CENTUM VP
Security Guide

IM 33J01C30-01EN

IM 33J01C30-01EN

9th Edition

Introduction

This manual is a guide for implementing security measures in the CENTUM VP system from a viewpoint of information technology (IT).

It explains security models and setting details of CENTUM VP. Please read this manual to learn about the details of security settings.

The intended readers of this manual are engineers who examine construction and operation of the CENTUM VP system.

9th Edition : Aug. 2019 (YK)

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:

  ```
  .ALΔPIC010Δ-SC
  ```

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

  Example:

  ```
  .PRΔTAG{Δ.sheet name}
  ```

Conventions Used to Show Key or Button Operations

- Characters enclosed by brackets [ ]
  When characters are enclosed by brackets in the description of a key or button operation, it indicates a key on the keyboard, a 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:

  Imax (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 Security Guide

IM 33J01C30-01EN 9th Edition

CONTENTS

1. Overview....................1-1

1.1 Security Threats to be Handled....................1-2

1.2 Security Measures....................1-3

2. Security Models....................2-1

2.1 Overview of Security Models....................2-2

2.2 User/Group Management....................2-12

2.2.1 User Management Methods....................2-13

2.2.2 CENTUM VP User Authentication Modes....................2-14

2.2.3 User/Group Management....................2-17

2.2.4 User Name and Password Policies....................2-25

2.2.5 Special User....................2-26

3. Details of Security Measures....................3-1

3.1 Access Control....................3-2

3.1.1 Access Permissions to Files and Folders....................3-3

3.1.2 Registry Configuration and User/Group....................3-7

3.1.3 DCOM (OPC) and User/Group....................3-11

3.1.4 Local Security and User/Group....................3-12

3.2 Personal Firewall Tuning....................3-13

3.3 Stopping Unused Window Services....................3-18

3.4 IT Environment Settings Common to IT Security Versions 2.0 and 1.0........ 3-20

3.4.1 Disabling NetBIOS over TCP/IP....................3-21

3.4.2 HDD Password Function by BIOS....................3-22

3.5 Group Policy Settings in IT Security Version 2.0....................3-23

3.5.1 Disabling the Built-in Administrator Account or Changing the User Name....................3-24

3.5.2 Applying the Software Restriction Policies....................3-25

3.5.3 Applying the StorageDevicePolicies Function....................3-27

3.5.4 Disabling USB Storage Devices....................3-28

3.5.5 Applying the Password Policies....................3-29

3.5.6 Advanced Audit Policy Configuration....................3-30

3.5.7 Applying the Account Lockout Policy....................3-33

3.5.8 User Rights Assignment....................3-34

3.5.9 Security Options..3-35

3.5.10 Administrative Template.. 3-37

3.5.11 User Configuration - Administrative Template............................3-45

3.6 Group Policy Settings in IT Security Version 1.0..................................3-46

3.6.1 Disabling the Built-in Administrator Account or Changing the User Name..3-47

3.6.2 Hiding the Last Logon User Name... 3-48

3.6.3 Applying the Software Restriction Policies.................................3-49

3.6.4 Applying AutoRun Restrictions..3-50

3.6.5 Applying the StorageDevicePolicies Function.............................3-51

3.6.6 Disabling USB Storage Devices...3-52

3.6.7 Changing the LAN Manager Authentication Level...................... 3-53

3.6.8 Applying the Password Policies.. 3-54

3.6.9 Applying the Audit Policy..3-55

3.6.10 Applying the Account Lockout Policy.. 3-56

4. Selection of Security Functions..4-1

4.1 Items to be Considered before Setting Security Functions.................... 4-2

4.2 Model Cases...4-5

5. Precautions on Operations...5-1

5.1 Windows Account Management..5-2

5.1.1 Common Account Management..5-3

5.1.2 Individual Account Management... 5-4

5.1.3 Common Precautions for Common Account Management/Individual Account Management... 5-5

5.2 Related Programs...5-6

5.3 Precautions regarding security when introducing and operating a CENTUM VP system.. 5-7

6. Utility Programs for Security Settings..6-1

6.1 IT Security Tool...6-2

6.2 Running the IT Security Tool...6-4

6.3 Changing the IT Security Settings.. 6-5

6.3.1 Procedure for Computers Installed with the CENTUM VP Software... 6-6

6.3.2 Procedures for a File Server or Domain Controller....................... 6-9

6.4 Saving the IT Security Settings...6-13

6.4.1 Procedure for Computers Installed with the CENTUM VP Software... 6-14

6.4.2 Procedure for a File Server or Domain Controller.......................6-17

6.5 Restoring the IT Security Settings...6-18

6.5.1 Procedure for Computers Installed with the CENTUM VP Software... 6-19

6.5.2 Procedure for a File Server or Domain Controller.......................6-21

6.6 Changing the Security Setting File Password....................................... 6-22

6.6.1 Procedure for Computers Installed with the CENTUM VP Software... 6-23

6.6.2 Procedure for a File Server or Domain Controller........................ 6-25

6.7 Importing/Exporting the IT Security Setting File.................................... 6-26

6.8 Viewing the Information Configured by the IT Security Tool..................6-28

6.9 Active Directory-Based Consolidated Management of IT Security Settings 6-29

6.9.1 Creating Group Policy Objects.. 6-30

6.9.2 Applying Group Policy Objects to an Organizational Unit............ 6-32

6.10 Other Utility Programs.. 6-34

6.10.1 CreateCentumProcess.. 6-35

6.10.2 CreateUgsProcess.. 6-36

6.10.3 CreateLicenseProcess.. 6-37

6.10.4 CreateAdsProcess... 6-38

6.10.5 CreateAdsAgent.. 6-39

6.10.6 CreateRDCProcess...6-40

6.10.7 CreateOffuser..6-41

6.10.8 YWVNETCreateVNTUser... 6-42

6.10.9 ChangeOffuserPassword.. 6-44

6.10.10 OFFUSEREnabler...6-45

6.10.11 OFFUSERDisabler..6-46

6.10.12 StorageDeviceCTL..6-47

6.10.13 ITSecuritySettingItemExport...6-49

Blank Page

CENTUM VP Security Guide

IM 33J01C30-01EN 9th Edition

CONTENTS

Appendix

Appendix 1. IT Security Setting Items..App.1-1

Appendix 1.1 IT Security Version 2.0..App.1-2

Appendix 1.1.1 Setting Items for a Computer with CENTUM VP Software Installed..App.1-3

Appendix 1.1.2 Setting Items for a File Server or Domain Controller................. .... App.1-12

Appendix 1.2 IT Security Version 1.0..App.1-24

Appendix 1.2.1 Setting Items for a Computer with CENTUM VP Software Installed..App.1-25

Appendix 1.2.2 Setting Items for a File Server or Domain Controller................. .... App.1-28

Blank Page

1. Overview

This manual is a guide for implementing security measures on the product and for its operation.

By operating the system with security measures implemented, the product is protected from existing and future security threats.

The security models described in this manual are based on general configuration of the product. You must consider engineering and operation practices when applying these models to the actual systems.

■ Security-related Terms Used in the Manual

The following table describes the security-related terms.

Table 1-1 Security-related Terms

Term	Explanation
IT security	Security measures considered based on given IT environment, in order to protect the system and handle current and future security threats including cyber terrorism.
User authentication mode	A function that prescribes user management method of Windows user and users used in CENTUM VP. There are two modes: Windows authentication mode and CENTUM authentication mode.
CENTUM authentication mode	One of user authentication modes. In this mode, users used in CENTUM VP as well as their access permissions are managed independently in CENTUM VP.
Windows authentication mode	One of user authentication modes. This mode links credentials of Windows users and CENTUM VP users. There are two ways to sign on the HIS, by Windows Type Single Sign On or HIS Type Single Sign On.
HIS Type Single Sign On	A user sign on type that when Windows authentication mode is selected as the user authentication mode, the user sign on will be performed on HIS user-in dialog box.
Windows Type Single Sign On	A user sign on type that when Windows authentication mode is selected as the user authentication mode, the user sign on will be performed on Windows logon dialog box.
Kerberos authentication	The default authentication method of Windows domain and it is used in a domain environment where the server and client PCs are mixed for single sign on. Once a user is authenticated; the authentication will be valid for entire system.
Personal firewall	Firewall operating on PC and domain controllers, including firewalls other than the Windows standard firewall.
Two-factor authentication	Two-factor authentication means using two types of authentication methods to authenticate a user: for example, authentication by fingerprint and password. Performing the same type of authentication twice, such as to perform password authentication twice, is not called two-factor authentication.
Security Zone	A security zone is a physical or logical area where only permitted users can access. Equipment and facilities in a security zone require special management and are insulated from other areas.

1.1 Security Threats to be Handled

This section describes the security threats that the security functions of the product should deal with.

■ Security Threats

The security threats that can harm the CENTUM VP system are as follows:

1. Attacks over the network
   Threats to the CENTUM VP system from people without any rights to the CENTUM VP system via networks such as intranets, as well as the resultant threats of leakage of important data of the CENTUM VP system.
2. Direct attack to a system by operating on an HIS or on a PC installed with system builders
   Threats from unauthorized individuals to the CENTUM VP system by directly operating an HIS or the PC installed with system builders to affect the system for the purpose of stealing important data.
3. Theft of an HIS or PC installed with system builders or theft of data
   Threats where an HIS or PC installed with system builders is stolen or data are stolen from it for the purpose of analyzing the data.

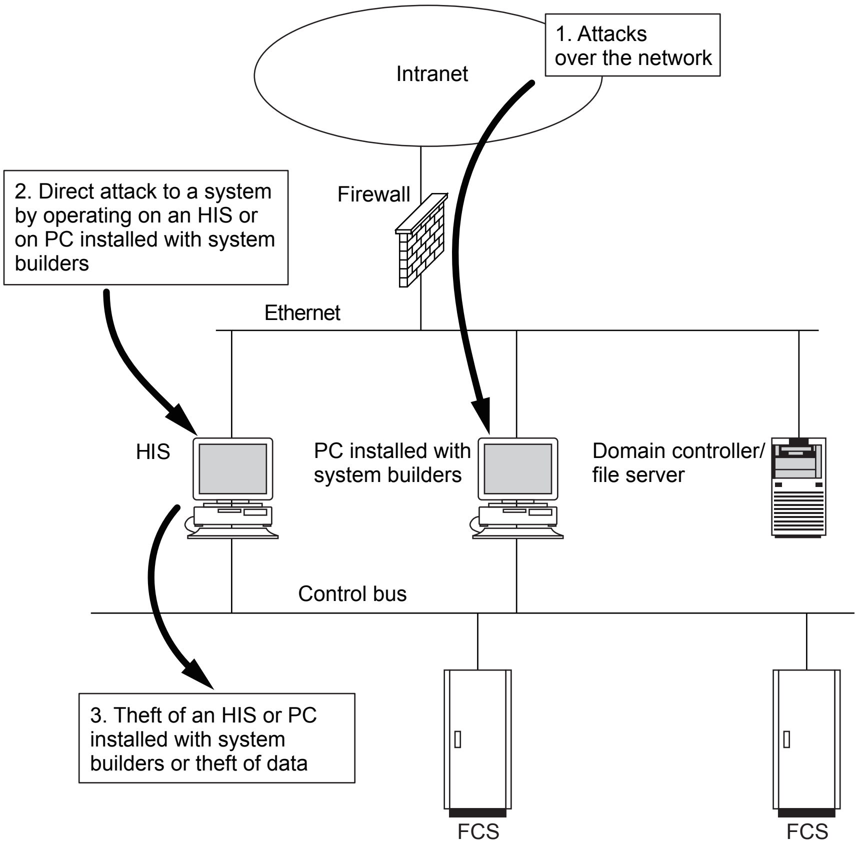

1. Attacks over the network
Intranet
2. Direct attack to a system by operating on an HIS or on PC installed with system builders
Firewall
Ethernet
HIS
PC installed with system builders
Domain controller/ file server
Control bus
3. Theft of an HIS or PC installed with system builders or theft of data
FCS
FCS

Figure 1.1-1 Security Threats

1.2 Security Measures

This section describes the security measures against security threats. Identify security measure items required for the product and, from among them, select the required security measures according to the level of security strength.

■ Security Measures and Handled Security Threats

In order to fight against security threats, we arranged security measures applied in security guides for each OS issued by Microsoft and general business network environment and optimized as a set of security measures for the product. Two IT security versions, 2.0 and 1.0, are available, which provide security measures that cover different ranges. These two versions are described as follows.

- IT security version 2.0
  This version was designed after reconsidering the IT security version1.0 and includes more security measures. It supports the Standard and Strengthened security models.
- IT security version 1.0
  This version had been offered as the security measures of CENTUM VP R6.03 and earlier versions. It supports the Legacy, Standard, and Strengthened security models.

IT security version 2.0 and IT security version1.0 can coexist in the same project.

The following tables show the security measures and the threats that each measure handles for each security version.

[1]: Attacks over the network

[2]: Direct attacks by operation of HIS or computer with system builders

[3]: Theft of HIS or computer with system builders or theft of data

Table 1.2-1 Security Measures and Handled Threats - IT security version 2.0

Security measure	Threat handled		
	[1]	[2]	[3]
Password Policy-[Minimum password length]	Yes	Yes	No
Password Policy-[Minimum password age]	Yes	Yes	No
Password Policy-[Maximum password age]	Yes	Yes	No
Password Policy-[Enforce password history]	Yes	Yes	No
Disable ‘Password Policy-[Store passwords using reversible encryption]'	Yes	Yes	No
Password Policy-[Password must meet complexity requirements]	Yes	Yes	No
Access Control for files and folders	Yes	Yes	No
Access control for product registry	Yes	Yes	No
Access Control for DCOM (OPC) objects	Yes	Yes	No
Personal firewall tuning	Yes	No	No
Set 'Personal Firewall-[Allow unicast response]’ to ‘No’	Yes	No	No
Stopping unused Windows services	Yes	No	No
Account Lockout Policy-[Account lockout threshold]	Yes	Yes	No
Account Lockout Policy-[Reset account lockout counter after]	Yes	Yes	No
Account Lockout Policy-[Account lockout duration]	Yes	Yes	No
Disabling NetBIOS over TCP/IP	Yes	No	No

Continues on the next page

Table 1.2-1 Security Measures and Handled Threats - IT security version 2.0 (Table continued)

Security measure	Threat handled		
	[1]	[2]	[3]
Applying the StorageDevicePolicies function	No	Yes	Yes
Disabling USB storage devices	No	Yes	Yes
Applying the software restriction policies	Yes	Yes	No
User Rights Assignment-[Access this computer from the network]	Yes	No	No
User Rights Assignment-[Add workstations to domain]	Yes	Yes	No
User Rights Assignment-[Allow log on locally]	No	Yes	No
User Rights Assignment-[Deny log on locally]	No	Yes	No
Security Options-[Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings]	Yes	Yes	No
Security Options-[Devices: Prevent users from installing printer drivers]	No	Yes	No
Security Options-[Devices: Restrict CD-ROM access to locally logged-on user only]	Yes	No	No
Security Options-[Devices: Restrict floppy access to locally logged-on user only]	Yes	No	No
Disable 'Security Options-[Domain controller: Allow server operators to schedule tasks]’	No	Yes	No
Disable 'Security Options-[Domain controller: Refuse machine account password changes]’	No	Yes	No
Security Options-[Domain member: Require strong (Windows 2000 or later) session key]	Yes	No	No
Set 'Security Options-[Interactive logon: Display user information when the session is locked]' to 'Do not display user information’	No	Yes	No
Security Options-[Interactive logon: Do not display last user name]	No	Yes	No
Disable 'Security Options-[Interactive logon: Do not require CTRL+ALT+DEL]’	No	Yes	No
Security Options-[Interactive logon: Machine inactivity limit]	No	Yes	No
Security Options-[Interactive logon: Prompt user to change password before expiration]	Yes	Yes	No
Security Options-[Microsoft network server: Digitally sign communications (if client agrees)]	Yes	No	No
Security Options-[Microsoft network server: Server SPN target name validation level]	Yes	No	No
[MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)]	Yes	No	No
Disable [MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)]	Yes	No	No
[MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)]	Yes	No	No
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts]	Yes	No	No

Continues on the next page

Table 1.2-1 Security Measures and Handled Threats - IT security version 2.0 (Table continued)

Security measure	Threat handled		
	[1]	[2]	[3]
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts and shares]	Yes	No	No
Security Options-[Network access: Do not allow storage of passwords and credentials for network authentication]	Yes	No	No
Security Options-[Network security: Allow Local System to use computer identity for NTLM]	Yes	No	No
Disable 'Security Options-[Network security: Allow LocalSystem NULL session fallback]'	Yes	No	No
Security Options-[Network security: Force logoff when logon hours expire]	No	Yes	No
Security Options-[Network security: LAN Manager authentication level]	Yes	No	No
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) clients]	Yes	No	No
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) servers]	Yes	No	No
Disable 'Security Options-[Shutdown: Allow system to be shut down without having to log on]'	No	Yes	No
Security Options-[User Account Control: Admin Approval Mode for the Built'-in Administrator account]	No	Yes	No
Security Options-[User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode]	No	Yes	No
Advanced Audit Policy Configuration-[Audit Credential Validation]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Computer Account Management]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Other Account Management Events]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Security Group Management]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit User Account Management]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Process Creation]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Directory Service Access]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Directory Service Changes]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Account Lockout]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Logoff]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Logon]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Other Logon/Logoff Events]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Special Logon]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Removable Storage]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Audit Policy Change]	Yes	Yes	No

Continues on the next page

Table 1.2-1 Security Measures and Handled Threats - IT security version 2.0 (Table continued)

Security measure	Threat handled		
	[1]	[2]	[3]
Advanced Audit Policy Configuration-[Audit Authentication Policy Change]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Filtering Platform Policy Change]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit MPSSVC Rule-Level Policy Change]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Other Policy Change Events]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Sensitive Privilege Use]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit IPsec Driver]	No	Yes	No
Advanced Audit Policy Configuration-[Audit Other System Events]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Security State Change]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit Security System Extension]	Yes	Yes	No
Advanced Audit Policy Configuration-[Audit System Integrity]	Yes	Yes	No
Personalization-[Prevent enabling lock screen camera]	No	Yes	No
Personalization-[Prevent enabling lock screen slide show]	No	Yes	No
WLAN Settings-[Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services]	Yes	No	No
SCM-[Enable LSA Protection]	Yes	Yes	No
SCM-[Lsass.exe audit mode]	Yes	Yes	No
Group Policy-[Configure registry policy processing]	Yes	Yes	No
Internet Communication settings-[Turn off downloading of print drivers over HTTP]	Yes	No	No
Internet Communication settings-[Turn off Event Viewer "Events.asp" links]	Yes	No	No
Internet Communication settings-[Turn off Internet download for Web publishing and online ordering wizards]	Yes	No	No
Internet Communication settings-[Turn off printing over HTTP]	Yes	No	No
Internet Communication settings-[Turn off Search Companion content file updates]	Yes	No	No
Internet Communication settings-[Turn off the "Publish to Web" task for files and folders]	Yes	No	No
Internet Communication settings-[Turn off the Windows Customer Experience Improvement Program]	Yes	No	No
Internet Communication settings-[Turn off the Windows Messenger Customer Experience Improvement Program]	Yes	No	No
Logon-[Do not display network selection UI]	Yes	Yes	No
Logon-[Do not enumerate connected users on domain-joined computers]	No	Yes	No
Logon-[Do not process the legacy run list]	No	Yes	No
Logon-[Do not process the run once list]	No	Yes	No

Continues on the next page

Table 1.2-1 Security Measures and Handled Threats - IT security version 2.0 (Table continued)

Security measure	Threat handled		
	[1]	[2]	[3]
Disable 'Logon-[Enumerate local users on domain-joined computers]'	No	Yes	No
Logon-[Turn off app notifications on the lock screen]	No	Yes	No
Mitigation Options-[Untrusted Font Blocking]	Yes	Yes	No
Remote Procedure Call-[Enable RPC Endpoint Mapper Client Authentication]	Yes	Yes	No
User Profiles-[Turn off the advertising ID]	Yes	No	No
App Privacy-[Let Windows apps access account information]	Yes	No	No
App Privacy-[Let Windows apps access call history]	Yes	No	No
App Privacy-[Let Windows apps access contacts]	Yes	No	No
App Privacy-[Let Windows apps access email]	Yes	No	No
App Privacy-[Let Windows apps access location]	Yes	No	No
App Privacy-[Let Windows apps access messaging]	Yes	No	No
App Privacy-[Let Windows apps access motion]	Yes	No	No
App Privacy-[Let Windows apps access the calendar]	Yes	No	No
App Privacy-[Let Windows apps access the camera]	Yes	No	No
App Privacy-[Let Windows apps access the microphone]	Yes	No	No
App Privacy-[Let Windows apps access trusted devices]	Yes	No	No
App Privacy-[Let Windows apps control radios]	Yes	No	No
App Privacy-[Let Windows apps sync with devices]	Yes	No	No
App runtime-[Block launching Windows Store apps with Windows Runtime API access from hosted content]	Yes	No	No
AutoPlay Policies-[Turn off Autoplay]	No	Yes	No
AutoPlay Policies-[Disallow Autoplay for non-volume devices]	No	Yes	No
Data Collection and Preview Builds-[Allow Telemetry]	Yes	No	No
Data Collection and Preview Builds-[Do not show feedback notifications]	Yes	No	No
Event Log Service(Application)-[Specify the maximum log file size (KB)]	Yes	Yes	No
Event Log Service(Security)-[Specify the maximum log file size (KB)]	Yes	Yes	No
Event Log Service(System)-[Specify the maximum log file size (KB)]	Yes	Yes	No
File Explorer-[Turn off heap termination on corruption]	No	Yes	No
HomeGroup-[Prevent the computer from joining a homegroup]	Yes	No	No
OneDrive-[Prevent the usage of OneDrive for file storage]	Yes	No	No
OneDrive-[Save documents to OneDrive by default](Save documents to the local PC by default)	Yes	No	No
Remote Desktop Connection Client-[Do not allow passwords to be saved]	Yes	No	No
Device and Resource Redirection-[Do not allow drive redirection]	Yes	No	No

Continues on the next page

Table 1.2-1 Security Measures and Handled Threats - IT security version 2.0 (Table continued)

Security measure	Threat handled		
	[1]	[2]	[3]
Security-[Always prompt for password upon connection]	Yes	No	No
Security-[Require secure RPC communication]	Yes	No	No
Security-[Require user authentication for remote connections by using Network Level Authentication]	Yes	No	No
Session Time Limits-[Set time limit for active but idle Remote Desktop Services sessions]	Yes	No	No
Sync your settings-[Do not sync Apps]	Yes	No	No
Sync your settings-[Do not sync start settings]	Yes	No	No
Disable 'Windows Error Reporting-[Automatically send memory dumps for OS-generated error reports]'	Yes	No	No
Disable 'Windows Logon Options-[Sign'-in last interactive user automatically after a system'-initiated restart]'	No	Yes	No
Notifications-[Turn off toast notifications on the lock screen]	No	Yes	No
Disabling Built-in Administrator Account or Changing User Name	Yes	Yes	No
HDD password function by BIOS	No	No	Yes

Table 1.2-2 Security Measures and Handled Threats - IT security version 1.0

Security measure	Threat handled		
	[1]	[2]	[3]
Access control	Yes	Yes	No
Personal firewall tuning	Yes	No	No
Stopping unused Windows services	Yes	No	No
Disabling the built-in Administrator account or changing its user name	Yes	Yes	No
Hiding the last logon user name	Yes	Yes	No
Applying the software restriction policies	Yes	Yes	No
Applying AutoRun restrictions	No	Yes	No
Applying the StorageDevicePolicies function	No	Yes	Yes
Disabling USB storage devices	No	Yes	Yes
Disabling NetBIOS over TCP/IP	Yes	No	No
Changing the LAN Manager authentication level	Yes	No	No
Applying the password policy	Yes	Yes	No
Applying the audit policy	Yes	Yes	No
Applying the account lockout policy	Yes	Yes	No
HDD password function by BIOS	No	No	Yes

2. Security Models

The product provides three types of security models, Legacy model, Standard model, and Strengthened model, according to the required security strength, in order to flexibly accommodate system configuration and operation. Required security measure items are incorporated in the security models.

2.1 Overview of Security Models

This section describes the features of security models and the relationship between security models and their corresponding security measures.

■ Security Models

The features of the three security models, Legacy model, Standard model, and Strengthened model, are as follows:

- Legacy model
  This model does not strengthen security. Use this model when you connect the system with YOKOGAWA products that do not support security measures.
- Standard model
  This model places importance on operation of the product and collaboration with other systems (Exaopc, ProSafe-RS, and so on) to guard against "attacks over the network" and "direct attack to a system by operating on an HIS or on a computer with system builders." The Standard model does not guard against "Theft of HIS or computer with system builders or theft of data" because its threat is considered minor due to the characteristics of the product.
- Strengthened model
  This model takes all measures against any security treats. If all security measures are taken, operation and so on may be affected. Take measures according to the characteristics of each system for non-mandatory items.

IMPORTANT

Please consult YOKOGAWA if IT security of the Strengthened model is required.

■ Security Models and Security Measures

As a security measure for CENTUM VP, the IT Security Tool is provided. Using the IT Security Tool, you can implement security measures on each computer.

If you want to implement consolidated security measures under a domain environment, you can also use the group policy objects (referred to as GPOs in this chapter) provided by YOKOGAWA together.

IMPORTANT

Even if you are intending to implement GPO file based security measures, you must configure the security settings by running the IT Security Tool in advance. Note that the security configuration by the GPO file overrides the security configuration by the IT Security Tool.

With security configuration using the IT Security Tool, settings of some security measure items differ, depending on the differences in the IT Security Tool version and the security model. In addition, IT security version 2.0 includes some security measure items to be configured for the purpose to match the product specification rather than to fight against security threats.

SEE ALSO

For more information about security measures, refer to:

3., “Details of Security Measures” on page 3-1

For more information about creating a GPO file, refer to:

6.9.1, “Creating Group Policy Objects” on page 6-30

For more information about applying a GPO file, refer to:

6.9.2, “Applying Group Policy Objects to an Organizational Unit” on page 6-32

● Security Measures to Fight Against Security Threats

The following table shows the security measure items against security threats and their configuration in IT security version 2.0.

“Defined/Not defined” in the Configuration by GPO file column indicates whether the security measure item is defined to be configured in the GPO file that is created based on the group policy provided by YOKOGAWA.

- Defined
  The security measure, which is adopted by YOKOGAWA, is defined in the GPO file.
- Not defined
  The security measure is not defined in the GPO file.

“Applied/Not applied” in the Configuration by IT Security Tool column indicates whether the security measure item is configured by the IT Security Tool, applying the predefined setting, for each security model.

- Applied
  The security measure, which is adopted by YOKOGAWA, is configured by the IT Security Tool so that it is applied.
- Not applied
  Because YOKOGAWA decided not to adopt the security measure, it is configured by the IT Security Tool so as not to be applied.

TIP

The setting values set by the IT Security Tool can be changed by the user for some security measure items and cannot be changed for others. To find out which security measure items can be changed, refer to the appendix.

Table 2.1-1 Security Measures in IT Security Version 2.0

Security measure	Configuration by GPO file	Configuration by IT Security Tool	
		Standard model	Strengthened model
Password Policy-[Minimum password length]	Defined	Not applied	Applied
Password Policy-[Minimum password age]	Defined	Not applied	Applied
Password Policy-[Maximum password age]	Defined	Not applied	Applied
Password Policy-[Enforce password history]	Defined	Not applied	Applied
Disable ‘Password Policy-[Store passwords using reversible encryption]’	Defined	Not applied	Applied
Password Policy-[Password must meet complexity requirements]	Defined	Not applied	Applied
Access control for files and folders (*1)	Not defined	Applied	Applied
Access control for product registry (*1)	Not defined	Applied	Applied
Access control for DCOM (OPC) objects (*1)	Not defined	Applied	Applied

Continues on the next page

Table 2.1-1 Security Measures in IT Security Version 2.0 (Table continued)

Security measure	Configuration by GPO file	Configuration by IT Security Tool	
		Standard model	Strengthened model
Personal Firewall tuning (*2)	Not defined	Applied	Applied
Set 'Personal Firewall-[Allow unicast response]' to ‘No’ (*3)	Not defined	Applied	Applied
Stopping unused Windows services (*2)	Not defined	Not applied	Applied
Account Lockout Policy-[Account lockout threshold]	Defined	Not applied	Applied
Account Lockout Policy-[Reset account lockout counter after]	Defined	Not applied	Applied
Account Lockout Policy-[Account lockout duration]	Defined	Not applied	Applied
Disabling NetBIOS over TCP/IP (*1)	Not defined	Applied (*4)	Applied (*4)
Applying the StorageDevicePolicies function	Defined	Applied	Applied
Disabling USB storage devices	Defined	Applied	Applied
Applying the software restriction policies	Not defined	Applied	Applied
User Rights Assignment-[Access this computer from the network]	Not defined	Applied(*5)(*6)	Applied(*5)(*6)
User Rights Assignment-[Add workstations to domain]	Not defined	Applied (*5)	Applied (*5)
User Rights Assignment-[Allow log on locally]	Not defined	Applied(*6)	Applied
User Rights Assignment-[Deny log on locally]	Not defined	Applied	Applied
Security Options-[Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings]	Defined	Applied	Applied
Security Options-[Devices: Prevent users from installing printer drivers]	Defined	Applied	Applied
Security Options-[Devices: Restrict CD-ROM access to locally logged-on user only]	Defined	Applied	Applied
Security Options-[Devices: Restrict floppy access to locally logged-on user only]	Defined	Applied	Applied
Disable 'Security Options-[Domain controller: Allow server operators to schedule tasks]’	Not defined	Applied (*5)	Applied (*5)
Disable 'Security Options-[Domain controller: Refuse machine account password changes]’	Not defined	Applied (*5)	Applied (*5)
Security Options-[Domain member: Require strong (Windows 2000 or later) session key]	Defined	Applied	Applied
Set 'Security Options-[Interactive logon: Display user information when the session is locked]' to 'Do not display user information’	Defined	Not applied	Applied
Security Options-[Interactive logon: Do not display last user name]	Defined	Applied	Applied
Disable 'Security Options-[Interactive logon: Do not require CTRL+ALT+DEL]’	Defined	Applied	Applied
Security Options-[Interactive logon: Machine inactivity limit]	Not defined	Applied(*6)	Applied(*6)
Security Options-[Interactive logon: Prompt user to change password before expiration]	Defined	Applied	Applied
Security Options-[Microsoft network server: Digitally sign communications (if client agrees)]	Defined	Applied	Applied

Continues on the next page

Table 2.1-1 Security Measures in IT Security Version 2.0 (Table continued)

Security measure	Configuration by GPO file	Configuration by IT Security Tool	
		Standard model	Strengthened model
Security Options-[Microsoft network server: Server SPN target name validation level]	Defined	Applied	Applied
[MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)]	Not defined	Applied	Applied
Disable [MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)]	Not defined	Applied	Applied
[MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)]	Not defined	Applied	Applied
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts]	Defined	Applied	Applied
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts and shares]	Defined	Applied	Applied
Security Options-[Network access: Do not allow storage of passwords and credentials for network authentication]	Defined	Applied	Applied
Security Options-[Network security: Allow Local System to use computer identity for NTLM]	Defined	Applied	Applied
Disable 'Security Options-[Network security: Allow LocalSystem NULL session fallback]’	Defined	Applied	Applied
Security Options-[Network security: Force logoff when logon hours expire]	Not defined	Applied (*5)	Applied (*5)
Security Options-[Network security: LAN Manager authentication level]	Defined	Applied	Applied
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) clients]	Defined	Applied	Applied
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) servers]	Defined	Applied	Applied
Disable 'Security Options-[Shutdown: Allow system to be shut down without having to log on]'	Defined	Applied	Applied
Security Options-[User Account Control: Admin Approval Mode for the Built-in Administrator account]	Defined	Applied	Applied
Security Options-[User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Credential Validation]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Computer Account Management]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Other Account Management Events]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Security Group Management]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit User Account Management]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Process Creation]	Defined	Applied	Applied

Continues on the next page

Table 2.1-1 Security Measures in IT Security Version 2.0 (Table continued)

Security measure	Configuration by GPO file	Configuration by IT Security Tool	
		Standard model	Strengthened model
Advanced Audit Policy Configuration-[Audit Directory Service Access]	Not defined	Applied (*5)	Applied (*5)
Advanced Audit Policy Configuration-[Audit Directory Service Changes]	Not defined	Applied (*5)	Applied (*5)
Advanced Audit Policy Configuration-[Audit Account Lockout]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Logoff]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Logon]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Other Logon/ Logoff Events]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Special Logon]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Removable Storage]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Audit Policy Change]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Authentication Policy Change]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Filtering Platform Policy Change]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit MPSSVC Rule-Level Policy Change]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Other Policy Change Events]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Sensitive Privilege Use]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit IPsec Driver]	Not defined	Applied (*5)	Applied (*5)
Advanced Audit Policy Configuration-[Audit Other System Events]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Security State Change]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Security System Extension]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit System Integrity]	Defined	Applied	Applied
Personalization-[Prevent enabling lock screen camera]	Defined	Applied	Applied
Personalization-[Prevent enabling lock screen slide show]	Defined	Applied	Applied
WLAN Settings-[Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services] (*7)	Defined	Applied	Applied
SCM-[Enable LSA Protection] (*7)	Defined	Not applied	Applied
SCM-[Lsass.exe audit mode] (*7)	Defined	Not applied	Applied
Group Policy-[Configure registry policy processing]	Defined	Applied	Applied
Internet Communication settings-[Turn off downloading of print drivers over HTTP]	Defined	Applied	Applied

Continues on the next page

Table 2.1-1 Security Measures in IT Security Version 2.0 (Table continued)

Security measure	Configuration by GPO file	Configuration by IT Security Tool	
		Standard model	Strengthened model
Internet Communication settings-[Turn off Event Viewer "Events.asp" links]	Defined	Applied	Applied
Internet Communication settings-[Turn off Internet download for Web publishing and online ordering wizards]	Defined	Applied	Applied
Internet Communication settings-[Turn off printing over HTTP]	Defined	Applied	Applied
Internet Communication settings-[Turn off Search Companion content file updates]	Defined	Applied	Applied
Internet Communication settings-[Turn off the "Publish to Web" task for files and folders]	Defined	Applied	Applied
Internet Communication settings-[Turn off the Windows Customer Experience Improvement Program]	Defined	Applied	Applied
Internet Communication settings-[Turn off the Windows Messenger Customer Experience Improvement Program]	Defined	Applied	Applied
Logon-[Do not display network selection UI]	Defined	Applied	Applied
Logon-[Do not enumerate connected users on domain-joined computers]	Defined	Applied	Applied
Logon-[Do not process the legacy run list]	Defined	Not applied	Applied
Logon-[Do not process the run once list]	Defined	Not applied	Applied
Disable 'Logon-[Enumerate local users on domain-joined computers]'	Defined	Applied	Applied
Logon-[Turn off app notifications on the lock screen]	Defined	Applied	Applied
Mitigation Options-[Untrusted Font Blocking]	Defined	Applied	Applied
Remote Procedure Call-[Enable RPC Endpoint Mapper Client Authentication]	Defined	Not applied	Applied
User Profiles-[Turn off the advertising ID]	Defined	Applied	Applied
App Privacy-[Let Windows apps access account information]	Defined	Applied	Applied
App Privacy-[Let Windows apps access call history]	Defined	Applied	Applied
App Privacy-[Let Windows apps access contacts]	Defined	Applied	Applied
App Privacy-[Let Windows apps access email]	Defined	Applied	Applied
App Privacy-[Let Windows apps access location]	Defined	Applied	Applied
App Privacy-[Let Windows apps access messaging]	Defined	Applied	Applied
App Privacy-[Let Windows apps access motion]	Defined	Applied	Applied
App Privacy-[Let Windows apps access the calendar]	Defined	Applied	Applied
App Privacy-[Let Windows apps access the camera]	Defined	Applied	Applied
App Privacy-[Let Windows apps access the microphone]	Defined	Applied	Applied
App Privacy-[Let Windows apps access trusted devices]	Defined	Applied	Applied
App Privacy-[Let Windows apps control radios]	Defined	Applied	Applied
App Privacy-[Let Windows apps sync with devices]	Defined	Applied	Applied
App runtime-[Block launching Windows Store apps with Windows Runtime API access from hosted content]	Defined	Applied	Applied
AutoPlay Policies-[Turn off Autoplay]	Defined	Applied	Applied

Continues on the next page

Table 2.1-1 Security Measures in IT Security Version 2.0 (Table continued)

Security measure	Configuration by GPO file	Configuration by IT Security Tool	
		Standard model	Strengthened model
AutoPlay Policies-[Disallow Autoplay for non-volume devices]	Defined	Applied	Applied
Data Collection and Preview Builds-[Allow Telemetry]	Defined	Applied	Applied
Data Collection and Preview Builds-[Do not show feedback notifications]	Defined	Applied	Applied
Event Log Service(Application)-[Specify the maximum log file size (KB)]	Defined	Applied	Applied
Event Log Service(Security)-[Specify the maximum log file size (KB)]	Defined	Applied	Applied
Event Log Service(System)-[Specify the maximum log file size (KB)]	Defined	Applied	Applied
File Explorer-[Turn off heap termination on corruption]	Defined	Applied	Applied
HomeGroup-[Prevent the computer from joining a homegroup]	Defined	Applied	Applied
OneDrive-[Prevent the usage of OneDrive for file storage]	Defined	Applied	Applied
OneDrive-[Save documents to OneDrive by default] (Save documents to the local PC by default)	Defined	Applied	Applied
Remote Desktop Connection Client-[Do not allow passwords to be saved]	Defined	Applied	Applied
Device and Resource Redirection-[Do not allow drive redirection] (*3)	Defined (*8)	Applied	Applied
Security-[Always prompt for password upon connection]	Not defined	Applied(*6)	Applied(*6)
Security-[Require secure RPC communication]	Defined	Applied	Applied
Security-[Require user authentication for remote connections by using Network Level Authentication]	Defined	Applied	Applied
Session Time Limits-[Set time limit for active but idle Remote Desktop Services sessions]	Not defined	Applied(*6)	Applied(*6)
Sync your settings-[Do not sync Apps]	Defined	Applied	Applied
Sync your settings-[Do not sync start settings]	Defined	Applied	Applied
Disable 'Windows Error Reporting-[Automatically send memory dumps for OS-generated error reports]'	Defined	Applied	Applied
Disable 'Windows Logon Options-[Sign'-in last interactive user automatically after a system'-initiated restart]'	Defined	Applied	Applied
Notifications-[Turn off toast notifications on the lock screen]	Defined	Applied	Applied
Disabling the built-in Administrator account or changing its user name	Not defined	Not applied	The IT Security Tool does not configure this setting. You must configure it manually.
HDD password function by BIOS (*1)	Not defined	Not applied	The IT Security Tool does not configure this setting. You must configure it manually.

*1: This security setting item is not affected by group policy

*2: This setting can be controlled by group policy but can also be configured for each computer using the IT Security Tool.

*3: This setting is not configured on UGS.

*4: If the network connection name is "UACS Ethernet," set disabling NetBIOS over TCP/IP regardless of the security model or user management.

*5: Configure this setting in the domain controller.

*6: This setting is configured on the UACS station.

*7: If you want to change the setting value in Active Directory-based consolidated management, select either “Enabled” or “Disabled” for this item.

*8: This security setting item is not included in the YOKOGAWA GPO file for UGS which is provided for consolidated management using Active Directory.

TIP

With IT security version 2.0, different security setting items are configured among stations, file server, and domain controller.

● Security Measures to Match the Product Specification

The following table shows the security measure items to match the product specification and their configuration in IT security version 2.0.

“Defined/Not defined” in the Configuration by GPO file column indicates whether the security measure item is defined to be configured in the GPO file that is created based on the group policy provided by YOKOGAWA.

- Defined
  The security measure, which is adopted by YOKOGAWA, is defined in the GPO file.
- Not defined
  The security measure is not defined in the GPO file.

“Applied/Not applied” in the Configuration by IT Security Tool column indicates whether the security measure item is configured by the IT Security Tool, applying the predefined setting, for each security model.

- Applied

  The security measure, which is adopted by YOKOGAWA, is configured by the IT Security Tool so that it is applied.
- Not applied

  Because YOKOGAWA decided not to adopt the security measure, it is configured by the IT Security Tool so as not to be applied.

Table 2.1-2 Security Measures Configured to Match the Product Specification in IT Security Version 2.0

Security measure	Configuration by GPO file	Configuration by IT Security Tool	
		Standard model	Strengthened model
User Rights Assignment-[Create global objects]	Not defined	Applied	Applied
User Rights Assignment-[Log on as a batch job]	Not defined	Applied	Applied
User Rights Assignment-[Log on as a service]	Not defined	Applied	Applied
[MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended except for highly secure environments)]	Not defined	Applied	Applied
Security Options-[Network access: Let Everyone permissions apply to anonymous users]	Not defined	Applied	Applied
Security Options-[Network security: Do not store LAN Manager hash value on next password change]	Not defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit RPC Events]	Defined	Applied	Applied
Advanced Audit Policy Configuration-[Audit Application Generated]	Defined	Applied	Applied

Continues on the next page

Table 2.1-2 Security Measures Configured to Match the Product Specification in IT Security Version 2.0 (Table continued)

Security measure	Configuration by GPO file	Configuration by IT Security Tool	
		Standard model	Strengthened model
Disable ‘Audit Process Creation-[Include command line in process creation events]’	Defined	Applied	Applied
Internet Communication settings-[Turn off access to the Store]	Defined	Applied	Applied
Video and Display Settings-[Turn Off the Display (On Battery)]	Defined	Applied (*1)	Applied (*1)
Video and Display Settings-[Turn Off the Display (Plugged In)]	Defined	Applied (*1)	Applied (*1)
Cloud Content-[Do not show Windows Tips]	Defined	Applied	Applied
Cloud Content-[Turn off Microsoft consumer experiences]	Defined	Applied	Applied
Data Collection and Preview Builds-[Disable pre-release features or settings]	Defined	Applied	Applied
Data Collection and Preview Builds-[Toggle user control over Insider builds]	Defined	Applied	Applied
Disable ‘Search-[Allow Cortana]’	Defined	Applied	Applied
Search-[Don't search the web or display web results in Search]	Defined	Applied	Applied
Search-[Don't search the web or display web results in Search over metered connections]	Defined	Applied	Applied
Software Protection Platform-[Turn off KMS Client Online AVS Validation]	Defined	Applied	Applied
Store-[Turn off Automatic Download and Install of updates]	Defined	Applied	Applied
Store-[Turn off Automatic Download of updates on Win8 machines]	Defined	Applied	Applied
Store-[Turn off the offer to update to the latest version of Windows]	Defined	Applied	Applied
Store-[Turn off the Store application]	Defined	Applied	Applied
Endpoint Protection-[Turn off Endpoint Protection]	Defined	Applied	Applied

*1: Select Undefined for this setting on the UACS station.

● Security Measures to Fight Against Security Threats

The following table shows the security measure items against security threats and their configuration in IT security version 2.0.

“Defined/Not defined” in the Configuration by GPO file column indicates whether the security measure item is defined to be configured in the GPO file that is created based on the group policy provided by YOKOGAWA.

- Defined
  The security measure, which is adopted by YOKOGAWA, is defined in the GPO file.
- Not defined
  The security measure is not defined in the GPO file.

“Applied/Not applied” in the Configuration by IT Security Tool column indicates whether the security measure item is configured by the IT Security Tool, applying the predefined setting, for each security model.

- Applied

The security measure, which is adopted by YOKOGAWA, is configured by the IT Security Tool so that it is applied.

- Not applied
  Because YOKOGAWA decided not to adopt the security measure, it is configured by the IT Security Tool so as not to be applied.

TIP

The setting values set by the IT Security Tool can be changed by the user for some security measure items and cannot be changed for others. To find out which security measure items can be changed, refer to the appendix.

Table 2.1-3 Security Measures in IT Security Version 1.0

Security measure	Configuration by GPO file	Configuration by IT Security Tool		
		Legacy model	Standard model	Strengthened model
Access control (*1)	Not defined	Not applied	Applied	Applied
Personal firewall tuning	Not defined	Not applied	Applied	Applied
Stopping unused Windows services	Not defined	Not applied	Not applied	Applied
Disabling the built-in Administrator account or changing its user name	Not defined	Not applied	Not applied	The IT Security Tool does not configure this setting. You must configure it manually.
Hiding the Last Logon User Name	Defined	Applied	Applied	Applied
Applying the software restriction policies	Not defined	Not applied	Applied	Applied
Applying AutoRun restrictions	Defined	Applied	Applied	Applied
Applying the StorageDevicePolicies function	Defined	Not applied	Applied	Applied
Disabling USB storage devices	Defined	Not applied	Applied	Applied
Disabling NetBIOS over TCP/IP	Not defined	Not applied (*2)	Applied (*2)	Applied (*2)
Changing the LAN Manager authentication level	Defined	Not applied	Applied	Applied
Applying the password policy	Defined	Not applied	Not applied	Applied
Applying the audit policy	Defined	Not applied	Not applied	Applied
Applying the account lockout policy	Defined	Not applied	Not applied	Applied
HDD password function by BIOS (*1)	Not defined	Not applied	Not applied	The IT Security Tool does not configure this setting. You must configure it manually.

*1: This security setting item is not affected by group policy
*2: If the network connection name is "UACS Ethernet," set disabling NetBIOS over TCP/IP regardless of the security model or user management.

2.2 User/Group Management

This section describes the relationship between Windows user management types and the product. Access control is set for each user group explained in this section.

2.2.1 User Management Methods

Windows provides two methods of managing users: standalone management and domain management.

The product also supports a user management method called combination management that combines standalone management and domain management.

Table 2.2.1-1 User Management Methods

User management type	Required configuration	Operation	Feature
Standalone management	Configuration of the system built up with the product only.	Operated by registering user accounts used in each of all the PCs of HIS and system builders.	• Simple configuration not requiring domain controller. • Since account management is required for each PC, all PCs must be maintained at user account maintenance, making this method not suited for large-scale systems. • It is not possible to separate administrative rights to the computer and maintenance rights to the product.
Domain management	Construction of domain controller is required in addition to the system built up with the product.	Operated by registering user accounts used to the domain controller.	• Centralized management of users is possible, allowing less human errors. • It is possible to separate administrative rights to the computer and maintenance rights to the product.
Combination management	Construction of domain controller is required in addition to the system built up with the product.	Operated the same way as for the domain management in normal operation.	• Even if a domain controller is not available, continuous operation is possible by managing accounts of each PC. • It is not possible to separate administrative rights to the computer and maintenance rights to the product.

TIP

With combination management, users are normally managed by domain management. When required, users can be managed by standalone management. An example case is as follows:
In normal operation, user creation is centralized at an administrative section using the domain management. However, it is desired that assignment of rights to users is enabled on certain PCs on the authority of the person in charge at a site.

2.2.2 CENTUM VP User Authentication Modes

Two user authentication modes are provided to authenticate users of CENTUM VP, Windows authentication mode and CENTUM authentication mode.

- Windows authentication mode
  Users are authenticated using Windows functions.
- CENTUM authentication mode
  Users are authenticated using specific functions of CENTUM VP.

IMPORTANT

The Windows authentication mode is available only when Standard security model or strengthened security model is applied.

The CENTUM VP users that need to be authenticated are users of the following groups:

- HIS group users
  Users who use the operation and monitoring function. These users are registered using the Security Builder.
- ENG group user
  A collective term for system engineers, recipe engineers, and report users who are registered at installation of the Access Control Package or the Access Administrator Package (FDA:21 CFR Part 11 compliant).

The following table shows the users and the builders that are used to manage the users.

Table 2.2.2-1 Users and Builders Managing Users

User		Builder managing user		Explanation
HIS group user		Security Builder		Users of the operation and monitoring function
ENG group user	System engineer	ENG Group User Registration Builder (*1)	Engineers’ Account Builder for system engineers	Engineers who perform engineering tasks in the System View and various builders started from the System View
	Recipe engineer		Engineers’ Account Builder for recipe engineers	Engineers who use the recipe function
	Report user		Users’ Account Builder for report users	Users of the report function

*1: A collective term for Engineers’ Account Builder for system engineers, Engineers’ Account Builder for recipe engineers, and Users’ Account Builder for report users.

When Windows authentication mode is set, the user authentication that is performed when a user tries to use the operation and monitoring function or system builders will be based on Windows users.

The user authentication mode can be applied to the following units:

- HIS group user: For each project (for each project in the case of multiple project connection)
- ENG group user: For each engineers’ account file and users’ account file

■ Precautions at Setting User Authentication Mode

Configure as follows to unify the user management type and passwords within the CENTUM VP system.

- Use the CENTUM authentication mode if a R4.02 or earlier version HIS exists in a project.
- When Windows authentication mode is used, ensure that the user management type is unified to either domain management (combination management) or standalone management.
- One or more projects can be linked to a single Windows domain only (Windows domains:project = 1:N).

■ User Authentication of HIS Group Users

In the case of HIS group users, the affected range of user authentication mode setting is each project.

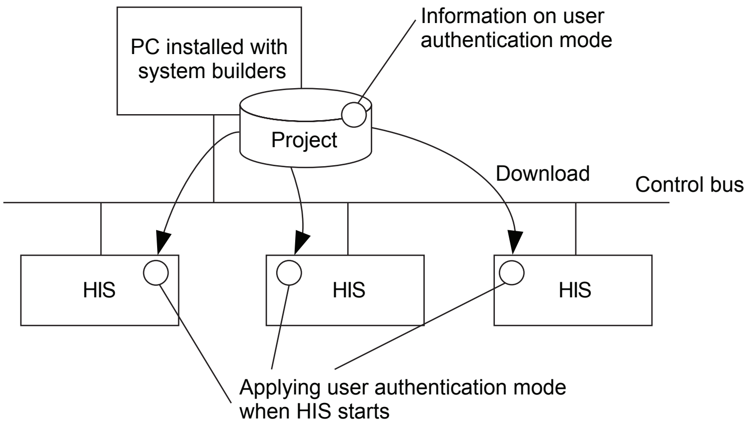

PC installed with system builders
Information on user authentication mode
Project
Download
Control bus
HIS
HIS
HIS
Applying user authentication mode when HIS starts

Figure 2.2.2-1 Affected Range of User Authentication Mode (HIS Group Users)

The user authentication mode is set in the project properties of the System View. Downloading is required after it is set. The downloaded user authentication mode information (CENTUM authentication mode or Windows authentication mode) is used as follows.

- If the Standard model is set as the security model of HIS, the selected authentication mode downloaded to the HIS will take effect when the HIS is restarted.
- If the Standard model is set as the security model of HIS and the downloaded user authentication mode is different from the current user authentication mode while the operation and monitoring functions are running, a system alarm will occur. The user authentication mode will change when the HIS is restarted.
- If the Legacy model is set as the security model of HIS and the downloaded user authentication mode is the Windows authentication mode, a system alarm will occur. The CENTUM authentication mode remains unchanged even if the HIS is restarted. In this case, you need to set the Standard model for the security model of HIS using the IT Security Tool or revert to CENTUM authentication mode.

IMPORTANT

Although the user authentication mode is not switched until the HIS is restarted, the settings in the Security Builder are changed to the downloaded information. If a user is deleted, the deleted user cannot be used.
For gradually migrating the system from the CENTUM authentication mode to the Windows authentication mode, temporarily keeping CENTUM authentication mode in the running HIS may be necessary, thus you need to keep the HIS users in the Security Builder.

Single Sign On

When the user authentication mode for HIS group users is set to Windows authentication mode, a user can log on to HIS after passing a single user authentication. This is referred to as single sign on. There are following two types of single sign on.

- Windows Type Single Sign On
  If a user logs on from the Windows logon dialog box, this user will automatically logon the operation and monitoring console, i.e., the user becomes user-in status of the Operation and Monitoring Functions. On the user-in dialog box, you can switch user. When you set a user to user-out status, the user you previously logged on the Windows will become user-in status.
- HIS Type Single Sign On
  When a PC is started, this function automatically makes the user log onto Windows as OFFUSER (default user) and starts the operation and monitoring function. After automatic logon via the HIS Type Single Sign On, the CENTUM desktop is always applied.

TIP

In CENTUM authentication mode, anonymous user be used to sign on the operation and monitoring console due to HS group users are able to share information. However, In Windows authentication mode, the anonymous user is restricted for singing on so as to improve the operation traceability and securer operation.

User Authentication of ENG Group Users

In the case of ENG group users, the affected range of user authentication mode setting is each engineers' account file or users' account file.

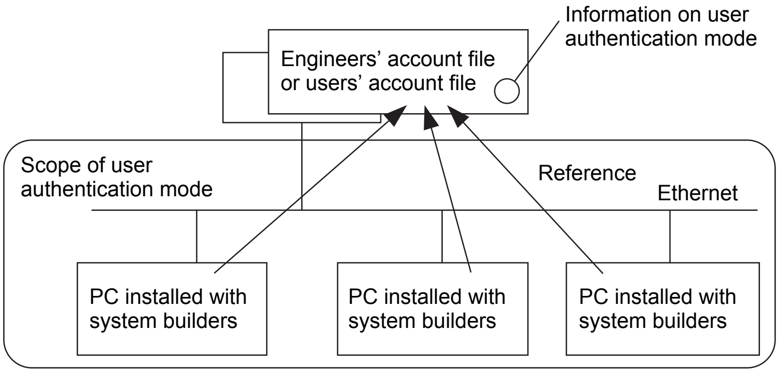

Information on user authentication mode
Engineers' account file or users' account file
Scope of user authentication mode
Reference
Ethernet
PC installed with system builders
PC installed with system builders
PC installed with system builders

Figure 2.2.2-2 Affected Range of User Authentication Mode (ENG Group Users)

The user authentication modes are set using the Access Control Utilities.

The information on user authentication mode is immediately reflected and used at the timing of user authentication.

2.2.3 User/Group Management

Users and groups are described as follows:

■ Combination of User Management and Security Model for Windows

Four security configuration types are available, depending on the combination of the Windows user management type and the security model.

- Type 1: Legacy Model
- Type 2: Standard Model / Strengthened Model - Standalone Management
- Type 3: Standard Model / Strengthened Model - Domain Management
- Type 4: Standard Model / Strengthened Model - Combination Management

TIP

No matter what security model is applied, the CENTUM VP installer creates a CTM_MAINTENANCE group and adds the user who installed the CENTUM VP software to this group.
Moreover, if domain management type or combination management type is used for user management, the CTM_MAINTENANCE group in the domain should be used instead of CTM_MAINTENANCE group in the local PC.

IMPORTANT

- When you create users or groups, do not use the following group names, which are reserved by the CENTUM VP system:
  - CTM_HISIS
  - ADS_SERVICE
  - ADS_SERVICE_LCL
- In order to use system builders, you must also configure security settings for AD projects in addition to the IT security settings.

SEE ALSO

For more information about security of AD projects, refer to:

C1.1.6, “Controlling access to AD projects” in Automation Design Suite Basics (IM 33J10A10-01EN)

● Type 1: Legacy Model

After running the IT Security Tool, the following users and user groups will be automatically created.

Table 2.2.3-1 Legacy Model

User name/group name	Type	Created location	Member of	Explanation
CENTUM	User	Local PC	Users	User created when the system is installed, in the same way as for CS 3000. Note that the default password is set to "Yokogawa1" and it is requested to change the password at the first logon.
CTM_PROCESS	User	Local PC	Users	User account for running CENTUM VP processes (Windows services) that does not have Windows logon rights.

Continues on the next page

Table 2.2.3-1 Legacy Model (Table continued)

User name/group name	Type	Created location	Member of	Explanation
UGS_PROCESS	User	Local PC	Administrators	User account for running CENTUM VP processes (Windows services) that does not have Windows logon rights. It is created only on UGS and used to run UGS-related processes.
LIC_PROCESS	User	Local PC	Users	User account for running license management processes (Windows services) that does not have Windows logon rights.
ADS_PROCESS	User	Local PC	Users	User account for running Automation Design Server processes (Windows services) that does not have Windows logon rights.
RDC_PROCESS	User	Local PC	Users	User account for running the processes for the computer switchover type UGS function (Windows services) that does not have Windows logon rights.
PSF_PROCESS	User	Local PC	Users	User account that is created on a computer with the license for the Engineering Server Function and used when backing up a project.
ADS_AGENT	User	Local PC	• Users • Performance Monitor Users	User account for running station information management processes that does not have Windows logon rights.

IMPORTANT

Use these user accounts only for running CENTUM VP products.

SEE ALSO

For more information about Automation Design Server, refer to:

A., “Overview of Automation Design Suite” in Automation Design Suite Basics (IM 33J10A10-01EN)

● Type 2: Standard Model/Strengthened Model - Standalone Management

After running the IT Security Tool, the following users and user groups will be automatically created.

Table 2.2.3-2 Standard Model/Strengthened Model - Standalone Management

User name/group name	Type	Created location	Member of	Explanation
CTM_OPERATOR	Group	Local PC	Users (*1)	Group of users for operators.
CTM_ENGINEER	Group	Local PC	Users (*1)	Group of users who use the System View and so on for engineering of CENTUM VP.
CTM_ENGINEER_ADM	Group	Local PC	Administrators (*1)	Group of users who use the System View and so on for engineering of CENTUM VP with stronger rights than CTM_ENGINEER.

Continues on the next page

Table 2.2.3-2 Standard Model/Strengthened Model - Standalone Management (Table continued)

User name/group name	Type	Created location	Member of	Explanation
CTM_OPC	Group	Local PC	Users (*1)	Group that is used for other programs to connect CENTUM VP. For example, it is used when performing OPC communication with CENTUM VP.
CTM_MAINTENANCE	Group	Local PC	Administrators (*1)	Group of users who perform system installation and CENTUM VP maintenance.
ADS_MANAGER	Group	Local PC	Users(*1)	Group of users who use the Automation Design Suite Administration Tool to manage Automation Design Server of CENTUM VP.
OFFUSER	User	Local PC	Users	User used for automatic logon by HIS Type Single Sign On in Windows authentication mode. It has minimum rights for the Windows environment.
CTM_PROCESS	User	Local PC	Users	User account for running CENTUM VP processes (Windows services) that does not have Windows logon rights.
UGS_PROCESS	User	Local PC	Administrators	User account for running CENTUM VP processes (Windows services) that does not have Windows logon rights. It is created only on UGS and used to run UGS-related processes.
LIC_PROCESS	User	Local PC	Users	User account for running license management processes (Windows services) that does not have Windows logon rights.
ADS_PROCESS	User	Local PC	Users	User account for running Automation Design Server processes (Windows services) that does not have Windows logon rights.
RDC_PROCESS	User	Local PC	• Users • CTM_OPC	User account for running the processes for the computer switch-over type UGS function (Windows services) that does not have Windows logon rights.
PSF_PROCESS	User	Local PC	Users	User account that is created on a computer with the license for the Engineering Server Function and used when backing up a project.
ADS_AGENT	User	Local PC	• Users • Performance Monitor Users • CTM_OPC	User account for running station information management processes that does not have Windows logon rights.

*1: You need to add the users who belong to the created group to the group shown in the “Member of” column.

IMPORTANT

- Use these user accounts and groups only for running CENTUM VP products.
- If you change the security model, existing user groups may be deleted or their names may be modified without confirmation.

SEE ALSO For more information about Automation Design Server, refer to:

A., “Overview of Automation Design Suite” in Automation Design Suite Basics (IM 33J10A10-01EN)

● Type 3: Standard Model/Strengthened Model - Domain Management

After running the IT Security Tool, the following users and user groups will be automatically created.

Table 2.2.3-3 Standard Model/Strengthened Model - Domain Management

User name/group name	Type	Created location	Member of	Explanation
CTM_OPERATOR	Group	Domain controller	Domain Users (*1)	Group of users for operators.
CTM_ENGINEER	Group	Domain controller	Domain Users (*1)	Group of users who use the System View and so on for engineering of CENTUM VP.
CTM_ENGINEER_ADM	Group	Domain controller	Domain Admins (*1)	Group of users who use the System View and so on for engineering of CENTUM VP with stronger rights than CTM_ENGINEER.
CTM_OPC	Group	Domain controller	Domain Users (*1)	Group that is used for other programs to connect CENTUM VP. For example, it is used when performing OPC communication with CENTUM VP.
CTM_OPC_LCL	Group	Local PC	Users (*1)	Supplementary group for users not supporting domain management, such as users embedded in the EXA package, having the same rights as CTM_OPC. It is not used in normal operation.
CTM_MAINTENANCE	Group	Domain controller	Domain Admins (*1)	Group of users who perform system installation and CENTUM VP maintenance.
CTM_MAINTENANCE_LCL	Group	Local PC	Administrators (*1)	Emergency group used when the domain environment is abnormal, having the same rights as CTM_MAINTENANCE. It is not used in normal operation. After the installation of CENTUM VP is completed in the domain environment, the administrator user of each PC (local user) should be manually added to this local group.
ADS_MANAGER	Group	Domain controller	Domain Users (*1)	Group of users who use the Automation Design Suite Administration Tool to manage Automation Design Server of CENTUM VP.

Continues on the next page

Table 2.2.3-3 Standard Model/Strengthened Model - Domain Management (Table continued)

User name/group name	Type	Created location	Member of	Explanation
OFFUSER	User	Local PC	Users	User used for automatic logon by HIS Type Single Sign On in Windows authentication mode. It has minimum rights for the Windows environment.
CTM_PROCESS	User	Local PC	Users	User account for running CENTUM VP processes (Windows services) that does not have Windows logon rights.
UGS_PROCESS	User	Local PC	Administrators	User account for running CENTUM VP processes (Windows services) that does not have Windows logon rights. It is created only on UGS and used to run UGS-related processes.
LIC_PROCESS	User	Local PC	Users	User account for running license management processes (Windows services) that does not have Windows logon rights.
ADS_PROCESS	User	Local PC	Users	User account for running Automation Design Server processes (Windows services) that does not have Windows logon rights.
RDC_PROCESS	User	Local PC	• Users • CTM_OPC_LCL	User account for running the processes for the computer switchover type UGS function (Windows services) that does not have Windows logon rights.
PSF_PROCESS	User	Local PC	Users	User account that is created on a computer with the license for the Engineering Server Function and used when backing up a project.
ADS_AGENT	User	Local PC	• Users • Performance Monitor Users • CTM_OPC_LCL	User account for running station information management processes that does not have Windows logon rights.

*1: You need to add the users who belong to the created group to the group shown in the “Member of” column.

IMPORTANT

- Use these user accounts and groups only for running CENTUM VP products.
- If you change the security model, existing user groups may be deleted or their names may be modified without confirmation.

SEE ALSO For more information about Automation Design Server, refer to:

A., “Overview of Automation Design Suite” in Automation Design Suite Basics (IM 33J10A10-01EN)

● Type 4: Standard Model/Strengthened Model - Combination Management

After running the IT Security Tool, the following users and user groups will be automatically created.

Table 2.2.3-4 Standard Model/Strengthened Model - Combination Management

User name/group name	Type	Created location	Member of	Explanation
CTM_OPERATOR	Group	Domain controller	Domain Users (*1)	Group of users for operators.
CTM_OPERATOR_LCL	Group	Local PC	Users (*1)	Group of users for operators that is used in a PC where standalone management is performed.
CTM_ENGINEER	Group	Domain controller	Domain Users (*1)	Group of users who use the System View and so on for engineering of CENTUM VP.
CTM_ENGINEER_LCL	Group	Local PC	Users (*1)	Group of users who perform CENTUM VP system engineering by using System View and other programs. This group is used in a PC where standalone management is performed.
CTM_ENGINEER_ADM	Group	Domain controller	Domain Admins (*1)	Group of users who use the System View and so on for engineering of CENTUM VP with stronger rights than CTM_ENGINEER.
CTM_ENGINEER_ADM_LCL	Group	Local PC	Administrators (*1)	Group of users who perform CENTUM VP system engineering on a PC where standalone management is applied. This group has stronger rights than CTM_ENGINEER.
CTM_OPC	Group	Domain controller	Domain Users (*1)	Group that is used for other programs to connect CENTUM VP. For example, it is used when performing OPC communication with CENTUM VP.
CTM_OPC_LCL	Group	Local PC	Users (*1)	Supplementary group for users not supporting domain management, such as users embedded in the EXA package, having the same rights as CTM_OPC. It is not used in normal operation.
CTM_MAINTENANCE	Group	Domain controller	Domain Admins (*1)	Group of users who perform system installation and CENTUM VP maintenance.
CTM_MAINTENANCE_LCL	Group	Local PC	Administrators (*1)	Emergency group used when the domain environment is abnormal, having the same rights as CTM_MAINTENANCE. It is not used in normal operation. After the installation of CENTUM VP is completed in the domain environment, the administrator user of each PC (local user) should be manually added to this local group.
ADS_MANAGER	Group	Domain controller	Domain Users (*1)	Group of users who use the Automation Design Suite Administration Tool to manage Automation Design Server of CENTUM VP.

Continues on the next page

Table 2.2.3-4 Standard Model/Strengthened Model - Combination Management (Table continued)

User name/group name	Type	Created location	Member of	Explanation
ADS_MANAGER_LCL	Group	Local PC	Users (*1)	Group of users who use the Automation Design Suite Administration Tool on a PC where standalone management is applied to manage Automation Design Server of CENTUM VP.
OFFUSER	User	Local PC	Users	User used for automatic logon by HIS Type Single Sign On in Windows authentication mode. It has minimum rights for the Windows environment.
CTM_PROCESS	User	Local PC	Users	User account for running CENTUM VP processes (Windows services) that does not have Windows logon rights.
UGS_PROCESS	User	Local PC	Administrators	User account for running CENTUM VP processes (Windows services) that does not have Windows logon rights. It is created only on UGS and used to run UGS-related processes.
LIC_PROCESS	User	Local PC	Users	User account for running license management processes (Windows services) that does not have Windows logon rights.
ADS_PROCESS	User	Local PC	Users	User account for running Automation Design Server processes (Windows services) that does not have Windows logon rights.
RDC_PROCESS	User	Local PC	• Users • CTM_OPC_LCL	User account for running the processes for the computer switchover type UGS function (Windows services) that does not have Windows logon rights.
PSF_PROCESS	User	Local PC	Users	User account that is created on a computer with the license for the Engineering Server Function and used when backing up a project.
ADS_AGENT	User	Local PC	• Users • Performance Monitor Users • CTM_OPC_LCL	User account for running station information management processes that does not have Windows logon rights.

*1: You need to add the users who belong to the created group to the group shown in the “Member of” column.

IMPORTANT

- Use these user accounts and groups only for running CENTUM VP products.
- If you change the security model, existing user groups may be deleted or their names may be modified without confirmation.

SEE ALSO For more information about Automation Design Server, refer to:

A., “Overview of Automation Design Suite” in Automation Design Suite Basics (IM 33J10A10-01EN)

■ The Users and User Groups Added by the Vnet/IP Interface Package

When Vnet/IP interface package is installed, the users and user groups in the following table are automatically created.

The users and user groups other than LIC_PROCESS are used only for Vnet/IP interface package. They do not affect the CENTUM VP software.

Table 2.2.3-5 Added Users and Groups

User name/group name	Type	Created location	Member of	Explanation
VNT_ALL	Group	Local PC	-	Group of users who can read/write in the directory of Vnet/IP interface package. Do not include the users who can sign-in to Windows in this group.
VNT_ VNET_VVIF	Group	Local PC	-	Group of users for running the processes (like Windows services) of Vnet/IP interface package. Do not include the users who can sign-in to Windows in this group.
VNT_NVP_ CMDIF	Group	Local PC	-	
VNT_NVP_MNGIF	Group	Local PC	-	
VNT_COMMON	User	Local PC	VNT_ALL	User who can read/write in the directory of Vnet/IP interface package. Windows sign-in rights are not granted.
VNT_NVP_CORE	User	Local PC	• VNT_VNET_VVIF • VNT_NVP_CMDIF • VNT_NVP_MNGIF • VNT_ALL • Performance Monitor Users	Users for running the processes (like Windows services) of Vnet/IP interface package. Windows sign-in rights are not granted.
VNT_BKNET	User	Local PC	• VNT_VNET_VVIF • VNT_NVP_MNGIF • VNT_ALL	
LIC_PROCESS	User	Local PC	• VNT_ALL • Users	LIC_PROCESS is a common user for products which support License Manager. It is used for accepting licenses. When installing Vnet/IP interface package, if LIC_PROCESS is not present, LIC_PROCESS user is created and configured.

IMPORTANT

The users and user groups that are automatically created when Vnet/IP interface package is installed are valid only on local PCs. Do not manage the users and user groups in the domain controller. And, do not include the users who can sign-in to Windows in this group.

2.2.4 User Name and Password Policies

The policies regarding the Windows user names and passwords are in Windows environment. While, the HIS group users and ENG group users are defined with a certain policies. The HIS group users, ENG group users and the Windows users in Windows authentication mode need to be created according to these policies.

■ User Name

The following table shows the user name convention.

Table 2.2.4-1 User Name Convention

Item	Details
Number of characters	Up to 16 characters
Character type	Alphanumeric including symbols of ! # $ % ( ) - . ^ _ { } ~ Double-byte character is invalid
Restriction	Capital letters only The first character can be an alpha or numeric character as well as a symbol of ^ _ { } ~ A period character cannot be put at the last place.

TIP

ENG group user and HIS group user names can be created with capital letters only. Windows user names are not case sensitive, but it is recommended to use the capital letters.

■ Password

The following table shows the rules for passwords.

Table 2.2.4-2 Password Convention

Item	Details
Number of characters	The password of a HIS group user or ENG group user can be defined using up to 32 alpha-numeric characters. The password of a Windows user used in Windows authentication mode can be defined using up to 63 alpha-numeric characters.
Character type	Alphanumeric and space characters and the following symbols can be used: ! “ # $ % & ‘ ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
Restriction	Restricted by password policies set in Windows

TIP

The passwords for HIS group users are restricted by the password policies defined by HIS Utility.

The passwords for ENG group users are restricted by the password policies defined Access Control Utilities.

2.2.5 Special User

This section explains special HIS group users and ENG group users linked to Windows users in Windows authentication mode.

■ Users for Local Authentication

As a locally authenticated user, the following user name can be used:

User names starting with "_" (underscore)

These users are authenticated in the PCs used by these users in the Windows authentication mode. These users are used at emergency, for example when a domain controller is down while the users of the PC are managed in domain management or combination management. The special user accounts are not used under normal circumstances. In standalone management, there is no need to create these users.

When a special user name is used on the User-in dialog box of the operation and monitoring functions, a system alarm is generated under the following circumstance:

- When the domain management is functioning and access to the domain controller is unimpeded

Under this circumstance, an emergency user account is used even though the user authentication processing on the domain is normally performed. Since it may weaken the security of the system, a system alarm will be issued for notification.

■ OFFUSER

OFFUSER in the Windows authentication mode has the following characteristics.

- OFFUSER is only used for automatically logon by HIS Type Single Sign On in the Windows authentication mode.
- It is created as a local user regardless of the domain or standalone management.
- The initial password contains 32 characters and is not disclosed (the password can be changed but the changed password needs to be standardized on all HISs of the CENTUM VP system).

3. Details of Security Measures

This section describes the security measures for each security type in detail.

3.1 Access Control

By minimizing the access rights of the users of the product, you can prevent unauthorized access, leakage, tampering, and destruction of important data in the product. Access permissions to files, folders, registries, DCOM modules, and local security policy are controlled by using the Windows access control functions.

Access control is performed for each user or group. Users have only the rights that are granted to them or to the group they belong to.

3.1.1 Access Permissions to Files and Folders

In the product, accesses to files and folders are controlled for each file or folder. Access to files and folders by users is restricted by controlling the permissions to execute, read, write, and delete in user or group units. In the product, access permissions are granted for each folder.

TIP

If a file in a folder requires different access permissions, the access permissions for the file can be separately granted.

■ Target Folders

The following table describes the main target folders with controlled access.

Table 3.1.1-1 Target Folders

Target folder	Description
<CENTUM VP installation folder>	The folder in which CENTUM VP packages are installed.
<ProgramFiles32> (*1) \Yokogawa\IA\iPCS\Platform\License	The folder in which files required to run license management programs are installed.
〈ProgramFiles32〉 (*1) \Yokogawa\IA\iPCS\Platform\Program	The folder in which license management programs are installed.
〈ProgramFiles32〉 (*1) \Yokogawa\IA\iPCS\Platform\SECURITY	The folder in which IT Security Tool and so on are installed.
〈ProgramFiles32〉 (*1) \Yokogawa\IA\iPCS\Platform\PC-Redundancy\Tool	The folder in which the Redundancy Management Tool for computer switchover type UGS is installed.
〈ProgramFiles32〉 (*1) \Yokogawa\IA\iPCS\Platform\PC-Redundancy\Agent	The folder in which the programs related to computer switchover type UGS are installed.
〈ProgramFiles32〉 (*1) \Yokogawa\IA\iPCS\Products\CENTUMVP	The folder storing CENTUM VP programs, which is installed under the Program Files folder.
〈ProgramFiles32〉 (*1) \Yokogawa\IA\iPCS\Products\ADSuite	The folder in which programs that are related to Automation Design Server and module-based engineering are installed.
〈ProgramFiles64〉 (*2) \Yokogawa\IA\iPCS\Platform\PC-Redundancy\Agent	The folder in which the programs related to computer switchover type UGS are installed.
〈ProgramFiles64〉 (*2) \Yokogawa\IA\iPCS\Products\ADSuite	The folder in which programs that are related to Automation Design Server and module-based engineering are installed.
〈ProgramFiles64〉 (*2) \Yokogawa\IA\iPCS\Products\CENTUMVP	The folder storing CENTUM VP programs, which is installed under the Program Files folder.
〈ProgramFiles64〉 (*2) \Yokogawa\IA\iPCS\Products\CIMAgent	The folder in which programs related to station information management processes are installed.
〈ProgramFiles32〉 (*1) \Yokogawa\IA\iPCS\Products\Platform	The folder in which the log server and so on are installed.
〈ProgramData〉 (*3) \Yokogawa\IA\iPCS\Platform\License	The folder in which license management data and so on are installed.
〈ProgramData〉 (*3) \Yokogawa\IA\iPCS\Platform\Security	The folder in which setting files for IT Security Tool and so on are installed.
〈ProgramData〉 (*3) \Yokogawa\IA\iPCS\Platform\PC-Redundancy\Agent	The folder in which data that is related to computer switchover type UGS is installed.
〈ProgramData〉 (*3) \Yokogawa\IA\iPCS\Products\CentumVP	The folder in which CENTUM VP logs and so on are created.

Continues on the next page

Table 3.1.1-1 Target Folders (Table continued)

Target folder	Description
〈ProgramData〉 (*3) \Yokogawa\IA\iPCS\Products\Platform	The folder in which the management data of online manuals and so on are created.
〈ProgramData〉 (*3) \Yokogawa\IA\iPCS\Products\ChronusENG	The folder in which data that is related to Automation Design Server and module-based engineering is installed.
〈ProgramData〉 (*3) \Yokogawa\IA\iPCS\Products\CIMAgent	The folder in which data related to station information management processes is installed.
〈ProgramData〉 (*3) \Yokogawa\IA\iPCS\Products\AccessRef\CTM-PSF	The folder in which data handled by CENTUM VP is installed.
〈ProgramFiles32〉 (*1) \Yokogawa\PROFIBUS_Configurator	The folder in which PROFIBUS-DP Configurator or PROFINET Configurator is installed.
〈ProgramData〉 (*3) \Yokogawa\SYCONnet	The folder in which data files of PROFIBUS-DP Configurator or PROFINET Configurator are stored.
〈ProgramFiles32〉 (*1) \Common Files\Hilscher	The folder in which the files related to PROFIBUS-DP Configurator or PROFINET Configurator are stored.
〈ProgramFiles32〉 (*1) \Common Files\Hilscher GmbH	The folder in which the files related to PROFIBUS-DP Configurator or PROFINET Configurator are stored.
〈windir〉 (*4) \system32	The folder in which Windows maintenance tools are installed. (*5)
〈windir〉 (*4) \SysWOW64(*6)	The folder in which Windows maintenance tools are installed. (*5)
〈Project folder〉	The folder in which CENTUM VP project files are stored.
CTM_PJTS_DBSF	The shared folder to be created on a file server, HIS, or PC installed with system builders. For an HIS or PC installed with system builders, you need to create this folder when you store project data to a location other than the default folder.
〈ProgramFiles64〉 (*2)\Yokogawa\IA\iPCS\Platform\VnetIPSoftStack	The folder in which Vnet/IP interface package related files and data are stored.
〈ProgramData〉 (*3)\Yokogawa\IA\iPCS\Platform\VnetIPSoftStack	The folder in which Vnet/IP interface package related files and data are stored.
〈ProgramData〉 (*3) \Yokogawa\IA\iPCS\Products\AccessRef\VnetIPSoftStack	The folder in which Vnet/IP interface package related files and data are stored.

*1: 〈ProgramFiles32〉 refers to the following folder. This example is when the system drive is drive C.
For Windows 10, Windows 7, Windows Server 2016, Windows Server 2012 R2, and Windows Server 2008 R2,
`C:\Program Files (x86)`
For Windows Server 2008
`C:\Program Files`

*2: 〈ProgramFiles64〉 refers to the following folder. This example is when the system drive is drive C.
For Windows 10, Windows 7, Windows Server 2016, Windows Server 2012 R2, and Windows Server 2008 R2,
`C:\Program Files`

*3: 〈ProgramData〉 refers to the following folder. This example is when the system drive is drive C.
`C:\ProgramData`

*4: 〈windir〉 refers to the following folder. This example is when the system drive is drive C.
`C:\Windows`

*5: Access permissions are set for certain files in the folder.

*6: Only for Windows 10, Windows 7, Windows Server 2016, Windows Server 2012 R2, and Windows Server 2008 R2.

■ Access Permissions for Programs

Functions that each user can use are restricted by setting access permissions for each CENTUM VP function (program) for each user or group.

The following table shows the access permissions to run the programs registered in the Start menu that are granted to each user or group. Only the users or users of a group having the access permission can run the program.

Note that HIS is not started from the Start menu.

TIP

Access permissions for execution are also set for each user or group for the program files with the extension exe, com, bat, cmd, or vbs that are not registered in the Start menu.

Table 3.1.1-2 Access Permissions for Programs that are Started from the Start Menu

Items on Start Menu	User/group (*1)									
	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
HIS (*2)	Yes	Yes	Yes	No	Yes	No	No	No	No	No
HIS Utility	No	No	No	No	Yes	No	No	No	No	No
Access Control Utilities	No	No	Yes	No	Yes	No	No	No	No	No
Graphic Builder	Yes (*3)	Yes	Yes	No	Yes	No	No	No	No	No
Graphic Compatibility Check Tool	No	Yes	Yes	No	Yes	No	No	No	No	No
System View	No	Yes	Yes	No	Yes	No	No	No	No	No
Software Configuration Viewer	No	Yes	Yes	No	Yes	No	No	No	No	No
Consolidated Historical Viewer	No	Yes	Yes	No	Yes	No	No	No	No	No
Copy Tool for Fieldbus associated files	No	Yes	Yes	No	Yes	No	No	No	No	No
Project’s Attribution Utility	No	Yes	Yes	No	Yes	No	No	No	No	No
Linked-Part List Window	No	Yes	Yes	No	Yes	No	No	No	No	No
Device Panel	No	Yes	Yes	No	Yes	No	No	No	No	No
Recipe View	No	Yes	Yes	No	Yes	No	No	No	No	No
Report Package	No	Yes	Yes	No	Yes	No	No	No	No	No
Logic Test Tool	No	Yes	Yes	No	Yes	No	No	No	No	No
Command Prompt	Yes	Yes	Yes	No	Yes	No	No	Yes	No	No
Project Save	No	Yes	Yes	No	Yes	No	No	No	No	No
Log Save	Yes	Yes	Yes	No	Yes	No	No	Yes	No	No
N-IO Node Security	No	Yes	Yes	No	Yes	No	No	No	No	No
Configurator of CAMS for HIS	No	Yes	Yes	No	Yes	No	No	No	No	No
CAMS for HIS Migration Tool	No	Yes	Yes	No	Yes	No	No	No	No	No
Alarm Generator of CAMS for HIS	No	Yes	Yes	No	Yes	No	No	No	No	No
SEM OPC Interface Settings	No	Yes	Yes	No	Yes	No	No	No	No	No
SOE Database Backup	No	No	Yes	No	Yes	No	No	No	No	No
SOE Database Property	No	Yes	Yes	No	Yes	No	No	No	No	No
SOE Database Restore	No	No	Yes	No	Yes	No	No	No	No	No
SOE Server Monitoring Settings	No	Yes	Yes	No	Yes	No	No	No	No	No
Specify SOE Trigger	No	Yes	Yes	No	Yes	No	No	No	No	No
SOE Server Configurator	No	Yes	Yes	No	Yes	No	No	No	No	No
SOE Viewer	Yes	Yes	Yes	No	Yes	No	No	No	No	No
UACS Migration Tool	No	Yes	Yes	No	Yes	No	No	No	No	No

Continues on the next page

Table 3.1.1-2 Access Permissions for Programs that are Started from the Start Menu (Table continued)

Items on Start Menu	User/group (*1)									
	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
UACS Utility	No	No	No	No	Yes	No	No	No	No	No
AD Organizer	No	Yes	Yes	No	Yes	No	No	No	Yes	No
ADS Administration Tool	No	No	No	No	No	No	No	Yes	Yes	No
Dependency Analyzer	No	Yes	Yes	No	Yes	No	No	No	Yes	No
SIOS Statistic Collector	No	No	No	No	Yes	No	No	No	No	No
License Manager	Yes	Yes	Yes	No	Yes	No	Yes	No	No	No
IT Security Tool	No	No	No	No	Yes	No	No	No	No	No
Redundancy Management Tool	(*4)									
VnetIP interface management tool	(*5)									

*1: User/Group
[1]: CTM_OPERATOR/CTM_OPERATOR_LCL/OFFUSER
[2]: CTM_ENGINEER/CTM_ENGINEER_LCL
[3]: CTM_ENGINEER_ADM/CTM_ENGINEER_ADM_LCL
[4]: CTM_OPC/CTM_OPC_LCL
[5]: CTM_MAINTENANCE/CTM_MAINTENANCE_LCL
[6]: CTM_PROCESS/UGS_PROCESS
[7]: LIC_PROCESS
[8]: ADS_MANAGER/ADS_MANAGER_LCL
[9]: ADS_PROCESS
[10]: RDC_PROCESS/PSF_PROCESS/ADS_AGENT

*2: Functions not started from the Start menu

*3: The Graphic Builder is required to use the Builder Reference Package (option) in HIS.

*4: The program can be run depending on the access permission of <ProgramFiles32>.

*5: The Vnet/IP interface management tool starts. Users who belong to the Administrators group or the Users group can run the tool. The users in the Administrators group can configure the Vnet station address and monitor the Vnet/IP interface package. The users in the Users group can only monitor the Vnet/IP interface package.

IMPORTANT

The members of CTM_ENGINEER_ADM, CTM_ENGINEER_ADM_LCL, CTM_MAINTENANCE, or CTM_MAINTENANCE_LCL, who belong to the Administrators group, cannot start the operation and monitoring function and the test function. However, the user of the built-in Administrator account can exceptionally start these functions even if it belongs to the Administrators group.

3.1.2 Registry Configuration and User/Group

You can control access to the registries used by the product to prevent tampering and destruction of them.

■ Registry Types

Access control is applied to three types of registries.

Table 3.1.2-1 Registry Types

Type	Description
CENTUM Related	CENTUM related registries
DCOM Related	DCOM communication (OPC) related registries
PROFIBUS-DP Configurator and PROFINET Configurator Related	PROFIBUS-DP Configurator and PROFINET Configurator related registries.

■ Registry Keys

The following tables show the registry keys that are subjected to access control.

Table 3.1.2-2 CENTUM Related Registry Keys

Name	Registry Key	Description
CENTUM Registry	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\YOKOGAWA]	Registry created at installation of CENTUM VP
CS3000 Registry	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\YOKOGAWA\CS3000]	Registry used by programs of CENTUM VP
CentumProductInfo Registry	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\YOKOGAWA\CentumProductInfo]	Registry in which product information of CENTUM VP is stored
CENTUMVP Registry	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\YOKOGAWA\CENTUMVP]	Registry used by the installer
CS3K Registry	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\YOKOGAWA\CS3K]	Registry used by the installer
VHFD Registry	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\YOKOGAWA\VHFD]	Registry related to control bus
Exaopc Registry	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\YOKOGAWA\Exaopc]	Registry related to Exaopc
EXA Registry	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\YOKOGAWA\EXA]	Registry related to Exa products
PKGCOM Registry	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\YOKOGAWA\PKGCOM]	Registry related to Exa products

Table 3.1.2-3 DCOM Related Registry Keys

Name	Registry Key	Description
OpcEnum Registry	[HKEY_CLASSES_ROOT\AppID\{13486D44-4821-11D2-A494-3CB306C10000}]	DCOM related registry for OpcEnum
OPC Alarms Registry	[HKEY_CLASSES_ROOT\AppID\{21FF9972-DE40-11D1-B324-00A024770B10}]	DCOM related registry for Yokogawa CSHIS OPC Alarms
BKCLcs Registry	[HKEY_CLASSES_ROOT\AppID\{79142CD2-0ABE-11D4-8F5C-0060B0C3BE1F}]	DCOM related registry for BKCLcs
CS Batch Server Registry	[HKEY_CLASSES_ROOT\AppID\{A232A362-E94E-11D1-AB29-0060B0174D72}]	DCOM related registry for Yokogawa CS Batch Server

Continues on the next page

Table 3.1.2-3 DCOM Related Registry Keys (Table continued)

Name	Registry Key	Description
CS DCOM Server Registry	[HKEY_CLASSES_ROOT\AppID\{b75cd3f2-a692-11d2-a06e-006008ab9b09}]	DCOM related registry for Yokogawa CS DCOM Server
OPC Server Registry	[HKEY_CLASSES_ROOT\AppID\{E6C32641-F1CF-11d0-B0E4-080009CCD384}]	DCOM related registry for Yokogawa CSHIS OPC Server
OPC HDA Server Registry	[HKEY_CLASSES_ROOT\AppID\{FCF966F4-D7E8-11D1-9702-00C04FBC25BF}]	DCOM related registry for Yokogawa CSHIS OPC HDA Server
Exaopc HDA Server Registry	[HKEY_CLASSES_ROOT\AppID\{6CE76D12-D100-11D2-9804-00C04FBC25BF}]	DCOM related registry for Yokogawa Exaopc HDA Server
CSSEM Alarm & Events Automation Server Registry	[HKEY_CLASSES_ROOT\AppID\{415397C0-833D-408B-AAC7-538CA112707C}]	DCOM related registry for Yokogawa CSSEM Alarm & Events Automation Server
CSSEM HDA Server Registry	[HKEY_CLASSES_ROOT\AppID\{271BCFF2-47BC-468C-BD54-559593428624}]	DCOM related registry for Yokogawa CSSEM HDA Server

Table 3.1.2-4 PROFIBUS-DP Configurator and PROFINET Configurator Related Registry Keys

Name	Registry Key
PROFIBUS Configurator Registry	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hilscher GmbH]
PROFIBUS International Registry	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PROFIBUS International]
PROFIBUS DTMs Registry	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Yokogawa\DTMs]
PROFIBUS GenericSlaveDTM Registry	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Yokogawa\GenericSlaveDTM]
PROFIBUS Sycon_net Registry	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Yokogawa\SyCon_net]

■ Access Permissions for Registries

The following table shows the access permissions for registries.

Table 3.1.2-5 Access Permissions for CENTUM Related Registries

Registry	User/group (*1)													
	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]
CENTUM Registry	-	-	-	-	-	-	-	-	F	F	-	-	-	-
CS3000 Registry	F	F	F	F	F	F	F	-	R	F	-	-	-	-
CentumProductInfo Registry	-	-	-	-	F	-	-	-	F	F	-	-	-	-
CENTUMVP Registry	-	-	-	-	F	-	-	-	F	F	-	-	-	-
CS3K Registry	F	F	F	F	F	F	F	F	R	F	-	-	-	-
VHFD Registry	F	F	F	F	F	F	F	-	R	F	-	-	-	-
Exaopc Registry	F	F	F	F	F	F	F	F	-	F	-	-	-	-
EXA Registry	F	F	F	F	F	F	F	F	-	F	-	-	-	-
PKGCOM Registry	-	F	-	-	F	F	-	-	-	F	-	-	-	-

*1: User/Group
[1]: CTM_OPERATOR/CTM_OPERATOR_LCL/OFFUSER
[2]: CTM_ENGINEER/CTM_ENGINEER_LCL
[3]: CTM_ENGINEER_ADM/CTM_ENGINEER_ADM_LCL
[4]: CTM_OPC/CTM_OPC_LCL
[5]: CTM_MAINTENANCE/CTM_MAINTENANCE_LCL
[6]: CTM_PROCESS
[7]: UGS_PROCESS
[8]: LIC_PROCESS
[9]: Everyone
[10]: SYSTEM

[11]: SERVICE
[12]: ADS_MANAGER/ADS_MANAGER_LCL
[13]: ADS_PROCESS
[14]: RDC_PROCESS/PSF_PROCESS/ADS_AGENT
Types of permissions
F: Full control
R: Read
-: No permission

Table 3.1.2-6 Access Permissions for DCOM Related Registries

Registry	User/group (*1)													
	[1] (*2)	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]
OpcEnum Registry	F	F	F	F	F	F	-	-	-	F	R	-	-	-
OPC Alarms Registry	F	F	F	F	F	F	-	-	-	F	R	-	-	-
BKCLcs Registry	F	F	F	F	F	F	-	-	-	F	R	-	-	-
CS Batch Server Registry	F	F	F	F	F	F	-	-	-	F	R	-	-	-
CS DCOM Server Registry	F	F	F	F	F	F	-	-	-	F	R	-	-	-
OPC Server Registry	F	F	F	F	F	F	-	-	-	F	R	-	-	-
OPC HDA Server Registry	F	F	F	F	F	F	-	-	-	F	R	-	-	-
Exaopc HDA Server Registry	F	F	F	F	F	F	-	-	-	F	R	-	-	-
CSSEM Alarm & Events Automation Server Registry	F	F	F	F	F	F	-	-	-	F	R	-	-	-
CSSEM HDA Server Registry	F	F	F	F	F	F	-	-	-	F	R	-	-	-

*1: User/Group
[1]: CTM_OPERATOR/CTM_OPERATOR_LCL/OFFUSER
[2]: CTM_ENGINEER/CTM_ENGINEER_LCL
[3]: CTM_ENGINEER_ADM/CTM_ENGINEER_ADM_LCL
[4]: CTM_OPC/CTM_OPC_LCL
[5]: CTM_MAINTENANCE/CTM_MAINTENANCE_LCL
[6]: CTM_PROCESS
[7]: UGS_PROCESS
[8]: LIC_PROCESS
[9]: Everyone
[10]: SYSTEM
[11]: SERVICE
[12]: ADS_MANAGER/ADS_MANAGER_LCL
[13]: ADS_PROCESS
[14]: RDC_PROCESS/PSF_PROCESS/ADS_AGENT
Types of permissions
F: Full control
R: Read
-: No permission

*2: Only the read permission (R) is granted to OFFUSER.

Table 3.1.2-7 Access Permissions for PROFIBUS-DP Configurator and PROFINET Configurator Related Registries

Registry	User/group(*1)											
	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]
PROFIBUS Configurator Registry	-	F	F	-	F	-	-	-	F	-	-	-
PROFIBUS International Registry	-	F	F	-	F	-	-	-	F	-	-	-
PROFIBUS DTMs Registry	-	F	F	-	F	-	-	-	F	-	-	-
PROFIBUS GenericSlaveDTM Registry	-	F	F	-	F	-	-	-	F	-	-	-
PROFIBUS Sycon_net Registry	-	F	F	-	F	-	-	-	F	-	-	-

*1: [1]: CTM_OPERATOR/CTM_OPERATOR_LCL/OFFUSER
[2]: CTM_ENGINEER/CTM_ENGINEER_LCL
[3]: CTM_ENGINEER_ADM/CTM_ENGINEER_ADM_LCL
[4]: CTM_OPC/CTM_OPC_LCL
[5]: CTM_MAINTENANCE/CTM_MAINTENANCE_LCL
[6]: CTM_PROCESS/UGS_PROCESS

[7]: LIC_PROCESS
[8]: Everyone
[9]: SYSTEM
[10]: ADS_MANAGER/ADS_MANAGER_LCL
[11]: ADS_PROCESS
[12]: RDC_PROCESS/PSF_PROCESS/ADS_AGENT
Types of permissions
F: Full control
-: No permission

3.1.3 DCOM (OPC) and User/Group

Considering software packages (including third party packages) that communicate with CENTUM VP by DCOM, you can apply access control to DCOM components.

■ Setting for the Entire PC

The setting for the entire PC is as follows:

- Legacy model
  Default authentication level: None
- Standard model or Strengthened model
  Default authentication level: Connect

■ Settings for Individual DCOM Components

The DCOM components installed together with CENTUM VP are configured so that rights to execute OPC communication from the local computer and remote computers are granted to all users and groups from [1] to [9] listed below.

To OFFUSER, a right to execute from the local computer is granted.

[1]: CTM_OPERATOR/CTM_OPERATOR_LCL

[2]: CTM_ENGINEER/CTM_ENGINEER_LCL

[3]: CTM_ENGINEER_ADM/CTM_ENGINEER_ADM_LCL

[4]: CTM_OPC/CTM_OPC_LCL

[5]: CTM_MAINTENANCE/CTM_MAINTENANCE_LCL

[6]: CTM_PROCESS/UGS_PROCESS

[7]: SYSTEM

[8]: ADS_MANAGER/ADS_MANAGER_LCL

[9]: ADS_PROCESS

To PSF_PROCESS, no rights are granted for access to DCOM components.

3.1.4 Local Security and User/Group

In addition to the Windows standard security policy, the following local security policy items are set for each user and group.

Table 3.1.4-1 Permissions Set for Local Security Policy

Policies	User/group (*1)													
	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]
Create global objects	No	No	No	No	No	No	Yes	Yes	No	No	No	No	No	No
Debug programs	No	No	Yes	Yes	No	Yes	Yes	No	No	No	No	No	No	No
Log on as a batch job	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	No
Log on as a service	No	No	No	No	No	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Deny log on locally	Yes (*2)	No	No	No	No	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Allow log on locally (*3)	No	No	Yes	Yes	No	Yes	No	No	No	No	No	No	No	No

*1: User/Group
[1]: OFFUSER
[2]: CTM_OPERATOR/CTM_OPERATOR_LCL
[3]: CTM_ENGINEER/CTM_ENGINEER_LCL
[4]: CTM_ENGINEER_ADM/CTM_ENGINEER_ADM_LCL
[5]: CTM_OPC/CTM_OPC_LCL
[6]: CTM_MAINTENANCE/CTM_MAINTENANCE_LCL
[7]: CTM_PROCESS
[8]: UGS_PROCESS
[9]: LIC_PROCESS
[10]: ADS_MANAGER/ADS_MANAGER_LCL
[11]: ADS_PROCESS
[12]: RDC_PROCESS/ADS_AGENT
[13]: PSF_PROCESS
[14]: VNT_COMMON, VNT_NVP_CORE, VNT_BKNET

*2: When the local PC is a file server.

*3: This policy is effective only for UACS station and it does not affect to others. In a UACS station, you can log on only as an administrator or the user accounts that belong to the groups listed as Yes in this table.

TIP

The PSF_PROCESS user is not granted permissions to each local security policy.

3.2 Personal Firewall Tuning

You can minimize connections from networks to the PCs in the system to fight against attacks by unauthorized persons.

■ Types of Exception Settings

Required communication ports are set as exception so that the functions of CENTUM VP can operate.

The following table describes the types of exception settings of the personal firewall.

Table 3.2-1 Types of Exception Settings

Type	Description
CENTUM related	Communication ports used by CENTUM related programs
Vnet/IP interface package related	Communication ports used by Vnet/IP interface package
DCOM related	Communication ports used by programs that perform DCOM communication (including OPC communication)
File sharing related	Communication ports used by Windows file sharing functions
Windows related	Communication ports used by Windows functions (excluding file sharing functions)
Computer switchover type UGS related	Communication ports used by computer switchover type UGS

■ CENTUM Related Exceptional Settings

The following table lists the CENTUM related exceptional settings.

Table 3.2-2 CENTUM Related Exceptional Settings

Service name/ execution file name	Protocol : port number	Package name or function name	Remarks
BKHOdeq.exe	TCP:20109	Standard Operation and Monitoring Function	Required when CENTUM VP is communicating with CENTUM CS system
BKHOdeq.exe	TCP:20171	Standard Operation and Monitoring Function	None
BKHTrGthr.exe	TCP:20110	Standard Operation and Monitoring Function	None
BKHLongTerm.exe	TCP:20183	Standard Operation and Monitoring Function	None
MnsServer.exe	UDP:34301	Standard Operation and Monitoring Function	None
BKBCopyD.exe	TCP:20111	Process Management Package	None
BKBBDFH.exe	TCP:20174	Process Management Package	None
BKBRECP.exe	TCP:20177	Process Management Package	None
BKBBDFH.exe	TCP:20178	Process Management Package	None
BKBRECP.exe	TCP:20179	Process Management Package	None

Continues on the next page

Table 3.2-2 CENTUM Related Exceptional Settings (Table continued)

Service name/ execution file name	Protocol : port number	Package name or function name	Remarks
BKESimmgr.exe	TCP:34205	Expanded Test Functions FCS Simulator Package HIS Simulator Package UACS Simulator Package	None
BKFSim_vhfd.exe	TCP:20010 ~ 20013 UDP:20010 ~ 20013	Expanded Test Functions FCS Simulator Package HIS Simulator Package UACS Simulator Package	None
Remote desktop service	TCP:3389	Server for Remote Operation and Monitoring Function Unified Gateway Station (UGS2) Standard Function	None
BKHFms.exe	TCP:20181	Multiple Project Connection Package	Only required in one PC within the CENTUM VP system
BKHFms.exe	TCP:20101	Multiple Project Connection Package	None
BKHFms.exe	TCP:20102	Multiple Project Connection Package	None
BKHFms.exe	TCP:20105	Multiple Project Connection Package	None
BKFApcsMng.exe	TCP:20184	APCS Control function	APCS/GSGW
sqlservr.exe	TCP:1433	SOE Server Package	SOE SQLServer
BKHProgMon.exe	UDP:34325	SOE Server Package	SOE
BKVMngService.exe	TCP:34333	SIOS	SIOS related
CAMSServer.exe	TCP:8819 TCP:8820 UDP:8819	CAMS for HIS Functions	CAMS
CAMSLogSvr.exe	UDP:8820	CAMS for HIS Functions	CAMS
Yokogawa.IA.iPCS.CENTUMVP.HIS.AlarmSetpoint.UI.exe	TCP:34419	Standard Operation and Monitoring Function	None
Yokogawa.IA.iPCS.Platform.License.LicenseManager.Service.exe	TCP:34417	License Management Function	None
Yokogawa.IA.iPCS.CENTUMVP.UGS.Facade.Service.exe	TCP:38000	UGS	None
Yokogawa.IA.iPCS.CENTUMVP.UGS.ENG.FileTransferServiceDispatcher.exe	TCP:38010 ~ 38012	UGS	None
Yokogawa.IA.iPCS.CENTUMVP.UGS.FB.Host.exe	TCP:40111 TCP:40113 ~ 40115	UGS	None
Yokogawa.IA.iPCS.CENTUMVP.UGS.System.Service.exe	TCP:38020 TCP:40112 TCP:40116	UGS	None
Yokogawa.IA.iPCS.CENTUMVP.UGS.Vnet.Host.exe	TCP:40117	UGS	None

Continues on the next page

Table 3.2-2 CENTUM Related Exceptional Settings (Table continued)

Service name/ execution file name	Protocol : port number	Package name or function name	Remarks
Yokogawa.IA.iPCS.CENTUMVP.UGS.Data-Sync.Host.exe	TCP: 38030	UGS	None
durm_udp.exe	UDP:1099	UGS	None
opxdas.exe	TCP:135	UGS	None
eqpmdc.exe	TCP:502	UGS	None
eqpfcx.exe	TCP:1090	UGS	None
eqpabc.exe	TCP:44818	UGS	None
IIS(FTP)	TCP:38040	UGS	UGS redundancy function (network switchover type)
Yokogawa.IA.iPCS.CENTUMVP.HIS.HISIS.HI-SInfService.exe	TCP:34420	Standard Operation and Monitoring Function	None
Yokogawa.IA.iPCS.ChronusENG.Serv-ices.Service.exe	Can be specified by the user TCP:34473 (default)	Automation Design Server	None
Yokogawa.IA.iPCS.ChronusENG.CIM-Agent.exe	Can be specified by the user TCP:34497 (default)	CENTUM VP station	Not affected by licenses
UACS.Client.ClientManager.exe	UDP:34568 UDP:34569	UACS UACS Simulator Package	
UACS.Kernel.exe	UDP:34570 UDP:34571 TCP:34572 TCP:34573 TCP:34574 TCP:34575	UACS UACS Simulator Package	
UACS.HistoricalServer.exe	TCP:34580 TCP:34581	UACS UACS Simulator Package	
UACS.HealthChecker.exe	TCP:34582 TCP:34583	UACS UACS Simulator Package	

■ Vnet/IP Interface Package Related Exceptional Settings

The following table lists the Vnet/IP interface package related exceptional settings.

Table 3.2-3 Vnet/IP Interface Package Related Exceptional Settings

Package name	Protocol : port number	Remarks
Vnet/IP interface package	UDP:520 UDP:5313 UDP:9940	Enable sending/receiving in the UDP ports mentioned on the left that are used in the Vnet/IP interface package

■ DCOM Related Exceptional Settings

The following table lists the DCOM related exceptional settings.

Table 3.2-4 DCOM Related Exceptional Settings

Service name/ execution file name	Protocol : port number	Assumed package name	Remarks
DCOM service	TCP:135	Programs using OPC communication	Required when using OPC communication.
DCOM service	TCP:20501 to 20550	Programs using OPC communication	Required when using OPC communication.

■ File Sharing Related Exceptional Settings

The following table lists the file sharing related exceptional settings.

Table 3.2-5 File Sharing Related Exceptional Settings

Service name/execution file name	Protocol : port number	Function name	Remarks
Sharing files and printers	TCP:139 UDP:137 UDP:138	NetBIOS	-
Sharing files and printers	TCP:445	Direct Hosting	If NetBIOS is disabled, separate means of name resolution, such as HOSTS file and registration to DNS, is required.
Sharing files and printers	UDP:5355	LLMNR	-

■ Windows Related Exceptional Settings

The following table lists the Windows related exceptional settings.

Table 3.2-6 Windows Related Exceptional Settings

Service name/execution file name	Protocol : port number	Server/station
Enable ICMP (*1)	ICMP	Domain controller File server CENTUM VP station
Kerberos Authentication	TCP:88 UDP:88	Domain controller
LDAP(Active Directory)	TCP:389 UDP:389	Domain controller
DNS	TCP:53 UDP:53	Domain controller
Windows Time	UDP:123	UGS
Network discovery	UDP:137 UDP:138 UDP:5355 UDP:3702 UDP:1900 TCP:2869 TCP:5358 TCP:5357 UDP:3702	CENTUM VP station

*1: This item may be ICMPv4 or ICMPv6, depending on the OS.

■ Caution

In a domain environment, this setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.

SEE ALSO For more information about the settings for managing the security policies of client computers collectively on a domain controller, refer to:

6.9, “Active Directory-Based Consolidated Management of IT Security Settings” on page 6-29

■ Allow unicast response

From IT security version 2.0, the Allow unicast response option is set to “No.”

Applications that use multicasting or broadcasting cannot receive the response.

TIP This setting is not configured on UGS.

3.3 Stopping Unused Window Services

You can reinforce security by stopping unused Windows services to prevent attacks by unauthorized persons. If vulnerabilities of Windows services are abused, user information in the product may be stolen or important data in the product may be leaked, tampered, or destroyed. In the worst case, attackers may steal the domain administrator rights.

■ Unused Windows Services

The following tables show the Windows services that can be stopped in IT security version 2.0 and IT security version 1.0.

Table 3.3-1 Windows Services That can be Stopped – IT security version 2.0

Service	Windows OS (*1)					
	10	7	2016	2012 R2	2008 R2	2008
Delivery Optimization (*2)	Yes (*3)	-	-	-	-	-
DHCP Client (*2)	No	Yes (*3)	No	Yes (*3) (*4)	Yes (*3)	Yes (*3)
Diagnostic Policy Service (*2)	Yes (*3)	Yes (*3)	Yes (*3)	Yes (*3)	Yes (*3)	Yes (*3)
Connected User Experiences and Telemetry (*2)	Yes (*3)	-	Yes (*3)	-	-	-
dmwappushsvc (*2)	Yes (*3)	-	Yes (*5)	-	-	-
Downloaded Maps Manager (*2)	Yes (*3)	-	Yes (*3)	-	-	-
IP Helper (*2)	Yes (*3)	Yes (*3)	Yes (*3)	Yes (*3)	Yes (*3)	Yes (*3)
IPsec Policy Agent (*2)	Yes (*5)	Yes (*5)	Yes (*5)	Yes (*5)	Yes (*5)	Yes (*3)
Offline Files (*2)	Yes (*5)	Yes (*3)	Yes (*7)	-	-	Yes (*5)
Program Compatibility Assistant Service (*2)	Yes (*3)	Yes (*3)	Yes (*3)	-	-	-
Remote Registry (*6)	Yes (*7)	Yes (*5)	Yes (*3)	Yes (*3)	Yes (*3)	Yes (*3)
Shell Hardware Detection (*8)	Yes (*3)	Yes (*3)	Yes (*3)	Yes (*3)	Yes (*3)	Yes (*3)
WebClient (*8)	Yes (*5)	Yes (*5)	-	-	-	-
Windows Error Reporting Service (*2)	Yes (*5)	Yes (*5)	Yes (*5)	Yes (*5)	Yes (*5)	Yes (*3)
Windows Push Notifications System Service (*2)	Yes (*3)	-	Yes (*3)	-	-	-

*1: 10: Windows 10
7: Windows 7
2016: Windows Server 2016
2012 R2: Windows Server 2012 R2
2008 R2: Windows Server 2008 R2
2008: Windows Server 2008
Yes: Service that can be stopped
No: Service that must not be stopped
–: Service that does not exist in the OS

*2: Unnecessary in the product.

*3: Because the Startup type for the Windows service is set to "Automatic" with the initial OS setting, it is changed to "Disabled" by the IT Security Tool.

*4: The DHCP client service is used in computer switchover type UGS.

*5: Because the Startup type for the Windows service is set to "Manual" with the initial OS setting, the IT Security Tool does not change this setting.

*6: Not required because the functions are not used and there are problems in terms of security.

*7: Because the Startup type for the Windows service is set to "Disabled" with the initial OS setting, the IT Security Tool does not change this setting.

*8: Not required because the functions are not used.

Table 3.3-2 Windows Services That can be Stopped – IT security version 1.0

Service	Windows OS (*1)					
	10	7	2016	2012 R2	2008 R2	2008
DHCP Client (*2)	No	Yes (*6)	No	Yes (*6) (*3)	Yes (*6)	Yes (*6)
Windows Error Reporting Service (*4)	Yes (*5)	Yes (*5)	Yes (*5)	Yes (*5)	Yes (*5)	Yes (*6)
IP Helper (*4)	Yes (*6)	Yes (*6)	Yes (*6)	Yes (*6)	Yes (*6)	Yes (*6)
IPsec Policy Agent (*4)	Yes (*5)	Yes (*5)	Yes (*5)	Yes (*5)	Yes (*5)	Yes (*6)
Offline Files (*4)	Yes (*5)	Yes (*6)	Yes (*8)	-	-	Yes (*5)
Remote Registry (*7)	Yes (*8)	Yes (*5)	Yes (*6)	Yes (*6)	Yes (*6)	Yes (*6)
Shell Hardware Detection (*9)	Yes (*6)	Yes (*6)	Yes (*6)	Yes (*6)	Yes (*6)	Yes (*6)
WebClient (*9)	Yes (*5)	Yes (*5)	-	-	-	-

*1: 10: Windows 10
7: Windows 7
2016: Windows Server 2016
2012 R2: Windows Server 2012 R2
2008 R2: Windows Server 2008 R2
2008: Windows Server 2008
Yes: Service that can be stopped
No: Service that must not be stopped
–: Service that does not exist in the OS

*2: Unnecessary because DHCP services are not used in the product.

*3: The DHCP client service is used in computer switchover type UGS.

*4: This service is not required in this product.

*5: Because the Startup type for the Windows service is set to "Manual" with the initial OS setting, the IT Security Tool does not change this setting.

*6: Because the Startup type for the Windows service is set to "Automatic" with the initial OS setting, it is changed to "Disabled" by the IT Security Tool.

*7: Not required because the functions are not used and there are problems in terms of security.

*8: Because the Startup type for the Windows service is set to "Disabled" with the initial OS setting, the IT Security Tool does not change this setting.

*9: Not required because the functions are not used.

■ Caution

In a domain environment, this setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.

SEE ALSO

For more information about the settings for managing the security policies of client computers collectively on a domain controller, refer to:

6.9, “Active Directory-Based Consolidated Management of IT Security Settings” on page 6-29

3.4 IT Environment Settings Common to IT Security Versions 2.0 and 1.0

This section describes the IT environment settings that are common to IT security versions 2.0 and 1.0. There may be cases where it is not possible to implement certain security functions depending on the conditions of the individual systems. For this reason, examine whether implementation is possible for each function before the implementation.

3.4.1 Disabling NetBIOS over TCP/IP

It is recommended to disable NetBIOS because attackers may be able to acquire a list of services running on the target computer and a list of users by using NetBIOS.

■ Settings

If the network connection name is "UACS Ethernet," set “Disable NetBIOS over TCP/IP.”

■ Cautions

Keep the following points in mind when disabling NetBIOS over TCP/IP.

- The computer name and station name must be the same.
- The computer name must be resolved by the DNS or HOSTS file.

3.4.2 HDD Password Function by BIOS

This function is provided in most PCs and protects HDD by using the ATA command that controls HDD. In normal BIOS password setting, it is possible to refer to data in HDD by removing the hard disk from a PC and connecting it to another PC. A HDD password locks the HDD itself, and it prohibits reading data even if HDD is removed and connected to another computer. Even if a PC is stolen, there is no fear that important data of the product leaks from the stolen PC. It is impossible to recover the data in the HDD once the HDD password is forgotten, and the password is required to enter when starting the computer. For this reason, this function must be introduced with greatest care.

Please contact the PC manufacturer whether or not this function is provided and how to set the function.

3.5 Group Policy Settings in IT Security Version 2.0

This section describes the group policy settings in IT security version 2.0. There may be cases where it is not possible to implement certain security functions depending on the conditions of the individual systems. For this reason, examine whether implementation is possible for each function before the implementation.

3.5.1 Disabling the Built-in Administrator Account or Changing the User Name

We recommend that you disable the built-in Administrator account because the built-in accounts that are created during the installation of Windows are easy targets of password cracking. On the Dual-redundant Platform for Computer of a computer switchover type UGS, an account for administration work and an account for maintenance work are provided. We also recommend that you change the user names of these accounts.

■ Cautions (when Disabling the Built-in Administrator Account)

You must consider the following points when you disable the built-in Administrator account:

- Disable the built-in Administrator account after creating a user with administrative rights.
- Be careful not to include root, su, admin, and other words meaning administrator in the name of user with administrator rights.
- Securely control users with administrator rights because they are required for operations.
- In a domain environment, this setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.

SEE ALSO

For more information about the settings for managing the security policies of client computers collectively on a domain controller, refer to:

6.9, “Active Directory-Based Consolidated Management of IT Security Settings” on page 6-29

■ Cautions when Changing the User Names on the Dual-redundant Platform for Computer of a Computer Switchover Type UGS

On the Dual-redundant Platform for Computer of a computer switchover type UGS, two accounts with administrative rights are provided with the default user names "ADMINISTRATOR" and "PATCHUSER." We recommend that you change these user names. You can change the user names by using the Redundancy Management Tool.

TIP

- ADMINISTRATOR
  User who connects to the maintenance server of the Dual-redundant Platform for Computer by using the Redundancy Management Tool and performs administrative work.
- PATCHUSER
  User who logs on to the Dual-redundant Platform for Computer and performs maintenance works such as patch program application.

Note the following points when you change the user name:

- The new user name must not contain the string "root", "su", or "admin", which implies an administrator.
- Manage the user names securely because they are required to perform administration work or maintenance work.

SEE ALSO

For more information about how to change user names by using the Redundancy Management Tool, refer to:

“■ Account settings” in D1.2.1, “Setting up redundant operations - Active UGS” in Unified Gateway Station Reference (IM 33J20C10-01EN)

3.5.2 Applying the Software Restriction Policies

The software restriction policies function of Windows restricts the execution of programs by setting the following types of rules:

- Restriction on path
- Restriction on hash
- Restriction on certificate
- Restriction on the Internet zone

In the product, path rules are applied to provide an environment where users can run only the specified programs. This prevents illegal execution of programs even if harmful programs are copied in a temporary folder or other locations of the computer.

The IT Security Tool supports Restriction on path. If this restriction is applied, other coexisting packages may not run.

■ Settings

The restriction on path of CENTUM VP is added to the restriction on path.

Specifically, the following paths are added.

- `%ALLUSERSPROFILE%\Microsoft\Windows\Templates` (*1)
- `%ALLUSERSPROFILE%\Templates`
- `%ALLUSERSPROFILE%\Yokogawa\IA\iPCS\Products\ChronusENG\Data\Projects` (*2)
- `%localappdata%\Microsoft\OneDrive\*\FileSyncConfig.exe` (*3)
- `%ProgramFiles%` (*4)
- `%ProgramFiles(x86)%` (*5)
- `%ProgramW6432%` (*6)
- `%ProgramFiles%\Yokogawa\IA\iPCS\Platform\Security\PROGRAM`
- `%ProgramFiles(x86)%\Yokogawa\IA\iPCS\Platform\Security\PROGRAM`
- `%SystemRoot%` (*7)
- CENTUM VP installation folder (*8)

The following rules are deleted.

- "Ink" and "mdb" are deleted from [Designated File Types Properties].

*1: %ALLUSERSPROFILE% refers to the following folder. This example is when the system drive is drive C.
`C:\ProgramData`
*2: This path is added when the Automation Design Master Database is to be stored in the default location.
*3: For Windows 10 only
*4: %ProgramFiles% refers to the following folder. This example is when the system drive is drive C.
`C:\Program Files`
*5: %ProgramFiles(x86)% refers to the following folder. This example is when the system drive is drive C.
`C:\Program Files(x86)`
*6: %ProgramW6432% refers to the following folder. This example is when the system drive is drive C.
`C:\Program Files`
*7: %SystemRoot% refers to the following folder. This example is when the system drive is drive C.
`C:\Windows`
*8: CENTUM VP installation folder refers to the following folder. This example is when the system drive is drive C.
`C:\CENTUMVP` (default value)

■ Cautions

This function can be configured by the IT Security Tool; however, in a domain environment, the setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.

SEE ALSO For more information about the settings for managing the security policies of client computers collectively on a domain controller, refer to:

6.9, “Active Directory-Based Consolidated Management of IT Security Settings” on page 6-29

● Cautions regarding Availability of Tools and Functions when Software Restriction Policies are Applied

You cannot use the following tools when software restriction policies are applied.

- Fieldbus engineering tool
- Device management tool

When you run an FCS simulator using the test function, you cannot enable the following functions when software restriction policies are applied.

- Plant training system (Exatif)
- Off-site blocks, enhanced switch instrument blocks, and valve pattern monitors

● Cautions when Software Restriction Policies are Applied

Observe the following points when software restriction policies are applied.

- When you install the software of the product or third party software from removable storage media, log on to the PC as an administrative user and run the setup program by right-clicking the program and selecting [Run as Administrator].
- When you run a program with an extension .bat, .cmd, reg, or .vbs, start the command prompt from the start menu by right-clicking the Command Prompt (cmd.exe) and selecting [Run as Administrator]. Then, run the program from the command prompt window.
- Microsoft Excel, Microsoft SQL Server, OPC server used for GSGW or SIOS, and third party software must be installed under `%ProgramFiles%` or `%ProgramFiles(x86)%`.
- Updating programs for display drivers may be installed immediately under drive C. When you update the driver, log on to the PC as an administrative user and run the updating program by right-clicking the program and selecting [Run as Administrator].
- When you extract a project backup file, create a temporary folder for extraction in a location separate from the product installation folder, such as the location immediately under the drive C, and store the project backup file, PJT.exe, in that folder. After you store the file PJT.exe, right-click on it and select [Run as Administrator] to extract it.
- When you install an OPC client, log on to the PC as an administrative user and run the OPC client setup program by right-clicking the program and selecting [Run as Administrator].
- User-created ActiveX controls must be stored under `<CENTUM VP installation folder>\his\users`.

● Precautions for Applying Software Restriction Policies

Keep the following points in mind before applying the software restriction policies.

- Microsoft Excel, Microsoft SQL Server, OPC server used for GSGW or SIOS, user-created ActiveX controls, and third party software must be installed in folders under the path that is to be added as software restriction policies. If these items are already installed in other folders, you need to reinstall them.

3.5.3 Applying the StorageDevicePolicies Function

By using the StorageDevicePolicies function of Windows, you can set removable storage media connected on USB ports as read-only devices. You can use this function to prevent theft of data by unauthorized users. You can use the StorageDeviceCTL utility of the product to temporarily grant write permissions to users.

SEE ALSO For more information about the StorageDeviceCTL, refer to:

6.10, “Other Utility Programs” on page 6-34

■ Setting

The following table shows the setting.

Table 3.5.3-1 Setting

Policy	Setting
Removable Disks: Deny write access	Enabled

■ Cautions

Keep the following points in mind when applying the StorageDevicePolicies function.

- If this function is applied on Windows Server 2008 R2, you cannot use StorageDeviceCTL to temporarily grant write permissions. To cancel the read-only state, you need to clear the [Applying the StorageDevicePolicies function] check box of the IT Security Tool's detailed settings and run the tool again. Note that, to disable taking out of data using removable storage media without using this function, you need to take security measures such as putting a cover on USB ports.
- In a domain environment, this setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.

SEE ALSO For more information about the settings for managing the security policies of client computers collectively on a domain controller, refer to:

6.9, “Active Directory-Based Consolidated Management of IT Security Settings” on page 6-29

3.5.4 Disabling USB Storage Devices

This function disables the use of USB storage devices such as USB memories. You can use this function to prevent theft of data by unauthorized users.

You can use the StorageDeviceCTL utility of the product to temporarily grant write permissions to users.

SEE ALSO For more information about the StorageDeviceCTL, refer to:

6.10, “Other Utility Programs” on page 6-34

■ Setting

The following table shows the setting.

Table 3.5.4-1 Setting

Policy	Setting
Floppy Drives: Deny execute access	Enabled
Floppy Drives: Deny read access	Enabled
Floppy Drives: Deny write access	Enabled
Removable Disks: Deny execute access	Enabled
Removable Disks: Deny read access	Enabled
Removable Disks: Deny write access	Enabled
WPD Devices: Deny read access	Enabled
WPD Devices: Deny write access	Enabled

■ Cautions

Keep the following points in mind when disabling USB storage devices.

- If this function is applied to Windows Server 2008 R2, you cannot use StorageDeviceCTL to temporarily grant write permissions. To cancel the disabling, you need to clear the [Disabling USB storage devices] check box of the IT Security Tool's detailed settings and run the tool again. To disable taking out of data using removable storage media without using this function, you need to take security measures such as putting a cover on USB ports.
- In a domain environment, this setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.

SEE ALSO For more information about the settings for managing the security policies of client computers collectively on a domain controller, refer to:

6.9, “Active Directory-Based Consolidated Management of IT Security Settings” on page 6-29

3.5.5 Applying the Password Policies

The strength of security for user authentication changes significantly depending on the set password. It is recommended to secure minimum password strength by applying the password policies.

■ Settings

The following table shows the settings.

Table 3.5.5-1 Settings

Policy	Setting
Minimum password length	12 characters or more
Minimum password age	One day
Validity period of password	70 days
Enforce password history	2 passwords
Password must meet complexity requirements	Enabled
Store password using reversible encryption	Disabled

■ Cautions

Keep the following points in mind when applying the password policies.

- If the password policies are made stricter, not only the load of password management on users but also the load of operation administrators to manage user's passwords increases.
- In a domain environment, this setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.

SEE ALSO For more information about the settings for managing the security policies of client computers collectively on a domain controller, refer to:

6.9, “Active Directory-Based Consolidated Management of IT Security Settings” on page 6-29

3.5.6 Advanced Audit Policy Configuration

Collected account logon conditions and events related to security serve as data useful in detecting abnormal system conditions in early stages and to trace causes of troubles when problems related to security occur. With IT security version 2.0, more detailed audit policy configuration is possible. Each setting item is described as follows.

■ Account Logon

The following table shows the setting.

Table 3.5.6-1 Setting

Policy	Setting
Audit Credential Validation	Both the Success and Failure check boxes are selected.

■ Account Management

The following table shows the setting.

Table 3.5.6-2 Setting

Policy	Setting
Audit Computer Account Management	The Success check box is selected.
Audit Other Account Management Events	Both the Success and Failure check boxes are selected.
Audit Security Group Management	Both the Success and Failure check boxes are selected.
Audit User Account Management	Both the Success and Failure check boxes are selected.

■ Detailed Tracking

The following table shows the setting.

Table 3.5.6-3 Setting

Policy	Setting
Audit Process Creation	The Success check box is selected.
Audit RPC events	Both the Success and Failure check boxes are cleared. (*1)

*1: In the case of domain controller and file server, both the Success and Failure check boxes are selected.

■ DS Access

This setting is for domain controllers only.

The following table shows the setting.

Table 3.5.6-4 Setting

Policy	Setting
Audit Directory Service Access	Both the Success and Failure check boxes are selected.
Audit Directory Service Changes	Both the Success and Failure check boxes are selected.

■ Logon/Logoff

The following table shows the setting.

Table 3.5.6-5 Setting

Policy	Setting
Audit Account Lockout	The Success check box is selected.
Audit Logoff	The Success check box is selected.
Audit Logon	Both the Success and Failure check boxes are selected.
Audit Other Logon/Logoff Events	Both the Success and Failure check boxes are selected.
Audit Special Logon	The Success check box is selected.

■ Object Access

The following table shows the setting.

Table 3.5.6-6 Setting

Policy	Setting
Audit Application Generated	Both the Success and Failure check boxes are cleared. (*1)
Audit Removable Storage	Both the Success and Failure check boxes are selected.

*1: In the case of domain controller and file server, both the Success and Failure check boxes are selected.

■ Policy Change

The following table shows the setting.

Table 3.5.6-7 Setting

Policy	Setting
Audit Policy Change	Both the Success and Failure check boxes are selected.
Audit Authentication Policy Change	Both the Success and Failure check boxes are selected.
Audit Filtering Platform Policy Change	Both the Success and Failure check boxes are selected.
Audit MPSSVC Rule-Level Policy Change	Both the Success and Failure check boxes are selected.
Audit Other Policy Change Events	Both the Success and Failure check boxes are selected.

■ Privilege Use

The following table shows the setting.

Table 3.5.6-8 Setting

Policy	Setting
Audit Sensitive Privilege Use	Both the Success and Failure check boxes are selected.

■ System

The following table shows the setting.

Table 3.5.6-9 Setting

Policy	Setting
Audit Other System Events	Both the Success and Failure check boxes are selected.
Audit Security State Change	Both the Success and Failure check boxes are selected.
Audit Security System Extension	Both the Success and Failure check boxes are selected.
Audit System Integrity	Both the Success and Failure check boxes are selected.
Audit IPsec Driver (*1)	Both the Success and Failure check boxes are selected.

*1: This setting is for domain controllers only.

3.5.7 Applying the Account Lockout Policy

This function is effective to protect the product from attacks such as online cracking.

■ Settings

The following table shows the settings.

Table 3.5.7-1 Settings

Policy	Setting
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	15 minutes
Account lockout duration	15 minutes

TIP

The setting values of the account lockout policies of the Dual-redundant Platform for Computer of a computer switchover type UGS are the same as the values in the previous table. Note that the account lockout policies are always applied on the Dual-redundant Platform for Computer of a computer switchover type UGS. These account lockout policies are used for user authentication of the Redundancy Management Tool.

■ Cautions

Keep the following points in mind when applying the account lockout policies.

- If this policy is applied and you fail to log on repeatedly, logging on to that user account will be disabled until the time set for “Reset account lockout counter after” elapses.
- In a domain environment, this setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.
- When you add a computer switchover type UGS to a Windows domain, set “Account lockout threshold” to “20 invalid logon attempts” on the domain controller.

SEE ALSO

For more information about the settings for managing the security policies of client computers collectively on a domain controller, refer to:

6.9, “Active Directory-Based Consolidated Management of IT Security Settings” on page 6-29

3.5.8 User Rights Assignment

With this function, only the specified users or groups are allowed to perform a certain operation.

■ Settings

The following table shows the settings.

Table 3.5.8-1 Settings

Policy	Group to delete	Group to add
Access this computer from the network (*1) (*2)	All the registered accounts (*1)(*2)	Administrators (*1) (*2) Authenticated Users (*1) (*2) Enterprise Domain Controllers (*1)
Add workstations to domain (*1)	Authenticated User	Administrators

*1: This setting is configured in the domain controller.
*2: This setting is configured on the UACS station.

3.5.9 Security Options

Various security options are enabled or disabled.

■ Settings

The following table shows the settings.

Table 3.5.9-1 Settings

Policy	Setting
Audit : Force audit policy subcategory settings (Windows Vista or later) to overwrite audit policy category settings	Enabled
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user only	Enabled
Devices: Restrict floppy access to locally logged-on user only	Enabled
Domain controller: Allow server operators to schedule tasks (*1)	Disabled
Domain controller: Refuse machine account password changes (*1)	Disabled
Domain member: Require strong (Windows 2000 or later) session key	Enabled
Interactive logon: Display user information when the session is locked	User display name, domain and user names
Interactive logon: Do not display last user name	Enabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Machine inactivity limit (*2)	Enabled 900 seconds
Interactive logon: Prompt user to change password before expiration	Enabled 14 days
Microsoft network server: Digitally sign communications (if client agrees)	Enabled
Microsoft network server: Server SPN target name validation level	Enabled Accept if provided by client
MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended except for highly secure environments)	Disabled
MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)	Enabled Highest protection, source routing is completely disabled
MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)	Disabled
MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)	Enabled 3
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled

Continues on the next page

Table 3.5.9-1 Settings (Table continued)

Policy	Setting
Network access: Do not allow storage of passwords and credentials for network authentication	Enabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network security: Allow Local System to use computer identity for NTLM	Enabled
Network security: Force logoff when logon hours expire (*1)	Enabled
Network security: Allow LocalSystem NULL session fallback	Disabled
Network security: LAN Manager authentication level	Enabled Send NTLMv2 response only
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Enabled • Require NTLMv2 session security • Require 128-bit encryption Both check boxes are selected.
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Enabled • Require NTLMv2 session security • Require 128-bit encryption Both check boxes are selected.
Network security: Do not store LAN Manager hash value on next password change	Enabled
Shutdown: Allow system to be shut down without having to log on	Disabled
User Account Control: Admin Approval Mode for the Built'-in Administrator account	Enabled
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Enabled Prompt for consent on the secure desktop

*1: This setting is configured in the domain controller.
*2: This setting is configured on the UACS station.

■ Cautions

On Windows Server 2008 and later version OS, the four setting items beginning with “MSS:” that are set as Security Options do not appear in the Local Group Policy Management Editor. Check their current setting by running the gpresult command.

3.5.10 Administrative Template

This section describes the group policy settings that are defined in the administrative template.

■ Personalization (Control Panel)

● Setting

The following table shows the setting.

Table 3.5.10-1 Setting

Policy	Setting
Prevent enabling lock screen camera	Enabled
Prevent enabling lock screen slide show	Enabled

■ WLAN Settings (Network)

● Setting

The following table shows the setting.

Table 3.5.10-2 Setting

Policy	Setting
Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services	Disabled

■ Audit Process Creation (System)

● Setting

The following table shows the setting.

Table 3.5.10-3 Setting

Policy	Setting
Include command line in process creation events	Disabled

TIP

If this option is enabled, the command line information of each process will be recorded to the security event log in text format as part of the Audit Process Creation event 4688, "A new process has been created." For example, if you set a password by using the CreateCentumProcess tool, the password specified as an argument is recorded in the event log.

■ Group Policy (System)

● Setting

The following table shows the setting.

Table 3.5.10-4 Setting

Policy	Setting
Configure registry policy processing	The check box of Process even if the Group Policy objects have not changed is selected.

■ Internet Communication Management (System)

● Setting

The following table shows the setting.

Table 3.5.10-5 Setting

Policy	Setting
Turn off access to the Store	Enabled
Turn off downloading of print drivers over HTTP	Enabled
Turn off Event Viewer "Events.asp" links	Enabled
Turn off Internet download for Web publishing and online ordering wizards	Enabled
Turn off printing over HTTP	Enabled
Turn off Search Companion content file updates	Enabled
Turn off the "Publish to Web" task for files and folders	Enabled
Turn off the Windows Customer Experience Improvement Program	Enabled
Turn off the Windows Messenger Customer Experience Improvement Program	Enabled

■ Logon (System)

● Settings

The following table shows the settings.

Table 3.5.10-6 Settings

Policy	Setting
Do not display network selection UI	Enabled
Do not enumerate connected users on domain-joined computers	Enabled
Enumerate local users on domain-joined computers	Disabled
Turn off app notifications on the lock screen	Enabled

■ Mitigation Options (System)

● Setting

The following table shows the setting.

Table 3.5.10-7 Setting

Policy	Setting
Untrusted Font Blocking	Enabled Block untrusted fonts and log events

- **Cautions**

If this setting is enabled, fonts that are not installed in %Windir%\Font (normally, C:\Windows \Font) cannot be used. In that case, install the fonts to be used in the above folder. You can install fonts by right-clicking the font and selecting [Install].

■ Power Management (System)

● Settings

The following table shows the settings.

Table 3.5.10-8 Settings

Policy	Settings
Turn Off the Display (On Battery) (*1)	Enabled 0
Turn Off the Display (Plugged In) (*1)	Enabled 0

*1: Undefined is selected for this setting on the UACS station.

■ User Profile (System)

● Setting

The following table shows the setting.

Table 3.5.10-9 Setting

Policy	Setting
Turn off the advertising ID	Enabled

■ App Privacy (Windows Component)

● Setting

The following table shows the setting.

Table 3.5.10-10 Setting

Policy	Setting
Let Windows apps access account information	Enabled Force Deny
Let Windows apps access call history	Enabled Force Deny
Let Windows apps access contacts	Enabled Force Deny
Let Windows apps access email	Enabled Force Deny
Let Windows apps access location	Enabled Force Deny
Let Windows apps access messaging	Enabled Force Deny
Let Windows apps access motion	Enabled Force Deny

Continues on the next page

Table 3.5.10-10 Setting (Table continued)

Policy	Setting
Let Windows apps access the calendar	Enabled Force Deny
Let Windows apps access the camera	Enabled Force Deny
Let Windows apps access the microphone	Enabled Force Deny
Let Windows apps access trusted devices	Enabled Force Deny
Let Windows apps control radios	Enabled Force Deny
Let Windows apps sync with devices	Enabled Force Deny

■ App Runtime (Windows Component)

● Setting

The following table shows the setting.

Table 3.5.10-11 Setting

Policy	Setting
Block launching Windows Store apps with Windows Runtime API access from hosted content	Enabled

● Cautions

This policy disables starting of Windows store applications that are directly accessed by Windows runtime API from Web content.

■ AutoPlay Policies (Windows Component)

These policies prevent automatic execution of programs from external media. This setting is effective as a measure against viruses that infect computers through USB memory devices (USB worms).

● Setting

The following table shows the setting.

Table 3.5.10-12 Setting

Policy	Setting
Turn off Autoplay	Enabled All drives
Disallow Autoplay for non-volume devices	Enabled

● Cautions

- If the AutoRun function for the drive is disabled, the installation menu does not start just by inserting the software medium of the product.
- If an HIS set is used, Autoplay is turned off for all drives regardless of the applied security model. This is a measure against USB worms.

- In a domain environment, this setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.

SEE ALSO For more information about the settings for managing the security policies of client computers collectively on a domain controller, refer to:

6.9, “Active Directory-Based Consolidated Management of IT Security Settings” on page 6-29

■ Cloud Content (Windows Component)

● Setting

The following table shows the setting.

Table 3.5.10-13 Setting

Policy	Setting
Do not show Windows tips	Enabled
Turn off Microsoft consumer experiences	Enabled

■ Data Collection and Preview Builds (Windows Component)

● Setting

The following table shows the setting.

Table 3.5.10-14 Setting

Policy	Setting
Allow Telemetry	Enabled 0 - Security [Enterprise Only]
Disable pre-release features or settings	Disabled
Do not show feedback notifications	Enabled
Toggle user control over Insider builds	Disabled

■ Event Log Service (Windows Component)

● Setting

The following table shows the setting.

Table 3.5.10-15 Setting

Policy	Setting
Specify the maximum log file size (KB)	Enabled 32768 KB

■ File Explorer (Windows Component)

● Setting

The following table shows the setting.

Table 3.5.10-16 Setting

Policy	Setting
Turn off heap termination on corruption	Disabled

HomeGroup (Windows Component)

Setting

The following table shows the setting.

Table 3.5.10-17 Setting

Policy	Setting
Prevent the computer from joining a homegroup	Enabled

OneDrive (Windows Component)

Setting

The following table shows the setting.

Table 3.5.10-18 Setting

Policy	Setting
Prevent the usage of OneDrive for file storage	Enabled
Save documents to OneDrive by default (Save documents to the local PC by default)	Enabled

Remote Desktop Service (Windows Component)

Settings

The following table shows the settings.

Table 3.5.10-19 Settings

Policy	Setting
Do not allow passwords to be saved	Enabled
Do not allow drive redirection (*1)	Enabled
Always prompt for password upon connection (*2)	Enabled
Require secure RPC communication	Enabled
Require user authentication for remote connections by using Network Level Authentication	Enabled
Set time limit for active but idle Remote Desktop Services sessions (*2) (*3)	Enabled 1h

*1: This setting is not configured on UGS.
*2: This setting is configured on the UACS station.
*3: An active but idle Remote Desktop Services session is disconnected when the specified time limit is reached.

Search (Windows Component)

Setting

The following table shows the setting.

Table 3.5.10-20 Setting

Policy	Setting
Allow Cortana	Disabled
Don't search the web or display web results in Search	Enabled
Don't search the web or display web results in Search over metered connections	Enabled

■ Software Protection Platform (Windows Component)

● Setting

The following table shows the setting.

Table 3.5.10-21 Setting

Policy	Setting
Turn off KMS Client Online AVS Validation	Enabled

■ Store (Windows Component)

● Setting

The following table shows the setting.

Table 3.5.10-22 Setting

Policy	Setting
Turn off Automatic Download of updates on Win8 machines	Enabled
Turn off Automatic Download and Install of updates	Enabled
Turn off the offer to update to the latest version of Windows	Enabled
Turn off the Store application	Enabled

■ Sync Your Settings (Windows Component)

● Setting

The following table shows the setting.

Table 3.5.10-23 Setting

Policy	Setting
Do not sync Apps	Enabled
Do not sync start settings	Enabled

■ Windows Defender (Windows Component)

● Setting

The following table shows the setting.

Table 3.5.10-24 Setting

Policy	Setting
Turn off Windows Defender	Enabled

■ Windows Error Reporting (Windows Component)

● Setting

The following table shows the setting.

Table 3.5.10-25 Setting

Policy	Setting
Automatically send memory dumps for OS-generated error reports	Disabled

■ Windows Logon Options (Windows Component)

● Setting

The following table shows the setting.

Table 3.5.10-26 Setting

Policy	Setting
Sign-in last interactive user automatically after a system-initiated restart	Disabled

3.5.11 User Configuration - Administrative Template

■ Notifications (Taskbar and Start Menu)

● Setting

The following table shows the setting.

Table 3.5.11-1 Setting

Policy	Setting
Turn off toast notifications on the lock screen	Enabled

3.6 Group Policy Settings in IT Security Version 1.0

This section describes the group policy settings in IT security version 1.0. There may be cases where it is not possible to implement certain security functions depending on the conditions of the individual systems. For this reason, examine whether implementation is possible for each function before the implementation.

3.6.1 Disabling the Built-in Administrator Account or Changing the User Name

The same cautions apply as for IT security version 2.0.

SEE ALSO For more information about the precautions when disabling the built-in Administrator account or changing its user name, refer to:

3.5.1, “Disabling the Built-in Administrator Account or Changing the User Name” on page 3-24

3.6.2 Hiding the Last Logon User Name

You can hide the last logon user name on the logon dialog box to prevent leakage of valid user names in the system.

■ Caution

Keep the following points in mind when hiding the last logon user name.

- You must enter a user name on every logon attempt if you apply this security measure.
- In a domain environment, this setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.

SEE ALSO

For more information about the settings for managing the security policies of client computers collectively on a domain controller, refer to:

6.9, "Active Directory-Based Consolidated Management of IT Security Settings" on page 6-29

3.6.3 Applying the Software Restriction Policies

The same setting and cautions apply as for IT security version 2.0.

SEE ALSO For more information about the settings that are configured when applying the software restriction policies, refer to:

“■ Settings” on page 3-25

For more information about the precautions when applying the software restriction policies, refer to:

“■ Cautions” on page 3-25

3.6.4 Applying AutoRun Restrictions

This restriction prevents automatic execution of programs when a DVD-ROM or other medium is inserted to the drive or a USB port. This is an effective measure against virus (USB worm) infecting computers via USB memory.

■ Setting Values

The AutoRun function is disabled for all drives.

■ Cautions

Keep the following points in mind when applying AutoRun restrictions.

- The installation menu does not start just by inserting the software medium of the product.
- In a domain environment, this setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.

3.6.5 Applying the StorageDevicePolicies Function

The same cautions apply as for IT security version 2.0.

SEE ALSO For more information about the precautions when applying the StorageDevicePolicies function, refer to:

“■ Cautions” on page 3-27

3.6.6 Disabling USB Storage Devices

The same cautions apply as for IT security version 2.0.

SEE ALSO For more information about the precautions when disabling USB storage devices, refer to:

“■ Cautions” on page 3-28

3.6.7 Changing the LAN Manager Authentication Level

Windows has LM authentication, NTLM authentication and NTLMv2 authentication methods for backward compatibility.

For the environment of the product, use of NTLMv2 authentication is recommended. LM authentication is not recommended since its method of hashing user's password (LM hash algorithm) is very vulnerable.

■ Setting

The following table shows the setting.

Table 3.6.7-1 Setting

Policy	Setting
Changing the LAN Manager Authentication Level	Send NTLMv2 response only
Do not allow storage of passwords and credentials for network authentication	Enabled
Minimum session security for NTLM SSP based (including secure RPC) clients	Require NTLMv2 session security Require 128-bit encryption
Minimum session security for NTLM SSP based (including secure RPC) servers	Require NTLMv2 session security Require 128-bit encryption
Let Everyone permissions apply to anonymous users	Disabled

■ Cautions

- Ensure that the settings of “Minimum session security for NTLM SSP based (including secure RPC) clients” and “Minimum session security for NTLM SSP based (including secure RPC) servers” are consistent on all terminals.
- In a domain environment, this setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.

SEE ALSO For more information about the settings for managing the security policies of client computers collectively on a domain controller, refer to:

6.9, “Active Directory-Based Consolidated Management of IT Security Settings” on page 6-29

3.6.8 Applying the Password Policies

The strength of security for user authentication changes significantly depending on the set password. It is recommended to secure minimum password strength by applying the password policies.

SEE ALSO For more information about the precautions when applying the password policy, refer to:

"■ Cautions" on page 3-29

■ Settings

The following table shows the settings.

Table 3.6.8-1 Settings

Policy	Settings
Minimum password length	12 characters or more
Change prohibition period of password	One day
Validity period of password	90 days
Storage of password history	24 passwords stored (25 password types or more are required)
Password must meet complexity requirements	Enabled
Store password using reversible encryption	Disabled

3.6.9 Applying the Audit Policy

Collected account logon conditions and events related to security serve as data useful in detecting abnormal system conditions in early stages and to trace causes of troubles when problems related to security occur. It is recommended to set appropriate audit policies.

■ Settings

The following table shows the settings.

Table 3.6.9-1 Settings

Policy	Settings
Audit account logon events	Both the Success and Failure check boxes are selected.
Audit account management	Both the Success and Failure check boxes are selected.
Audit object access	The Failure check box is selected.
Audit system events	Both the Success and Failure check boxes are selected.
Audit directory service access	Both the Success and Failure check boxes are selected.
Audit process tracking	The Success check box is selected.
Audit policy change	Both the Success and Failure check boxes are selected.
Audit logon events	Both the Success and Failure check boxes are selected.
Audit privilege use	Both the Success and Failure check boxes are selected.

■ Cautions

Keep the following points in mind when applying the audit policies.

- If the number of event types collected is increased, the system performance is affected.
- The number of generated events varies depending on the types of collected events and system operations. Determine the event collection size appropriate for the system operation conditions.
- In a domain environment, this setting may be overwritten with the setting in the domain controller, depending on the group policies of the domain controller. If this is your case, change the setting in the domain controller.

SEE ALSO For more information about the settings for managing the security policies of client computers collectively on a domain controller, refer to:

6.9, “Active Directory-Based Consolidated Management of IT Security Settings” on page 6-29

3.6.10 Applying the Account Lockout Policy

The same setting and cautions apply as for IT security version 2.0.

SEE ALSO For more information about the settings that are configured when applying the account lockout policy, refer to:

“■ Settings” on page 3-33

For more information about the precautions when applying the account lockout policy, refer to:

“■ Cautions” on page 3-33

4. Selection of Security Functions

In order to set security functions, it is necessary to take various items into consideration. This chapter explains the items to be considered and model cases that serve as reference when setting security functions.

4.1 Items to be Considered before Setting Security Functions

This section explains items to be considered when setting security functions.

■ Considerations on Determining Security Functions

The following items need to be considered according to the actual implementations.

These items should be determined before installing the software of the product.

- IT security version
- Security Model
- Windows user management type
- User authentication mode

● Selecting IT Security Version

Select either of the following versions according to the extent of configuration for security measures.

Table 4.1-1 Selecting IT Security Version

IT security version	Selection Criterion
2.0	This version includes more security policies compared to the security measures that had been offered until CENTUM VP R6.03. In addition, the administrative template for group policies is included as the target of security configuration. The Legacy model is no longer supported in IT security version 2.0.
1.0	This version had been offered as the security measures of CENTUM VP R6.03 and earlier versions.

● Selecting Security Model

A security model needs to be selected from the following three types.

Table 4.1-2 Selecting Security Model

Security Model	Selection Criterion
Legacy Model	Select this model when upgrading the system from a CENTUM project of R6.03 or earlier without changing the existing security settings or when sharing Windows users among multiple operators. The Legacy model can be selected only with IT security version 1.0. If this model is selected, the system remains vulnerable against information leak and attacks by worms and viruses.
Standard Model (Recommended)	It is recommended to select this model unless you have a specific reason not to. This model provides minimum security settings necessary for the product, considering secure operation of the system as well as collaboration with other systems.
Strengthened Model	Select this model when security level higher than the Standard model is required. Consult Yokogawa agent when implementing this model.

● Windows User Management

Select Windows user management method according to the system size and configuration from the following three types.

Table 4.1-3 Selecting User Management Type

User Management	Selection Criterion
Standalone Management	This type is suitable for relatively small-scale systems because the user accounts and passwords of all PCs of a system need to be kept consistent.
Domain Management	This type is suitable for systems that implement a centralized user management. When this type is selected, it is recommended to set a new, dedicated domain controller when constructing the system.
Combination Management	This type is suitable for the system where user management is centralized but some users are allowed to be independently managed in local PCs.

● User Authentication Mode

Select one of the following user authentication modes based on the operation conditions and security policies.

Table 4.1-4 Selecting User Authentication Mode

User Authentication Mode	Selection Criterion
CENTUM Authentication Mode	This mode performs the same authentications as the CENTUM systems prior version R4.03. Select this mode when the Windows users and CENTUM users are authenticated separately.
Windows Authentication Mode	Select this mode when the Windows users, CENTUM operation and monitoring users and system configuration users are authenticated together. This mode is suitable for the system that the higher level security is applied.

When Windows authentication mode is selected, only one authentication is required before operating the HIS. This is referred to as Single Sign On.

There are following two types of single sign on. You can select either type on each HIS or PC installed with system builders.

Table 4.1-5 Selecting Single Sign On

Type	Remarks
Windows Type Single Sign On	When switching user, you need to log off Windows first and then use a different user account to log on.
HIS Type Single Sign On	This type is suitable for the PC used as a HIS operation and monitoring console. Switching user can be performed on User-In dialog box of HIS instead of logging off and logging on Windows. However, switching user on HIS only changes the operation and monitoring privilege on HIS console but the permissions on manipulating Windows programs (for an example, permissions to manipulate Start Menu items) are retained to the privilege of the user (OFFUSER) who automatically logged on Windows. Moreover, if the OFFUSER logs off Windows, for logging on Windows again, you need to restart the PC.

■ Precautions when Setting Security Functions

The following table lists the precautions to be observed when setting security measures.

Table 4.1-6 Precautions when Setting Security Functions

Security function	Item to be considered
Screen Saver Function	If the HIS type single sign on of Windows authentication mode is selected, [On resume, password protected] option is not available.

Continues on the next page

Table 4.1-6 Precautions when Setting Security Functions (Table continued)

Security function	Item to be considered
Password protection for CTM_PROCESS/ UGS_PROCESS/LIC_PROCESS/RDC_PROCESS/ OFFUSER	CTM_PROCESS/UGS_PROCESS/LIC_PROCESS/RDC_PROCESS/ OFFUSER (*1) are changed, it is necessary to match passwords on all computers where CTM_PROCESS/UGS_PROCESS/LIC_PROCESS/ RDC_PROCESS/OFFUSER (*1) exist regardless of the user management type.
Operation Keyboard User Switch Function	If access control for each user utilizing the Windows authentication mode as the user authentication mode is being examined, it is necessary to consider use of the operation keyboard user switch function upon understanding that it is not suited for access control of each user because user rights can be upgraded temporarily.
Setting IT Security for File Server/Domain controller	If the IT Security Tool is used either on a file server or a domain controller, it is necessary to install .NET Framework 3.0 or a later version. (*2)

*1: OFFUSER is required only when the HIS Type Single Sign On of the Windows authentication mode is used for operation.
*2: .NET Framework3.5 SP1 is included in the CENTUM VP installation medium.

4.2 Model Cases

This section describes the recommended settings for the following model cases:

- Case where CENTUM VP is newly implemented
- Case where a project database is placed on a file server
- Case where users are centrally managed within the CENTUM VP system only
- Case where users are centrally managed in multiple CENTUM VP systems
- Case where Yokogawa products not supporting IT security are included in the system
- Case where a system prioritizing security is constructed
- Case where YOKOGAWA products with IT security version 1.0 or equivalent security are included in the system

■ Case where CENTUM VP is Newly Implemented (System with Fewer HISs that Comprehensive User Management is Not Required)

Table 4.2-1 Case where CENTUM VP is Newly Implemented

Security function	Recommended setting
Selection of IT security version	2.0
Security model	Standard model
Windows user management	Standalone management
User authentication mode	Windows authentication mode
Software Restriction Policies	N/A
Screen Saver Function	[On resume, password protected] option should not be checked.
CTM_PROCESS/OFFUSER Password	Not required to change password
Operation Keyboard User Switch Function	Enable the user switch function
File Server	If a file server is constructed, apply the Standard model (standalone management) as IT security.
Domain controller	Not required

■ Case where a Project Database is Placed on a File Server

Table 4.2-2 Case where a Project Database is Placed on a File Server

Security function	Recommended setting
Selection of IT security version	2.0
Security model	Standard model
Windows user management	Standalone management
User authentication mode	Windows authentication mode
Software Restriction Policies	Apply
Screen Saver Function	[On resume, password protected] option should not be checked.
CTM_PROCESS/OFFUSER Password	Not required to change password
Operation Keyboard User Switch Function	Enable the user switch function
File Server	Standard model (standalone management)
Domain controller	Not required

■ Case where Users are Centrally Managed within the CENTUM VP System Only

Table 4.2-3 Case where Users are Centrally Managed within the CENTUM VP System Only

Security function	Recommended setting
Selection of IT security version	2.0
Security model	Standard model
Windows user management	Domain management
User authentication mode	Windows authentication mode
Software Restriction Policies	Apply
Screen Saver Function	[On resume, password protected] option should not be checked.
CTM_PROCESS/OFFUSER Password	Not required to change password
Operation Keyboard User Switch Function	Disable the user switch function
File Server	Construct the server if there are 10 or more PCs of HIS and system builders. If a file server is constructed, apply the Standard model (domain/combination management) as IT security.
Domain controller	Construct anew (apply the Standard model (domain/combination management) as IT security).

■ Case where Users are Centrally Managed in Multiple CENTUM VP Systems

Table 4.2-4 Case where Users are Centrally Managed in Multiple CENTUM VP Systems

Security function	Recommended setting
Selection of IT security version	2.0
Security model	Standard model
Windows user management	Combination management
User authentication mode	Windows authentication mode
Software Restriction Policies	Apply
Screen Saver Function	[On resume, password protected] option should not be checked.
CTM_PROCESS/OFFUSER Password	Not required to change password
Operation Keyboard User Switch Function	Disable the user switch function
File Server	Construct the server if there are 10 or more PCs of HIS and system builders. If a file server is constructed, apply the Standard model (domain/combination management) as IT security.
Domain controller	Reuse an existing server (apply the Standard model (domain/combination management) as IT security. Alternatively, conform to the security policies of the implemented users).

■ Case where Yokogawa Products not Supporting IT Security are Included in the System

Table 4.2-5 Case where Yokogawa Products not Supporting IT Security are Included in the System

Security function	Recommended setting
Selection of IT security version	1.0 (*1)
Security model	Legacy model
Windows user management	Standalone management
User authentication mode	CENTUM authentication mode
Software Restriction Policies	N/A
Screen Saver Function	[On resume, password protected] option should not be checked.
CTM_PROCESS/OFFUSER Password	Not required to change password
Operation Keyboard User Switch Function	Enable the user switch function
File Server	Construct a server if there are 10 or more PCs of HIS and system builders. Apply the Legacy model of IT security settings.
Domain controller	Not required

*1: To select Legacy model as the security model, set the IT security version to 1.0.

■ Case where a System Prioritizing Security is Constructed

When constructing a system prioritizing security, examine the security taking the operation fully into consideration.

Table 4.2-6 Case where a System Prioritizing Security is Constructed

Security function	Recommended setting
Selection of IT security version	2.0
Security model	Strengthened model
Windows user management	Domain management
User authentication mode	Windows authentication mode
Software Restriction Policies	Apply
Screen Saver Function	[On resume, password protected] option should be checked.
CTM_PROCESS/OFFUSER Password	Required to change password
Operation Keyboard User Switch Function	Disable the user switch function
File Server	Strengthened model (domain/combination management)
Domain controller	Construct anew (apply the Strengthened model (domain/combination management) as IT security).

Blank Page

5. Precautions on Operations

This section describes the precautions related to security when operating the product.

5.1 Windows Account Management

Two types of Windows account management are assumed, common account management and individual account management, considering sharing of the user accounts often used in the systems that were built before the security functions are introduced.

■ Common Account Management and Individual Account Management

The following table shows the differences between the common account management and individual account management.

Table 5.1-1 Common Account Management and Individual Account Management

Account management method	Operation form	Convenience of operation		Security strength	
Common account management	A Windows account is shared by multiple users.	High	The same operability as the systems that were built before the security functions are introduced.	Low	Highly anonymous and disadvantageous.
Individual account management	A Windows account is assigned to a single user.	Low	Windows logoff and logon are required at personnel shift, and thus cumbersome compared to the systems that were built before the security functions are introduced.	High	Advantageous because access control of each user is possible.

5.1.1 Common Account Management

The common account management is highly convenient to operate because it is similar to the conventional account management of the systems that were built before the security functions are introduced. However, from the security point of view, anonymity is high and security strength level is low. When applying the common account management, take personnel education and security of operation environment fully into consideration.

■ Use of Accounts

If the common accounts are used, it is recommended to group accounts by rights of users and use common accounts within a group. By grouping by rights of users, it becomes possible to prohibit operations on the product by users without rights and to narrow down user groups when tracing the trouble occurrence. It is considered that more usable trace data is obtained compared to the case when common accounts are used among all users.

■ Password Management

Considering security, it is recommended to change passwords periodically. It is possible to handle password cracking attacks by periodically changing passwords. If common accounts are used, it is recommended to change passwords at the timing when members using the common accounts are changed. By changing passwords, illegal access from previously authorized people is prevented.

■ Automatic Logon Function

If the automatic logon function is used, it is recommended to assign accounts belonging to the CTM_OPERATOR group to users to whom the automatic logon function is applied. If accounts belonging to other user groups are set, people without rights to the CENTUM VP system might inadvertently use system builders, and so on.

5.1.2 Individual Account Management

With the individual account management, it is possible to minimize rights on accounts by specifying PC users. Moreover, it is possible to trace trouble occurrence more efficiently because users can be identified. However, the individual account management is different from conventional operations on several points, such as Windows log off/log on becomes necessary at personnel shift. More careful consideration is required when implementing the individual account management.

■ Account Maintenance

If user rights are changed, it is recommended to promptly change account rights.

By performing account maintenance immediately, it becomes possible to handle illegal access by users who used to have rights before and/or unexpected attacks from attackers.

For example, if a user left the job, delete the account of the user; if the scope of charge of a maintenance personnel is changed, change the group to which the personnel belongs.

■ Password Management

Considering security, it is recommended to change passwords periodically. Password cracking can be prevented by periodically changing the user passwords.

5.1.3 Common Precautions for Common Account Management/Individual Account Management

This section lists precautions common to the common account management and individual account management.

■ System Audit

It is recommended to perform system audit periodically. By doing so, it is possible to detect system abnormalities in early stages, which leads to early discovery of signs of troubles and accidents. If any abnormalities are found, consult network administrators or experts to take appropriate measures.

■ Account Management by Standalone Management

When managing accounts by standalone management, it is not only necessary to create the same user account for all PCs used by users and PCs installed with system builders on which project databases exist, but also unify passwords of registered accounts. Note that, when changing a password, it is also necessary to change the password to the same new password on all the PCs in which the same account is registered.

■ Account Management by Domain Management

If the time on the domain controller and the time on PCs in the system of the product significantly differ (5 minutes or longer by default), the authentication function does not work properly in the domain environment. Pay attention to the time deviation between the domain controller and each PC.

■ CTM_MAINTENANCE Group

CTM_MAINTENANCE, which is a group for maintenance, has very powerful rights, including administrator rights. It is desired to treat accounts belonging to CTM_MAINTENANCE as invalid accounts under normal operation and enable the accounts when they are in need. Moreover, setting valid periods for accounts at the timing to enable the accounts is also an effective security measure.

■ Users who can Use OPC

Users who can use OPC can use the DCOM function on remote sites, so it is desired to minimize the number of registered users who can use OPC to reduce their influences on the system. Moreover, if target users use only programs, deleting the logon right is also an effective measure.

■ User Creation Method for Groups Having Windows Administrator Rights

When creating a user belonging to CTM_ENGINEER_ADM, CTM_ENGINEER_ADM_LCL, CTM_MAINTENANCE, or CTM_MAINTENANCE_LCL, it is necessary to add the user to either the Administrators group or the Domain Admins group as well.

5.2 Related Programs

This section explains the following related programs.

- Windows Security Patches
- Antivirus software

■ Windows Security Patches

It is assumed that security patches are applied according to the customer's security policy.

YOKOGAWA recommends to apply Windows security patches to the product. 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.

As is noted as zero-day attack, attacks that take advantage of the software vulnerability can occur right after the disclosure of the vulnerability (security hole).

Note that when security patches and service packs are applied to the product, existing security settings (firewall setting and local security setting) may be changed. If security patches and service packs are applied, make sure that the existing security settings are valid.

■ Antivirus Software

It is recommended to install antivirus software tested by YOKOGAWA on PCs and domain controllers within the system before starting operations. For more information about application of antivirus software, contact YOKOGAWA Service.

If search engines and pattern files of antivirus software are updated, it may have unexpected rebooting or unexpected influence on other operations of PC. Exercise sufficient cautions when updating antivirus software, such as checking the operation beforehand using a test purpose PC.

5.3 Precautions regarding security when introducing and operating a CENTUM VP system

This section describes general precautions regarding security when introducing and operating a CENTUM VP system.

■ Remote access to HIS and computer installed with system builders

When you implement remote access to HIS and computer installed with system builders by using the HIS-TSE function, you can adopt two-factor authentication using Windows functions.

■ Informing Users of Entry to a Security Zone

When the product is installed in a security zone, you can use the following measure so that the user who is trying to log on to the system is informed that he/she is entering a security zone and the subsequent operations will be performed in the security zone. Take this measure if necessary:

For the Windows local security policy under Control Panel, select [Local Policy] > [Security Options]and configure the following policies:

- [Interactive logon: Message title for users attempting to log on]
- [Interactive logon: Message text for users attempting to log on]

■ If Behavior Suspected to be Resulting from Vulnerability is Found

If you find any behavior of the product suspected to be resulting from the vulnerability of our products, please inform YOKOGAWA.

Blank Page

6. Utility Programs for Security Settings

This section describes the IT Security Tool and other utility programs for security setting.

6.1 IT Security Tool

The IT Security Tool is the security configuration tool for YOKOGAWA system products. You need to use this tool to provide security measures on computers where the product is installed.

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

IMPORTANT

- When changing the roles of a computer such as changing the HIS/ENG in the file servers, you need to reinstall the OS.
- When the IT security configured for a computer is wrong, such as configuring IT security settings for file server in a HIS/ENG, you need to reinstall the OS.

■ Functional Overview of the IT Security Tool

The following table describes the functions of the IT Security Tool.

Table 6.1-1 Functions of the IT Security Tool

Function	Description
Information	Displays the summary of the security settings that were configured by the IT Security Tool.
Setup	According to the selected IT security version, configures the security settings by setting the security model and user management type.
Save	Saves the security settings of the OS. The security settings are encrypted with a specified password (encryption key).
Restore	Restores the security settings of the OS to the saved security settings.
Change Password (Encryption Key)	Changes the password (encryption key) of the saved security settings. This function is used when you want to change the password periodically.
Import or Export	Exports the information configured by the IT Security Tool to a file. Or, imports an exported file.

When IT security version 2.0 is selected, only the Standard model is available for security model. The user management type is selectable from Domain, Combination, and Standalone management.

When IT security version 1.0 is selected, either the Standard model or Legacy model can be selected for security model. The user management type is selectable from Domain, Combination, and Standalone management.

The default display of the IT security setup window differs depending on whether the tool is used during new installation or upgrading from an earlier version of the product.

■ IT Security Version

IT security versions are classified based on the strength of the security settings of each security model and the extent of settings.

● IT Security Version 2.0

This version was designed after reconsidering the IT security version1.0 and includes more security measures.

● IT Security Version 1.0

This version had been offered as the security measures of CENTUM VP R6.03 and earlier versions.

■ Security Models

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

● Standard Model

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

TIP

If you need a higher level of security than what the Standard model provide, the Strengthened model is available. Please consult YOKOGAWA if IT security of the Strengthened model is required.

● Legacy Model

This model does not strengthen security. This model can be used if the priority is to be compatible with CENTUM CS 3000 R3 or earlier versions, and to integrate with other YOKOGAWA products that do not support the IT Security Tool. Since this model disables Windows Firewall, you need to consider the possible impact of this model's vulnerability to information leaks, worms, and virus attacks when you select this model.

■ User Management Types

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

● Domain Management

Select this option when managing user and group accounts using the Windows domain controller.

● Standalone Management

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

● Combination Management

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

6.2 Running the IT Security Tool

SEE ALSO For more information about running the IT Security Tool, refer to:

“■ Running the IT Security Tool” in B4.7, “Configuring IT Security Settings” in CENTUM VP Installation (IM 33J01C10-01EN)

6.3 Changing the IT Security Settings

This section describes how to change the security settings that have been applied.

Changing the security settings may do the following:

- Change the security model
- Change the IT security version
- Change the user management type
- Change Individual setting items

IMPORTANT

Before you change the IT security settings, take a backup of the current security settings.

SEE ALSO

For more information about backing up the security settings, refer to:

6.4, “Saving the IT Security Settings” on page 6-13

6.3.1 Procedure for Computers Installed with the CENTUM VP Software

This section describes the procedures for changing the security settings on a computer where the software of the product is installed.

■ Precautionary Notes

Precautionary notes on changing IT security settings on a computer installed with the software of the product are as follows:

● Changing the Security Model When a Product Supporting Old IT Security Functions Coexists

To change the security model on a computer where any other products that support old IT security functions are installed, you need to have the MAINTENANCE rights for the product supporting old IT security functions. Log on as a user who is a member of both the MAINTENANCE and CTM_MAINTENANCE groups and change the security model. When you change the security model, first change the security model for the product supporting old security functions, and then change the security model for CENTUM VP.

The versions of the products supporting old IT security functions are as follows:

- CENTUM VP earlier than R5.01
- PRM earlier than R3.10
- ProSafe-RS earlier than R3.01
- Exaopc earlier than R3.70
- Exapilot earlier than R3.90
- Exaplog earlier than R3.40

When any one of these products is installed on the same computer, the IT security version is 1.0. You can check the IT security version in the Current setting information dialog box.

SEE ALSO For more information about how to call up the Current setting information dialog box, refer to:

6.8, “Viewing the Information Configured by the IT Security Tool” on page 6-28

● Changing to Legacy Model When User Authentication Mode is Windows Authentication Mode

When changing to the Legacy model for a system using Windows authentication, you must change it to use CENTUM authentication.

SEE ALSO For more information about CENTUM authentication mode setting, refer to:

B4.11.1, “Setting CENTUM Authentication Mode” in CENTUM VP Installation (IM 33J01C10-01EN)

● Changing the User Management Type When User Authentication Mode is Windows Authentication Mode

If you have changed the user management type from Standalone type to Domain/Combination type, or vice versa, you need to configure the settings for using Windows authentication again.

SEE ALSO For more information about Windows authentication mode setting, refer to:

C4., “Changing from CENTUM Authentication Mode to Windows Authentication Mode” in CENTUM VP Installation (IM 33J01C10-01EN)

● When the User Management Type is Not Changed

You can configure the IT security settings without removing/adding the computer from/to the domain.

● Changing from Legacy/Standard Model (Standalone Management) to Standard Model (Domain/Combination Management)

Before you configure the IT security settings, add the computer to the domain.

● Changing from Standard Model (Domain/Combination Management) to Legacy/Standard Model (Standalone Management)

Before you configure the IT security settings, remove the computer from the domain.

● Changing the IT Security Version Only

Just change the IT security version, with no additional procedure.

● Changing the IT Security Version and Security Model/User Management Type at the Same Time

Terminate all applications that are running.

IMPORTANT

Before you change the IT security settings, take a backup of the current security settings.

■ User Who Can Change IT Security Settings

To be able to change the IT security settings, you need to have the required rights depending on the applied security model and user management type.

Table 6.3.1-1 User Who Can Change IT Security Settings

Currently applied security model and user management type		Security model and user management type to be applied		
		Legacy model	Standard model	
			Standalone type	Domain/Combination type
Legacy model		Local user who belongs to both the Administrators and CTM_MAINTENANCE groups of the local computer		Domain user who belongs to both the Domain Admins and CTM_MAINTENANCE groups of the domain (*1)
				Local user who belongs to both the Administrators and CTM_MAINTENANCE groups of the local computer(*1)(*2)
				Domain user who belongs to both the Administrators and CTM_MAINTENANCE groups of the local computer(*1)
Standard model	Standalone type			Local user who belongs to both the Administrators and CTM_MAINTENANCE groups of the local computer(*1)(*2)
				Domain user who belongs to both the Administrators and CTM_MAINTENANCE groups of the local computer(*1)
	Domain/Combination type	Local user who belongs to both the Administrators and CTM_MAINTENANCE_LCL groups of the local computer (*3)		Domain user who belongs to both the Domain Admins and CTM_MAINTENANCE groups of the domain(*1)
				Local user who belongs to both the Administrators and CTM_MAINTENANCE groups of the local computer(*1)(*2)
				Domain user who belongs to both the Administrators and CTM_MAINTENANCE_LCL groups of the local computer(*1)

*1: Log on to the computer when the computer is connected to the domain.
*2: While changing, the user name and password of the domain administrator are required.
*3: Before you change the IT security settings, remove the computer from the domain.

■ Changing Procedure

1. Log on to the computer as the user who changes the security settings.
2. From the Start menu, start the IT Security Tool.
3. Click [Setup].
4. Select the security model and user management type you want to change to.
   The rest of the procedure is the same as that for the normal setups.

SEE ALSO

For more information about running the IT Security Tool, refer to:

> "■ Running the IT Security Tool" in B4.7, "Configuring IT Security Settings" in CENTUM VP Installation (IM 33J01C10-01EN)

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)

6.3.2 Procedures for a File Server or Domain Controller

This section describes the procedures for changing the security settings on a computer that serves only as a file server or a domain controller computer.

IMPORTANT

When you change the IT security settings on a file server or domain controller computer, prepare the initial security settings that were saved before using the IT Security Tool.

■ User Who Can Change IT Security Settings on a File Server

To be able to change the IT security settings on a file server, you need to have the required rights depending on the applied security model and user management type.

Table 6.3.2-1 User Who Can Change Security Settings

Currently applied security model and user management type		Security model and user management type to be applied		
		Legacy model	Standard model	
			Standalone type	Domain/Combination type
Legacy model		Local user who belongs to the Administrators group of the local computer	Local user who belongs to both the Administrators and CTM_MAINTENANCE groups of the local computer	Domain user who belongs to both the Domain Admins and CTM_MAINTENANCE groups of the domain (*1)
				Local user who belongs to both the Administrators and CTM_MAINTENANCE groups of the local computer(*1)(*2)
				Domain user who belongs to both the Administrators and CTM_MAINTENANCE groups of the local computer(*1)
Standard model	Standalone type	Local user who belongs to both the Administrators and CTM_MAINTENANCE groups of the local computer		Local user who belongs to both the Administrators and CTM_MAINTENANCE groups of the local computer(*2)(*3)
				Domain user who belongs to both the Administrators and CTM_MAINTENANCE groups of the local computer(*2)(*3)
	Domain/Combination type	Local user who belongs to both the Administrators and CTM_MAINTENANCE_LCL groups of the local computer (*4)		Domain user who belongs to both the Domain Admins and CTM_MAINTENANCE groups of the domain(*1)
				Local user who belongs to both the Administrators and CTM_MAINTENANCE_LCL groups of the local computer(*1)(*2)
				Domain user who belongs to both the Administrators and CTM_MAINTENANCE_LCL groups of the local computer(*1)

*1: Log on to the computer while it is connected to the domain.
*2: While changing, entry of the user name and password of the domain user is required.
*3: Certain task is required while the computer is not joining the domain and after the computer joined the domain.
*4: Before you change the IT security settings, remove the computer from the domain.

User Who Can Change IT Security Settings on the Domain Controller

When changing the IT security settings on the domain controller computer, log on the computer as a user who belongs to both the Domain Admins and CTM_MAINTENANCE groups of the domain.

Changing Procedure

The following three procedures are described here.

- Basic procedure
- Procedure to change from Standard model (Standalone management) to Standard model (Domain/Combination management) on a file server
- Procedure to change from Standard model (Domain/Combination management) to Standard model (Standalone management) on a file server

Basic Procedure for Changing Security Settings

1. Log on as the user who changes the security settings.
2. Start the installation menu from the software medium of the product, and click [Setting IT Security (File server/domain controller use)] to start the IT Security Tool.
3. Click [Restore].
4. Select a file that the previous security settings are saved prior to running the IT Security Setting Tool so as to restore the securities.
   For a file server, if it is not a domain member now, use the file holding the initial security settings that were saved while it was standalone. If it is a domain member now, use the file holding the initial security settings that were saved after it joined the domain.
5. After restoring is completed, restart the computer.
6. For a file server, if its domain membership is to be changed, add to or remove from the domain.
7. Start the installation menu again and click [Setting IT Security (File server/domain controller use)] to start the IT Security Tool.
8. Click [Setup].
9. Select the security model and the user management type you want to change to.
   The rest of steps are the same as the procedure for the first time setup.

SEE ALSO For more information about how to start the installation menu, refer to:

B4.6, “Installing the CENTUM VP Software” in CENTUM VP Installation (IM 33J01C10-01EN)

For more information about restoring the security settings of a file server or domain controller computer where the CENTUM VP software is not installed, refer to:

6.5.2, “Procedure for a File Server or Domain Controller” on page 6-21

For more information about the first time configuring the security settings on a file server with the CENTUM VP software not installed, refer to:

B6.1, “Setting Up a Computer that Serves Only as a File Server” in CENTUM VP Installation (IM 33J01C10-01EN)

For more information about the first time configuring the security settings on a domain controller computer with the CENTUM VP software not installed, refer to:

B2.4, “Configuring Security Settings for the Domain Controller” in CENTUM VP Installation (IM 33J01C10-01EN)

● When Changing from Standard Model (Standalone Management) to Standard Model (Domain/Combination Management) on a File Server

For this change, you need to save the security settings after the file server computer joined a domain because the security settings are changed by joining the domain. Follow these steps to make the change:

1. Log on as an administrative user who belongs to both the Administrators and CTM_MAINTENANCE groups of the local computer
2. Start the installation menu from the software medium of the product.
3. Click [Setting IT Security (File server/domain controller use)] to start the IT Security Tool.
4. Restore the initial security settings saved (while the computer is not a member of a domain) before you fist time used the IT Security Tool to setup security.
5. After restarting, add the computer to the domain.
6. Log on as the same administrative user you previously logged on in step 1.
7. Start the installation menu and click [Setting IT Security (File server/domain controller use)].
   The IT Security Tool starts.
8. Click [Save].
9. Save the security settings as the initial settings right after it joined a domain.
10. On the IT Security Tool's menu, click [Setup].
11. Select the security model and user management type for the file server, and run the setup.
12. After applying the security settings, restart the computer.

● When Changing from Standard Model (Domain/Combination Management) to Standard Model (Standalone Management) on a File Server

For this change, the timing of removal from the domain is different from the basic procedure.

1. Log on as an administrative user who belongs to both the Administrators and CTM_MAINTENANCE_LCL groups of the local computer
2. Remove the computer from the domain.
3. Restart the computer, and log on as the same administrative user that you logged on in step 1.

4. Start the installation menu from the software medium of the product.
5. Click [Setting IT Security (File server/domain controller use)] to start the IT Security Tool.
6. Click [Restore] to restore the initial security settings that were saved before the IT Security Tool was first used to setup security (before the computer joined a domain).
7. Restart the computer.
8. Log on as the same administrative user you previously logged on in step 1.
9. Start the installation menu from the software medium of the product.
10. Click [Setting IT Security (File server/domain controller use] to start the IT Security Tool.
11. Click [Setup], select Standard model and Standalone management for the file server, and run the setup.
12. After applying the security settings, restart the computer.

■ Changing the IT Security Version

Follow these steps to change the IT security version from 1.0 to 2.0 on a file server or domain controller computer:

1. Start the installation menu from the software medium of the product, and start the IT Security Tool.
2. Click [Restore] to restore the initial settings that were saved by using the saving function of the IT Security Tool before the computer went into operation. After restore, restart PC.
3. Perform Step 1.
   Perform the following steps 4 to 5 by using the IT Security Tool.
4. Click [Save] and save the restored settings.
5. Click [Setup], and set the security model that you want to apply.

6.4 Saving the IT Security Settings

You can save the security settings on the local computer using the Save function.

The saved IT security settings can be restored by using the Restore function of the IT Security Tool as necessary.

■ User Who Can Save Security Settings

To be able to save the IT security settings, you need to have the required rights depending on the applied security model and user management type.

Table 6.4-1 User Who Can Save Security Settings

Currently applied security model and user management type		
Legacy model	Standard model	
	Standalone type	Domain/Combination type
User who belongs to the Administrators group of the local computer	User who belongs to both the Administrators and CTM_MAINTENANCE groups of the local computer	User who belongs to both the Administrators and CTM_MAINTENANCE_LCL groups of the local computer
		User who belongs to both the Domain Admins and CTM_MAINTENANCE groups of the domain

■ Regarding the Files that Hold the Saved Security Settings

Saving the security settings creates two files with extensions of .hed and .csf.

When restoring the saved security settings, both files are required.

6.4.1 Procedure for Computers Installed with the CENTUM VP Software

This section describes the procedures for saving the security settings on a computer where the software of the product is installed.

■ Saving Procedure

1. From the Start menu, start the IT Security Tool.
2. Click [Save].
   The Specify destination page appears.

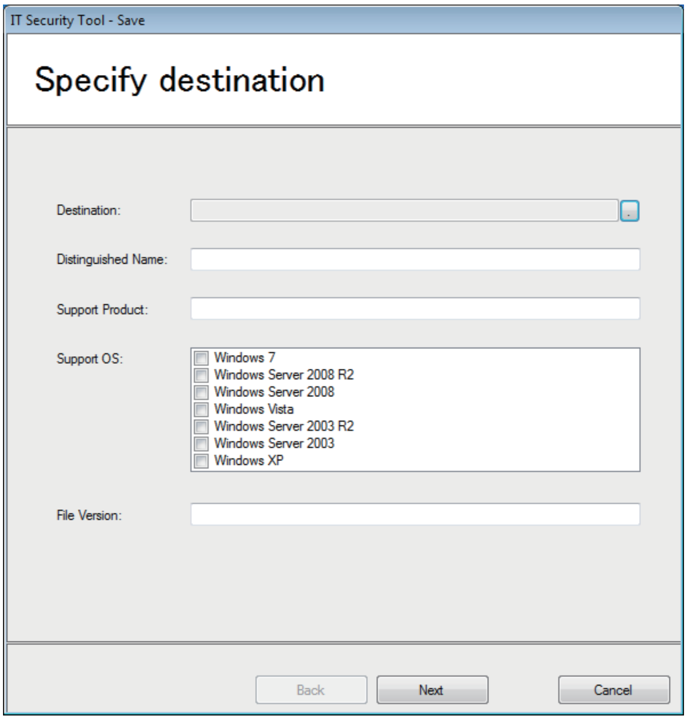
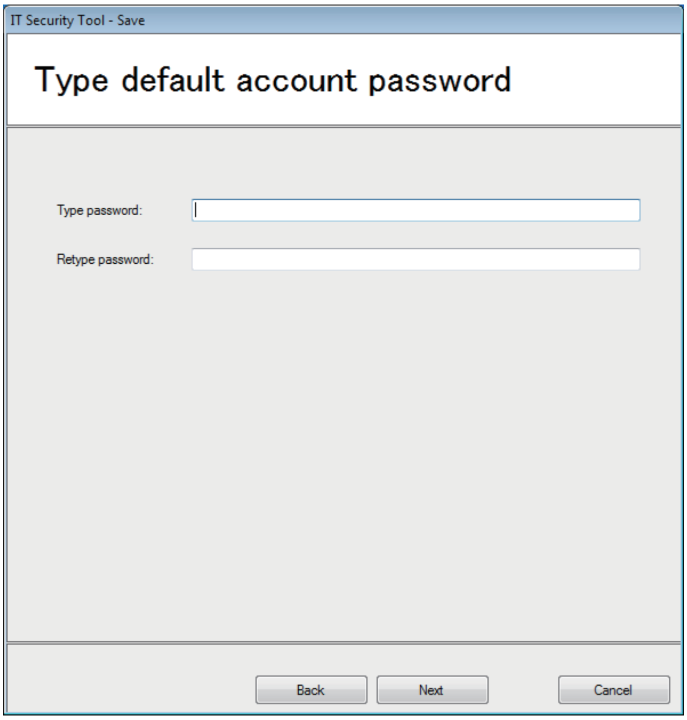


Figure 6.4.1-1 Specify Destination

3. Specify the destination folder and enter other required settings.
   The Distinguished Name and File Version are omissible.
4. Click [Next].
   The Type default account password page appears.



Type default account password

Type password:

Retype password:

Figure 6.4.1-2 Type Default Account Password

5. Enter the password for use as the initial account password and click [Next].

TIP

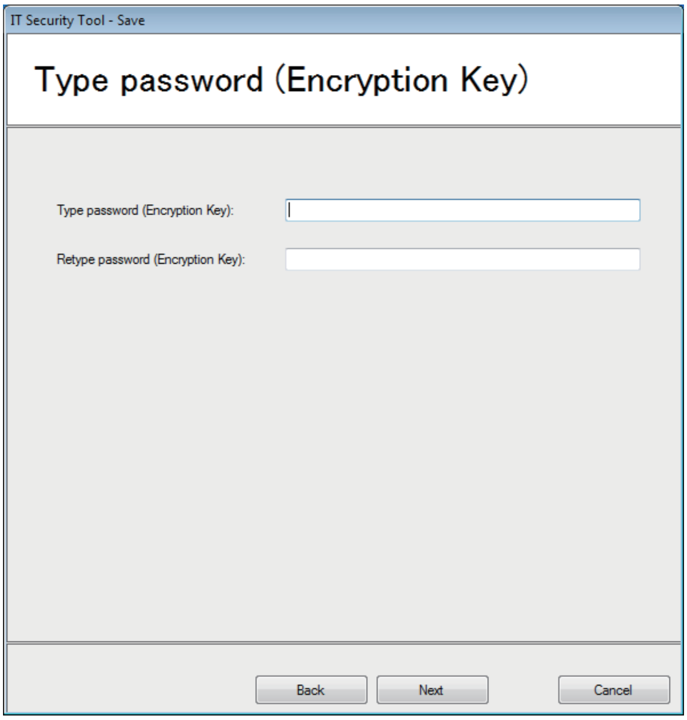
This default password will be used when you recover the accounts that were saved with this tool. If the saved account does not exists at restoration, the account is created. This default password will be set as the initial password of the created account.

If multiple accounts have been created, the same password is set for all accounts.

If the set password does not meet the password policy for restoration, an error will occur when recovering an account.

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

The page for entering the password for use as the encryption key of the saved data appears.



IT Security Tool - Save

Type password (Encryption Key)

Type password (Encryption Key):

Retype password (Encryption Key):

Figure 6.4.1-3 Type Password (Encryption Key)

6. Enter the Encryption Key and then click [Next].
   Saving of the security settings starts.

IMPORTANT

- If this password (encryption key) is lost, the saved security settings cannot be restored. The password (encryption key) must be carefully kept by the customer.
- The password (encryption key) must be at least one character.
- The password can consist of upper-case and lower-case alphanumeric characters and the following symbols: ` ~ ! @ # $ % ^ & *( ) _ + - = { } | \ : " ; ' < > ? , . /

  Double-byte characters cannot be used.

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

IMPORTANT

If any save failures are displayed, contact YOKOGAWA Service.

SEE ALSO

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)

6.4.2 Procedure for a File Server or Domain Controller

To save the IT security settings on a computer that serves only as a file server or a domain controller computer, start the installation menu from the software medium of the product and click [Setting IT Security (File server/domain controller use)] to start the IT Security Tool. The rest of steps are the same as the procedure for computers where the software of the product is installed.

IMPORTANT

You cannot save the group policy settings that were distributed from the domain controller. You can save only local group policy settings.

SEE ALSO

For more information about how to start the installation menu, refer to:

B4.6, “Installing the CENTUM VP Software” in CENTUM VP Installation (IM 33J01C10-01EN)

6.5 Restoring the IT Security Settings

You can restore the security settings of a local computer that were saved by using the Save function.

■ Preparation for Restoration

According to the user management type of the security settings to be restored, the computer may be required to join a domain or removed from a domain. To restore to the Legacy model or Standard model with Standalone management, the computer needs to be removed from a domain. To restore to the Standard model with Domain or Combination management, the computer needs to join a domain.

■ User Who Can Restore Security Settings

To be able to restore the IT security settings, you need to have the required rights depending on the applied security model and user management type.

Table 6.5-1 User Who Can Restore Security Settings

Security model and user management type to be restored to		
Legacy model	Standard model	
	Standalone type	Domain/Combination type
User who belongs to the Administrators group of the local computer	User who belongs to both the Administrators and CTM_MAINTENANCE groups of the local computer	User who belongs to both the Administrators and CTM_MAINTENANCE_LCL groups of the local computer (*1)
		User who belongs to both the Domain Admins and CTM_MAINTENANCE groups of the domain

*1: Log on as a user who belongs to the groups shown in the cell below when the CTM_MAINTENANCE_LCL group does not exist on the local computer (that is, when the security model and user management type set before restoration is Legacy model or Standard model with Standalone management).

6.5.1 Procedure for Computers Installed with the CENTUM VP Software

This section describes the procedures for restoring the security settings on a computer where the software of the product is installed.

IMPORTANT

If you saved the security settings by using the IT Security Tool, you must restore the same user management status as the saved status.

■ Restoring Procedure

1. From the Start menu, start the IT Security Tool.
2. Click [Restore].
   The Select Security Setting File page appears.

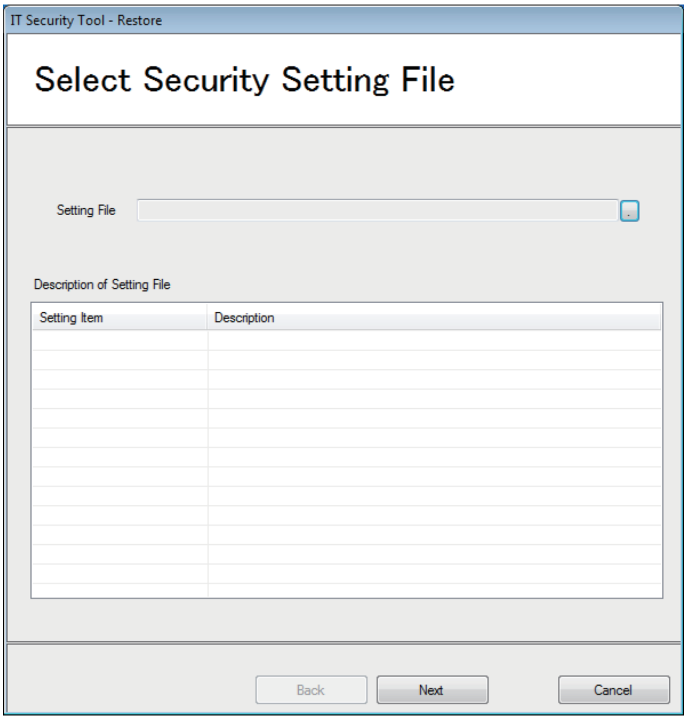

IT Security Tool - Restore
Select Security Setting File
Setting File
Description of Setting File
Setting Item
Description
Back
Next
Cancel

Figure 6.5.1-1 Select Security Setting File

3. Click [...] next to the Setting File box.
   The Open dialog box appears.
4. Select the file you want to use for restoration and then click [Open].

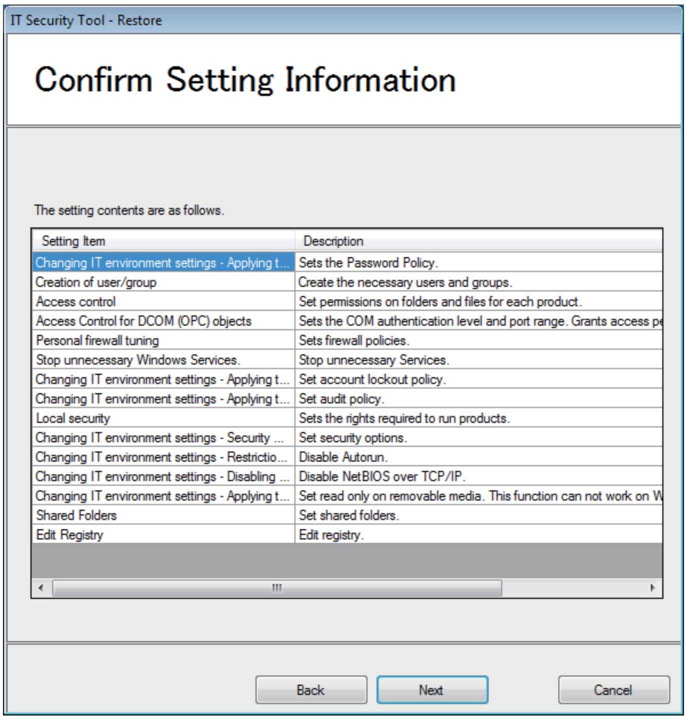
TIP

Among the saved and created files, you need to select a file with .hed extension.

A dialog box appears, prompting you to enter the password (encryption key) for reading the selected file.

5. Enter the password (encryption key) that was set when the file was saved and click [OK].
   If the selected file is restorable, the details are displayed in the Select Security Setting File page.
6. Click [Next].

The Confirm Setting Information page appears.



Confirm Setting Information

The setting contents are as follows.

Setting Item	Description
Changing IT environment settings - Applying t...	Sets the Password Policy.
Creation of user/group	Create the necessary users and groups.
Access control	Set permissions on folders and files for each product.
Access Control for DCOM (OPC) objects	Sets the COM authentication level and port range. Grants access pe
Personal firewall tuning	Sets firewall policies.
Stop unnecessary Windows Services.	Stop unnecessary Services.
Changing IT environment settings - Applying t...	Set account lockout policy.
Changing IT environment settings - Applying t...	Set audit policy.
Local security	Sets the rights required to run products.
Changing IT environment settings - Security ...	Set security options.
Changing IT environment settings - Restrictio...	Disable Autorun.
Changing IT environment settings - Disabling ...	Disable NetBIOS over TCP/IP.
Changing IT environment settings - Applying t...	Set read only on removable media. This function can not work on W
Shared Folders	Set shared folders.
Edit Registry	Edit registry.

Figure 6.5.1-2 Confirm Setting Information

TIP

Items displayed in the Confirm Setting Information page represent the items accessed when restoring the saved security settings. Although the descriptions of these items are affirmative sentences, it doesn't mean that all of these settings will be applied. Note that the status of whether each item is set to be applied or not is not displayed on the screen.

7. Confirm the settings and click [Next].
   When the setup process is complete, the Setup Completed page appears.

TIP

If there are any items that failed to be set, a list of failed items is displayed.

8. Select the check box for [Restart Now] and click [Finish].
9. Click [Close] to end the IT Security Tool.

IMPORTANT

If any setup failures are displayed, contact YOKOGAWA Service.

SEE ALSO

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)

6.5.2 Procedure for a File Server or Domain Controller

To restore the IT security settings on a computer that serves only as a file server or a domain controller computer, start the installation menu from the software medium of the product and click [Setting IT Security (File server/domain controller use)] to start the IT Security Tool. The rest of steps are the same as the procedure for computers where the software of the product is installed.

SEE ALSO For more information about how to start the installation menu, refer to:

B4.6, “Installing the CENTUM VP Software” in CENTUM VP Installation (IM 33J01C10-01EN)

6.6 Changing the Security Setting File Password

You can change the password (encryption key) for security setting files used by the IT Security Tool.

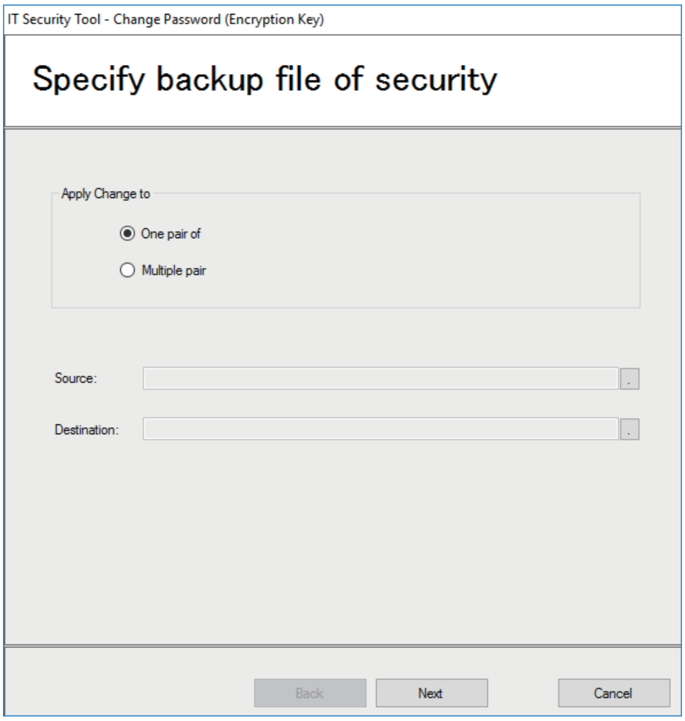
6.6.1 Procedure for Computers Installed with the CENTUM VP Software

This section describes the procedure for changing the password (encryption key) for security setting files on a computer where the software of the product is installed.

When changing password, the two files with .hed version and .csf version having same file name are considered as a set. You can select either [One pair of] or [Multiple pair] for changing passwords. If you select [Multiple pair], the passwords of all the files within the specified folder are changed.

■ Changing Procedure

1. Log on as a member of the CTM_MAINTENANCE group and start the IT Security Tool from the Start menu.
2. Click [Change Password (Encryption Key)].
   The Specify backup file of security page appears.



IT Security Tool - Change Password (Encryption Key)

Specify backup file of security

Apply Change to

● One pair of

○ Multiple pair

Source:

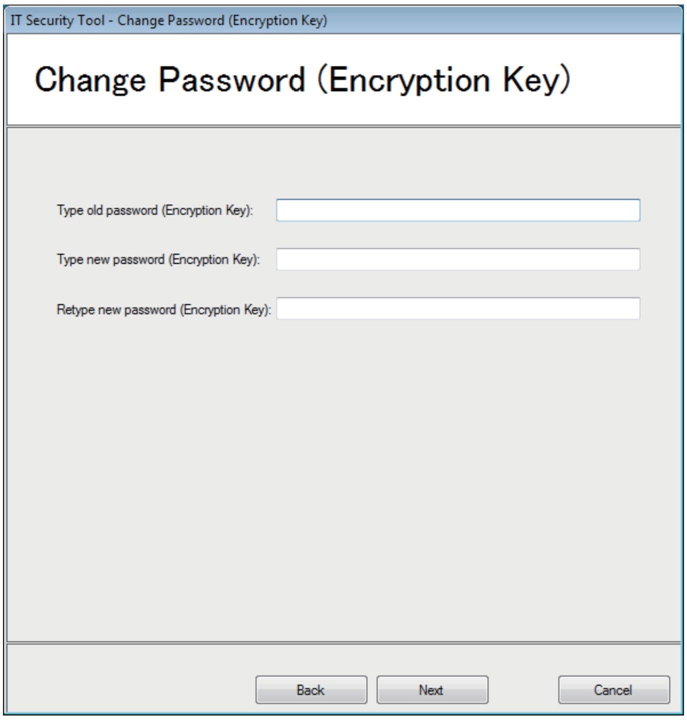
Destination:

Figure 6.6.1-1 Specify backup file of security

3. Select either of the Apply change to options and set as follows :
   - For changing the encryption key of one pair

     In the [Apply change to] section, select [One pair of], and select the folder where the file set before change and the file set after change are to be saved. Select .hed file as the file set before change.
   - For changing the encryption key of multiple pair

     In the [Apply change to] section, select [Multiple pair], select the folder that contains the file set before change and the folder in which the file set after change is to be saved.
4. Click [Next].
   The Change Password (Encryption Key) page appears.



IT Security Tool - Change Password (Encryption Key)

Change Password (Encryption Key)

Type old password (Encryption Key):

Type new password (Encryption Key):

Retype new password (Encryption Key):

Figure 6.6.1-2 Change Password (Encryption Key)

5. Enter the old and the new encryption keys and click [Next].
   When the changing process is completed, the Changed Password (Encryption Key) page appears.
6. Click [Finish].
7. On the IT Security Tool menu, click [Close].

SEE ALSO

For more information about mapping of CENTUM VP applications that can be called up 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)

6.6.2 Procedure for a File Server or Domain Controller

This section describes the procedure for changing the password (encryption key) for security setting files on a computer that serves only as a file server or a domain controller computer.

■ Changing Procedure

1. Log on as a member of the CTM_MAINTENANCE group.
2. Start the installation menu from the software medium of the product, and click [Setting IT Security(File server/domain controller use)] to start the IT Security Tool.
   The rest of steps are the same as the procedure for computers where the software of the product is installed.

SEE ALSO For more information about how to start the installation menu, refer to:

B4.6, “Installing the CENTUM VP Software” in CENTUM VP Installation (IM 33J01C10-01EN)

6.7 Importing/Exporting the IT Security Setting File

You can export and import the IT security settings configured by the IT Security Tool. Although the IT Security Tool has the functions to save and restore the security settings, you cannot use them to restore the OS dependent settings onto a different OS version. You can use the export and import functions for configuration onto a different OS version.

■ Export Procedure - IT Security Tool

1. Log on as a member of the CTM_MAINTENANCE group.
2. From the Start menu, start the IT Security Tool.

TIP

For a file server or a domain controller, start the installation menu from the software medium of the product, and click [Setting IT Security(File server/domain controller use)] to start the IT Security Tool.

3. From the main menu of the tool, click [Import or Export].
   The Export or Import the Selection State of Setting Items dialog box appears.
4. In the Operation selection section, select [Export].
   The default file name of the export destination appears in the File selection box. If you want to export to a file with a name other than the default file name, change the file name directly or click the button to the right of the text box and specify a file.

TIP

Specify xml as the file extension. When any other extension is specified, '.xml' is added automatically to the end of the file name.

5. Click [Execute].
   The information is written to the specified file, and the Export or Import the Selection State of Setting Items dialog box closes.

SEE ALSO

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)

■ Export Procedure - ITSecuritySettingItemExport.exe

To export the IT security settings that were configured before R6.04, use the ITSecuritySettingItemExport tool.

1. Log on as a member of the CTM_MAINTENANCE group.
2. Select `\\CENTUM\SECURITY\ITSecuritySettingItemExport.exe` in the software medium.
3. The file is exported to the following fixed folder.
   `C:\ProgramData\Yokogawa\IA\iPCS\Platform\Security\Config\DisplaySelectInfo.xml`

■ Import Procedure - IT Security Tool

1. Log on as a member of the CTM_MAINTENANCE group.
2. From the Start menu, start the IT Security Tool.

TIP

For a file server or a domain controller, start the installation menu from the software medium of the product, and click [Setting IT Security(File server/domain controller use)] to start the IT Security Tool.

3. From the main menu of the tool, click [Import or Export].
   The Export or Import the Selection State of Setting Items dialog box appears.
4. In the Operation selection section, select [Import].
   In the File selection box, type the name of the file you want to import or click the button to the right of the text box and specify a file.
5. Click [Execute].
   The specified file is read, and the Export or Import the Selection State of Setting Items dialog box closes.
6. From the main menu of the tool, click [Setup].
   The imported settings are applied, and the IT Security Settings dialog box appears.

SEE ALSO

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)

6.8 Viewing the Information Configured by the IT Security Tool

You can view the security information of the computer that was configured by the IT Security Tool.

The information displayed is classified into three categories:

- IT Security Tool information
  Displays the information on the version, copy right, and issuer of the IT Security Tool.
- Basic information on IT security settings
  Displays the security model, user management type, and IT security version set by the IT Security Tool.
- IT security setting status
  Displays the status of IT security setting for all YOKOGAWA products that are installed on the computer where the IT Security Tool is started.

  The products for which IT security setting is completed are listed under ITSecuritySetting-Completed.

  The products for which IT security setting is not yet applied are listed under InstallCompleted.

■ Procedure for Viewing

1. Log on as a member of the CTM_MAINTENANCE group.
2. From the Start menu, start the IT Security Tool.

TIP

For a file server or a domain controller, start the installation menu from the software medium of the product, and click [Setting IT Security(File server/domain controller use)] to start the IT Security Tool.

3. Click the [Information] button.
   The Current setting information dialog box appears.

SEE ALSO

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)

6.9 Active Directory-Based Consolidated Management of IT Security Settings

Windows Active Directory has a feature called Group Policy that is used to centrally manage the IT environment of computers and users. Using this Group Policy, you can manage the security policies for client computers within the domain in bulk by offering files for importing IT security settings. The following tasks are required:

- On the domain controller, create group policy objects for implementing security policies.
- By using Active Directory services, create Organizational Units on the domain controller and apply the group policy objects.

TIP

In Active Directory-based consolidated management of Group Policy on Windows Server 2008, the settings under Advanced Audit Policy Configuration, one of the Group Policy category items, cannot be managed or applied to client computers. In addition, on client computers running Windows Server 2008, the settings under Advanced Audit Policy Configuration cannot be configured from Active Directory.

6.9.1 Creating Group Policy Objects

Follow these steps to create group policy objects for implementing security policies on the domain controller:

1. Insert the installation medium of the product into the drive of the domain controller computer.
2. Using Explorer, copy the following file to any folder on the domain controller. You must copy the file to a folder to which the administrator of the domain can access.
   `<Drive of software medium> : \CENTUM¥SECURITY\GPOFiles\xxx\CTM_Standard_xxx.zip`
   - When the value of xxx is 2.0, the file corresponds to the Standard model of IT security version 2.0
   - When the value of xxx is 1.0, the file corresponds to the Standard model of IT security version 1.0
3. Double click the file that you have copied.
   The file expands into files for import.
4. Open Control Panel.
5. Select [Administrative Tools] > [Group Policy Management].
   The Group Policy Management dialog box appears.
6. In the left pane, right-click [Group Policy Objects] and select [New].
   The New GPO dialog box appears.
7. Set as follows:
   - Type any name for [Name].
   - Select [(none)] for [Source Starter GPO].
8. Click [OK].
   A new group policy object is created.
9. Right-click the new group policy object and select [Import Settings].
   The [Import Settings Wizard] appears.
10. Click [Next].
    A dialog box appears, prompting you to back up the existing settings.
11. Since it is a newly created group policy object, click [Next] without backing up.
    [Backup location] appears.
12. In the [Backup folder], select the parent folder of the folder to be imported, and click [Next].
    A list of importable group polices that are stored under the selected parent folder appears.

TIP

If you want to view the setting information of the group policy object, click [View Settings...]. The information is displayed in Microsoft Internet Explorer.

13. Select the group policy and click [Next].
    A confirmation dialog box appears, showing whether the group policy to be imported contains any references to security principals or UNC paths.

TIP

The following message is displayed in the confirmation dialog box.

“Scan Results:

The Backup do not contain any references to security principals or UNC paths. To continue, click [Next].”

14. Click [Next].

The [Completing the Import Settings Wizard] dialog box appears.

15. Click [Finish].
    Importing of the group policy object starts.

16. When the importing is completed, confirm the imported policy in [Group Policy Management].
    Open Control Panel and select [Administrative Tools] - [Group Policy Management] to open Group Policy Management . In the left pane, right-click the target group policy and select [View].

Creation of a group policy object is now completed. Subsequently, you need to create Organizational Units on the domain controller and apply group policy objects to them.

6.9.2 Applying Group Policy Objects to an Organizational Unit

Follow these steps to apply group policy objects to an Organizational Unit on the domain controller:

1. Log on to the domain controller as an administrative user.
2. Open Control Panel.
3. Select [Administrative Tools] > [Active Directory Users and Computers].
   Active Directory Users and Computers appears.
4. In the left pane, right-click the domain controller where you want to create an Organizational Unit, and select [New] > [Organizational Unit].
   New Object - Organizational Unit appears.
5. Set as follows:
   - In the [Name] box, type any name for the Organizational Unit.
   - Select the [Protect container from accidental deletion] check box.
6. Click [OK].
   A new Organizational Unit is created.
7. As necessary, build a hierarchy of Organizational Units. You can build it by repeating steps 4 to 6.
8. In the left pane of Active Directory Users and Computers, select [Computers]. From the computers list that is displayed, select the computers to be added to Organizational Units, and drag and drop them to the target Organizational Units as desired. A warning message regarding moving the objects appears, but click [Yes] to continue.

TIP

The computers that belong to an Organizational Unit must be limited to computers to which the same group policies are to be applied. Because you will apply group policies to the Organizational Units in the subsequent procedure, ensure that one Organizational Unit does not contain computers with different IT security levels.

Also ensure that Unified Gateway Stations do not belong to the same Organizational Unit as the following stations:

- HIS
- APCS
- Generic subsystem gateway station
- System integration OPC station
- License management station

Creation of Organizational Units is now completed. The next task is to apply group policy objects to the Organizational Units.

■ Deleting an Organizational Unit

If the Protect container from accidental deletion check box was selected in the [New Object - Organizational Unit] dialog box at the creation of an Organizational Unit, a message appears when you delete that Organizational Unit. Follow these steps to delete such an Organizational Unit:

1. Open Control Panel.
2. Select [Administrative Tools] > [Active Directory Users and Computers].
   [Active Directory Users and Computers] appears.
3. Right-click the Organizational Unit that you want to delete and select [Properties], then click the Object tab. If the Object tab is not displayed, you can make it visible by selecting [View] > [Advanced Features] in [Active Directory Users and Computers].

4. Clear the Protect container from accidental deletion check box, and click [OK].
   Now you can delete this Organizational Unit.

5. Delete the Organizational Unit.

Deletion of an Organizational Unit is now completed.

■ Applying Group Policy Objects to an Organizational Unit

Follow these steps:

1. Open Control Panel.

2. Select [Administrative Tools] > [Group Policy Management].
   [Group Policy Management] appears.

3. In the left pane, select [Group Policy Objects]. From the object list that is displayed, select the group policy that you want to apply, and drag and drop them to the target Organizational Unit.
   A confirmation dialog box appears.

4. Click [OK].
   [Group Policy Management Console] appears. If you change the applied group policy object here, you are notified that the change will be shared with other Organizational Units.

5. Click [OK].

6. Restart the domain controller.

Application of group policy objects is now completed.

TIP

Even if you do not restart the domain controller, the group policy object will be updated when the group policy checking function of the OS runs.

● Canceling Application of Group Policy Objects to an Organizational Unit

Even if you cancel application of a group policy object to an Organizational Unit, the group policy object itself is not deleted.

Follow these steps:

1. Open Control Panel.

2. Select [Administrative Tools] > [Group Policy Management].
   [Group Policy Management] appears.

3. Select the Organizational Unit in the left pane, right-click the group policy object that you want to cancel application, and select [Delete].
   A confirmation message appears.

4. Click [OK].

Application of a group policy object for an Organizational Unit has been canceled.

6.10 Other Utility Programs

This section describes the utility programs other than the IT Security Tool.

6.10.1 CreateCentumProcess

This utility creates the CTM_PROCESS user. It also enables you to change the password for the CTM_PROCESS user.

■ Detailed Explanation

CreateCentumProcess is used on the file server where project databases are placed or PCs running other software packages that collaborate with CENTUM VP. This tool creates the CTM_PROCESS user and automatically sets a password for it. If you want to manage the password, you can specify an option to set a desired password.

■ Start Method

Follow these steps to run CreateCentumProcess.

1. Log on using an administrative user account.
2. Insert the CENTUM VP software medium into the drive and run the following command from the command prompt window.

   ```
   <Drive of software medium>:\CENTUM\SECURITY\Yokogawa.IA.iPCS.Platform.Securit
   y.CreateCentumProcess.exe
   ```

   If the CTM_PROCESS user does not exist, it is created and a password is set automatically. The passwords for Windows services registered for use by the CTM_PROCESS user are also set.

   If the CTM_PROCESS user already exists, its password is changed to the initial password.

TIP

If you want to set a desired password, run the following command:

```
<Drive of software medium>:\CENTUM\SECURITY\Yokogawa.IA.iPCS.Platform.Security.CreateCentumProc
ess.exe -p (password to be set)
```

You can specify a password within 127 characters. No password is not allowed. If the CTM_PROCESS user does not exist, it is created and the specified password is set. At the same time, the passwords for Windows services registered for use by the CTM_PROCESS user are also changed to the specified password.

If the CTM_PROCESS user already exists, its password is changed to the specified password.

IMPORTANT

Note the following points when you change the password:

- Ensure that the same password is set on all the PCs where the CTM_PROCESS user exists, such as CENTUM VP stations, PCs running other software packages that collaborate with CENTUM VP, and file servers.
- After you change the password of an existing CTM_PROCESS user, restart the PC.

6.10.2 CreateUgsProcess

This utility creates the UGS_PROCESS user. It also enables you to change the password for the UGS_PROCESS user.

■ Detailed Explanation

CreateUgsProcess is used on the PC running the OPC server that communicates with UGS. This tool creates the UGS_PROCESS user and automatically sets a password for it. If you want to manage the password, you can specify an option to set a desired password.

■ Start Method

Follow these steps to run CreateUgsProcess.

1. Log on using an administrative user account.
2. Insert the CENTUM VP software medium into the drive and run the following command from the command prompt window.

```
<Drive of software medium>:\CENTUM\SECURITY\Yokogawa.IA.iPCS.Platform.Securit
y.CreateUgsProcess.exe
```

   If the UGS_PROCESS user does not exist, it is created and a password is set automatically. At the same time, the passwords for Windows services registered for use by the UGS_PROCESS user are also set.

   If the UGS_PROCESS user already exists, its password is changed to the initial password.

TIP

If you want to set a desired password, run the following command:

```
<Drive of software medium>:\CENTUM\SECURITY\Yokogawa.IA.iPCS.Platform.Security.CreateUgsProcess
.exe -p (password to be set)
```

You can specify a password within 127 characters. No password is not allowed. If the UGS_PROCESS user does not exist, it is created and the specified password is set. At the same time, the passwords for Windows services registered for use by the UGS_PROCESS user are also changed to the specified password.

If the UGS_PROCESS user already exists, its password is changed to the specified password.

IMPORTANT

Note the following points when you change the password:

- Ensure that the same password is set on UGS and all the PCs running the OPC server that communicates with UGS, where the UGS_PROCESS user exists.
- After you change the password of an existing UGS_PROCESS user, restart the PC.

6.10.3 CreateLicenseProcess

This utility creates the LIC_PROCESS user. It also enables you to change the password for the LIC_PROCESS user.

■ Detailed Explanation

CreateLicenseProcess is used on the file server where project databases are placed or PCs running ProSafe-RS that collaborates with CENTUM VP. This tool creates the LIC_PROCESS user and automatically sets a password for it. If you want to manage the password, you can specify an option to set a desired password.

■ Start Method

Follow these steps to run CreateLicenseProcess.

1. Log on using an administrative user account.
2. Insert the CENTUM VP software medium into the drive and run the following command from the command prompt window.

   ```
   <Drive of software medium>:\CENTUM\SECURITY\Yokogawa.IA.iPCS.Platform.License
   .CreateLicenseProcess.exe
   ```

   If the LIC_PROCESS user does not exist, it is created and a password is set automatically. At the same time, the passwords for Windows services registered for use by the LIC_PROCESS user are also set.

   If the LIC_PROCESS user already exists, its password is changed to the initial password.

TIP

If you want to set a desired password, run the following command:

```
<Drive of software medium>:\CENTUM\SECURITY\Yokogawa.IA.iPCS.Platform.License.CreateLicenseProc
ess.exe -p (password to be set)
```

You can specify a password within 127 characters. No password is not allowed. If the LIC_PROCESS user does not exist, it is created and the specified password is set. At the same time, the passwords for Windows services registered for use by the LIC_PROCESS user are also changed to the specified password.

If the LIC_PROCESS user already exists, its password is changed to the specified password.

IMPORTANT

Note the following points when you change the password:

- Ensure that the same password is set on all the PCs where the LIC_PROCESS user exists, such as CENTUM VP stations, ProSafe-RS SENG, and file servers.
- After you change the password of an existing LIC_PROCESS user, restart the PC.

6.10.4 CreateAdsProcess

This utility creates the ADS_PROCESS user. It is also used to change the password of the ADS_PROCESS user.

■ Detailed Explanation

CreateAdsProcess is a tool that is used on the Automation Design Server computer where the Automation Design Master Database is stored. This tool creates the ADS_PROCESS user and automatically sets a password for it. If you want to manage the password, you can specify an option to set a desired password.

■ Start Method

Follow these steps to start CreateAdsProcess:

1. Log on using an administrative user account.
2. Insert the CENTUM VP software medium into the drive and run the following command by using the command prompt:

   ```
   <Drive of software medium>:\CENTUM\SECURITY\Yokogawa.IA.iPCS.ChronusENG.Security.CreateAdsProcess.exe
   ```

   If the ADS_PROCESS user does not exist, it is created and a password is set automatically. The passwords for Windows services registered for use by the ADS_PROCESS user are also set.

   If the ADS_PROCESS user already exists, its password is changed to the default password.

TIP

If you want to set a desired password, run the following command:

```
<Drive of software medium>:\CENTUM\SECURITY\Yokogawa.IA.iPCS.ChronusENG.Security.CreateAdsProcess.exe -p (password to be set)
```

You can set a password up to 127 characters long. No password is not allowed. If the ADS_PROCESS user does not exist, it is created and the specified password is set. At the same time, the passwords for Windows services that are registered for use by the ADS_PROCESS user are also changed to the specified password.

If the ADS_PROCESS user already exists, its password is changed to the specified password.

IMPORTANT

Note the following points when you change the password:

- Ensure that the same password is set on all the AD Server PCs where the ADS_PROCESS user exists.
- After you change the password of an existing ADS_PROCESS user, restart the PC.

SEE ALSO

For more information about Automation Design Server, refer to:

A., “Overview of Automation Design Suite” in Automation Design Suite Basics (IM 33J10A10-01EN)

6.10.5 CreateAdsAgent

Using this utility, you can change the password of the ADS_AGENT user.

■ Detailed Explanation

CreateAdsAgent is used on computers where CENTUM VP is installed. By running this tool, you can set a desired password for the ADS_AGENT user.

TIP

For more information about running this tool, contact YOKOGAWA Service.

■ Start Method

Follow these steps to start CreateAdsAgent.

1. Log on as a user with administrative rights.
2. Insert the CENTUM VP software medium into the drive and run the following command from the command prompt window.

```
<Drive of software medium>:\CENTUM\SECURITY\Yokogawa.IA.iPCS.ChronusENG.Secur
ity.CIM.CreateAdsAgent.exe -p (password to be set)
```

   You can set a password within 127 characters. Setting a password is mandatory.

   When you run this command, the passwords for Windows services registered for use by the ADS_AGENT user are also changed to the same password.

TIP

If you run the command without specifying a password, the default password is set.

IMPORTANT

Note the following points when you change the password:

- Ensure that the same password is set on all the PCs where the ADS_AGENT user exists.
- After you change the password of an existing ADS_AGENT user, restart the PC.

6.10.6 CreateRDCProcess

This utility creates the RDC_PROCESS user. It is also used to change the password of the RDC_PROCESS user.

■ Detailed Explanation

CreateRDCProcess is a tool that is used on a computer switchover type UGS. This tool creates the RDC_PROCESS user and automatically sets a password for it. If you want to manage the password, you can specify an option to set a desired password.

■ Start Method

Follow these steps to start CreateRDCProcess:

1. Log on using an administrative user account.
2. Insert the CENTUM VP software medium into the drive and run the following command by using the command prompt:

   ```
   <Drive of software medium>:\CENTUM\SECURITY\Yokogawa.IA.iPCS.Platform.Redundancy.CreateRDCProcess.exe
   ```

   If the RDC_PROCESS user does not exist, it is created and a password is set automatically.

   If the RDC_PROCESS user exists, its password is changed to the default password.

TIP

If you want to set a desired password, run the following command:

```
<Drive of software medium>:\CENTUM\SECURITY\Yokogawa.IA.iPCS.Platform.Redundancy.CreateRDCProcess.exe -p (password to be set)
```

You can specify a password within 127 characters. No password is not allowed. If the RDC_PROCESS user does not exist, it is created and the specified password is set.

If the RDC_PROCESS user exists, its password is changed to the specified password.

IMPORTANT

Note the following points when you change the password:

- When changing the password of RDC_PROCESS, ensure that the same password is set on all the computers where the RDC_PROCESS user exists. If the passwords do not match between the computers where the RDC_PROCESS user exists, the system may not operate properly.
- If you have changed the password of existing RDC_PROCESS user, restart the computer.
- When you change the password of RDC_PROCESS, the passwords for Windows services that are registered for use by the RDC_PROCESS user are also changed to the specified password.

6.10.7 CreateOffuser

This utility creates OFFUSER. It also sets the password for OFFUSER. This tool is run on PCs of other systems, file servers, and CS 3000 HIS.

IMPORTANT

If you want to change the password of OFFUSER on CENTUM VP HIS, use ChangeOffuser-Password.

If you use CreateOffuser on CENTUM VP HIS, you can no longer log on by using the OFFUSER account. If this problem occurs, you can restore in either of the following ways:

- Use ChangeOffuserPassword that is installed on CENTUM VP HIS to change the password.
- Delete OFFUSER that is registered to the local security policy [Deny log on locally].

■ Detailed Explanation

This tool creates OFFUSER and automatically sets a password for it. If you want to manage the password, you can specify an option to set a desired password.

■ Start Method

Follow these steps to run CreateOffuser.

1. Log on using an administrative user account.
2. Insert the CENTUM VP software medium into the drive and run the following command from the command prompt window.

```
<Drive of software medium>:\CENTUM\SECURITY\Yokogawa.IA.iPCS.Platform.Securit
y.CreateOffuser.exe
```

   If OFFUSER does not exist, it is created and a password is set automatically.

   If OFFUSER already exists, its password is changed to the initial password.

TIP

If you want to set a desired password, run the following command:

```
<Drive of software medium>:\CENTUM\SECURITY\Yokogawa.IA.iPCS.Platform.Security.CreateOffuser.ex
e -p (password to be set)
```

You can specify a password within 127 characters. No password is not allowed. If OFFUSER does not exist, it is created and the specified password is set.

If OFFUSER already exists, its password is changed to the specified password.

IMPORTANT

Note the following points when you change the password:

- Ensure that the same password is set on all the PCs where OFFUSER exists, such as CENTUM VP stations, PCs running other software packages that collaborate with CENTUM VP, and file servers.
- After you change the password of existing OFFUSER, restart the PC.

6.10.8 YWVNETCreateVNTUser

YWVNETCreateVNTUser is a utility program that changes the password of the users for running Vnet/IP Interface Package. This utility changes the password of the following users:

- VNT_COMMON
- VNT_NVP_CORE
- VNT_BKNET

IMPORTANT

- When you change the password, you must prepare an ISO format file of the CENTUM VP software medium in advance.
- To be able to change the password, Vnet/IP Interface Package must be installed. Before you change the password, make sure that Vnet/IP Interface Package is installed on the computer.
- After you change the password, restart the virtual machine.

■ Start Method

Follow these steps to start YWVNTCreatVNTUser.

1. Sign in to the host OS of the virualization host computer as an administrative user.
2. Copy the ISO format file of the CENTUM VP software medium to a folder in the host OS.
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. On the left pane of Hyper-V Manager, select the virtualization host computer.
   The virtual machines on the selected virtualization host computer appear on the middle pane.
6. Right-click the virtual machine on which you want to run YWVNTCreatVNTUser, and select [Connect].
   The Connect Virtual Machine window appears.

TIP

The Connect Virtual Machine window may be displayed full-screen. If it is displayed full-screen, click [Restore] to exit the full-screen mode.

7. From the menu bar of the Connect Virtual Machine window, select [Media] > [DVD Drive] > [Insert Disk].
   The Open dialog box appears.
8. Specify the ISO format file of the CENTUM VP software medium that you copied.
   The selected ISO format file is mounted to the virtual machine.
9. In the Connect Virtual Machine window, select [Start] > [Windows System].
   A list of Windows system tools appears.
10. Right-click [Command Prompt] and select [Run as administrator].
11. Run the following command from the command prompt window:
    <Mounted drive>`:\CENTUM\security\ywvnetcreatevntuser.exe -u user name -p password to be set`

    You can set a password within 127 characters. Setting a password is mandatory.

12. Restart the virtual machine.

IMPORTANT

- You must run this utility with Vnet/IP Interface Package installed. If you have changed the password by using this utility while Vnet/IP Interface Package is not installed, change the password again after installing Vnet/IP Interface Package.
- If you install Vnet/IP Interface Package after changing the password, the changed password will be reset. Therefore, change the password again.

6.10.9 ChangeOffuserPassword

This utility sets the password for OFFUSER. It is run on CENTUM VP HIS.

Detailed Explanation

If the password of OFFUSER should be managed by the user, the user can change the password by running ChangeOffuserPassword specifying a desired password.

Start Method

Follow these steps to run ChangeOffuserPassword.

1. Log on using an administrative user account.
2. Run the following command.
   This example is when the system drive is drive C.

   ```
   C:\Program Files (x86)\Yokogawa\IA\iPCS\Platform\SECURITY\PROGRAM\Yokogawa.IA
   .iPCS.Platform.Security.ChangeOffuserPassword.exe -p (password to be set)
   ```

   You can specify a password within 127 characters. No password is not allowed. The password is changed to the specified password. If OFFUSER does not exist, OFFUSER is created.

TIP

When you change the currently set password to the initial password, run the command as follows:

This example is when the system drive is drive C.

```
C:\Program Files (x86)\Yokogawa\IA\iPCS\Platform\SECURITY\PROGRAM\Yokogawa.IA.iPCS.Platform.Sec
urity.ChangeOffuserPassword.exe
```

IMPORTANT

Note the following points when you change the password:

- Ensure that the same password is set on all the PCs where OFFUSER exists, such as CENTUM VP stations, PCs running other software packages that collaborate with CENTUM VP, and file servers.
- After you change the password of existing OFFUSER, restart the PC.

6.10.10 OFFUSEREnabler

This utility changes the password of OFFUSER temporarily to “!centumvp123.”

■ Detailed Explanation

When an administrative user runs OFFUSEREnabler command, the password of OFFUSER will be changed to “!centumvp123” and the OFFUSER account can be used to log on Windows. To reset the password of OFFUSER account to the initial password (not disclosed), you need to run the OFFUSERDisabler command. If a standard model or strengthened model of security settings is applied in the PC, running the OFFUSEREnabler command requires the privilege of CTM_MAINTENANCE group.

■ Start Method

The program can be started as follows.

1. Log on using an administrative user account.
2. Use Windows Explorer to open the following folder.
   This example is when the system drive is drive C.

   ```
   C:\Program Files (x86)\Yokogawa\IA\iPCS\Platform\SECURITY\PROGRAM\
   ```
3. Double click the following program file in the folder.
   `Yokogawa.IA.iPCS.Platform.Security.OFFUSEREnabler.exe`

6.10.11 OFFUSERDisabler

This program resets the password of OFFUSER to initial password.

■ Detailed Explanation

When an administrative user runs OFFUSERDisabler command, the password of OFFUSER will be changed to the initial password (not disclosed).

If a standard model or strengthened model of security settings is applied in the PC, running the OFFUSERDisabler command requires the privilege of CTM_MAINTENANCE group.

■ Start Method

The program can be started as follows.

1. Log on using an administrative user account.
2. Use Windows Explorer to open the following folder.
   This example is when the system drive is drive C.

   `C:\Program Files (x86)\Yokogawa\IA\iPCS\Platform\SECURITY\PROGRAM\`
3. Double click the following program file in the folder.
   `Yokogawa.IA.iPCS.Platform.Security.OFFUSERDisabler.exe`

6.10.12 StorageDeviceCTL

This utility temporarily cancels the following disabling of storage devices.

- Disabling of write permissions set by applying the StorageDevicePolicies function
- Disabling set by applying "Disabling USB storage devices"

■ Detailed Explanation

When you cannot write to storage devices due to application of the StorageDevicePolicies function or disabling of USB storage devices, you can execute StorageDeviceCTL to cancel the effect of these security measures temporarily. Writing to storage devices is enabled while StorageDeviceCTL is running.

Start this tool, connect a USB storage device to the PC, and then perform writing tasks.

The CTM_MAINTENANCE right is required to execute the tool.

Use this tool only on PCs for which the StorageDevicePolicies function or disabling of USB storage devices is set.

IMPORTANT

- Be sure to make the PC recognize the storage device after starting this tool.
- When the StorageDevicePolicies function or "Disabling USB storage devices" is applied on Windows Server 2008 R2, you cannot use this utility to cancel the disabling.
- When you start this utility on a Windows Server 2008 computer where the product is not installed, a dialog box confirming stopping of services may be displayed. If displayed, click the [Close] of the dialog box.

■ Start Method

Follow these steps to start StorageDeviceCTL:

1. Use Windows Explorer to open the following folder.
   This example is when the system drive is drive C.

   ```
   C:\Program Files (x86)\Yokogawa\IA\iPCS\Platform\SECURITY\PROGRAM\
   ```

2. Double click the following program file in the folder.

   ```
   Yokogawa.IA.iPCS.Platform.Security.StorageDeviceCTL.exe
   ```

   The task is displayed only in the taskbar immediately after the start.

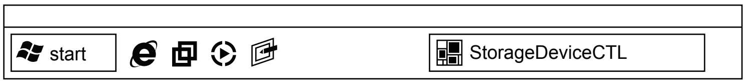


Figure 6.10.12-1 Taskbar

3. Connect the USB storage device to the computer.
4. Read/write necessary data from/to the USB storage device.
5. Remove the USB storage device from the computer.

TIP

To remove a USB storage device, right-click the [Safely Remove Hardware and Eject Media] icon from the task tray and select [Eject USB Flash Disk] to stop the device.

6. Click [StorageDeviceCTL] from the taskbar and then click [WriteStop].

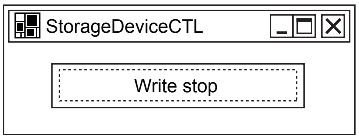


Figure 6.10.12-2 StorageDeviceCTL Dialog Box

StorageDeviceCTL ends and USB storage devices are disabled again.

SEE ALSO

For more information about the StorageDevicePolicies function, refer to:

3.5.3, “Applying the StorageDevicePolicies Function” on page 3-27

For more information about disabling USB storage devices, refer to:

3.5.4, “Disabling USB Storage Devices” on page 3-28

6.10.13 ITSecuritySettingItemExport

This utility exports the security model, user management type, changes made to settings, and IT security version number that were set by the IT Security Tool of R5.01 to R6.03 to a file.

■ Detailed Explanation

The exported information is the settings at the last IT security configuration of the environment where you run the utility.

By importing the exported file using the IT Security Tool, you can restore the security setting status that was configured by the IT Security Tool of the environment where the information was exported.

■ Start Method

Follow these steps to run the ITSecuritySettingItemExport utility:

1. Log on as a user with administrative rights.
2. Insert the software medium of the product into the drive, and run the following command from the command prompt:
   ```
   <Drive of software medium>:\CENTUM\SECURITY\ITSecuritySettingItemExport.exe
   ```
3. After running the utility, a file is automatically created and a confirmation dialog box appears. Click [OK] to save the file.

IMPORTANT

- This utility is available only on computers where a YOKOGAWA system product is installed. It is not available on a file server or domain controller, where security configuration is performed by using the IT Security Tool without installing product software.
- The account used to run this utility must belong to the maintenance group of the product.
- The folder and file that are exported by this utility have a fixed name. If they exist on the computer already, the file will be overwritten.
- When you cannot access the folder and file that are exported by this utility, an access violation error message appears.

Blank Page

Appendix 1. IT Security Setting Items

This section describes the security setting items that are configured with IT security version 2.0 and IT security version 1.0.

Appendix 1.1 IT Security Version 2.0

This section describes the security setting items that are configured with IT security version 2.0 along with their default values and whether they can be modified. However, some security setting items may not appear depending on the OS version or the station type.

Appendix 1.1.1 Setting Items for a Computer with CENTUM VP Software Installed

This section provides lists of the security setting items for a computer on which the product software is installed for each combination of security model and user management type.

■ Security Setting Items for Standard Model with Standalone Management

The following table shows the security setting items for the combination of Standard model and Standalone management.

Table Appendix 1.1.1-1 Standard Model - Standalone Management

Setting item	Default check box state	Modification
Creating local users and groups	Selected	Fixed
Access control for files and folders	Selected	Fixed
Access control for product registry	Selected	Fixed
Access control for DCOM (OPC) objects	Selected	Fixed
Personal firewall tuning	Selected	Fixed
Set 'Personal Firewall-[Allow unicast response]' to 'No' (*1)	Selected	Editable
Disabling NetBIOS over TCP/IP	Clear	Editable
Applying the StorageDevicePolicies function	Clear	Editable
Disabling USB storage devices	Clear	Editable
Applying the software restriction policies	Clear	Editable
User Rights Assignment-[Access this computer from the network] (*2)	Selected	Editable
User Rights Assignment-[Allow log on locally] (*2)	Selected	Editable
User Rights Assignment-[Deny log on locally]	Selected	Fixed
Security Options-[Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings]	Selected	Editable
Security Options-[Devices: Prevent users from installing printer drivers]	Selected	Editable
Security Options-[Devices: Restrict CD-ROM access to locally logged-on user only]	Selected	Editable
Security Options-[Devices: Restrict floppy access to locally logged-on user only]	Selected	Editable
Security Options-[Domain member: Require strong (Windows 2000 or later) session key]	Selected	Editable
Security Options-[Interactive logon: Do not display last user name]	Selected	Fixed
Disable 'Security Options-[Interactive logon: Do not require CTRL +ALT+DEL]'	Selected	Editable
Security Options-[Interactive logon: Machine inactivity limit] (*2)	Selected	Editable
Security Options-[Interactive logon: Prompt user to change password before expiration]	Selected	Editable
Security Options-[Microsoft network server: Digitally sign communications (if client agrees)]	Selected	Editable
Security Options-[Microsoft network server: Server SPN target name validation level]	Selected	Editable

Continues on the next page

Table Appendix 1.1.1-1 Standard Model - Standalone Management (Table continued)

Setting item	Default check box state	Modification
[MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)]	Selected	Editable
Disable [MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)]	Selected	Editable
[MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)]	Selected	Editable
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts]	Selected	Editable
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts and shares]	Selected	Editable
Security Options-[Network access: Do not allow storage of passwords and credentials for network authentication]	Selected	Editable
Security Options-[Network security: Allow Local System to use computer identity for NTLM]	Selected	Editable
Disable 'Security Options-[Network security: Allow LocalSystem NULL session fallback]’	Selected	Editable
Security Options-[Network security: LAN Manager authentication level]	Selected	Fixed
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) clients]	Selected	Editable
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) servers]	Selected	Editable
Disable 'Security Options-[Shutdown: Allow system to be shut down without having to log on]'	Selected	Editable
Security Options-[User Account Control: Admin Approval Mode for the Built'-in Administrator account]	Selected	Editable
Security Options-[User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Credential Validation]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Computer Account Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Account Management Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security Group Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit User Account Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Process Creation]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Account Lockout]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Logoff]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Logon]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Logon/Logoff Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Special Logon]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Removable Storage]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Audit Policy Change]	Selected	Editable

Continues on the next page

Table Appendix 1.1.1-1 Standard Model - Standalone Management (Table continued)

Setting item	Default check box state	Modification
Advanced Audit Policy Configuration-[Audit Authentication Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Filtering Platform Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit MPSSVC Rule-Level Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Policy Change Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Sensitive Privilege Use]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other System Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security State Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security System Extension]	Selected	Editable
Advanced Audit Policy Configuration-[Audit System Integrity]	Selected	Editable
Personalization-[Prevent enabling lock screen camera]	Selected	Editable
Personalization-[Prevent enabling lock screen slide show]	Selected	Editable
WLAN Settings-[Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services]	Selected	Editable
Group Policy-[Configure registry policy processing]	Selected	Editable
Internet Communication settings-[Turn off downloading of print drivers over HTTP]	Selected	Editable
Internet Communication settings-[Turn off Event Viewer "Events.asp" links]	Selected	Editable
Internet Communication settings-[Turn off Internet download for Web publishing and online ordering wizards]	Selected	Editable
Internet Communication settings-[Turn off printing over HTTP]	Selected	Editable
Internet Communication settings-[Turn off Search Companion content file updates]	Selected	Editable
Internet Communication settings-[Turn off the "Publish to Web" task for files and folders]	Selected	Editable
Internet Communication settings-[Turn off the Windows Customer Experience Improvement Program]	Selected	Fixed
Internet Communication settings-[Turn off the Windows Messenger Customer Experience Improvement Program]	Selected	Fixed
Logon-[Do not display network selection UI]	Selected	Editable
Logon-[Do not enumerate connected users on domain-joined computers]	Selected	Editable
Disable 'Logon-[Enumerate local users on domain-joined computers]'	Selected	Editable
Logon-[Turn off app notifications on the lock screen]	Selected	Editable
Mitigation Options-[Untrusted Font Blocking]	Selected	Editable
User Profiles-[Turn off the advertising ID]	Selected	Editable
App Privacy-[Let Windows apps access account information]	Selected	Editable
App Privacy-[Let Windows apps access call history]	Selected	Editable
App Privacy-[Let Windows apps access contacts]	Selected	Editable

Continues on the next page

Table Appendix 1.1.1-1 Standard Model - Standalone Management (Table continued)

Setting item	Default check box state	Modification
App Privacy-[Let Windows apps access email]	Selected	Editable
App Privacy-[Let Windows apps access location]	Selected	Editable
App Privacy-[Let Windows apps access messaging]	Selected	Editable
App Privacy-[Let Windows apps access motion]	Selected	Editable
App Privacy-[Let Windows apps access the calendar]	Selected	Editable
App Privacy-[Let Windows apps access the camera]	Selected	Editable
App Privacy-[Let Windows apps access the microphone]	Selected	Editable
App Privacy-[Let Windows apps access trusted devices]	Selected	Editable
App Privacy-[Let Windows apps control radios]	Selected	Editable
App Privacy-[Let Windows apps sync with devices]	Selected	Editable
App runtime-[Block launching Windows Store apps with Windows Runtime API access from hosted content]	Selected	Editable
AutoPlay Policies-[Turn off Autoplay]	Selected	Editable
AutoPlay Policies-[Disallow Autoplay for non-volume devices]	Selected	Editable
Cloud Content-[Do not show Windows Tips]	Selected	Editable
Cloud Content-[Turn off Microsoft consumer experiences]	Selected	Editable
Data Collection and Preview Builds-[Allow Telemetry]	Selected	Editable
Data Collection and Preview Builds-[Disable pre-release features or settings]	Selected	Editable
Data Collection and Preview Builds-[Do not show feedback notifications]	Selected	Editable
Data Collection and Preview Builds-[Toggle user control over Insider builds]	Selected	Editable
Event Log Service(Application)-[Specify the maximum log file size (KB)]	Selected	Editable
Event Log Service(Security)-[Specify the maximum log file size (KB)]	Selected	Editable
Event Log Service(System)-[Specify the maximum log file size (KB)]	Selected	Editable
File Explorer-[Turn off heap termination on corruption]	Selected	Editable
HomeGroup-[Prevent the computer from joining a homegroup]	Selected	Editable
OneDrive-[Prevent the usage of OneDrive for file storage]	Selected	Editable
OneDrive-[Save documents to OneDrive by default](Save documents to the local PC by default)	Selected	Editable
Remote Desktop Connection Client-[Do not allow passwords to be saved]	Selected	Editable
Device and Resource Redirection-[Do not allow drive redirection] (*1)	Selected	Editable
Security-[Always prompt for password upon connection] (*2)	Selected	Editable
Security-[Require secure RPC communication]	Selected	Editable
Security-[Require user authentication for remote connections by using Network Level Authentication]	Selected	Editable
Session Time Limits-[Set time limit for active but idle Remote Desktop Services sessions] (*2)	Selected	Editable

Continues on the next page

Table Appendix 1.1.1-1 Standard Model - Standalone Management (Table continued)

Setting item	Default check box state	Modification
Disable ‘Search-[Allow Cortana]’	Selected	Editable
Software Protection Platform-[Turn off KMS Client Online AVS Validation]	Selected	Editable
Sync your settings-[Do not sync Apps]	Selected	Editable
Sync your settings-[Do not sync start settings]	Selected	Editable
Disable 'Windows Error Reporting-[Automatically send memory dumps for OS-generated error reports]'	Selected	Fixed
Disable 'Windows Logon Options-[Sign'-in last interactive user automatically after a system'-initiated restart]'	Selected	Editable
Notifications-[Turn off toast notifications on the lock screen]	Selected	Editable

*1: On UGS, this check box is cleared and you cannot change it.
*2: This setting is applicable only on the UACS station.

■ Security Setting Items for Standard Model with Domain or Combination Management

The following table shows the security setting items for the combination of Standard model and Domain or Combination management.

Table Appendix 1.1.1-2 Standard Model - Domain/Combination Management

Setting item	Default check box state	Modification
Creating local users and groups	Selected	Fixed
Creating domain users and groups	Selected	Fixed
Access control for files and folders	Selected	Fixed
Access control for product registry	Selected	Fixed
Access control for DCOM (OPC) objects	Selected	Fixed
Personal firewall tuning	Selected	Fixed
Set 'Personal Firewall-[Allow unicast response]' to ‘No’ (*1)	Selected	Editable
Disabling NetBIOS over TCP/IP	Selected	Editable
Applying the StorageDevicePolicies function	Clear	Editable
Disabling USB storage devices	Clear	Editable
Applying the software restriction policies	Clear	Editable
User Rights Assignment-[Access this computer from the network] (*2)	Selected	Editable
User Rights Assignment-[Allow log on locally] (*2)	Selected	Editable
User Rights Assignment-[Deny log on locally]	Selected	Fixed
Security Options-[Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings]	Selected	Editable
Security Options-[Devices: Prevent users from installing printer drivers]	Selected	Editable
Security Options-[Devices: Restrict CD-ROM access to locally logged-on user only]	Selected	Editable
Security Options-[Devices: Restrict floppy access to locally logged-on user only]	Selected	Editable

Continues on the next page

Table Appendix 1.1.1-2 Standard Model - Domain/Combination Management (Table continued)

Setting item	Default check box state	Modification
Security Options-[Domain member: Require strong (Windows 2000 or later) session key]	Selected	Editable
Security Options-[Interactive logon: Do not display last user name]	Selected	Fixed
Disable 'Security Options-[Interactive logon: Do not require CTRL +ALT+DEL]'	Selected	Editable
Security Options-[Interactive logon: Machine inactivity limit] (*2)	Selected	Editable
Security Options-[Interactive logon: Prompt user to change password before expiration]	Selected	Editable
Security Options-[Microsoft network server: Digitally sign communications (if client agrees)]	Selected	Editable
Security Options-[Microsoft network server: Server SPN target name validation level]	Selected	Editable
[MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)]	Selected	Editable
Disable [MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)]	Selected	Editable
[MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)]	Selected	Editable
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts]	Selected	Editable
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts and shares]	Selected	Editable
Security Options-[Network access: Do not allow storage of passwords and credentials for network authentication]	Selected	Editable
Security Options-[Network security: Allow Local System to use computer identity for NTLM]	Selected	Editable
Disable 'Security Options-[Network security: Allow LocalSystem NULL session fallback]'	Selected	Editable
Security Options-[Network security: LAN Manager authentication level]	Selected	Fixed
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) clients]	Selected	Editable
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) servers]	Selected	Editable
Disable 'Security Options-[Shutdown: Allow system to be shut down without having to log on]'	Selected	Editable
Security Options-[User Account Control: Admin Approval Mode for the Built'-in Administrator account]	Selected	Editable
Security Options-[User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Credential Validation]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Computer Account Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Account Management Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security Group Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit User Account Management]	Selected	Editable

Continues on the next page

Table Appendix 1.1.1-2 Standard Model - Domain/Combination Management (Table continued)

Setting item	Default check box state	Modification
Advanced Audit Policy Configuration-[Audit Process Creation]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Account Lockout]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Logoff]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Logon]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Logon/Logoff Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Special Logon]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Removable Storage]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Audit Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Authentication Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Filtering Platform Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit MPSSVC Rule-Level Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Policy Change Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Sensitive Privilege Use]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other System Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security State Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security System Extension]	Selected	Editable
Advanced Audit Policy Configuration-[Audit System Integrity]	Selected	Editable
Personalization-[Prevent enabling lock screen camera]	Selected	Editable
Personalization-[Prevent enabling lock screen slide show]	Selected	Editable
WLAN Settings-[Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services]	Selected	Editable
Group Policy-[Configure registry policy processing]	Selected	Editable
Internet Communication settings-[Turn off downloading of print drivers over HTTP]	Selected	Editable
Internet Communication settings-[Turn off Event Viewer "Events.asp" links]	Selected	Editable
Internet Communication settings-[Turn off Internet download for Web publishing and online ordering wizards]	Selected	Editable
Internet Communication settings-[Turn off printing over HTTP]	Selected	Editable
Internet Communication settings-[Turn off Search Companion content file updates]	Selected	Editable
Internet Communication settings-[Turn off the "Publish to Web" task for files and folders]	Selected	Editable
Internet Communication settings-[Turn off the Windows Customer Experience Improvement Program]	Selected	Fixed
Internet Communication settings-[Turn off the Windows Messenger Customer Experience Improvement Program]	Selected	Fixed
Logon-[Do not display network selection UI]	Selected	Editable

Continues on the next page

Table Appendix 1.1.1-2 Standard Model - Domain/Combination Management (Table continued)

Setting item	Default check box state	Modification
Logon-[Do not enumerate connected users on domain-joined computers]	Selected	Editable
Disable 'Logon-[Enumerate local users on domain-joined computers]'	Selected	Editable
Logon-[Turn off app notifications on the lock screen]	Selected	Editable
Mitigation Options-[Untrusted Font Blocking]	Selected	Editable
User Profiles-[Turn off the advertising ID]	Selected	Editable
App Privacy-[Let Windows apps access account information]	Selected	Editable
App Privacy-[Let Windows apps access call history]	Selected	Editable
App Privacy-[Let Windows apps access contacts]	Selected	Editable
App Privacy-[Let Windows apps access email]	Selected	Editable
App Privacy-[Let Windows apps access location]	Selected	Editable
App Privacy-[Let Windows apps access messaging]	Selected	Editable
App Privacy-[Let Windows apps access motion]	Selected	Editable
App Privacy-[Let Windows apps access the calendar]	Selected	Editable
App Privacy-[Let Windows apps access the camera]	Selected	Editable
App Privacy-[Let Windows apps access the microphone]	Selected	Editable
App Privacy-[Let Windows apps access trusted devices]	Selected	Editable
App Privacy-[Let Windows apps control radios]	Selected	Editable
App Privacy-[Let Windows apps sync with devices]	Selected	Editable
App runtime-[Block launching Windows Store apps with Windows Runtime API access from hosted content]	Selected	Editable
AutoPlay Policies-[Turn off Autoplay]	Selected	Editable
AutoPlay Policies-[Disallow Autoplay for non-volume devices]	Selected	Editable
Cloud Content-[Do not show Windows Tips]	Selected	Editable
Cloud Content-[Turn off Microsoft consumer experiences]	Selected	Editable
Data Collection and Preview Builds-[Allow Telemetry]	Selected	Editable
Data Collection and Preview Builds-[Disable pre-release features or settings]	Selected	Editable
Data Collection and Preview Builds-[Do not show feedback notifications]	Selected	Editable
Data Collection and Preview Builds-[Toggle user control over Insider builds]	Selected	Editable
Event Log Service(Application)-[Specify the maximum log file size (KB)]	Selected	Editable
Event Log Service(Security)-[Specify the maximum log file size (KB)]	Selected	Editable
Event Log Service(System)-[Specify the maximum log file size (KB)]	Selected	Editable
File Explorer-[Turn off heap termination on corruption]	Selected	Editable
HomeGroup-[Prevent the computer from joining a homegroup]	Selected	Editable
OneDrive-[Prevent the usage of OneDrive for file storage]	Selected	Editable
OneDrive-[Save documents to OneDrive by default](Save documents to the local PC by default)	Selected	Editable

Continues on the next page

Table Appendix 1.1.1-2 Standard Model - Domain/Combination Management (Table continued)

Setting item	Default check box state	Modification
Remote Desktop Connection Client-[Do not allow passwords to be saved]	Selected	Editable
Device and Resource Redirection-[Do not allow drive redirection] (*1)	Selected	Editable
Security-[Always prompt for password upon connection] (*2)	Selected	Editable
Security-[Require secure RPC communication]	Selected	Editable
Security-[Require user authentication for remote connections by using Network Level Authentication]	Selected	Editable
Session Time Limits-[Set time limit for active but idle Remote Desktop Services sessions] (*2)	Selected	Editable
Disable ‘Search-[Allow Cortana]’	Selected	Editable
Software Protection Platform-[Turn off KMS Client Online AVS Validation]	Selected	Editable
Sync your settings-[Do not sync Apps]	Selected	Editable
Sync your settings-[Do not sync start settings]	Selected	Editable
Disable 'Windows Error Reporting-[Automatically send memory dumps for OS-generated error reports]'	Selected	Fixed
Disable 'Windows Logon Options-[Sign'-in last interactive user automatically after a system'-initiated restart]'	Selected	Editable
Notifications-[Turn off toast notifications on the lock screen]	Selected	Editable

*1: On UGS, this check box is cleared and you cannot change it.
*2: This setting is applicable only on the UACS station.

Appendix 1.1.2 Setting Items for a File Server or Domain Controller

This section provides lists of the security setting items for a file server or a domain controller for each combination of security model and user management type.

■ Security Setting Items for File Server: Standard Model with Standalone Management

The following table shows the security setting items for the combination of Standard model and Standalone management on a file server.

Table Appendix 1.1.2-1 File Server: Standard Model - Standalone Management

Setting item	Default check box state	Modification
Creating local users and groups	Selected	Fixed
Access control for files and folders	Selected	Fixed
Personal firewall tuning	Selected	Fixed
Set 'Personal Firewall-[Allow unicast response]' to ‘No’	Selected	Editable
Disabling NetBIOS over TCP/IP	Clear	Editable
Applying the StorageDevicePolicies function	Clear	Editable
Disabling USB storage devices	Clear	Editable
User Rights Assignment-[Deny log on locally]	Selected	Fixed
Security Options-[Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings]	Selected	Editable
Security Options-[Devices: Prevent users from installing printer drivers]	Selected	Editable
Security Options-[Devices: Restrict CD-ROM access to locally logged-on user only]	Selected	Editable
Security Options-[Devices: Restrict floppy access to locally logged-on user only]	Selected	Editable
Security Options-[Domain member: Require strong (Windows 2000 or later) session key]	Selected	Editable
Security Options-[Interactive logon: Do not display last user name]	Selected	Editable
Disable 'Security Options-[Interactive logon: Do not require CTRL+ALT+DEL]’	Selected	Editable
Security Options-[Interactive logon: Prompt user to change password before expiration]	Selected	Editable
Security Options-[Microsoft network server: Digitally sign communications (if client agrees)]	Selected	Editable
Security Options-[Microsoft network server: Server SPN target name validation level]	Selected	Editable
[MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)]	Selected	Editable
Disable [MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)]	Selected	Editable

Continues on the next page

Table Appendix 1.1.2-1 File Server: Standard Model - Standalone Management (Table continued)

Setting item	Default check box state	Modification
[MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)]	Selected	Editable
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts]	Selected	Editable
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts and shares]	Selected	Editable
Security Options-[Network access: Do not allow storage of passwords and credentials for network authentication]	Selected	Editable
Security Options-[Network security: Allow Local System to use computer identity for NTLM]	Selected	Editable
Disable 'Security Options-[Network security: Allow LocalSystem NULL session fallback]’	Selected	Editable
Security Options-[Network security: LAN Manager authentication level]	Selected	Fixed
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) clients]	Selected	Editable
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) servers]	Selected	Editable
Disable 'Security Options-[Shutdown: Allow system to be shut down without having to log on]'	Selected	Editable
Security Options-[User Account Control: Admin Approval Mode for the Built'-in Administrator account]	Selected	Editable
Security Options-[User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Credential Validation]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Computer Account Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Account Management Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security Group Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit User Account Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Process Creation]	Selected	Editable
Advanced Audit Policy Configuration-[Audit RPC Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Account Lockout]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Logoff]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Logon]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Logon/ Logoff Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Special Logon]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Application Generated]	Selected	Editable

Continues on the next page

Table Appendix 1.1.2-1 File Server: Standard Model - Standalone Management (Table continued)

Setting item	Default check box state	Modification
Advanced Audit Policy Configuration-[Audit Removable Storage]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Audit Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Authentication Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Filtering Platform Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit MPSSVC Rule-Level Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Policy Change Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Sensitive Privilege Use]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other System Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security State Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security System Extension]	Selected	Editable
Advanced Audit Policy Configuration-[Audit System Integrity]	Selected	Editable
Personalization-[Prevent enabling lock screen camera]	Selected	Editable
Personalization-[Prevent enabling lock screen slide show]	Selected	Editable
WLAN Settings-[Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services]	Selected	Editable
Group Policy-[Configure registry policy processing]	Selected	Editable
Internet Communication settings-[Turn off downloading of print drivers over HTTP]	Selected	Editable
Internet Communication settings-[Turn off Event Viewer "Events.asp" links]	Selected	Editable
Internet Communication settings-[Turn off Internet download for Web publishing and online ordering wizards]	Selected	Editable
Internet Communication settings-[Turn off printing over HTTP]	Selected	Editable
Internet Communication settings-[Turn off Search Companion content file updates]	Selected	Editable
Internet Communication settings-[Turn off the "Publish to Web" task for files and folders]	Selected	Editable
Internet Communication settings-[Turn off the Windows Customer Experience Improvement Program]	Selected	Fixed
Internet Communication settings-[Turn off the Windows Messenger Customer Experience Improvement Program]	Selected	Fixed
Logon-[Do not display network selection UI]	Selected	Editable
Logon-[Do not enumerate connected users on domain-joined computers]	Selected	Editable
Disable 'Logon-[Enumerate local users on domain-joined computers]'	Selected	Editable

Continues on the next page

Table Appendix 1.1.2-1 File Server: Standard Model - Standalone Management (Table continued)

Setting item	Default check box state	Modification
Logon-[Turn off app notifications on the lock screen]	Selected	Editable
Mitigation Options-[Untrusted Font Blocking]	Selected	Editable
User Profiles-[Turn off the advertising ID]	Selected	Editable
App Privacy-[Let Windows apps access account information]	Selected	Editable
App Privacy-[Let Windows apps access call history]	Selected	Editable
App Privacy-[Let Windows apps access contacts]	Selected	Editable
App Privacy-[Let Windows apps access email]	Selected	Editable
App Privacy-[Let Windows apps access location]	Selected	Editable
App Privacy-[Let Windows apps access messaging]	Selected	Editable
App Privacy-[Let Windows apps access motion]	Selected	Editable
App Privacy-[Let Windows apps access the calendar]	Selected	Editable
App Privacy-[Let Windows apps access the camera]	Selected	Editable
App Privacy-[Let Windows apps access the microphone]	Selected	Editable
App Privacy-[Let Windows apps access trusted devices]	Selected	Editable
App Privacy-[Let Windows apps control radios]	Selected	Editable
App Privacy-[Let Windows apps sync with devices]	Selected	Editable
App runtime-[Block launching Windows Store apps with Windows Runtime API access from hosted content]	Selected	Editable
AutoPlay Policies-[Turn off Autoplay]	Selected	Editable
AutoPlay Policies-[Disallow Autoplay for non-volume devices]	Selected	Editable
Cloud Content-[Do not show Windows Tips]	Selected	Editable
Cloud Content-[Turn off Microsoft consumer experiences]	Selected	Editable
Data Collection and Preview Builds-[Allow Telemetry]	Selected	Editable
Data Collection and Preview Builds-[Disable pre-release features or settings]	Selected	Editable
Data Collection and Preview Builds-[Do not show feedback notifications]	Selected	Editable
Data Collection and Preview Builds-[Toggle user control over Insider builds]	Selected	Editable
Event Log Service(Application)-[Specify the maximum log file size (KB)]	Selected	Editable
Event Log Service(Security)-[Specify the maximum log file size (KB)]	Selected	Editable
Event Log Service(System)-[Specify the maximum log file size (KB)]	Selected	Editable
File Explorer-[Turn off heap termination on corruption]	Selected	Editable
HomeGroup-[Prevent the computer from joining a homegroup]	Selected	Editable
OneDrive-[Prevent the usage of OneDrive for file storage]	Selected	Editable
OneDrive-[Save documents to OneDrive by default](Save documents to the local PC by default)	Selected	Editable

Continues on the next page

Table Appendix 1.1.2-1 File Server: Standard Model - Standalone Management (Table continued)

Setting item	Default check box state	Modification
Remote Desktop Connection Client-[Do not allow passwords to be saved]	Selected	Editable
Device and Resource Redirection-[Do not allow drive redirection]	Selected	Editable
Security-[Require secure RPC communication]	Selected	Editable
Security-[Require user authentication for remote connections by using Network Level Authentication]	Selected	Editable
Disable ‘Search-[Allow Cortana]’	Selected	Editable
Software Protection Platform-[Turn off KMS Client Online AVS Validation]	Selected	Editable
Sync your settings-[Do not sync Apps]	Selected	Editable
Sync your settings-[Do not sync start settings]	Selected	Editable
Disable 'Windows Error Reporting-[Automatically send memory dumps for OS-generated error reports]'	Selected	Fixed
Disable 'Windows Logon Options-[Sign'-in last interactive user automatically after a system'-initiated restart]'	Selected	Editable
Notifications-[Turn off toast notifications on the lock screen]	Selected	Editable

■ Security Setting Items for File Server: Standard Model with Domain or Combination Management

The following table shows the security setting items for the combination of Standard model and Domain or Combination management on a file server.

Table Appendix 1.1.2-2 File Server: Standard Model - Domain/Combination Management

Setting item	Default check box state	Modification
Creating local users and groups	Selected	Fixed
Creating domain users and groups	Selected	Fixed
Access control for files and folders	Selected	Fixed
Personal firewall tuning	Selected	Fixed
Set 'Personal Firewall-[Allow unicast response]' to ‘No’	Selected	Editable
Disabling NetBIOS over TCP/IP	Selected	Editable
Applying the StorageDevicePolicies function	Clear	Editable
Disabling USB storage devices	Clear	Editable
User Rights Assignment-[Deny log on locally]	Selected	Fixed
Security Options-[Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings]	Selected	Editable
Security Options-[Devices: Prevent users from installing printer drivers]	Selected	Editable
Security Options-[Devices: Restrict CD-ROM access to locally logged-on user only]	Selected	Editable
Security Options-[Devices: Restrict floppy access to locally logged-on user only]	Selected	Editable

Continues on the next page

Table Appendix 1.1.2-2 File Server: Standard Model - Domain/Combination Management (Table continued)

Setting item	Default check box state	Modification
Security Options-[Domain member: Require strong (Windows 2000 or later) session key]	Selected	Editable
Security Options-[Interactive logon: Do not display last user name]	Selected	Editable
Disable 'Security Options-[Interactive logon: Do not require CTRL+ALT+DEL]’	Selected	Editable
Security Options-[Interactive logon: Prompt user to change password before expiration]	Selected	Editable
Security Options-[Microsoft network server: Digitally sign communications (if client agrees)]	Selected	Editable
Security Options-[Microsoft network server: Server SPN target name validation level]	Selected	Editable
[MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)]	Selected	Editable
Disable [MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)]	Selected	Editable
[MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)]	Selected	Editable
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts]	Selected	Editable
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts and shares]	Selected	Editable
Security Options-[Network access: Do not allow storage of passwords and credentials for network authentication]	Selected	Editable
Security Options-[Network security: Allow Local System to use computer identity for NTLM]	Selected	Editable
Disable 'Security Options-[Network security: Allow LocalSystem NULL session fallback]’	Selected	Editable
Security Options-[Network security: LAN Manager authentication level]	Selected	Fixed
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) clients]	Selected	Editable
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) servers]	Selected	Editable
Disable 'Security Options-[Shutdown: Allow system to be shut down without having to log on]'	Selected	Editable
Security Options-[User Account Control: Admin Approval Mode for the Built'-in Administrator account]	Selected	Editable
Security Options-[User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Credential Validation]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Computer Account Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Account Management Events]	Selected	Editable

Continues on the next page

Table Appendix 1.1.2-2 File Server: Standard Model - Domain/Combination Management (Table continued)

Setting item	Default check box state	Modification
Advanced Audit Policy Configuration-[Audit Security Group Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit User Account Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Process Creation]	Selected	Editable
Advanced Audit Policy Configuration-[Audit RPC Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Account Lockout]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Logoff]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Logon]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Logon/ Logoff Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Special Logon]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Application Generated]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Removable Storage]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Audit Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Authentication Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Filtering Platform Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit MPSSVC Rule-Level Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Policy Change Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Sensitive Privilege Use]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other System Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security State Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security System Extension]	Selected	Editable
Advanced Audit Policy Configuration-[Audit System Integrity]	Selected	Editable
Personalization-[Prevent enabling lock screen camera]	Selected	Editable
Personalization-[Prevent enabling lock screen slide show]	Selected	Editable
WLAN Settings-[Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services]	Selected	Editable
Group Policy-[Configure registry policy processing]	Selected	Editable
Internet Communication settings-[Turn off downloading of print drivers over HTTP]	Selected	Editable

Continues on the next page

Table Appendix 1.1.2-2 File Server: Standard Model - Domain/Combination Management (Table continued)

Setting item	Default check box state	Modification
Internet Communication settings-[Turn off Event Viewer "Events.asp" links]	Selected	Editable
Internet Communication settings-[Turn off Internet download for Web publishing and online ordering wizards]	Selected	Editable
Internet Communication settings-[Turn off printing over HTTP]	Selected	Editable
Internet Communication settings-[Turn off Search Companion content file updates]	Selected	Editable
Internet Communication settings-[Turn off the "Publish to Web" task for files and folders]	Selected	Editable
Internet Communication settings-[Turn off the Windows Customer Experience Improvement Program]	Selected	Fixed
Internet Communication settings-[Turn off the Windows Messenger Customer Experience Improvement Program]	Selected	Fixed
Logon-[Do not display network selection UI]	Selected	Editable
Logon-[Do not enumerate connected users on domain-joined computers]	Selected	Editable
Disable 'Logon-[Enumerate local users on domain-joined computers]'	Selected	Editable
Logon-[Turn off app notifications on the lock screen]	Selected	Editable
Mitigation Options-[Untrusted Font Blocking]	Selected	Editable
User Profiles-[Turn off the advertising ID]	Selected	Editable
App Privacy-[Let Windows apps access account information]	Selected	Editable
App Privacy-[Let Windows apps access call history]	Selected	Editable
App Privacy-[Let Windows apps access contacts]	Selected	Editable
App Privacy-[Let Windows apps access email]	Selected	Editable
App Privacy-[Let Windows apps access location]	Selected	Editable
App Privacy-[Let Windows apps access messaging]	Selected	Editable
App Privacy-[Let Windows apps access motion]	Selected	Editable
App Privacy-[Let Windows apps access the calendar]	Selected	Editable
App Privacy-[Let Windows apps access the camera]	Selected	Editable
App Privacy-[Let Windows apps access the microphone]	Selected	Editable
App Privacy-[Let Windows apps access trusted devices]	Selected	Editable
App Privacy-[Let Windows apps control radios]	Selected	Editable
App Privacy-[Let Windows apps sync with devices]	Selected	Editable
App runtime-[Block launching Windows Store apps with Windows Runtime API access from hosted content]	Selected	Editable
AutoPlay Policies-[Turn off Autoplay]	Selected	Editable
AutoPlay Policies-[Disallow Autoplay for non-volume devices]	Selected	Editable
Cloud Content-[Do not show Windows Tips]	Selected	Editable
Cloud Content-[Turn off Microsoft consumer experiences]	Selected	Editable
Data Collection and Preview Builds-[Allow Telemetry]	Selected	Editable

Continues on the next page

Table Appendix 1.1.2-2 File Server: Standard Model - Domain/Combination Management (Table continued)

Setting item	Default check box state	Modification
Data Collection and Preview Builds-[Disable pre-release features or settings]	Selected	Editable
Data Collection and Preview Builds-[Do not show feedback notifications]	Selected	Editable
Data Collection and Preview Builds-[Toggle user control over Insider builds]	Selected	Editable
Event Log Service(Application)-[Specify the maximum log file size (KB)]	Selected	Editable
Event Log Service(Security)-[Specify the maximum log file size (KB)]	Selected	Editable
Event Log Service(System)-[Specify the maximum log file size (KB)]	Selected	Editable
File Explorer-[Turn off heap termination on corruption]	Selected	Editable
HomeGroup-[Prevent the computer from joining a homegroup]	Selected	Editable
OneDrive-[Prevent the usage of OneDrive for file storage]	Selected	Editable
OneDrive-[Save documents to OneDrive by default](Save documents to the local PC by default)	Selected	Editable
Remote Desktop Connection Client-[Do not allow passwords to be saved]	Selected	Editable
Device and Resource Redirection-[Do not allow drive redirection]	Selected	Editable
Security-[Require secure RPC communication]	Selected	Editable
Security-[Require user authentication for remote connections by using Network Level Authentication]	Selected	Editable
Disable ‘Search-[Allow Cortana]’	Selected	Editable
Software Protection Platform-[Turn off KMS Client Online AVS Validation]	Selected	Editable
Sync your settings-[Do not sync Apps]	Selected	Editable
Sync your settings-[Do not sync start settings]	Selected	Editable
Disable 'Windows Error Reporting-[Automatically send memory dumps for OS-generated error reports]'	Selected	Fixed
Disable 'Windows Logon Options-[Sign'-in last interactive user automatically after a system'-initiated restart]'	Selected	Editable
Notifications-[Turn off toast notifications on the lock screen]	Selected	Editable

■ Security Setting Items for Domain Controller: Standard Model with Standalone Management

The following table shows the security setting items for the Standard model on a domain controller.

Table Appendix 1.1.2-3 Domain Controller: Standard Model

Setting item	Default check box state	Modification
Creating domain users and groups	Selected	Fixed
Access control for files and folders	Selected	Editable

Continues on the next page

Table Appendix 1.1.2-3 Domain Controller: Standard Model (Table continued)

Setting item	Default check box state	Modification
Access control for DCOM (OPC) objects	Selected	Fixed
Personal firewall tuning	Selected	Fixed
Set 'Personal Firewall-[Allow unicast response]' to 'No'	Selected	Editable
Disabling NetBIOS over TCP/IP	Selected	Editable
Applying the StorageDevicePolicies function	Clear	Editable
Disabling USB storage devices	Clear	Editable
User Rights Assignment-[Access this computer from the network]	Selected	Editable
User Rights Assignment-[Add workstations to domain]	Selected	Editable
Security Options-[Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings]	Selected	Editable
Security Options-[Devices: Prevent users from installing printer drivers]	Selected	Editable
Security Options-[Devices: Restrict CD-ROM access to locally logged-on user only]	Selected	Editable
Security Options-[Devices: Restrict floppy access to locally logged-on user only]	Selected	Editable
Disable 'Security Options-[Domain controller: Allow server operators to schedule tasks]'	Selected	Editable
Disable 'Security Options-[Domain controller: Refuse machine account password changes]'	Selected	Editable
Security Options-[Domain member: Require strong (Windows 2000 or later) session key]	Selected	Editable
Security Options-[Interactive logon: Do not display last user name]	Selected	Editable
Disable 'Security Options-[Interactive logon: Do not require CTRL+ALT+DEL]'	Selected	Editable
Security Options-[Interactive logon: Prompt user to change password before expiration]	Selected	Editable
Security Options-[Microsoft network server: Digitally sign communications (if client agrees)]	Selected	Editable
Security Options-[Microsoft network server: Server SPN target name validation level]	Selected	Editable
[MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)]	Selected	Editable
Disable [MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)]	Selected	Editable
[MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)]	Selected	Editable
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts]	Selected	Editable
Security Options-[Network access: Do not allow anonymous enumeration of SAM accounts and shares]	Selected	Editable
Security Options-[Network access: Do not allow storage of passwords and credentials for network authentication]	Selected	Editable

Continues on the next page

Table Appendix 1.1.2-3 Domain Controller: Standard Model (Table continued)

Setting item	Default check box state	Modification
Security Options-[Network security: Allow Local System to use computer identity for NTLM]	Selected	Editable
Disable 'Security Options-[Network security: Allow Local-System NULL session fallback]’	Selected	Editable
Security Options-[Network security: Force logoff when logon hours expire]	Selected	Editable
Security Options-[Network security: LAN Manager authentication level]	Selected	Fixed
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) clients]	Selected	Editable
Security Options-[Network security: Minimum session security for NTLM SSP based (including secure RPC) servers]	Selected	Editable
Disable 'Security Options-[Shutdown: Allow system to be shut down without having to log on]'	Selected	Editable
Security Options-[User Account Control: Admin Approval Mode for the Built'-in Administrator account]	Selected	Editable
Security Options-[User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Credential Validation]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Computer Account Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Account Management Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security Group Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit User Account Management]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Process Creation]	Selected	Editable
Advanced Audit Policy Configuration-[Audit RPC Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Directory Service Access]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Directory Service Changes]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Account Lockout]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Logoff]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Logon]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Logon/Logoff Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Special Logon]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Application Generated]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Removable Storage]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Audit Policy Change]	Selected	Editable

Continues on the next page

Table Appendix 1.1.2-3 Domain Controller: Standard Model (Table continued)

Setting item	Default check box state	Modification
Advanced Audit Policy Configuration-[Audit Authentication Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Filtering Platform Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit MPSSVC Rule-Level Policy Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other Policy Change Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Sensitive Privilege Use]	Selected	Editable
Advanced Audit Policy Configuration-[Audit IPsec Driver]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Other System Events]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security State Change]	Selected	Editable
Advanced Audit Policy Configuration-[Audit Security System Extension]	Selected	Editable
Advanced Audit Policy Configuration-[Audit System Integrity]	Selected	Editable
Personalization-[Prevent enabling lock screen camera]	Selected	Editable
Personalization-[Prevent enabling lock screen slide show]	Selected	Editable
Logon-[Do not display network selection UI]	Selected	Editable
AutoPlay Policies-[Disallow Autoplay for non-volume devices]	Selected	Editable
Event Log Service(Application)-[Specify the maximum log file size (KB)]	Selected	Editable
Event Log Service(Security)-[Specify the maximum log file size (KB)]	Selected	Editable
Event Log Service(System)-[Specify the maximum log file size (KB)]	Selected	Editable
File Explorer-[Turn off heap termination on corruption]	Selected	Editable
Security-[Require secure RPC communication]	Selected	Editable
Store-[Turn off Automatic Download and Install of updates]	Selected	Editable
Store-[Turn off Automatic Download of updates on Win8 machines]	Selected	Editable
Store-[Turn off the offer to update to the latest version of Windows]	Selected	Editable
Store-[Turn off the Store application]	Selected	Editable
Sync your settings-[Do not sync Apps]	Selected	Editable
Sync your settings-[Do not sync start settings]	Selected	Editable
Disable 'Windows Error Reporting-[Automatically send memory dumps for OS-generated error reports]'	Selected	Editable
Disable 'Windows Logon Options-[Sign'-in last interactive user automatically after a system'-initiated restart]'	Selected	Editable

Appendix 1.2 IT Security Version 1.0

This section describes the security setting items that are configured with IT security version 1.0 along with their default values and whether they can be modified. However, some security setting items may not appear depending on the OS version.

Appendix 1.2.1 Setting Items for a Computer with CENTUM VP Software Installed

This section provides lists of the security setting items for a computer on which the product software is installed for each combination of security model and user management type.

■ Security Setting Items for Legacy Model

The following table shows the security setting items for the Legacy model.

Table Appendix 1.2.1-1 Legacy Model

Setting item	Default check box state	Modification	Remarks
Creating local users and groups	Selected	Fixed	None
Access control for files and folders	Selected	Fixed	Adds full control access permissions to the Everyone group. For some tools' folders under the Windows folder, reverts to the access permissions of parent folders.
Access control for product registry	Selected	Fixed	Adds full control access permissions to the Everyone group.
Access control for DCOM (OPC) objects	Selected	Fixed	Adds full control access permissions to the Everyone group.
Personal firewall tuning	Selected	Fixed	Disables the personal firewall.
Local security	Selected	Fixed	Grants access permissions to the Everyone group.
Changing IT environment settings - Hiding the last logon user name	Selected	Editable	None
Changing IT environment settings - Applying AutoRun restrictions	Selected	Editable	None

SEE ALSO For more information about creation of users/groups, refer to:

"■ Combination of User Management and Security Model for Windows" on page 2-17

■ Security Setting Items for Standard Model with Standalone Management

The following table shows the security setting items for the combination of Standard model and Standalone management.

Table Appendix 1.2.1-2 Standard Model - Standalone Management

Setting item	Default check box state	Modification
Creating local users and groups	Selected	Fixed
Access control for files and folders	Selected	Fixed
Access control for product registry	Selected	Fixed
Access control for DCOM (OPC) objects	Selected	Fixed
Personal firewall tuning	Selected	Fixed
Local security	Selected	Fixed

Continues on the next page

Table Appendix 1.2.1-2 Standard Model - Standalone Management (Table continued)

Setting item	Default check box state	Modification
Changing IT environment settings - Changing the LAN Manager authentication level	Selected	Editable
Changing IT environment settings - Hiding the last logon user name	Selected	Editable
Changing IT environment settings - Applying AutoRun restrictions	Selected	Editable
Changing IT environment settings - Disabling NetBIOS over TCP/IP	Clear	Editable
Changing IT environment settings - Applying the StorageDevicePolicies function	Clear	Editable
Changing IT environment settings - Disabling USB storage devices	Clear	Editable
Changing IT environment settings - Applying software restriction policies	Clear	Editable

SEE ALSO For more information about creation of users/groups, refer to:

"■ Combination of User Management and Security Model for Windows" on page 2-17

■ Security Setting Items for Standard Model with Domain or Combination Management

The following table shows the security setting items for the combination of Standard model and Domain or Combination management.

Table Appendix 1.2.1-3 Standard Model - Domain/Combination Management

Setting item	Default check box state	Modification
Creating local users and groups	Selected	Fixed
Creating domain users and groups	Selected	Fixed
Access control for files and folders	Selected	Fixed
Access control for product registry	Selected	Fixed
Access control for DCOM (OPC) objects	Selected	Fixed
Personal firewall tuning	Selected	Fixed
Local security	Selected	Fixed
Changing IT environment settings - Changing the LAN Manager authentication level	Selected	Editable
Changing IT environment settings - Hiding the last logon user name	Selected	Editable
Changing IT environment settings - Applying AutoRun restrictions	Selected	Editable
Changing IT environment settings - Disabling NetBIOS over TCP/IP	Selected	Editable
Changing IT environment settings - Applying the StorageDevicePolicies function	Clear	Editable
Changing IT environment settings - Disabling USB storage devices	Clear	Editable

Continues on the next page

Table Appendix 1.2.1-3 Standard Model - Domain/Combination Management (Table continued)

Setting item	Default check box state	Modification
Changing IT environment settings - Applying software restriction policies	Clear	Editable

SEE ALSO For more information about creation of users/groups, refer to:

"■ Combination of User Management and Security Model for Windows" on page 2-17

Appendix 1.2.2 Setting Items for a File Server or Domain Controller

This section provides lists of the security setting items for a file server or a domain controller for each combination of security model and user management type.

■ Security Setting Items for File Server: Legacy Model

The following table shows the security setting items for the Legacy model on a file server.

Table Appendix 1.2.2-1 File Server: Legacy Model

Setting item	Default check box state	Modification	Remarks
Creating local users and groups	Selected	Fixed	Creates the CTM_PROCESS user.
Access control for files and folders	Selected	Fixed	For the Windows folder, reverts to the access permissions of parent folders. For the Project folder, adds full control access permissions to the Everyone group.
Personal firewall tuning	Selected	Fixed	Disables the personal firewall.
Local security	Selected	Fixed	Grants access permissions to the Everyone group.

■ Security Setting Items for File Server: Standard Model with Standalone Management

The following table shows the security setting items for the combination of Standard model and Standalone management on a file server.

Table Appendix 1.2.2-2 File Server: Standard Model - Standalone Management

Setting item	Default check box state	Modification
Creating local users and groups	Selected	Fixed
Access control for files and folders	Selected	Fixed
Personal firewall tuning	Selected	Fixed
Local security	Selected	Fixed
Changing IT environment settings - Applying the audit policy	Selected	Editable
Changing IT environment settings - Changing the LAN Manager authentication level	Selected	Editable
Changing IT environment settings - Applying AutoRun restrictions	Selected	Editable
Changing IT environment settings - Disabling NetBIOS over TCP/IP	Clear	Editable
Changing IT environment settings - Applying the StorageDevicePolicies function	Clear	Editable
Changing IT environment settings - Disabling USB storage devices	Clear	Editable

SEE ALSO For more information about creation of users/groups, refer to:

"■ Combination of User Management and Security Model for Windows" on page 2-17

■ Security Setting Items for File Server: Standard Model with Domain or Combination Management

The following table shows the security setting items for the combination of Standard model and Domain or Combination management on a file server.

Table Appendix 1.2.2-3 File Server: Standard Model - Domain/Combination Management

Setting item	Default check box state	Modification
Creating local users and groups	Selected	Fixed
Creating domain users and groups	Selected	Fixed
Access control for files and folders	Selected	Fixed
Personal firewall tuning	Selected	Fixed
Local security	Selected	Fixed
Changing IT environment settings - Applying the audit policy	Selected	Editable
Changing IT environment settings - Changing the LAN Manager authentication level	Selected	Editable
Changing IT environment settings - Applying AutoRun restrictions	Selected	Editable
Changing IT environment settings - Disabling NetBIOS over TCP/IP	Selected	Editable
Changing IT environment settings - Applying the Storage-DevicePolicies function	Clear	Editable
Changing IT environment settings - Disabling USB storage devices	Clear	Editable

SEE ALSO For more information about creation of users/groups, refer to:

"■ Combination of User Management and Security Model for Windows" on page 2-17

■ Security Setting Items for Domain Controller: Standard Model with Domain or Combination Management

The following table shows the security setting items for the combination of Standard model and Domain or Combination management on a domain controller.

Table Appendix 1.2.2-4 Domain Controller: Standard Model - Domain or Combination Management

Setting item	Default check box state	Modification
Creating domain users and groups	Selected	Fixed
Access control for files and folders	Selected	Editable
Access control for DCOM (OPC) objects	Selected	Fixed
Personal firewall tuning	Selected	Fixed
Changing IT environment settings - Applying the audit policy	Selected	Editable
Changing IT environment settings - Changing the LAN Manager authentication level	Selected	Editable

Continues on the next page

Table Appendix 1.2.2-4 Domain Controller: Standard Model - Domain or Combination Management (Table continued)

Setting item	Default check box state	Modification
Changing IT environment settings - Applying AutoRun restrictions	Selected	Editable
Changing IT environment settings - Disabling NetBIOS over TCP/IP	Selected	Editable
Changing IT environment settings - Applying the StorageDevicePolicies function	Clear	Editable
Changing IT environment settings - Disabling USB storage devices	Clear	Editable

TIP

The IT Security Tool creates only the users and groups that are to be created on the domain.

SEE ALSO

For more information about creation of users/groups, refer to:

"■ Combination of User Management and Security Model for Windows" on page 2-17

Revision Information

Title : CENTUM VP Security Guide
Manual No. : IM 33J01C30-01EN

Aug. 2019/9th Edition/R6.07 or later

2.1 Added footnotes about the UACS station in “● Security Measures to Fight Against Security Threats.”

3.1.1 Added PROFINET Configurator in “■ Target Folders.”
Added UACS Migration Tool in “■ Access Permissions for Programs.”

3.1.2 Added PROFINET Configurator in “■ Registry Types.”
Added PROFINET Configurator in “■ Registry Keys.”

Added PROFINET Configurator in “■ Access Permissions for Registries.”

3.1.4 Added local security policy on the UACS station.

3.4.1 Added “■ Settings.”

3.5.10 Added footnotes about the UACS station in “■ Remote Desktop Service (Windows Component).”

Appendix 1.1.1 Added footnotes about the UACS station in “■ Security Setting Items for Standard Model with Standalone Management.”
Added footnotes about the UACS station in “■ Security Setting Items for Standard Model with Domain or Combination Management.”

Aug. 2018/8th Edition/R6.06

1.2 Added footnotes about the UACS station in “● Security Measures to Fight Against Security Threats.”

2.1 Updated tables and descriptions in “■ Security Models and Security Measures.”

2.2.3 Deleted descriptions from “■ Combination of User Management and Security Model for Windows.”

Added a new section “■ The Users and User Groups Added by the Vnet/IP Interface Package.”

3.1.1 Added a folder related to Automation Design Suite in “Table: Target Folders” in “■ Target Folders.”

Added a folder related to Vnet/IP interface package in “Table: Target Folders” in “■ Target Folders.”

Added a description about Windows Server 2016 in the footnotes of “Table: Target Folders” in “■ Target Folders.”

Added the Vnet/IP interface management tool in “Table: Access Permissions for Programs that are Started from the Start Menu” in “■ Access Permissions for Programs.”

3.1.4 Added users/user groups related to Vnet/IP interface package in “Table: Permissions Set for Local Security Policy.”

3.2 Added a section “■ Vnet/IP Interface Package Related Exceptional Settings.”

3.3 Updated the “Table: Windows Services That can be Stopped – IT security version 2.0” in “■ Unused Windows Services” with Windows Server 2016 information.

Updated the “Table: Windows Services That can be Stopped – IT security version 1.0” in “■ Unused Windows Services” with Windows Server 2016 information.

3.5.2 Updated descriptions in “● Cautions when Software Restriction Policies are Applied.”

3.5.6 Added descriptions in “■ Detailed Tracking.”

Added descriptions in “■ Object Access.”

3.5.9 Added descriptions in “Table: Settings” in “■ Settings.”

6.1 Added descriptions

6.6.1 Changed a picture and changed descriptions in “■ Changing Procedure.”

6.6.2 Deleted descriptions in “Changing Procedure.”

6.7 Deleted a description and added a TIP in “■ Export Procedure - IT Security Tool.”

Deleted descriptions in “■ Export Procedure - ITSecuritySettingItemExport.exe.”

Deleted descriptions in “■ Import Procedure - IT Security Tool.”

6.8 Deleted a description in “■ Procedure for Viewing.”

6.9.1 Updated descriptions.

6.10 Reviewed structure of sections.

6.10.8 Added “CreateVNTUser.”

Appendix 1.1.1 Updated the table.

Appendix 1.1.2 Updated the table.

Nov. 2017/7th Edition/R6.05

2.1 Updated “Table: Security Measures Corresponding to Security Models - IT security version 2.0.”

2.2.3 Added descriptions in "Table: Legacy Model.”

Added descriptions in "Table: Standard Model/Strengthened Model - Standalone Management.”

Added descriptions in "Table: Standard Model/Strengthened Model - Domain Management.”

Added descriptions in "Table: Standard Model/Strengthened Model - Combination Management.”

3.1.1 Added descriptions in "Table: Target Folders.”

Added descriptions in "Table: Access Permissions to Programs that are Started from the Start Menu.”

3.1.2 Added descriptions in "Table: Access Permissions for CENTUM Related Registries.”

Added descriptions in "Table: Access Permissions for DCOM Related Registries.”

Added descriptions in "Table: Access Permissions for PROFIBUS-DP Configurator Related Registries.”

3.1.4 Added descriptions in "Table: Permissions Set for Local Security Policy.”

3.2 Added descriptions in "Table: CENTUM Related Exceptional Settings.”

3.5.5 Updated "Table: Settings.”

3.6.8 Updated "Table: Settings.”

6.10 Added descriptions

Added a new section “■ CreateAdsAgent.”

Corrected error in “● Start Method” in “■ ChangeOffuserPassword.”

Apr. 2017/6th Edition/R6.04

1.2 Updated to introduce IT security versions for stronger system security.

2.1 Updated to introduce IT security versions for stronger system security.

3. Updated to introduce IT security versions for stronger system security.

4. Updated to introduce IT security versions for stronger system security.

6. Reorganized.

Appendix Newly added.

Sep. 2016/5th Edition/R6.03.10

2.2.3 Updated the descriptions of the RDC_PROCESS user

3.1.1 Updated descriptions in "■ Target Folders."

3.2 Updated descriptions in "■ Types of Exception Settings."

Updated descriptions in "■ CENTUM Related Exceptional Settings."

Deleted the section "■ Settings of the Redundant Platform for the UGS Redundancy Function (Computer Switchover Type)."

3.3 Updated descriptions in "■ Unused Windows Services."

3.4.1 Updated descriptions.

Changed the title of "■ Cautions when Changing the User Names on the Redundant Platform for the UGS Redundancy Function (Computer Switchover Type)" to "■ Cautions when Changing the User Names on the Dual-redundant Platform for Computer of a Computer Switchover Type UGS" and updated descriptions.

3.4.11 Updated descriptions in "■ Settings."

Added descriptions in "■ Cautions."

6.2 Updated descriptions in "● Detailed Explanation" in "■ CreateRDCProcess."

Jun. 2016/4th Edition/R6.03

2.2.3 Added RDC_PROCESS to user names.

3.1.1 Added UGS redundancy related folders and user/group names.

3.1.2 Added Windows Server 2012 R2 to OS descriptions, and added RDC_PROCESS to user names.

3.1.4 Added RDC_PROCESS to user names.

3.2 Added descriptions of the UGS redundancy function.

3.3 Added Windows Server 2012 R2 to OS descriptions.

3.4.1 Added descriptions of the UGS redundancy function, and added Windows Server 2012 R2 to OS descriptions.

3.4.3 Added Windows Server 2012 R2 to OS descriptions.

3.4.11 Added descriptions of the UGS redundancy function.

6.2 Added descriptions of RDC_PROCESS.

Dec. 2015/3rd Edition/R6.02

3.1.1 ADSuite folder name has been updated.

6.2 Description has been added to the IMPORTANT note for CreateAdsProcess.

Apr. 2015/2nd Edition/R6.01.10

2.2.3 Descriptions have been updated.

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