right pane, double-click [Start a program on connection].
The Start a program on connection dialog box appears.
5. Select [Disabled] from the items in [Start a program on connection] and click [OK].

B8.4 SOE

This section describes the following settings.

- Settings for bandwidth
- Settings for limiting maximum number of connections
- Settings for limiting sessions per user
- Settings for Windows network

B8.4.1 Settings for Bandwidth

Specify the bandwidth in the host OS of the virtualization host computer.

Follow these steps to configure the bandwidth:

1. Sign in to the host OS of virtualization host computer as an administrative user.
2. From the Start menu, select [Server Manager].
Server Manager starts.
3. From the menu bar of Server Manager, select [Tools] > [Hyper-V Manager].
Hyper-V Manager starts.
4. In the left pane of Hyper-V Manager, select the virtualization host computer. The virtual machines on the selected virtualization host computer are displayed on the middle pane.
Select the virtual machine and select [Settings] in the right click menu.
The configuration dialog box appears.
5. From the menu of configuration dialog box, select [Add Hardware] > [Network adapters] and click [Add].
6. In the bandwidth management, set the [Maximum Bandwidth] to 100 MB.
7. Click [OK].

B8.4.2 Settings for Limiting Maximum Number of Connections

Specify the limit of concurrent connection in the guest OS on the virtual machine.

SEE

ALSO For more information about how to set the limit of maximum number of connections, refer to:

B8.2.2, “Settings for Limiting Maximum Number of Connections” on page B8-9

B8.4.3 Settings for Limiting Sessions Per User

Specify the number of sessions per user in the guest OS on the virtual machine.

**SEE
ALSO**

For more information about how to set the limit of sessions per user, refer to:

B8.2.3, “Settings for Limiting Sessions Per User” on page B8-10

B8.4.4 Settings for Windows Network

Specify the following address for the IP address of VnetIPBUS2 which serves as the control network 2.

192.168.(128 + domain number).(129 + station number)

C. Maintenance

This section describes the tasks required in the operation and maintenance of stations after they have been newly set up.

Blank Page

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 33J01C20-01EN)

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 33J01C20-01EN)

■ Preparation for Deactivating Packages

When an active package is deactivated, the settings configured when the package was active will be lost. When the package is activated again, the settings need to be reconfigured.

Blank Page

C2. Changing the Location of Engineering Data for Reference

The location of the engineering data for reference by HIS that was set at the installation of the CENTUM VP software can be changed as necessary.

■ Changing Procedure

Follow these steps to change the location of the engineering data for reference:

1. Start the operation and monitoring function on the HIS.
2. On the Name Input Toolbox of the Browser Bar, enter ".SH" in the Window Name Input box.

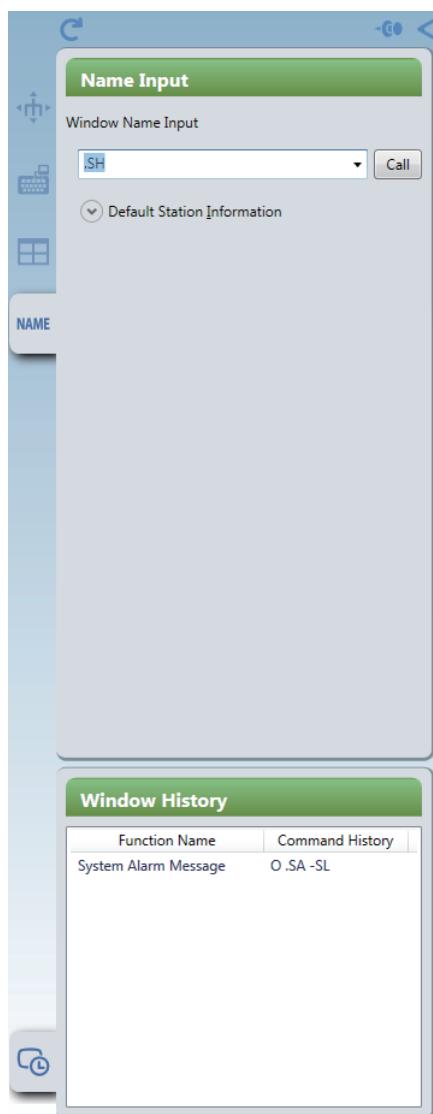


Figure C2-1 Browser Bar

3. Click [Call].
The HIS Setup window appears.
4. Click the [Equalize] tab.

5. In the Referenced Database drop-down list box, select the station for reference of engineering data.

C3. 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

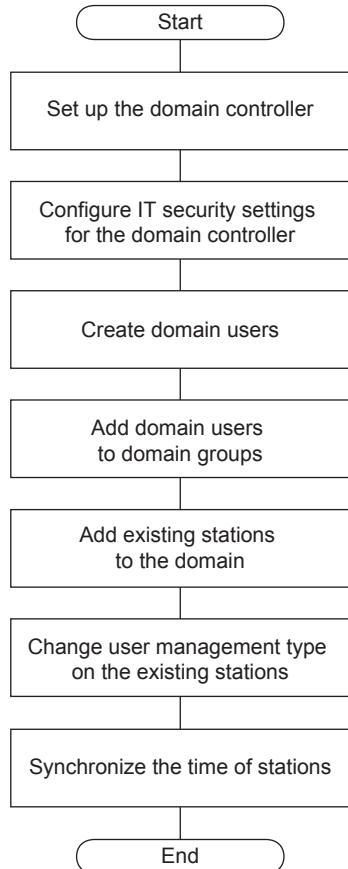


Figure C3-1 Workflow for Setting Up the Windows Domain Environment Later

■ 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 2016/Windows Server 2012 R2)” on page B2-5
- B2.3, “Configuring the Domain Controller (Windows Server 2008 R2/Windows Server 2008)” on page B2-7

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

B2.4, “Configuring Security Settings for the Domain Controller” on page B2-9

For more information about creating domain users, refer to:

“■ Creating a Domain User” on page B2-16

For more information about how to add domain users to domain groups, refer to:

“■ Adding Domain Users to Domain Groups” on page B2-17

For more information about how to add client computers to the domain, refer to:

B2.6, “Adding Client Computers to the Domain” on page B2-21

For more information about changing the user management type, refer to:

6.3, “Changing the IT Security Settings” in CENTUM VP Security Guide (IM 33J01C30-01EN)

For more information about how to synchronize the time of the stations within a domain, refer to:

B2.8, “Setting Up Time Synchronization in Windows Domain Environment” on page B2-28

C4. Changing from CENTUM Authentication Mode to Windows Authentication Mode

This section describes the procedure for migrating from the CENTUM authentication mode to the Windows authentication mode.

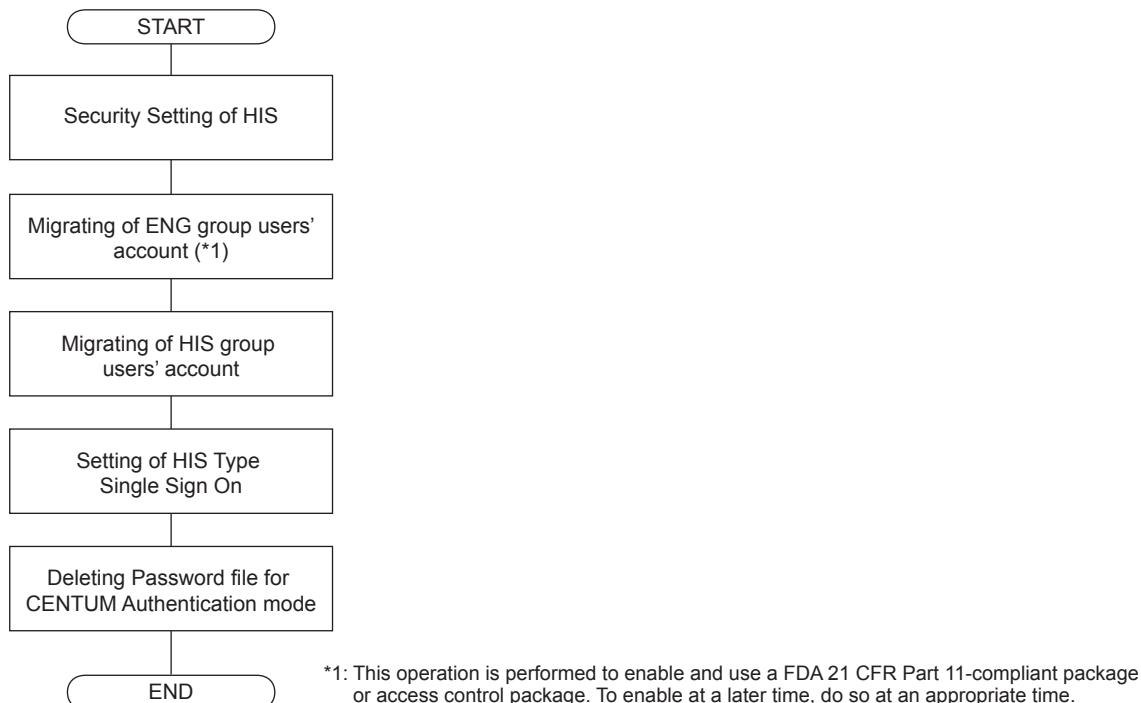


Figure C4-1 Workflow

■ Security Setting of HIS

Configure security settings on each computer when the standard operation and monitoring function is activated.

SEE ALSO For more information about Security Setting of HIS, refer to:

- “■ Security Setting of HIS” on page B4-139

■ Migrating User Accounts of ENG Group

Perform this operation if one or more of the Standard Engineering Function, Recipe Management Package, or Report Package, as well as the Access Administrator Package (FDA:21 CFR Part 11 compliant) or Access Control Package, are enabled. If the Access Administrator Package (FDA:21 CFR Part 11 compliant) or Access Control Package is to be activated at a later time, migrate the ENG group users after activating the package.

● Deleting Registered Users from User Environment Settings Table

Perform this operation on the computers on which one or more of the Standard Engineering Function, Recipe Management Package, or Form Package, as well as the Access Administrator Package (FDA:21 CFR Part 11 compliant) or Access Control Package, are activated. Be-

fore migrating ENG group users, you should delete all users that are registered to the user environment settings on the Access Control Utility.

IMPORTANT

If the standard operation and monitoring function is activated on the computer you are setting up, the user environment settings configured on the Access Control Utility are the same as those configured on the HIS Utility.

Do not perform this operation if you have already finished migrating the HIS group users.

1. Log on as a user of the CTM_MAINTENANCE or CTM_ENGINEER_ADM group.
2. Start Access Control Utility.
3. On General tab, click [Setting].
The User Environment Settings dialog box appears.
4. Select the user and click [Delete].
The Delete User dialog box appears.
5. Enter the password of the selected user and then click [OK].
6. Repeat steps 4 and 5 to delete all the users.

● Creating Windows User Accounts

When creating a Windows user account for the same user registered on the engineering builder, if the computer is a member of a Windows domain, the user should also be created in the domain. For stand alone computers, the same user should be created in all stand-alone computers.

TIP

Before migrating the user accounts, if a Windows user account satisfies the following conditions, the Windows user account can be used without being migrated.

- The Windows user account managed in a domain or in the host computer is not changed before and after the user migration.
- The Windows user account is put in a proper user group of standard model security settings.
- An identical user name is registered in ENG group.

SEE ALSO

For more information about creating Windows user accounts, refer to:

B4.9.1, "When the Standard Model with Standalone Management Security Settings are Applied" on page B4-103

● Setting Windows Operating Environment for Users

This operation needs to be performed on the computer where the created user account to log on.

SEE ALSO

For more information about setting Windows environment, refer to:

B4.10, "Configuring Windows Environment Settings for Each User" on page B4-107

● Setting User Environment

This operation needs to be performed on the computer where the created user account to log on.

SEE ALSO

For more information about setting user environment, refer to:

- “● Setting User Environment” on page B4-141

- **Setting Windows Authentication Mode to Authenticate ENG Group Users**

Perform the following procedure on the computer used for ENG group user management.

SEE ALSO

For more information about the procedure for setting Windows authentication mode to authenticate ENG group users, refer to:

- “● Setting Windows Authentication Mode to Authenticate ENG Group Users” on page B4-143

■ Migrating User Accounts of HIS Group

Migrate HIS group user accounts.

- **Deleting Registered Users from User Environment Settings Table**

Perform this setting on the computers on which the standard operation and monitoring function is activated. Before migration, you should delete all users that are registered to the user environment settings on the Access Control Utility.

IMPORTANT

If the Access Administrator Package (FDA:21 CFR Part 11 compliant) or Access Control Package is activated on the computer you are setting up, the user environment settings configured on the Access Control Utility are the same as those configured on the HIS Utility. Do not perform this operation if you have already finished migrating the ENG group users.

1. Log on as a user of the CTM_MAINTENANCE or CTM_ENGINEER_ADM group.
2. Start HIS Utility.
3. On User tab, click [Setting].
User Environment Settings dialog box appears.
4. Choose a user name and click [Delete].
The Delete User dialog box appears.
5. Enter the password of the selected user and click [OK].
6. Repeat steps 4 and 5 to delete all the users.

- **Creating Windows User Accounts**

When creating a Windows user account for the same user registered on the engineering builder, if the computer is a member of a Windows domain, the user should also be created in the domain.

TIP

Before migrating the user accounts, if a Windows user account satisfies the following conditions, the Windows user account can be used without being migrated.

- The Windows user account managed in a domain or in the host computer is not changed before and after the user migration.
- The Windows user account is put in a proper user group of standard model security settings.
- An identical user name is registered in HIS group.

SEE ALSO

For more information about creating Windows user accounts, refer to:

B4.9.1, "When the Standard Model with Standalone Management Security Settings are Applied" on page B4-103

● Setting Windows Operating Environment for Users

This operation needs to be performed on the computer where the created user account to log on.

SEE ALSO

For more information about setting Windows environment, refer to:

B4.10, "Configuring Windows Environment Settings for Each User" on page B4-107

● Setting User Environment

Perform this setting on the computers on which the standard operation and monitoring function is activated. Configure the settings for each HIS group user.

SEE ALSO

For more information about setting user environment, refer to:

"● Setting User Environment" on page B4-141

● Setting Windows Authentication Mode to Authenticate HIS Group Users

The following operations need to be performed on the computer used for creating and configuring project.

SEE ALSO

For more information about the procedure for setting Windows authentication mode to authenticate HIS group users, refer to:

"● Setting Windows Authentication Mode to Authenticate HIS Group Users" on page B4-144

● Deleting ONUSER and ENGUSER

The following operations need to be performed on the computer used for creating and configuring project.

IMPORTANT

- When the user authentication mode of a project is changed and downloaded, the new mode will not be valid until the HIS is restarted; only the settings on the security builder are changed.
- When temporarily keeping the HIS terminals that run in the CENTUM authentication mode, such as when migrating in phases from the CENTUM authentication mode to the Windows authentication mode, the users to be used on those HISs need to be kept within the security builder. Perform this operation when migrating all HISs to the Windows authentication mode.

1. Use an administrative user account to logon.
2. Start Security Builder.
3. Select the [Valid User] tab.
4. Choose ONUSER and ENGUSER to delete them.
5. On System View, run [Download Project Common Section].

● Restarting the HIS

Perform this setting on the computers on which the standard operation and monitoring function is activated.

1. If [Download Project Common Section] has not been performed on the computer used for creating and configuring projects after the authentication mode was changed, run [Download Project Common Section].
2. Restart the HIS.

TIP

When the user authentication mode of a project is changed and downloaded, the new mode does not take effect until the HIS is restarted.

Do not restart the HIS when temporarily keeping some HIS terminals in CENTUM authentication mode, such as when migrating the system in phases from CENTUM authentication mode to Windows authentication mode.

■ Setting HIS Type Single Sign On

Configure these settings to use the HIS type single sign on function on the computers where the standard operation and monitoring function is activated.

SEE ALSO

For more information about setting HIS Type single sign on, refer to:

“■ Setting HIS Type Single Sign On” on page B4-145

■ Deleting CENTUM Authentication Password File

When the HIS passwords are comprehensively controlled, this operation needs to be performed on the computer where the password file is placed.

1. Use the administrator account to log on the computer where the password file for comprehensive control is placed.
Specifically, this is the computer specified at Reference Database on the Equalize tab of the HIS Setup window.
2. Delete <project's top folder>\ETC\Password.odc.

TIP

Which project is the current project can be found using the Project's Attribution Utility.

Blank Page

C5. 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 C5-1 Folder Backups

Contents	Folder	When to back up
Backup of entire Windows	All hard disk	Back up when changes have been made to the system (program installation, setup completed, etc.). Back up after exiting all applications including the operation and monitoring function.
Automation Design Master Database (ADMDB)	-	-
VP project	Project folders	Back up the folders after exiting the System View.
Customized menu file	Folder storing the customized menu file	-
CENTUM VP database for operation & monitoring function	Every function folder such as Report, PICOT, etc	-
Engineering data defined on CAMS for HIS configurator	-	-

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 CENTUM VP-related folders.

**SEE
ALSO**

For more information about backing up ADMDB, refer to:

C1.1.2, "Backing up and restoring the ADMDB" in Automation Design Suite Basics (IM 33J10A10-01EN)

C5.1 Backing Up the Entire Windows

This section describes how to back up the entire Windows.

■ 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 the procedure for creating the repair disk, refer to:

Windows-related manual or the web site of Microsoft Corporation

C5.2 Backing Up VP Projects

After performing engineering operations, be sure to back up the engineering data.

You can use the following methods to back up a VP project:

- Back up from System View
- Back up from Maintenance Menu
- Back up to AD project

TIP

It is assumed that the tuning parameters are saved beforehand.

■ Backup from System View

To back up a project, select [Tools] > [Start Backup...] from the tool bar in System View.

SEE ALSO

For more information about backing up projects, refer to:

2.6, "Project Data Backup" in Engineering Reference Vol.1 (IM 33J10D10-01EN)

■ Backup from Maintenance Menu

First edit the batch file to specify the data to be backed up, and then run Projectsave to back up a project.

For more information about the backup method, backup content, and the method of editing the batch file, see the PDF file located in <CENTUM VP installation folder>\HIS\Tool.

If a message is output at the start of the backup process, the batch file needs to be edited. Follow the instructions in the displayed message.

IMPORTANT

Before performing a backup or restoring operation, be sure to delete the old folder in the backup location when backing up a project or in the restore location when restoring a project.

If a file in the project folder is overwritten, the dependency relationship in the project file may be broken, disabling operations in System View or causing unexpected errors.

■ Back up to AD project

You need to back up the VP project to AD project before backing up ADMDB or exporting the AD project.

SEE ALSO

For more information about backing up VP project to AD project, refer to:

B1.5.1, "Managing VP projects" in Automation Design Suite Basics (IM 33J10A10-01EN)

C5.3 Backing Up the Customized Menu File

Back up the customized menu file that is used for context menus into a removable storage medium.

■ Customized Menu File

<CENTUM VP Installation Folder>\HIS\SPCONF\BKHMenuDef.xml

The customized menu file modified with HIS Menu Editor is placed with the above path.

TIP

The following files are used for context menus;

- default menu file
- customized menu file

The default Menu file is installed by the installer. It will be automatically overwritten by the installer at the time of revision upgrade.

C5.4 Backing Up the Database of CENTUM VP Operation and Monitoring Function

Back up the data for each function, such as reports and PICOT.

C5.4.1 Backing Up Reports

Copy a report definition file into a removable storage medium by using the copy tool of the report package.

C5.4.2 Backing Up PICOT

Copy the contents in the following directory to a storage medium using Windows Explorer.

<CENTUM VP Installation Folder>\his\users\save\BKUPICOT

C5.5 Backing Up the Engineering Data Defined on CAMS for HIS Configurator

Use the backup tool from the menu bar of the CAMS for HIS configurator.

C6. Upgrading the System

This section describes the procedure for the following types of upgrades.

- Upgrade from CENTUM CS 3000 to CENTUM VP R6
- Upgrade from CENTUM CS 1000 to CENTUM VP R6
- Upgrade from CENTUM VP R4 or R5 to R6
- Upgrade CENTUM R6 to a later revision

SEE ALSO

For more information about cautionary notes on upgrading the system, refer to:

C11., “Cautionary Notes for Upgrading” on page C11-1

■ Administrative User Who Performs the Upgrading Tasks

The CENTUM VP software must be upgraded on the same computer by an administrative user shown in the following table.

Table C6-1 Administrative User Who Performs the Upgrading Tasks

Security model and user management type to be applied		
Legacy Model	Standard Model	
	Standalone Management	Domain/Combination Management
Local user who belongs to the Administrators local group and CTM_MAINTENANCE local group	Local user who belongs to the Administrators local group and CTM_MAINTENANCE local group	<ul style="list-style-type: none"> • Domain user who belongs to the Domain Admins domain group and CTM_MAINTENANCE domain group • Domain user who belongs to the Administrators local group and CTM_MAINTENANCE_LCL local group • Local user who belongs to the Administrators local group and CTM_MAINTENANCE_LCL local group (*1)

*1: The domain user name and password must be entered during installation.

TIP

If the user management type is Domain or Combination management, install the software while the computer is added to the domain.

■ Tasks to be performed after the version up, revision up or upgrade

The following works are required as the preparation for starting engineering.

- Creating an Automation Design project (AD project)
- Registering the existing VP project to the AD project

SEE ALSO

For more information about the preparation for starting engineering, refer to:

B., “Starting engineering” in Automation Design Suite Basics (IM 33J10A10-01EN)

C6.1 Upgrading from CENTUM CS 3000 to CENTUM VP R6

The Windows OS supported by CENTUM VP R6 are different from those supported by CS 3000; therefore, you need to install the CENTUM VP software anew on a computer running the OS supported by CENTUM VP R6 and then transfer the existing project database.

C6.1.1 Procedures for the Upgrade

■ Workflow of the Upgrade

The workflow of the upgrade is as follows. Perform the upgrading tasks according to this flow chart.

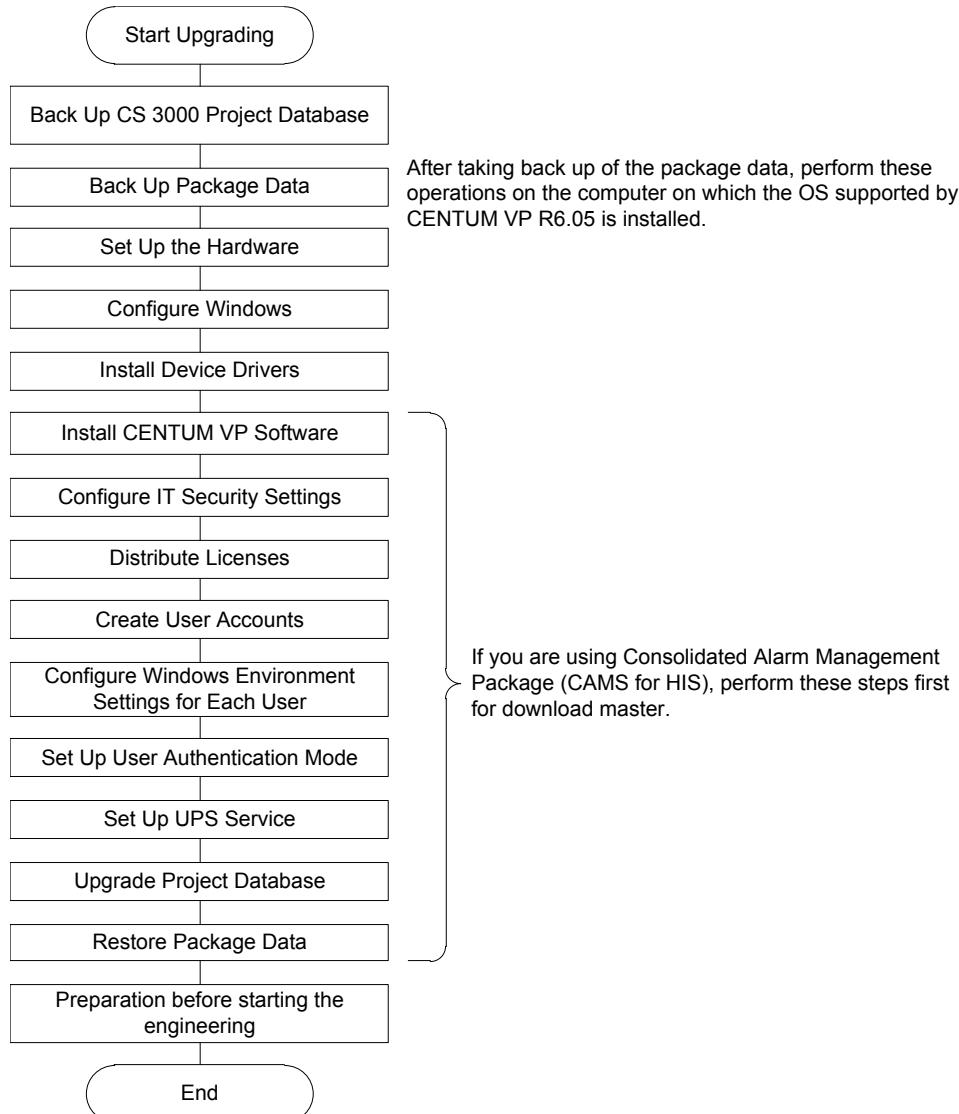


Figure C6.1.1-1 Upgrade Procedure

IMPORTANT

The program for upgrading CS 3000 projects and of CENTUM VP software must be installed on an OS with which R6 performance is guaranteed. You need to set up Windows before the installation.

■ Back Up CS 3000 Project Database

Back up the necessary project database of CS 3000.

SEE ALSO For more information about backing up the project database, refer to:

C5.2, "Backing Up VP Projects" on page C5-3

■ Back Up Package Data

Back up the necessary data of each software package used in CS 3000.

SEE ALSO For more information about the details of backing up the package data, refer to:

C6.1.2, "Backing up and Restoring CS 3000 Package Data" on page C6-8

■ Set Up the Hardware

Set up the hardware.

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

B4.1, "Setting Up the Hardware" on page B4-2

■ Set Up Windows

Configure Windows settings.

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

B4.2, "Setting Up Windows" on page B4-7

■ Install Device Drivers

Install communication drivers such as the control bus driver, as well as device drivers such as the USB driver for OPKB.

SEE ALSO For more information about how to install the device drivers, refer to:

- B4.3, "Configuring Network Settings" on page B4-43
- B4.4, "Installing the USB Driver for the Operation Keyboard" on page B4-77
- B4.5, "Tasks Required for Setting Up the Console Type HIS" on page B4-79

■ Install the CENTUM VP Software

Install the CENTUM VP software.

SEE ALSO For more information about the CENTUM VP software installation procedure, refer to:

B4.6, "Installing the CENTUM VP Software" on page B4-85

■ Configure IT Security Settings

Configure IT security settings.

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

B4.7, "Configuring IT Security Settings" on page B4-94

■ Distribute Licenses

Distribute licenses to the station.

For upgrading to a newer version, the license medium comes with a package list . By importing this package list to License Manager, the station configuration definitions and package assignments to each station that are necessary for license distribution are generated.

**SEE
ALSO**

For more information about distributing licenses, refer to:

B4.8, "Distributing and Accepting Licenses" on page B4-101

■ Create User Accounts

Create user accounts.

**SEE
ALSO**

For more information about creating user accounts, refer to:

B4.9, "Creating User Accounts" on page B4-102

■ 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:

B4.10, "Configuring Windows Environment Settings for Each User" on page B4-107

■ Set User Authentication Mode

Set up for the desired user authentication mode.

**SEE
ALSO**

For more information about setting the user authentication mode, refer to:

B4.11, "Setting Up for User Authentication Modes" on page B4-135

■ Set Up the Uninterruptible Power Source (UPS) Service

Set up the uninterruptible power source (UPS) service.

**SEE
ALSO**

For more information about setting up the UPS service, refer to:

B4.12, "Setting Up the Uninterruptible Power Supply (UPS) Service" on page B4-149

■ Upgrade the Project Database

1. Restore the CS 3000 project database that was created before the upgrade in an appropriate location.
2. Start the Project's Attribution Utility.
3. Register the project database in the System View.
4. Start the System View.
The project database is upgraded automatically to the new version.

IMPORTANT

Specifications of the graphic features differ between CS 3000 and CENTUM VP.

To convert CS 3000 graphic files to CENTUM VP R6 graphic files considering the compatibility in display and behaviors, you need to perform specific procedures.

SEE ALSO

For more information about the Project's Attribution Utility, refer to:

2.3, "Project's Attribution Utility" in Engineering Reference Vol.1 (IM 33J10D10-01EN)

● HIS Database Conversion Tool

If a CS 3000 HIS is included in the project, it will be upgraded to a CENTUM VP HIS. When "HIS Database Conversion Tool" is displayed, select the check boxes of the stations to be converted to CENTUM VP HIS and clear the check boxes of the stations that are not to be converted.

- When HIS is converted to CENTUM VP HIS, all CS 3000 graphic files of the station are automatically converted to CENTUM VP graphic formats.
- You also can start "HIS Database Conversion Tool" from the Tool menu of System View by selecting [HIS Database Conversion Tool].

TIP

After upgrading to the station type of CENTUM VP HIS with the HIS database conversion tool, the station type can be changed from the HIS Properties of the System View.

SEE ALSO

For more information about the procedure to convert CS 3000 graphic files to CENTUM VP graphic files considering the compatibility in display and behaviors, refer to:

Graphic Conversion Guide (IM 33J01C40-01EN)

● Graphic File Converter

You can use the Graphic File Converter to convert CS 3000 graphic files to CENTUM VP graphic files, file by file. The graphic files converted to CENTUM VP formats can be imported and edited using the CENTUM VP graphic builder.

Follow these steps to convert graphic files:

1. Start the Graphic File Converter.
2. Add the CS 3000 graphic file or folder to be converted.
3. Specify the output target folder and click [Convert].
A dialog box showing the progress of the conversion appears.

TIP

If the file conversion is successful, Successful appears in the Status column, Failed if unsuccessful, when the conversion is finished.

4. Click [Close] to exit the Graphic File Converter.

SEE ALSO

For more information about the procedure to convert CS 3000 graphic files to CENTUM VP graphic files considering the compatibility in display and behaviors, refer to:

Graphic Conversion Guide (IM 33J01C40-01EN)

■ Restore the Backed Up Package Data

Restore the data for each package that was backed up.

**SEE
ALSO**

For more information about how to restore data for each package, refer to:

C6.1.2, "Backing up and Restoring CS 3000 Package Data" on page C6-8

■ Note on Instrument Faceplate Highlight

From CENTUM VP R5.03.00, the instrument faceplate highlight function is supported. This feature can be turned off.

**SEE
ALSO**

For more information about instrument faceplate highlight, refer to:

2.7, "Highlighting of Instrument Faceplates" in Human Interface Stations Reference Vol.2 (IM 33J05A11-01EN)

For more information about turning on/off the instrument faceplate highlight, refer to:

“● Instrument Faceplate Highlight” in “■ The Settings on Action Tab” in 1.2, “The Settings on HIS Utility” in Human Interface Stations Reference Vol.1 (IM 33J05A10-01EN)

■ Notes When PROFIBUS Is Used

If you install ALP111 that was used in CENTUM CS 3000 R3.06 or earlier versions into the ER bus node of CENTUM VP R5, perform either of the following tasks:

- After upgrading to CENTUM VP R5, download the communication driver of ALP111 again.
- Perform IOM download to the ALP111 from the system builder or the IOM status display window of HIS.

C6.1.2 Backing up and Restoring CS 3000 Package Data

This section identifies the data that need to be backed up and describes how to back up and restore them.

■ Data Required to be Backed Up and Restored

The following table shows the data that needs "Backup/Restoration" for each package.

Among the data you need to back up and restore, some must be backed up while CS 3000 is running and others must be backed up while CS 3000 is not running.

You backup data in CS 3000 and restore them in CENTUM VP.

Table C6.1.2-1 Data to Back Up While CS 3000 Is Running

Package	Name	Related CENTUM VP R6 Packages	Data back up/restore
LHS1100 LHM1101	Standard Operation and Monitoring Function	VP6H1100	HIS Setup Information
LHS1150	Server for Remote Operation and Monitoring Function	VP6H1150	The same as LHS1100
LHS4200	Historical Message Integration Package (meeting FDA Regulations)	VP6H4200	The data stored in the Historical integrated server
LHS4700	Advanced Alarm Filter Package	VP6H4700	Advanced Alarm Filter Configuration Data
LHS6510	Long-term Data Archive Package	VP6H6510	Long-term storage data
LHS6530	Report Package	VP6H6530	Report configuration data
LHS5100 LHM5100	Standard Builder Function (*1)	VP6E5100	Project database
LHS5150	Graphic Builder	VP6E5150	Project database
LHS5160	CS Batch 3000 (*2)	VP6E5165	Project database
LHS5161	CS Batch 3000 Recipe Management Package (*3)	VP6E5166	Recipe database
LFS1250	Generic Subsystem Gateway Package	VP6F1250	OPC server definition information file and item definition information file

*1: For CENTUM VP R6, this corresponds to Standard Engineering Function.

*2: For CENTUM VP R6, this corresponds to Batch Builder.

*3: For CENTUM VP R6, this corresponds to Recipe Management Package.

Table C6.1.2-2 Data to Back Up While CS 3000 Is Not Running

Package	Name	Related CENTUM VP R6 Packages	Data back up/restore
LHS1100 LHM1101	Standard Operation and Monitoring Function	VP6H1100	Database Related to HIS
LHS1150	Server for Remote Operation and Monitoring Function	VP6H1150	The same as LHS1100

Continues on the next page

Table C6.1.2-2 Data to Back Up While CS 3000 Is Not Running (Table continued)

Package	Name	Related CENTUM VP R6 Packages	Data back up/restore
LHS4800	Consolidated Alarm Management Software (CAMS for HIS)	VP6H1100 (Included in the Operation and Monitoring Function)	<ul style="list-style-type: none"> • Message Monitor data • Configurator data • Run-time data base • Backup of run-time database • Historical data • Scenario files of Alarm Generator Tools • Historical Viewer data • OPC A&E server configuration • CAMS for HIS server configuration • Equalization scope configuration
LHS6710 LHM6710	FCS Data Setting/Acquisition Package (PICOT)	VP6H6710	Configuration data
LHS5110	Access Control Package	VP6E5110	Configuration data
LHS5170	Access Administrator Package (FDA: 21 CFR Part 11 compliant)	VP6E5170	Audit trail database
LPC6900	SOE Server Package	VP6P6900	Back up/restore the SQL server database.
LPC6920	SOE Viewer Package	VP6P6920	Back up the configuration files.

■ Backing UP and Restoring the Data to Be Backed Up While CS 3000 Is Running

The following data should be backed up while CS 3000 is running.

Make a backup, and restore it using the Import function of each package.

IMPORTANT

Backing up and restoration of a project database covers the data of the Standard Builder Function, Graphic Builder Package, CS Batch 3000 Builder, and CS Batch 3000 Recipe Management Package.

● Standard Operation and Monitoring Function - HIS Setup Information

- Backup

Use the export function of the HIS Setup window to back up the registry information of the HIS.

- Restore

Use the import function of the HIS Setup window to import the file that was backed up.

SEE ALSO

For more information about export and import functions of the HIS Setup window, refer to:

“■ [Import] and [Export] of HIS Setup Window” in 4.3, “HIS Setup Window” in Human Interface Stations Reference Vol.1 (IM 33J05A10-01EN)

● Historical Message Integration Package

The data stored in the Historical message integration server can be inherited. To inherit the data, you need to perform on each HIS the task to maintain the continuity of sequence numbers of the historical message files stored in the Historical message integration server and set up the destination folder for storing historical messages again.

- Back up sequence numbers on each HIS

Log on as an administrative user and run the following command to stop the operation and monitoring function.

```
<CS 3000 installation folder>\his\tool\BKHHisStop.exe
```

Use Explorer to save the file with the latest sequence number from among the following files onto a removable medium.

```
<CS 3000 installation folder>\Log\HISHIST\HISHISTnnnn-YYYYMMDD.log (nnnn: sequence number)
```

- Tasks on the Historical message integration server

Log on as an administrative user and copy the file with the latest sequence number that you have saved to the folder corresponding to each HIS on the Historical message integration server.

Folder on the server: <Share name>\HisHist\HISddss (dd: domain number; ss: station number)

TIP

From the names of the folders in the above storage location on the server, you can find out the HISs that are under consolidated historical message management. If the HIS before replacement is damaged and the latest historical message file is unavailable, refer to the HIS folder in the above storage location on the server and keep a record of the sequence number. In this case, you cannot port the latest historical message file to the server.

- Restore the sequence number

Log on to the upgraded HIS as an administrative user and run the following command to stop the operation and monitoring function.

```
<CENTUM VP installation folder>\his\tool\BKHHisStop.exe
```

Make the following HISHIST storage folder empty.

Storage folder: <CENTUM VP installation folder>\Log\HISHIST

Execute the following command at the command prompt.

```
<CENTUM VP installation folder>\his\tool\SetSeqNo.batΔ<the latest sequence number you kept in step 2> (Δ: space character)
```

Restart the HIS and confirm that a historical message file of the sequence number you backed up plus one has been created in the HISHIST folder.

Configure the server storage definition file and connect to the Historical message integration server to start the storing of messages.

SEE ALSO

For more information about setting up the storage destination folder, refer to:

8.1.1, "Setting Up the Storage Destination Folder for Historical Message Save Files" in Human Interface Stations Reference Vol.2 (IM 33J05A11-01EN)

● Advanced Alarm Filter Package

- Backup

Using the Export function of the Advanced Alarm Filter package, back up the filter configuration data.

- Restore

Using the Import function of the Advanced Alarm Filter package, restore the filter configuration data.

SEE ALSO

For more information about details of Export and Import of alarm filter definition, refer to:

7.5.3, "Advanced Alarm Filter Window" in Human Interface Stations Reference Vol.2 (IM 33J05A11-01EN)

● Long-Term Data Archive Package

- Backup

Use the archive feature of the Long-Term Data Archive Package to back up the data to an external storage medium.

Also back up the following BKHLogFile.txt file.

\\\<HIS name>\LTDATA\LOG\BKHLogFile.txt

- Restore

The retrieve feature of the Long-Term Data Archive Package can be used to restore the backup files from the external storage medium to the hard disk of HIS.

The BKHLogFile.txt file should be restored to the following path or to the path where it was archived from.

SEE ALSO

For more information about details of archiving and retrieving operations, refer to:

4.2.4, "Archival and Retrieval Operations" in Optional Functions Reference (IM 33J05H10-01EN)

● Report Package

- Backup

Copy a report definition file into a removable storage medium by using the copy tool of the report package.

- Restore

Copy a report definition file in the removable storage medium into the restored computer by using the copy tool of the report package.

SEE ALSO

For more information about copying report configuration data, refer to:

- "■ Copy to Other Computer" in 2.5.3, "Report Printout on Other Computer" in Optional Functions Reference (IM 33J05H10-01EN)
- 2.1, "Settings for Report Package" in Optional Functions Reference (IM 33J05H10-01EN)

● Data of Generic Subsystem Gateway Package

Back up the definition file in the following folder of GSGW, and restore it after the upgrade.

- OPC server definition information file:

<CS 3000 installation folder>\apcs\GPLS\BKEOPCSVRDef.csv

- Item definition information file:

<CS 3000 installation folder>\apcs\GPLS\BKEOPCITEMDef.csv

■ Backing UP and Restoring the Data to Be Backed Up While CS 3000 Is Not Running

The following data should be backed up while CS 3000 is not running.

Before backing up the data on CS 3000, you must completely exit all engineering functions of CS 3000. When restoring the data on CENTUM VP, you must exit all CENTUM VP functions.

As for these Data, after the installation of CENTUM VP, the target file or folder should be copied to a relatively same location under the <CENTUM VP installation folder>. If a file with the same name exists in the destination folder, overwrite it.

● Standard Operation and Monitoring Function - HIS-related Database

1. In command prompt, run the following command, and stop the operation and monitoring functions.

<CS 3000 installation folder>\his\tool\BKHHisstop.exe

2. Back up and restore the following HIS-related files. Folder name of restored data:

<CENTUM VP installation folder>

<CS 3000 installation folder>\his\database	: Voice messages, etc.
<CS 3000 installation folder>\his\recipe	: Recipes and Control recipes
<CS 3000 installation folder>\his\save	: Closed data, Scheduler, and so on
<CS 3000 installation folder>\his\Trend	: Trend data
<CS 3000 installation folder>\his\spconf	: Context menus, etc.
<CS 3000 installation folder>\his\Media\User	: Media data

TIP

The tokuchu files are located in the following folder. Please check with the Yokogawa department in charge of tokuchu to confirm whether these files can be restored and used after the upgrade installation.

<CS 3000 installation folder>\his\spconf

<CS 3000 installation folder>\his\user

● Consolidated Alarm Management Software (CAMS for HIS)

You must backup the data of CAMS for HIS after backing up other package data and while the CAMS for HIS is disabled.

You must restore the data of CAMS for HIS after restoring the HIS related databases and while the CAMS for HIS is disabled.

SEE ALSO

For more information about backing up and restoring the CAMS for HIS data, refer to:

C6.1.3, "Backing up and restoring the CAMS for HIS data" on page C6-14

● FCS Data Setting/Acquisition Package (PICOT)

1. Exit PICOT.

Click PICOT in the Windows taskbar to open. From the File menu, select [Exit]. PICOT exits.

2. Back up and restore configuration files.

- Backup

Back up the configuration files in the following folder of this Package.

<CS 3000 installation folder>\his\users\save\BKUPICOT

- Restore

Restore the backed up files to the following folder.

<CENTUM VP installation folder>\his\users\save\BKUPICOT

SEE ALSO

For more information about details of definition files, refer to:

3.2, "Component Files and Processing Flow of PICOT" in Optional Functions Reference (IM 33J05H10-01EN)

- **Access Control Package and Access Administrator Package (FDA:21 CFR Part11 compliant)**

- Backup

If the “engineers’ account files for referencing” specified in Access Control Utilities is under CS 3000 software folder, back up all files in the folder. In doing so, give “FULL” control to Everyone for the file EngPassword2.odc.

- Restore

Restore the file and reconfigure by the Access Control utility.

- **Backup and Restoration for the SOE Server**

Back up and restore the SQL server database.

**SEE
ALSO**

For more information about the backup and restore SQL server database, refer to:

9.4.3, “Maintenance of SOE Server Databases” in Optional Functions Reference (IM 33J05H10-01EN)

C6.1.3 Backing up and restoring the CAMS for HIS data

In the CAMS for HIS, there is one HIS as the Download Master and the other HISs within the equalization scope.

The data transfer procedure is same in all the HISs, but you must first restore the data of CAMS for HIS on the Download Master HIS. Then, follow the same procedure for restoring data of the other HISs.

This section describes the back up procedure and restoring procedure of the data of CAMS for HIS.

SEE ALSO

For more information about CAMS for HIS download master, refer to:

- “■ System Configuration when Using CAMS for HIS” in A1., “CAMS for HIS Overview” in Consolidated Alarm Management Software Reference (IM 33J05A21-01EN)

■ Backing up CAMS for HIS data

The back up procedure for CAMS for HIS data is as explained below:

1. Log on as an administrator to each HIS of the existing CS 3000 that is within the equalization scope.
2. Disable the CAMS for HIS in the CAMS for HIS tab of the HIS Utility and restart the HIS.
3. In each HIS, backup all the files present in the following CAMS folder.
`<CS 3000 installation folder>\CAMS`

TIP

If you do not need CAMS for HIS historical data, you do not have to back up files in the following folder.

`<CS 3000 installation folder>\CAMS\hist`

The back up of CAMS for HIS data is completed.

■ Operations before restoring CAMS for HIS data

The procedure for the operations that must be completed before starting the restoring work of CAMS for HIS data is as follows:

1. Install the CENTUM VP software on the download master HIS.
 Then, configure IT security settings, distribute licenses, create user account, configure Windows environment settings for each user, set user authentication mode, and set up the Uninterrupted Power Supply (UPS).
2. Shutdown all the HISs that are within the equalization scope.
3. Start download master.
4. Restore the CS 3000 Package Data of databases other than CAMS for HIS.
5. In the `<CENTUM VP installation folder>`, delete the `CAMS\hist` and `CAMS\hisis` folders and all the files within them, if any.

The operations that must be performed before restoring CAMS for HIS data is completed.

■ Restoring CAMS for HIS data on CAMS for HIS download master

Perform the restoring operation of the CAMS for HIS data first for the CAMS for HIS download master. Then, perform the restoring operation for other HISs.

Follow these steps to restore the CAMS for HIS data on CAMS for HIS download master:

- After confirming that CAMS for HIS is disabled, copy the following folders and files from the backed up CAMS for HIS database to the same location under the <CENTUM VP installation folder>.

Folder:

CAMS\Client	(CAMS for HIS Message Monitor data)
CAMS\configurator	(CAMS for HIS configurator data)
CAMS\database	(CAMS for HIS run-time database)
CAMS\defhist	(CAMS for HIS database backup)
CAMS\hist	(CAMS for HIS historical folder)
CAMS\ScenarioFiles	(Scenario files of CAMS for HIS Alarm Generator Tools)
CAMS\Viewer	(CAMS for HIS Historical Viewer data)

Files:

CAMS\CAMSCapture.bin	(Setup OPC A&E server)
CAMS\ServerConfig.xml	(Setup CAMS for HIS Server)
CAMS\SystemScopeDefinition.bin	(Setup Equalization Scope)

- After the files are copied, enable CAMS for HIS in the CAMS for HIS tab of HIS Utility and restart HIS.

If the version of the existing CS 3000 is earlier than R3.08.50, perform steps 3 and 4. If the version is R3.08.50 or later, go to step 5.

- Start the CAMS for HIS Configurator that you were using before upgrading.

Run the following command from the command prompt.

<CENTUM VP installation folder>\CAMS\CAMSConfigurator.exe -o

- In the opened CAMS for HIS Configurator, back up the CAMS for HIS database.
- Open the HIS on which Standard Engineering Function is installed.
- Restore the existing CS 3000 project database into an appropriate location of the HIS that you opened in step 5.
- Start the Project's Attribution Utility.
- Register the project database in the System View.
- Start the System View.
The project database is upgraded automatically to the new version.
- Start the CAMS for HIS migration tool.
- Replace the existing CS 3000 CAMS for HIS database by using the migration tool.
- Start the System View from the HIS that is installed with Standard Engineering Function.
- Select the download master in the System View and run [Download Project Common Section].

Restoring the CAMS for HIS data in the CAMS for HIS download master is completed.

SEE ALSO

For more information about CAMS for HIS migration tool, refer to:

B3.6, "Migration Tool" in Consolidated Alarm Management Software Reference (IM 33J05A21-01EN)

■ Restoring CAMS for HIS data in HISs other than CAMS for HIS download master

Perform this restoring operation after completing the restoring operation in CAMS for HIS download master.

Follow these steps to restore the CAMS for HIS data in HISs other than CAMS for HIS download master:

1. Install the CENTUM VP software on HISs other than the download master. Then, configure IT security settings, distribute licenses, create user account, configure Windows environment settings for each user, set user authentication mode, and set up the Uninterrupted Power Supply (UPS).
2. Restore the CS 3000 Package Data of databases other than CAMS for HIS.
3. In the <CENTUM VP installation folder>, delete CAMS\hist and CAMS\hisis folders and all the files within them.
4. After confirming that CAMS for HIS is disabled, copy the following folders and files from the backed up CAMS for HIS database to the same location under the <CENTUM VP installation folder>.

Folder:

CAMS\Client	(CAMS for HIS Message Monitor data)
CAMS\configurator	(CAMS for HIS configurator data)
CAMS\database	(CAMS for HIS run-time database)
CAMS\defhist	(CAMS for HIS database backup)
CAMS\hist	(CAMS for HIS historical folder)
CAMS\ScenarioFiles	(Scenario files of CAMS for HIS Alarm Generator Tools)
CAMS\Viewer	(CAMS for HIS Historical Viewer data)

Files:

CAMS\CAMSCapture.bin	(Setup OPC A&E server)
CAMS\ServerConfig.xml	(Setup CAMS for HIS Server)
CAMS\SystemScopeDefinition.bin	(Setup Equalization Scope)

5. After data is copied, enable CAMS for HIS in the CAMS for HIS tab of HIS Utility, and then restart the HIS.
6. Start the System View in the HIS installed with Standard Engineering Function.
7. Select the HISs other than the download master in the System View and run [Download Project Common Section].

Restoring the CAMS for HIS data in the HISs other than CAMS for HIS download master is completed.

■ Common operation in all HISs

1. Ensure that CAMS for HIS is enabled for all HISs in the CAMS for HIS tab of HIS Utility.
2. Start the CAMS for HIS Index File Generator in all the HISs.

Restoring the CAMS for HIS data is completed.

**SEE
ALSO**

For more information about CAMS for HIS Index File Generator, refer to:

“■ Improvements in CAMS for HIS Historical Viewer Search” on page C11-27

C6.2 Upgrading from CENTUM CS 1000 to CENTUM VP R6

The Windows OS supported by CENTUM VP R6 are different from those supported by CS 1000; therefore, you need to install the CENTUM VP software anew on a computer running the OS supported by CENTUM VP R6 and then transfer the existing project database.

C6.2.1 Procedures for the Upgrade

This section describes how to upgrade the system.

■ Workflow of the Upgrade

The workflow of the upgrade is as follows. Perform the upgrading tasks according to this flow chart.

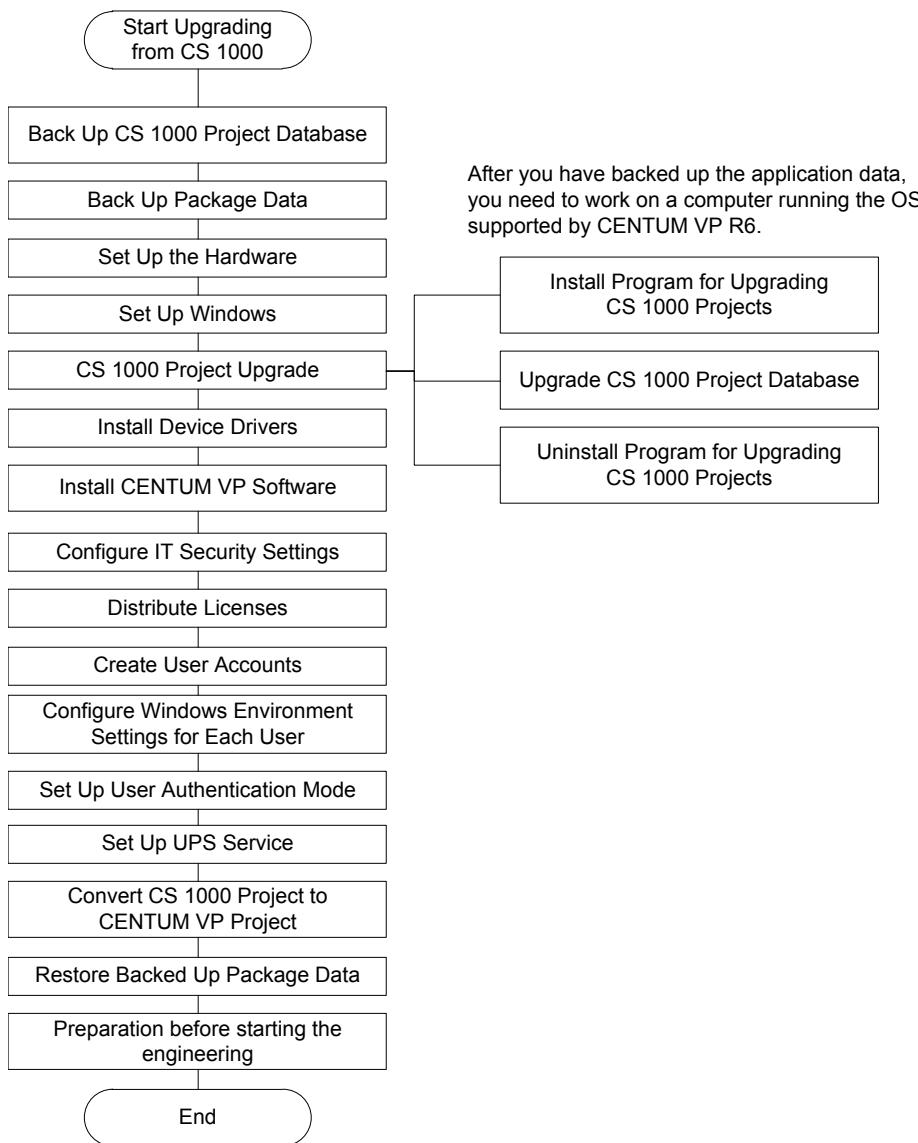


Figure C6.2.1-1 Upgrade Procedure

IMPORTANT

- The program for upgrading CS 1000 projects and of CENTUM VP software must be installed on an OS with which R6 performance is guaranteed. You need to set up Windows before the installation.
- After the conversion of the CS 1000 project database is completed, be sure to uninstall the program for upgrading CS 1000 projects before installing the CENTUM VP software.

■ Back Up CS 1000 Project Database

Back up the necessary project database of CS 1000.

SEE ALSO For more information about backing up the project database, refer to:

C5.2, "Backing Up VP Projects" on page C5-3

■ Back Up Package Data

Back up necessary package data used in CS 1000.

If Access Control function is enabled, disable it.

SEE ALSO For more information about how to back up package data, refer to:

C6.2.2, "Backing up and Restoring CS 1000 Package Data" on page C6-25

For more information about the access control settings, refer to:

2.1, "Rights Check and Engineer Authentication" in Compliance with FDA: 21CFR Part 11 (IM 33J10D21-01EN)

■ Set Up the Hardware

Set up the hardware.

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

B4.1, "Setting Up the Hardware" on page B4-2

■ Set Up Windows

Configure Windows settings.

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

B4.2, "Setting Up Windows" on page B4-7

■ Install the Program for Upgrading CS 1000 Projects

Install the program for upgrading CS 1000 projects on the computer on which CENTUM VP is to be installed. (*1)

*1: Use the same CENTUM VP software medium for the installation.

TIP The program for upgrading CS 1000 projects can only upgrade a CS 1000 project database to a CENTUM VP-compatible revision.

1. Use the Administrator account to log on.
2. Exit from all applications that are running.
3. Insert the CENTUM VP software medium into the DVD-ROM 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 [CS 1000 Project DB conversion] on the installation menu.
The Welcome dialog box appears.

TIP

- If CS 3000 or CENTUM VP software is already installed, an error dialog box is displayed and you cannot install the program.
 - If the Windows redistributable modules required to run CENTUM VP, such as Microsoft .NET Framework, are not already installed, a dialog box appears, prompting you to install such modules.
- Click [Install] to install them. If you click [Cancel], the installation of the CENTUM VP software is discontinued.

The following modules are required for CENTUM VP.

- Microsoft .NET Framework 4.6.2
- MSXML 6.0 SP1
- Microsoft Visual C++ 2017 Redistributable Package
- OPCCOM ProxyStub

When installation of these modules is started, the display in the status field changes accordingly. Restarting the computer may be required after installing the modules. If required, restart the computer and then continue the CENTUM VP installation after the computer is restarted.

5. Click [Next].
A dialog box for specifying the installation folder appears.
6. Specify the destination folder for installation and click [Next].
The Confirm Settings dialog box appears.
7. Confirm the displayed contents and click [Install].
When the installation is completed, the installation completion dialog box appears.
8. Click [Finish] to restart the computer.

■ Upgrade Revision of CS 1000 Project Database

1. Restore the CS 1000 project database before the Upgrade revision in an appropriate location.
2. Start the Project's Attribution Utility.
3. Register the project database in the System View.
4. Start the System View.
The project database is upgraded to the new revision automatically.

SEE ALSO

For more information about the Project's Attribution Utility, refer to:

2.3, "Project's Attribution Utility" in Engineering Reference Vol.1 (IM 33J10D10-01EN)

■ Uninstall the Program for Upgrading CS 1000 Projects

Uninstall the program for upgrading CS 1000 projects in the same procedure as that for uninstalling the CENTUM VP software.

SEE ALSO

For more information about how to uninstall the software, refer to:

C7.1.3, "Uninstalling the CENTUM VP Software" on page C7-10

■ Install Device Drivers

Install communication drivers such as the control bus driver, as well as device drivers such as the USB driver for OPKB.

SEE

ALSO For more information about how to install the device drivers, refer to:

- B4.3, "Configuring Network Settings" on page B4-43
- B4.4, "Installing the USB Driver for the Operation Keyboard" on page B4-77
- B4.5, "Tasks Required for Setting Up the Console Type HIS" on page B4-79

■ Install the CENTUM VP Software

Install the CENTUM VP software in the same procedure as a new installation.

SEE

ALSO For more information about the CENTUM VP software installation procedure, refer to:

- B4.6, "Installing the CENTUM VP Software" on page B4-85

■ Configure IT Security Settings

Configure IT security settings.

SEE

ALSO For more information about IT security, refer to:

- B4.7, "Configuring IT Security Settings" on page B4-94

■ Distribute Licenses

Distribute the licenses to the station.

For upgrading, the license key file comes with a package list. By importing this package list to License Manager, the station configuration definitions and package assignments to each station that are necessary for license distribution are generated.

SEE

ALSO For more information about how to distribute licenses, refer to:

- B4.8, "Distributing and Accepting Licenses" on page B4-101

■ Create User Accounts

Create user accounts.

SEE

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

- B4.9, "Creating User Accounts" on page B4-102

■ 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:

- B4.10, "Configuring Windows Environment Settings for Each User" on page B4-107

■ Set User Authentication Mode

Set up for the desired user authentication mode.

SEE ALSO

For more information about setting the user authentication mode, refer to:

B4.11, "Setting Up for User Authentication Modes" on page B4-135

■ Set Up the Uninterruptible Power Source (UPS) Service

Set up the uninterruptible power source (UPS) service.

SEE ALSO

For more information about setting up the UPS service, refer to:

B4.12, "Setting Up the Uninterruptible Power Supply (UPS) Service" on page B4-149

■ Convert CS 1000 Project to CENTUM VP Project

Use the conversion tool to convert the project database to a CENTUM VP project database.

IMPORTANT

Specifications of the graphic features differ between CS 1000 and CENTUM VP.

To convert CS 1000 graphic files to CENTUM VP R6 graphic files considering the compatibility in display and behaviors, you need to perform specific procedures.

● HIS Database Conversion Tool

If a CS 1000 HIS is included in the project, it will be upgraded to a CENTUM VP HIS. When "HIS Database Conversion Tool" is displayed, select the check boxes of the stations to be converted to CENTUM VP HIS and clear the check boxes of the stations that are not to be converted.

- When HIS is converted to CENTUM VP HIS, all CS 1000 graphic files of the station are automatically converted to CENTUM VP graphic formats.
- You also can start "HIS Database Conversion Tool" from the Tool menu of System View by selecting [HIS Database Conversion Tool].

SEE ALSO

For more information about the procedure to convert CS 1000 graphic files to CENTUM VP graphic files considering the compatibility in display and behaviors, refer to:

Graphic Conversion Guide (IM 33J01C40-01EN)

● Graphic File Converter

You can use the Graphic File Converter to convert CS 1000 graphic files to CENTUM VP graphic files, file by file. The graphic files converted to CENTUM VP formats can be imported and edited using the CENTUM VP graphic builder.

Follow these steps to convert graphic files:

1. Start the Graphic File Converter.
2. Add the CS 1000 graphic file or folder to be converted.
3. Specify the output target folder and click [Convert].
A dialog box showing the progress of the conversion appears.

TIP

If the file conversion is successful, Successful appears in the Status column, Failed if unsuccessful, when the conversion is finished.

-
4. Click [Close] to exit the Graphic File Converter.

SEE ALSO

For more information about the procedure to convert CS 1000 graphic files to CENTUM VP graphic files considering the compatibility in display and behaviors, refer to:

Graphic Conversion Guide (IM 33J01C40-01EN)

■ Restore Backed Up Package Data

Restore the data for each package that was backed up.

SEE ALSO

For more information about how to restore data for each package, refer to:

C6.2.2, "Backing up and Restoring CS 1000 Package Data" on page C6-25

■ Note on Instrument Faceplate Highlight

From CENTUM VP R5.03.00, the instrument faceplate highlight function is supported. This feature can be turned off.

SEE ALSO

For more information about instrument faceplate highlight, refer to:

2.7, "Highlighting of Instrument Faceplates" in Human Interface Stations Reference Vol.2 (IM 33J05A11-01EN)

For more information about turning on/off the instrument faceplate highlight, refer to:

“● Instrument Faceplate Highlight” in “■ The Settings on Action Tab” in 1.2, “The Settings on HIS Utility” in Human Interface Stations Reference Vol.1 (IM 33J05A10-01EN)

C6.2.2 Backing up and Restoring CS 1000 Package Data

This section identifies the data that need to be backed up and describes how to back up and restore them.

■ Data Required to be Backed Up and Restored

Package data you need to back up and restore are listed in the following table.

Back up in CS 1000 and restore in CENTUM VP.

Table C6.2.2-1 Backup and Restoration of CS 1000 Package Data

Package	Name	Related CENTUM VP R6 Packages	Data to back up/restore
PHS1101	Standard Operation and Monitoring Function	VP6H1100	<ul style="list-style-type: none"> • HIS Setup Information • Database Related to HIS
PHS4200	Historical Message Integration Package (meeting FDA Regulations)	VP6H4200	The data stored in the Historical message integration server
PHS4700	Advanced Alarm Filter Package	VP6H4700	Advanced alarm filter configuration data
PHS6510	Long-Term Data Archive Package	VP6H6510	Long-term storage data
PHS6530	Report Package	VP6H6530	Report configuration data
PHS6710	FCS Data Setting/Acquisition Package (PICOT)	VP6H6710	Configuration data
PHS5100	Standard Builder Function (*1)	VP6E5100	Project database
PHS5110	Access Control Package	VP6E5110	Configuration data
PHS5151	Graphic Builder	VP6E5150	Project database
PHS5160	CS Batch 1000 Builder(*2)	VP6E5165	Project database
PHS5161	CS Batch 1000 Recipe Management Package(*3)	VP6E5166	Recipe database
PHS5170	Access Administrator Package(FDA:21 CFR Part 11 compliant)	VP6E5170	Audit trail database

*1: For CENTUM VP R6, this corresponds to Standard Engineering Function.

*2: For CENTUM VP R6, this corresponds to Batch Builder.

*3: For CENTUM VP R6, this corresponds to Recipe Management Package.

■ Backing UP and Restoring the Data to Be Backed Up While CS 1000 Is Running

You need to back up the following data while CS 1000 is running.

Make a backup, and restore it using the Import function in each package.

IMPORTANT

Backing up and restoration of a project database covers the data of the Standard Builder Function, Graphic Builder Package, CS Batch 1000 Builder, and CS Batch 1000 Recipe Management Package.

● Standard Operation and Monitoring Function - HIS Setup Information

1. Export and import HIS configuration data

Using Export function in HIS Setup, back up HIS Registry data.

For restoring HIS configuration data after installation, edit the backup file (File extension: .reg) as follows using a text editor, and import it.

- Before : HKEY_LOCAL_MACHINE\SOFTWARE\YOKOGAWA\BenKei\HIS\COMMON
- After : HKEY_LOCAL_MACHINE\SOFTWARE\YOKOGAWA\CS3K\HIS\COMMON

2. Set Number of Tags

On the Station tab of HIS Setup, set a new Number of Tags for CENTUM VP.

SEE ALSO

For more information about export and import functions of the HIS Setup window, refer to:

“■ [Import] and [Export] of HIS Setup Window” in 4.3, “HIS Setup Window” in Human Interface Stations Reference Vol.1 (IM 33J05A10-01EN)

● Historical Message Integration Package

The data stored in the Historical message integration server can be inherited. To inherit the data, you need to perform on each HIS the task to maintain the continuity of sequence numbers of the historical message files stored in the Historical message integration server and set up the destination folder for storing historical messages again.

- Back up sequence numbers on each HIS

Log on as an administrative user and run the following command to stop the operation and monitoring function.

```
<CS 1000 installation folder>\his\tool\BKHHisStop.exe
```

Use Explorer to save the file with the latest sequence number from among the following files onto a removable medium.

```
<CS 1000 installation folder>\Log\HISHIST\HISHISTnnnn-YYYYMMDD.log (nnnn: sequence number)
```

- Tasks on the Historical message integration server

Log on as an administrative user and copy the file with the latest sequence number that you have saved to the folder corresponding to each HIS on the Historical message integration server.

Folder on the server: <Share name>\HisHist\HISddss (dd: domain number; ss: station number)

TIP

From the names of the folders in the above storage location on the server, you can find out the HISs that are under consolidated historical message management. If the HIS before replacement is damaged and the latest historical message file is unavailable, refer to the HIS folder in the above storage location on the server and keep a record of the sequence number. In this case, you cannot port the latest historical message file to the server.

- Restore the sequence number

Log on to the upgraded HIS as an administrative user and run the following command to stop the operation and monitoring function.

```
<CENTUM VP installation folder>\his\tool\BKHHisStop.exe
```

Make the following HISHIST storage folder empty.

Storage folder: <CENTUM VP installation folder>\Log\HISHIST

Execute the following command at the command prompt.

<CENTUM VP installation folder>\his\tool\SetSeqNo.batΔ<the latest sequence number you kept in step 2> (Δ: space character)

Restart the HIS and confirm that a historical message file of the sequence number you backed up plus one has been created in the HISHIST folder.

Configure the server storage definition file and connect to the Historical message integration server to start the storing of messages.

SEE ALSO

For more information about setting up the storage destination folder, refer to:

8.1.1, "Setting Up the Storage Destination Folder for Historical Message Save Files" in Human Interface Stations Reference Vol.2 (IM 33J05A11-01EN)

- **Advanced Alarm Filter Package**

- Backup

Using the Export function in the Advanced Alarm Filter package, back up the filter configurations.

- Restore

Using the Import function in the Advanced Alarm Filter package, restore the filter configurations.

SEE ALSO

For more information about details of Export and Import of alarm filter definition, refer to:

7.5.3, "Advanced Alarm Filter Window" in Human Interface Stations Reference Vol.2 (IM 33J05A11-01EN)

- **Long-Term Data Archive Package**

- Backup

The archive feature of the Long-Term Data Archive Package can be used to backup the data to the external storage medium for long-term storage.

The BKHLogFile.txt in the following path should also be archived.

\\\LTDATA\LOG\BKHLogFile.txt

- Restore

The retrieve feature of the Long-Term Data Archive Package can be used to restore the backup files from the external storage medium to the hard disk of HIS.

The BKHLogFile.txt file should be restored to the following path or to the path where it was archived from.

SEE ALSO

For more information about details of archiving and retrieving operations, refer to:

4.2.4, "Archival and Retrieval Operations" in Optional Functions Reference (IM 33J05H10-01EN)

- **Report Package**

- Backup

Copy a report definition file into a removable storage medium by using the copy tool of the report package.

- Restore

Copy a report definition file in the removable storage medium into the restored computer by using the copy tool of the report package.

SEE ALSO

For more information about copying report configuration data, refer to:

- “■ Copy to Other Computer” in 2.5.3, “Report Printout on Other Computer” in Optional Functions Reference (IM 33J05H10-01EN)
- 2.1, “Settings for Report Package” in Optional Functions Reference (IM 33J05H10-01EN)

■ Backing UP and Restoring the Data to Be Backed Up While CS 1000 Is Not Running

You need to back up the following data offline before deleting the CS 1000 folder.

Before backing up the data on CS 1000, you must completely exit all operation and monitoring functions of CS 1000. When restoring the data on CENTUM VP, you must exit all CENTUM VP functions.

After you install CENTUM VP, make a copy of those data to a relatively same location under <CENTUM VP installation folder>. If a file with the same name exists in the destination folder, overwrite it.

● Operation and Monitoring Function - HIS-related Database

You need to bac kup the voice message configuration, media data, context menus configuration. The backups of these data can be restored later. However, if the voice messages were not applied, same as other customized functions such as context menus, the files may not exist for backup if the function are not used.

1. In command prompt, run the following command, and stop the operation and monitoring functions.
`<CS1000 installation folder>\his\tool\BKHHisstop.exe`
2. Back up and restore the following HIS-related files. Folder name of restored data:
`<CENTUM VP installation folder>\his\database\ops\MediaDef.odb`: Voice message configuration file
`<CS1000 installation folder>\his\Media\User`: Media data (User\ All files in this folder)
`<CS1000 installation folder>\his\spconf\BKHMenuDef.xml`: Context menus configuration file

● FCS Data Setting/Acquisition Package (PICOT)

1. Exit PICOT

In the Windows taskbar, click PICOT to open. From File menu, select [Exit]. PICOT exits.

2. Back up and restore configuration files.

- Backup

Make a backup copy of the setup file stored in the following folder.

`<CS 1000 installation folder>\his\users\save\BKUPICOT`

- Restore

Restore the backed-up file to the following folder.

`<CENTUM VP installation folder>\his\users\save\BKUPICOT`

SEE ALSO

For more information about details of definition files, refer to:

- 3.2, “Component Files and Processing Flow of PICOT” in Optional Functions Reference (IM 33J05H10-01EN)

- **Access Control Package and Access Administrator Package (FDA:21 CFR Part11 compliant)**

- Backup

If “engineers’ account files for referencing” specified in Access Control Utilities is under the CS 1000 installation folder, back up all files in the folder. In the backup, add Full control to Everyone for the file EngPassword2.odc.

- Restore

Restore the file and set up in Access Control Utilities.

C6.3 Upgrading CENTUM VP R4/R5 to R6

The Windows OS supported by CENTUM VP R4/R5 are different from CENTUM VP R6 except for one part. Therefore, you need to install the CENTUM VP software on a PC running the OS supported by CENTUM VP R6 and then transfer the existing project database.

TIP

If the existing CENTUM project is already installed in the OS supported by CENTUM VP R6, skip the following steps.

- Back up the CENTUM project database
- Back up the package data
- Set up the hardware

■ Workflow of the Upgrade

The workflow of the upgrade is as follows. Perform the upgrading tasks according to this flow chart.

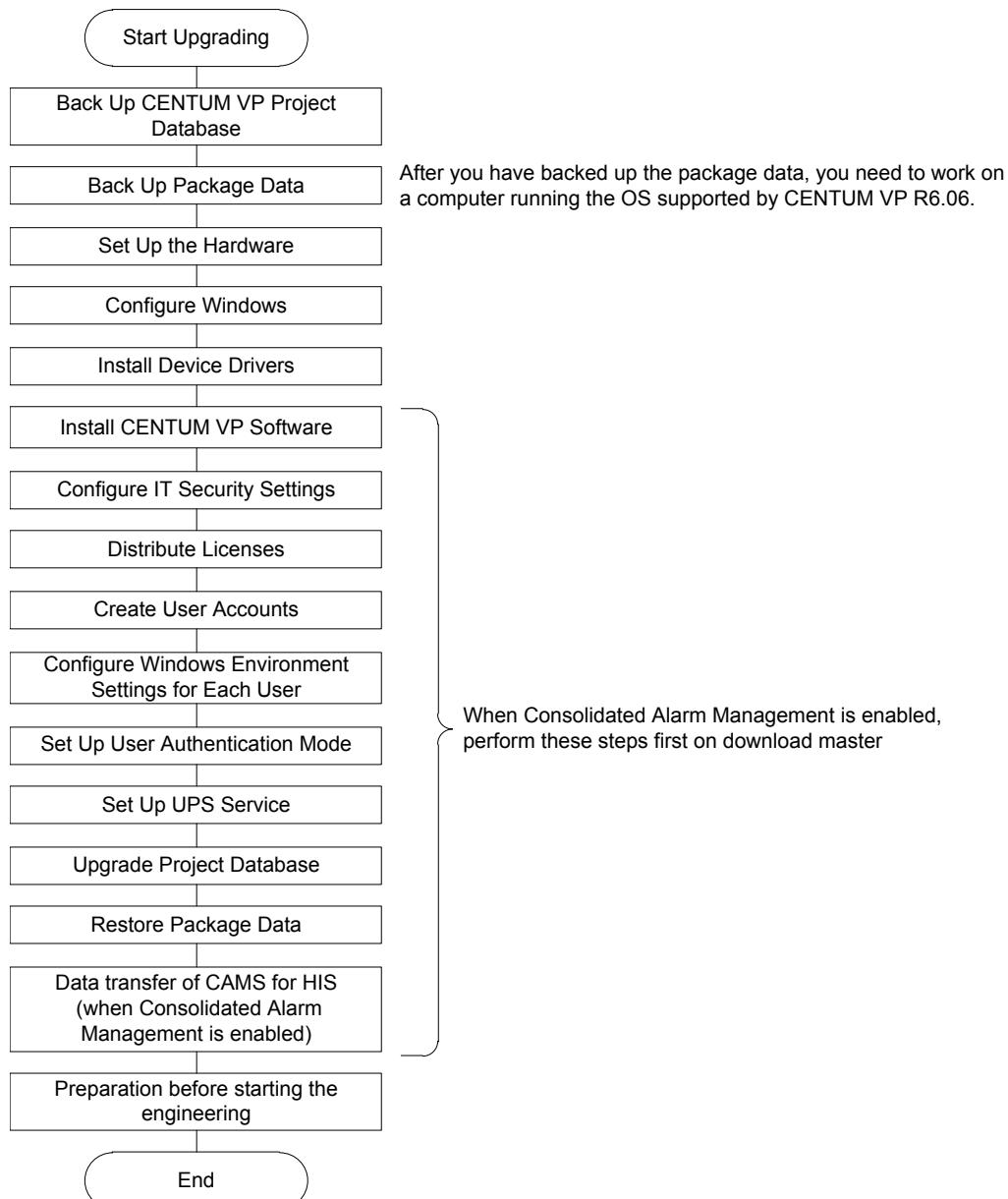


Figure C6.3-1 Upgrade Procedure

■ Back up the CENTUM project database

In the existing CENTUM project, back up the required project database.

If the existing CENTUM project is already installed in the OS supported by CENTUM VP R6, skip this step.

SEE ALSO

For more information about backing up the project database, refer to:

C5.2, "Backing Up VP Projects" on page C5-3

■ Back up package data

In the package that you are using in the existing CENTUM project, back up package-wise data that is required to be saved.

If the existing CENTUM project is already installed in the OS supported by CENTUM VP R6, skip this step.

■ Setting up the hardware

Perform hardware setting.

If the existing CENTUM project is already installed in the OS supported by CENTUM VP R6, skip this step.

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

B4.1, "Setting Up the Hardware" on page B4-2

■ Setting up Windows

Configure Windows settings.

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

B4.2, "Setting Up Windows" on page B4-7

■ Installing the Device Drivers

Install communication drivers such as control bus driver, as well as device drivers such as USB driver for OPKB.

If the existing CENTUM project is already installed in the OS supported by CENTUM VP R6, update the device drivers.

SEE ALSO For more information about how to install the device drivers, refer to:

- B4.3, "Configuring Network Settings" on page B4-43
- B4.4, "Installing the USB Driver for the Operation Keyboard" on page B4-77
- B4.5, "Tasks Required for Setting Up the Console Type HIS" on page B4-79

■ Update Device Drivers

The procedure for upgrading drivers are shown as follows.

● Control Bus Driver

1. Uninstall the control bus driver.
2. Install the control bus driver.
3. Configure Windows Network.

SEE ALSO For more information about uninstalling the control bus driver, refer to:

"■ Uninstalling Control Bus Driver" on page C7-13

For more information about installing the control bus driver, refer to:

B4.3.1, "Installing the Control Bus Driver" on page B4-44

For more information about configuring Windows network settings, refer to:

B4.3.4, "Configuring Windows Network Settings" on page B4-51

● Vnet/IP Open Communication Driver

1. Uninstall the Vnet/IP open communication driver.
2. Install the Vnet/IP open communication driver.
3. Configure Windows Network.

SEE ALSO

For more information about uninstalling the Vnet/IP open communication driver, refer to:

“■ Uninstalling the Vnet/IP Open Communication Driver” on page C7-14

For more information about installing the Vnet/IP open communication driver, refer to:

B4.3.2, “Installing the Vnet/IP Open Communication Driver” on page B4-46

For more information about configuring Windows network settings, refer to:

B4.3.4, “Configuring Windows Network Settings” on page B4-51

● RAS Driver – If AIP261/AIP262 Card is Continuously Used

1. Uninstall the RAS driver.
2. Install the RAS driver.

SEE ALSO

For more information about uninstalling the RAS driver, refer to:

“■ Uninstalling RAS Driver” on page C7-18

For more information about installing the RAS driver, refer to:

“■ Installing the RAS Driver” on page B4-82

● RS-232C Driver – If AIP261/AIP262 Card is Continuously Used

1. Uninstall the RS-232C driver.
2. Install the RS-232C driver.

SEE ALSO

For more information about uninstalling the RS-232C driver, refer to:

“■ Uninstalling RS-232C Driver” on page C7-18

For more information about installing the RS-232C driver, refer to:

“■ Installing the RS-232C Driver” on page B4-79

● USB Driver for Operation Keyboard

1. Uninstall the USB driver for operation keyboard.
2. Install the USB driver for operation keyboard.

IMPORTANT

Shut down the HIS before you install the USB driver for operation keyboard. When the installation of the USB driver for operation keyboard is complete, the HIS restarts.

**SEE
ALSO**

For more information about uninstalling the USB driver for operation keyboard, refer to:

“■ Uninstalling the USB Driver for OPKB” on page C7-17

For more information about installing the USB driver for operation keyboard, refer to:

B4.4, “Installing the USB Driver for the Operation Keyboard” on page B4-77

■ Install the CENTUM VP Software

Install the CENTUM VP software.

TIP

The CENTUM VP software installation is the same as a new installation procedure with the following difference.

- As for CENTUM VP R4, a dialog box is displayed to confirm the upgrade installation
When the dialog box for confirming the upgrade installation is displayed, click [Next].
The following settings are not required as they are acquired from the information that has been installed.
 - Name
 - Company name
 - Installation folder
 - Station type
 - Reference database
 - Console type of the station
- A dialog box is displayed to update custom faceplate file.
If the custom faceplates were defined in HIS with CENTUM VP R4, the existing custom faceplate files can be automatically converted in CENTUM VP R6 custom faceplate files. This conversion is performed right before the installation is completed. While this conversion is being done, a progress bar is displayed.
- Procedure when the software restriction policy is applied with IT security setting.
When the software restriction policy is applied to CENTUM VP R4 or R5 with IT security setting, right-click Launcher.exe in the top folder of the software media and select [Run as administrator] to start the installer.

**SEE
ALSO**

For more information about the CENTUM VP software installation procedure, refer to:

B4.6, “Installing the CENTUM VP Software” on page B4-85

■ Configure IT Security Settings

Configure IT security settings.

**SEE
ALSO**

For more information about IT security, refer to:

B4.7, “Configuring IT Security Settings” on page B4-94

■ Distribute Licenses

If the system is upgraded from CENTUM VP R4, distribute licenses to the station. If the system is upgraded from CENTUM VP R5, upgrade the licenses before you distribute them to the station.

**SEE
ALSO**

For more information about distributing licenses, refer to:

B4.8, “Distributing and Accepting Licenses” on page B4-101

■ Create User Accounts

Create user accounts.

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

B4.9, "Creating User Accounts" on page B4-102

■ 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:

B4.10, "Configuring Windows Environment Settings for Each User" on page B4-107

■ Set User Authentication Mode

Set up for the desired user authentication mode.

SEE ALSO For more information about setting the user authentication mode, refer to:

B4.11, "Setting Up for User Authentication Modes" on page B4-135

■ Set Up the Uninterruptible Power Source (UPS) Service

Set up the uninterruptible power source (UPS) service.

SEE ALSO For more information about setting up the UPS service, refer to:

B4.12, "Setting Up the Uninterruptible Power Supply (UPS) Service" on page B4-149

■ Upgrade the Project Database

In the case of a computer installed with only system builders, starting System View and opening the project database will automatically upgrade the database. During the upgrade, the graphic file update tool is automatically started to convert the R4 graphic files to the latest graphic format.

● Cautionary Notes for the Graphic File Update Tool

Keep in mind the following points when using the graphic file update tool.

- The user cannot select the stations for which the graphic files are to be upgraded. All stations will be the target.
- The only stations targeted for the upgrade of the graphic files are the HISs of R4.01.00 and later.
- The graphic file update tool cannot be cancelled once executed.

● Graphic File Update Tool Target Files

The following files are upgraded.

- Graphic files of a revision between R4.01.00 and R4.03.00
(File extension: edf)
- Working graphic files of a revision between R4.01.00 and R4.03.00

(File extension: wkf)

- Link parts files of a revision between R4.01.00 and R4.03.00
(File extension: lpx)
- User-defined default files of a revision between R4.01.00 and R4.03.00

TIP

Files with the .sva extension will be upgraded when upgrading the graphic builder. The sva files and graphic files created on R4 or the older version will be converted to the latest graphic format while imported on the graphic builder.

■ Transferring CAMS for HIS data when upgrading

In the CAMS for HIS, there is one HIS as the Download Master and the other HISs within the equalization scope.

The data transfer procedure is same in all the HISs, but you must first restore the data of CAMS for HIS on the Download Master HIS. Then, follow the same procedure for restoring the data of other HISs.

This section describes the back up procedure and restoring procedure of the data of CAMS for HIS.

SEE ALSO

For more information about CAMS for HIS download master, refer to:

- System Configuration when Using CAMS for HIS" in A1., "CAMS for HIS Overview" in Consolidated Alarm Management Software Reference (IM 33J05A21-01EN)

● Backing up the CAMS for HIS data

You must backup the data of CAMS for HIS after completing the backup procedure of other package data and while the CAMS for HIS is disabled.

Follow these steps to back up the CAMS for HIS data:

1. Log on as an administrator into each HIS of the existing CENTUM project within the equalization scope.
2. Disable the CAMS for HIS in the CAMS for HIS tab of the HIS Utility, and then restart the HIS.
3. In each HIS, backup all the files present in the following CAMS folder.
<CENTUM installation folder>\CAMS

TIP

If you do not need CAMS for HIS historical data, you do not have to back up files in the following folder.

- <CENTUM installation folder>\CAMS\hist
- <CENTUM installation folder>\CAMS\hisis (if present)

The back up of CAMS for HIS data is completed.

● Operations before restoring CAMS for HIS data

You must restore the data of CAMS for HIS after restoring the HIS related databases and while the CAMS for HIS is disabled.

Follow these steps for operations that must be completed before starting the restoring work of CAMS for HIS data:

1. Install CENTUM VP software in the download master HIS.
Then, configure IT security settings, distribute licenses, create user account, configure Windows environment settings for each user, set user authentication mode, and set up the Uninterrupted Power Supply (UPS).

2. Shutdown all the HISs within the equalization scope.
3. Start download master.
4. Restore the package data of CENTUM project of databases other than CAMS for HIS.
5. In the <CENTUM VP installation folder>, delete CAMS\hist and CAMS\hisis folders and all the files within them, if any.

The operations that must be performed before restoring CAMS for HIS data is completed.

● Restoring CAMS for HIS data on CAMS for HIS download master

Perform the restoring operation of CAMS for HIS data first for the CAMS for HIS download master. Then, perform the restoring operation on other HISs.

Follow these steps to restore the CAMS for HIS data on CAMS for HIS download master:

1. After confirming that CAMS for HIS is disabled, copy the following folders and files from the backed up CAMS for HIS database to the same location under <CENTUM VP installation folder>.

Folders:

CAMS\Client	(CAMS for HIS Message Monitor data)
CAMS\configurator	(CAMS for HIS configurator data)
CAMS\database	(CAMS for HIS run-time database)
CAMS\defhist	(CAMS for HIS database backup)
CAMS\hist	(CAMS for HIS historical folder)
CAMS\hisis	(If present)
CAMS\ScenarioFiles	(Scenario files of CAMS for HIS Alarm Generator Tools)
CAMS\Viewer	(CAMS for HIS Historical Viewer data)
CAMS\Save	(Alarm set value management data)

Files:

CAMS\CAMSCapture.bin	(Setup OPC A&E server)
CAMS\ServerConfig.xml	(Setup CAMS for HIS Server)
CAMS\SystemScopeDefinition.bin	(Setup Equalization Scope)

2. After the files are copied, enable CAMS for HIS in the CAMS for HIS tab of HIS Utility and restart HIS.

If the version of the existing CENTUM project is earlier than CS 3000 R3.08.50, perform steps 3 and 4. If the version is CS 3000 R3.08.50 or later, go to step 5.

3. Start the CAMS for HIS Configurator that you were using before upgrading.

Run the following command from the command prompt.

<CENTUM VP installation folder>\CAMS\CAMSConfigurator.exe -o

4. In the opened CAMS for HIS Configurator, back up CAMS for HIS database.

5. Open the HIS on which Standard Engineering Function is installed.

6. Restore the existing CENTUM project database into an appropriate location of the HIS that you opened in step 5.

7. Start the Project's Attribution Utility.

8. Register the project database in the System View.

9. Start the System View.

The project database is upgraded automatically to the new version.

If the version of the existing CENTUM project is earlier than CENTUM VP R4.02, perform steps 10 and 11. If the version is CENTUM VP R4.02 or later, go to step 12.

10. Start the CAMS for HIS migration tool.
11. Replace the CAMS for HIS database of CENTUM project by using the migration tool.
12. Start the System View in the HIS installed with Standard Engineering Function.
13. Select the download master in the System View and run [Download Project Common Section].

Restoring the CAMS for HIS data in the CAMS for HIS download master is completed.

SEE ALSO

For more information about CAMS for HIS migration tool, refer to:

B3.6, "Migration Tool" in Consolidated Alarm Management Software Reference (IM 33J05A21-01EN)

- **Restoring CAMS for HIS data in HISs other than CAMS for HIS download master**

Perform this restoring operation after completing the restoring operation in CAMS for HIS download master.

Follow these steps to restore the CAMS for HIS data in HISs other than CAMS for HIS download master:

1. Install the CENTUM VP software in all HISs other than download master. Then, configure IT security settings, distribute licenses, create user account, configure Windows environment settings for each user, set user authentication mode, and set up the Uninterrupted Power Supply (UPS).
2. Restore the package data of CENTUM project of databases other than CAMS for HIS.
3. In the <CENTUM VP installation folder>, delete CAMS\hist and CAMS\hisis folders and all the files within them.
4. After confirming that CAMS for HIS is disabled, copy the following folders and files from the backed up CAMS for HIS database to the same location under <CENTUM VP installation folder>.

Folders:

CAMS\Client	(CAMS for HIS Message Monitor data)
CAMS\configurator	(CAMS for HIS configurator data)
CAMS\database	(CAMS for HIS run-time database)
CAMS\defhist	(CAMS for HIS database backup)
CAMS\hist	(CAMS for HIS historical folder)
CAMS\hisis	(If present)
CAMS\ScenarioFiles	(Scenario files of CAMS for HIS Alarm Generator Tools)
CAMS\Viewer	(CAMS for HIS Historical Viewer data)
CAMS\Save	(Alarm set value management data)

Files:

CAMS\CAMSCapture.bin	(Setup OPC A&E server)
CAMS\ServerConfig.xml	(Setup CAMS for HIS Server)
CAMS\SystemScopeDefinition.bin	(Setup Equalization Scope)

5. After data is copied, enable CAMS for HIS in the CAMS for HIS tab of HIS Utility, and then restart the HIS.

6. Start the System View in the HIS installed with Standard Engineering Function.
7. Select the HIS other than download master in the System View and run [Download Project Common Section].

Restoring the CAMS for HIS data in the HISs other than CAMS for HIS download master is completed.

- **Common operation in all HIS**

1. Ensure that CAMS for HIS is enabled for all HISs in the CAMS for HIS tab of HIS Utility. If the version of the existing CENTUM project is earlier than CENTUM VP R5.01, perform step 2.
2. Start the CAMS for HIS Index File Generator in all the HISs.

Restoring the CAMS for HIS data is completed.

**SEE
ALSO**

For more information about CAMS for HIS Index File Generator, refer to:

“■ Improvements in CAMS for HIS Historical Viewer Search” on page C11-27

C6.4 Upgrading CENTUM R6 to a Later Revision

This section describes the procedure for upgrading CENTUM VP R6 to a later revision on a computer.

■ Scope of Software Revision Upgrade

The CENTUM VP software must be of the same revision for each VP project. Upgrading the CENTUM VP software to a later revision is explained by using the following examples where the scope of required revision upgrade is different.

- When there is one VP project
- When there are multiple AD projects and VP projects
- When the AD server and system builders coexist on a single computer

● Scope of Software Revision Upgrade When There Is One VP Project

The following figure shows an example of system configuration when there is one VP project.

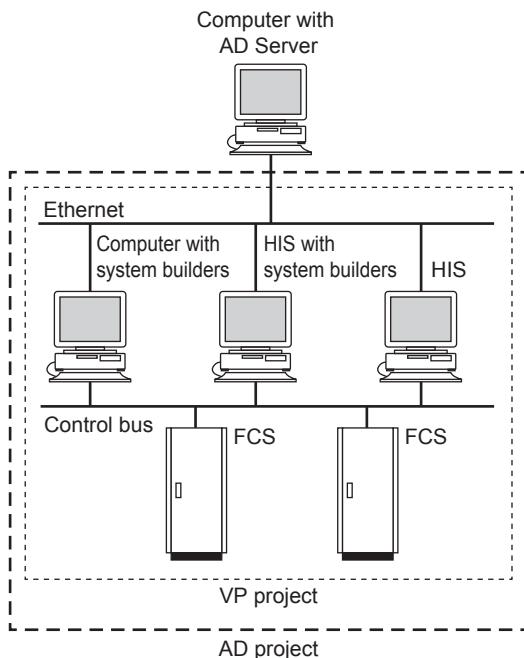


Figure C6.4-1 Example of System Configuration When There Is One VP Project

With the system configuration in the figure, upgrading the CENTUM VP software to a later revision requires the software to be upgraded to the same revision on all computers and HISs including the computer with AD server.

● Scope of Software Revision Upgrade When There Are Multiple AD Projects and VP Projects

The AD server permits registration of multiple AD projects, and multiple VP projects can be registered under one AD project. And, computers with system builders and HISs are registered to a VP project.

The following figure shows an example of this system configuration.

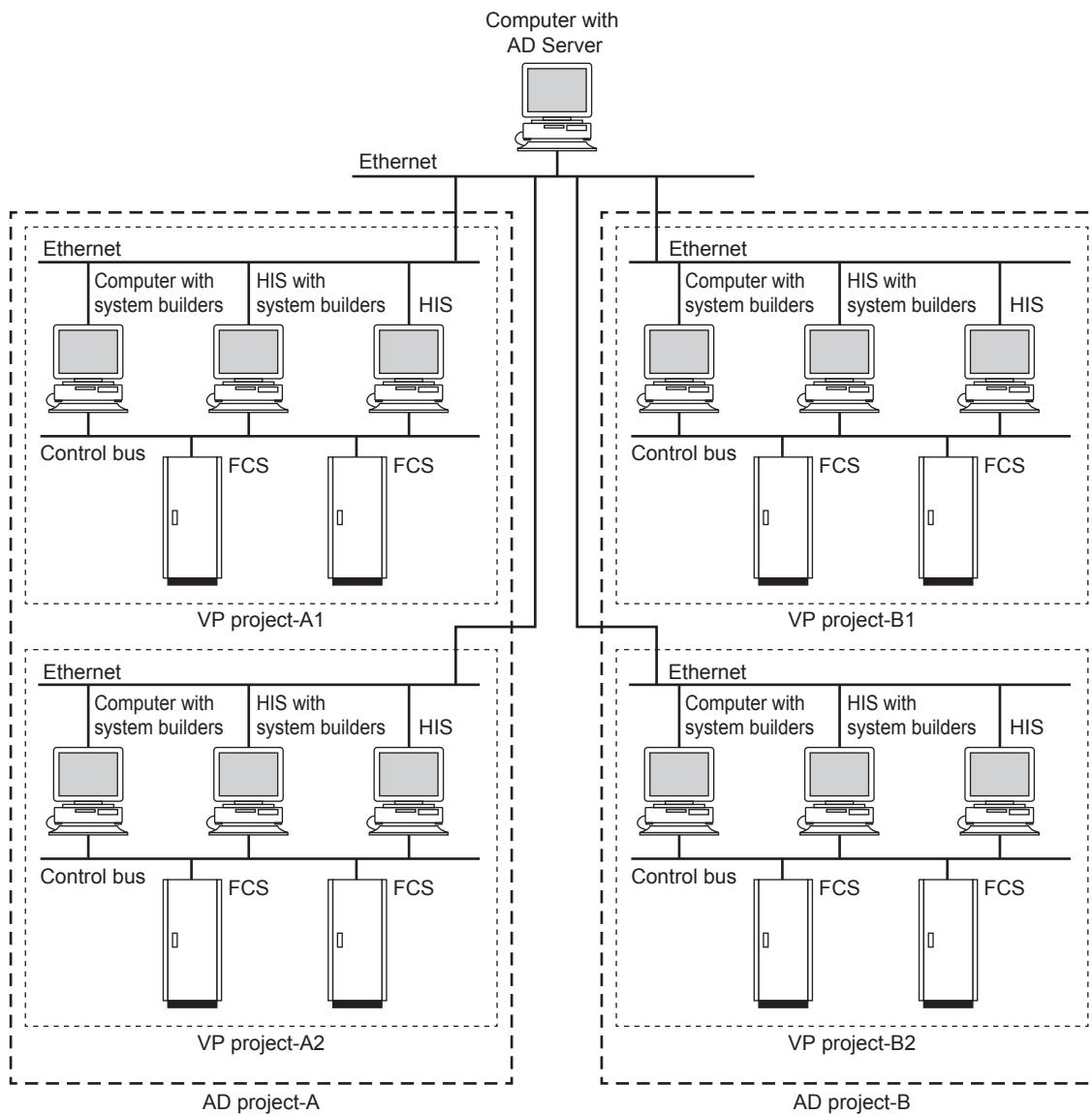


Figure C6.4-2 Example of System Configuration When There Are Multiple AD Projects and VP Projects

With the system configuration in the figure, it is recommended that, when upgrading the CENTUM VP software to a later revision, the software be upgraded to the same revision on all computers and HISs including the computer with AD server.

If the software cannot be upgraded to the same revision on all computers with system builders and HISs, make sure that the same revision is used in each VP project. Even in this case, be sure to upgrade the AD server to the latest revision.

In the example shown in the figure, the following configuration is possible.

- AD server: Latest revision
- VP project-A1 computers and HISs software: Latest revision
- VP project-A2 computers and HISs software: Older revision
- VP project-B1 computers and HISs software: Older revision
- VP project-B2 computers and HISs software: Older revision

IMPORTANT

- If multiple revisions coexist like this, you must upgrade the AD server to the latest revision.
You can use AD Organizer if the revision of the AD server is newer than that of the system builders, but you cannot if the revision of the AD server is older.
- If VP projects of different revisions coexist, you can view, but cannot edit, the settings of the FCSs that are added with a newer revision by using the AD Organizer of the older revision. You cannot view or edit the settings of the nodes and I/O modules that belong to FCS of the station type that is added with a newer revision by using the AD Organizer of the older revision.

● Scope of Software Revision Upgrade When the AD Server and System Builders Coexist on a Single Computer

The AD server and system builders can coexist on a single computer.

The following figure shows an example of system configuration when there are multiple AD projects and VP projects and the AD server and system builders coexist on a single computer.

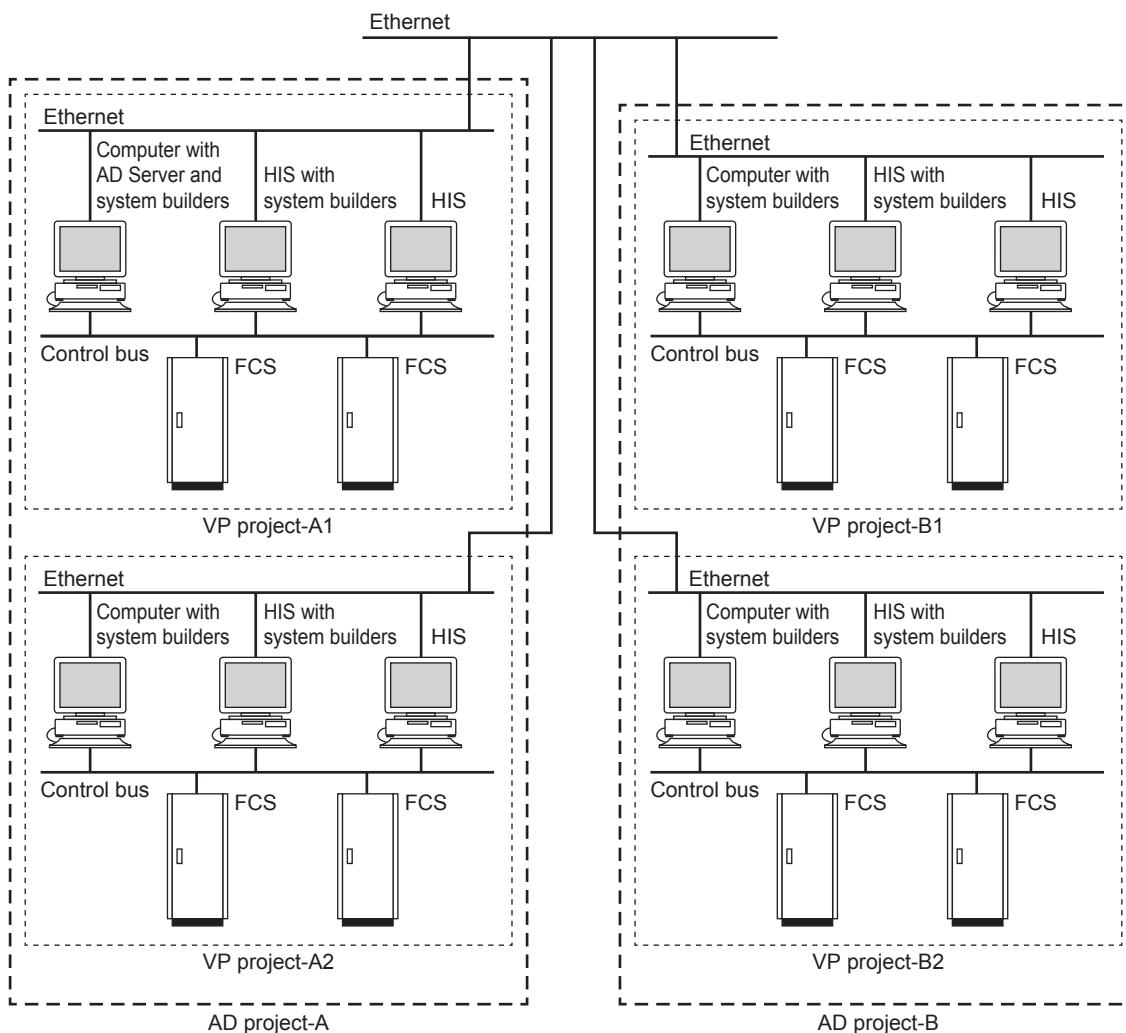


Figure C6.4-3 Example of System Configuration When the AD Server and System Builders Coexist on a Single Computer

In the figure, the AD server is installed on the VP project-A1 computer.

If the AD server and system builders coexist on a single computer, the AD server and system builders cannot be of different revisions.

With the system configuration in the figure, upgrading the AD server to the latest revision requires the software to be upgraded to the latest revision at least on all VP project-A1 computers and HISs.

If the software cannot be upgraded on all VP project-A1 computers and HISs, change the system configuration by moving the AD server to an independent computer and upgrading it to the latest revision, or moving the AD server to a computer or HIS in a VP project where software will be upgraded to the latest revision.

TIP

To move the AD server, back up the ADMDB on the AD server at the source, and then restore the ADMDB on the AD server at the destination.

IMPORTANT

If VP projects of different revisions coexist, you can view, but cannot edit, the settings of the FCSs that are added with a newer revision by using the AD Organizer of the older revision. You cannot view or edit the settings of the nodes and I/O modules that belong to FCS of the station type that is added with a newer revision by using the AD Organizer of the older revision.

SEE ALSO

For more information about backing up and restoring the ADMDB, refer to:

C1.1.2, "Backing up and restoring the ADMDB" in Automation Design Suite Basics (IM 33J10A10-01EN)

■ Workflow of the Upgrade

The following figure shows the workflow for upgrading a computer on which CENTUM VP software is already installed.

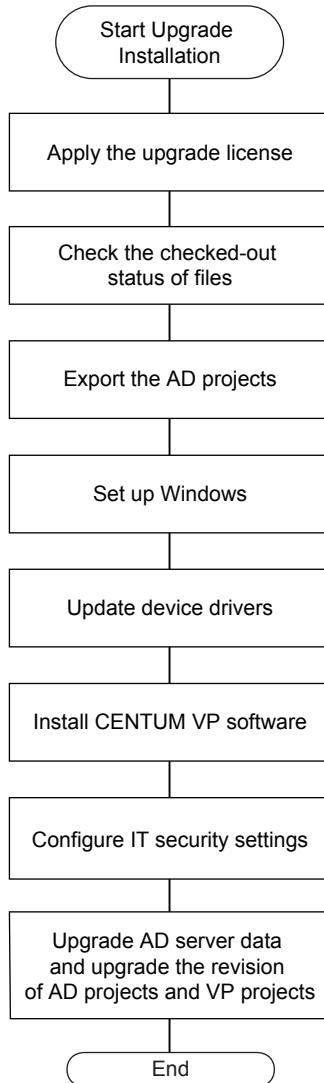


Figure C6.4-4 Upgrade Procedure

IMPORTANT

When you upgrade CENTUM VP software, install the new version by overwriting the earlier version without uninstalling it.

If you uninstall R6.04 or later versions, the new version of CENTUM VP software cannot be installed. In that case, reinstall the uninstalled CENTUM VP software and overwrite it with the new version.

■ Applying the Upgrade License

Distribute and accept the upgrade licenses when you upgrade CENTUM VP R6.04 or later versions. If the upgrade licenses are already accepted, you need not take any action.

IMPORTANT

Make sure that the issue date of the newer version of CENTUM VP is earlier than the date of expiry of the upgrade license.

SEE ALSO

For more information about distribute and accept upgrade licenses, refer to:

- Distributing and accepting upgrade licenses” in 5., “Working with upgrade licenses” in License Management (IM 33J01C20-01EN)

■ Checking the Checked-out Status of Files

Make sure that all files have been checked in for all AD projects on the AD server. If one or more files are currently checked out, use AD Organizer to check it/them in or cancel its/their checked-out status, or use the ADS Administration Tool to forcibly cancel its/their checked-out status.

IMPORTANT

You must check in, or cancel the checked-out status of, a file or files currently checked out, before upgrading the CENTUM VP software to a later revision.

Upgrade the CENTUM VP software first, and then upgrade the AD projects. If any of the files remains checked out, the revision upgrade of AD projects fails with an error.

TIP

There is no need to generate the file being modified before the revision upgrade. The master status and work status of AD project files do not change before and after the revision upgrade. Files modified before the revision upgrade can be subjected to generation after the revision upgrade.

SEE ALSO

For more information about how to check the checked-out status of AD project files, refer to:

- C1.1.9, “Forcibly canceling the checked-out status of currently checked out files” in Automation Design Suite Basics (IM 33J10A10-01EN)
- C1.3.7, “Forcibly canceling the checked-out status of currently checked out files” in Automation Design Suite Basics (IM 33J10A10-01EN)

■ Exporting AD Projects

Export the AD projects as a way of backing them up so that they can be restored in case the revision upgrade encounter a problem.

Back up all VP projects to the AD projects, and then export all AD projects including the revision history information.

SEE ALSO

For more information about backing up VP projects to an AD project, refer to:

- Backing up a VP project to the AD project” in ■ Operating VP projects” in B1.5.1, “Managing VP projects” in Automation Design Suite Basics (IM 33J10A10-01EN)

For more information about exporting AD projects, refer to:

- C1.3.4, “Exporting AD projects” in Automation Design Suite Basics (IM 33J10A10-01EN)

■ Setting Up Windows

The procedure to configure Windows is as follows:

- **Applying the Root Certificate**

When upgrading from R6.03.10 or earlier on a Windows 7 or Windows Server 2008 R2 computer, apply the root certificate.

**SEE
ALSO**

For more information about the procedure for applying the root certificate in Windows 7, refer to:

“■ Applying the root certificate” on page B4-22

For more information about the procedure for applying the root certificate in Windows Server 2008 R2, refer to:

“■ Applying the root certificate” on page B4-41

● **Installing the Windows Update Programs**

If all the following conditions are satisfied, download and apply the Windows update programs.

- Upgrading from version R6.04.00 or earlier.
- The OS is Windows 7 or Windows Server 2008 R2.

**SEE
ALSO**

For more information about Windows update program, refer to:

“● Downloading the Windows Update Program (Windows 7 or Windows Server 2008 R2)” on page B1-4

■ **Updating Device Drivers**

The procedures for updating drivers are shown as follows.

● **Control Bus Driver**

1. Uninstall the control bus driver.
2. Install the new control bus driver.
3. Configure Windows network settings.

**SEE
ALSO**

For more information about uninstalling the control bus driver, refer to:

“■ Uninstalling Control Bus Driver” on page C7-13

For more information about installing the control bus driver, refer to:

B4.3.1, “Installing the Control Bus Driver” on page B4-44

For more information about configuring Windows network settings, refer to:

B4.3.4, “Configuring Windows Network Settings” on page B4-51

● **Vnet/IP Open Communication Driver**

1. Uninstall the Vnet/IP open communication driver.
2. Install the new Vnet/IP open communication driver.
3. Configure Windows network settings.

**SEE
ALSO**

For more information about uninstalling the Vnet/IP open communication driver, refer to:

“■ Uninstalling the Vnet/IP Open Communication Driver” on page C7-14

For more information about installing the Vnet/IP open communication driver, refer to:

B4.3.2, “Installing the Vnet/IP Open Communication Driver” on page B4-46

For more information about configuring Windows network settings, refer to:

B4.3.4, “Configuring Windows Network Settings” on page B4-51

● Vnet/IP Interface Package

If a virtual machine is used, follow these steps:

1. Uninstall the Vnet/IP Interface Package.
2. Install the new Vnet/IP Interface Package.
3. Configure Windows network settings.

SEE ALSO

For more information about uninstalling the Vnet/IP Interface Package, refer to:

“■ Uninstalling the Vnet/IP Interface Package on a Virtual Machine” on page C7-15

For more information about installing the Vnet/IP Interface Package, refer to:

B4.3.3, “Installing the Vnet/IP Interface Package on a Virtual Machine” on page B4-48

For more information about configuring Windows network settings, refer to:

B4.3.7, “Notes on Using a Virtual Machine” on page B4-75

● RAS Driver – If the AIP261/AIP262 Card is Continuously Used

1. Uninstall the RAS driver.
2. Install the new RAS driver.

SEE ALSO

For more information about uninstalling the RAS driver, refer to:

“■ Uninstalling the Vnet/IP Interface Package on a Virtual Machine” on page C7-15

For more information about installing the RAS driver, refer to:

“■ Installing the RAS Driver” on page B4-82

● RS-232C Driver – If the AIP261/AIP262 Card is Continuously Used

1. Uninstall the RS-232C driver.
2. Install the new RS-232C driver.

SEE ALSO

For more information about uninstalling the RS-232C driver, refer to:

“■ Uninstalling RS-232C Driver” on page C7-18

For more information about installing the RS-232C driver, refer to:

“■ Installing the RS-232C Driver” on page B4-79

● USB Driver for Operation Keyboard

1. Uninstall the USB driver for operation keyboard.
2. Install the new USB driver for operation keyboard.

IMPORTANT

Shut down the HIS before you install the USB driver for operation keyboard. When the installation of the USB driver for operation keyboard is complete, the HIS restarts.

**SEE
ALSO**

For more information about uninstalling the USB driver for operation keyboard, refer to:

“■ Uninstalling the USB Driver for OPKB” on page C7-17

For more information about installing the USB driver for operation keyboard, refer to:

B4.4, “Installing the USB Driver for the Operation Keyboard” on page B4-77

■ Installing the CENTUM VP Software

Install the CENTUM VP software.

TIP

Upgrade installation of the CENTUM VP software is basically the same as for a new installation, except the following points:

- Since the following items are gathered automatically from the previously installed contents, there is no need to enter them again.
 - Name
 - Company name
 - Installation folder
 - Station type
 - Location of project database
 - Console type of the station
- After installation of CENTUM VP software, the message announcing to wait for a while is displayed during the activation of the software packages.

**SEE
ALSO**

For more information about the CENTUM VP software installation procedure, refer to:

B4.6, “Installing the CENTUM VP Software” on page B4-85

● Precautions at Installation of .NET Framework

Any attempt to install .NET Framework may fail if CENTUM VP software is installed on a computer where the legacy IT security model is applied. If this error occurs, perform the work-around.

**SEE
ALSO**

For more information about the workaround for failing to install .NET Framework, refer to:

C10.1.6, “Failing to install .NET Framework” on page C10-9

■ Configuring IT Security Settings

Configure IT security settings.

**SEE
ALSO**

For more information about IT security, refer to:

B4.7, “Configuring IT Security Settings” on page B4-94

■ Upgrading the AD Server Data and Upgrading the Revision of AD Projects and VP Projects

Upgrade the AD server data and upgrade the AD projects and VP projects to a later revision.

SEE

ALSO For more information about upgrading the AD server data and upgrading the revision of AD projects and VP projects, refer to:

B2., "How to start engineering after upgrading the CENTUM VP software" in Automation Design Suite Basics (IM 33J10A10-01EN)

C6.5 Upgrading the Computer Dedicated to License Management

This section describes how to upgrade the computer dedicated to license management.

■ Version up Procedure

1. Set up Windows.
2. Install only the license management software from the CENTUM VP 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

3. Version up the license.
4. Configure IT security settings.
5. Configure Windows environment settings for each user.

SEE ALSO

For more information about setting up Windows, refer to:

“● Set Up Windows” on page B7-1

For more information about the procedure for installing the license management software, refer to:

B7., “Setting Up the Computer Dedicated to License Management” on page B7-1

For more information about version up procedure of license, refer to:

4., “Upgrading the Licenses from CENTUM VP R5 to R6, or from ProSafe-RS R3 to R4” in License Management (IM 33J01C20-01EN)

For more information about IT security, refer to:

B4.7, “Configuring IT Security Settings” on page B4-94

For more information about configuring Windows environment settings for each user, refer to:

“● Configure Windows Environment Settings for Each User” on page B7-3

■ Upgrade Procedure

1. When upgrading from R6.03.10 or earlier, set up Windows.
2. Install only the license management software from the CENTUM VP 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

3. Configure IT security settings.

4. When upgrading from R6.03.10 or earlier, configure Windows environment settings for each user.

**SEE
ALSO**

For more information about setting up Windows, refer to:

- “● Set Up Windows” on page B7-1

For more information about the procedure for installing the license management software, refer to:

- B7., “Setting Up the Computer Dedicated to License Management” on page B7-1

For more information about IT security, refer to:

- B4.7, “Configuring IT Security Settings” on page B4-94

For more information about configuring Windows environment settings for each user, refer to:

- “● Configure Windows Environment Settings for Each User” on page B7-3

C6.6 Replacing the Operation Keyboard

In CENTUM VP R5.03.00 or later versions, the following operation keyboards are available:

- Operation Keyboard for Single-loop Operation (Model: AIP830)
- Operation Keyboard for Eight-loop Simultaneous Operation (Model: AIP831)

To replace the operation keyboard with AIP830 or AIP831, you must perform the required tasks according to the type of the currently used operation keyboard.

IMPORTANT

You cannot replace the eight-loop operation keyboard of enclosed display style console-type HIS or open display style console-type HIS with AIP830 or AIP831. You can only replace the single-loop operation keyboard of open display style console-type HIS with AIP830.

■ Replacing the USB Operation Keyboard (AIP827) with AIP830

No particular task is required when replacing AIP827 with AIP830. Just replace the operation keyboard.

■ Replacing the USB Operation Keyboard (AIP827) with AIP831

Replace the operation keyboard, and then distribute and accept the license for AIP831.

**SEE
ALSO**

For more information about distributing and activating licenses, refer to:

B4.8, "Distributing and Accepting Licenses" on page B4-101

■ Replacing the Single-loop Operation Keyboard of Open Display Style Console-type HIS with AIP830

1. Replace the operation keyboard.
2. Install the USB driver for the operation keyboard.
3. On the [Action] tab of HIS Utility, select [Configuration Operation Keyboard] > [Serial Port No.] > [USB].

**SEE
ALSO**

For more information about installing the USB driver for operation keyboard, refer to:

B4.4, "Installing the USB Driver for the Operation Keyboard" on page B4-77

C6.7 Replacing the Card for Control Bus

With CENTUM VP, you must use the control bus interface card or the Vnet/IP interface card as the card for control bus. When replacing any of these cards, you must uninstall and reinstall the driver.

■ Procedure for Replacing the Card for Control Bus

Follow these steps to replace the card for control bus:

1. With the card installed, uninstall the driver.

TIP

If both the control bus driver and the Vnet/IP open communication driver are installed, uninstall both.

2. Turn off the power of the computer and replace the card.
3. Turn on the power of the computer, and install the drivers that are required for the new card.

SEE ALSO

For more information about the procedure for uninstalling the driver, refer to:

C7.1.4, “Uninstalling the Device Drivers” on page C7-13

For more information about the procedure for installing the driver, refer to:

B4.3, “Configuring Network Settings” on page B4-43

Blank Page

C7. Uninstalling the CENTUM VP Software

This section describes how to uninstall the CENTUM VP software and device drivers. Procedures are provided for the following two cases:

- Uninstallation on the CENTUM stations or computers
- Uninstallation on the computer dedicated to license management

Note, however, that uninstalling the CENTUM VP software does not remove the project database, user settings, registries, and so on. If you need to remove CENTUM VP software completely, reinstall your operating system.

C7.1 Uninstallation on the CENTUM Stations or Computers

This section describes the procedure for uninstallation on the CENTUM stations or computers.

Related stations or computers are shown as follows.

- HIS
- APCS
- SIOS
- GSGW
- UGS
- UACS station
- Computers installed with only system builders
- Computers installed with only AD server
- CENTUM VP stations and computers on the virtualization platform

IMPORTANT

When CENTUM VP is installed on the same computer with ProSafe-RS, do not uninstall CENTUM VP. If the function is no longer needed, delete the licenses of CENTUM VP packages.

C7.1.1 Disabling the CENTUM Desktop Environment Settings

If the Standard Operation and Monitoring Functions, FDA: 21 CFR Part 11 Compliant Package or the Access Control Package is activated, you need to delete the registered users on the User Environment Settings window and clear the check box for [Enable HIS Type Single Sign On] before uninstalling the CENTUM VP software.

■ Disabling Procedure

1. Logon as an administrative user.
2. Start HIS Utility.
3. On the User tab, click [Setting].
The User Environment Settings dialog box appears.

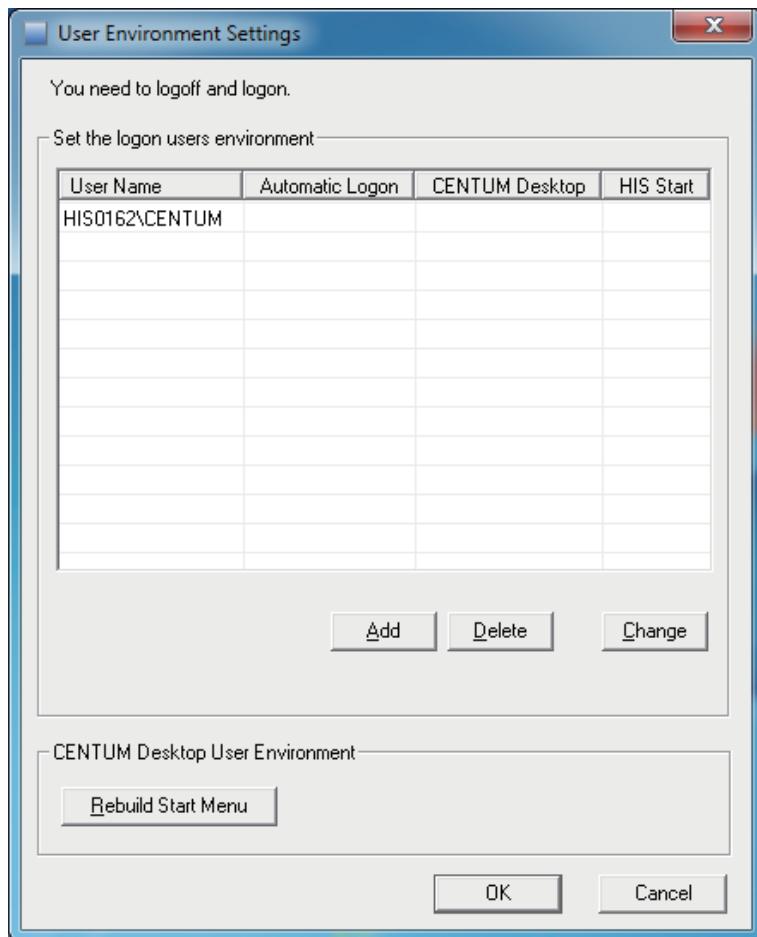


Figure C7.1.1-1 User Environment Settings Dialog Box (Environment Settings for Each Logon User)

4. Select the user and click [Delete].
The Delete User dialog box appears.

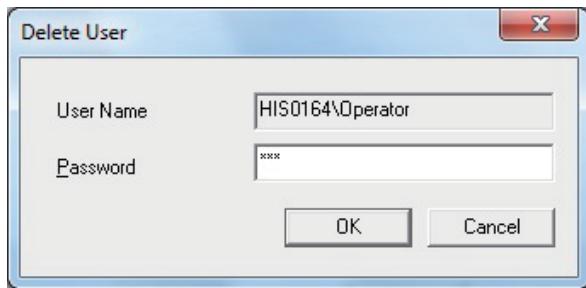


Figure C7.1.1-2 Delete User Dialog Box

5. Enter the password for the selected user and click [OK].
6. Repeat steps 4 and 5 to delete all users.
7. In the case of Windows Authentication mode, clear the check box for [Enable HIS Type Single Sign On].
8. Click [OK] to close the User Environment Settings dialog box and the HIS Utility dialog box.

C7.1.2 Restoring Various Windows Settings

When the CENTUM VP software was installed, some of the Windows settings were automatically changed. This section describes how to restore these Windows settings when uninstalling the CENTUM VP software.

IMPORTANT

Do not restore Windows settings if any YOKOGAWA product other than CENTUM VP (ProSafe-RS, PRM, etc.) is installed on the computer and you will continue to use it.

■ Showing Account Icons in the Logon Display

1. Log on as an administrative user.
2. Open Control Panel.
3. Select [System and Security] > [Administrative Tools] > [Local Security Policy].
The Local Security Policy window appears.
4. In left pane, select [Local Policies] > [Security Options] to display Policy.
Policy is displayed in the right pane.
5. From the Policy list, double-click [Interactive logon: Do not display last user name].
The properties dialog box for that policy appears.

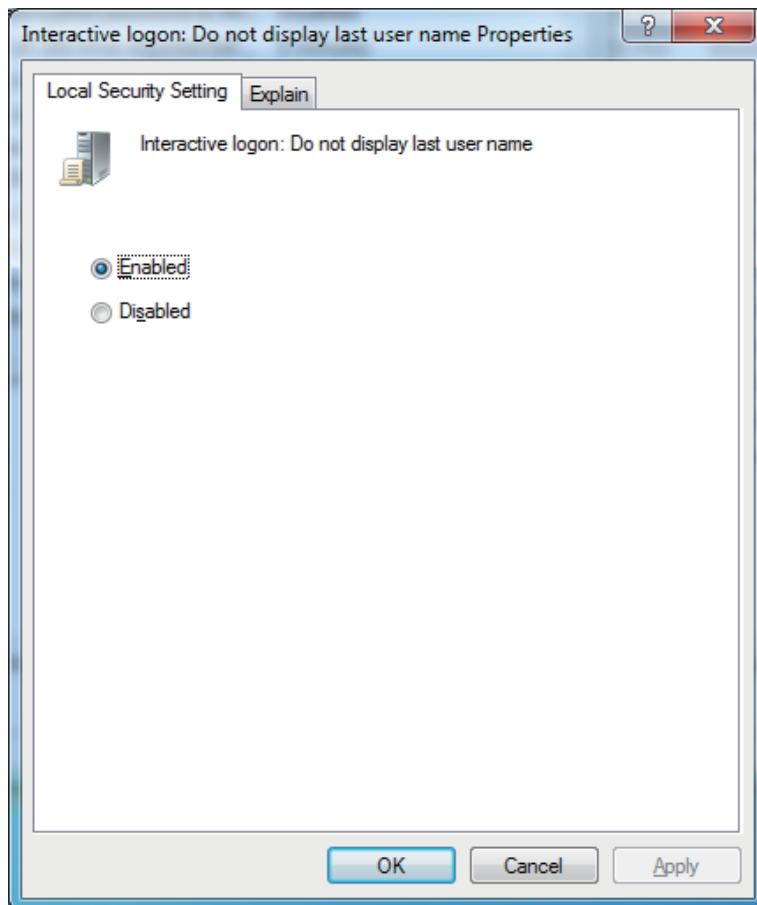


Figure C7.1.2-1 Properties of Interactive logon: Do not display last user name

6. Select [Disabled] and click [OK].

7. Restart the computer.

■ Enabling Fast User Switching

1. Log on as an administrative user.
2. Open Command Prompt.
3. Enter `gpedit.msc`.
Local Group Policy Editor appears.
4. In the left pane, select [Computer Configuration] > [Administrative Templates] > [System] > [Logon] and double-click [Hide entry points for Fast User Switching].
The properties dialog box for that policy appears.

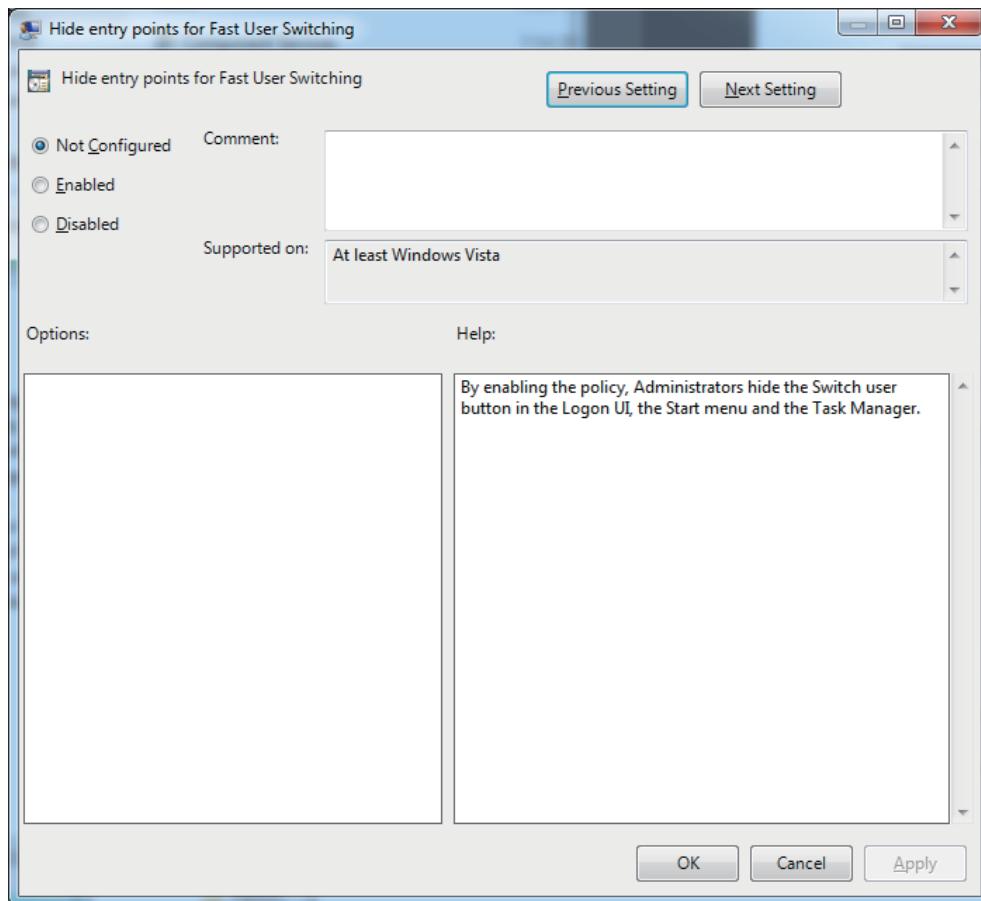


Figure C7.1.2-2 Properties of Hide entry points for Fast User Switching

5. Select [Disabled] and click [OK].
6. Restart the computer.

■ Enabling Windows Security Center Alerts

The procedures for enabling Windows Security Center alerts are described. This setting should be done for each user account.

IMPORTANT

In Windows 10, this operation is not required because alerts are enabled automatically.

- **For Windows 7 or Windows Server 2008 R2**

1. Log on using the user account for which to enable Action Center alerts.
2. Open Control Panel.
3. Set Small icons for the display on the Control Panel .
4. Choose [Notification Area Icons] from the displayed items.
The Notification Area Icons dialog box appears.

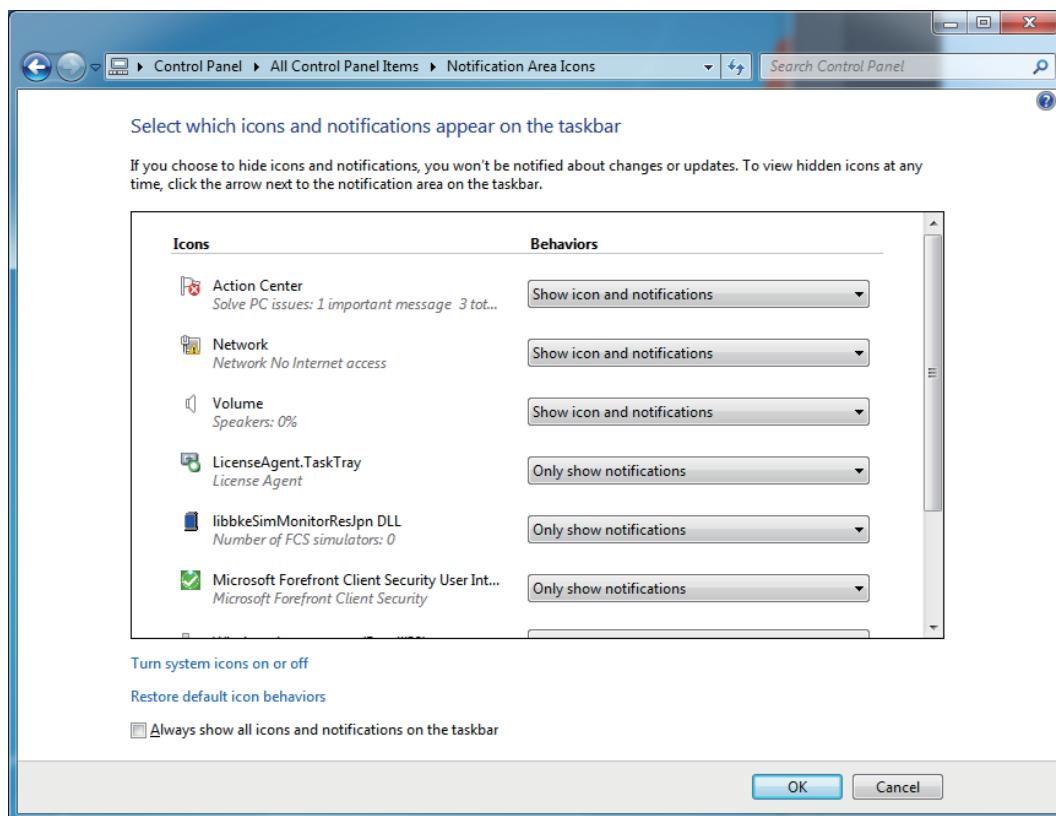


Figure C7.1.2-3 Notification Area Icons Dialog Box

5. Set the Action Center setting to [Show icon and notifications].

■ Enabling Windows Update

This section describes how to enable Windows Update.

- **For Windows 10 or Windows Server 2016**

1. Sign in as an administrative user.
2. Open Command Prompt.
3. Enter `gpedit.msc`.
Local Group Policy Editor appears.
4. In the left pane, select [Computer Configuration] > [Administrative Templates] > [Windows Components] > [Windows Update].
5. In the right pane, double-click [Configure Automatic Updates].
The Configure Automatic Updates dialog box appears.
6. Select [Enabled] and click [OK].

- **For Windows 7 or Windows Server 2008 R2**

1. Log on using an administrative user account.
2. Open Control Panel.
3. Select [System and Security] > [Windows Update].
The Windows Update window appears.
4. Click [Change Settings].
The Change Settings window appears.

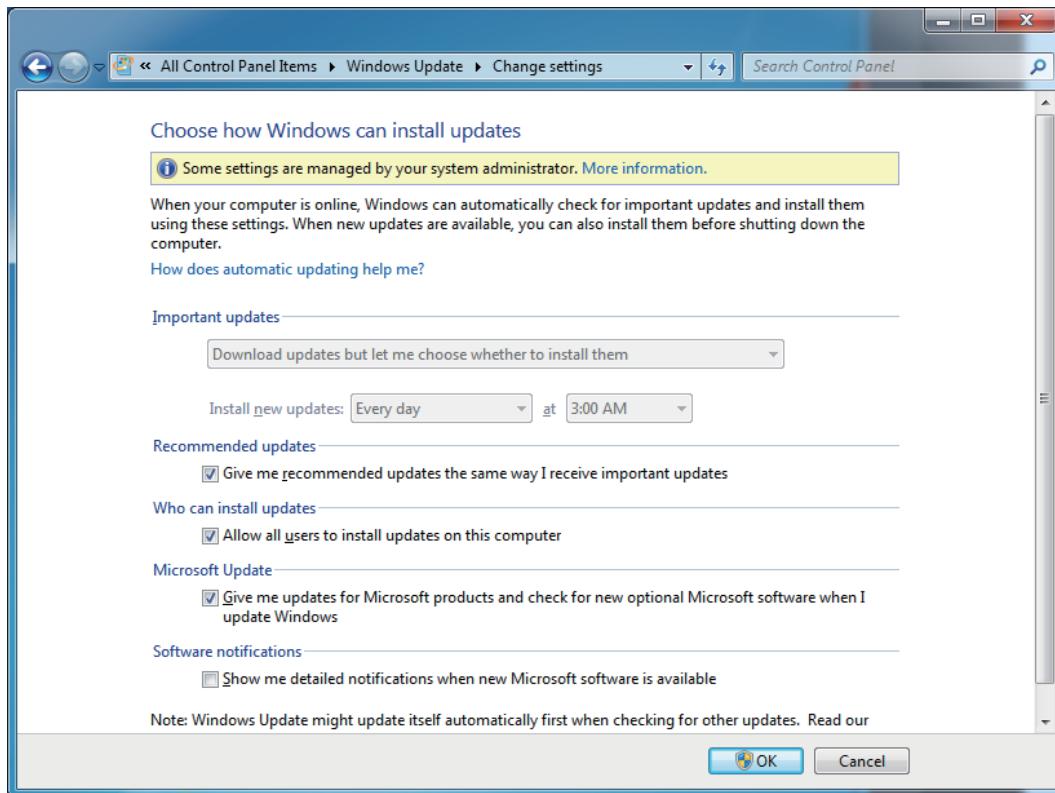


Figure C7.1.2-4 Change Settings

5. Set the Important updates setting to [Install updates automatically] and click [OK].

■ Enabling Windows Defender

Windows Defender is a standard feature of Windows 10 and Windows 7 that defends the computer against all the unwanted software such as spyware and other threats to security.

- **For Windows 10 or Windows Server 2016**

1. Sign in as an administrative user.
2. Open Command Prompt.
3. Enter `gpedit.msc`.
Local Group Policy Editor appears.
4. In the left pane, select [Computer Configuration] > [Administrative Templates] > [Windows Components] > [Windows Defender].
5. In the right pane, double-click [Turn off Windows Defender].
The Turn off Windows Defender dialog box appears.

6. Select [Not Configured] and click [OK].

- **For Windows 7**

1. Logon as an administrative user.
2. Open Control Panel.
3. Select [Large icons] or [Small icons] from the View drop-down list, and select [Windows Defender].
A dialog box appears, informing that this program is disabled.

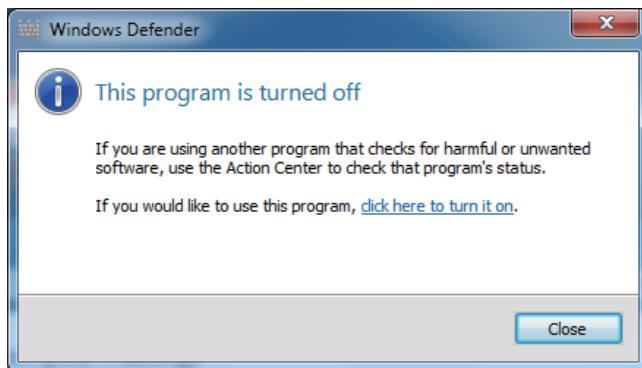


Figure C7.1.2-5 Windows Defender

4. Click [[click here to turn it on](#)].
Windows Defender starts.
5. Click [X] to close the Windows Defender window.

C7.1.3 Uninstalling the CENTUM VP Software

This section describes how to uninstall the CENTUM VP software.

If you uninstall the CENTUM VP software, the license management software is also uninstalled. However, the license management data, IT Security Tool, customized items of each software package, and project data will not be deleted.

TIP

The IT Security Tool is also used by YOKOGAWA products other than CENTUM VP. Therefore, even if you uninstall the CENTUM VP 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 computer, you need to delete the licenses to deactivate the individual software packages before uninstalling the CENTUM VP software.

1. Log on as an administrative user.
2. Terminate all the running applications.
3. If the Standard Operation and Monitoring Functions or the Access Control Package is activated and automatic starting of HIS and automatic logon to HIS are set, disable them using HIS Utility.
4. Delete the licenses to deactivate any packages that are activated.

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 33J01C20-01EN)

■ Uninstallation Procedure

After deactivating the packages (deleting the licenses), follow these steps to uninstall the CENTUM VP software:

1. Open Control Panel.
2. Select [Programs] > [Programs and Features].
The Programs and Features window appears.

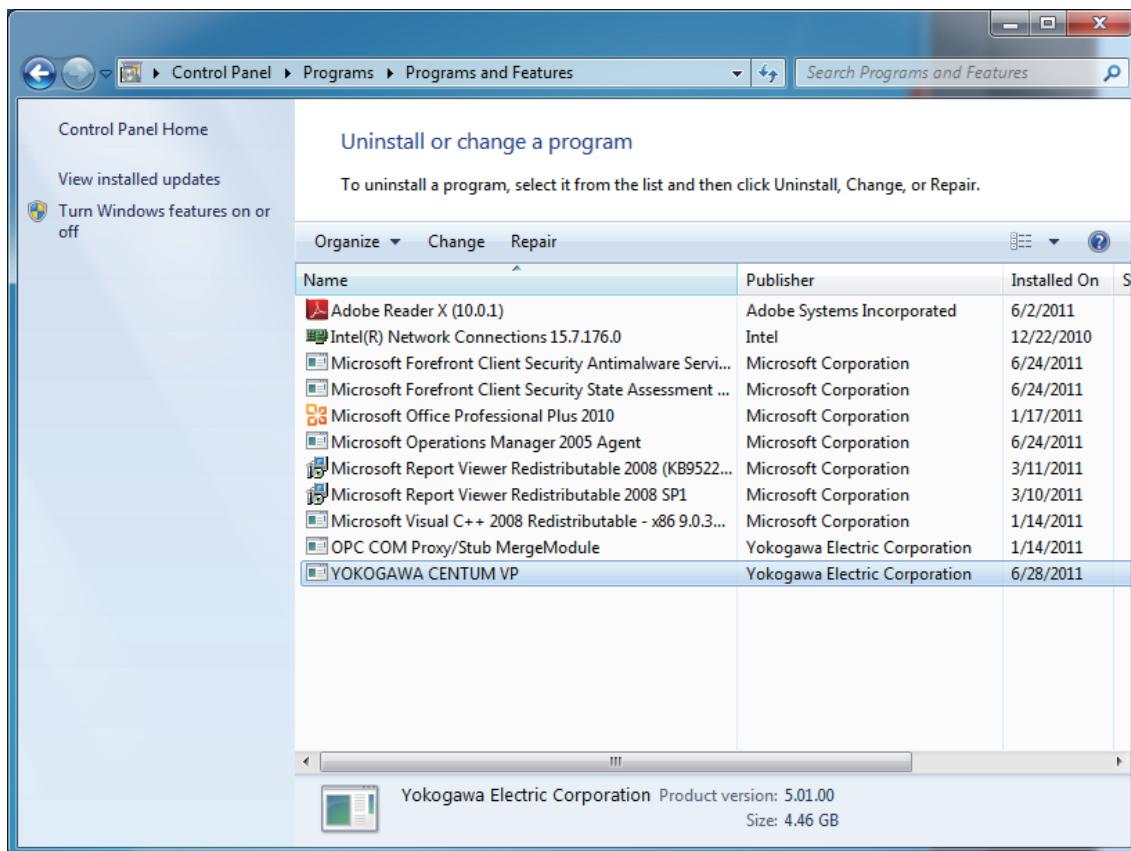


Figure C7.1.3-1 Programs and Features window

3. Select [YOKOGAWA CENTUM VP] 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.

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.

6. 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.

7. 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].

■ Uninstalling the IT Security Tool

Even if you uninstall the CENTUM VP software, the IT Security Tool remains.

To uninstall the IT Security Tool, follow these steps:

IMPORTANT

If the following YOKOGAWA products remain on the computer, do not uninstall the IT Security Tool.

- PRM : R3.10 or later
 - ProSafe-RS : R3.01 or later
 - Exaopc : R3.70 or later
 - Exapilot : R3.90 or later
 - Exaplog : R3.40 or later
-

1. Log on as an administrative user.
2. Insert the CENTUM VP software medium into the drive.
3. Start the following command by selecting [Run As Administrator]:
<CENTUM VP software medium drive>:\CENTUM\Security\DeleteITSecurity.cmd

C7.1.4 Uninstalling the Device Drivers

This section describes how to uninstall the device drivers.

■ Precautions for When Uninstalling the Control Bus Driver

Before you uninstall the control bus driver, be sure to disable the control bus driver.

Follow these steps to disable the control bus driver:

1. Sign in as an administrative user.
2. Open Control Panel.
3. Select [Network and Internet] > [Network and Sharing Center].
The Network and Sharing Center window appears.
4. Select [Change adapter settings].
The Network Connections window appears.
5. Right-click [Yokogawa Vnet Adapter] and select [Disable].
An error dialog box regarding disabling connection appears.
6. Click [OK].
7. Restart the computer.
8. Perform steps 1 to 4.
9. In the Network Connections window, confirm that the control bus driver is disabled.

TIP

If the control bus driver is not disabled, perform the procedure from step 2 again.

■ Uninstalling Control Bus Driver

Follow these steps to uninstall the control bus driver.

1. Log on using an administrative user account.
2. Terminate all applications that are running.
3. Insert the CENTUM VP 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.
4. Click [Control Bus Driver].
The following dialog box appears.



Figure C7.1.4-1 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 B4-69

■ Uninstalling the Vnet/IP Open Communication Driver

Follow these steps to uninstall the Vnet/IP open communication driver:

1. Log on using an administrative user account.
 2. Terminate all applications that are running.
 3. Insert the CENTUM VP 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.
4. Click [Vnet/IP Open com driver].
The following dialog box appears.



Figure C7.1.4-2 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 B4-69

■ Uninstalling the Vnet/IP Interface Package on a Virtual Machine

Follow these steps to uninstall the Vnet/IP Interface Package:

TIP

Unlike actual Vnet/IP stations, if you uninstall the Vnet/IP Interface Package from a virtual machine, the virtual machine results in a Station Fail status immediately.

● Procedure 1: Uninstall the Vnet/IP Interface Package

Follow these steps to uninstall the Vnet/IP Interface Package:

1. Sign in to the guest OS on the virtual machine as an administrative user.
2. Terminate all applications that are running.
3. Sign out from the guest OS on the virtual machine.
4. Sign in to the host OS on the virtualization host computer as an administrative user.

5. Copy an ISO format file of the CENTUM VP software medium and paste it into a folder in the host OS on the virtualization host computer.
6. From the Start menu, select [Server Manager].
Server Manager starts.
7. From the menu bar of Server Manager, select [Tools] > [Hyper-V Manager].
Hyper-V Manager starts.
8. In the left pane of Hyper-V Manager, select the virtualization host computer. The virtual machines on the selected virtualization host computer are displayed on the middle pane.
Select the virtual machine and click [Connect] in the right click menu.
The virtual machine connection window appears.

TIP

The virtual machine connection window may appear full-screen. If it appears full-screen, click [Undo] to exit full-screen.

9. From the menu bar of the virtual machine connection window, select [Media] > [DVD Drive] > [Insert Disk].
A file opening dialog box appears.
10. Specify the copied ISO format file of the CENTUM VP software medium.
The selected ISO format file is mounted on the virtual machine.
 - 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 folder where the ISO file of the CENTUM VP software is stored.
The installation menu appears.
11. On the installation menu, click [Control Bus Driver].
A setup selection dialog box appears.
12. Select [UNINSTALL] and click [OK].
A dialog box appears, confirming the uninstallation.
13. Click [OK].
The uninstallation starts.
14. In the uninstallation complete dialog box that appears upon completion of the uninstallation, click [OK].
15. Restart the virtual machine.

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 B4-69

● Procedure 2: Disable the RIP Listener Service

This section describes how to disable the RIP Listener service.

IMPORTANT

Disabling of the RIP Listener service may fail when the Default Authentication Level of DCOM is configured to [None]. If this error occurs, perform the workaround.

Follow these steps to disable the RIP Listener service on Windows Server 2016:

1. Sign in to the guest OS on the virtual machine as an administrative user.
2. From the Start menu, select [Windows System].
A list of Windows System appears.
3. Right-click on the [Command Prompt], select [Run as Administrator].
4. Run the following command:
`dism /online /disable-feature /featurename:rasrip`
5. Confirm that the message, "The operation completed successfully." appears.

SEE ALSO

For more information about the workaround when disabling of the RIP Listener service fails, refer to:

- Failed to Disable the RIP Listener Service" on page C10-22

■ Uninstalling the USB Driver for OPKB

Follow these steps to uninstall the USB driver for the operation keyboard:

1. Log on using an administrative user account.
2. Terminate all applications that are running.
3. Confirm that the operation keyboard is connected to the USB port and the operation keyboard power is turned on.
4. Insert the CENTUM VP 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.

5. Click [USB driver for Operation Keyboard].
The following dialog box appears.



Figure C7.1.4-3 Setup Selection Dialog Box

6. Select [UNINSTALL] and then click [OK].
A dialog box appears, confirming the uninstallation.
7. Click [OK].
The uninstallation starts.
8. In the uninstallation complete dialog box that appears upon completion of the uninstallation, click [OK].
9. Restart the computer.

■ Uninstalling RS-232C Driver

Follow these steps to uninstall the RS-232C driver.

1. Log on using an administrative user account.
 2. Terminate all applications that are running.
 3. Insert the CENTUM VP 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.
4. Click [RS driver for Console HIS].
A dialog box appears, prompting you to select the PC interface.
 5. Select the PC interface of the driver to be uninstalled, and click [Install].
A dialog box appears, confirming the setup.



Figure C7.1.4-4 Setup Confirmation Dialog Box

6. Select [UNINSTALL] and then click [OK].
A dialog box appears, confirming the uninstallation.
7. Click [OK].
When the driver has been removed, the uninstallation completed dialog box appears.
8. Click [OK] to finish.

■ Uninstalling RAS Driver

To uninstall the RAS driver, follow the procedure below.

1. Log on using an administrative user account.

2. Terminate all applications that are running.
3. Insert the CENTUM VP 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.

4. Click [RAS driver for Console HIS].
A dialog box appears, prompting you to select the console type and the PC interface.
5. Select the PC interface of the driver to be uninstalled, and click [Install].
A dialog box appears, confirming the setup.

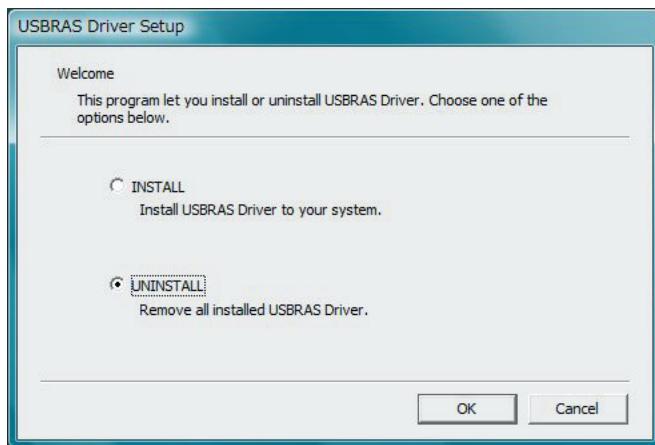


Figure C7.1.4-5 Setup Confirmation Dialog Box

6. Select [UNINSTALL] and then click [OK].
A dialog box appears, confirming the uninstallation.
7. Click [OK].
When the driver has been removed, the uninstallation completed dialog box appears.
8. Click [OK].
9. Restart the computer.

C7.2 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 using an administrative user account.
2. Open Control Panel.
3. Select [Programs] > [Programs and Features].
The Programs and Features window appears.
4. From the program list, select [YOKOGAWA CENTUM VP] and click [Change].
The Welcome dialog box appears.
5. Click [Next].
A dialog box for confirming the uninstallation appears.
6. Click [Delete].
Uninstallation starts and a dialog box showing the progress of uninstallation appears.
7. 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].

C8. Reinstalling the CENTUM VP Software

This section describes how to reinstall the CENTUM VP 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.

C8.1 When the Computer Used is the Same

This section describes the procedure for reinstalling the CENTUM VP 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 CENTUM VP software and install the CENTUM VP 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.

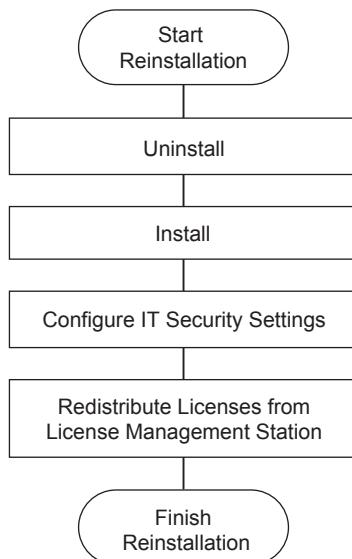


Figure C8.1-1 Flow of Reinstallation for a License-Assigned Station

- **Uninstall the CENTUM VP Software**

Uninstall the CENTUM VP software.

SEE ALSO

For more information about the uninstallation procedure, refer to:

C7.1.3, “Uninstalling the CENTUM VP Software” on page C7-10

- **Install the CENTUM VP Software**

Install the CENTUM VP software.

SEE ALSO

For more information about the installation procedure, refer to:

B4.6, “Installing the CENTUM VP Software” on page B4-85

- **Configure IT Security Settings**

Configure IT security settings in the same way as that for a new installation of the CENTUM VP software.

SEE ALSO

For more information about the security settings, refer to:

B4.7, “Configuring IT Security Settings” on page B4-94

- Redistribute Licenses from the License Management Station**

Redistribute the licenses from the license management station.

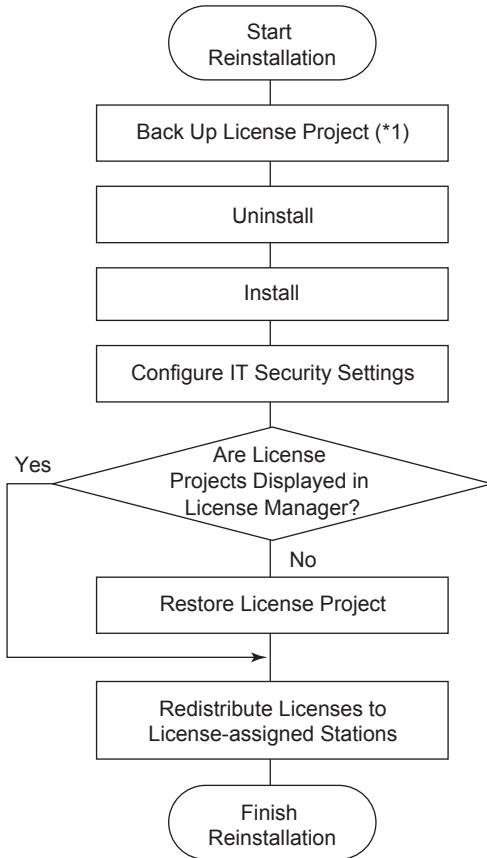
SEE ALSO

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 33J01C20-01EN)

■ 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 CENTUM VP 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.

Figure C8.1-2 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 33J01C20-01EN)

- **Uninstall the CENTUM VP Software**

Uninstall the CENTUM VP software. For a computer dedicated to license management, uninstall the license management software.

SEE

ALSO For more information about the procedure for uninstalling the CENTUM VP software, refer to:

C7., “Uninstalling the CENTUM VP Software” on page C7-1

For more information about the procedure for uninstallation on the computer dedicated to license management, refer to:

C7.2, “Uninstallation on the computer Dedicated to License Management” on page C7-20

- **Install the CENTUM VP Software**

Install the CENTUM VP software. For a computer dedicated to license management, install the license management software.

SEE

ALSO For more information about the procedure for installing the license management software, refer to:

B7., “Setting Up the Computer Dedicated to License Management” on page B7-1

- **Configure IT Security Settings**

Configure IT security settings in the same way as that for a new installation of the CENTUM VP software.

SEE

ALSO For more information about the security settings, refer to:

B4.7, “Configuring IT Security Settings” on page B4-94

- **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 33J01C20-01EN)

- **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 33J01C20-01EN)

C8.2 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 CENTUM VP software can no longer be used due to damage or other reasons.

TIP

If the HIS to be reinstalled is under the management of the Historical Message Integration Package, you must perform the task to maintain the continuity of sequence numbers of the historical message file before you connect the new computer to the historical message integration server.

SEE ALSO

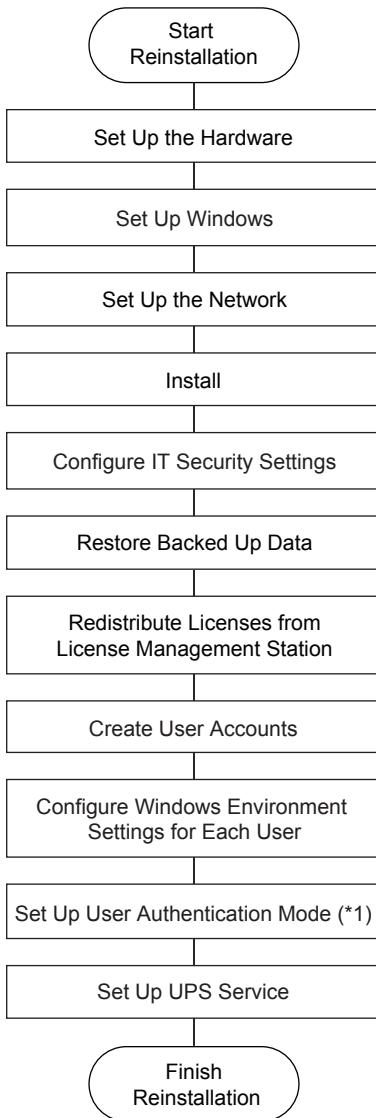
For more information about continuity of the sequence number of historical message files, refer to:

- “Historical Message Integration Package” on page C6-9

■ Reinstallation for a License-Assigned Station

This section describes the reinstallation procedure for a license-assigned station.

The workflow of reinstallation is as follows.



*1: This task is not required if the project data have been restored properly.

Figure C8.2-1 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.

- **Set Up the Hardware**

Set up the hardware.

SEE ALSO

For more information about setting up the hardware, refer to:

B4.1, “Setting Up the Hardware” on page B4-2

- **Set Up Windows**

Configure Windows settings on the new computer.

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

B4.2, "Setting Up Windows" on page B4-7

● Set Up the Network

Configure the network settings on the new computer.

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

B4.3, "Configuring Network Settings" on page B4-43

● Install the CENTUM VP Software

Install the CENTUM VP software on the new computer.

SEE ALSO For more information about the procedure for installing the CENTUM VP software, refer to:

B4.6, "Installing the CENTUM VP Software" on page B4-85

● Configure IT Security Settings

Configure IT security settings in the same way as that for a new installation of the CENTUM VP software.

SEE ALSO For more information about the security settings, refer to:

B4.7, "Configuring IT Security Settings" on page B4-94

● 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:

C5., "Backing Up the System" on page C5-1

● 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 33J01C20-01EN)

● Create User Accounts

Create user accounts.

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

B4.9, "Creating User Accounts" on page B4-102

● 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:
B4.10, "Configuring Windows Environment Settings for Each User" on page B4-107

- **Set User Authentication Mode**

Set up for the desired user authentication mode.

This task is not required if the project data have been restored properly.

**SEE
ALSO**

For more information about setting the user authentication mode, refer to:
B4.11, "Setting Up for User Authentication Modes" on page B4-135

- **Set Up the Uninterruptible Power Source (UPS) Service**

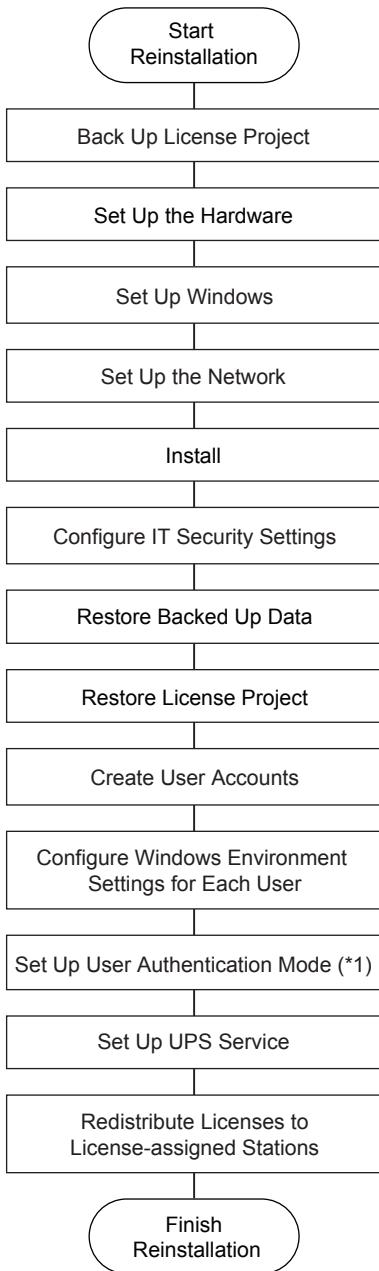
Set up the uninterruptible power source (UPS) service.

**SEE
ALSO**

For more information about setting up the UPS service, refer to:
B4.12, "Setting Up the Uninterruptible Power Supply (UPS) Service" on page B4-149

■ Reinstallation for the License Management Station

The license management station can be a computer installed with the CENTUM VP 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: This task is not required if the project data have been restored properly.

Figure C8.2-2 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.

● 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 33J01C20-01EN)

● Set Up the Hardware

Set up the hardware.

SEE ALSO

For more information about setting up the hardware, refer to:

B4.1, "Setting Up the Hardware" on page B4-2

● Set Up Windows

Configure Windows settings on the new computer.

SEE ALSO

For more information about setting up Windows, refer to:

B4.2, "Setting Up Windows" on page B4-7

● Set Up the Network

Configure the network settings on the new computer.

SEE ALSO

For more information about configuring network settings, refer to:

B4.3, "Configuring Network Settings" on page B4-43

● Install the CENTUM VP Software

Install the CENTUM VP software on the new computer. For a computer dedicated to license management, install the license management software.

SEE ALSO

For more information about the procedure for installing only the license management software, refer to:

B7., "Setting Up the Computer Dedicated to License Management" on page B7-1

● Configure IT Security Settings

Configure IT security settings in the same way as that for a new installation of the CENTUM VP software.

SEE ALSO

For more information about the security settings, refer to:

B4.7, "Configuring IT Security Settings" on page B4-94

● 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:

C5., "Backing Up the System" on page C5-1

● 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 33J01C20-01EN)

- **Create User Accounts**

Create user accounts.

SEE ALSO

For more information about creating user accounts, refer to:

B4.9, “Creating User Accounts” on page B4-102

- **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:

B4.10, “Configuring Windows Environment Settings for Each User” on page B4-107

- **Set User Authentication Mode**

Set up for the desired user authentication mode.

This task is not required if the project data have been restored properly.

SEE ALSO

For more information about setting the user authentication mode, refer to:

B4.11, “Setting Up for User Authentication Modes” on page B4-135

- **Set Up the Uninterruptible Power Source (UPS) Service**

Set up the uninterruptible power source (UPS) service.

SEE ALSO

For more information about setting up the UPS service, refer to:

B4.12, “Setting Up the Uninterruptible Power Supply (UPS) Service” on page B4-149

- **Redistribute Licenses to License-Assigned Stations**

Redistribute licenses to the license-assigned stations.

SEE ALSO

For more information about redistributing licenses to the license-assigned stations, refer to:

3.4, “Redistributing licenses to license-assigned stations” in License Management (IM 33J01C20-01EN)

Blank Page

C9. Cases that Require Attention in IT Security Setting

This section describes the cases where you must pay attention when configuring IT security settings.

C9.1 Including CENTUM CS 3000 R3 HIS in a VP Project of CENTUM VP Standard Model

This section describes the procedure for including a CENTUM CS 3000 R3 HIS in a VP project of CENTUM VP Standard model.

IMPORTANT

- Use CENTUM Authentication as the user authentication mode on all HISs.
- If any of the following software packages are installed on the CENTUM CS 3000 R3 HIS, you cannot include it in the CENTUM VP system. You must upgrade the CENTUM CS 3000 R3 HIS to CENTUM VP.
 - LHS5100/LHM5100 : Standard Builder Function
 - LHS5160 : CS Batch 3000 Process Management Package
 - LHS5425 : Expanded Test Functions
 - LHS5426 : FCS Simulator Package
 - LHS5427 : HIS Simulator Package
- Under this configuration, the effectiveness of security measures drops compared to when the entire system is unified with CENTUM VP Standard models. It is recommended that this configuration be considered temporary and the system be unified with CENTUM VP Standard models in a planned manner.

■ Accessing Data of CENTUM VP from CS 3000 R3 HIS

To enable access to CENTUM VP data from CENTUM CS 3000 R3 HIS, create an account named CENTUM on CENTUM VP computers.

- **Standalone Management**

Follow these steps when the user management type is Standalone management:

1. On CENTUM VP computers, create an account named CENTUM as a member of the CTM_OPC and CTM_OPERATOR groups.
However, on the following computers, create a CENTUM account as a member of the CTM_OPC and CTM_ENGINEER groups.
 - Computer with recipe engineers' account file
 - Computer with audit trail database of the recipe function
2. For the CENTUM account you have created, set the same password as the one set for the CENTUM account on the CENTUM CS 3000 R3 HIS.

- **Domain Management**

When the user management type is Domain management, change it to Combination management and perform the procedure for Combination management.

- **Combination Management**

Follow these steps when the user management type is Combination management:

1. On CENTUM VP computers, create an account named CENTUM as a member of the CTM_OPC_LCL and CTM_OPERATOR_LCL groups.
However, on the following computers, create a CENTUM account as a member of the CTM_OPC_LCL and CTM_ENGINEER_LCL groups.

- Computer with recipe engineers' account file
 - Computer with audit trail database of the recipe function
2. For the CENTUM account you have created, set the same password as the one set for the CENTUM account on the CENTUM CS 3000 R3 HIS.

■ Accessing Data of CENTUM CS 3000 R3 HIS from CENTUM VP

To enable access to data of CENTUM CS 3000 R3 HIS from CENTUM VP, create user accounts on CENTUM CS 3000 R3 HIS.

● Standalone Management

Follow these steps when the user management type is Standalone management:

1. On CENTUM CS 3000 R3 HIS, register all user accounts registered in CENTUM VP computers.
2. Match the passwords of each user account between CENTUM VP and CENTUM CS 3000 R3 HIS.
3. Log on to the CENTUM CS 3000 R3 HIS as an administrative user.
4. Terminate all the running applications.
5. Insert the CENTUM VP software medium into the drive.
The installation menu starts automatically, but click [Close] to close it.
6. Run the following command:
`<Drive of CENTUM VP software medium>:\CENTUM\SECURITY\yokogawa.IA.iPCS.Platfo
rm.Security.CreateCentumProcess.exe`

The utility for creating the CTM_PROCESS account starts, and the CTM_PROCESS account is created.

● Domain Management

When the user management type is Domain management, change it to Combination management and perform the procedure for Combination management.

● Combination Management

Follow these steps when the user management type is Combination management:

1. On CENTUM CS 3000 R3 HIS, register the accounts with the same user names as the user accounts registered in the domain.
2. On CENTUM CS 3000 R3 HIS, register all local user accounts registered in CENTUM VP computers.
3. Match the passwords of each user account among the domain user accounts, local accounts of CENTUM VP computers, and local accounts of CENTUM CS 3000 R3 HIS.
4. Log on to the CENTUM CS 3000 R3 HIS as an administrative user.
5. Terminate all the running applications.
6. Insert the CENTUM VP software medium into the drive.
The installation menu starts automatically, but click [Close] to close it.Run the following command:
7. Run the following command.

`<Drive of CENTUM VP software medium>:\CENTUM\SECURITY\yokogawa.IA.iPCS.Platfo
rm.Security.CreateCentumProcess.exe`

The utility for creating the CTM_PROCESS account starts, and the CTM_PROCESS account is created.

C9.2 Including CENTUM VP HIS of Legacy Model in a VP Project of CENTUM VP Standard Model

This section describes the procedure for including CENTUM VP HIS of Legacy model in a VP project of CENTUM VP Standard model.

IMPORTANT

- Use CENTUM Authentication as the user authentication mode on all HISs.
- On a computer where the following packages are activated, select the Standard security model.
 - Engineering Server Function
 - Standard Engineering Function
 - Batch Builder (VP Batch)
 - Expanded Test Functions
 - FCS Simulator Package
 - HIS Simulator Package
 - SEM OPC Interface Package

Also select the Standard security model on a computer where a VP project database is placed.

- You can also add CENTUM VP HIS of Legacy model to the domain.
- Under this configuration, the effectiveness of security measures drops compared to when the entire system is unified with CENTUM VP Standard model. It is recommended that this configuration be considered temporary and the system be unified with CENTUM VP Standard model in a planned manner.

■ Accessing Data of Standard Model Computer from CENTUM VP HIS of Legacy Model

To enable access to data on a computer of Standard model from a CENTUM VP HIS of Legacy model, user accounts for the CENTUM VP HIS of Legacy model must be created on the computer of Standard model.

The procedure for creating user accounts varies depending on the user management type.

● Standalone Management

Follow these steps to create user accounts when the user management type is Standalone management:

1. On the computer of Standard model, create the current users on the CENTUM VP HIS of Legacy model as user accounts in the CTM_OPERATOR group. However, the users who use the recipe function should be created as user accounts in the CTM_ENGINEER group.
2. Set the same password for the same user on all computers.

● Domain Management

Follow these steps to create user accounts when the user management type is Domain management:

1. Add the CENTUM VP HIS of Legacy model to the domain.
In addition, if the Legacy model CENTUM VP HIS is R4, disable the Windows Firewall for the domain network after adding the HIS to the domain.
2. Create user accounts for the CENTUM VP HIS of Legacy model, in the CTM_OPERATOR group of the domain.
However, the users who use the recipe function should be created as user accounts in the CTM_ENGINEER group.

TIP

Hereafter, on the CENTUM VP HIS of Legacy model, use the domain user accounts that you have created.

● Combination Management

Follow these steps to create user accounts when the user management type is Combination management:

1. Add the CENTUM VP HIS of legacy model to the domain.
In addition, if the Legacy model CENTUM VP HIS is R4, disable the Windows Firewall for the domain network after adding the HIS to the domain.
2. Perform either of the following settings:
 - If the CENTUM VP HIS of Legacy model should be used by domain users, create the domain users as user accounts in the CTM_OPERATOR group of the domain.
However, the users who use the recipe function should be created as user accounts in the CTM_ENGINEER group.
 - If the CENTUM VP HIS of Legacy model should be used by local users, create the users as user accounts in the CTM_OPERATOR_LCL group on all computers of Standard model.
However, the users who use the recipe function should be created as user accounts in the CTM_ENGINEER_LCL group.

■ Accessing Data of CENTUM VP HIS of Legacy Model from Standard Model Computers

To enable access to data on CENTUM VP HIS of Legacy model from a computer of Standard model, user accounts for the computer of Standard model must be created on the CENTUM VP HIS of Legacy model.

The procedure for creating user accounts varies depending on the user management type.

● Standalone Management

Follow these steps to create user accounts when the user management type is Standalone management:

1. On the CENTUM VP HIS of Legacy model, create the current users on the computer of Standard model.
2. Set the same password for the same user on all computers.

● Domain Management

If the user management type is Domain management, there is no need to create new user accounts so long as the CENTUM VP HIS of Legacy model is added to the domain.

In addition, if the Legacy model CENTUM VP HIS is R4, disable the Windows Firewall for the domain network after adding the HIS to the domain.

- **Combination Management**

Follow these steps to create user accounts when the user management type is Combination management.

1. Add the CENTUM VP HIS of legacy model to the domain.
In addition, if the Legacy model CENTUM VP HIS is R4, disable the Windows Firewall for the domain network after adding the HIS to the domain.
2. Create the current local users on the computer of Standard model, as user accounts on the CENTUM VP HIS of Legacy model.
3. Set the same password for the same user on all computers.

C9.3 Connecting Multiple Projects

When connecting multiple projects, how security should be set varies depending on the system to be connected.

IMPORTANT

Set the Standard model or Legacy model as a unified security model within the project.

C9.3.1 Connecting CENTUM VP Project of Standard Model and CENTUM VP Project of Legacy Model

When connecting CENTUM VP project of Standard model and CENTUM VP project of Legacy model, certain settings are required according to the system to be connected.

TIP

- The user authentication mode for the CENTUM VP project of Standard model may be either the Windows authentication mode or CENTUM authentication mode. However, the user authentication mode must be unified within each project.
- A CENTUM VP project computer of Legacy model can be also added to the domain.

IMPORTANT

Under this configuration, the effectiveness of security measures drops compared to when the entire system is unified with CENTUM VP Standard models. It is recommended that this configuration be considered temporary and the system be unified with CENTUM VP Standard models in a planned manner.

■ Accessing Data of CENTUM VP Computer of Standard Model from CENTUM VP Project Computer of Legacy Model

To enable access to data on a CENTUM VP project computer of Standard model from a CENTUM VP project computer of Legacy model, create the current user accounts for the CENTUM VP project of Legacy model on the CENTUM VP project computer of Standard model. The procedure varies depending on the user management type.

● Standalone Management

Follow these steps to create user accounts when the user management type is Standalone management:

- Specify the CENTUM VP project computers of Standard model to which the CENTUM VP project computers of Legacy model are to be connected.
- On these computers, create all current users for the CENTUM VP project computer of Legacy model as user accounts in the CTM_OPERATOR group. However, on computers that satisfy the following conditions, create them as user accounts in the CTM_ENGINEER group:
 - Computer with engineers' account file and recipe engineers' account file
 - Computer with system builders
 - Computer with audit trail database of the recipe function
- Set the same password for the same user on all computers.

SEE ALSO

For more information about CENTUM VP project computer of standard model to which the CENTUM VP project computer of legacy model will connect, refer to:

“■ Computers That Are Connected When Connecting Projects” on page C9-11

● Domain Management

Follow these steps to create user accounts when the user management type is Domain management:

- Add the CENTUM VP project computers of Legacy model to the domain. In addition, if the Legacy model CENTUM VP HIS is R4, disable the Windows Firewall for the domain network after adding the HIS to the domain.

2. Create user accounts for the CENTUM VP project computer of Legacy model, in the CTM_OPERATOR group of the domain.
However, the users who use the system builders or recipe function should be created as user accounts in the CTM_ENGINEER group.

TIP

Hereafter, on the CENTUM VP project computers of Legacy model, use the domain user accounts that you have created.

● Combination Management

Follow these steps to create user accounts when the user management type is Combination management:

1. Add the CENTUM VP project computers of Legacy model to the domain.
In addition, if the Legacy model CENTUM VP HIS is R4, disable the Windows Firewall for the domain network after adding the HIS to the domain.
2. Perform either of the following settings:
 - If the CENTUM VP project computers of Legacy model should be used by domain users, create the domain users as user accounts in the CTM_OPERATOR group of the domain.
However, the users who use the system builders or recipe function should be created as user accounts in the CTM_ENGINEER group.
 - If the CENTUM VP project computers of Legacy model should be used by local users, specify the CENTUM VP project computers of Standard model to which the CENTUM VP project computers of Legacy model are to be connected. On these computers, create the current users on the computer of Legacy model as accounts in the CTM_OPERATOR_LCL group.
However, on computers that satisfy the following conditions, create them as user accounts in the CTM_ENGINEER_LCL group:
 - Computer with recipe engineers' account file
 - Computer with audit trail database of the recipe function

SEE**ALSO**

For more information about CENTUM VP project computer of standard model to which the CENTUM VP project computer of legacy model will connect, refer to:

“■ Computers That Are Connected When Connecting Projects” on page C9-11

■ Accessing data of CENTUM VP Computer of Legacy Model from CENTUM VP Project Computer of Standard Model

To enable access to data on a CENTUM VP project computer of Legacy model from a CENTUM VP project computer of Standard model, create the current user accounts for the CENTUM VP project of Standard model on the CENTUM VP project computer of Legacy model. The procedure varies depending on the user management type.

● Standalone Management

Follow these steps to create user accounts when the user management type is Standalone management:

1. Specify the CENTUM VP project computers of Legacy model to which the CENTUM VP project computers of Standard model are to be connected.
2. On these computers, create all user accounts currently used on the CENTUM VP project computer of Standard model. If the Windows authentication mode is used in the CENTUM VP project computer of Standard model, also create OFFUSER.
3. Set the same password for the same user on all computers.

SEE ALSO

For more information about CENTUM VP project computer of legacy model to which the CENTUM VP project computer of standard model will connect, refer to:

“■ Computers That Are Connected When Connecting Projects” on page C9-11

For more information about how to create OFFUSER, refer to:

6.10.7, “CreateOffuser” in CENTUM VP Security Guide (IM 33J01C30-01EN)

● Domain Management

Follow these steps to create user accounts when the user management type is Domain management:

1. Add the CENTUM VP project computers of Legacy model to the domain.
In addition, if the Legacy model CENTUM VP HIS is R4, disable the Windows Firewall for the domain network after adding the HIS to the domain.
2. If the Windows authentication mode is used with the CENTUM VP project computers of Standard model, create OFFUSER on the CENTUM VP project computers of Legacy model.

SEE ALSO

For more information about how to create OFFUSER, refer to:

6.10.7, “CreateOffuser” in CENTUM VP Security Guide (IM 33J01C30-01EN)

● Combination Management

Follow these steps to create user accounts when the user management type is Combination management:

1. Add the CENTUM VP project computers of Legacy model to the domain.
In addition, if the Legacy model CENTUM VP HIS is R4, disable the Windows Firewall for the domain network after adding the HIS to the domain.
2. If the Windows authentication mode is used with the CENTUM VP project computers of Standard model, create OFFUSER on the CENTUM VP project computers of Legacy model.
3. Perform either of the following settings:
 - If the CENTUM VP project computers of Legacy model should be used by domain users, create the domain users as user accounts in the CTM_OPERATOR group of the domain.
However, the users who use the system builders or recipe function should be created as user accounts in the CTM_ENGINEER group.
 - If the CENTUM VP project computers of Legacy model should be used by local users, specify the CENTUM VP project computers of Legacy model to which the CENTUM VP project computers of Standard model are to be connected. On these computers, create the current users on the computer of Standard model as accounts in the CTM_OPERATOR_LCL group.
However, on computers that satisfy the following conditions, create them as user accounts in the CTM_ENGINEER_LCL group:
 - Computer with recipe engineers' account file
 - Computer with audit trail database of the recipe function

SEE ALSO

For more information about how to create OFFUSER, refer to:

6.10.7, "CreateOffuser" in CENTUM VP Security Guide (IM 33J01C30-01EN)

For more information about CENTUM VP project computer of legacy model to which the CENTUM VP project computer of standard model will connect, refer to:

"■ Computers That Are Connected When Connecting Projects" on page C9-11

■ Computers That Are Connected When Connecting Projects

Projects are connected by DCOM (OPC) connection or shared folder connection.

The following computers are connected by a DCOM (OPC) or shared folder:

TIP

Connection is made to these computers regardless of whether connecting from a Standard model to a Legacy model, or connecting from a Legacy model to a Standard model.

- HIS in the connection target project, which exists in the system configuration definition of the source project
- Computer on which project database is placed
- Computer to be referenced for message summary, which is specified in Referenced Message in the .SH HIS Setup window.
- Computer to be referenced by the SOE viewer
- Computer on which long-term data archive files exist
- Computer used as a long-term storage of CAMS for HIS historical data
- Computer specified as a long-term storage of historical message files
- Computer on which a recipe management database is placed, when recipe management and process management are shared among projects
- Computer with the Exaopc OPC Interface Package (for HIS) installed, which is specified from the Report Package
- Computer on which the Exaopc OPC Interface Package (for HIS) specified in the OPC client setting procedure on the SOE Server computer is installed
- Computer on which the Exaopc OPC Interface Package (for HIS) specified as the destination to notify continuous authentication failures to under the Engineering Function, Recipe Function and/or Report Function, in the Access Control Package or Access Administrator Package (FDA:21 CFR Part 11 compliant), is installed
- Computer on which an engineers' account file, recipe engineers' account file, user security file for Report Package or each audit trail database in the Access Control Package or Access Administrator Package (FDA:21 CFR Part 11 compliant)

TIP

The HIS in the connection target project, which exists in the system configuration definition, is connected when Log Save is performed on any HIS.

C9.3.2 Connecting CENTUM VP Project and CENTUM CS 1000/CS 3000 R3 Project

When connecting a CENTUM VP project and a CENTUM CS 1000/CS 3000 R3 project, certain settings are required according to the system to be connected.

The CENTUM VP project is assumed as a standard model.

TIP

- The user authentication mode for the CENTUM VP project may be either the Windows authentication mode or CENTUM authentication mode. However, the user authentication mode must be unified within each project.
- Always use Standalone management for the user management type on CENTUM CS 1000/CS 3000 R3 computers.

IMPORTANT

Under this configuration, the effectiveness of security measures drops compared to when the entire system is unified with CENTUM VP Standard models. It is recommended that this configuration be considered temporary and the system be unified with CENTUM VP Standard models in a planned manner.

■ Referencing a CENTUM VP Project Computer from a CENTUM CS 1000/CS 3000 R3 Project Computer

To reference data of a CENTUM VP project from a CENTUM CS 1000/CS 3000 R3 project computer, create user accounts on the CENTUM VP computers.

- **Standalone Management**

Follow these steps when the user management type is Standalone management:

1. Specify the CENTUM VP project computer to which the CENTUM CS 1000/CS 3000 R3 project computers will connect.
2. On these computers, create an account named CENTUM as a member of the CTM_OPC and CTM_OPERATOR groups.
3. On a computer that satisfies the following conditions, create the current users of the system builders or recipe function as members of the CTM_OPC and CTM_ENGINEER groups.
 - Computer with engineers' account file and recipe engineers' account file
 - Computer with system builders
 - Computer with audit trail database of the recipe function
4. Set the same password for the same user on all computers.

SEE ALSO

For more information about the CENTUM VP project computers to which CENTUM CS 1000/CS 3000 R3 project computers will connect, refer to:

“● CENTUM VP Project Computer Connected from a CENTUM CS 1000/CS 3000 R3 Project Computer” on page C9-13

- **Domain Management**

When the user management type is Domain management, change it to Combination management and perform the procedure for Combination management.

● Combination Management

Follow these steps when the user management type is Combination management:

1. Specify the CENTUM VP project computers to which the CENTUM CS 1000/CS 3000 R3 project computers will connect.
2. On these computers, create an account named CENTUM as a member of the CTM_OPC and CTM_OPERATOR groups.
3. On a computer that satisfies the following conditions, create the current users of the system builders or recipe function as members of the CTM_OPC_LCL and CTM_ENGI-NEER_LCL groups.
 - Computer with engineers' account file and recipe engineers' account file
 - Computer with system builders
 - Computer with audit trail database of the recipe function
4. Set the same password for the same user on all computers.

SEE ALSO

For more information about the CENTUM VP project computers to which CENTUM CS 1000/CS 3000 R3 project computers will connect, refer to:

- “● CENTUM VP Project Computer Connected from a CENTUM CS 1000/CS 3000 R3 Project Computer” on page C9-13

● CENTUM VP Project Computer Connected from a CENTUM CS 1000/CS 3000 R3 Project Computer

Projects are connected by DCOM (OPC) connection or shared folder connection.

The following computers are connected by a DCOM (OPC) or shared folder.

- Computer on which project database is placed
- Computer to be referenced for message summary, which is specified in Referenced Message in the .SH HIS Setup window.
- Computer to be referenced by the SOE viewer
- Computer on which long-term data archive files exist
- Computer used as a long-term storage of CAMS for HIS historical data
- Computer specified as a long-term storage of historical message files
- Computer on which a recipe management database is placed, when recipe management is performed in CENTUM VP and process management is preformed in CENTUM CS 3000 R3
- Computer on which the Exaopc OPC Interface Package (for HIS) specified from the Report Package is installed
- Computer on which the Exaopc OPC Interface Package (for HIS) specified in the OPC client setting procedure on the SOE Server computer is installed
- Computer on which the Exaopc OPC Interface Package (for HIS) specified as the destination to notify continuous authentication failures to under the Engineering Function, Recipe Function and/or Report Function, in the Access Control Package or Access Administrator Package (FDA:21 CFR Part 11 compliant), is installed
- Computer on which an engineers' account file, recipe engineers' account file, user security file for Report Package or each audit trail database in the Access Control Package or Access Administrator Package (FDA:21 CFR Part 11 compliant)

■ Accessing CENTUM CS 1000/CS 3000 R3 Project from CENTUM VP Project Computer

To reference data of a CENTUM CS 1000/CS 3000 R3 project from a CENTUM VP project computer, create user accounts on the CENTUM CS 1000/CS 3000 R3 computers.

● Standalone Management

Follow these steps when the user management type is Standalone management:

1. Specify the CENTUM CS 1000/CS 3000 R3 project computers to which the CENTUM VP project computers will connect.
2. On these computers, create all user accounts registered in CENTUM VP computers and the CTM_PROCESS account.

SEE ALSO

For more information about how to create the user accounts and the CTM_PROCESS account, refer to:

- “● Standalone Management” on page C9-3

For more information about the CENTUM CS 1000/CS 3000 R3 project computers to which the CENTUM VP project computers will connect, refer to:

- “● CENTUM CS 1000/CS 3000 R3 Project Computer Connected from CENTUM VP Project Computer” on page C9-14
-

● Domain Management

When the user management type is Domain management, change it to Combination management and perform the procedure for Combination management.

● Combination Management

Follow these steps when the user management type is Combination management:

1. Specify the CENTUM CS 1000/CS 3000 R3 project computers to which the CENTUM VP project computers will connect.
2. On these computers, create the domain user accounts, all local user accounts registered in CENTUM VP computers, and the CTM_PROCESS account.

SEE ALSO

For more information about how to create the user accounts and the CTM_PROCESS account, refer to:

- “● Combination Management” on page C9-3

For more information about the CENTUM CS 1000/CS 3000 R3 project computers to which the CENTUM VP project computers will connect, refer to:

- “● CENTUM CS 1000/CS 3000 R3 Project Computer Connected from CENTUM VP Project Computer” on page C9-14
-

● CENTUM CS 1000/CS 3000 R3 Project Computer Connected from CENTUM VP Project Computer

Projects are connected by DCOM (OPC) connection or shared folder connection.

The following computers are connected by a DCOM (OPC) or shared folder:

- CENTUM CS 1000/CS 3000 R3 HIS that exists in the system configuration definition of the CENTUM VP project
- Computer on which project database is placed
- Computer to be referenced for message summary, which is specified in Referenced Message in the .SH HIS Setup window.

- Computer to be referenced by the SOE viewer
- Computer on which long-term data archive files exist
- Computer used as a long-term storage of CAMS for HIS historical data
- Computer specified as a long-term storage of historical message files
- Computer on which a recipe management database is placed, when recipe management is performed in CENTUM CS 3000 R3 and process management is preformed in CENTUM VP
- Computer on which the Exaopc OPC Interface Package (for HIS) specified from the Report Package is installed
- Computer on which the Exaopc OPC Interface Package (for HIS) specified in the OPC client setting procedure on the SOE Server computer is installed
- Computer on which the Exaopc OPC Interface Package (for HIS) specified as the destination to notify continuous authentication failures to under the Engineering Function, Recipe Function and/or Report Function, in the Access Control Package or Access Administrator Package (FDA:21 CFR Part 11 compliant), is installed
- Computer on which an engineers' account file, recipe engineers' account file, user security file for Report Package or each audit trail database in the Access Control Package or Access Administrator Package (FDA:21 CFR Part 11 compliant)

TIP

The CENTUM CS 1000/CS 3000 R3 HIS that exists in the system configuration definition is connected when Log Save is performed on other HIS.

C9.3.3 Connecting CENTUM VP Project and CENTUM CS Project

When connecting a CENTUM VP project and a CENTUM CS project, use the Standard model as the security model for the CENTUM VP project.

IMPORTANT

Under this configuration, the effectiveness of security measures drops compared to when the entire system is unified with CENTUM VP Standard models. It is recommended that this configuration be considered temporary and the system be unified with CENTUM VP Standard models in a planned manner.

■ Accessing CENTUM CS Project Database from CENTUM VP Project Computer

To access the project database of CENTUM CS from CENTUM VP, no special settings are required.

■ Accessing CENTUM VP Project Database from CENTUM CS Computer

To access the project database of CENTUM VP from CENTUM CS, the file management service (BK FMS) must be automatically started on the computer on which the project database of CENTUM VP is placed.

Follow these steps to automatically start the file management service:

1. Log on to the computer as an administrative user.
2. Open Control Panel.
3. Select [System and Security] > [Administrative Tools] > [Service].
The Services window appears.
4. Double-click BK FMS.
The BK FMS Properties dialog box appears.
5. On the General tab, click [Start].
The BK FMS service starts.
6. From the Startup Type drop-down list on the General tab, select [Automatic].
7. Click [OK].

TIP

Do not change the logon account of the BK FMS service from CTM_PROCESS.

C9.4 Using a File Server or Domain Controller where IT Security Settings Were Configured on CENTUM VP R4

When using a file server or domain controller where IT security settings were configured on CENTUM VP R4, you need to configure the IT security settings again.

■ To Apply the Same Security Settings as Before

You can use the IT Security Tool of CENTUM VP R5 to apply the settings, without using the saved initial IT security settings.

■ To Change the Security Settings

1. Use the initial IT security setting data that were saved before the IT security was configured on CENTUM VP R4 to restore the security settings to the initial status.
2. Run the IT Security Tool of CENTUM VP R5 or later to apply new settings.

SEE ALSO

For more information about restoring the IT security settings on the file server or domain controller, refer to:

6.5.2, "Procedure for a File Server or Domain Controller" in CENTUM VP Security Guide (IM 33J01C30-01EN)

Blank Page

C10. Troubleshooting

This section describes the causes of and remedies for problems that may occur.

C10.1 Windows Related Troubleshooting

This section describes how to handle problems related to Windows.

C10.1.1 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 C10.1.1-1 User Account Control Dialog Box (When Logged on as a Non-administrative User)

C10.1.2 Error Occurs when Server Manager is Started

An error may occur when the server manager is started.

Condition for Occurrence

This problem occurs when the Default Authentication Level of DCOM is configured to None.

TIP

For example, the Default Authentication Level of DCOM is configured to None in the following cases:

- Security model is configured to Legacy model.
- The Default Authentication Level of DCOM is configured to None to enable communication with other computers.

Workaround

You can avoid this problem with the following procedure. However, if you perform this procedure, revert to the original setting after working with the server manager.

1. Open Control Panel.
2. Select [System and Security] > [Administrative Tools] > [Component Services].
The Component Services window appears.
3. Select [Console Root] > [Component Services] > [Computers] > [My Computer], then select [Properties] from the context menu.

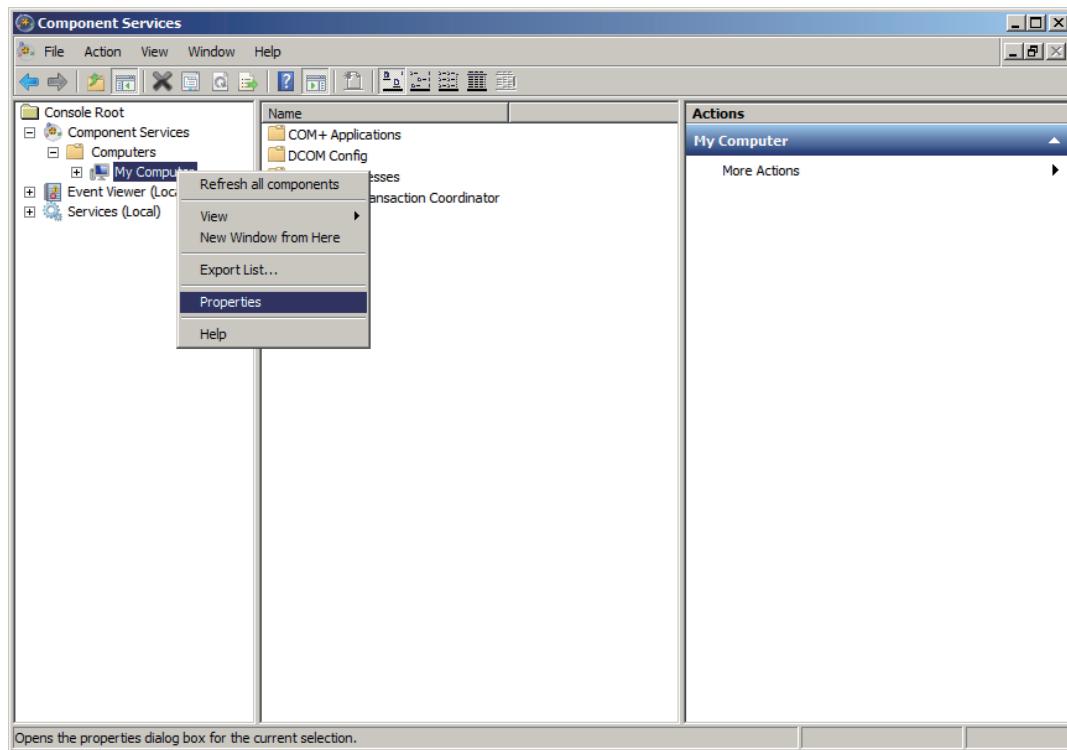


Figure C10.1.2-1 Component Services

The My Computer Properties dialog box appears.

4. From the Default Authentication Level drop-down list, select [Connect], and then click [OK].

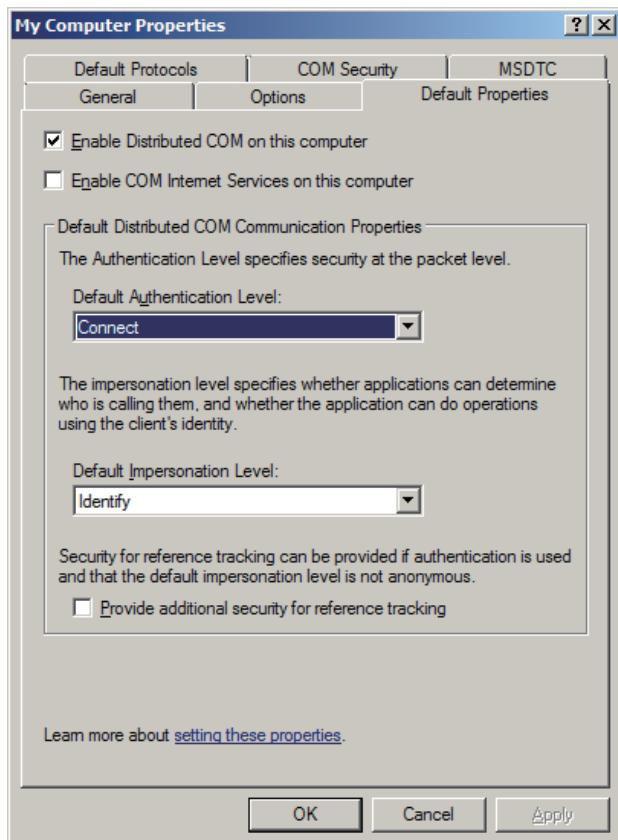


Figure C10.1.2-2 My Computer Properties

C10.1.3 Cannot Manage User Accounts in the User Accounts Dialog Box of Control Panel

You may not be able to create user accounts or perform other user account managing operations in the User Accounts dialog box of Control Panel.

■ Condition for Occurrence

This problem occurs when the Default Authentication Level of DCOM is configured to None.

TIP

For example, the Default Authentication Level of DCOM is configured to None in the following cases:

- Security model is configured to Legacy model.
- The Default Authentication Level of DCOM is configured to None to enable communication with other computers.

■ Workaround

Follow these steps to avoid this problem:

1. Open Control Panel.
2. Select [System and Security] > [Administrative Tools] > [Computer Management]. The Computer Management window appears.
3. In the left pane, select [Computer Management] > [System Tools] > [Local Users and Groups].
4. In the center pane, create a user or perform other operations.

C10.1.4 Installed Update Programs are Not Displayed in the Programs and Features Window of Control Panel

Update programs installed on the computer may not be displayed in the Programs and Features window of Control Panel.

■ Condition for Occurrence

This problem occurs when the Default Authentication Level of DCOM is configured to None.

TIP

For example, the Default Authentication Level of DCOM is configured to None in the following cases:

- Security model is configured to Legacy model.
 - The Default Authentication Level of DCOM is configured to None to enable communication with other computers.
-

■ Workaround

Follow these steps to avoid this problem.

1. Log on as an administrative user.
2. Open Command Prompt.
3. Run the following command.
`wmic qfe list full`

Information about the update programs installed on the computer is displayed.

TIP

If you enter the command as follows, information about the installed update programs is output to a file in the html format. This file is created in the folder where you run the command.

```
wmic qfe list full /format:htable > results.html
```

C10.1.5 Cannot Install Microsoft Updates

Installation of Microsoft updates may fail with Error 80070543.

■ Condition for Occurrence

This problem occurs when the Default Authentication Level of DCOM is configured to None.

TIP

For example, the Default Authentication Level of DCOM is configured to None in the following cases:

- Security model is configured to Legacy model.
 - The Default Authentication Level of DCOM is configured to None to enable communication with other computers.
-

■ Workaround

You can avoid this problem with the following procedure.

1. Change the default authentication level of DCOM from [None] to [Connect].
 2. Restart the computer.
 3. Install the Microsoft updates.
 4. Change the default authentication level of DCOM from [Connect] back to [None].
 5. Restart the computer.
-

SEE ALSO

For more information about how to change the default authentication level of DCOM, refer to:

C10.1.2, "Error Occurs when Server Manager is Started" on page C10-4

C10.1.6 Failing to install .NET Framework

An attempt to install .NET Framework may fail.

■ Condition for Occurrence

This problem occurs when the Default Authentication Level of DCOM is configured to None.

TIP

For example, the Default Authentication Level of DCOM is configured to None in the following cases:

- Security model is configured to Legacy model.
 - The Default Authentication Level of DCOM is configured to None to enable communication with other computers.
-

■ Workaround

You can avoid this problem with the following procedure.

1. Change the Default Authentication Level of DCOM from [None] to [Connect].
 2. Restart the computer.
 3. Install the .NET Framework.
-

SEE**ALSO**

For more information about how to change the default authentication level of DCOM, refer to:

C10.1.2, "Error Occurs when Server Manager is Started" on page C10-4

C10.1.7 The System Locks Up

Contact YOKOGAWA service.

C10.1.8 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 the software that can coexist with CENTUM VP, refer to:

- “● Software that can Coexist with CENTUM VP” on page A3-2
-

C10.1.9 Print Order Does Not Match the Spooled Order

When the Self-Document Printing function is used, the order of documents output to the printer may be different from the print order.

■ Cause

If the [Start printing immediately] option is selected in the Advanced setting in the Printer properties and a large volume of documents are spooled, the documents sent to the printer may sometimes be printed out first.

■ Remedy

To print the documents in the order they are spooled, you need to select the [Start printing after last page is spooled] option in the Advanced setting in the Printer properties.

The following is a procedure for configuring this setting using HP LaserJet 4050 Series PS as an example. Change your printer setting based on this example.

1. Log on as an administrative user.

TIP

If the printer is a network shared printer, log on the printer server with administrative user privileges.

2. Open Control Panel.
3. Select [Hardware and Sound] > [Devices and Printers].
The Devices and Printers window appears.
4. Select the printer you want to use, and then right-click to select [Printer Properties].
The printer's properties dialog box appears.

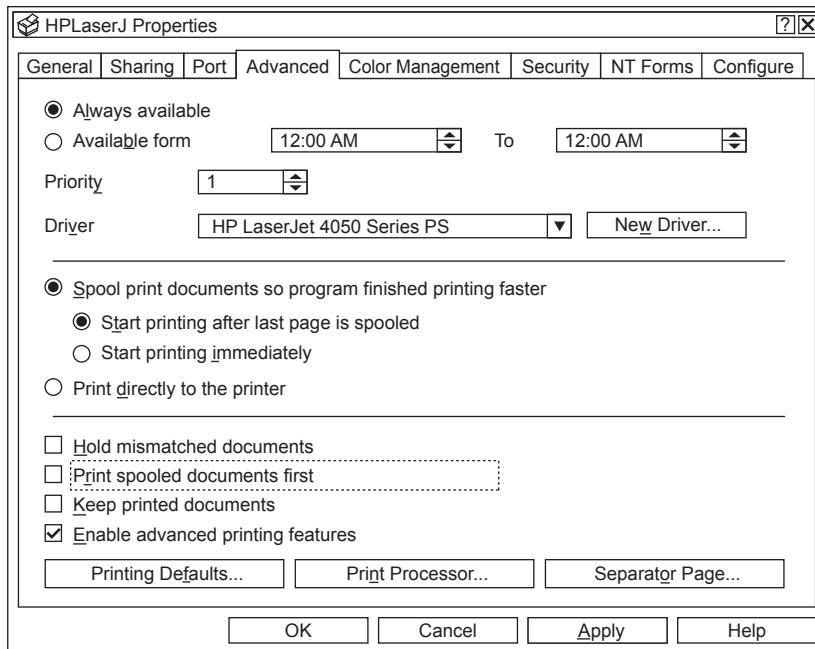


Figure C10.1.9-1 Printer Properties

5. Select the [Advanced] tab and select [Start printing after last page is spooled].
6. Clear the check box for [Print spooled documents first].
7. Click [OK].
The properties dialog box closes.

C10.2 Troubleshooting Related to Network

This section describes how to handle problems related to the network.

C10.2.1 Precaution on Network Cable Connection

With Windows 7, the Set Network Location dialog box may appear when the cable is wired for network connection. If the dialog box appears, select [Public network].



Figure C10.2.1-1 Set Network Location Dialog Box

With Windows 10 and Windows Server 2016, a network charm bar may appear from the right side of the desktop when the cable is wired. If it appears, select [No].

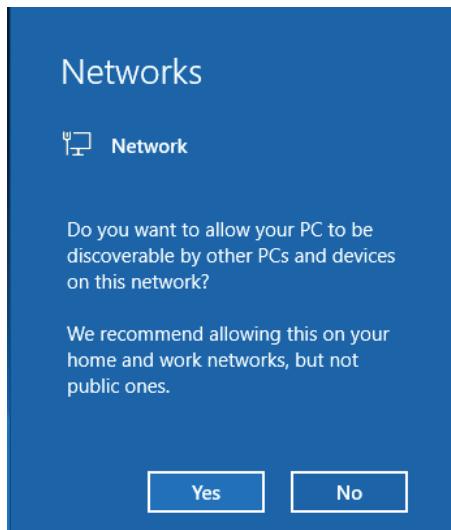


Figure C10.2.1-2 Network Charm Bar

C10.2.2 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 with the operation by clicking [Yes], [Continue] or [Allow] (if the user has administrator rights).

■ Confirming Installation Result

Check if the network driver is properly installed. If the driver is not operating properly, install it again.

- **Adapter Driver for Control Bus Driver**

When the control bus driver is added, the adapter driver "Yokogawa Vnet Adapter" appears under Network Adapters on Device Manager.

If the adapter driver does not start properly, "!" appears on the adapter driver icon.

Follow these steps to display Device Manager:

1. Log on using an administrative user account.
2. Open Control Panel.
3. Select [System and Security] > [System] > [Device Manager].

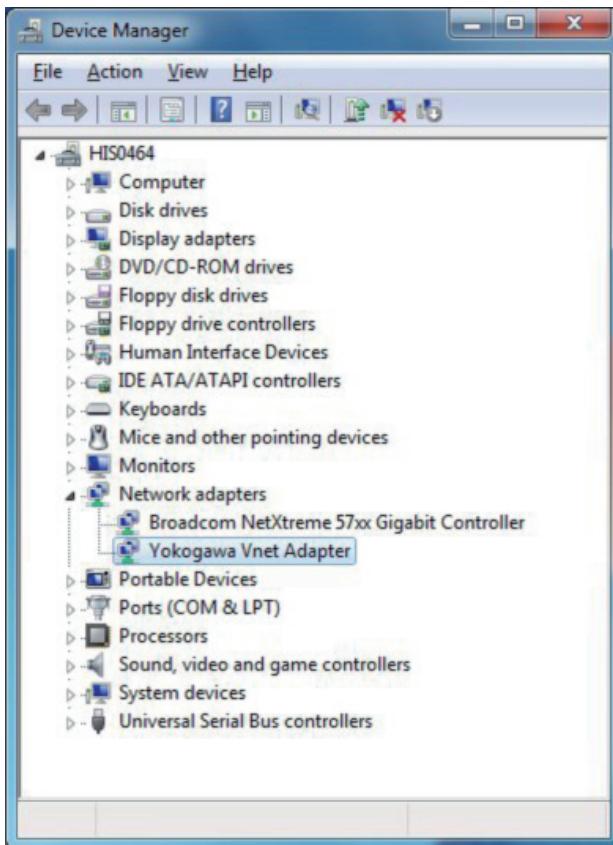


Figure C10.2.2-1 Adapter Driver Added Properly

- **Protocol Driver for Control Bus Driver (Windows 10, Windows Server 2016)**

When the control bus driver is added, the protocol driver is installed together with the adapter driver.

The operating condition of the protocol driver can be checked in Command Prompt.

Follow these steps to check the operating condition of the protocol driver:

1. Sign in as a general user or administrative user.
2. Open Command Prompt.
3. Enter `sc query VLTDI`, and then press the [Enter] key.
The condition of the protocol driver is shown. If RUNNING is shown under STATE, the driver is operating properly.

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\CENTUM>sc query VLTDI

SERVICE_NAME: VLTDI
    TYPE               : 1   KERNEL_DRIVER
    STATE              : 4   RUNNING
                           (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE    : 0   (0x0)
    SERVICE_EXIT_CODE : 0   (0x0)
    CHECKPOINT        : 0x0
    WAIT_HINT         : 0x0

C:\Users\CENTUM>
```

Figure C10.2.2-2 Protocol Driver Operating Properly

- **Protocol Driver for Control Bus Driver (Windows 7, Windows Server 2012 R2, Windows Server 2008 R2)**

When the control bus driver is added, the protocol driver is installed together with the adapter driver.

The protocol driver "Yokogawa Vnet Protocol" appears under Non-Plug and Play Drivers in Device Manager.

If the protocol driver does not start properly, "!" appears on the protocol driver icon.

Follow these steps to display the protocol driver:

1. Log on as an administrative user.
2. Open Control Panel.
3. Select [System and Security] > [System] > [Device Manager].
Device Manager appears.
4. On the menu bar, select [View] > [Show hidden devices].
The protocol driver "Yokogawa Vnet Protocol" appears under Non-Plug and Play Drivers.

TIP

If the "Yokogawa Vnet Protocol" driver does not appear immediately after the driver installation, restart the computer.

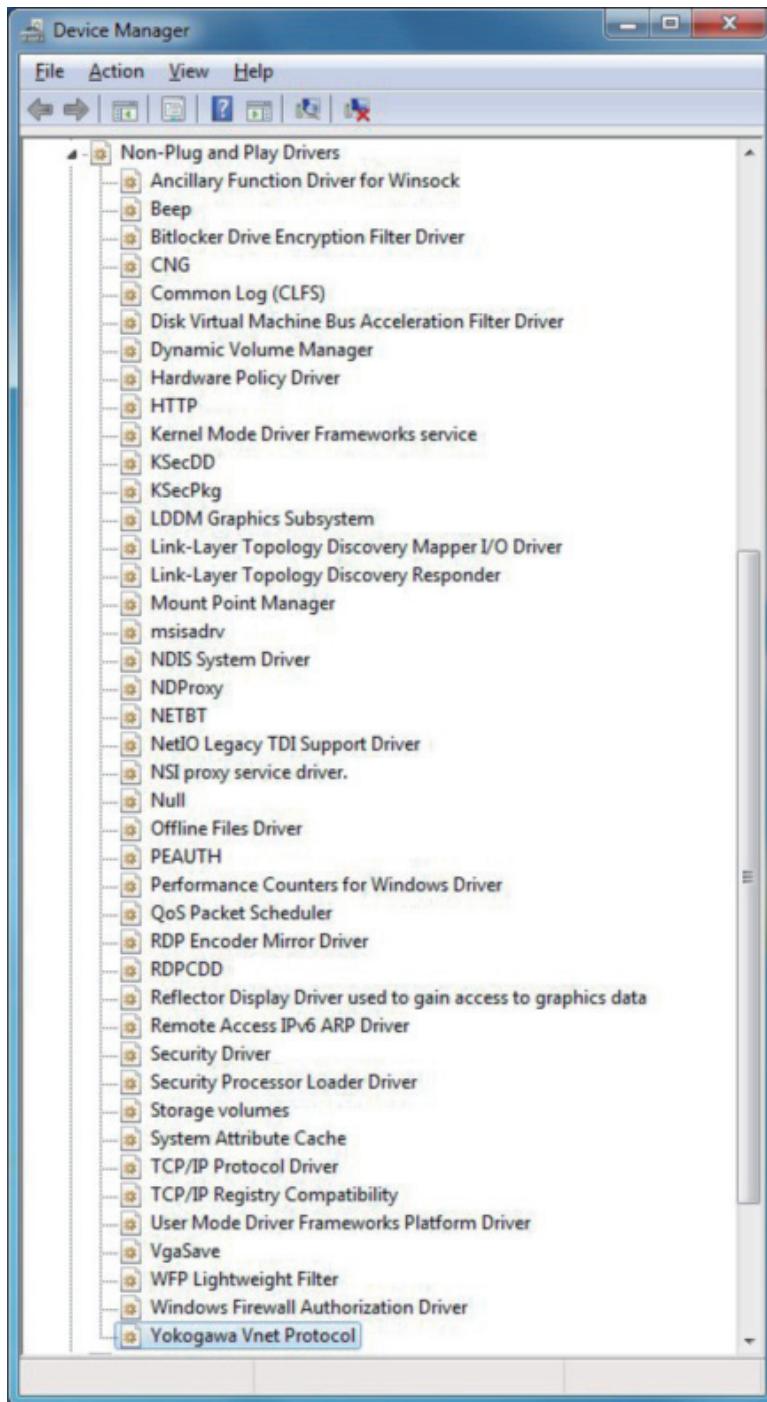


Figure C10.2.2-3 Protocol Driver Operating Properly

● **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 Manger:

1. Log on as an administrative user.
2. Open Control Panel.
3. Select [System and Security] > [System] > [Device Manager].

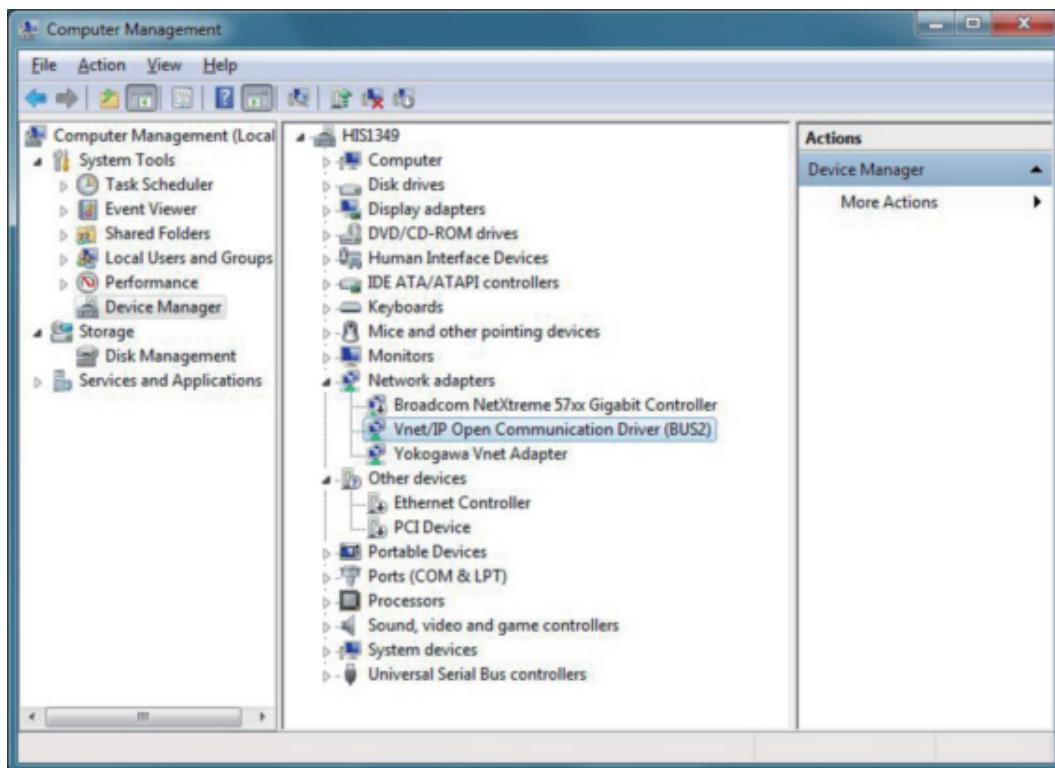


Figure C10.2.2-4 Adapter Driver Added Properly

■ 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.

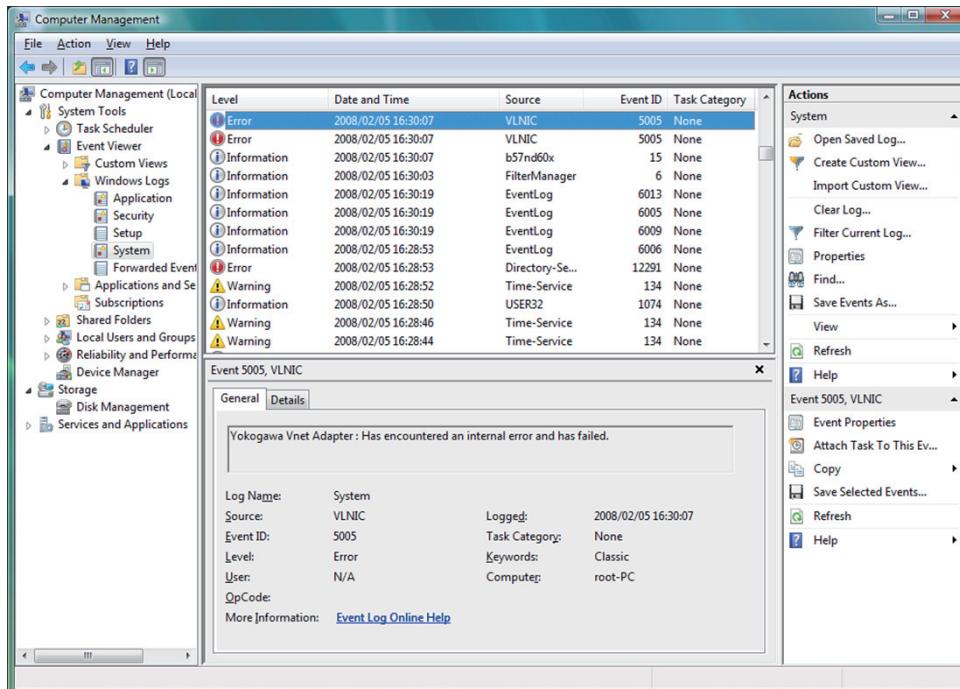


Figure C10.2.2-5 Event Viewer Recording VLNIC Errors (System)

1. Double-click a VLNIC error.

The Event Properties dialog box appears.

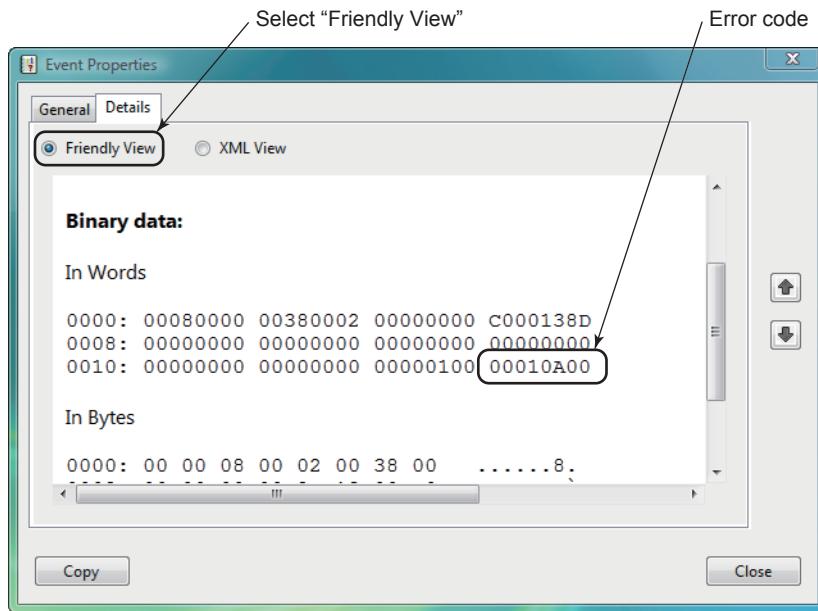


Figure C10.2.2-6 Event Properties

- 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 C10.2.2-1 Error Codes Generated when Starting the Driver

Code (*1)	Meaning
000101**	RAM parity error (failure of VF702/VF701/VI702/VI701 card)
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.

■ Restarted the Computer After Deleting the Vnet/IP Open Communication Driver without Removing the Vnet/IP Interface Card from the Computer

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 displays a message regarding driver installation.

In this case, ignore the prompting message and do not install the driver.

■ 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 C10.2.2-7 Windows Security Dialog Box (for Network Adapter)

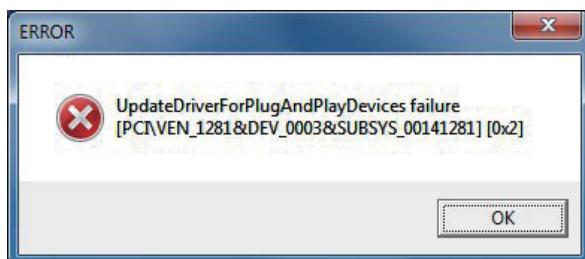


Figure C10.2.2-8 Error Message (for Network Adapter)

- **Control Bus Driver**

1. After restarting the computer, click [Control Bus Drier] 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 restart the computer. 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.

■ Failed to Disable the RIP Listener Service

You may fail to disable the RIP Listener service.

● Condition for Occurrence

This problem occurs when the Default Authentication Level of DCOM is configured to [None].

TIP

For example, the Default Authentication Level of DCOM is configured to None in the following cases:

- The security model is configured to Legacy model.
- The Default Authentication Level is configured to None to communicate with other computers.

● Remedy

You can avoid this problem with the following procedure.

1. Change the Default Authentication Level of DCOM from [None] to [Connect].
2. Restart the applicable virtual machine.
3. Install or uninstall the RIP Listener service.

SEE ALSO

For more information about how to change the default authentication level of DCOM, refer to:

C10.1.2, “Error Occurs when Server Manager is Started” on page C10-4

C10.3 Troubleshooting Related to CENTUM Products

This section describes how to handle problems related to CENTUM products.

C10.3.1 An Error Occurs when Downloading to an HIS after Changing Its IP Address

If the setting of Ethernet TCP/IP Protocol, which is set on the Network tab of the HIS properties called up on System View, is different from the default setting and the IP address of the HIS is changed, an error may occur during downloading to the HIS from the builder. If this error occurs, perform the following steps.

1. Log on to the HIS with the download error, using an administrative user account.
2. Open the following file using Notepad and correct the IP address to the one that corresponds to the computer name, and save.
`<CENTUM VP Installation folder>\COMMON\ETC\lmhosts.cs`
3. Select [Run as Administrator] from the context menu, open the command prompt, and run the following command.
 - `nbtstat -R` (R must be in capital) : updates the NetBIOS Cache table (to write the correction made in step 2).
 - `nbtstat -c` (c must be in small letter) : displays the NetBIOS Cache table.
4. Make sure that the Project Common Items are downloadable to the HIS.
5. Log on using a CTM_ENGINEER group's account and download the Project Common Items to all the HISs.

**SEE
ALSO**

For more information about downloading the Project Common Items to all the HISs, refer to:

- “■ Downloading the Project Common Items” in A2.7, “Procedure 7 Downloading the Contents Defined” in Engineering Tutorial (IM 33J10D20-01EN)
-

C10.3.2 Failure to Connect to the Remote Operation and Monitoring Server

When connecting to the remote operation and monitoring server (HIS-TSE server), if the message “The client could not connect to the remote computer.” is displayed and connection fails, the failure may be caused by the following problems:

- The order of network card bindings is reversed: the control bus interface card has higher priority than the Ethernet card

In Control Panel, select [Network and Internet] > [Network and Sharing Center]. The Network and Sharing Center window appears.

Select [Change adapter settings]. The Network Connections window appears.

From the Advanced menu on the Network Connections window, select [Advanced Settings]. In the Advanced Settings dialog box that appears, change the bindings setting so as to give higher priority to the Ethernet card.

TIP

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

- Settings of the network adapter for the remote desktop service is incorrect

Click [Connections] in the left pane of the Remote Desktop Service Configuration window. The RDPTcp connection is displayed in the right pane. Right-click [RDP-Tcp] connection and choose [Properties].

In the RDP-Tcp Properties dialog box that appears, set the Ethernet card on the Network Adapter tab.

- HIS-TSE server is not set to allow remote connections

Right-click [My Computer] and select [Properties]. The System Properties dialog box appears. On the Remote tab, select the check box for [Allow users to connect remotely to this computer].

- Applied Windows updates are different between HIS-TSE server and HIS-TSE client

This issue is caused by the Windows update provided in March 2018. Apply the same Windows update to both HIS-TSE server and HIS-TSE client. If the same Windows update cannot be applied to them, specify a setting for Local Group Policy Editor in HIS-TSE client.

In Command Prompt of HIS-TSE client, type `gpedit.msc` and start Local Group Policy Editor. In the left pane, select [Computer Configuration] > [Administrative Templates] > [System] > [Credentials Delegation]. In the right pane, select [Enable] for Encryption Oracle Remediation and select [Vulnerable] for Protection Level.

C10.3.3 AIP262 (AUX Board with USB Interface) USB Cable Disconnected from the Computer when Operation and Monitoring Function is Running

If the USB cable gets disconnected from the USB port of the computer or the AUX board while the HIS is running, a system alarm message (No. 0241) is generated.

If this occurs, reconnect the USB cable to the connecting port when the USB driver was installed and restart the computer.

If the USB cable was disconnected for maintenance purpose, be sure to reconnect the cable to the original connecting port on the computer.

If you are not sure about the connecting port on the computer when the driver was last installed, reinstall the driver on the computer.

**SEE
ALSO**

For more information about reinstalling the drivers, refer to:

- B4.4, "Installing the USB Driver for the Operation Keyboard" on page B4-77
 - B4.5, "Tasks Required for Setting Up the Console Type HIS" on page B4-79
-

C10.3.4 Shortcut to AD Organizer Disappeared from the Start Menu

If the following two licenses are assigned to one computer, deleting one license deletes the shortcut to AD Organizer from the Start menu:

- CENTUM VP Standard Engineering Function of 4,000 logical I/O points or less (Model: VP6E5100-V10N01 or VP6E5100-V10N02)
- Safety System Engineering and Maintenance Function of ProSafe-RS

In this case, redistribute the remaining license, and a shortcut to AD Organizer will be created in the Start menu. Follow these steps to redistribute the license.

1. Start License Manager on the license management station.
2. Export the package list.
3. Delete the applicable license for the target license-assigned station.
4. Distribute the license to the license-assigned station and thereby send a license deletion command.
5. Start License Manager on the license-assigned station to accept the change in license.
6. Start License Manager on the license management station.
7. Import the package list that has been exported.
8. Distribute the license to the target license-assigned station.
9. Start License Manager on the license-assigned station to accept the change in license.

SEE ALSO

For more information about export and import a package list, refer to:

3.9.1, "Importing and exporting package lists" in License Management (IM 33J01C20-01EN)

For more information about deleting the licenses, refer to:

"■ Deleting a license from a license-assigned station" in 3.2.1, "Modifying license assignments" in License Management (IM 33J01C20-01EN)

For more information about how to distribute licenses, refer to:

3.2.2, "Distributing modified licenses" in License Management (IM 33J01C20-01EN)

For more information about accepting licenses, refer to:

3.2.3, "Accepting modified licenses" in License Management (IM 33J01C20-01EN)

Blank Page

C11. Cautionary Notes for Upgrading

This section describes the cautionary notes on upgrading CENTUM VP.

■ How to Read This Section

When you upgrade a CENTUM system, read all the cautionary notes, from the next version or revision of the existing system to the latest revision, and perform the tasks.

For example, when you upgrade from R4.01.60 to R5.01.20, you need to perform all the tasks described in the sections from "C11.3 Upgrading to R4.02.00" through "C11.8 Upgrading to R5.01.20."

C11.1 Upgrading to R4.01.33

This section describes the cautionary notes regarding upgrading to R4.01.33.

■ Data Characters Displayed in Graphic View

Data character display in graphic view has been improved in R4.01.33. As a result, the display positions of data characters may be different between R4.01.33 or a later revision and a revision prior to R4.01.33.

With a CENTUM VP revision prior to R4.01.33, when the tag list is specified as the display data type to display data characters in graphic view, the data string length was fixed to seven digits. Consequently, data items that require more than seven digits (such as SUM values) were too large to be displayed and were displayed with asterisks (*****).

With R4.01.33 or a later revision, when the tag list is specified as the display data type, the actual number of digits required to display the data value will be used to display the data characters, resolving the problem of incomplete data display. (This is described as “default specification of R4.01.33 and later revisions.”) Due to the fact, however, that the number of displayed digits changes from a fixed length to an adjustable length, the display positions may change after the version is upgraded.

TIP

Items of the data values with more than 7 digits

- Function block common items: AFLS, AF, ALRM, AOFS, MODE, RAW, SUM, VN, BSTS
- Calculation block: RV, RVnn
- FUNC-VAR block: Xnn, Ynn
- BDSET, BDSET-1C, BDSET-2, BDSET-2C, BDSET-1L, BDSET-2L, BDA, BDA-C blocks: DTnn, DHnn, DLnn
- SEBOLP1 to SEBOLP3 blocks: CHnn, DTnn
- SFC, UNIT user defined data items and so on

■ Cases Where Data Character Display Position Changes After Upgrade

Data character display position changes after the upgrade if the condition 1 below is true and condition 2 below is false.

The following data character display tab can be found in the data character display properties dialog box.

Condition 1:

Condition 1 is true if all of the following are true.

- The check box for [Is Advanced Alignment] is selected on the Data Character Display tab.
- [Tag List] is selected as the Type under Display Format on the Data Character Display tab.
- The length of tag list display is set to other than seven digits.

Condition 2:

Condition 2 is true if any of the following is true.

- [Left] is selected in Alignment and the check box for [Show Engineering Unit] is not selected on the Data Character Display tab.
- [Left Tight] is selected in Alignment on the Data Character Display tab.
- [Distributed] is selected in Alignment and the check box for [Show Engineering Unit] is not selected on the Data Character Display tab.

■ Addressing Data Character Display Position Change After Upgrade

To address any changes in the data character display position after the upgrade, you can select a specification of data character display of a revision prior to R4.01.33 (the same specification as that of R4.01.00) in the registry.

- Registry = 0: Default specification for R4.01.33 or a later revision (Default setting)
- Registry = 1: Specification for a revision prior to R4.01.33 (same specification as that of R4.01.00)

The figure below illustrates the display in the following situations when the check box for [Is Advanced Alignment] is selected.

- When a specification of a revision prior to R4.01.33 is selected, or when a specification of a revision R4.01.33 or later, but with the specification prior to R4.01.33 (the same specification as that of R4.01.00) is selected (Registry = 1)
- When the default specification for R4.01.33 or later is selected (Registry = 0)

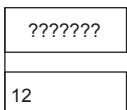
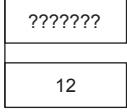
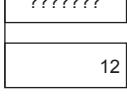
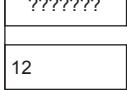
IMPORTANT

When data character string display type is defined as Tag List, the number of digits will be determined when running the graphic.

After defining the data character string displayed on the builder, if further changes are performed on the builder regarding the number of digits setting in the tag list, the display area of the data character string may become larger than what you previously defined. If the Is Advanced Alignment option is selected, the display area is enlarged from the base of the left end.

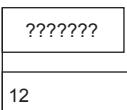
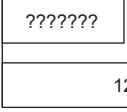
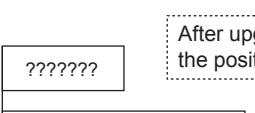
When defining the graphic builder, this feature should be put in mind.

- Specification Prior R4.01.33
- Choose specification prior R4.01.33 for R4.01.33 or later version (Registry =1)(*1)

		Number of Displayed Digits = 7 (Fixed)
Left Left Tight		
Center		
Right Right Tight Compact Center		
Distributed		

Only displays 7 digits even TagList is specified.
 For the data value with more than 8 digits,
 asterisks (******) will be displayed.
 For the text data with more than 8 digits,
 the extra characters will be truncated.

- Choose the default specification of R4.01.33 or later version (Registry =0)

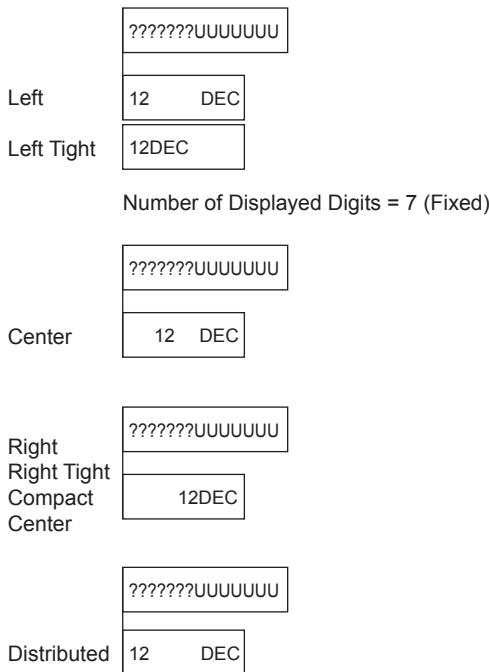
 	Upper: Defined on Builder
	Lower: Displayed on Graphic View
	When Number of Displayed Digits = 16 (defined with TagList)
 	

After upgrading to R4.01.33 or later,
 the position changed.

*1: After setting Registry=1, the number of digits will
 be fixed to 7 digits regardless whether the [Is Advanced
 Alignment] option is checked or not.

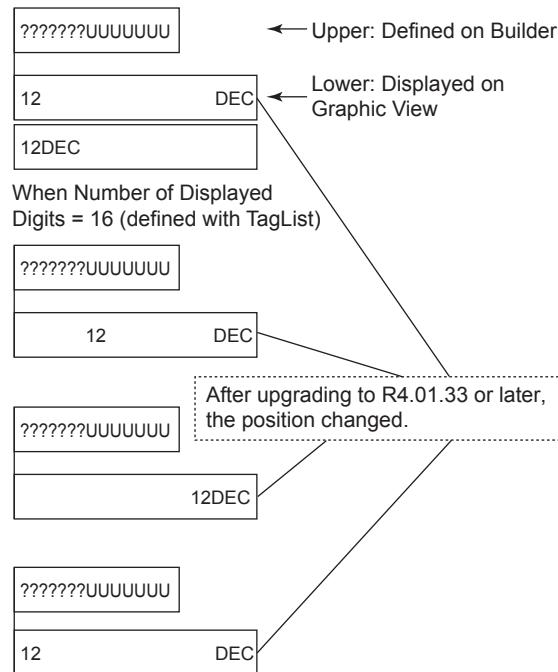
Figure C11.1-1 Displays on Builder and Graphic View (No Engineering Unit)

- Specification Prior R4.01.33
- Choose specification prior R4.01.33 for R4.01.33 or later version (Registry =1)(*1)



Only displays 7 digits even TagList is specified.
For the data value with more than 8 digits,
asterisks (******) will be displayed.
For the text data with more than 8 digits,
the extra characters will be truncated.

- Choose the default specification of R4.01.33 or later version (Registry =0)



*1: After setting Registry=1, the number of digits will be fixed to 7 digits regardless whether the [Is Advanced Alignment] option is checked or not.

Figure C11.1-2 Displays on Builder and Graphic View (With Engineering Unit)

SEE ALSO

For more information about the registry setting for R4.01.00 compatibility, refer to:

C11.1.2, "Setting Registry for R4.01.00 Compatibility" on page C11-9

■ Dealing with Data Character Problems of Different Version Software

In order to deal with the problems of the data character digits, the problems are classified into the following three cases:

- When using Prior R4.01.33 version software (Specification of R4.01.00)
- When using R4.01.33 or a later version software and choosing the default specification of R4.01.33 or a later version software (Registry=0).
- When using R4.01.33 or a later version software and choosing the legacy specification of R4.01.00 software (Registry=1).

Table C11.1-1 Dealing with Problems of Different Version Software

Revision	Problem	
	Number of Digits: Fixed to 7 and cannot display 8 digits or more.	Display Position: Different from that of R4.01.33 or earlier versions.
Prior R4.01.33 (R4.01.00 Specification)	Use different methods instead of Tag List.	- (Irrelevant)

Continues on the next page

Table C11.1-1 Dealing with Problems of Different Version Software (Table continued)

Revision	Problem	
	Number of Digits: Fixed to 7 and cannot display 8 digits or more.	Display Position: Different from that of R4.01.33 or earlier versions.
R4.01.33 or Later Registry=0 (Default Specification for R4.01.33 or later versions)	- (Irrelevant) Note: Limited to displayed the number of digits of defined by Tag List.	<ul style="list-style-type: none"> A running system or a tested system, no further engineering generations on the builders (*1): Set the registry to have the same specification of R4.01.00 (Registry=1). Note: Make sure it is acceptable for your system that the number of digits can be displayed is fixed to 7. When more settings are required on the builder Clear the checkbox for [Is Advanced Alignment], or use another method without using the tag list option.
R4.01.33 or Later Registry=1 (Legacy Specification same as R4.01.00)	Use different methods instead of Tag List.	<ul style="list-style-type: none"> - (Irrelevant) Note: Specification is the same as R4.01.00

*1: If a different measure has been taken to deal with the display position problem, it may become difficult for some systems to solve the problem by changing settings on the graphic builder.

TIP

For the system that under the engineering generation phase, it is better to use the specification of R4.01.33 or later versions (Registry=0) to define the data character display.

If you want to keep the display position as the specification of R4.01.00, after upgrading to R4.01.33 or a later version, you need to set the registry according to the procedure.

SEE ALSO

For more information about the registry setting for R4.01.00 compatibility, refer to:

C11.1.2, "Setting Registry for R4.01.00 Compatibility" on page C11-9

C11.1.1 Setups After Installation

Under the following circumstances, the setups below need to be performed accordingly.

■ Unused Ethernet Cards on Computer for Operation and Monitoring Function

If you connect two or more Ethernet cards to a computer used for the operation and monitoring function, you have to follow the steps below to “disable” the unused Ethernet cards in Network properties. Administrator’s privileges are required to specify this setting.

- **On Windows XP/Windows Server 2003**

1. From the Start menu, select [Control Panel] > [Network Connections].
The Network Connections window appears.
2. Right-click the unused Ethernet connection and select [Disable].

- **On Windows Vista/Windows Server 2008**

1. From the Start menu, select [Control Panel] > [Network and Internet] > [Network and Sharing Center].
The Network and Sharing Center window appears.
2. Select [Manage network connection].
The Network Connections window appears.
3. Right-click the unused Ethernet connection and select [Disable].

■ Notes on HIS installed on Windows Server 2008

If you install the operation and monitoring function on Windows Server 2008, configure the following setting. Administrator’s privileges are required to specify this setting.

1. From the Start menu, select [Control Panel] > [System].
The System Properties window appears.
2. Select the [Advanced] tab and click [Settings] of Performance.
The Performance Options dialog box appears.
3. Select the [Advanced] tab and select [Programs] in Processor Scheduling.

■ Change Primary Direct (PRD) Button Design

The design of the Primary Direct button on toolbar of tuning window is changed as follows:

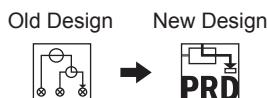


Figure C11.1.1-1 Change Primary Direct (PRD) Button Design

To revert from new design to old design, or to change from the old design to new design, you need to double click the following commands respectively. The button design change becomes valid when you open the tuning window next time.

- Revert to the old design prior CENTUM VP R4.01.33
<CENTUM VP installation folder>\his\tool\OldPRDIcon.reg
- Change to new design
<CENTUM VP installation folder>\his\tool\NewPRDIcon.reg

■ Notice on Handling FIO Analog Output Module (Current Output)

After upgrading, if the following settings are made for an FIO analog output module (current output) on the IOM builder, run downloading to the output module.

- Reverse Output is specified.
- OOP Clear is enabled.

C11.1.2 Setting Registry for R4.01.00 Compatibility

If you want to set the data character display (where the [Is Advanced Alignment] option is checked and the Tag List type is defined as the display format) is conform to R4.01.00 specification, you need to redefine the registry for data character display of HIS in the system.

TIP

The explanation in this section is provided as a measure to cope with the problem that the display positions of data characters in graphic view may change after upgrading when Advanced Alignment or Tag list is specified as the display type for data characters, which was mentioned in the earlier part in the section "Upgrading to R4.01.33."

IMPORTANT

After reverting to R4.01.00 compatible specification, the data character string on Graphic View will be fixed to 7 digits. For the data items that require more than 7 digits (such as SUM values), the data value will be too large to be displayed but displayed with asterisks (*****).

Make sure the data values are not having more than 7 digits.

The procedure for changing the registry related to the data character display is as follows.

To use the same specification as R4.01.00, log on as an administrative user and perform these steps:

1. Use Windows Explorer to open the <CENTUM VP installed folder>HIS\tool, and double-click SetAdvancedAlignmentR40100CompatibleR40126.reg program in the folder.
The registry is set to 1, which specify the use of R4.01.00-compatible specification.

TIP

To reset to the default specification of R4.01.33 or later versions, log on as an administrative user and do the following:

Use Windows Explorer to open the <CENTUM VP installed folder>HIS\tool, and double-click ResetAdvancedAlignmentR40100CompatibleR40126.reg program in the folder.

The registry is reset to 0, which specify the use of R4.01.33 or later versions' default specification.

2. Restart the computer.

TIP

Once you changed the registry setting regarding the data character display (IsNumberOfDigitTypeCheck), the setting is retained during installation. When you perform upgrading installation, you do not need to do the setting again because the previously set value is applied.

C11.2 Upgrading to R4.01.60

To use the new functions added in R4.01.60 after upgrading from CENTUM VP R4.01.33 to R4.01.60, special tasks may be required depending on the function you want to use.

The cautions mentioned below apply to when upgrading from R4.01.33 to R4.01.60.

If you are upgrading from a revision earlier than R4.01.33 to R4.01.60, also read the cautions for upgrading between revisions described in earlier sections.

C11.2.1 Cautions Regarding Object Blinking on Graphic View

The specifications regarding object blinking on Graphic View are changed in R4.01.60 version software.

■ Differences in Blinking Specification

For objects blinking in graphic view, the color specification of the object in the moment when it is not blinking (*1) has changed in R4.01.60.

*1: The state in which the object is not blinking refers to the moment when the object is "not lit" as opposed to "being lit."

- Prior R4.01.60 Versions

When the object blinks at off status, the object turns to transparent color.

- R4.01.60 and Later Versions

When the object blinks off, the object turns to the same color of the canvas.

The detailed object blinking behaviors of R4.01.60 and later versions are indicated as follows:

Table C11.2.1-1 Detailed Object Blinking Behaviors of R4.01.60

Component	Name Behavior while Blinks off	Remarks
Line	Line color changes to canvas color	
Arc	Line color changes to canvas color	
Poly Line	Line color changes to canvas color	
Pen Tool	Line color changes to canvas color	When a line closes, the enclosure part will be treated as an object. The filling color of the object changes to canvas color.
Rectangle	Filling color changes to canvas color	Rectangle Filling color changes to canvas color If the filling color is transparent, the line color will change to canvas color.
Fill Area	Filling color changes to canvas color	Fill Area Filling color changes to canvas color If the filling color is transparent, the line color will change to canvas color.
Sector	Filling color changes to canvas color	Sector Filling color changes to canvas color If the filling color is transparent, the line color will change to canvas color.
Ellipse	Filling color changes to canvas color	Ellipse Filling color changes to canvas color If the filling color is transparent, the line color will change to canvas color.
Circle	Filling color changes to canvas color	Circle Filling color changes to canvas color If the filling color is transparent, the line color will change to canvas color.
Marker	Highlighted part changes to transparent.	
Text	Text color changes to canvas color	
Data Circle	Foreground color changes to canvas color	
Data Arrow	Arrow color changes to transparent.	
Data Bar	Foreground color changes to canvas color	
Data Character	Text color changes to canvas color	
Push Button	Background color changes to canvas color	

C11.2.2 Selecting Actions of Graphic Objects

You can select the following actions for the controls on graphic views that were created on CS 1000/CS 3000.

- Action of the transparent controls when the modifier condition is satisfied
- Action of the text controls and data character controls for which [Transparent] is specified as the background color and also [Invert] is specified as the modifier action
- Action of the text controls and data character controls for which both [Blink] and [Invert] are specified as the modifier action

If you have made these selections, download the project common part to all HISs.

SEE ALSO

For more information about selecting actions of graphic objects, refer to:

7.22.2, "Selecting Actions of Graphic Objects" in Engineering Reference Vol.2 (IM 33J10D11-01EN)

C11.2.3 Number of Operation Windows

After upgrading installation, the settings for displaying the number of operation and monitoring windows will be reset to default.

The number of displayed windows needs to be defined according to the system environment settings.

SEE ALSO

For more information about the number of operation and monitoring windows displayed, refer to:

- “● Settings Related to Operation Screen Mode and Number of Windows” in “■ Settings Related to Multiple-Monitor in the HIS Setup Window” in 10.5, “Setting the Multiple-Monitor Environment” in Human Interface Stations Reference Vol.2 (IM 33J05A11-01EN)
-

C11.2.4 If Multiple-Monitor Support Package is used

If Multiple-Monitor Support Package is used, pay attention to the following notices:

■ HIS Setup Window Settings

In the R4.01.60 environment, if either of the following setting items on the HIS Setup window has been changed from the initial value, the setting is reset to the initial value during upgrading installation. Change the setting as necessary.

- On the Display tab, change the Number of Container Windows if Windows Mode is selected for Operation Screen Mode. (*1)
- On the Display tab, change the Number of Pop-Up Windows if Full Screen Mode is selected for Operation Screen Mode. (*2)

*1: Initial value is 5

*2: Initial value is 2

TIP

The number of container windows for windows mode and the number of pop-up windows for full screen mode settings are counted on the bases per monitor in the environment prior R4.01.60. From R4.01.60, theses numbers are counted on the basis per HIS. When upgrading to R4.01.60 or a later version, these numbers will be set with the initial values.

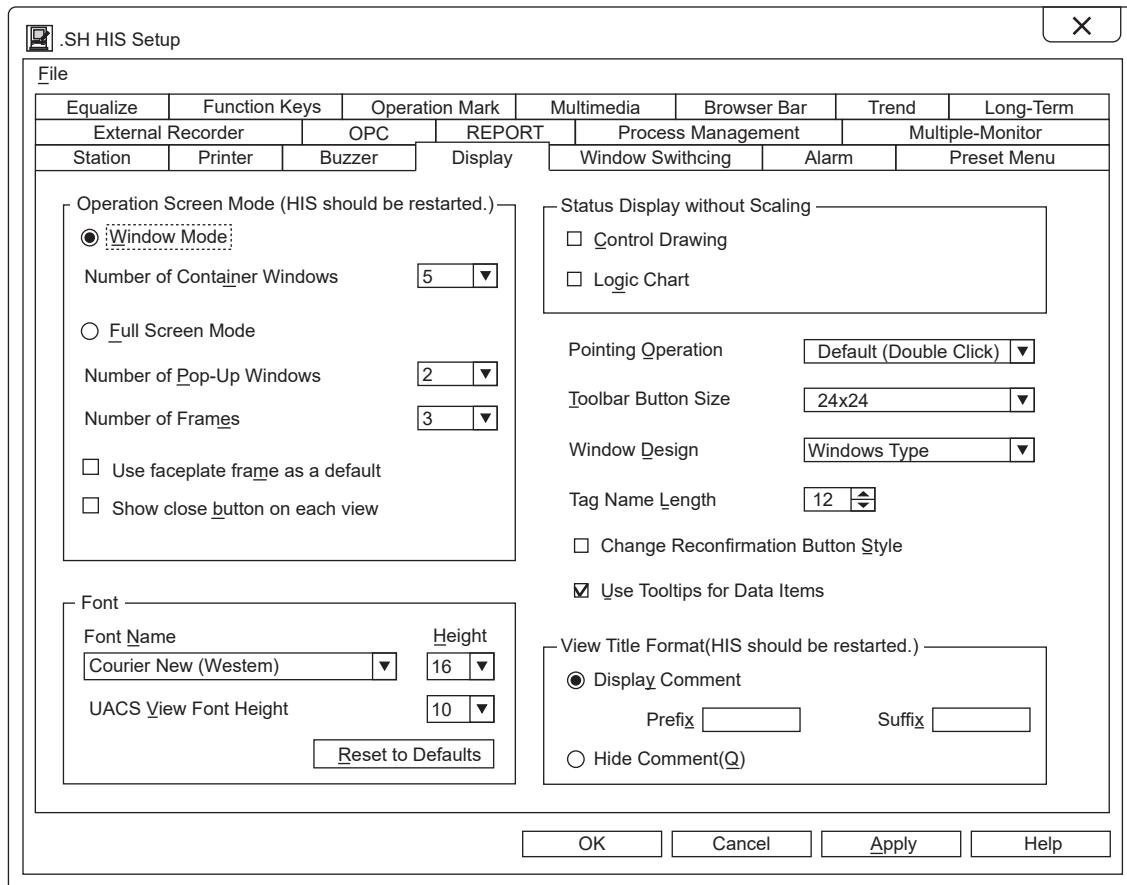


Figure C11.2.4-1 Display Tab in HIS Setup Window

SEE

ALSO For more information about setting the number of container windows or pop-up windows (operation screen mode), refer to:

- “■ Settings in the Display Tab” in 4.3.4, “Display Tab” in Human Interface Stations Reference Vol.1 (IM 33J05A10-01EN)

■ Using System Function Key to Call Identical Windows on Same Monitor

The specification to use CPYn command to call the identical windows is changed.

SEE

ALSO For more information about using the Copy Window (CPYn) command, refer to:

- “● Copy Window (CPYn) n= 1 to 4” in “■ System function key for validating Multiple-Monitor Support Package” in 9.2.3, “Assigning Execution of a System Function Key Command” in Human Interface Stations Reference Vol.2 (IM 33J05A11-01EN)

For more information about calling an identical window, refer to:

- “● Restrict Identical Windows in Same Monitor” in “■ Overview of Multiple-Monitor” in 10., “Multiple-Monitor” in Human Interface Stations Reference Vol.2 (IM 33J05A11-01EN)

C11.2.5 Refresh Period of Views

The specification regarding the refresh period of Views is changed.

**SEE
ALSO**

For more information about refresh period of Views, refer to:

- Refresh Period of Views Determined by HIS" in 2.2, "Operation Screen Mode" in Human Interface Stations Reference Vol.1 (IM 33J05A10-01EN)
-

C11.2.6 Frame Color of Graphic Tag Objects

When selecting a component on Graphic View, if the option of [Activate Tag Object] is specified on the graphic builder, the selected component will be indicated with a frame. The color of this frame is orange for the versions prior R4.01.60. From R4.01.60, this color becomes green.

On R4.02.00 or later versions, you can change the color of this frame to a desired color.

SEE ALSO

For more information about changing the frame color, refer to:

- “● Frame Color of Graphic Tag Object” on page C11-21
-

C11.2.7 Operation Disabled Frame Color of Graphic Push Button and Softkey

When a graphic push button and softkey is guarded from the operations, the color of the Operation Disabled Frame is black for the versions prior R4.01.60. From R4.01.60, this color becomes white.

C11.2.8 Notice on Control Actions of Graphic View

On the graphic builder, the specifications regarding the controls for calling menu dialog, calling windows and so on are upgraded. If the required parameter of a control is not properly entered, when calling the Graphic View, the control cannot be displayed.

(Related Controls)

- Push Button
- Touch Target
- Softkeys
- Overview

(The required parameters)

- Label or Data for Call Menu Dialog on Function tab
- Parameter for Call Window on Function tab
- Parameter for Instrument Command Operation on Function tab
- Program name for Execute the Program by File Name on Function tab
- Parameter for Call Data Input Dialog on Function tab
- Parameter for Data-Item-Dependent Menu Dialog on Function tab
- Panel set name for Call Panel Set on Function tab
- Parameter for Others on Function tab

C11.3 Upgrading to R4.02.00

To use the new functions added in R4.02.00 after upgrading from CENTUM VP R4.01.60 to R4.02.00, special tasks may be required depending on the function you want to use.

The cautions mentioned below apply to when upgrading from R4.01.60 to R4.02.00.

If you are upgrading from a revision earlier than R4.01.60 to R4.02.00, also read the cautions for upgrading between revisions described in earlier sections.

■ Builders

Cautions related to builders are described as follows:

- **Setting Communication Speed**

The communication speed of ALR111/121 communication module can be defined on the ALR111/121 properties sheet of CENTUM VP R4.02.00 is 38400bps or lower.

When the speed is set to 57600 bps or faster for an existing project and you open the module's Properties dialog box after upgrading to CENTUM VP R4.02.00, the setting value will be checked, and an error will occur if the value is set outside of the range.

Note, however, that even if a value outside of the range is specified for an existing project, communications will still be established at the specified speed with R4.02.00 or a later revision as long as you do not open the Properties dialog box.

- **Data Connection between FF Faceplate Blocks and FCS Function Blocks**

In CENTUM VP R4.01.60, when data connection between a FF faceplate block and FCS function block FF is created, during generation, a warning message will occur and the downloading will abandon the connection data. Consequently, the application will not properly function.

If this problem occurs, you need to do the following after installing R4.02.

1. Start the control drawing builder.
2. Open the property sheet of the FF faceplate block that caused the warning message, and click [OK].
If there are multiple blocks causing the warning message in the same drawing, it should be performed for any one of the blocks.
3. On the control drawing builder, run [File] > [Download].
Then, it will correctly generate the connection information and download to the FCS, ALF111, and pertinent devices.
4. Perform the same operations to all the control drawings that have the same problem.

■ HIS Functions

Cautions related to the operation and monitoring function are described as follows:

- **Leading Zeros of Graphic Data Character Display**

When the data character display is defined as follows, the data are displayed with leading zeros in R4.02.00 while the data were displayed without leading zeros in R4.01.00.

Table C11.3-1 Leading Zeros of Graphic Data Character Display

Setting	Pattern 1	Pattern 2
Is Advanced Alignment	Unchecked	Unchecked
Type	Number, %, Hex	Tag List (Hex)

Continues on the next page

Table C11.3-1 Leading Zeros of Graphic Data Character Display (Table continued)

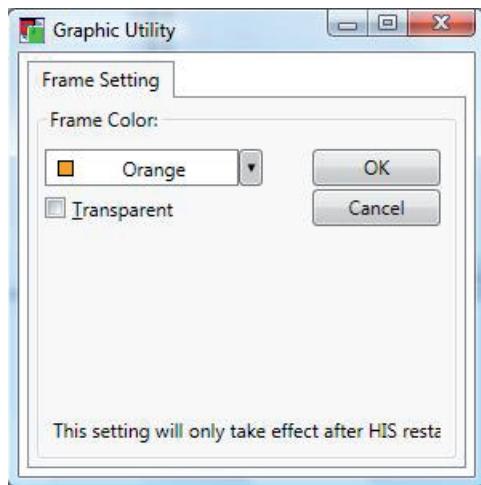
Setting	Pattern 1	Pattern 2
Alignment	No	No, Right
Leading Zeros	Checked	-

- **Frame Color of Graphic Tag Object**

On a graphic window, if an object that the option of [Activate Tag Object] is checked is selected, a frame will be displayed to show that the object is being selected. In R4.01.60 or earlier version software, this frame is displayed in orange while in a version later than R4.01.60, this frame becomes green.

You can change this frame color of the selected tag object by performing the following procedure on each HIS. If you want to set the same frame color on multiple HISs, refer to the TIP at the end of this section.

1. Log on using an administrative user account.
2. Under the Program Folder of Windows, find the following path: C:\Program Files\YOKOGA WA\IA\iPCS\Products\CENTUMVP\Program\ and then double-click the following file: Yokoga wa.IA.iPCS.Platform.View.Graphic.Utility.FrameColorSettingTool.exe
The tool for changing frame colors starts.

**Figure C11.3-1 Graphic Utility**

The currently valid frame color is displayed in the box. If you select a color with text color name, the text of the color name is displayed. Otherwise, the color name is displayed in a hexadecimal code (such as #FF123456). You cannot directly enter a text name.

3. You can only click the button for picking up color, and then choose a color on the color palette.

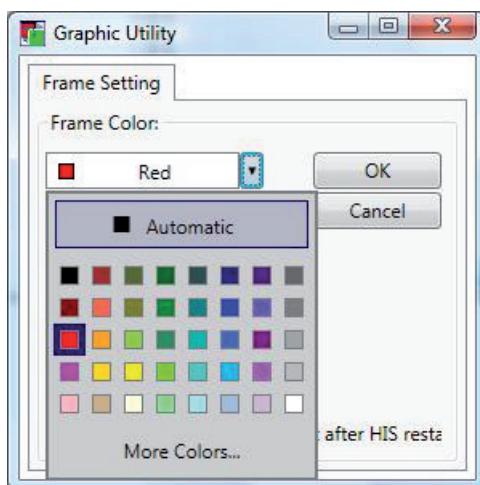


Figure C11.3-2 Color Picker

If you click [More Colors], the Color Setting dialog box appears.

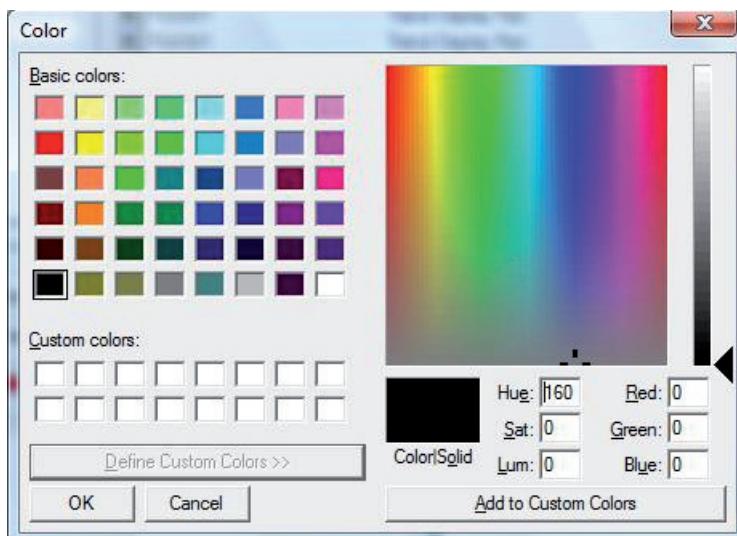


Figure C11.3-3 Color Setting Dialog Box

You can choose a customized color in this dialog box.

If you want to change the color of the frame of a tag object to transparent, select the [Transparent] check box.

4. After you have selected the color, click [OK].
The selected color is saved in a file and the following message is displayed.

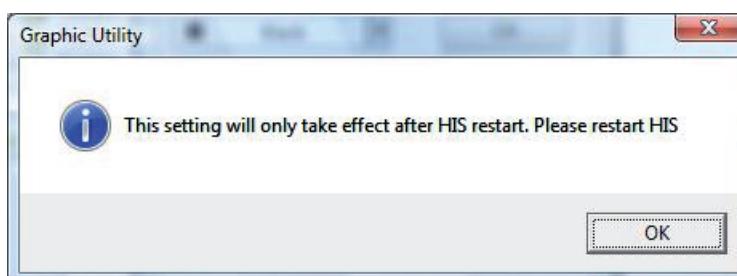


Figure C11.3-4 Message for Confirming Restarting

5. Restart the HIS.

TIP

When applying the same setting to multiple HISs, you can simply copy the definition file to the HISs.

Definition file:

<All Users Application data>\Yokogawa\IA\iPCS\Products\CentumVP\Graphic\Config\UserConfig.xml

Place the definition file in the same folder location and restart the HIS.

■ FCS Functions

Cautions related to FCS are described as follows:

- **Normalization CALCULUS I/O Data**

Based on the specifications changed in R4.02.00, the following items are changed accordingly.

Table C11.3-2 Normalization of CALCULUS I/O Data

	4.01.60	R4.02.00
Data Limit	Between 0 and 1 after normalization.	Between -1 and +1 after normalization.
CPV=RV	Invalid	Valid
Scale high/low limits	Normalized value used in calculation	Actual value used in calculation

For the data, how to handle the limit values and CPV=RV is changed in R4.02.00. Therefore, after upgrading the FCS offline downloading need to be performed.

Since how to handle the scale high/low limits are also changed R4.02.00, after upgrading, besides the FCS offline downloading, the downloading on the control drawing builder (*1) also need to be performed.

*1: On the control drawing builder, you only need to open the builder and perform downloading. You do not need to edit anything.

■ Communication Functions

Cautions related to communication functions are as follows:

- **Control Bus Driver**

To use the control bus driver of CENTUM VP R4.02.00 or later on Windows Vista or Windows Server 2008 computers, you must apply the hotfix module KB971060.

The hotfix module KB971060 is applied with the installer of CENTUM VP R4.02.00 or later.

C11.4 Upgrading to R4.02.30

To use the new functions added in R4.02.30 after upgrading from CENTUM VP R4.02.00 to R4.02.30, special tasks may be required depending on the function you want to use.

The cautions mentioned below apply to when upgrading from R4.02.00 to R4.02.30.

If you are upgrading from a revision earlier than R4.02.00 to R4.02.30, also read the cautions for upgrading between revisions described in earlier sections.

■ About Unit Transition Conditions

In R4.02.30, the following problems which occurred in the earlier versions have been solved.

- If any 8-characters-long data item names are contained in the transition conditions for a unit instrument, the FCS cannot judge the transition conditions correctly and the unit status goes to SUSPEND.
If a problem such as above occurs, perform the following operations after installing R4.02.30 to resolve the problem.

● Downloading the Unit Procedures or Unit Recipes

Download the unit procedures or unit recipes that contain the above mentioned transition conditions in the following manners.

- If the unit procedure was defined with the functional block detail builder, use the control drawing builder to make a change to the applicable unit instrument (specifically, change the tag comment and then restore it), and then perform downloading.
- If the unit procedure is shared, use the unit procedure builder to perform downloading.
- If the unit recipe procedure is used, check if there is any batch that is running or a reserved batch that is using the applicable recipe. If you find such a batch that is running, terminate the batch. Delete any such reserved batch. Make sure that there is no batch that is running or reserved that is using the applicable recipe before downloading the recipe using the recipe procedure builder.

C11.5 Upgrading to R4.03.00

To use the new functions added in R4.03.00 after upgrading from CENTUM VP R4.02.30 to R4.03.00, special tasks may be required depending on the function you want to use.

The cautions mentioned below apply to when upgrading the version from R4.02.30 to R4.03.00.

If you are upgrading from a revision earlier than R4.02.30 to R4.03.00, also read the cautions for upgrading between revisions described in earlier sections.

■ Windows Standard Control Stencils Removed

From R4.03.00, the Windows Standard Control stencil was removed.

The Picture box control that used to appear on the Windows Standard Control stencil was moved to the Basic shapes stencil. For the applications that already include the controls on the Windows Standard Control stencil, do the following to cope with this change.

- If the Button object of the Windows Standard Control stencil is used, use PushButton of the Buttons and Data Display Controls stencil instead.
- If the Label and Text Box are used, use Text of the Basic Shape Controls stencil instead.

It is not recommended to use the Windows Standard Control stencil, however, you can display the stencil in this way: Click [Open Stencil] on the File tab on the ribbon to open the dialog box for designating a stencil file, and designate the following file.

For Windows XP:

C:\Documents and Settings\All Users\Data Application \Yokogawa\IA\iPCS\Products\CentumVP\Graphic\WindowsControls.sdx

For Windows Vista:

C:\ProgramData\Yokogawa\IA\iPCS\Products\CentumVP\Graphic\Controls.sdx Windows

■ Cautionary Notes for Batch-Related Windows

The operation of the product overview has been changed in R4.03.

SEE ALSO

For more information about the product overview, refer to:

7.2, "Product Overview" in Batch Management System Reference (IM 33J05L10-01EN)

■ Color Changes in Batch-Related Windows

The display colors in the batch-related windows have changed in R4.03.

The white characters with the black background in the previous revisions have now changed to black characters with the white background.

■ Operation for Acknowledging Process Alarm in Graphic Window

The operation for acknowledging the process alarm in the Graphic window was allowed if the applicable function block was included in the operation and monitoring range specified by the security builder. Now in R4.03.00, this operation can be performed if the applicable function block is included in the range to be acknowledged as specified by the security builder.

■ Cautionary Notes for Using the MoveCursor Function in the Graphic Interface

In R4.03 or a later revision, the MoveCursor function cannot be used to move the cursor unless the graphic view is in focus.

■ Downloading Database to HIS

After you upgrade to R4.03.00, download the database to the HIS using the following procedures.

- Downloading the project's common section to the HIS from the System View
In the System View, select the upgraded HISs and then download the project common section.
Alternatively, the following procedure can be used.
- Downloading the project common section to all HISs from the System View
In the System View, select the project that includes the upgraded HISs and then download the project common section.

Through this operation, you can download the common section to all stations in the Equalization Scope that are included in the project at once.

If none of the operations above is performed, the following buttons will be grayed out and disabled in the FCS status display view.

- Save tuning parameter button
- Load IOM button
- Start FCS button
- Stop FCS button

■ When FF Faceplate Block is Connected for Remote Cascade Loop

In CENTUM VP R4.02.00, when data item of a FF faceplate block is connected to a terminal of a FCS function block, during generation, a warning message will occur and the downloading will abandon the connection data. Consequently, the application will not properly function and, to be careful, there is no error message to indicate this abnormality.

If this problem occurs, do the following after installing R4.03.00.

1. Start the control drawing builder.
2. Open the property sheet of the FF faceplate block that caused the warning message, and click [OK].

TIP

If there are multiple blocks causing the warning message in the same drawing, it should be performed for any one of the blocks.

3. On the control drawing builder, run [File] > [Download].
Then, it will correctly generate the connection information and download to the FCS, ALF111, and pertinent devices.
4. Perform the same operations to all the control drawings that have the same problem.

C11.6 Upgrading to R5.01.00

To use the new functions added in R5.01.00 after upgrading from CENTUM VP R4.03.00 to R5.01.00, special tasks may be required depending on the function you want to use.

The cautions mentioned below apply to when upgrading from R4.03.00 to R5.01.00.

If you are upgrading from a revision earlier than R4.03.00 to R5.01.00, also read the cautions for upgrading between revisions described in earlier sections.

■ CENTUM Data Access Library

If you are using the OPC security function supported in CENTUM VP R5.01 or later in the VB.NET application created using the CENTUM data access library of a revision earlier than CENTUM VP R5.01, you must reposition the CENTUM data access library.

Follow these steps to reposition the CENTUM data access library.

1. Delete the CENTUM data access library in the existing VB.NET application form from the form.
2. In Solution Explorer, double-click the [My Project] node of the target project.
3. In Project Designer, click the [Reference Configuration] tab.
4. In the Reference Configuration dialog box, click the reference for AxInterop.libbkuCENTUM.dll and Interop.libbkuCENTUM.dll.
5. Click [Delete].
6. Place the CENTUM data access library in the form.
7. In Solution Explorer, click the target project.
8. From the [Build] menu, click [Rebuild] to rebuild the target project.

IMPORTANT

When you reposition the CENTUM data access library based on the procedure above, the property value set by the existing VB.NET application in the CENTUM data access library will be initialized. Be sure to check the setting in the existing properties before performing this procedure and reconfigure the setting after the library has been repositioned.

SEE ALSO

For more information about positioning the library, refer to:

2.2, "Using the CENTUM Data Access Library" in CENTUM Data Access Library (IM 33J05F10-01EN)

■ Improvements in CAMS for HIS Historical Viewer Search

The search functions of the CAMS for HIS Historical Viewer have been significantly improved in CENTUM VP R5.01.00. With this version, an index file can be internally generated automatically to narrow down the search. With versions R4.03.00 or prior, a search required a long time because all historical files (of up to 20 GB capacity) were targeted for the search unless a specific period was specified.

Therefore, you can do the following to generate an index file for the historical files saved R4.03.00 or prior versions so as to utilize the R5.01.00 feature to search these historical files.

- **Applicable Target HISs**

The HISs on which CAMS for HIS was enabled in R4.03.00 or prior will be the target.

● Operation Procedure

Follow these steps to create an index file for the historical files in R4.03.00 and prior.

TIP

It can take up to approximately one hour and 30 minutes to generate an index file (when there is a historical file of up to 20 GB capacity). You can still perform operation and monitoring on the HISs while the index file is being generated.

1. Run the following file to start the CAMS for HIS Index File Generator.

<CENTUM VP Installation Folder>\CAMS\CAMSHistIndex.exe

The CAMS for HIS Index File Generator dialog box appears.

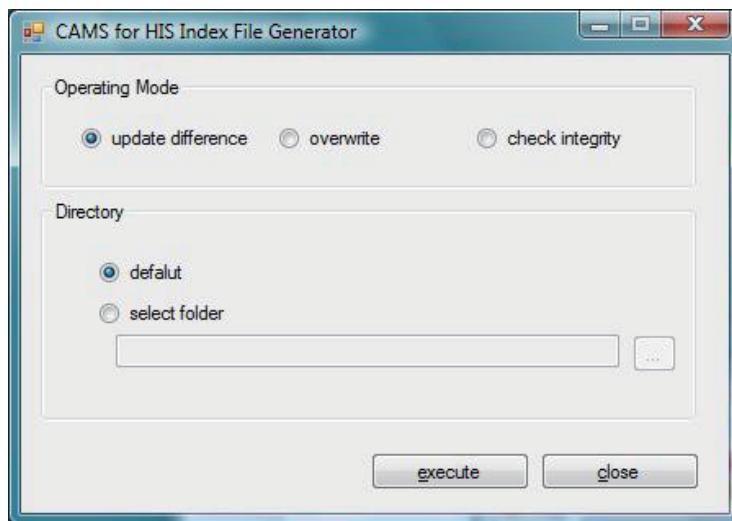


Figure C11.6-1 CAMS for HIS Index File Generation Tool Dialog Box

2. Specify the operating mode and the directory.

Table C11.6-1 Operation Modes and Directories

Item Name		Description
Operating Mode	Update only the differences	If an existing index file exists, only the differences will be updated. If there is no existing file, a new index file will be created
	Overwrite	A new index file will be created whether there is an existing file or not.
	Consistency check	The existing index file will be loaded and checked for consistency.
Directories	Standard	The CAMS for HIS standard folder will be selected when generating the index.
	Specified directory	The long-term archive folder will be selected when generating the index. Only the folder named CamsHist can be specified.

3. Click [execute].
A confirmation dialog box appears.
4. Click [OK].
The processing starts and a dialog box appears to indicate the progress.
5. When the processing is complete, the Complete dialog box appears; so click [OK].

TIP

If there is an error while the index file is being generated, the error detail is output to the following file. Review the error detail and generate a new index file again.

<CENTUM VP Install folder>\CAMS\LOG\MNTLOG\CAMSHistIndex{0|1|2}.log

■ Addressing the Graphic File Format Change

The file format used in CENTUM VP R5.01.00 was changed first in R4 for performance improvement of the graphic file. Accordingly, the HIS needs to be downloaded after an upgrade.

■ Upgrading of FCS

If you are not using the new functions added in R5.01.00, you can complete the FCS version upgrade simply through an offline download to the FCS from the upgraded system builder function. Even if the offline download cannot be performed, the following functions will still be available if included in the functions of the version before the upgrade.

- Online maintenance and save tuning parameters functions using the system builder function upgraded to R5.01.00
- Operation and monitoring function upgraded to R5.01.00

● Using the New Functions Added in R5.01.00

To use the following new functions added in R5.01.00, you need to perform the specific actions.

Table C11.6-2 New Functions and Actions Required for FCS

Function Name	FCS Prior to Upgrading	
	R1, R2, R3	R4.01 to R4.03
AFV30, AFV40 (FFCS-V)	-	X
CAL Process Alarm Notification	-	○
Change to PRD Mode in CAL	-	○

○: Offline download is required for FCS.

X: Offline download is required for FCS after new FCS is created and all existing engineering data items are imported. In addition, the FCS hardware needs to be replaced.

-: Not applicable

■ Display of Customizable Faceplate

In CENTUM VP R5.01.00, for improving the graphic performances, the graphic file format is changed from R4. Consequently, if the customizable faceplates were used in the existing project, after upgrading to R5.01.00, the following command needs to be executed using Windows Explorer in the HIS to upgrade the customizable faceplate files. You can copy the following path to the HIS and double click it. Without running this command, the previous version customizable faceplates cannot be displayed on R5.01.00 HIS.

<Program Files Folder (usually "C:\Program Files")>\YOKOGAWA\IA\iPCS\Products\CENTUMVP\Program\Yokogawa.IA.iPCS.CENTUMVP.HIS.Graphic.CustomFaceplateUpdtTool.exe

■ Colors of Graphic View Margins

In the previous versions, the colors of top, bottom, left and right margins of graphic view are all white. From R5.01.00, the margins will be displayed in the same color of the canvas.

However, you can revert to display the margins in white by running the following command using Windows Explorer.

- 32bit OS (Windows Vista, Windows Server 2008)
<CENTUM VP Installed Folder>\his\tool\SetCanvasSpaceColorWhite.reg
- 64bit OS (Windows 7, Windows Server 2008 R2)
<CENTUM VP install folder>\his\tool\SetCanvasSpaceColorWhite_64bit.reg

You can revert again to display the margins in canvas color by running the following command:

- 32bit OS (Windows Vista, Windows Server 2008)
<CENTUM VP install folder>\his\tool\ResetCanvasSpaceColorWhite.reg
- 64bit OS (Windows 7, Windows Server 2008 R2)
<CENTUM VP install folder>\his\tool\ResetCanvasSpaceColorWhite_64bit.reg

■ Graphic Font and Text Width

When upgrading Windows operating environment from XP to Vista or Windows 7, the width of the texts may be different under the following circumstances:

- When the specified font does not exist
Example: Meiryo
- When Latin font texts are displayed in Japanese environment
Example: Courier New
- When displaying alphabets with proportional fonts
Example: Arial, Times New Roman

You can adjust the width by changing fonts or changing texts.

■ Adjust Height of Windows Taskbar to Suit Graphic Builder Canvas

Windows 7 taskbar is 10 dots higher than the taskbar of Windows XP and Vista. Therefore, if the taskbar is always displayed on the HIS desktop, the displaying area for graphic views and other HIS windows becomes smaller and a vertical scrollbar is displayed.

In this case, change the Windows 7 taskbar to a smaller height or automatically hide the taskbar.

■ Check Actions of .NET Controls and ActiveX Controls

If the Windows operating system is changed to Windows Vista or Windows 7, you need to confirm the actions of the user-defined .NET controls and ActiveX controls.

■ Display Online Manuals

Only one session is allowed for displaying the online manuals.

If you try to display the online manuals through multiple sessions with remote operation and monitoring server, a dialog box will be prompted warning that only one session is allowed. Make sure that no other session is used for displaying the online manuals.

■ Touch Targets of Graphic Views

In CENTUM VP R4 and R5, behavior of touch targets differs when they are placed on the following controls:

- Touch target

- Instrument faceplate control
- User control (ActiveX control, Windows form control)

In R4, while the function condition of the touch target placed on the above-mentioned control is not met, the function assigned to the control is executed on meeting the function condition set for it. In R5, while the function condition of the touch target placed on the above-mentioned control is not met, the function assigned to the control is not executed even if the function condition set for it is met.

Use the Touch Target Check Tool to find such overlapping touch targets and correct the graphic file.

● Detecting Overlapping Touch Targets

1. Run the following file to start the Touch Target Check Tool.

<ProgramFiles folder>\YOKOGAWA\IA\iPCS\Products\CENTUMVP\Program\Yokogawa.IA.iPCS.CENTUMVP.ENG.UTY.TouchTargetCheckTool.exe

2. Click [Browse] and select the top folder of the project database.

3. Click [Check] to start detection.

After the checking is completed, a dialog box appears, showing the results of detection. If overlapping touch targets are found, a summary of the check and links to the detailed information are displayed in the dialog box.

- Summary of detection results

<CENTUM VP installation folder>\eng\Temp\Window\TouchTargetCheckTool\TouchTargetCheckSummary_yyyyMMdd_HHmmss.csv

yyyyMMdd: Year, month, and date

HHmmss: Hour, minute, and second

The following information is output:

- Path name of the graphic file (.edf)
- Success/failure of the check
- Number of detected touch targets
- Error message (if the check ended up in an error)
- Details of detection results

<CENTUM VP installation folder>\eng\Temp\Window\TouchTargetCheckTool\TouchTargetCheckDetails_yyyyMMdd_HHmmss.csv

yyyyMMdd: Year, month, and date

HHmmss: Hour, minute, and second

The following information is output:

- Path name of the graphic file (.edf)
- Object name of the touch target
- Coordinates
- Group name (if the touch target is contained in a grouped object)

4. Confirm the touch targets referring to the result of detection and correct the graphic file.

C11.7 Upgrading to R5.01.10

To use the new functions added in R5.01.10 after upgrading from CENTUM VP R5.01.00 to R5.01.10, special tasks may be required depending on the function you want to use.

The cautions mentioned below apply to when upgrading from R5.01.00 to R5.01.10.

If you are upgrading from a revision earlier than R5.01.00 to R5.01.10, also read the cautions for upgrading between revisions described in earlier sections.

■ Master Recipe Download

After the system upgrade, execute Download or Master Download from the Recipe View to download master recipes. If not executed, the tree view hierarchy will not be displayed in the Recipe Selection dialog box.

To download master recipes, select [Download] or [Master Download] from the [Load] menu in the Recipe View.

C11.8 Upgrading to R5.02.00

To use the new functions added in R5.02.00 after upgrading from CENTUM VP R5.01.20 to R5.02.00, special tasks may be required depending on the function you want to use.

The cautions mentioned below apply to when upgrading from R5.01.20 to R5.02.00.

If you are upgrading from a revision earlier than R5.01.20 to R5.02.00, also read the cautions for upgrading between revisions described in earlier sections.

■ Upgrading the Server for Remote Operation and Monitoring Function

If the server for remote operation and monitoring function of CENTUM VP earlier than R5.02.00 is used on Windows Server 2008 and also a license for connecting eight sessions is used, make sure that the required size of virtual memory is available on the computer.

If the required size of virtual memory is not ensured, operation and monitoring from the remote computer may be disabled due to lack of memory.

**SEE
ALSO**

For more information about the required virtual memory size, refer to:

“■ Procedure 2: Set Up Windows” on page B5-20

■ Vnet/IP Bus Status

If the Vnet/IP firmware revision is Rev.13 or later, the Vnet/IP bus status displayed during bus errors only indicates the bus errors of the HISs that belong to the domain where bus errors have occurred. It does not indicate the bus communication status of other domains.

C11.9 Upgrading to R5.03.00

To use the new functions added in R5.03.00 after upgrading from CENTUM VP R5.02.00 to R5.03.00, special tasks may be required depending on the function you want to use.

The cautions mentioned below apply to when upgrading from R5.02.00 to R5.03.00.

If you are upgrading from a revision earlier than R5.02.00 to R5.03.00, also read the cautions for upgrading between revisions described in earlier sections.

■ Unified Gateway Station (UGS)

Cautions related to UGS are as follows:

- **Create Account on the OPC Server Computer**

When connecting UGS of R5.03.00 to an OPC DA server or OPC A&E server, create the UGS_PROCESS user account on the OPC server computer.

**SEE
ALSO**

For more information about connecting UGS to an OPC DA server or OPC A&E server, refer to:

“■ Configuring security settings for connecting to an OPC DA server or OPC A&E server” in D2.4, “Building a non-redundant UGS” in Unified Gateway Station Reference (IM 33J20C10-01EN)

- **Download Taglist to HIS**

After upgrading to R5.03.00, download the taglists of all UGSs to HIS.

■ Update Device Drivers

When upgrading CENTUM VP to R5.03.00, update device drivers such as the control bus driver and Vnet/IP open communication driver.

**SEE
ALSO**

For more information about how to update the device drivers, refer to:

“■ Update Device Drivers” on page C6-32

■ Upgrading of FCS

If you are not using the new functions added in R5.03.00, you can complete the FCS version upgrade simply through an offline download to the FCS from the upgraded system builder function. Even if the offline download cannot be performed, the following functions will still be available if included in the functions of the version before the upgrade.

- Online maintenance and save tuning parameters functions using the system builder function upgraded to R5.03.00
- Operation and monitoring function upgraded to R5.03.00

- **Using the New Functions Added in R5.03.00**

To use the new functions added in R5.03.00, you need to perform the tasks shown in the following table.

Table C11.9-1 New Functions and Required Tasks

Function	Upgrade system builder function	Re-create FCS and import existing engineering data	Offline download to FCS	Upgrade operation and monitoring function	Download the project common section to all HISs
Test function supporting high-speed scan	Yes	No	No	No	No
Function block writes to output module during OOP	Yes	No	Yes	No	No
Function block tracks output module during OOP	Yes	No	Yes	Yes	No
Prohibit setting SV to a value beyond the range of SVL and SVH	Yes	No	No	No	Yes
Pass calculation block's input QST status to CPV	Yes	No	Yes	No	No
Output limiter in PRD mode	Yes	No	Yes	No	No
Apply same permission level of PV to CPV	Yes	No	No	No	Yes
Subsystem communication function How to switch dual redundancy I/O module status display in the node status display dialog box	Yes	No	Yes	No	No
Unit instrument with recipe operation Unit operation instrument	Yes	Yes	Yes	Yes	Yes
ALP121	Yes	Yes	Yes	No	No

● Apply same permission level of PV to CPV

In CENTUM VP R5.03, this option was added to the Detailed Settings tab of the Create New Project dialog box.

The default setting of this option differs, depending on whether the project was created with R5.03 or a later version or the project was updated from an existing project. If you want to implement the same behavior between projects in multiple project connection, change this setting as necessary.

SEE ALSO

For more information about the details of this option, refer to:

- “● Apply same permission level of PV to CPV” in “■ Detailed Setting of Project” in 2.2, “Creating a New Project” in Engineering Reference Vol.1 (IM 33J10D10-01EN)

● Output tracking of function block in the OOP status

In CENTUM VP R5.03, this option was added to the Detailed Settings tab of the FCS Constants builder.

The default setting of this option differs, depending on whether the FCS was created with the system builder of R5.03 or later or with the system builder of a version earlier than R5.03. If you want to implement the same behavior between FCSs, change this setting as necessary.

SEE ALSO

For more information about the details of this option, refer to:

- “■ Function block tracks output module during OOP” in 2.10, “Function block tracks output module during OOP : FFCS Series/KFCS2/LFCS2/RFC5” in Engineering Reference Vol.1 (IM 33J10D10-01EN)

■ CENTUM Data Access Library

If you are using user application that was created by using the CENTUM data access library of a revision earlier than CENTUM VP R5.03, migration is required.

● Migration of User Applications Created by VB6

The user applications created by VB6 cannot be used in the CENTUM Data Access Library environment newer than R5.03. For using the user applications created by VB6 in the CENTUM Data Access Library environment newer than R5.03, you need to use VB.NET to migrate the VB6 applications.

The detailed procedure to use VB.NET to migrate the applications created by VB6 varies for different user applications. The details will not be explained in this document.

● Migration of User Applications Created with VB.NET

On a computer for development, follow these steps to migrate the user application:

1. Cancel references to the CENTUM data access library of a version earlier than R5.03.
2. Set up the CENTUM data access library of R5.03 or newer.
3. Reassign the CENTUM data access library of R5.03 or newer.

The details of each procedure are described below.

● Releasing references to the CENTUM data access library prior to R5.03

The procedure is the same as the procedure for migration to an R6.06 or newer environment.

SEE ALSO

For more information about the procedure to cancel references to the CENTUM data access library of a version earlier than R5.03, refer to:

“• Releasing references to the CENTUM data access library prior to R5.03” in “■ Migration of User Applications Created by VB.NET” in 2.8.1, “Migrating user applications created prior to R5.03 into an environment of R6.06 or newer” in CENTUM Data Access Library (IM 33J05F10-01EN)

● Setting up the CENTUM data access library of R5.03 or newer

IMPORTANT

Once this work is performed, references to the CENTUM data access library prior to R5.03 can no longer be released.

Be sure to perform this work after releasing references.

If development work is being performed on a HIS, upgrade the revision of the CENTUM VP system to R5.03 or newer.

If development work is being performed on a computer that does not function as an HIS, set up a library of R5.03 or newer.

SEE ALSO

For more information about CENTUM VP system upgrading on HIS, refer to:

C6., “Upgrading the System” on page C6-1

For more information about setting up the CENTUM data access library on a computer other than HIS, refer to:

2.1, “Setting up the CENTUM Data Access Library in a Computer that is Not an HIS” in CENTUM Data Access Library (IM 33J05F10-01EN)

- **Reassigning the CENTUM data access library of R5.03 or newer**

1. Assign the new CENTUM data access library controls to the form.
2. Change the names of the controls of the CENTUM data access library to the names that have been written down in "● Releasing references to the CENTUM data access library prior to R5.03."
3. Change the properties of the controls of the CENTUM data access libraries to the property values that have been written down in "● Releasing references to the CENTUM data access library prior to R5.03."
4. When using the following events, you need to reassign the events.
 - MsgEvent event
 - ShutdownEvent event
5. On the Solution Explorer, click the target project.
6. On the [Build] menu of the targeted project, click [Rebuild].
Rebuild will be executed.

SEE

For more information about MsgEvent event, refer to:

“■ MsgEvent Event” in 3.3.1, “Alarms and Messages Notification” in CENTUM Data Access Library (IM 33J05F10-01EN)

For more information about ShutdownEvent event, refer to:

“■ ShutdownEvent Event” in 3.3.2, “HIS Shutdown Notification” in CENTUM Data Access Library (IM 33J05F10-01EN)

C11.10 Upgrading to R5.03.20

To use the new functions added in R5.03.20 after upgrading from CENTUM VP R5.03.00 to R5.03.20, special tasks may be required depending on the function you want to use.

The cautions mentioned below apply to when upgrading from R5.03.00 to R5.03.20.

If you are upgrading from a revision earlier than R5.03.00 to R5.03.20, also read the cautions for upgrading between revisions described in earlier sections.

■ Downloading Database to Computers in the Project

After you have upgraded to R5.03.20, use System View to download the project common section to each computer in the project.

After the downloading is complete, restart the computer.

■ Message Monitor of CAMS for HIS

The following items of the Message Monitor of CAMS for HIS are changed by this upgrading.

Table C11.10-1 Changed Items

Item	R5.03.20	Earlier than R5.03.20	Remarks
Number of messages that can be shelved by One-Shot Shelving	100 messages per user	No limitation	If you attempt to shelve messages exceeding the maximum number, an operation error message is displayed. If messages have already been shelved exceeding the maximum number before upgrading, the excess messages are deleted from the shelf when upgrading.
Number of alarm sources that can be shelved by Continuous Shelving	100 alarm sources per user	No limitation	If you attempt to shelve alarm sources exceeding the maximum number, an operation error message is displayed. If alarm sources have already been shelved exceeding the maximum number before upgrading, the excess alarm sources are deleted from the shelf when upgrading.

■ Changes in Alarm Suppressing Functions when CAMS for HIS is Used

The behaviors when Suppression is executed or alarms are suppressed in AOF mode are changed.

SEE ALSO

For more information about the changed behaviors, refer to:

- Actions of an HIS when Process Alarm Messages are Suppressed" in A6.1, "How the Result of Message Processing in the Message Monitor of CAMS for HIS is Displayed in Other Operation and Monitoring Windows" in Consolidated Alarm Management Software Reference (IM 33J05A21-01EN)

■ When Multiple Projects are Connected

When multiple projects are connected, if the lower project is a revision earlier than R5.03.20, the alarm engineering information cannot be shared. In this case, define the alarm engineering information of the lower project in the OtherProject node of the upper project.

**SEE
ALSO**

For more information about the task when the CENTUM software of the lower project is a version earlier than R5.03.20, refer to:

- “■ When the Lower Project Consists of CENTUM Software Earlier than R5.03.20” in A7.1, “Project Connection Patterns when CAMS for HIS is Enabled” in Consolidated Alarm Management Software Reference (IM 33J05A21-01EN)

C11.11 Upgrading to R5.04.00

To use the new functions added in R5.04.00 after upgrading from CENTUM VP R5.03.20 to R5.04.00, special tasks may be required depending on the function you want to use.

The cautions mentioned below apply to when upgrading from R5.03.20 to R5.04.00.

If you are upgrading from a revision earlier than R5.03.20 to R5.04.00, also read the cautions for upgrading between revisions described in earlier sections.

■ Upgrading of FCS

If you are not using the new functions added in R5.04.00, you can complete the FCS version upgrade simply through an offline download to the FCS from the upgraded system builder function. Even if the offline download cannot be performed, the following functions will still be available if included in the functions of the version before the upgrade.

- Online maintenance and save tuning parameters functions using the system builder function upgraded to R5.04.00
- Operation and monitoring function upgraded to R5.04.00

● Using the New Functions Added in R5.04.00

To use the new functions added in R5.04.00, you need to perform the tasks shown in the following table.

Table C11.11-1 New Functions and Required Tasks

Function	Upgrade system builder function	Re-create FCS and import existing engineering data	Offline download to FCS	Upgrade operation and monitoring function	Download the project common section to all HISs
Delayed process alarm detection	Yes	No	Yes	No	No
Reactions process input error on terminals except for IN terminal	Yes	No	Yes	No	No
Reactions at DI module failure	Yes	No	Yes	No	No

■ Coexistence with Sequence of Event Recorder (SOE)

SOE viewer, SOE server configurator, and SOE server of R5.03.20 or earlier cannot exist with SOE viewer, SOE server configurator, and SOE server of the revision of R5.04.00 or later in the same project. In such a case, upgrade products of R5.03.20 or earlier to those of R5.04.00 or later.

C11.12 Upgrading to R5.04.20

To use the new functions added in R5.04.20 after upgrading from CENTUM VP R5.04.00 to R5.04.20, special tasks may be required depending on the function you want to use.

If you are upgrading from a revision earlier than R5.04.00 to R5.04.20, also read the cautions for upgrading between revisions described in earlier sections.

■ Re-creating Logic Chart Status Display Files

If the version of your system before upgrading was R5.02.00 to R5.04.00, you must re-create the status display files for control drawings containing LC64-E. Otherwise, signal lines may be displayed in wrong colors in logic chart views.

● Procedure for Re-creating Logic Chart Status Display Files

In this task, you handle control drawing files containing LC64-E:

1. From System View, select [Tools] > [Search by Name].
The name search tool starts.
2. Enter "LC64-E" as the block name and run the search.
The control drawing files containing LC64-E are displayed in the result list.
3. Select one of the control drawing files and click the [Start Builder] button.
The control drawing builder opens.
4. In the control drawing builder, click the [Create Working File] button on the toolbar.
5. Close the control drawing builder.
6. Repeat steps 3 to 5 for all the control drawing files containing LC64-E blocks.
7. From System View, select [FCS] > [All Generation].
The All Generation dialog box appears.
8. The working files that you created in step 4 are displayed in the dialog box. Click the [Select All] button to select the files for generation and click [Start].
The status display files are re-created.

TIP

- Re-creation of status display files updates the engineering database, and thus you need to perform this task on only one HIS or computer where system builders are installed. You do not need to perform it on any other stations.
- If you perform only the re-creation of status display files, tuning parameter saving is not required.

C11.13 Upgrading to R6.01.00

To use the new functions added in R6.01 after upgrading from CENTUM VP R5.04.20 to R6.01, special tasks may be required depending on the function you want to use.

The cautions mentioned below apply to when upgrading from R5.04.20 to R6.01.

If you are upgrading from a revision prior to R5.04.20 to R6.01, be sure to read the cautions for revision up between revisions described in earlier sections.

■ Recovery messages when Suppresion is applied

From CENTUM VP R6.01, You can specify displaying or not displaying recovery messages when Suppression is applied by CAMS for HIS. If you change the settings, perform download-ing the project common section to all HISs in the project.

The following table shows the default behaviors when you newly create a project and when you upgrade the project from old revisions. When you upgrade the project, you do not need to set the recovery message behavior anew because the behavior before the upgrade is inher-ited.

Table C11.13-1 Default behaviors of displaying recovery messages

Project's condition	Default behavior
Newly created	Displays recovery messages
Upgraded from R5.03.00 or earlier	Displays recovery messages
Upgraded from R5.03.20 or later	Displays no recovery messages

C11.14 Upgrading to R6.01.10

To use the new functions added in R6.01.10 after upgrading from CENTUM VP R6.01.00 to R6.01.10, special tasks may be required depending on the function you want to use.

The cautions mentioned below apply to when upgrading from R6.01.00 to R6.01.10.

If you are upgrading from a revision earlier than R6.01.00 to R6.01.10, also read the cautions for upgrading between revisions described in earlier sections.

■ Precautions about the tasks after upgrading the system

After you have upgraded the system, you must register the existing VP project in an AD project in order to enable history management of the VP project. The registration may take a few tens of minutes. You cannot edit the VP project while it is being registered.

C11.15 Upgrading to R6.02.00

To use the new functions added in R6.02.00 after upgrading from CENTUM VP R6.01.10 to R6.02.00, special tasks may be required depending on the function you want to use.

The cautions that are described in this section apply to when upgrading from R6.01.10 to R6.02.00.

If you are upgrading from a revision earlier than R6.01.10 to R6.02.00, also read the cautions for upgrading between revisions described in earlier sections.

■ Operation and Monitoring Function

Cautions related to the operation and monitoring function are described as follows:

- **Precaution when upgrading HIS**

After upgrading HIS from R6.01.10 or an earlier version to R6.02, select the HIS in System View and run the Download to HIS command.

- **Trend Block Expansion**

All HISs within each project must be installed with R6.02.00, except for CS 3000 HIS.

On any HIS installed with R6.01.10 or an earlier revision, do not select the "Expand Number of Trend Blocks (R6.02.00 or Later)" check box on the Detailed Settings tab of HIS properties.

- **Trend controls in graphic views**

From CENTUM VP R6.02.00, trend data that is collected by other HIS (other station trend) can be displayed through trend controls in graphic views.

With this enhancement, the trend point display of a trend control may change from local station trend to other station trend after upgrading to R6.02.00.

If this happens, you must be careful because the display will change as follows although the trend of the same process data is displayed:

- The trend sampling period changes.
- The trend is not displayed when the HIS that is referenced for other station trend is stopped.

This problem occurs if both of the following conditions are met for certain process data:

- The sampling period that is set for the trend control does not match the sampling period in local station trend.
- The sampling period that is set for the trend control matches the sampling period in other station trend.

To restore the trend control display, change the sampling period setting of the trend control to a value that is defined for the process data of the local station trend.

■ CAMS for HIS

Cautions related to CAMS for HIS are as follows:

- **Notes on Revision Upgrade of HIS**

Take note of the following points when upgrading the HIS to a later revision.

- Downloading the project common section

After upgrading the HIS from R6.01.10 or earlier revision to R6.02, download the project common section to the HIS in System View.

- Customizing the toolbar of the CAMS for HIS Message Monitor
Upgrading the HIS from R6.01.10 or earlier revision to R6.02 adds the [Suppression List Window] button and [Shelving List Window] button to the toolbar.
If the toolbar was already customized in R6.01.10 or earlier, these two buttons are added in the rightmost position while the current customization settings are maintained. If you do not need these buttons, delete them by using the toolbar customization function after the revision upgrade.

SEE ALSO

For more information about customizing the toolbar, refer to:

“■ Items Set in the Toolbar Tab” in B1.4.3, “Operations by the Operator to Customize the Message Monitor of CAMS for HIS” in Consolidated Alarm Management Software Reference (IM 33J05A21-01EN)

● Notes When HISs of Different Revisions Exist

HIS revision upgrade requires that all HISs in the same VP project are upgraded. However, the VP project may involve HISs of differ revisions before the entire revision upgrade process is complete.

In this case, take note of the following points if the CAMS for HIS Message Monitor must be customized.

- Download master
The download master must be an HIS installed with R6.02. If an HIS installed with R6.01.10 or earlier is used as the download master, the customized settings of the CAMS for HIS Message Monitor that were configured by using CAMS for HIS Configurator will not be reflected in the HISs installed with R6.02.

TIP

Also when upgrading to R6.02 or a later revision, make sure that the download master is an HIS installed with the latest revision.

- Customizing the CAMS for HIS Message Monitor
When the CAMS for HIS Message Monitor is to be customized by an operator, the operator should use an HIS installed with R6.02 for the customization and reflection of changes. If an HIS installed with R6.01.10 or an earlier revision is used to perform the customization and reflection of changes, the customized settings will not be reflected in R6.02 HISs.
- Toolbar buttons displayed on R6.01.10 or earlier HIS
The [Suppression List Window] button and [Shelving List Window] button are not displayed on the toolbar on HISs installed with R6.01.10 or earlier.

SEE ALSO

For more information about download master for CAMS for HIS, refer to:

“■ System Configuration when Using CAMS for HIS” in A1., “CAMS for HIS Overview” in Consolidated Alarm Management Software Reference (IM 33J05A21-01EN)

For more information about CAMS for HIS Configurator, refer to:

B1.5, “Configurator of CAMS for HIS” in Consolidated Alarm Management Software Reference (IM 33J05A21-01EN)

For more information about customization of CAMS for HIS Message Monitor by operators, refer to:

B1.4.3, “Operations by the Operator to Customize the Message Monitor of CAMS for HIS” in Consolidated Alarm Management Software Reference (IM 33J05A21-01EN)

● Procedure for Changing the Download Master to an Additional HIS When HISs of Different Revisions Are Used

If you add R6.02 HISs to the scope of equalization where there are only R6.01.10 or earlier HISs, you must change the download master to an R6.02 HIS.

In this case, follow these steps to carry over the customized settings of the CAMS for HIS Message Monitor to the download master installed with R6.02:

1. Add R6.02 HISs to the system and then download the project common section to all HISs.
2. Add the R6.02 HISs to the existing scope of equalization and then restart all HISs. At this time, restart the R6.02 HISs last.

TIP

At this point, the download master should remain an R6.01.10 or earlier HIS.

3. Confirm that the customized settings of the CAMS for HIS Message Monitor have been reflected in the R6.02 HISs.
4. On the download master, which is an R6.01.10 or earlier HIS, cancel the download master setting and set one of the R6.02 HISs as the download master.
5. Restart the HIS whose download master setting was canceled and the HIS set as the new download master.

TIP

Here, the two HISs may be restarted in any order.

6. If necessary, on the download master HIS installed with R6.02, customize the CAMS for HIS Message Monitor and download the customized settings by using the CAMS for HIS Configurator.

SEE ALSO

For more information about setting the equalization scope and download master, refer to:

- “■ Items Set in the CAMS for HIS Tab” in B1.3, “Settings to Enable CAMS for HIS” in Consolidated Alarm Management Software Reference (IM 33J05A21-01EN)

C11.16 Upgrading to R6.03.00

To use the new functions added in R6.03.00 after upgrading from CENTUM VP R6.02.00 to R6.03.00, special tasks may be required depending on the function you want to use.

The cautions that are described in this section apply to when upgrading revision from R6.02.00 to R6.03.00.

If you are upgrading from a revision older than R6.02.00 to R6.03.00, also read the cautions for upgrading between revisions described in earlier sections.

■ Operation and Monitoring Function

Cautions related to the operation and monitoring function are described as follows:

- **FFCS-C Status Display View**

The status display view of FFCS-C that was engineered before CENTUM VP R6.03 does not display the component numbers of the FIO nodes. Follow these steps to display the component numbers:

1. Run offline download for the FCS with the target FIO.
2. In the Node Properties dialog box in System View, enter the component numbers and run online download.

■ CAMS for HIS

Cautions related to CAMS for HIS are as follows:

- **Shelving historical information Default Setting**

When you upgrade the revision of the CENTUM project to R6.03.00, the Shelving historical information check box is selected by default on the CAMS for HIS tab in the Project Properties dialog box.

If you are not using the shelving historical information, clear the check box on the applicable tab after upgrading the revision. Then, download the project common section again for the HISs from the System View.

SEE ALSO

For more information about the Shelving historical information option, refer to:

“■ Shelving historical information” in B1.1, “Alarm Actions and Other Configurations” in Consolidated Alarm Management Software Reference (IM 33J05A21-01EN)

- **Shelving Historical Information of the Project of a Revision Older Than R6.03.00**

Shelving historical information is not added to the A&E messages that are generated in CENTUM projects of a revision older than R6.03.00.

- **Prohibited Characters for Shelf Names**

With CAMS for HIS of a revision R6.03.00 or later, you cannot use some characters for shelf names. Before upgrading the revision, make sure that no prohibited characters are used in shelf names.

If any prohibited characters are used, change the shelf names containing such characters before or after upgrading the revision.

**SEE
ALSO**

For more information about prohibited characters for shelf names, refer to:

- List of CAMS for HIS Shelf Builder Setting Items" in B2.1, "CAMS for HIS Builders Setting Items" in Consolidated Alarm Management Software Reference (IM 33J05A21-01EN)

● **Changing the Shelf Names Before Upgrading to R6.03.00**

Follow these steps to change shelf names before upgrading to R6.03.00 in order to remove the prohibited characters:

1. Start the CAMS for HIS Shelf builder and export shelf names.
An external CSV file is created.
2. Open the CSV file in Microsoft Excel, delete the prohibited characters or replace them with other characters, and save the file.
3. Import the CSV file to the CAMS for HIS Shelf builder.
4. Save the file on the CAMS for HIS Shelf builder.

Proceed to perform the revision upgrade procedure.

**SEE
ALSO**

For more information about the CAMS for HIS Shelf builder, refer to:

- B1.2.5, "CAMS for HIS Shelf Builder" in Consolidated Alarm Management Software Reference (IM 33J05A21-01EN)

For more information about the export steps using the CAMS for HIS builder, refer to:

- Exporting" in ■ General Operations for Configuring Engineering Information" in B1.2.1, "Operations Common to Builders" in Consolidated Alarm Management Software Reference (IM 33J05A21-01EN)

For more information about the import steps using the CAMS for HIS builder, refer to:

- Importing" in ■ General Operations for Configuring Engineering Information" in B1.2.1, "Operations Common to Builders" in Consolidated Alarm Management Software Reference (IM 33J05A21-01EN)

● **Changing the Shelf Names After Upgrading to R6.03.00**

Follow these steps to change shelf names after upgrading to R6.03.00 in order to remove the prohibited characters:

1. Start the CAMS for HIS Shelf builder.
The Messages tab displays warning messages.
2. Change the shelf names that are shown in the warning messages, and save the change.
3. From System View, download the project common section to HISs.

**SEE
ALSO**

For more information about the CAMS for HIS Shelf builder, refer to:

- B1.2.5, "CAMS for HIS Shelf Builder" in Consolidated Alarm Management Software Reference (IM 33J05A21-01EN)

● **Operation History Display Format for Reset Shelving Operations When Different HIS Revisions Coexist**

If HISs of different revisions coexist in the VP project, for example, during a revision upgrade procedure, shelf names may not appear in the operation history of reset shelving operations, depending on the combination of the revisions of the HIS that is to be started and the HIS that is currently running. The following table shows the difference in display format of the operation history of reset shelving operations

Table C11.16-1 Operation History Display Format for Reset Shelving Operations

HIS to be started	HIS that is running		
	R6.03.00	R4.03.00 or later, but older than R6.03.00	Older than R4.03.00
R6.03.00	Shelf name displayed	Shelf name displayed	Shelf name not displayed
Older than R6.03.00	Shelf name not displayed		

■ FCS Functions

Cautions related to FCS are described as follows:

- **Change in the Default Setting of the Output Readback Function of FFCS-C Current Output Channels**

For the channels of I/O module (Model: A2MMM843) in FFCS-C (A2FV50S, A2FV50D) for which the signal type is set to Current Output or Current Output (HART Comm.), if the Detect OOP check box is not selected in the detailed channel settings in the IOM builder, the default setting for the output readback changes from "Yes" (output readback is checked) to "No" (output readback is not checked).

To use the channel without OOP detection and with the output readback check enabled, explicitly set the command ORBE=Yes.

Note that, if "Detect OOP" is selected, ORBE is set to Yes and the output readback check is enabled by default.

The following table shows the default values for ORBE.

Table C11.16-2 Default Values of ORBE

	R6.03	R6.01 and R6.02
When Detect OOP selected	Yes	Yes
When Detect OOP not selected	No	Yes

■ Exaopc

When you upgrade a CENTUM VP system that has connection to Exaopc of a version earlier than R3.74 to R6.03.00, upgrade the Exaopc to R3.75 or later.

If you do not upgrade Exaopc to R3.75 or a later version, the system behavior will be as follows:

TIP

The system that has connection to Exaopc includes the lower-level projects when multiple projects are connected.

- **Exaopc DA Server**

With Exaopc R3.70 to R3.74, data access of the DA server may be affected. For example, if FFCS-R or FFCS-C has been added to the system, the maximum throughput of data access with the DA server may decrease from 4000 item IDs/sec. to 2000 item IDs/sec..

With Exaopc R3.74, the maximum throughput can be fixed to 4,000 item IDs/sec.. For the details, refer to the descriptions of the maximum throughput of data access in the Exaopc IM.

- **Exaopc A&E Server**

The A&E server does not send newly added messages.

For example, the A&E server of Exaopc R3.74 does not send the computer switchover type UGS or FFCS-R related messages that have been added in R6.03.00 and later versions.

C11.17 Upgrading to R6.03.10

To use the new functions added in R6.03.10 after upgrading from CENTUM VP R6.03.00 to R6.03.10, special tasks may be required depending on the function you want to use.

The cautions that are described in this section apply to when upgrading revision from R6.03.00 to R6.03.10.

If you are upgrading from a revision older than R6.03.00 to R6.03.10, also read the cautions for upgrading between revisions described in earlier sections.

■ AD Suite

Cautions related to AD Suite are as follows:

- **Engineering Procedures for When Upgrading the AD Suite**

You do not need to upgrade the AD server data and the revision of VP projects. Only upgrade the revision of the AD projects.

**SEE
ALSO**

For more information about the engineering procedures for when upgrading the AD Suite, refer to:

B2., “How to start engineering after upgrading the CENTUM VP software” in Automation Design Suite Basics (IM 33J10A10-01EN)

■ Computer switchover type UGS

Cautions related to computer switchover type UGS are as follows:

- **Limitations on Network Addresses When Using a Computer Switchover Type UGS**

When using a computer switchover type UGS, there are limitations on network addresses for Ethernet and other networks.

**SEE
ALSO**

For more information about the limitations on network addresses when using a computer switchover type UGS, refer to:

Dual-redundant Platform for Computer Read Me First (IM 30A01A20-01EN)

C11.18 Upgrading to R6.04.00

To use the new functions added in R6.04.00 after upgrading from CENTUM VP R6.03.10 to R6.04.00, special tasks may be required depending on the function you want to use.

The cautions that are described in this section apply to when upgrading revision from R6.03.10 to R6.04.00.

If you are upgrading from a revision older than R6.03.10 to R6.04.00, also read the cautions for upgrading between revisions described in earlier sections.

■ IT security

Precautions related to IT security are described as follows:

- **Setting of IT Security When Upgrading**

Effective from R6.04.00, a setting called "IT Security Version" has been added to let you select IT Security Version 1.0 or IT Security Version 2.0. The IT security settings of R6.03.10 and earlier correspond to IT Security Version 1.0.

If you don't want to change the IT security settings when upgrading, select IT Security Version 1.0. Take note that the default IT security version used when upgrading is 1.0.

■ FCS

Precautions related to FCS are described as follows:

- **Function Block SI-1ALM**

The function block SI-1ALM is a new function added to R6.04.00. The SI-1ALM can be used with FFCS-V, FFCS-C and FFCS-R.

- **Digital I/O Module A2MDV843**

The digital I/O module A2MDV843 is a new hardware added to R6.04.00. The A2MDV843 can be used with FFCS-C and FFCS-R.

- **Adaptors A2SAM105H, A2SAM505H and A2SAT105**

Effective from R6.04.00, the current input/voltage input adaptor A2SAM105H, current output/voltage output adaptor A2SAM505H, and mV/TC/RTD input adaptor A2SAT105 can be used with FFCS-C.

- **Base Plates for Barrier A2BN4D and A2BN5D**

Effective from R6.04.00, the base plates for barrier A2BN4D and A2BN5D can be used with FFCS-R.

- **What You Need to Do to Use the New Function**

To use the new FCS functions in R6.04.00, you must do the following:

Table C11.18-1 What You Need to Do to Use the New Function

Function	Upgrade system builder function	Re-create FCS and import existing engineering data	Offline download to FCS	Upgrade operation and monitoring function	Download the project common section to all HISs
SI-1ALM	Yes	Yes	Yes	No	Yes
A2MDV843	Yes	No	Yes	No	No

Continues on the next page

Table C11.18-1 What You Need to Do to Use the New Function (Table continued)

Function	Upgrade system builder function	Re-create FCS and import existing engineering data	Offline download to FCS	Upgrade operation and monitoring function	Download the project common section to all HISs
A2SAM105H, A2SAM505H, A2SAT105 (*1)	Yes	No	Yes	No	No
A2BN4D, A2BN5D (*2)	Yes	No	Yes	YES (*3)	No

*1: When defined for FFCS-C

*2: When defined for FFCS-R

*3: When the status display of the base plate for barrier is used

■ Access Administrator Package (FDA:21 CFR Part 11 compliant)

Precautions related to the Access Administrator Package (FDA:21 CFR Part 11 compliant) are described as follows:

- **Checking the Storage Location of the Engineers' Account File**

If the engineers' account file, recipe engineers' account file or user security file for Report Package is located immediately under drive C, any attempt made by a user without administrative rights to log on in the CENTUM authentication mode will open an error dialog box.

If the engineers' account file, recipe engineers' account file or user security file for Report Package is located in any of the following folders or in the installation folder of YOKOGAWA product, an error message may appear:

- C:\CENTUMVP
- C:\Program Files (x86)\Yokogawa
- C:\Program Files\Yokogawa
- C:\Common Files\Hilscher
- C:\ProgramData\Yokogawa

Error messages that may appear are as follows:

- Could not acquire the setting of the lockout account.
- Invalid Password Information.

Ask Administrator to be able to access Password Information.

Follow these steps to check the storage location of the engineers' account file, recipe engineers' account file or user security file for Report Package:

1. Log on to Windows as one of the following users:

Table C11.18-2 User Who Can Start the Access Control Utility

Security model	User who can start the utility
Legacy Model	User who belongs to the Administrators group
Standard Model	User who belongs to both the Administrators group and CTM_ENGINEER_ADMIN group User who belongs to both the Administrators group and CTM_ENGI-NEER_ADMIN_LCL group User who belongs to both the Administrators group and CTM_MAINTENACNE group User who belongs to both the Administrators group and CTM_MAINTENACNE_LCL group

2. Start Access Control Utility.

A dialog box appears, prompting you to select the target for audit trail management and access control.

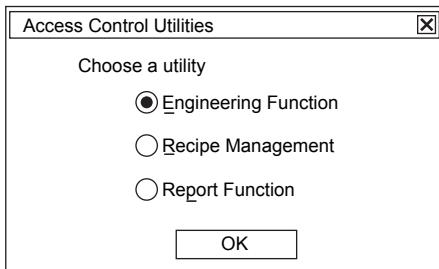


Figure C11.18-1 Dialog Box for Selecting the Target Feature

If the standard engineering function, recipe management package, and report package are all activated on a computer, you can implement different audit trail management and access control for each feature. In this dialog box, specify the feature for which you want to start Access Control Utility.

This dialog box does not appear if only one of the standard builder function, recipe management package, or report package is activated. The Access Control Utility for the package that is activated starts.

If none of these packages is activated, Audit Trail Database Viewer starts.

3. If the dialog box for selecting the target feature appears, select an appropriate radio button according to the file you want to check.
 - To check the storage location of the engineers' account file, select [Engineering Function].
 - To check the storage location of the recipe engineers' account file, select [Recipe Management].
 - To check the storage location of the user security file for Report Package, select [Report Function].
4. Click [OK].
The Access Control Utility appears.
5. Click the Access Control tab.
6. Check the path name to the file being referenced.
7. If the storage location of the file is inappropriate, use Explorer to copy the following files to an appropriate folder:

Table C11.18-3 Name of file to be copied

File to be moved	File name	Name of file to be copied together
Engineers' account file	EngSecurity.sva	EngPassword.odc
Recipe engineers' account file	RcpSecurity.sva	RcpPassword.odc
User security file for Report Package	RptSecurity.sva	RptPassword.odc

8. Change the path name settings in the Access Control Utility accordingly.
9. Click [OK].
The Access Control Utility closes.

● Checking the Top Folder of the Audit Trail Database

If the top folder of the audit trail database, recipe audit trail database, report audit trail database is located in the project folder, an error message will appear when an attempt is made to make a change to the Project Properties in System View, and the change will not be made.

Also, if the top folder of the audit trail database, recipe audit trail database or report audit trail database is located in any of the following folders or in the installation folder of YOKOGAWA product, an error message may appear:

- C:\CENTUMVP
- C:\Program Files (x86)\Yokogawa
- C:\Program Files\Yokogawa
- C:\Common Files\Hilscher
- C:\ProgramData\Yokogawa

Error messages that may appear are as follows:

- Audit Trail Database of the following project is invalid.
<Project name>
Access denied. err =0x5
Ask Administrator to be able to access Audit Trail Database.
- Cannot create file(FDA DB Connection File)
Ask Administrator to be able to access Audit Trail Database.
- Failed to record Audit Log.
Access denied. err =0x5

Follow these steps to check the top folder of the audit trail database, recipe audit trail database or report audit trail database:

1. Log on to Windows as one of the following users:

Table C11.18-4 User Who Can Start the Access Control Utility

Security model	User who can start the utility
Legacy Model	User who belongs to the Administrators group
Standard Model	User who belongs to both the Administrators group and CTM_ENGINEER_ADMIN group User who belongs to both the Administrators group and CTM_ENGI-NEER_ADMIN_LCL group User who belongs to both the Administrators group and CTM_MAINTENACNE group User who belongs to both the Administrators group and CTM_MAINTENACNE_LCL group

2. Start Access Control Utility.

A dialog box appears, prompting you to select the target for audit trail management and access control.

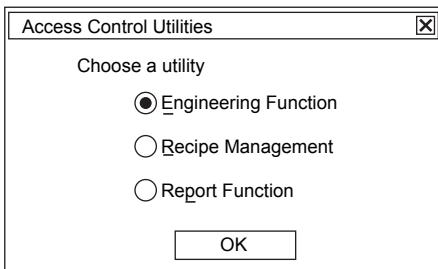


Figure C11.18-2 Dialog Box for Selecting the Target Feature

If the standard engineering function, recipe management package, and report package are all activated on a computer, you can implement different audit trail management and access control for each feature. In this dialog box, specify the feature for which you want to start Access Control Utility.

This dialog box does not appear if only one of the standard builder function, recipe management package, or report package is activated. The Access Control Utility for the package that is activated starts.

If none of these packages is activated, Audit Trail Database Viewer starts.

3. If the dialog box for selecting the target feature appears, select an appropriate radio button according to the file you want to check.
 - To check the top folder of the audit trail database, select [Engineering Function].
 - To check the top folder of the recipe audit trail database, select [Recipe Management].
 - To check the top folder of the report audit trail database, select [Report Function].
4. Click [OK].
The Access Control Utility appears.
5. Click the Electronic Record tab.
6. Check the folder path displayed in the Audit Trail Database box.
7. If the folder path is inappropriate, use Explorer to copy the top folder and all folders below it to an appropriate folder.
8. Click the [Change] button for the Audit Trail Database in the Access Control Utility, and change the top folder name of the audit trail database.
9. Click [OK].
The Access Control Utility closes.

■ AD Suite

Cautions related to AD Suite are as follows:

- **Formats in Which Module Files Are Saved**

If there are any logic charts (LC-64/LC-64E) using symbols with comment in the existing class modules or application modules and if you perform any one of the following operations on such class modules or application modules by using AD Organizer of R6.04 or later and check them in, the modules become unable to be checked out by AD Organizer of R6.03 or earlier.

- Save on the control drawing builder
- Save after changing the model on the control logic editor

If you perform these operations, the class module or application module is saved in the new file format.

With the class module or application module saved in the new file format, the comments of elements in a logic chart can be edited in the tag list area of the control logic editor.

TIP

Normally, if you select [Editable] for a class module parameter and update the module by using Update Module Manager, the corresponding parameter in the class-based application module remains unchanged.

However, if you update the class-based application module that was created in R6.03 or earlier by using the class module saved in the new format, the comment of elements in the logic chart of the class-based application module will be updated (only for the first update) even if [Editable] is selected for the comment of elements in the logic chart of the class module.

C11.19 Upgrading to R6.05.00

To use the newly added functions of R6.05.00 after upgrading from CENTUM VP R6.04.00 to R6.05.00, specific tasks may be required depending upon the function added.

Observe the cautions described in this section when upgrading from R6.04.00 to R6.05.00.

When upgrading from versions earlier than R6.04.00 to R6.05.00, follow all the cautions given between each upgrade along with the current caution notes.

■ Operation and Monitoring Function

Cautions related to the operation and monitoring function are as follows:

- **Auto Execution of Tag Duplication Check**

In versions earlier than R6.05.00, automatic checking of tag duplication was configured in HIS Setup window. However, in R6.05.00, this setting is no longer available and tag duplication is automatically checked without fail. If a tag name duplication is found, a system alarm message is generated.

TIP

- To identify duplicate tag names, execute the tag duplication check manually from the HIS Setup window.
- The length of the tag names are not automatically checked. To check the length of the tag names, execute the tag duplication check manually from the HIS Setup window.

SEE ALSO

For more information about how to check tag duplication manually, refer to:

- “• Check Duplicated Tag” in “■ Setup Items in the Equalization Tab” in 4.3.8, “Equalize Tab” in Human Interface Stations Reference Vol.1 (IM 33J05A10-01EN)

■ AD Suite

Cautions related to AD Suite are as follows:

- **Precaution When Adding Reference Tag Parameters**

In R6.05.00, you can define parameters for reference tags in class modules and application modules. When you use class modules that were created in R6.04.00 or earlier by handling them with AD Organizer of R6.05.00, note the following precaution:

Class modules created in R6.04.00 or earlier do not include reference tag parameters. Therefore, if you add any parameters to the reference tags of a class-based application module created from such a class module and then update the class-based application module, the reference tag parameters will be lost. So, when using reference tag parameters, you must first add reference tag parameters to the class module and then update the class-based application module.

SEE ALSO

For more information about updating an application module, refer to:

- D2.8, “Edit a class module and then update the class-based application module” in Automation Design Suite Module-based Engineering (IM 33J10A15-01EN)

- **Changes in the Validity Check Items for Drawing Modules**

Please note that the validity check items for drawing modules have been changed to improve the performance.

The validity of drawing modules is automatically checked when performing the following actions:

- When saving a drawing module

- When executing module binding
- When checking in a drawing module

In R6.05.00, validity will be checked for all the items by the time the drawing module is checked in. The items of validity checks that are performed before check-in have been changed.

Therefore, note that the time when problems are detected in the validity check of R6.05.00 differs from that of the versions R6.04.00 or earlier.

And, all the items are included in the validity check which is performed manually with the Validity Check button. Click Validity Check on the tool bar to check the validity of all the items during operation,

■ Batch

Cautions related to the Batch are as follows:

- **Cautions When Adding User-defined Common Blocks**

In R6.05.00, 951 or more user-defined common blocks can be created. As a rule, when creating 951 or more user-defined common blocks, upgrade all the HISs of the related VP projects to R6.05.00.

If this is not possible, make sure to upgrade at least the HIS of batch server station and the HIS with system builders installed to R6.05.00.

Further, when you use Exaopc OPC Interface Package (for HIS) to collect batch data, upgrade the HIS on which the Exaopc OPC Interface Package (for HIS) runs to R6.05.00.

TIP

As a rule, all the HISs of a VP project must be of the same version. Considering that the versions of HIS being different as mentioned above is a temporary phenomenon, upgrade the versions of all HISs to R6.05.00 as planned.

The following tasks are also required to collect batch data through Exaopc OPC Interface Package (for HIS):

1. Reconfiguring the OPC client

If an OPC client program is running on a computer that is different from the HIS on which Exaopc OPC Interface Package (for HIS) is running, reconfigure the OPC client settings on that computer.

2. Rebuilding the CENTUM data access library

If any user programs using the CENTUM data access library are running on a computer that is different from the HIS on which Exaopc OPC Interface Package (for HIS) is running, rebuild the CENTUM data access library on that computer.

- **Example of Upgrade When Adding User-defined Common Blocks**

This section describes about the HIS that requires upgrade and the computer on which tasks are required to be performed when the system configuration is as shown below.

IMPORTANT

As a rule, when you upgrade HIS, you need to upgrade all the HIS of the corresponding VP project. This section describes the computers that must be upgraded as minimum requirements when upgrading all the HISs is not possible. This configuration is considered temporary, and all computers should be upgraded as planned.

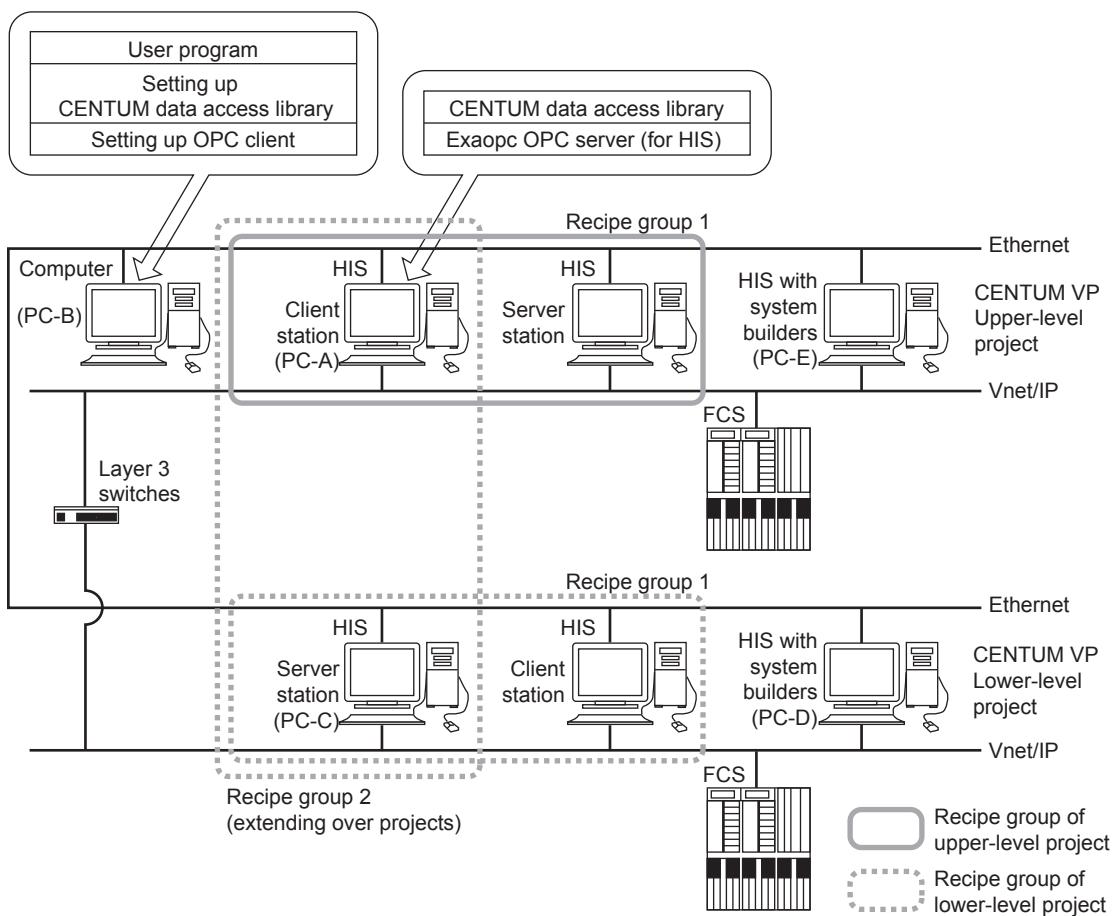


Figure C11.19-1 System Configuration

The details of the configuration shown in the figure is explained below.

- In Recipe group 2 of the lower-level project, the HIS (PC-A) of the upper-level project operates and monitors the recipe of lower-level project.
- The Exaopc OPC Interface Package (for HIS) runs on the HIS (PC-A) of the upper-level project which is specified in the Client station of the lower-level project.
- The user program that uses the CENTUM data access library in the computer (PC-B) connects to the Exaopc OPC Interface Package (for HIS) that runs on HIS (PC-A) and obtains the list of common block names by using the GetRcpBlkList.

The following are the minimum tasks required to be performed if 951 or more user-defined common blocks are created in the lower-level project of this system.

- Upgrade the CENTUM VP batch server station HIS (PC-C) of lower-level project to R6.05.00. At that time, upgrade the HIS with system builders in the lower-level project (PC-D) also to R6.05.00.
 - Upgrade the HIS (PC-A) that is specified in the client station of lower-level project and on which Exaopc OPC Interface Package (for HIS) runs to R6.05.00. At that time, upgrade the HIS with system builders (PC-E) of the upper-level project also to R6.05.00.
 - Re-configure the OPC client settings in the computer (PC-B). After that, rebuild the CENTUM data access library.
- Verifying the Effect on User Programs by using OPC Client Program and CENTUM Data Access Library**

When 951 or more user-defined common blocks are created, verify if the following programs require improvement.

- User program that obtains common block names list with the GetRcpBlkList method of CENTUM data access library.
- OPC Client program that obtains common block names list with BrowseOPCItemIDs method of extended batch server of Exaopc OPC Interface Package (for HIS).

C11.20 Upgrading to R6.06.00

To use the newly added functions of R6.06.00 after upgrading from CENTUM VP R6.05.00 to R6.06.00, specific tasks may be required depending upon the function added.

Observe the cautions described in this section when upgrading from R6.05.00 to R6.06.00.

When upgrading from versions earlier than R6.05.00 to R6.06.00, follow all the cautions given between each upgrade along with the current caution notes.

■ AD Suite

Cautions related to AD Suite are as follows:

- **Precautions Regarding the Behavior of P&ID Groups Defined in the Communication I/O List**

In R6.06.00, the P&ID Group column has been added to the Program Group Definition list and Communication Group Definition list. Since this P&ID Group column is configured as follows during an upgrade to R6.06.00 or later, change the P&ID Group values as necessary.

- If the P&ID group to which the I/O points defined in the Signal Definition list belong has been configured, that P&ID group is set in the P&ID Group column of the Program Group Definition list and Communication Group Definition list.
- If the I/O points that belong to the Program Group Definition list and the Communication Group Definition list are not defined in the Signal Definition list, the P&ID Group column of the Program Group Definition list and Communication Group Definition list will remain blank.
- If I/O points that belong to different P&ID groups share the same program group, the P&ID Group column of the Program Group Definition list and Communication Group Definition list will remain blank.

■ HIS OPC/CENTUM Data Access Library

If there is an HIS running an OPC server in the system and any user applications that communicate with that OPC server are used, you must carry out the following tasks.

The user application stated here refers to applications that use CENTUM data access library.

- **Task to be Performed on an OPC Client of User Application Development Environment**

Follow these steps on a computer for developing user applications using CENTUM data access library. However, you do not need to perform steps 1 and 2 if the development environment is an HIS.

1. Perform the CENTUM VP R6.06.00 client setup procedure.
2. When CENTUM data access library is used, apply the CENTUM data access library of CENTUM VP R6.06.00.
3. Rebuild the user applications that had been used in the system up to CENTUM R6.05 under the Microsoft Visual Studio 2017 development environment. If the user application is a .NET Framework application, specify .NET Framework version 4.6.2.

- **Task to be Performed on an OPC Client of User Application Execution Environment**

Follow these steps on a computer running user applications using CENTUM data access library. However, you do not need to perform steps 1 and 2 if the execution environment is an HIS. If the development environment is also the execution environment, perform only step 3.

1. Perform the CENTUM VP R6.06.00 client setup procedure.
2. When CENTUM data access library is used, apply the CENTUM data access library of CENTUM VP R6.06.00.
3. Replace the user applications using CENTUM data access library that had been used up to CENTUM VP R6.05 with the user applications that were created in the aforementioned “Task to be Performed on an OPC Client of User Application Development Environment.”

- **Upgrading Products When Two or More Upgrade License Support Products are Installed**

When CENTUM VP R6.04 or later and ProSafe-RS R4.03 or later, both of which support upgrade licenses, are installed on the same computer, follow these steps to upgrade them:

1. Distribute the upgrade licenses of the respective coexisting products.
2. Upgrade each product.

C11.21 Upgrading to R6.07.00

To use the newly added functions of R6.07.00 after upgrading from CENTUM VP R6.06.00 to R6.07.00, specific tasks may be required depending upon the function added.

Observe the cautions described in this section when upgrading from R6.06.00 to R6.07.00.

When upgrading from versions earlier than R6.06.00 to R6.07.00, follow all the cautions given between each upgrade along with the current caution notes.

■ PROFINET

When A2LP131 that is a PROFINET communication module is newly defined in the FCS created in R6.06 or earlier, create an FCS again.

SEE ALSO

For more information about hardware requirements for operating A2LP131, refer to:

PROFINET Communication Module (for N-IO/FIO) (GS 33J60G90-01EN)

■ Precautions related to the operation mode of AVR10D

The [Extended Mode] is added to the operation mode, and the [Extended Mode] is set by default when a new project is created. Also, when upgrading from the existing project, the operation mode prior to upgrading will be inherited.

SEE ALSO

For more information about the operation mode of AVR10D, refer to:

“• Operation Mode” in “■ Constant Tab” in 1.3, “Engineering of V net Router” in Communication Devices Reference (IM 33J20B10-01EN)

■ AD Suite

Cautions related to AD Suite are as follows:

● Precautions when engineering the FCS sequence library in AD Suite

When the VP project in which the CENTUM VP software revision is R6.06.00 or earlier is upgraded to R6.07.00 or later, the check box for [Define the SEQ libraries in AD Suite] of the FCS property created in R6.06.00 or earlier is cleared by default. Although the cleared state can be changed to the selected state at any time, it cannot be changed after it has been selected once. When this check box is selected, the FCS sequence library builder started from System View becomes read-only, and the FCS sequence library cannot be edited.

TIP

The check box for [Define the SEQ libraries in AD Suite] of the FCS property created in R6.07.00 or later is selected by default. It can be cleared only when creating a new FCS.

Follow these steps to engineer the FCS sequence library created in R6.06.00 or earlier with the AD suite.

1. In the FCS sequence library builder in System View, select [File] > [Save As] and save the FCS sequence library as a Save as (.sva) file.

TIP

The FCS sequence library builder of System View is a generic term for the following builders.

- FCS Sequence Library Builder (SEBOL User Function)
- FCS Sequence Library Builder (SFC Sequence)
- FCS Sequence Library Builder (Unit Procedure)

2. Select the check box for [Define the SEQ libraries in AD Suite] with the FCS property.

An FCS sequence library deletion confirmation message appears, and the FCS sequence library of this FCS is deleted.

3. Import the FCS sequence library that was saved as the Save as (.sva) file into the AD project.

SEE

For more information about importing the FCS sequence library into the AD project, refer to:

D5.12, "Importing an FCS sequence library" in Automation Design Suite Module-based Engineering (IM 33J10A15-01EN)

For more information about [Define the SEQ libraries in AD Suite] of the FCS property, refer to:

"■ Define the SEQ libraries in AD Suite: FFCS-C/FFCS-V" in 2.4.1, "Creating a New FCS" in Engineering Reference Vol.1 (IM 33J10D10-01EN)

For more information about engineering the FCS sequence library in AD Suite, refer to:

D5., "Engineering the FCS sequence library in AD Organizer" in Automation Design Suite Module-based Engineering (IM 33J10A15-01EN)

D. Connection with Other Products

CENTUM VP can be connected with YOKOGAWA products, such as ProSafe-RS, PRM, and Exaopc.

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.

Blank Page

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 CENTUM VP Security Guide (IM 33J01C30-01EN)

■ 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">• 01: When products are installed and operated on the same computer, and they cannot communicate or share files with each other.• 02: When products are installed and operated on separate computers, and they can communicate or share files with each other.• 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.
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.

IMPORTANT

- You cannot install two products that have integration type 02 on the same computer.
- 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 YOKOGAWA products relevant to the connection with CENTUM.

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
0121	CENTUM VP	Engineering Server Function
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
0205	ProSafe-RS	Engineering Server
0251	ProSafe-RS	SOE Viewer Package
0302	PRM	Plant Resource Manager Server
0401	Exaopc	Exaopc OPC Interface Package
0601	Exapilot	Exapilot Operation Efficiency Improvement Package Server
0651	Exapilot	Exapilot Operation Efficiency Improvement Package Client
0701	Exaplog	Exaplog Event Analysis Package Server
0801	Exaquantum	PIMS Server
0851	Exaquantum	Explorer Client
0951	Exasmoc	Exasmoc Client
1051	Exarqe	Exarqe Client
1551	Multivariable Optimizing Control/Robust Quality Estimation	Multivariable Optimizing Control/Robust Quality Estimation Package Client (APC Client)

*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.

IMPORTANT

When you install CENTUM VP and ProSafe-RS on the same computer, ensure that the software revision of CENTUM VP is R6.06.00 or later and the software revision of ProSafe-RS is R4.04.00 or later.

D1.1.1 CENTUM VP Standard Operation and Monitoring Function and ProSafe-RS SOE Viewer Package

By connecting CENTUM VP Standard Operation and Monitoring Function and ProSafe-RS SOE Viewer Package, you can view historical information of CENTUM VP HIS 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.

Table D1.1.1-1 Connection information

Integration code	0101-0251-03-04		
Product 1	Standard Operation and Monitoring Function of CENTUM VP R5.01 or later (*1)		
Product 2	SOE Viewer Package of ProSafe-RS R3.01 or later (*1)		
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."	

*1: When you install CENTUM VP and ProSafe-RS on the same computer, ensure that the software revision of CENTUM VP is R6.06.00 or later and the software revision of ProSafe-RS is R4.04.00 or later.

● When the Standard model is applied

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.

- When enabling collaboration with products installed on the same computer
Add the user account for using ProSafe-RS SOE Viewer to the CTM_OPERATOR group.
- When enabling collaboration with products installed on different computers
Register the user account for using ProSafe-RS SOE Viewer to the computer where CENTUM VP HIS runs. The user name and password of the user account to be registered must be the same as those of the user account that uses ProSafe-RS SOE Viewer.
Add the registered user account to CTM_OPERATOR group.

SEE ALSO

For more information about how to create user accounts and add them to groups in Domain or Combination management, refer to:

B2.5, "Creating Domain Users" on page B2-16

For more information about how to create user accounts and add them to groups in Standalone management, refer to:

B4.9.1, "When the Standard Model with Standalone Management Security Settings are Applied" on page B4-103

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) of CENTUM VP and SOE OPC Interface Package of ProSafe-RS are installed on the same computer.

If the computer installed with both packages comes under either of the following cases, perform all the procedures explained for each case.

- The computer installed with both packages is designated as the OPC server for OPC communication.
- The computer installed with both packages uses OPC client services.
- In a Domain management or Combination management system, the computer installed with both packages is designated as the OPC server on an OPC client computer that is not a member of the domain.

■ When the computer installed with both packages 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 R5.01 or later		
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 task 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 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:

B2.5, "Creating Domain Users" on page B2-16

For more information about how to create user accounts and add them to groups in Standalone management, refer to:

B4.9.1, "When the Standard Model with Standalone Management Security Settings are Applied" on page B4-103

● 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	User who logged on to Windows
Access Administrator Package (FDA:21 CFR Part 11 compliant)	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 are also included.

■ When the computer installed with both packages 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 R5.01 or later		
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_OPCT and PSF_OPCT 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:

B2.5, "Creating Domain Users" on page B2-16

For more information about how to create user accounts and add them to groups in Standalone management, refer to:

B4.9.1, "When the Standard Model with Standalone Management Security Settings are Applied" on page B4-103

● 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	User who logged on to Windows
Access Administrator Package (FDA:21 CFR Part 11 compliant)	User who logged on to Windows
FCS Data Setting/Acquisition Package (PICOT)	User who logged on to Windows
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 services

*1: Functions created using CENTUM Data Access Library 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 both packages 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 both packages 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	0101-0202-01-03
Product 1	Standard Operation and Monitoring Function of CENTUM VP R5.01 or later (*1)
Product 2	ProSafe-RS SOE OPC Interface Package of ProSafe-RS R3.01 or later (*1)
Security model	Standard model
User management type	Domain/Combination management
Required procedures	Refer to "● Required procedures for connection."

*1: When you install CENTUM VP and ProSafe-RS on the same computer, ensure that the software revision of CENTUM VP is R6.06.00 or later and the software revision of ProSafe-RS is R4.04.00 or later.

● 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:

B4.9.1, "When the Standard Model with Standalone Management Security Settings are Applied" on page B4-103

For more information about how to create user accounts and add them to groups in Domain or Combination management, refer to:

B2.5, "Creating Domain Users" on page B2-16

● 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	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 are also included.

D1.1.3 CENTUM VP System Builder Function and ProSafe-RS CENTUM VP Integration Package

By using ProSafe-RS CENTUM VP Integration 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	0102-0203-03-04		
Product 1	System Builder Function of CENTUM VP R5.01 or later (*1)		
Product 2	CENTUM VP Integration Package of ProSafe-RS R3.01 or later (*1)		
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."	

*1: When you install CENTUM VP and ProSafe-RS on the same computer, ensure that the software revision of CENTUM VP is R6.06.00 or later and the software revision of ProSafe-RS is R4.04.00 or later.

● 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:

B2.5, "Creating Domain Users" on page B2-16

For more information about how to create user accounts and add them to groups in Standalone management, refer to:

B4.9.1, "When the Standard Model with Standalone Management Security Settings are Applied" on page B4-103

D1.1.4 CENTUM VP System Builder Function and ProSafe-RS Safety System Engineering and Maintenance Function

By connecting CENTUM VP System Builder Function and ProSafe-RS Safety System Engineering and Maintenance Function, 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	0102-0201-03-04		
Product 1	System Builder Function of CENTUM VP R5.01 or later (*1)		
Product 2	Safety System Engineering and Maintenance Function of ProSafe-RS R3.01 or later (*1)		
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."	

*1: When you install CENTUM VP and ProSafe-RS on the same computer, ensure that the software revision of CENTUM VP is R6.06.00 or later and the software revision of ProSafe-RS is R4.04.00 or later.

- **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 Standalone management, refer to:

B4.9.1, "When the Standard Model with Standalone Management Security Settings are Applied" on page B4-103

For more information about how to create user accounts and add them to groups in Domain or Combination management, refer to:

B2.5, "Creating Domain Users" on page B2-16

D1.1.5 CENTUM VP Engineering Server Function and ProSafe-RS Safety System Engineering and Maintenance Function

When the CENTUM VP engineering server function and ProSafe-RS safety system engineering and maintenance function are connected, the AD Suite client function and server function work in collaboration so that I/O list engineering and change management function can be used.

■ Performing engineering and maintenance of a ProSafe-RS safety system by using a CENTUM VP engineering server

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

Table D1.1.5-1 Connection information

Integration code	0121-0201-03-02		
Product 1	Engineering Server Function of CENTUM VP R6.02 or later (*1)		
Product 2	Safety System Engineering and Maintenance Function of ProSafe-RS R4.01 or later (*1)		
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 "● When the Standard model is applied."	

*1: When you install CENTUM VP and ProSafe-RS on the same computer, ensure that the software revision of CENTUM VP is R6.06.00 or later and the software revision of ProSafe-RS is R4.04.00 or later.

● When the Legacy model is applied

On the AD Suite client computer and AD Suite server computer, create Windows users who use this function.

Use the ADS Administration Tool to register the Windows users to the engineering server.

● When the Standard model is applied

On the AD Suite client computer and AD Suite server computer, create Windows users who use this function.

Add the user accounts to the CTM_ENGINEER and PSF_ENGINEER groups. For Standalone management, perform this setting task on the computer where the CENTUM VP engineering server is used and also on the computer where the ProSafe-RS safety system engineering and maintenance function is used.

For Domain or Combination management, perform this setting task on the domain controller.

Use the ADS Administration Tool to register the Windows users to the engineering server.

D1.1.6 CENTUM VP System Builder Function and ProSafe-RS Engineering Server Function

When the CENTUM VP system generation function and ProSafe-RS engineering server function are connected, the AD Suite client function and server function work in collaboration so that the module-based engineering and change management function can be used.

■ Generating a CENTUM VP system using a ProSafe-RS engineering server

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

Table D1.1.6-1 Connection information

Integration code	0205-0102-03-02		
Product 1	Engineering Server Function of ProSafe-RS R4.01 or later (*1)		
Product 2	System Builder Function of CENTUM VP R6.02 or later (*1)		
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 "● When the Standard model is applied."	

*1: When you install CENTUM VP and ProSafe-RS on the same computer, ensure that the software revision of CENTUM VP is R6.06.00 or later and the software revision of ProSafe-RS is R4.04.00 or later.

● When the Legacy model is applied

On the AD Suite client computer and AD Suite server computer, create Windows users who use this function.

Use the ADS Administration Tool to register the Windows users to the engineering server.

● When the Standard model is applied

On the AD Suite client computer and AD Suite server computer, create Windows users who use this function.

Add the user accounts to the CTM_ENGINEER and PSF_ENGINEER groups. For Standalone management, perform this setting task on the computer where the CENTUM VP system builder function is used and also on the computer where the ProSafe-RS engineering server function is used.

For Domain or Combination management, perform this setting task on the domain controller.

Use the ADS Administration Tool to register the Windows users to the engineering server.

D1.2 CENTUM VP and PRM

This section describes the settings when connecting CENTUM VP and PRM.

D1.2.1 CENTUM VP Standard Operation and Monitoring Function and PRM Server

Connecting CENTUM VP Standard Operation and Monitoring Function and PRM Server enables PRM to retrieve messages from CENTUM VP.

Exaopc OPC Interface Package (for HIS) is required on the CENTUM VP computer.

■ Enabling PRM to retrieve messages from CENTUM VP R5 or later

The following table shows the connection information. The required procedures of connecting the products are provided after the table.

Table D1.2.1-1 Connection information

Integration code	0101-0302-02-03		
Product 1	Standard Operation and Monitoring Function of CENTUM VP R5.01 or later (*1)		
Product 2	Plant Resource Manager Server of PRM R3.30 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 on the CENTUM VP R5.01 or later computer."	Refer to "● When the Standard model is applied on the CENTUM VP R5.01 or later computer."	

*1: Exaopc OPC Interface Package (for HIS) is an optional function of CENTUM VP Standard Operation and Monitoring Function.

- **When the Legacy model is applied on the CENTUM VP R5.01 or later computer**

On the computer running CENTUM VP, you must use the CreateInternalUserAccount utility to create the PRMUSER account. The utility is included in the PRM installation medium.

Follow these steps to create the PRMUSER account:

1. Log on as a user with administrative rights.
2. Insert the PRM installation medium into the DVD drive.
3. Open the Command Prompt window and run the following command:
`<DVD drive>:\PRM\SecuritySettingUtility\CreateInternalUserAccount.exe -sm legacy`

The PRMUSER account is created.
4. Start HIS Utility.
5. Click the [OPC] tab.
6. In the Set logon options for connecting OPC server section, click [Change].
The Select Logon Type dialog box appears.
7. Select [Automatically logon the designated user for connecting OPC server].
8. Select [Designated user] or [Default user of R4.03 and earlier versions].
9. Click [OK].

SEE ALSO

For more information about the procedure for selecting the logon type on the OPC tab of HIS Utility, refer to:

“■ HIS Utility” in 1.2, “Engineering Related to OPC” in Optional Functions Reference (IM 33J05H10-01EN)

- **When the Standard model is applied on the CENTUM VP R5.01 or later computer**

On the computer running CENTUM VP, you must use the CreateInternalUserAccount utility to create the PRM_PROCESS and PRM_PROCESS2 user accounts. The utility is included in the PRM installation medium.

Follow these steps to create the PRM_PROCESS and PRM_PROCESS2 user accounts:

1. Log on as a user with administrative rights.
2. Insert the PRM installation medium into the DVD drive, and navigate to the following folder:
<DVD drive>:\PRM\SecuritySettingUtility
3. Double-click [CreateInternalUserAccount.exe].
The PRM_PROCESS and PRM_PROCESS2 user accounts are created and automatically added to one of the following groups:
Standalone management: CTM_OPCTM_OPCL
Domain management: CTM_OPCL
Combination management: CTM_OPCTM_OPCL
4. Start HIS Utility.
5. Click the [OPC] tab.
6. In the Set logon options for connecting OPC server section, click [Change].
The Select Logon Type dialog box appears.
7. Select a logon type.
8. Click [OK].

IMPORTANT

If you select [Logon transaction is required for connecting OPC server], you must specify the logon details when configuring message acquisition settings and alarm notification rules on the PRM Server computer.

SEE ALSO

For more information about the procedure for selecting the logon type on the OPC tab of HIS Utility, refer to:

“■ HIS Utility” in 1.2, “Engineering Related to OPC” in Optional Functions Reference (IM 33J05H10-01EN)

D1.2.2 PRM Server and CENTUM VP Standard Operation and Monitoring Function

Connecting PRM Server and CENTUM VP Standard Operation and Monitoring Function enables Consolidated Alarm Management Function (CAMS for HIS) of CENTUM VP to receive maintenance messages from PRM.

Exaopc OPC Interface Package (for HIS) is required on the CENTUM VP computer.

■ Enabling CAMS for HIS to receive maintenance messages from PRM

The following table shows the connection information. The required procedures of connecting the products are provided after the table.

Table D1.2.2-1 Connection information

Integration code	0302-0101-02-02		
Product 1	Plant Resource Manager Server		
Product 2	Standard Operation and Monitoring Function of CENTUM VP R4.03 or later (*1)		
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 "● When the Standard model is applied."	

*1: CAMS for HIS is included in Standard Operation and Monitoring Function.

● Notes

- CAMS for HIS classifies messages that are received from PRM as "Asset" alarm type (TypeOfAlarm). However, if the PRM Advanced Diagnostic Server package is installed, and the Send to the following HISs option is selected in the Advanced Diagnosis pane of the PRM Setup Tool, the messages are classified as "Guidance."
- To display the messages in the PRM Client and CAMS for HIS, you must define two alarm management rules in the Alarm Management Tool with the same conditions. However, you must set the Usage rule action to "Maintenance" in one rule and "Operator" in another rule.

● When the Legacy model is applied

Use HIS Utility of CENTUM VP to configure CAMS for HIS.

Follow these steps to configure CAMS for HIS:

- Log on as a user with administrative rights and start HIS Utility.
- On the [CAMS for HIS] tab of HIS Utility, select the [Enable CAMS for HIS] check box.
- Click [OPC A&E Server Connection].
The OPC A&E Server Connection dialog box appears.
- In the Computer Name of OPC A&E Server box, specify the computer name of the PRM Server.
- In the Program ID in OPC A&E Server box, type `Yokogawa.ExaopcAEPRM.1`.
- In the OPC A&E Server Connection dialog box, click [OK].
- In HIS Utility, click [OK].

- When the Standard model is applied

Follow these steps to configure CAMS for HIS:

1. On the PRM Server computer, create a user account, and then set a password for it.
We recommend that you name the user account as PRM_OPC_USER.
2. Add the user account that you created to one of the following groups:
Standalone management PRM_OPC
Domain management PRM_OPC_LCL
Combination management PRM_OPC or PRM_OPC_LCL

IMPORTANT

When you configure the OPC A&E Server Connection to PRM on a CENTUM HIS, you must specify the user name that you set here and the password that is used for CENTUM HIS Utility.

3. Configure CAMS for HIS in HIS Utility of CENTUM VP by performing these steps:
 - a. Log on as a user with administrative rights and start HIS Utility.
 - b. On the [CAMS for HIS] tab of HIS Utility, select the [Enable CAMS for HIS] check box.
 - c. Click [OPC A&E Server Connection].
The OPC A&E Server Connection dialog box appears.
 - d. In the Computer Name of OPC A&E Server box, specify the computer name of the PRM Server.
 - e. In the Program ID in OPC A&E Server box, type Yokogawa.ExaopcAEPRM.1.
 - f. Click [Apply].
The User Authentication of OPC A&E Server dialog box appears.
 - g. Specify the username and password of the user that you created on the PRM Server.
 - h. Click [OK].
 - i. In the OPC A&E Server Connection dialog box, click [OK].
 - j. In HIS Utility, click [OK].

D1.3 CENTUM VP and Exaopc

This section describes the settings when connecting CENTUM VP and Exaopc.

IMPORTANT

As a basic rule, the security model and user management type must be consistent in the products to be connected. However, CENTUM VP and Exaopc can be connected even if different security model or user management type is applied.

D1.3.1 CENTUM VP Standard Operation and Monitoring Function and Exaopc Server

Connecting CENTUM VP Standard Operation and Monitoring Function and Exaopc Server enables OPC clients to use data of CENTUM VP through the OPC interface.

■ Connecting CENTUM VP Standard Operation and Monitoring Function and Exaopc

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

Table D1.3.1-1 Connection information

Integration code	0101-0401-02-01		
Product 1	Standard Operation and Monitoring Function of CENTUM VP R5.01 or later		
Product 2	OPC Interface Package Server of Exaopc R3.70 or later		
Security model	Legacy model	Standard model	
User management type	-	Standalone management	Domain/Combination management
Required procedures	Refer to B1.6, "Connecting to CENTUM system" of NTPF100 Exaopc OPC Interface Package Installation Manual (IM 36J02A12-01E).		

Table D1.3.1-2 Connection information: Different security model - Case 1

Integration code	0101-0401-02-01		
Product 1	Standard Operation and Monitoring Function of CENTUM VP R5.01 or later		
Product 2	OPC Interface Package Server of Exaopc R3.70 or later		
Security model	Standard model (CENTUM VP) Legacy model (Exaopc)		
User management type	Standalone management	Domain/Combination management	
Required procedures	Refer to B1.6, "Connecting to CENTUM system" of NTPF100 Exaopc OPC Interface Package Installation Manual (IM 36J02A12-01E).		

Table D1.3.1-3 Connection information: Different security model - Case 2

Integration code	0101-0401-02-01		
Product 1	Standard Operation and Monitoring Function of CENTUM VP R5.01 or later		
Product 2	OPC Interface Package Server of Exaopc R3.70 or later		
Security model	Legacy model (CENTUM VP) Standard model (Exaopc)		
User management type	Standalone management	Domain/Combination management	
Required procedures	None		

D1.3.2 CENTUM VP System Builder Function and Exaopc Server

The expanded test function of CENTUM VP can work together with the Exaopc server.

■ Enabling collaboration between the expanded test function of CENTUM VP and Exaopc server

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

Table D1.3.2-1 Connection information

Integration code	0102-0401-02-01		
Product 1	System Builder Function of CENTUM VP R5.01 or later		
Product 2	OPC Interface Package Server of Exaopc R3.70 or later		
Security model	Legacy model	Standard model	
User management type	-	Standalone management	Domain/Combination management
Required procedures	Refer to B1.6, "Connecting to CENTUM system" of NTPF100 Exaopc OPC Interface Package Installation Manual (IM 36J02A12-01E).		

Table D1.3.2-2 Connection information: Different security model - Case 1

Integration code	0102-0401-02-01		
Product 1	System Builder Function of CENTUM VP R5.01 or later		
Product 2	OPC Interface Package Server of Exaopc R3.70 or later		
Security model	Standard model (CENTUM VP) Legacy model (Exaopc)		
User management type	Standalone management	Domain/Combination management	
Required procedures	Refer to B1.6, "Connecting to CENTUM system" of NTPF100 Exaopc OPC Interface Package Installation Manual (IM 36J02A12-01E).		

Table D1.3.2-3 Connection information: Different security model - Case 2

Integration code	0102-0401-02-01		
Product 1	System Builder Function of CENTUM VP R5.01 or later		
Product 2	OPC Interface Package Server of Exaopc R3.70 or later		
Security model	Legacy model (CENTUM VP) Standard model (Exaopc)		
User management type	Standalone management	Domain/Combination management	
Required procedures	Refer to B1.6, "Connecting to CENTUM system" of NTPF100 Exaopc OPC Interface Package Installation Manual (IM 36J02A12-01E).		

D1.4 CENTUM VP and Exapilot

This section describes the settings when connecting CENTUM VP and Exapilot.

D1.4.1 CENTUM VP Standard Operation and Monitoring Function and Exapilot Server

The purpose of this connection is to enable Exapilot server to read and write data on HIS through Exaopc OPC Interface Package (for HIS) by connecting CENTUM VP Standard Operation and Monitoring Function and Exapilot server. Different tasks are required for this connection, depending on whether these packages are used on the same computer or on separate computers.

Because Exapilot Server includes the Exapilot Client functions, what you can do through connection between CENTUM VP and Exapilot Client is also possible through connection between CENTUM VP and Exapilot Server. Therefore, when you are connecting CENTUM VP and Exapilot Server, please go through the contents about the connection in Exapilot Client also.

■ When using the packages on the same computer

The following table shows the connection information. Refer to the description provided after the table for the required procedures for connection.

Table D1.4.1-1 Connection information

Integration Code	0101-0601-03-02		
Product 1	CENTUM VP R4.03 or later - Standard Operation and Monitoring Function		
Product 2	Exapilot R3.95 or later - Operation Efficiency Improvement Package Server		
Security model	Legacy model	Standard model	
User management types	-	Standalone management	Domain management or Combination management
Required procedures	None	Refer to "● When Standard model is applied to both products."	

IMPORTANT

When Exapilot Server is installed on the computer where CENTUM VP R5.01 or later is installed, rebuilding of CENTUM desktop may be required.

● When Standard model is applied to both products

If Standard model is applied to both products, follow these steps:

1. On the CENTUM VP computer, add the PLT_PROCESS account to the following group:
For Standalone management : CTM_OPC
For Domain management or Combination management : CTM_OPC_LCL
2. On the Exapilot Server computer, add the CTM_PROCESS account to the following group:
For Standalone management : PLT_OPC
For Domain management or Combination management : PLT_OPC_LCL

■ When using the packages on separate computers

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

IMPORTANT

As a basic rule, unify the security model and user management type of the products that you want to connect. However, CENTUM VP and Exapilot can be connected even if the security model and user management type are different.

Table D1.4.1-2 Connection information

Integration code	0101-0601-03-02		
Product 1	CENTUM VP R4.03 or later - Standard Operation and Monitoring Function		
Product 2	Operation Efficiency Improvement Package Server of Exapilot R3.95 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 to both products."	Refer to "● When the Standard model is applied to both products."	

Table D1.4.1-3 Connection information: Different security model - Case 1

Integration code	0101-0601-03-02		
Product 1	CENTUM VP R4.03 or later - Standard Operation and Monitoring Function		
Product 2	Operation Efficiency Improvement Package Server of Exapilot R3.95 or later		
Security model	Standard model (CENTUM VP) Legacy model (Exapilot)		
User management type	Standalone management	Domain/Combination management	
Required procedures	Refer to "● When the Standard model is applied to CENTUM VP and the Legacy model to Exapilot."		

Table D1.4.1-4 Connection information: Different security model - Case 2

Integration code	0101-0601-03-02		
Product 1	CENTUM VP R4.03 or later - Standard Operation and Monitoring Function		
Product 2	Operation Efficiency Improvement Package Server of Exapilot R3.95 or later		
Security model	Legacy model (CENTUM VP) Standard model (Exapilot)		
User management type	Standalone management	Domain/Combination management	
Required procedures	Refer to "● When the Legacy model is applied to CENTUM VP and the Standard model to Exapilot."		

TIP

To connect a Legacy model applied computer and a Standard model applied computer on which NetBIOS over TCP/IP is disabled, you need to perform additional task for name resolution. Perform one of the following three tasks:

- Add the computer to the domain

Add the Legacy model computer to the same domain of the Standard model computer.

- Use DNS

Register the Legacy model computer on the DNS server, and set up both the Legacy model computer and the Standard model computer to use the DNS. In general, the domain controller of the domain including the Standard model computer is used as the DNS server.

- Use the hosts/lmhosts file

In hosts or lmhosts file of the Legacy model computer, register the computer name and the IP address of the Standard model computer. In hosts or lmhosts file of the Standard model computer, register the computer name and the IP address of the Legacy model computer.

● When the Legacy model is applied to both products

1. On the CENTUM VP computer, create a user account for running Exaopc server process. The default name of the user account is EXA. The password should also be EXA.
2. On the computer running Exapilot, log on by using a user account with administrative rights and run the following program to create the CTM_PROCESS user account.
<Drive of CENTUM VP software medium>:\CENTUM\SECURITY\Yokogawa.IA.iPCS.Platform.Security.CreateCentumProcess.exe

● When the Standard model is applied to both products

1. On the computer running CENTUM VP, log on by using a user account with administrative rights and run the following process execution account creation tool to create the PLT_PROCESS user account.
<Drive of Exapilot software medium>:\TOOLS\CreatePLTProcess.exe
2. On the CENTUM VP computer, add the user account that you have created, and added to the following user group, depending on the user management type:

Table D1.4.1-5 User management type and the group the user should belong to

CENTUM VP user management types	Exapilot user management types	Group the user should belong to
Standalone management	Standalone management	CTM_OPC
Domain or Combination management	Domain or Combination management	CTM_OPC_LCL
Standalone management	Domain or Combination management	CTM_OPC
Domain or Combination management	Standalone management	CTM_OPC_LCL

3. On the computer running Exapilot, log on by using a user account with administrative rights and run the following process execution account creation tool to create the CTM_PROCESS user account.
<Drive of CENTUM VP software medium>:\CENTUM\SECURITY\Yokogawa.IA.iPCS.Platform.Security.CreateCentumProcess.exe
4. On the Exapilot computer, add the user account that you have created to the following user group, depending on the user management type:

Table D1.4.1-6 User management type and the group the user should belong to

CENTUM VP user management types	Exapilot user management types	Group the user should belong to
Standalone management	Standalone management	PLT_OP
Domain or Combination management	Domain or Combination management	PLT_OP_LCL
Standalone management	Domain or Combination management	PLT_OP_LCL
Domain or Combination management	Standalone management	PLT_OP

- **When the Standard model is applied to CENTUM VP and the Legacy model to Exapilot**

1. On the CENTUM VP computer, create the process execution user account for Exapilot Server and add the account to the following user group, depending on the CENTUM VP user management type:
 - Standalone management on CENTUM VP: CTM_OP
 - Domain/Combination management on CENTUM VP: CTM_OP_LCL

The default name of the user account is EXA. The password should also be EXA.
2. On the Exapilot computer, log on as a user with administrative rights and run the following process execution account creation tool to create the CTM_PROCESS user account.
`<Drive of CENTUM VP software medium>:\CENTUM\SECURITY\Yokogawa.IA.iPCS.Platfo
rm.Security.CreateCentumProcess.exe`

- **When the Legacy model is applied to CENTUM VP and the Standard model to Exapilot**

1. On the computer running CENTUM VP, log on by using a user account with administrative rights and run the following process execution account creation tool to create the PLT_PROCESS user account.
`<Drive of Exapilot software medium>:\TOOLS\CreatePLTProcess.exe`
2. On the computer running Exapilot, log on by using a user account with administrative rights and run the following process execution account creation tool to create the CTM_PROCESS user account.
`<Drive of CENTUM VP software medium>:\CENTUM\SECURITY\Yokogawa.IA.iPCS.Platfo
rm.Security.CreateCentumProcess.exe`
3. Add the user account that you have created to the following user group, depending on the Exapilot user management type:
 - Standalone management on Exapilot: PLT_OP
 - Domain/Combination management on Exapilot: PLT_OP_LCL

D1.4.2 CENTUM VP Standard Operation and Monitoring Function and Exapilot Client

By connecting CENTUM VP Operation and Monitoring Function and Exapilot Client, you can perform the following tasks:

- Operate various Exapilot windows on CENTUM VP HIS
- Use the ActiveX components/.NET components of Exapilot in CENTUM VP graphics.

IMPORTANT

You can perform these tasks only when using CENTUM VP Standard Operation and Monitoring Function and Exapilot Client on the same computer.

■ Connecting CENTUM VP Standard Operation and Monitoring Function and Exapilot Client

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

Table D1.4.2-1 Connection information

Integration code	0101-0651-03-02		
Product 1	CENTUM VP R4.03 or later - Standard Operation and Monitoring Function		
Product 2	Operation Efficiency Improvement Package Client of Exapilot R3.95 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 to both products with Standalone management."	Refer to "● When the Standard model is applied to both products with Domain or Combination management."

● Notes

When using CENTUM VP Standard Operation and Monitoring Function and Exapilot Client on the same computer, note the following points about switching the user of CENTUM VP HIS.

- If user authentication is based on the logging off/on of Windows users, use the Windows authentication mode of Exapilot.
- If user authentication is based on the user switching in the User-In dialog box, use the Exapilot authentication mode.

Table D1.4.2-2 User authentication modes when using the packages on the same computer

CENTUM VP	Exapilot	
	Windows authentication mode	Exapilot authentication mode
CENTUM authentication mode	Available (*1)	Recommended
Windows authentication mode with HIS type single sign on	Available(*2)(*3)	Recommended
Windows authentication mode with Windows type single sign on	Recommended (*2)(*4)	Available

*1: In the Exapilot System Security window, register the Windows user account for operating the HIS after logging on to Windows and set the user rights required for Exapilot operation.

- *2: In the Exapilot System Security window, register the users who log on to HIS and grant them the user rights required for Exapilot operation. However, if you want to configure Auto Start of the message notification function, grant the operation rights to the user who logs on to Windows. Also, the user who automatically starts the message notification function must be a Windows log on user. (OFFUSER is the Windows log on user for HIS type single sign on.)
- *3: ActiveX components and .NET components of Exapilot that are embedded in the graphics are executed by OFFUSER, therefore when using ActiveX components and .NET components, register the OFFUSER of local computer in the Exapilot System Security window and set the required user rights.
- *4: ActiveX components and .NET components of Exapilot that are embedded in the graphics are executed by Windows log on user, therefore when using ActiveX components and .NET components, register the Windows log on user in the Exapilot System Security window and set the required user rights.

IMPORTANT

- When HIS type single sign on is used, do not log off Windows.
- The Windows user names used in Exapilot must satisfy the naming rules of CENTUM VP.

● When the Standard model is applied to both products with Standalone management

1. Log on to the Exapilot Server computer as a user with administrative rights and create the following user account, depending on the CENTUM VP user authentication mode:
 - When CENTUM VP uses CENTUM authentication mode:
User account used to log on to Windows when operating various Exapilot windows
 - When CENTUM VP uses Windows authentication mode:
User account used to log on to CENTUM VP HIS when operating various Exapilot windows
2. Add the user account you have created to the PLT_OPERATOR group.

● When the Standard model is applied to both products with Domain or Combination management

1. Add the following user account to the PLT_OPERATOR_LCL group, depending on the user authentication mode of CENTUM VP.
 - When CENTUM VP uses CENTUM authentication mode:
User account used to log on to Windows when operating various Exapilot windows
 - When CENTUM VP uses Windows authentication mode:
User account for logging on to CENTUM VP HIS to operate various Exapilot windows

● Setting function keys/preset menus when HIS type single sign on is enabled

To start an Exapilot window in the case of HIS type single sign on, it is necessary to assign the function to either a function key or the preset menu. This is because no Exapilot window can be started from the Start menu since the HIS Type Single Sign On remains always logged on to Windows with OFFUSER.

If you are connecting the products only to use ActiveX components and .NET components of Exapilot in CENTUM VP graphics, you do not need to configure these settings.

Table D1.4.2-3 Files to be assigned to start Exapilot windows

Start menu display	File path(*1)
Exapilot Builder	%EXA%\Program\PLTBuilder.exe
Exapilot Operation	%EXA%\Program\PLTMonitor.exe
Exapilot Event Record Display	%EXA%\Program\PLTEventHistory.exe
Software configuration viewer	%EXA%\Program\PMCSftView.exe
Exapilot Event Record Management	%EXA%\Program\PLTHistManager.exe

Continues on the next page

Table D1.4.2-3 Files to be assigned to start Exapilot windows (Table continued)

Start menu display	File path(*1)
Exapilot Option Configuration Viewer	%EXA%\Exapilot\tool\PLTOptInstall.exe
Exapilot Security	%EXA%\Program\PLTSecurity.exe
Exapilot Utility	%EXA%\Program\PLTUtility.exe
Exapilot Save-Restore	%EXA%\Program\PLTSaveRestore.exe
Exapilot prepare to run Main Procedure	%EXA%\Program\PLTProcPrepare.exe
Exapilot Variable Display	%EXA%\Program\PLTVariab le.exe
Exapilot Message Notification	%EXA%\Program\PLTMessageNotification.exe

*1: %EXA% stands for the installation folder name. The default is C:\EXA

1. Use the Function Key Assignment Builder of CENTUM VP to assign the functions to the function keys.
2. Use the HIS Setup Window to configure the preset menus.

D1.4.3 CENTUM VP System Builder Function and Exapilot Client

By using CENTUM VP System Builder Function and Exapilot Client, you can create CENTUM VP graphics that contain ActiveX components and .NET components of Exapilot.

■ Using CENTUM graphics containing Exapilot ActiveX components/.NET components

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

Table D1.4.3-1 Connection information

Integration code	0102-0651-03-01		
Product 1	CENTUM VP R4.03 or later - System Builder Function		
Product 2	Operation Efficiency Improvement Package Server of Exapilot R3.90 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 to both products."	

- **When the Standard model is applied to both products**

Follow these steps:

For Standalone management, perform this task on the computer where CENTUM VP graphics are created. For Domain or Combination management, perform this task on the domain controller.

1. Log on by using a user account with administrative rights.
2. Add the users who create CENTUM VP graphics to the CTM_ENGINEER and PLT_OPERATOR groups.

D1.5 CENTUM VP and Exaplog

This section describes the settings when connecting CENTUM VP and Exaplog.

D1.5.1 CENTUM VP Standard Operation and Monitoring Function and Exaplog Event Analysis Package Server

Connecting CENTUM VP Standard Operation and Monitoring Function and Exaplog Event Analysis Package Server enables Exaplog to acquire event data from CENTUM VP HIS. For this connection, different tasks are required, depending on whether these packages are used on the same computer or on separate computers.

■ When using the packages on the same computer

When using CENTUM VP Standard Operation and Monitoring Function and Exaplog Event Analysis Package Server on the same computer, no setting is required for connection regardless of whether the packages are operated individually or function together by communicating or sharing files each other.

■ When using the packages on separate computers

When using CENTUM VP Standard Operation and Monitoring Function and Exaplog Event Analysis Package Server on separate computers, certain settings are required for connection.

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

IMPORTANT

As a basic rule, the security model and user management type must be consistent in the products to be connected. However, CENTUM VP and Exaplog can be connected even if different security model or user management type is applied.

Table D1.5.1-1 Connection information

Integration code	0101-0701-03-02		
Product 1	Standard Operation and Monitoring Function of CENTUM VP R5.01 or later		
Product 2	Event Analysis Package Server of Exaplog R3.40 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 to both products."	Refer to "● When the Standard model is applied to both products."	

Table D1.5.1-2 Connection information: Different security model - Case 1

Integration code	0101-0701-03-02		
Product 1	Standard Operation and Monitoring Function of CENTUM VP R5.01 or later		
Product 2	Event Analysis Package Server of Exaplog R3.40 or later		
Security model	Standard model (CENTUM VP) Legacy model (Exaplog)		
Standalone management	Standalone management	Domain/Combination management	
Required procedures	Refer to "● When the Standard model is applied to CENTUM VP and the Legacy model to Exaplog."		

Table D1.5.1-3 Connection information: Different security model - Case 2

Integration code	0101-0701-03-02	
Product 1	Standard Operation and Monitoring Function of CENTUM VP R5.01 or later	
Product 2	Event Analysis Package Server of Exaplog R3.40 or later	
Security model Legacy model (CENTUM VP)	Legacy model (CENTUM VP) Standard model (Exaplog)	
Standalone management	Standalone management	Domain/Combination management
Required procedures	Refer to "● When the Legacy model is applied to CENTUM VP and the Standard model to Exaplog."	

TIP

To connect a Legacy model applied computer and a Standard model applied computer on which NetBIOS over TCP/IP is disabled, you need to perform additional task for name resolution. Perform one of the following three tasks:

- Add the computer to the domain
Add the Legacy model computer to the same domain of the Standard model computer.
- Use DNS
Register the Legacy model computer on the DNS server, and set up both the Legacy model computer and the Standard model computer to use the DNS. In general, the domain controller of the domain including the Standard model computer is used as the DNS server.
- Use the hosts/Imhosts file
In hosts or Imhosts file of the Legacy model computer, register the computer name and the IP address of the Standard model computer. In hosts or Imhosts file of the Standard model computer, register the computer name and the IP address of the Legacy model computer.

- **When the Legacy model is applied to both products**

On the computer running CENTUM VP, create the exaplog user account. The password for the exaplog user account should be the same as the password set for the exaplog user account on the Exaplog server computer.

- **When the Standard model is applied to both products**

1. On the computer running CENTUM VP, create the exaplog user account. The password for the exaplog user account should be the same as the password set for the exaplog user account on the Exaplog server computer.
2. Add the user account you have created to the following group:
Standalone management: CTM_OPERATOR
Domain or Combination management: CTM_OPC_LCL

- **When the Standard model is applied to CENTUM VP and the Legacy model to Exaplog**

1. On the computer running CENTUM VP, create the exaplog user account. The password for the exaplog user account should be the same as the password set for the exaplog user account on the Exaplog server computer.
2. Add the user account you have created to the following group:
Standalone management on CENTUM VP: CTM_OPERATOR
Domain or Combination management on CENTUM VP: CTM_OPC_LCL

- **When the Legacy model is applied to CENTUM VP and the Standard model to Exaplog**

On the computer running CENTUM VP, create the exaplog user account. The password for the exaplog user account should be the same as the password set for the exaplog user account on the Exaplog server computer.

D1.6 CENTUM VP and Exaquantum

This section describes the settings when connecting CENTUM VP and Exaquantum.

D1.6.1 CENTUM VP Standard Operation and Monitoring Function and Exaquantum PIMS Server

Connecting CENTUM VP Standard Operation and Monitoring Function and Exaquantum PIMS Server enables Exaquantum PIMS Server to acquire data from HIS and FCS of CENTUM VP through Exaopc OPC Interface Package (for HIS).

■ Enabling Exaquantum to acquire data from CENTUM VP HIS and FCS

When using CENTUM VP Standard Operation and Monitoring Function and Exaquantum PIMS Server on separate computers, certain settings are required for connection.

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

IMPORTANT

As a basic rule, the security model and user management type must be consistent in the products to be connected. However, CENTUM VP and Exaquantum can be connected even if different security model or user management type is applied.

Table D1.6.1-1 Connection information

Integration code	0101-0801-02-03		
Product 1	Standard Operation and Monitoring Function of CENTUM VP R5.01 or later		
Product 2	PIMS server of Exaquantum R2.70 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 to both products."	Refer to "● When the Standard model is applied to both products."	

Table D1.6.1-2 Connection information: Different security model - Case 1

Integration code	0101-0801-02-03		
Product 1	Standard Operation and Monitoring Function of CENTUM VP R5.01 or later		
Product 2	PIMS server of Exaquantum R2.70 or later		
Security model	Standard model (CENTUM VP) Legacy model (Exaquantum)		
Standalone management	Standalone management	Domain/Combination management	
Required procedures	Refer to "● When the Standard model is applied to CENTUM VP and the Legacy model to Exaquantum."		

Table D1.6.1-3 Connection information: Different security model - Case 2

Integration code	0101-0801-02-03		
Product 1	Standard Operation and Monitoring Function of CENTUM VP R5.01 or later		
Product 2	PIMS server of Exaquantum R2.70 or later		
Security model Legacy model (CENTUM VP)	Legacy model (CENTUM VP) Standard model (Exaquantum)		

Continues on the next page

Table D1.6.1-3 Connection information: Different security model - Case 2 (Table continued)

Standalone management	Standalone management	Domain/Combination management
Required procedures	Refer to "● When the Legacy model is applied to CENTUM VP and the Standard model to Exaquantum."	

● When the Legacy model is applied to both products

1. On the computer running CENTUM VP, create the Quantumuser account and set the same password as the Quantumuser on the Exaquantum computer.
2. On the Exaquantum computer, run the following process execution account creation tool to create the CTM_PROCESS user account.
`<Drive of CENTUM VP software medium>:\CENTUM\SECURITY\Yokogawa.IA.iPCS.Platform.Security.CreateCentumProcess.exe`
3. Set the logon type.
 - When compatibility with earlier versions is required:
 On the computer running CENTUM VP, set the logon type to [Default user of R4.03 and earlier versions] on the OPC tab of HIS Utility. On the computer running Exaopc, turn off the [OPC gateway security] option.
 - When logging on is required:
 On the computer running CENTUM VP, set the logon type on the OPC tab of HIS Utility. On the computer running Exaopc, set the OPC logon information for the OPC gateway in accordance with the settings of CENTUM VP.

● When the Standard model is applied to both products

1. Log on to the computer where CENTUM VP runs as an administrative user.
2. Insert Exaquantum Prerequisites DVD (Disk 1) into the drive.
3. Run the following command:
`<DVD drive>:\Misc\CPP2008\vcredist_x86.exe`
 Microsoft Visual C++ 2008 Redistributable Package is installed.
4. On the computer running CENTUM VP, create the QTM_PROCESS user account.
5. Add the QTM_PROCESS user account to the following group.
 Standalone management: CTM_OPC
 Domain/Combination management: CTM_OPC_LCL
6. On the Exaquantum computer, run the following process execution account creation tool to create the CTM_PROCESS user account.
`<Drive of CENTUM VP software medium>:\CENTUM\SECURITY\Yokogawa.IA.iPCS.Platform.Security.CreateCentumProcess.exe`
7. Add the CTM_PROCESS user account to the following group.
 Standalone management: QTM_OPC
 Domain/Combination management: QTM_OPC_LCL
8. Set the logon type.
 - When compatibility with earlier versions is required:
 On the computer running CENTUM VP, set the logon type to [Default user of R4.03 and earlier versions] on the OPC tab of HIS Utility. On the computer running Exaopc, turn off the [OPC gateway security] option.
 - When logging on is required:

On the computer running CENTUM VP, set the logon type on the OPC tab of HIS Utility. On the computer running Exaopc, set the OPC logon information for the OPC gateway in accordance with the settings of CENTUM VP.

● **When the Standard model is applied to CENTUM VP and the Legacy model to Exaquantum**

1. On the computer running CENTUM VP, create the Quantumuser user account.
2. Add the Quantumuser user account to the following group.
Standalone management: CTM_OPC
Domain/Combination management: CTM_OPC_LCL
3. On the Exaquantum computer, run the following process execution account creation tool to create the CTM_PROCESS user account.
<Drive of CENTUM VP software medium>:\CENTUM\SECURITY\Yokogawa.IA.iPCS.Platform.Security.CreateCentumProcess.exe
4. Set the logon type.
 - When compatibility with earlier versions is required:
On the computer running CENTUM VP, set the logon type to [Default user of R4.03 and earlier versions] on the OPC tab of HIS Utility. On the computer running Exaopc, turn off the [OPC gateway security] option.
 - When logging on is required:
On the computer running CENTUM VP, set the logon type on the OPC tab of HIS Utility. On the computer running Exaopc, set the OPC logon information for the OPC gateway in accordance with the settings of CENTUM VP.

● **When the Legacy model is applied to CENTUM VP and the Standard model to Exaquantum**

1. Log on to the computer where CENTUM VP runs as an administrative user.
2. Insert Exaquantum Prerequisites DVD (Disk 1) into the drive.
3. Run the following command:
<DVD drive>:\Misc\CPP2008\vcredist_x86.exe
Microsoft Visual C++ 2008 Redistributable Package is installed.
4. On the computer running CENTUM VP, create the QTM_PROCESS user account.
5. On the Exaquantum computer, run the following process execution account creation tool to create the CENTUM user account.
<Drive of CENTUM VP software medium>:\CENTUM\SECURITY\Yokogawa.IA.iPCS.Platform.Security.CreateCentumProcess.exe
6. Add the CENTUM user account to the following group.
Standalone management: QTM_OPC
Domain/Combination management: QTM_OPC_LCL
7. Set the logon type.
 - When compatibility with earlier versions is required:
On the computer running CENTUM VP, set the logon type to [Default user of R4.03 and earlier versions] on the OPC tab of HIS Utility. On the computer running Exaopc, turn off the [OPC gateway security] option.
 - When logging on is required:
On the computer running CENTUM VP, set the logon type on the OPC tab of HIS Utility. On the computer running Exaopc, set the OPC logon information for the OPC gateway in accordance with the settings of CENTUM VP.

D1.6.2 CENTUM VP Standard Operation and Monitoring Function and Exaquantum Explorer Client

You can install CENTUM VP Standard Operation and Monitoring Function and Exaquantum Explorer Client on the same computer to use Explorer Client on CENTUM VP HIS.

■ When using the packages on the same computer

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

Table D1.6.2-1 Connection information

Integration code	0101-0851-01-02		
Product 1	Standard Operation and Monitoring Function of CENTUM VP R5.01 or later		
Product 2	Explorer Client of Exaquantum R2.60 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 with Standalone management."	Refer to "● When the Standard model is applied to both products with Domain or Combination management."

- **Prerequisite**

When using CENTUM VP Standard Operation and Monitoring Function and Exasmoc Client on the same computer, install CENTUM VP Standard Operation and Monitoring Function first.

- **When the Standard model is applied with Standalone management**

1. If automatic logon is used on CENTUM VP HIS, disable automatic logon before installing Exaquantum Explorer Client.
2. If automatic starting of HIS is enabled for the user who installs the product, change the setting to disable it.
3. Restart the computer and log on by using a user account with administrative rights.
4. Run the following Exaquantum file.
`<Drive of Exaquantum software medium>:\TOOLS\QTMPreSetStdModel.bat`
The EXA_MAINTENANCE group is created, and the currently logged on user is added to the EXA_MAINTENANCE group.
5. The current user is automatically logged off; so, log on again using the same user account.
6. On the CENTUM VP HIS, restore the settings of automatic logon and automatic starting of HIS to the original state.

- **When the Standard model is applied with Domain or Combination management**

1. If automatic logon is used on CENTUM VP HIS, disable automatic logon before installing Exaquantum Explorer Client.
2. If automatic starting of HIS is enabled for the user who installs the product, change the setting to disable it.
3. On the domain controller, create the following groups:

EXA_MAINTENANCE
QTM_DATA_READ
QTM_DATA_WRITE
QTM_EXPLORER DESIGN
QTM_MAINTENANCE
QTM_OPC

4. Create a user account for installing Exaquantum and add the account to the EXA_MAINTENANCE and Domain Admins groups.

5. Run the following Exaquantum file.

<Drive of Exaquantum software medium>:\TOOLS\QTMPresetStdModelDom.bat

The EXA_MAINTENANCE_LCL group is created, and the currently logged on user is added to this group.

6. On the CENTUM VP HIS, restore the settings of automatic logon and automatic starting of HIS to the original state.

D1.7 Multivariable Optimizing Control/Robust Quality Estimation and CENTUM VP

This section describes the settings when connecting APC Client and CENTUM VP.

D1.7.1 CENTUM VP Standard Operation and Monitoring Function and APC Client

You can use the CENTUM VP Standard Operation and Monitoring Function and the APC Client on the same computer.

■ When using the packages on the same computer

When the APC Client and CENTUM VP are available on the same computer, you can connect them without any settings.

- **User authentication modes when Multivariable Optimizing Control/Robust Quality Estimation and CENTUM VP are installed on the same computer**

The following table describes the user authentication modes and settings when Multivariable Optimizing Control/Robust Quality Estimation and CENTUM VP are installed on the same computer.

Table D1.7.1-1 User authentication modes when Multivariable Optimizing Control/Robust Quality Estimation and CENTUM VP are installed on the same computer

CENTUM VP	Multivariable Optimizing Control/Robust Quality Estimation
CENTUM authentication mode	You must add the windows user group in the Assignment panel of the APC Builder and the user who belongs to this group can operate HIS.
Windows authentication mode: HIS type single sign on	You must register the HIS sign-on user to the windows user group and this group must be added to the Assignment panel of the APC Builder.
Windows authentication mode: Windows type single sign on	You must add the HIS sign-on user group in the Assignment panel of the APC Builder.

IMPORTANT

- Do not log off from Windows when you are using HIS type single sign on.
- The Windows user name that needs to be registered in Multivariable Optimizing Control/Robust Quality Estimation must follow the user naming conventions of CENTUM VP.

SEE ALSO

For more information about CENTUM VP user authentication mode, refer to:

2.2.2, "CENTUM VP User Authentication Modes" in CENTUM VP Security Guide (IM 33J01C30-01EN)

- **Setting function keys/preset menus when HIS type single sign on is enabled**

To start a Multivariable Optimizing Control/Robust Quality Estimation window in case of HIS-type single sign on, it is necessary to assign a function to either a function key or the preset menu. This is because no Multivariable Optimizing Control/Robust Quality Estimation window can be started from the Start menu since the HIS type single sign on remains always logged on to Windows with OFFUSER.

Table D1.7.1-2 List of file path assignments to individual Multivariable Optimizing Control/Robust Quality Estimation windows

Start menu	File path
Builder	<Installation top folder>\Yokogawa\APC\Programs\Yokogawa.AP.C.HMI.Configuration.ThickClient.exe

Continues on the next page

Table D1.7.1-2 List of file path assignments to individual Multivariable Optimizing Control/Robust Quality Estimation windows (Table continued)

Start menu	File path
Operation	<Installation top folder>\Yokogawa\APC\Programs\Yokogawa.AP.C.HMI.Runtime.ThickClient.exe
Data Collection Tool	C:\Windows\System32\cmd.exe /k "<Installation top folder>\Yokogawa\APC\Programs\DataCollectionTool.bat" "<Installation top folder>\Yokogawa\APC\Programs""
Software Configuration Viewer	<Installation top folder>\Yokogawa\APC\Programs\PMCSftView.exe

- Assignment of function keys
You can use the Function Key Assignment Builder of CENTUM VP to assign the required functions to the function keys.
- Setting of preset menus
You can use the HIS Setup window to configure the preset menus.

D1.8 CENTUM VP and Exasmoc

This section describes the settings when using CENTUM VP and Exasmoc on the same computer.

D1.8.1 CENTUM VP Standard Operation and Monitoring Function and Exasmoc Client

You can use CENTUM VP Standard Operation and Monitoring Function and Exasmoc Client on the same computer.

■ When using the packages on the same computer

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

Table D1.8.1-1 Connection information

Integration code	0101-0951-01-02		
Product 1	Standard Operation and Monitoring Function of CENTUM VP R5.01 or later		
Product 2	Exasmoc Client of Exasmoc R4.03		
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 "● When the Standard model is applied with Standalone management."	Refer to "● When the Standard model is applied to both products with Domain or Combination management."

● Prerequisite

When using CENTUM VP Standard Operation and Monitoring Function and Exasmoc Client on the same computer, install CENTUM VP Standard Operation and Monitoring Function first.

● When the Legacy model is applied

1. If automatic logon is used on CENTUM VP HIS, disable automatic logon before installing Exasmoc Client.
2. Restart the computer, log on by using the user account that was used when configuring the security settings of CENTUM VP, and then install Exasmoc.
3. Add the accounts of the users who use Exasmoc tools to CENTUM VP groups appropriately.
4. Configure the computer so that the above mentioned user accounts can be logged on.
5. On CENTUM VP HIS, configure function keys and the preset menu.
6. On the CENTUM VP HIS, restore the setting of automatic logon to the original state.

● When the Standard model is applied with Standalone management

1. If automatic logon is used on CENTUM VP HIS, disable automatic logon before installing Exasmoc Client.
2. Restart the computer, log on by using the user account that was used when configuring the security settings of CENTUM VP, and then install Exasmoc.
3. Add the accounts of the users who use Exasmoc tools to CENTUM VP groups appropriately.
4. Configure the computer so that the above mentioned user account can be logged on.
5. On CENTUM VP HIS, configure function keys and the preset menu.
6. On the CENTUM VP HIS, restore the setting of automatic logon to the original state.

- **When the Standard model is applied with Domain or Combination management**

1. If automatic logon is used on CENTUM VP HIS, disable automatic logon before installing Exasmoc Client.
2. As the account for installation, add a user account that is a member of the EXA_MAINTENANCE group to the CTM_MAINTENANCE group.
3. Add the accounts of the users who use Exasmoc tools to CENTUM VP groups appropriately.
4. Configure the computer so that the above mentioned user accounts can be logged on.
5. On CENTUM VP HIS, configure function keys and the preset menu.
6. On CENTUM VP HIS, restore the setting of automatic logon to the original state.

- **Configuring function keys and preset menu**

As necessary, assign each Exasmoc tool to a function key or to the preset menu of CENTUM VP so that the users can run Exasmoc tools.

To configure function keys, use the Function Key Assignment Builder; to configure the preset menu, use the [Execute a Program by File Name] command in the HIS Setup window.

The following table shows the Exasmoc tools that are registered to the Start menu and their corresponding paths.

Table D1.8.1-2 Start menu programs and corresponding paths

Program on the Start menu	Path
APC Builder	%ProgramFiles%\Yokogawa\IA\iPCS\Products\APC\Program\Yokogawa.IA.iPCS.APC.Builder.ScheduleBuilder.exe
APC HMI	%ProgramFiles%\Yokogawa\IA\iPCS\Products\APC\Program\Yokogawa.IA.iPCS.APC.WebHMI.ApcLocalClient.exe
Client Builder	%ProgramFiles%\Yokogawa\IA\iPCS\Products\APC\Program\Yokogawa.IA.iPCS.APC.Builder.ClientWindowBuilder.exe
Role Based Builder	%ProgramFiles%\Yokogawa\IA\iPCS\Products\APC\Program\Yokogawa.IA.iPCS.APC.Builder.RoleBasedBuilder.exe
Integration Builder	<Top folder of Exa>\Program\ZACItgBuilder.exe
Software Configuration Viewer	<Top folder of Exa>\Program\PMCSftView.exe

D1.9 CENTUM VP and Exasrqe

This section describes the settings when using CENTUM VP and Exarqe on the same computer.

D1.9.1 CENTUM VP Standard Operation and Monitoring Function and Exarqe Client

You can use CENTUM VP Standard Operation and Monitoring Function and Exarqe Client on the same computer.

■ When using the packages on the same computer

The following table shows the connection information. For required procedures for connection, read the descriptions that follow the table.

Table D1.9.1-1 Connection information

Integration code	0101-1051-01-02		
Product 1	Standard Operation and Monitoring Function of CENTUM VP R5.01 or later		
Product 2	Exarqe Client of Exarqe R4.03		
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 "● When the Standard model is applied with Standalone management."	Refer to "● When the Standard model is applied to both products with Domain or Combination management."

- **Prerequisite**

When using CENTUM VP Standard Operation and Monitoring Function and Exarqe Client on the same computer, install CENTUM VP Standard Operation and Monitoring Function first.

- **When the Legacy model is applied**

1. If automatic logon is used on CENTUM VP HIS, disable automatic logon before installing Exarqe Client.
2. Restart the computer, log on by using the user account that was used when configuring the security settings of CENTUM VP, and then install Exarqe.
3. Add the accounts of the users who use Exarqec tools to CENTUM VP groups appropriately.
4. Configure the computer so that the above mentioned user accounts can be logged on.
5. On CENTUM VP HIS, configure function keys and the preset menu.
6. On CENTUM VP HIS, restore the setting of automatic logon to the original state.

- **When the Standard model is applied with Standalone management**

1. If automatic logon is used on CENTUM VP HIS, disable automatic logon before installing Exarqe Client.
2. Restart the computer, log on by using the user account that was used when configuring the security settings of CENTUM VP, and then install Exarqe.
3. Add the accounts of the users who use Exarqec tools to CENTUM VP groups appropriately.
4. Configure the computer so that the above mentioned user accounts can be logged on.
5. On CENTUM VP HIS, configure function keys and the preset menu.
6. On CENTUM VP HIS, restore the setting of automatic logon to the original state.

- **When the Standard model is applied with Domain or Combination management**

1. If automatic logon is used on CENTUM VP HIS, disable automatic logon before installing Exarqe Client.
2. As the account for installation, add a user account that is a member of the EXA_MAINTENANCE group to the CTM_MAINTENANCE group.
3. Add the accounts of the users who use Exarqec tools to CENTUM VP groups appropriately.
4. Configure the computer so that the above mentioned user accounts can be logged on.
5. On CENTUM VP HIS, configure function keys and the preset menu.
6. On CENTUM VP HIS, restore the setting of automatic logon to the original state.

- **Configuring function keys and preset menu**

As necessary, assign each Exasmoc tool to a function key or to the preset menu of CENTUM VP so that the users can run Exarqe tools.

To configure function keys, use the Function Key Assignment Builder; to configure the preset menu, use the [Execute a Program by File Name] command in the HIS Setup window.

The following table shows the Exarqe tools that are registered to the Start menu and their corresponding paths.

Table D1.9.1-2 Start menu programs and corresponding paths

Program on the Start menu	Path
APC Builder	%ProgramFiles%\Yokogawa\IA\iPCS\Products\APC\Program\Yokogawa.IA.iPCS.APC.Builder.ScheduleBuilder.exe
APC HMI	%ProgramFiles%\Yokogawa\IA\iPCS\Products\APC\Program\Yokogawa.IA.iPCS.APC.WebHMI.ApcLocalClient.exe
Client Builder	%ProgramFiles%\Yokogawa\IA\iPCS\Products\APC\Program\Yokogawa.IA.iPCS.APC.Builder.ClientWindowBuilder.exe
Role Based Builder	%ProgramFiles%\Yokogawa\IA\iPCS\Products\APC\Program\Yokogawa.IA.iPCS.APC.Builder.RoleBasedBuilder.exe
Integration Builder	<Top folder of Exa>\Program\ZACItgBuilder.exe
Software Configuration Viewer	<Top folder of Exa>\Program\PMCSftView.exe

Blank Page

Appendix 1. Setting Switches

You can set the domain number and station number by configuring the switches provided on the printed circuit board of the control bus interface card or Vnet/IP interface card.

■ Domain Numbers and DIP Switch Positions

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

■ 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

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
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
.
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. Vnet/IP Interface Management Tool

By using the Vnet/IP Interface Management Tool, you can set the domain number and station number managed by the Vnet/IP Interface Package.

■ Changing the Domain Number and Station Number

Follow these steps to set the domain number and station number managed by the Vnet/IP Interface Package:

1. Sign in to the guest OS on the virtual machine as an administrative user. From the Start menu, select [YOKOGAWA Virtualization] > [VnetIP interface management tool].
2. Open the Settings tab of the Vnet/IP Interface Management Tool.
3. Set the domain number in [Domain No] and the station number in [Station No], and then click [Save].

TIP

You can set a number in the range from 1 to 31 as the domain number, and from 1 to 64 as the station number.

On a virtual machine where you run an FCS simulator that can be operated through remote connection from another HIS by installing the Expanded Test Functions and FCS Simulator Package, set both the domain number and the station number to 0.

Note that the license of Vnet/IP Interface Package is not required when using only the test function with the domain number and the station number set to 0.

4. Click [CLOSE], and restart the virtual machine.

■ Operation Status of the Vnet/IP Interface Package

The [Monitor] shows the following information:

- Version information of the Vnet/IP Interface Package
- Operation status of the Vnet/IP Interface Package
- Domain number and station number
- Presence of different Vnet/IP firmware versions

● Version information

The version number of the Vnet/IP Interface Package is displayed.

● Operation status

One of the following five operation statuses is displayed.

Stop:	Indicates that the Vnet/IP Interface Package is not functioning.
Starting:	Indicates that the domain number, station number, and configuration are being checked before the package goes into operation.
Waiting the license:	Indicates that the package is waiting for the license to be granted.
Working:	Indicates that the package is operating properly.
Stop (error message):	Indicates that the package is not functioning.

**SEE
ALSO**

For more information about the error messages, refer to:

“■ Responding to an Error Message” on page App.2-2

- **Domain number and station number**

The domain number and station number are displayed.

- **Presence of different Vnet/IP firmware versions**

The revision information of the Vnet/IP firmware is displayed. If more than one of stations use old firmwares, they are delimited with a comma.

Display example: 06R, 13L

Meaning: The Vnet/IP firmware implemented on the right side card of station number 6 and the Vnet/IP firmware implemented on the left side card of station number 13 are old.

■ Responding to an Error Message

This section describes the error messages that may be generated when you use the Vnet/IP Interface Management Tool and how to respond to them.

- **Invalid Windows service registration**

The condition for occurrence and the remedy for the message “Invalid Windows service registration” are explained as follows:

- Condition for occurrence

This error message is generated when any one of the Vnet/IP Interface Package services, “YWVNT BKNET Service,” “YWVNT VnetIP Stack Service,” and “YWVNT VnetIP Privileged Service” is not registered as Windows service, or the Vnet/IP Interface Package services are not configured to start automatically.

- Remedy

Install the Vnet/IP Interface Package again.

**SEE
ALSO**

For more information about the procedure to install the Vnet/IP Interface Package, refer to:

B4.3.3, “Installing the Vnet/IP Interface Package on a Virtual Machine” on page B4-48

- **BUS1 not found**

The condition for occurrence and the remedy for the message “BUS1 not found” are explained as follows:

- Condition for occurrence

This message is generated when the name of control network 1 is invalid.

- Remedy

Rename control network 1 to VnetIPBUS1.

**SEE
ALSO**

For more information about the name of control network 1, refer to:

“■ Rename Local Area Connections” on page B4-75

● BUS2 not found

The condition for occurrence and the remedy for the message “BUS2 not found” are explained as follows:

- Condition for occurrence

This message is generated when the name of control network 2 is invalid.

- Remedy

Rename control network 2 to VnetIPBUS2.

SEE ALSO

For more information about the name of control network 2, refer to:

“■ Rename Local Area Connections” on page B4-75

● Invalid domain number or station number

The condition for occurrence and the remedy for the message “Invalid domain number or station number” are explained as follows:

- Condition for occurrence

This message is generated when the domain number and station number managed by the Vnet/IP Interface Package are invalid.

- Remedy

Using the Vnet/IP Interface Management Tool, check the domain number and station number managed by the Vnet/IP Interface Package and set to the correct values.

SEE ALSO

For more information about how to set the domain number and station number managed by the Vnet/IP Interface Package, refer to:

“■ Changing the Domain Number and Station Number” on page App.2-1

● Station of the specified domain number and station number already exists

The condition for occurrence and the remedy for the message “Station of the specified domain number and station number already exists” are explained as follows:

- Condition for occurrence

This message is generated when the same domain number and station number are already used for another station.

- Remedy

Using the Vnet/IP Interface Management Tool, check the domain number and station number managed by the Vnet/IP Interface Package and set to the correct values.

SEE ALSO

For more information about how to set the domain number and station number managed by the Vnet/IP Interface Package, refer to:

“■ Changing the Domain Number and Station Number” on page App.2-1

● IT security not applied

The condition for occurrence and the remedy for the message “IT security not applied” are explained as follows:

- Condition for occurrence

This message is generated when IT security has not been applied after installation of the Vnet/IP Interface Package.

- Remedy
Apply IT security.

Appendix 3. Customization at Installation of Windows 10

This section describes how to customize Windows settings during installation of Windows 10 Enterprise 2016 LTSB.

TIP

You do not need to perform this customization on Windows 10 IoT Enterprise 2016 LTSB installed computers provided by YOKOGAWA.

■ Procedure for Customization at installation of Windows 10

The following screen appears during installation of Windows 10 Enterprise 2016 LTSB. Then, click Customize.

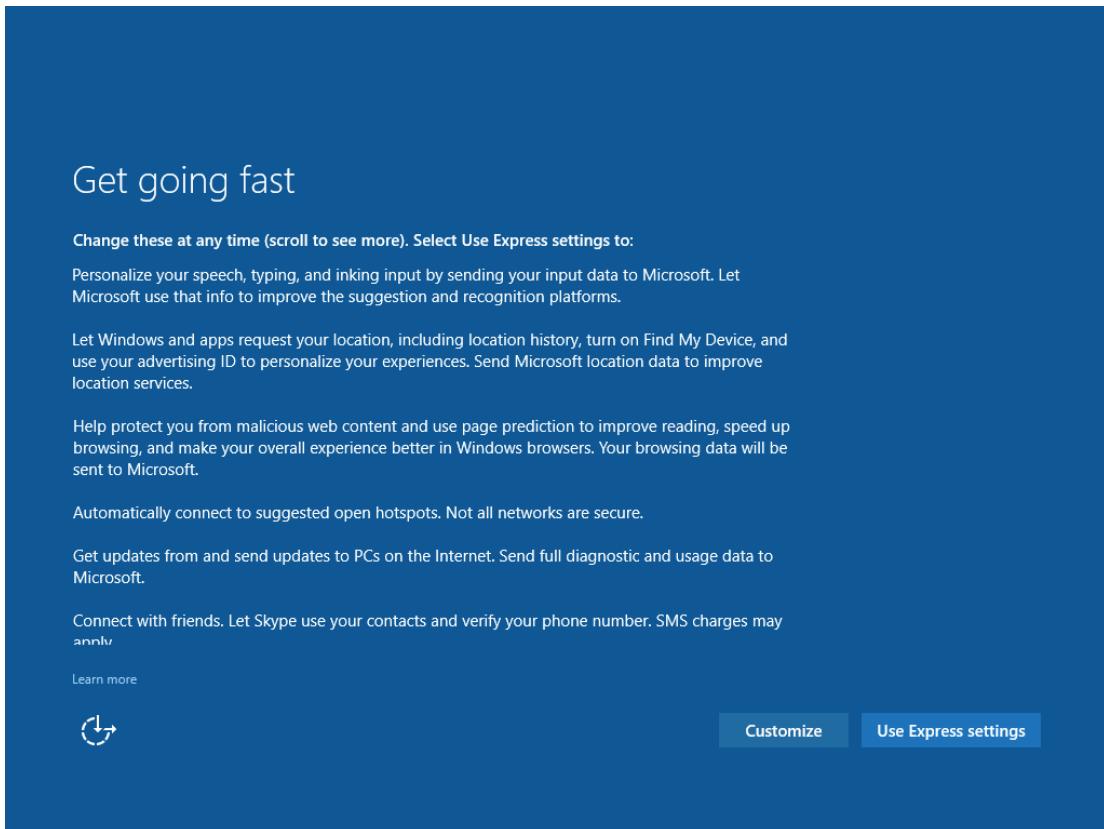


Figure Appendix 3-1 Screen That Appears When Installing Windows 10

In the Customize settings window, set all settings to Off.

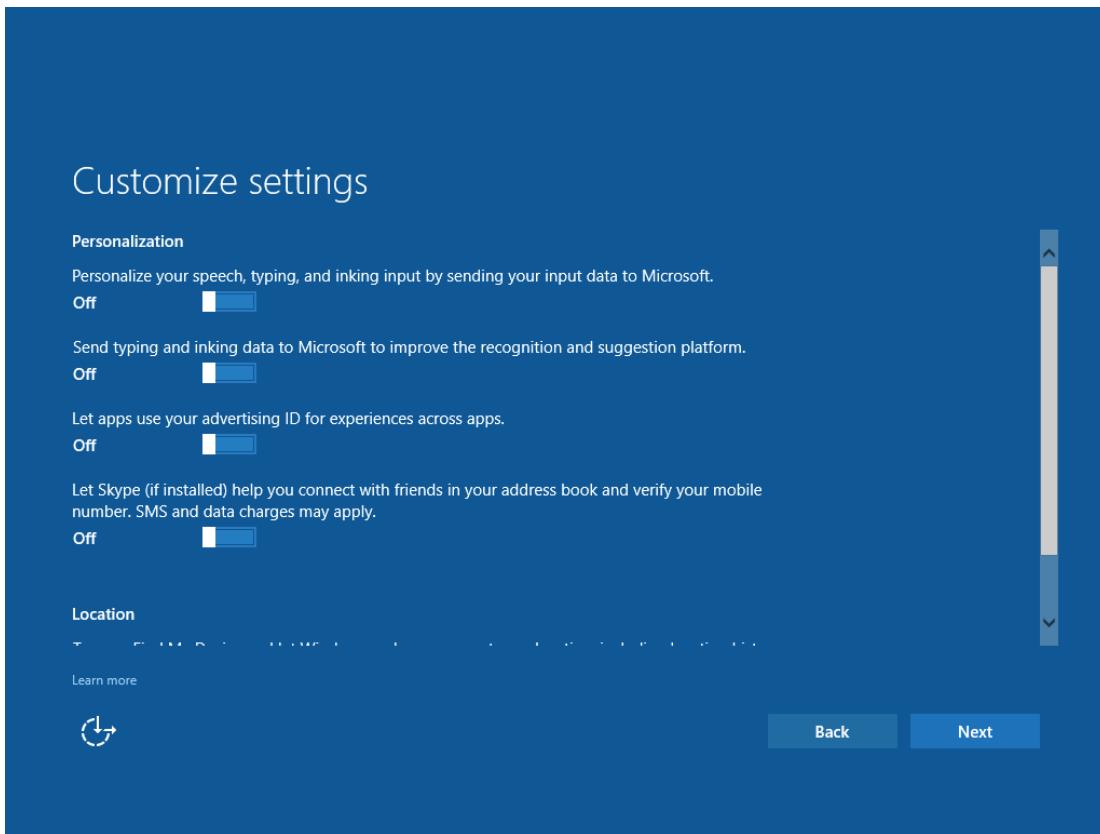


Figure Appendix 3-2 Customize settings Window - 1

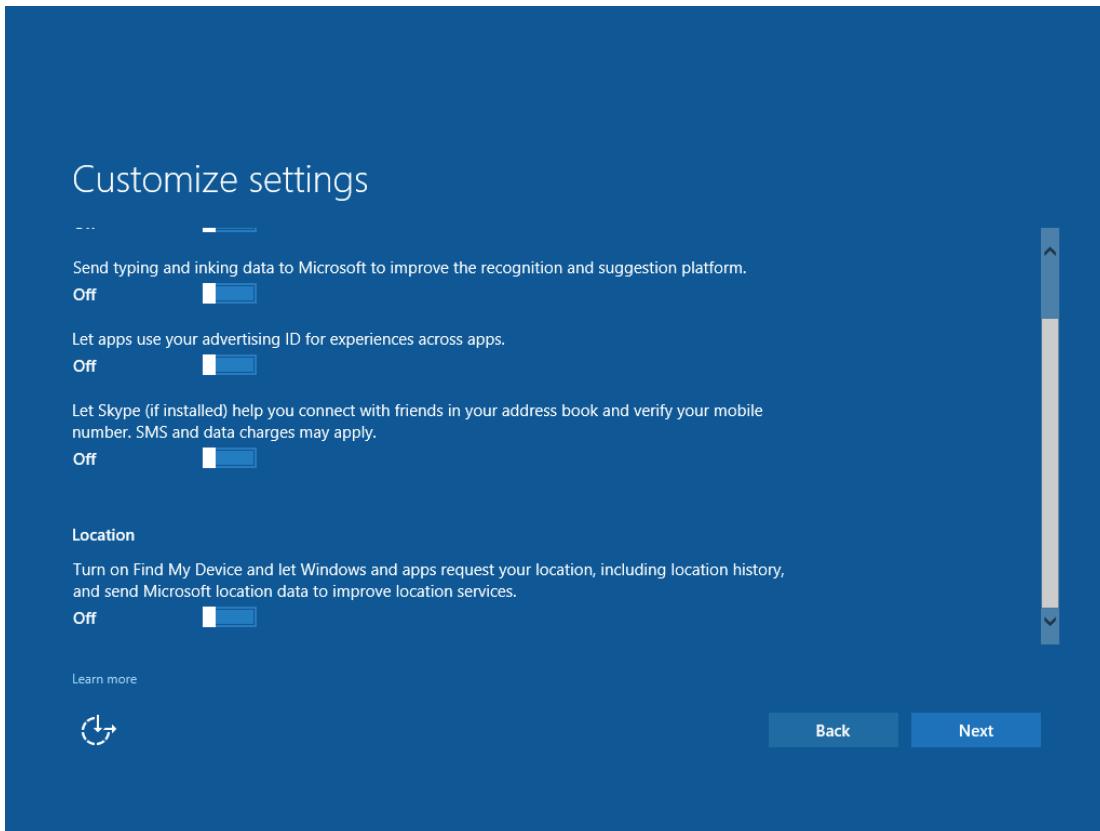


Figure Appendix 3-3 Customize settings Window - 2

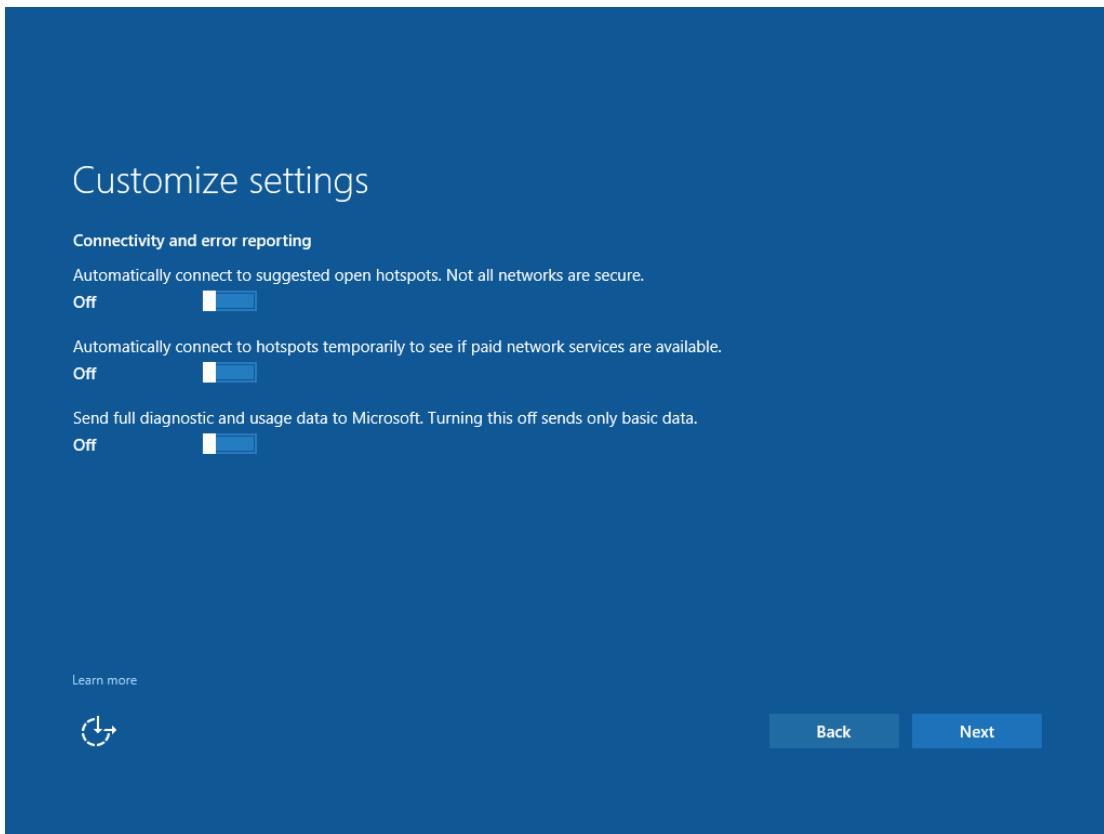


Figure Appendix 3-4 Customize settings Window - 3

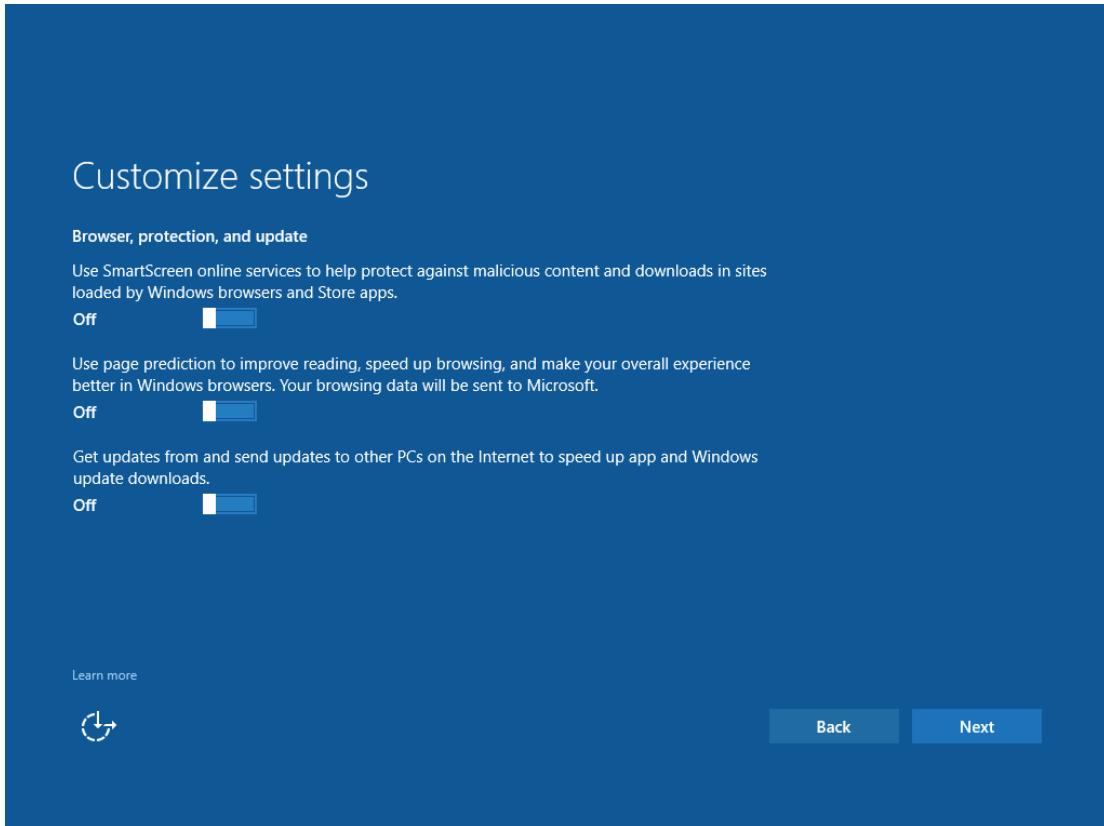


Figure Appendix 3-5 Customize settings Window - 4

Click Next to continue installing Windows 10 Enterprise 2016 LTSB.

Blank Page

CENTUM VP Installation

IM 33J01C10-01EN 9th Edition

INDEX

A

Adding a License.....C1-2

B

Backing Up.....C5-1
BKHBos.exe.....B5-38
Bus Converter.....B3-5

C

Cautionary Notes for Upgrading the CENTUM VP Version.....C11-1
CENTUM Authentication Mode.....B4-137
Changing the License Assignment.....C1-3
Communication Gateway Unit.....B3-13
Computer Dedicated to License Management. B7-1
Computer Name/Station Name.....B1-1
Control Bus Driver.....B4-44,C7-13
control bus interface card.....B4-2

D

Disk Defragmenter.....B4-11,B4-21,B4-26

E

ENG Group Users.....B4-140
Entry Class.....B4-71

F

File System.....B4-8,B4-15,B4-24,B4-36

H

Hardware Environment.....A3-1
HF Bus/RL Bus Interface Card.....B3-6
HIS Auto Start and Automatic Logon.....B4-84
HIS Group Users.....B4-143
HIS Type Single Sign On.....B4-145,C4-5

I

IP Address.....B1-1

L

License.....B4-101

O

Operation Keyboard.....B4-83

P

Password of Administrative User.....B1-2
PICOT.....C5-7
Processor Unit.....B3-2

R

RAS Driver.....B4-82,C7-18
Reinstalling.....C8-1
Remote Operation and Monitoring Function... B5-1
RemoteApp Programs.....B5-13,B5-35
Report Package.....C5-6
RS-232C Driver.....B4-79,C7-18

S

Security Model.....B1-2
Software Requirements.....A3-1
StartDesktop.bat.....B5-35
Subnet Mask.....B1-1

T

Tasks Required for Setting Up Console Type HIS B4-79
TCP/IP.....B4-69
Touch Panel.....B4-83
Troubleshooting.....C10-1

U

Uninstallation.....C7-1
Upgrade Installation from CENTUM CS 1000 to CENTUM VP R6.....C6-18
Upgrade Installation from CENTUM CS 3000 to CENTUM VP R6 C6-2
Upgrading from CENTUM VP R4/R5 to R6....C6-30

UPS (Uninterruptible Power Supply).....	B4-149
USB Driver for the Operation Keyboard (OPKB).....	B4-77,C7-17
User account.....	B4-102
User Authentication Mode.....	B4-135

V

V net Interface Card.....	B3-8
V net Router.....	B3-11
Virtual Memory.....	B4-8,B4-16,B4-24,B4-36

Vnet/IP interface card.....	B4-4
Vnet/IP Open Communication Driver...B4-46,C7-14	

W

Windows Authentication Mode.....	B4-139,C4-1
Windows Defender.....	B4-10,B4-19,B4-25
Windows Network Settings.....	B4-51
Windows Server 2008/Windows Server 2008 R2 Active Directory Domain Controller.....	B2-7

Revision Information

Title : CENTUM VP Installation

Manual No. : IM 33J01C10-01EN

Aug. 2019/9th Edition/R6.07 or later

- A2.2 Added descriptions.
- A2.2.1 Added descriptions.
- A2.2.13 Newly added.
- A3. Added descriptions.
- B1. Added and updated descriptions.
- B4. Added descriptions.
- B4.2 Added and updated descriptions.
- B4.3 Added and updated descriptions.
- B4.6 Added descriptions.
- B4.7 Added and deleted descriptions.
- B4.10 Added descriptions.
- B4.11.2 Updated descriptions.
- B5. Added descriptions.
- B5.1.1 Updated descriptions.
- B8.2.1 Added descriptions.
- B8.3.2 Updated descriptions.
- C6.1.1 Added descriptions.
- C6.1.2 Deleted descriptions.
- C6.4 Updated descriptions.
- C7.1 Added descriptions.
- C10.1.2 Deleted descriptions.
- C10.1.3 Deleted descriptions.
- C10.1.4 Deleted descriptions.
- C10.1.5 Deleted descriptions.
- C10.1.6 Deleted descriptions.
- C10.2.2 Deleted descriptions.
- C11.2.4 Updated descriptions.
- C11.21 Newly added.
- D1.1.1 Added and updated descriptions.
- D1.1.2 Updated descriptions.
- D1.1.3 Updated descriptions.
- D1.1.6 Updated descriptions.
- D1.2.1 Updated descriptions.
- D1.3.1 Updated and deleted descriptions.
- D1.3.2 Updated and deleted descriptions.

Aug. 2018/8th Edition/R6.06

- A2.2 Updated descriptions.
- A2.2.2 Newly added.
- A3. Updated descriptions.
- B1. Added descriptions.
- B2.6 Added descriptions.
- B4. Updated descriptions.
- B4.1 Updated descriptions.
- B4.2 Added descriptions.
- B4.3 Added and updated descriptions.
- B4.7 Updated descriptions.
- B4.10 Added and updated descriptions.
- B4.11.1 Updated descriptions.
- B5.1 Updated descriptions.
- B6. Updated descriptions.
- B8. Newly added.
- C6.1.1 Updated descriptions.
- C6.1.2 Updated descriptions.
- C6.1.3 Newly added.
- C6.3 Updated descriptions.
- C6.4 Updated descriptions.
- C7.1 Added descriptions.
- C7.1.4 Updated descriptions.
- C10.2 Added descriptions.
- C10.3.2 Added descriptions.
- C11.9 Added descriptions.
- C11.20 Added descriptions.
- D1.6.1 Added descriptions.
- Appendix 2. Updated descriptions.

Nov. 2017/7th Edition/R6.05

- B1. Added descriptions.
- B3.1 Added descriptions.
- B4.2 Updated descriptions.
- B4.2.2 Added descriptions.
- B4.2.4 Added descriptions.
- C2. Updated descriptions.
- C6.1.2 Added descriptions.
- C6.4 Added descriptions.
- C7.1 Added descriptions.
- C10.1 Updated descriptions.
- C11.15 Added and deleted descriptions.

C11.19 Newly added.

Apr. 2017/6th Edition/R6.04

General Descriptions of the Start menu are modified.
A2.2.10 Updated descriptions.
A3. Updated descriptions.
B1. Updated descriptions.
Entire B2. Added and modified descriptions.
B3.6 Added descriptions.
Entire B4. Added and modified descriptions.
Entire B5. Updated descriptions.
B6. Added descriptions.
B6.1 Updated descriptions.
B7. Added descriptions.
C5. Updated descriptions.
C5.2 Updated descriptions.
C6.3 Added descriptions.
C6.4 Added descriptions.
C6.5 Added descriptions.
C7.1 Updated descriptions.
C9. Updated descriptions.
C9.1 Updated descriptions.
C9.2 Newly added.
C9.3 Newly added.
Entire C10. Updated descriptions.
C10.1.7 Newly added.
C10.3.4 Newly added.
C11.18 Newly added.
D1. Updated descriptions.
D1.1.5 Newly added.
D1.1.6 Newly added.
Appendix 2. Newly added.

Sep. 2016/5th Edition/R6.03.10

A2.2 Updated descriptions.
A3. Updated descriptions.
B1. Added descriptions.
B2.5 Added descriptions.
B4. Updated descriptions.
B4.1 Updated descriptions.
B4.2 Updated descriptions.
B4.3 Added descriptions.

-
- B4.7 Added descriptions.
 - B4.10 Updated descriptions.
 - C11.16 Updated descriptions.
 - C11.17 Newly added.

Jun. 2016/4th Edition/R6.03

- A2.2 Added descriptions.
- A2.2.11 Newly added.
- A3. Updated descriptions.
- B2.5 Newly added.
- B3.6.2 Updated descriptions.
- B4.1 Updated descriptions.
- B4.2 Added descriptions.
- B4.2.3 Newly added.
- B4.3.1 Added descriptions.
- B4.3.2 Added descriptions.
- B4.3.3 Added descriptions.
- B4.3.5 Newly added.
- B4.6 Added descriptions.
- B4.10 Added descriptions.
- B4.10.3 Newly added.
- C6.4 Added descriptions.
- C6.7 Newly added.
- C10.1.7 Newly added.
- C11.16 Newly added.
- D1.1 Added descriptions.
- D1.1.1 Updated descriptions.
- D1.1.3 Updated descriptions.
- D1.1.4 Updated descriptions.
- D1.2.1 Updated descriptions.

Dec. 2015/3rd Edition/R6.02

- General Model names of the software media have been deleted.
- A3. Descriptions have been updated in "● Software that can Coexist with CENTUM VP."
- C6. Descriptions have been added.
- C6.4 Newly added.
- C11.15 Newly added.
- D1. Descriptions have been added to "● Package codes."
- D1.7 Newly added.

Apr. 2015/2nd Edition/R6.01.10

- C11.14 Newly added.

Mar. 2015/1st Edition/R6.01

Newly published.

■ For Questions and More Information

Online Query: A query form is available from the following URL.

<http://www.yokogawa.com/dcs/>

■ Written by Yokogawa Electric Corporation

■ Published by Yokogawa Electric Corporation

2-9-32 Nakacho, Musashino-shi, Tokyo 180-8750, JAPAN

Blank Page