User's
Manual

SMARTDAC+®

Model GX10/GX20/GP10/GP20

Advanced Security Function (/AS) User's Manual

vigilantplant®

YOKOGAWA ◆
Yokogawa Electric Corporation

IM 04L51B01-05EN
3rd Edition

Introduction

Thank you for purchasing the SMARTDAC+ Series GX10/GX20/GP10/GP20 (hereafter referred to as the GX or GP).
This manual explains how to use the Advanced Security Function (/AS option) of the GX/GP. **Although the display of GX20 is used in this manual, GX10/GP10/GP20 can be operated similarly.**
To ensure correct use, please read this manual thoroughly before beginning operation.

Notes

- The contents of this manual are subject to change without prior notice as a result of continuing improvements to the instrument's performance and functions.
- Every effort has been made in the preparation of this manual to ensure the accuracy of its contents. However, should you have any questions or find any errors, please contact your nearest YOKOGAWA dealer.
- Copying or reproducing all or any part of the contents of this manual without the permission of YOKOGAWA is strictly prohibited.

Trademarks

- vigilantplant is a registered trademark of Yokogawa Electric Corporation.
- SMARTDAC+ and SMARTDACPLUS are registered trademark of Yokogawa Electric Corporation.
- Microsoft and Windows are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
- Adobe and Acrobat are registered trademarks or trademarks of Adobe Systems Incorporated.
- Kerberos is a trademark of Massachusetts Institute of Technology (MIT).
- RC4 is a registered trademark of RSA Security Inc. in the United States and/or other countries.
- Company and product names that appear in this manual are registered trademarks or trademarks of their respective holders.
- The company and product names used in this manual are not accompanied by the registered trademark or trademark symbols (® and ™).

Using Open Source Software

This product uses open source software.
For details on using open source software, see Regarding the Downloading and Installing for the Software, Manuals and Labels (IM 04L61B01-11EN).

Revisions

May 2014	1st Edition
Dec 2014	2nd Edition
Dec 2015	3rd Edition

3rd Edition: Dec 2015 (YK)

Conventions Used in This Manual

Unit

K Denotes 1024. Example: 768K (file size)

k Denotes 1000.

Markings

⚠ **CAUTION**

Improper handling or use can lead to injury to the user or damage to the instrument. This symbol appears on the instrument to indicate that the user must refer to the user's manual for special instructions. The same symbol appears in the corresponding place in the user's manual to identify those instructions. In the manual, the symbol is used in conjunction with the word "WARNING" or "CAUTION."

WARNING

Calls attention to actions or conditions that could cause serious or fatal injury to the user, and precautions that can be taken to prevent such occurrences.

CAUTION

Calls attention to actions or conditions that could cause light injury to the user or cause damage to the instrument or user's data, and precautions that can be taken to prevent such occurrences.

Note

Calls attention to information that is important for the proper operation of the instrument.

Reference Item

▶ Reference to related operation or explanation is indicated after this mark.

Example: ▶ section 4.1

Conventions Used in the Procedural Explanations

Bold characters Denotes key or character strings that appear on the screen.

Example: **Volt**

A a # 1 Indicates the character types that can be used.

A uppercase alphabet, a lowercase alphabet, # symbol,

1 numbers

Procedure

Explanation

Carry out the procedure according to the step numbers. All procedures are written with inexperienced users in mind; depending on the operation, not all steps need to be taken.

Explanation gives information such as limitations related the procedure.

Path

Description

Indicates the setup screen and explains the settings.

Applicable Recorders

The contents of this manual correspond to the GX/GP with release number 3 (see the STYLE S number) and style number 1 (see the STYLE H number).

What This Manual Explains

This manual primarily explains how to use the login, audit trail, and signature functions of the advanced security function. For details on how to use other functions, see also the User's Manual (IM04L51B01-01EN).
For details on the communication functions, see the Communication Command User's Manual (IM04L51B01-17EN).

The GX20/GP20 standard type and large memory type are distinguished using the following notations.

- Standard type: GX20-1/GP20-1
- Large memory type: GX20-2/GP20-2

The following terms are used for references to other manuals:

Notation	Description
User's Manual	Model GX10/GX20/GP10/GP20 Paperless Recorder User's Manual Refers to the IM 04L51B01-01EN.
First Step Guide	Model GX10/GX20/GP10/GP20 Paperless Recorder First Step Guide Refers to the IM 04L51B01-02EN.
Multi-batch Function Manual	Model GX10/GX20/GP10/GP20/GM10 Multi-batch Function (/BT) User's Manual Refers to the IM 04L51B01-03EN.
Communication Command Manual	Model GX10/GX20/GP10/GP20 Paperless Recorder Communication Command User's Manual Refers to the IM 04L51B01-17EN.
Universal Viewer Manual	SMARTDAC+ STANDARD Universal Viewer User's Manual Refers to the IM 04L61B01-01EN.

Revision History

Edition	Product	Description
1	Release number 2 (Version 2.0x)	New edition
	Style number 1	
2	Release number 2 (Version 2.02)	Calibration correction has been added to user privileges.
	Style number 1	
3	Release number 3 (Version 3.01)	Support for Multi-batch function (/BT) and Aerospace heat treatment (/AH) has been added. Event log contents has been added.
	Style number 1	

Blank

Contents

Chapter 3 Password Management

Appendix

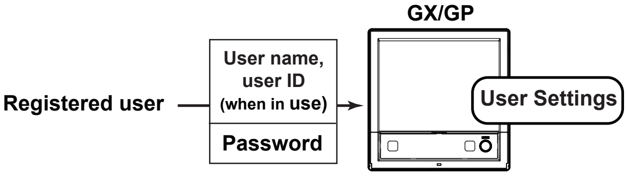
1.1 Using the Advanced Security Function

This section gives a general overview of how to use the advanced security function.

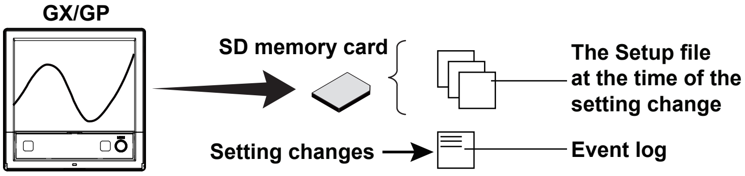
1.1.1 Operation Overview

Configuring Functions

First, you need to configure the GX/GP functions. You have to configure the measurement settings and then register GX/GP users. After you register users, to use the GX/GP, you will need to log in to it by entering a user name, user ID (when in use), and password.

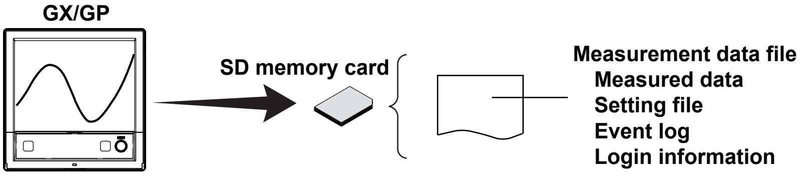


History of setting changes is recorded in an event log, and a new setting file is saved to an SD memory card.



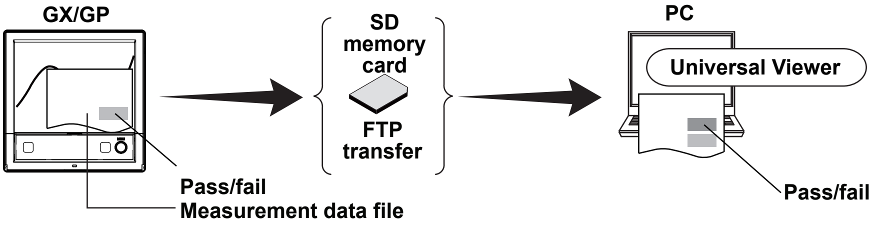
Measurement

Measured data (display or event data; see section 1.2) is recorded to the GX/GP internal memory and saved to files on an external storage medium. The measurement data file includes the settings at the time of measurement, a history of the operations (event log), and login (user) information.



Signing Files

You can check the measured data and the event log and add pass or fail data to the measurement data file. This is referred to as “signing.” Only permitted users can sign files. On the GX/GP, you can only sign measurement data files in the internal memory. You can sign measurement data files that have been saved to an external storage medium using the standard PC software, Universal Viewer.



1.1.2 GX/GP Operation Range

The GX/GP Manages Measured Data in Its Internal Memory

- You cannot change the measured data in the GX/GP internal memory. The only way you can delete the measured data is by initializing the internal memory.
- From the GX/GP, you can only sign measurement data files in the internal memory.
- Measured data in the internal memory can automatically be saved to a file on an external storage medium. During this operation, if a file with the same name exists on the external storage medium, it is overwritten unconditionally.

You Cannot Use the GX/GP to Change a Measurement Data File That Has Been Saved to an External Storage Medium

- You can view a measurement data file that has been saved to an external storage medium on the GX/GP, but you cannot change or delete it.
- The GX/GP cannot format external storage media.

1.1.3 PC Software

You can use the standard PC software, Universal Viewer, to view and sign GX/GP measurement data files.

▶ See the Universal Viewer Manual (IM 04L61B01-01EN).

1.1.4 Terminology

Administrator ▶section 1.3

A type of user that can be registered on the GX/GP. An administrator has access to all operations.

User ▶section 1.3

A type of user that can be registered on the GX/GP. You can limit the range of operations that a user has access to.

Monitor User ▶section 1.3

A type of user that can be registered on the GX/GP. A monitor user can only monitor the GX/GP by connecting to the Web application or FTP server.

User Privileges ▶section 1.3

The range of operations that a user can perform.

Login and Logout ▶section 1.3

Logging in is the act of entering a user name, user ID (when in use), and password that are registered on the GX/GP so that you can operate it. Logging out is the act of clearing the logged in status.

Audit Trail Function ▶section 1.5

This function saves information that can be used to retrace past operations.

Event Log ▶section 1.5

A log that lists setting changes and operations in a specified format in chronological order.

Signature Function, Signing ▶section 1.6

A function for checking saved data and adding pass-or-fail approval information and the user name to the measurement data file, or the act of adding such information.

Password Management Function ▶section 1.4

A function for managing the users who can access the GX/GP by using a KDC server connected to the network.

Auto Save ▶section 1.2

A method for automatically saving the data in the internal memory to the SD memory card.

Manual Save ▶section 1.2

A method for specifying an external storage medium and saving unsaved data in the internal memory to files on the storage medium when a given operation is carried out.

Media FIFO (First in first out) ▶section 1.2

A method for saving a new file to the SD memory card when there is not enough space, in which the oldest file is deleted and then the new file is saved.

Login Information ▶section 1.5, Universal Viewer Manual

A user’s password may change during operation. This can happen when the password expires. The login information is the user name and password information at the time that the measurement data file was created. To sign a measurement data file using Universal Viewer, you must log in as a user that is registered in the login information in that file. You cannot view the login information.l

1.2 Recording and Saving Data

This section explains the types of data that a GX/GP with the /AS advanced security option can record and how to save them.

1.2.1 Data Types

The types of data that the GX/GP can store to files are listed below.

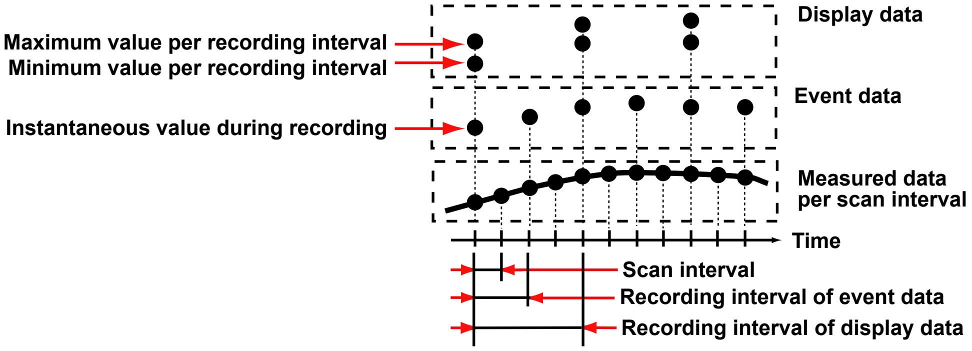
▶ For information about file name extensions, see page 1-14.

Data Type	Description
Display data	• Waveform data displayed on the trend display. The measured data is recorded at the specified trend interval. • The minimum and maximum values among the measured data within the trend interval are saved. • A header string (shared with other files) can be written in the file. • The file contains alarm and message information, an event log, login information, and setting parameters. • Data format: Binary (undisclosed) The data is encrypted.
Event data	• Measured data that is recorded at the specified recording interval. The only available recording mode is Free. You cannot start recording with triggers. • A header string (shared with other files) can be written in the file. • The file contains alarm and message information, an event log, login information, and setting parameters. • Data format: Binary (undisclosed) The data is encrypted.
Manual sampled data	• Instantaneous value of the measured data when a manual sample operation is executed. • A header string (shared with other files) can be written in the file. • Data format: Text
Report Data (/MT option)	• Hourly, daily, weekly, monthly, batch, daily custom report data. Report data is created at an interval that is determined by the report type (one hour for hourly reports, one day for daily reports, and so on). • A header string (shared with other files) can be written in the file. • Data format: Text • The data can be converted to Excel and PDF formats.
Snapshot data (screen image data)	• GX/GP screen image data. • Can be saved to an SD memory card or USB flash memory. • Data format: PNG
Setting parameters	• The setting parameters of the GX/GP. • Data format: Binary (undisclosed) The data is encrypted.
Alarm summary data	• The alarm summary information in the internal memory is saved to a text file. • Can be saved to a SD memory card and USB flash memory.

Display data and event data

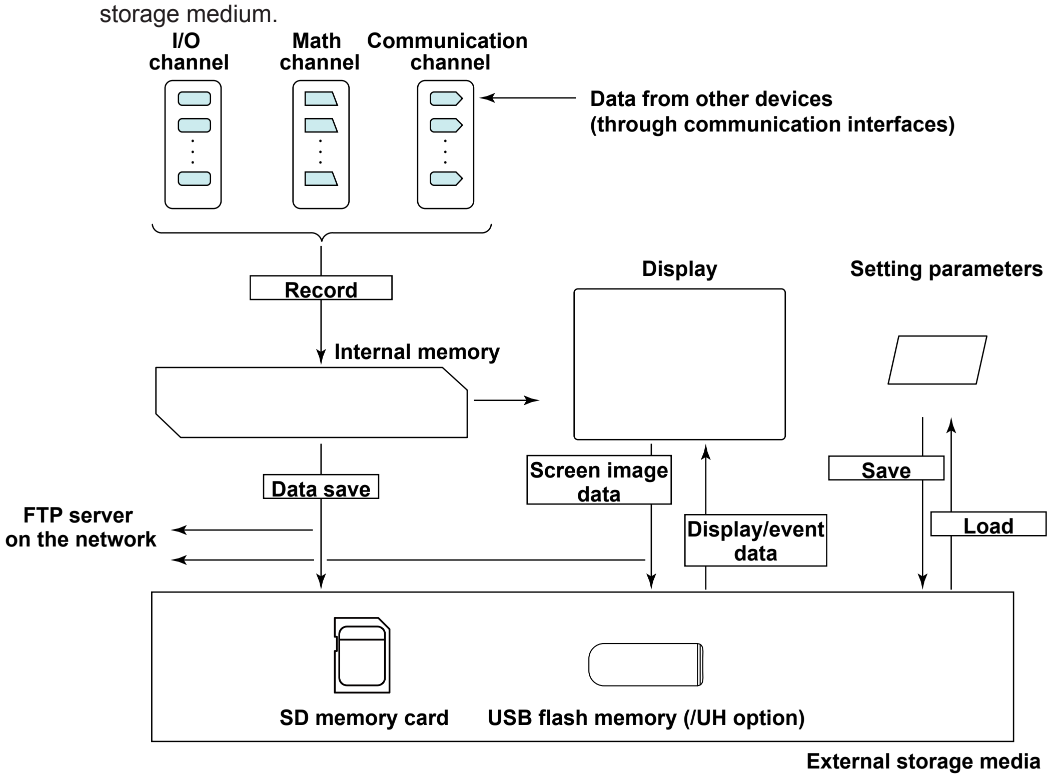
Display data can be likened to the conventional recording on the chart sheet and are useful for long-term recording.

Event data is useful when you wish to record the measured data in detail.


Maximum value per recording interval
Minimum value per recording interval
Instantaneous value during recording
Display data
Event data
Measured data per scan interval
Time
Scan interval
Recording interval of event data
Recording interval of display data

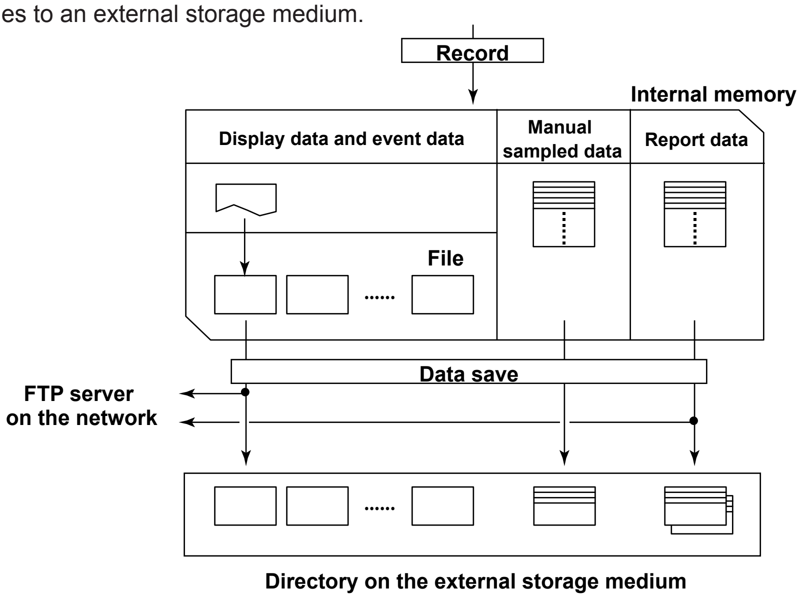
1.2.2 Data Recording and Storage Flowchart

Measured data is recorded once to the internal memory and then saved to the external storage medium.



Internal Memory

Display data and event data are held in files in the internal memory. They are also saved as files to an external storage medium.


Record
Internal memory
Display data and event data
Manual sampled data
Report data
File
......
Data save
FTP server on the network
......
Directory on the external storage medium

1.2.3 Display, Event, and Setting File Encryption

Display, event, and setting files are encrypted. You cannot change their data or delete them.

1.2.4 Display and Event Data Recording Methods

▶ For the setting procedure, see section 1.9, “Setting Recording Conditions (Recording mode, recording interval, saving interval)” and 1.8, “Setting Measurement Conditions (Scan interval, A/D integrate, etc.)” in the User’s Manual.
▶ For operating instructions, see section 2.1, “Starting and Stopping Recording and Computation” in the User’s Manual.

Type of Data to Record

You can choose to record display or event data.

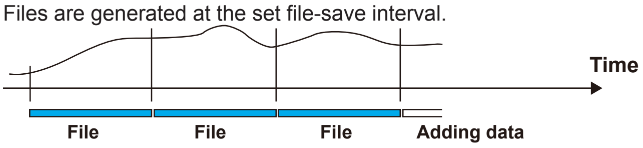
- **Choosing What Type of Data to Record**

  Record the type of data that meets your needs. Use the following examples for reference.
  Example 1: Record continuous waveform data only, just like conventional chart sheet recording instruments.
  Record the display data.
  Example 2: Continuously record data that is as detailed as possible.
  Record event data by specifying the recording interval.

Internal Memory

The measured data is partitioned and saved to files at set intervals. If the internal memory is full or if the number of display data files and event data files exceeds 500 for GX10/GP10 and GX20-1/GP20-1 or 1000 for GX20-2/GP20-2, files are overwritten from the oldest file.

Recording Conditions of Display Data

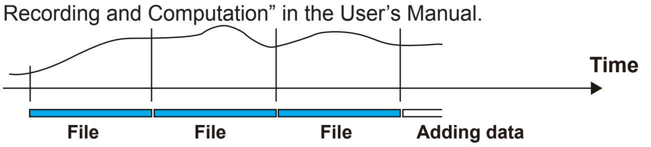
Item	Description
Channel type	You can set the channel type to measurement, computation, or communication.
Recording interval	Determined by the “trend interval” (see the following diagram). You cannot choose an interval that is shorter than the scan interval.
File generation	Files are generated at the set file-save interval.  A file is also created in the following instances. • When a file is created manually • When recording is stopped. • When file creation is executed with the event action function • After recovering from a power failure
Recording start/stop	You can start or stop recording on the menu screen or using **START/ STOP** key. ▶ For operating instructions, see section 2.1, “Starting and Stopping Recording and Computation” in the User’s Manual.

Trend Interval and Display Data Recording Interval

Trend Interval*	5s	10s	15s	30s	1min
Recording interval	100ms	200ms	500ms	1s	2s
Trend Interval*	2min	5min	10min	15min	20min
Recording interval	4s	10s	20s	30s	40s
Trend Interval*	30min	1h	2h	4h	10h
Recording interval	1min	2min	4min	8min	20min

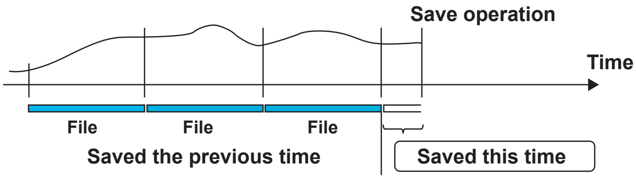
* You cannot choose a recording interval that is shorter than the scan interval.

Recording Conditions of Event Data

Item	Description
Channel type	Same as display data.
Recording interval	Choices are available in the range of 100 ms to 30 min. You cannot choose a recording interval that is shorter than the scan interval.
File generation	A file is generated when the set data length is reached. A file is also created in the following instances. • When a file is created manually • When recording is stopped • When file creation is executed with the event action function • After recovering from a power failure
Mode	Free (always recording) You can start or stop recording on the menu screen or using the **START/STOP** key. ▶ For operating instructions, see section 2.1, “Starting and Stopping Recording and Computation” in the User’s Manual. 

Creating Files through Touch Operation

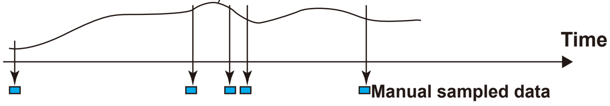
You can use touch operations to generate files.



▶ For operating instructions, see section 2.5.6, “Saving Display Data or Event Data during Recording through Touch Operation” in the User’s Manual (IM04L51B01-01EN).

1.2.5 Manual Sampled Data

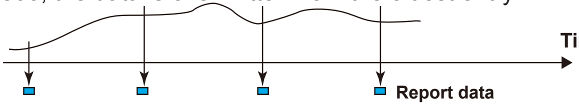
Manual sampled data is recorded to internal memory. If the number of manual sampled data entries exceeds 400, the data is overwritten from the oldest entry.



▶ For operating instructions, see section 2.5.3, “Manually Saving Instantaneous Values of Measured Data (Manual sample)” in the User’s Manual.

1.2.6 Report Data (/MT option)

Report data is saved to the internal memory. If the number of report data entries exceeds 800, the data is overwritten from the oldest entry.



▶ For the setting procedure, see section 1.12, “Setting the Report Function (/MT option)” in the User’s Manual.

1.2.7 Directories and File Saving on External Storage Medium

Types of External Storage Medium

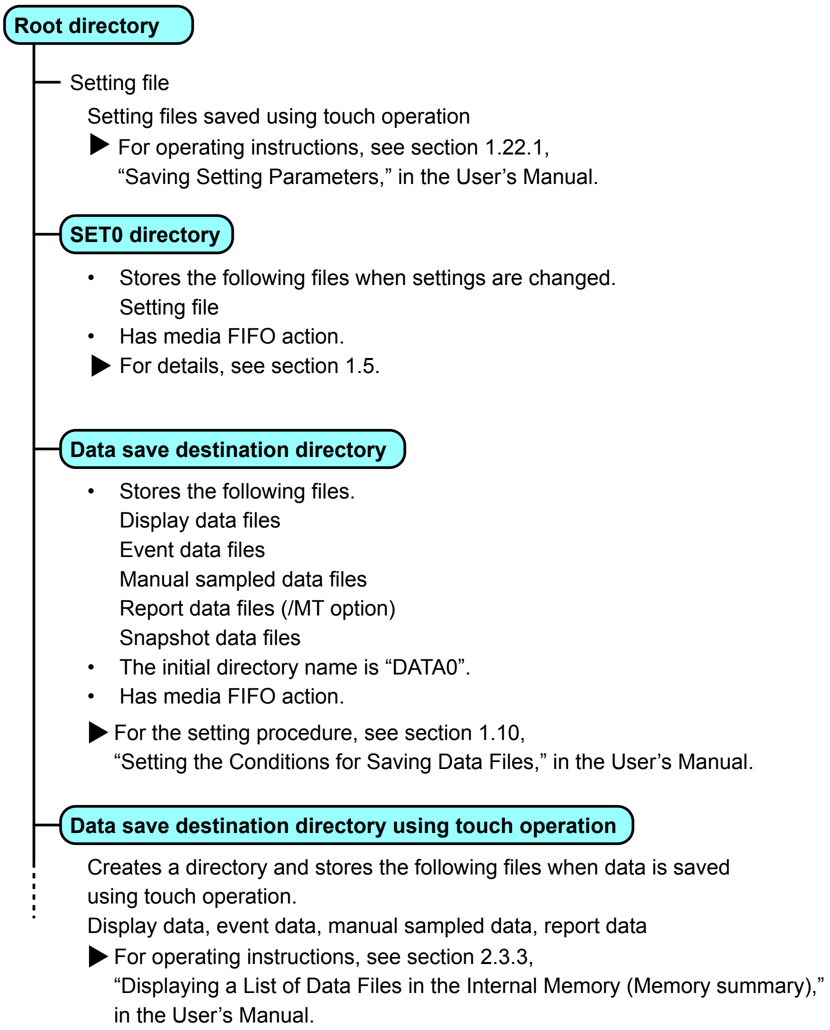
- SD memory card (1 GB or more)
- USB flash memory (/UH option)

SD Memory Card Directory

The directories that the GX/GP automatically creates in the SD memory card and the files that it saves are indicated below.

Note

- Do not place a file named “SET0” in the SD card.
- Do not place a file with the same name as the directory name (“DATA0” by default) in the storage medium for saving data.



Root directory

Setting file

Setting files saved using touch operation

▶ For operating instructions, see section 1.22.1, “Saving Setting Parameters,” in the User’s Manual.

SET0 directory

- Stores the following files when settings are changed.
  Setting file
- Has media FIFO action.

▶ For details, see section 1.5.

Data save destination directory

- Stores the following files.
  Display data files
  Event data files
  Manual sampled data files
  Report data files (/MT option)
  Snapshot data files
- The initial directory name is “DATA0”.
- Has media FIFO action.

▶ For the setting procedure, see section 1.10, “Setting the Conditions for Saving Data Files,” in the User’s Manual.

Data save destination directory using touch operation

Creates a directory and stores the following files when data is saved using touch operation.

Display data, event data, manual sampled data, report data

▶ For operating instructions, see section 2.3.3, “Displaying a List of Data Files in the Internal Memory (Memory summary),” in the User’s Manual.

Saved Files

GX/GPs with the advanced security option create the following types of files.

Type	Extension	Notes
Display data file	GSD	-
Event data file	GSE	-
Setting file	GSL	See page 1-14 and section 1.5.
Manual sampled data file	GMN	-
Snapshot data file	png	-
Report data file (/MT option)	GRE	-
	xlsx or xlsm	For use with the report template function
	pdf	

1.2.8 Saving Data to External Storage Medium

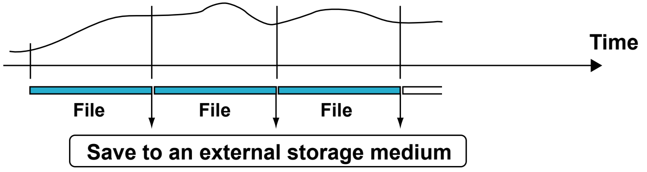
Auto Save

The following type of files are automatically saved: display data, event data, manual sampled data, and report data (/MT option).

Keep the SD memory card inserted in the drive at all times. The data in the internal memory is automatically saved to the SD memory card.

▶ For the setting procedure, see section 1.10, “Setting the Conditions for Saving Data Files” in the User’s Manual.

Auto Save Timing

Data Type	Description
Display data	The file is saved when the file is created.  Time File File File Save to an external storage medium
Event data	Same as display data.
Manual sampled data	The first time manual sample is executed, a manual sampled data file is created on the SD memory card. Data is appended to this file at every subsequent manual sample operation. A new file is created after manual sampled data is stored 100 times. ▶ For operating instructions, see section 2.5.3, “Manually Saving Instantaneous Values of Measured Data (Manual sample)” in the User’s Manual.
Report data	The first time report data is generated, a report data file is created on the SD memory card, and report data is stored. Report data is appended to this file at every report interval. **Dividing of the report files** The appending of the report data to the file is stopped at a specified time, and subsequent reports are saved to a new file. The file is divided in the unit shown in the table below. Also, when recording is stopped, all report files are divided. **Report template function** Every time a report file is divided, a report file is created according to the specified template format such as an Excel format or PDF format. The report file can also be printed. ▶ For the setting procedure, see section 1.12, “Setting the Report Function (/MT option)” in the User’s Manual.

Report Type	Report File	
	Separate	Combine
Hourly + Daily	🗎 a file for each daily report 🗎 hourly reports for a day	🗎 hourly reports for a day and a daily report
Daily + Weekly	🗎 a file for each weekly report 🗎 daily reports for a week	🗎 daily reports for a week and a weekly report
Daily + Monthly	🗎 a file for each monthly report 🗎 daily reports for a month	🗎 daily reports for a month and a monthly report
Batch	🗎 a file for each recording start/stop operation The file will be divided if the number of data entries exceeds 200.	🗎 a file for each recording start/stop operation The file will be divided if the number of data entries exceeds 200.
Day custom	🗎 a file for each file creation unit	🗎 a file for each file creation unit

Data Saved to Display and Event Data Files

The following data is saved to display and event data files.

Contents of the display data and event data files

- Header string (see section 1.10.1, “Setting the Save Directory, File Header, and File Name” in the User’s Manual)
- Batch information (when the batch function is in use, ▶ see section 1.11, “Setting the Batch Function” in the User’s Manual)
- Measured / computed data
- Setting parameters
- Login information (see section 1.1.4, “Terminology”)
- Event log (see section 1.5, “Audit Trail Function”)
- Alarm summary
- Approval information. (see section 1.6, “Signature Function”)

Save Destination

Files are saved to an SD memory card.

Data Save Destination Directory

You can specify the name of the directory that data will be saved to (the default directory is “DATA0”). The GX/GP will create the directory on the SD memory card and save data to it.
▶ For the setting procedure, see section 1.10, “Setting the Conditions for Saving Data Files” in the User’s Manual.

Note

Do not place a file with the same name as the directory name (“DATA0” by default) in the SD card.

Save Operation (When not using media FIFO)

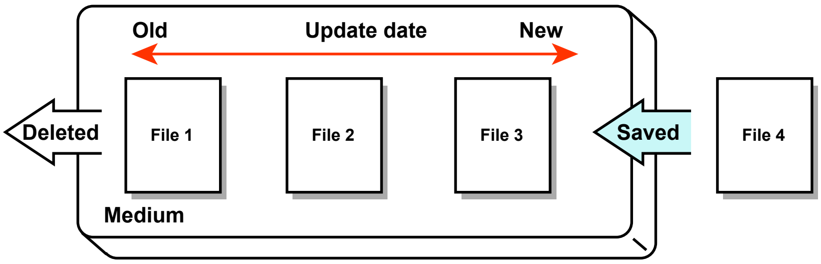
If there is not enough free space on the SD memory card, the GX/GP cannot save the data in the internal memory to the SD memory card. Replace the SD memory card before the data in the internal memory is overwritten.

Save Operation (Always retain most recent data file/media FIFO)

When saving the data files automatically, you can save the data so that the most recent data files are constantly retained in the SD memory card. This method allows you to use the GX/GP continuously without having to replace the SD memory card.

▶ For the setting procedure, see section 1.10, “Setting the Conditions for Saving Data Files” in the User’s Manual.

Operation



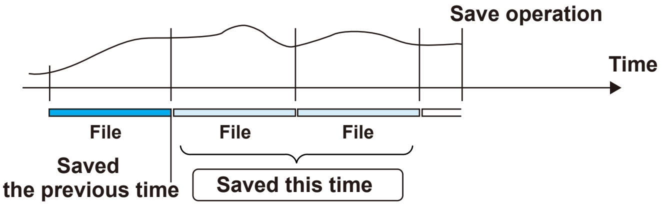
If not enough free space is available when saving a new data file to the SD memory card, files are deleted in order from the oldest data update date/time to save the new file. This operation is referred to as FIFO (first in first out).

- FIFO is used only when the following files are saved automatically. When files are saved using other methods, FIFO is not used.
  Display data files, event data files, report data files (/MT option), manual-sampled-data files, and snapshot data files.
- Files subject to deletion
  All files in the destination directory, except for the ones listed below, are subject to deletion. Files not subject to deletion:
  Hidden files, read-only files, files in the subdirectory within the save destination directory
- If the free space on the SD memory card would fall to less than 1 MB after the file is saved, the oldest files are deleted in order from the save destination directory before the file is saved. The GX/GP ensures that at least 1 MB of free space is available after a file is saved.
- Up to the most recent 1000 files are retained. If the number of files in the save destination directory exceeds 1000, the number of files is held at 1000 by deleting old files even if there is enough free space.
- If there are more than 1000 files already in the save destination directory, at least one file is always deleted before saving the new file. The number of files is not kept within 1000 in this case.

Manual Save (Collectively Storing Unsaved Data)

Unsaved data in the internal memory is stored in unit of files to the external storage medium (SD memory card or USB flash memory) when an external storage medium is inserted and a given operation is carried out.

▶ For instructions on how to save data manually, see section 2.5.2, “Manually Saving Measured Data (Collectively saving unsaved data)” in the User’s Manual.



Note

When you use manual save, it is important that you save the data in the internal memory to the external storage medium before the data is overwritten. Determine the usage condition of the internal memory and save the data to the external storage medium at appropriate times.

▶ For the setting procedure, see section 1.10, “Setting the Conditions for Saving Data Files” in the User’s Manual.

▶ For operating instructions, see section 2.1, “Starting and Stopping Recording and Computation” in the User’s Manual.

Data Saved to Display and Event Data Files

The same as for auto save.

Save Destination

You can select an SD memory card or USB flash memory (/UH option).

Data Save Destination Directory

You can specify the name of the directory that data will be saved to (the default directory is “DATA0”).

▶ For the setting procedure, see section 1.10, “Setting the Conditions for Saving Data Files” in the User’s Manual.

File Name

You can select what type of file name to use to save measured data to an SD memory card. The following three types are available.

Structure	Data Type	Description
Date	Display data Event data Manual sampled data Snapshot data Alarm summary data	7-digit Specified string Date . Extension **Example: 000123_AAAAAAAAAAA121231_174633.GSD**
	Report data (/MT option)	7-digit Specified string Date Type . Extension **Example: 000123_AAAAAAAAAAA121231_174633HD.GRE**
7-digit	Display data Event data Manual sampled data Snapshot data Alarm summary data	7-digit Specified string . Extension **Example: 000123_AAAAAAAAAAA.GSD**
	Report data	7-digit Specified string Type . Extension **Example: 000123_AAAAAAAAAAAHD.GRE**
Batch name	Display data Event data	7-digit Batch name . Extension **Example: 000123_BBBBBBBBBBBBBBBBBBBBBBBBBB.GSD**
	Report data	7-digit Date Type . Extension **Example: 000123_121231_174633HD.GRE**
	Manual sampled data Snapshot data Alarm summary data	7-digit Date . Extension **Example: 000123_121231_174633.GMN**

Item	Description	
7-digit	**Consists of** 6-digit number + 1-character delimiter	
	6-digit number*	A sequence number in chronological order. The number ranges from 000001 to 999999. If the number reaches 999999, it returns to 000000.
	1-character delimiter	Starts with '_' and takes on the following values: A to Z and 0 to 9. If a file with the same name exists in the specified directory, the file is saved by changing the delimiter to prevent overwriting. Example: Example: If a file named “000123_AAAAAAAAAAA.GSD” already exists, the file is saved to the name “000123AAAAAAAAAAAA.GSD.”
Date	YYMMDD_hhmmss	**YY: Year (lower two digits), MM: Month, DD: Day** **hh: Hour, mm: Minute, ss: Second**
Specified string	AAAAAAAAAAAAA	**Up to 16 alphanumeric characters can be used.**
Batch name	BBBBBBBBBBBB•••B	**Up to 41 alphanumeric characters can be used.**
Type	H_, D_, W_, M_, HD, DW, DM, B_, C_	**Report data type** **H_: Hourly, D_: Daily, W_: Weekly, M_: Monthly, HD: Hourly and daily, DW: Daily and weekly, DM: Daily and monthly, B_: Batch, C_: Daily custom**
Extension	Display data : GSD Event data : GSE Manual sampled data : GMN Alarm summary data : GAL Snapshot data : png	Report data : GRE Report data : xlsx or xlsm (report template function) Report data : pdf (report template function)

* When the multi-batch function (/BT option) is in use, the file name is batch group identifier + number + delimiter. For details, see the multi-batch function manual.

▶ For information about snapshot data, see page 1-16.

Saving Data through Touch Operation

You can carry out the following data save operations regardless of whether auto save or manual save is used.

▶ For operating instructions, see section 2.3.3, "Displaying a List of Data Files in the Internal Memory (Memory summary)" in the User's Manual.

Saving Alarm Summary Data

▶ For operating instructions, see section 2.3.1, "Listing the Log of Alarm Occurrences and Releases (Alarm Summary)" in the User's Manual.

Data Save Operation (applicable icon)	Description
Collectively save (All save)	Collectively saves all the data stored in the internal memory.
Collectively save display data and event data (Disp/Event save)	Collectively saves display data and event data stored in the internal memory.
Selectively save data (Selective data save)	Saves the specified display data or event data file.
Collectively save manual sampled data (Msample data save)	Collectively saves all the manual sampled data stored in the internal memory.
Collectively save report data (/MT option) (Report data save)	Collectively saves all the report data stored in the internal memory.
Alarm save	Saves the alarm summary data.

Save Destination

You can select an SD memory card or USB flash memory (/UH option).

Data Save Destination Directory

A directory is created with a name that is a combination of the data save destination directory name and the date/time, and the data is saved there.

Directory name: "Specified string"_YYMMDD_HHMMSS

Example: If a file is saved on September 30, 2014 at 17:06:42, the file will be saved to a directory with the name DATA0_140930_170642. "DATA0" is the specified string.

Note

The number of directories that you can create on the external storage medium varies depending on the length of the directory names. When the specified directory name is 5 characters long, about 170 directories can be created. When it is 20 characters long, about 120 directories can be created. An error occurs if you try to create directories exceeding this limit.

1.2.9 Other Types of Data That Can Be Stored

Setting Parameters When the Settings Are Changed

▶ For a description of the function, see section 1.5.

Setting parameters

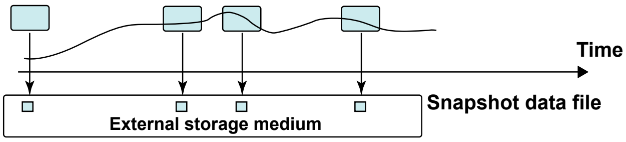
You can save the GX/GP setting parameters to an SD memory card or to USB flash memory (/UH option). The setting parameters is saved to the root directory.

Name of the setting file	Specified string .GSL **Example: ABCD10005.GSL**

▶ For operating instructions, see section 1.21, "Loading Settings," and section 1.22, "Saving Settings" in the User's Manual.

Snapshot Data

You can save images of the GX/GP screen in PNG format to an SD memory card or to USB flash memory (/UH option). It is saved in the same directory as display and event data. For file names, see the earlier description.



▶ For operating instructions, see section 2.5.4, "Saving and Printing Screen Image Data (Snapshot)" in the User's Manual.

1.2.10 Saving Data through an Ethernet Network

You can use the FTP client function to automatically transfer and save the following data to an FTP server through an Ethernet network: display data, event data, report data (/MT option), snapshot data (screen image data), setup data when the settings are changed.
You can also use the GX/GP as an FTP server. You can access the GX/GP from a personal computer and retrieve and store data files from both internal and external memory.
▶ For the setting procedure, see section 1.17.2, "Setting the FTP Client Function" in the User's Manual.
▶ For operating instructions, see section 3.3, "Accessing the Measurement Data File on the GX/GP from a PC (FTP server function)" in the User's Manual.

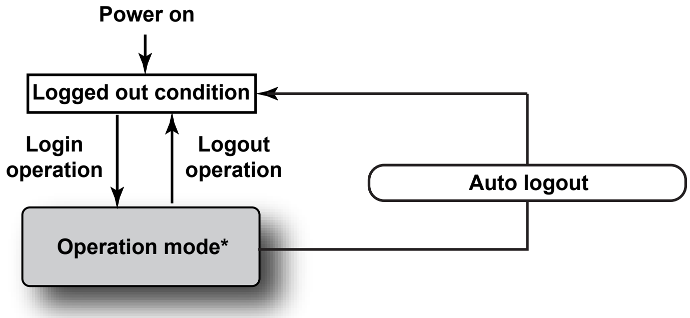
1.3 Login Function

You can allow only registered users to use the GX/GP.
▶ For the setting procedure, section 2.2.
▶ For operating instructions, section 2.3.

1.3.1 Logging In and Out Using Touch Operation

You need to enter user identification information (a user name, user ID (when in use), and password) to log in to the GX/GP in the following cases.

GX/GP Access Method	Login Necessary
Touch operation	When the power is turned on
	When logging in after logging out.



* This is the normal mode in which configuration and operation are performed.

Auto Logout

You can set the GX/GP to log a user out automatically when there is no touch operation over a specified period.
In the case of general communication using Ethernet, use the timeout function.
▶ See section 1.17.7, “Configuring the Server Function” in the User’s Manual.
In the case of general communication using serial communication, use the logout function.
▶ See section 1.18.1, “Setting Basic Communication Conditions” in the User’s Manual.

Operations Available While Logged Out

You can configure the GX/GP so that when you are logged out, in addition to just being able to log in, you can switch the screen using the Browse tab of the menu screen or from the favorite screen list.

1.3.2 Logging In and Out through Communication

You need to log in as a registered user in the following cases.
▶For details about logging in through communication, see the Communication Command Manual.

GX/GP Access Method	Function Accessed	Login
Ethernet	Setting and measurement server (General communication)	To send commands, you need to log in by entering user identification information (a user name, user ID (when in use), and password). There is a special command for logging out.
	Web application	To monitor the GX/GP, you need to log in by entering user identification information (a user name and password). Only Monitor level users can log in. To log out, close the Web page.
Serial	Setting and measurement function (General communication)	To send commands, you need to log in by entering user identification information (a user name, user ID (when in use), and password). There is a special command for logging out.

1.3.3 User Levels

There are three user levels: Administrator, User, and Monitor user.
Number of users that can be registered: 100

User Level		Description
Administrator	Admin	An administrator has access to all operations.
User	User	A user cannot access security settings. Nor can a user perform A/D calibration, enable the advanced security function, configure the encryption function or create keys for encryption/certificate, or upload I/O module firmware. You cannot set the multi batch function on or off or load settings that include the multi batch function on/off setting. You can specify the range of operations that a user can perform.
Monitor user	Monitor	A monitor user can only use the monitor function. The user cannot configure or operate the GX/GP.

Administrator

Item	Description	
Login methods	Touch operation	Users can log in using touch operation.
	Communication	Users can log in using general purpose communication (Ethernet or serial communication).
	Touch operation + Communication	Users can log in using touch operation and general purpose communication (Ethernet or serial communication).
Identification information	User name	Up to 20 characters and symbols
	User ID*	Up to 20 characters and symbols
	Password*	Between 6 and 20 characters and symbols
	Password expiration	Select one month, three months, or six months.

* Characters that cannot be used in passwords and user IDs: SP (space) ' ; DEL (7f)

Note

To use the login function, at least one administrator who can log in to the GX/GP using touch operation must be registered.
The user level of the user registered at User number 1 is fixed to **Admin**. You cannot change it.

User

Administrators register users.

Item	Description	
Login methods	Touch operation	Users can log in using touch operation. See “User Privileges.”
	Communication	Users can log in using general purpose communication (Ethernet or serial communication). See “User Privileges.”
	Touch operation + Communication	Users can log in using touch operation and general purpose communication (Ethernet or serial communication). See “User Privileges.”
Identification information	The same as for administrators.	

Monitor User

Administrators register Monitor users.

Item	Description	
Login methods	Touch operation	Users can log in using touch operation. Only monitoring is possible. The user cannot configure or operate the GX/GP except for changing the password.
	Communication	Users can log in through the FTP server or Web application. Only monitoring is possible. The user cannot configure or operate the GX/GP except for changing the password.
	Touch operation + Communication	Users can log in using touch operation and through the FTP server or Web application.
Identification information	User name	Up to 20 characters and symbols
	User ID*	Up to 20 characters and symbols
	Password*	Between 6 and 20 characters and symbols

* Characters that cannot be used in passwords and user IDs: SP (space) ' ; DEL (7f)

User Privileges (User Property)

The following operations can be enabled or disabled for each user. Operations performed using communication commands are included.
Up to 10 types of user privileges can be assigned to User level users.

Setup Item	Operation
Record	Start and stop recording (including the START/STOP key)
Math	Start, stop, reset computation (including the START/STOP key), and acknowledge data dropout
Data save	Save display data, save event data, manual sample, snapshot, reset timer, reset match time timer
Message	Write messages
Batch	Enter the batch name number, lot number, comment, and text field
Alarm ACK	Alarm acknowledge (including individual alarm ACK)
Communication	Start, stop, and test mail; test FTP, get and release network information; test printer output; test KDC; manually recover Modbus master; manually recover Modbus client ; and manually recover SLMP
Touch operation	Touch operation
Time set	Manual SNTP server time adjustment and date/time adjustment.
Setting operations	All setting operations
External media	Save, load, and list files; manually save data; save alarms; abort saving; create certificate signature requests (CSR); install certificates; install intermediate certificates; and save manually
System operations	Initialize, reconfigure system, use encryption/certificate, execute unverified certificate, and activate module
Output operations	Operate internal switches of type Manual and operate the relays of range type Manual.
Calibration correction	Configure calibration correction, Calibration reminder settings (/AH option).

* Release number 2 (version 2.02) and later

Signature Privileges (Sign In Property)

The following operations can be enabled or disabled for each user. Operations performed using communication commands are included.
Up to 8 types of signature privileges can be assigned to User level users.

Setup Item	Operation
Sign in 1 to Sign in 3	Signature operations

Explanation of User Privileges (User Property)

- Operations performed using communication commands are also limited. However, operations can always be performed through Modbus communication, regardless of the settings. ▶ section 2.2 in the Communication Command Manual
- Operations assigned by the event action function are always performed, regardless of the operation-restriction settings. If the event is a “User Function Key,” the operation will be restricted.
- If you lock computation, even if the starting and resetting of computation are enabled for the START/STOP key operation, computation will not be reset or started when recording starts.

User ID

You can choose whether or not to use a user ID.

User ID and Password

You cannot specify a user-ID and password pair that is already registered on the GX/GP.

Password Expiration

You can set a password expiration period (but not for Monitor users).

Number of Password Retries and User Invalidation

When a user is prompted for a password, if he or she enters the wrong password for the specified number of times (Password retry), the user’s account is invalidated, and the user cannot log in (Monitor users are not affected). An administrator can clear the “user locked” status by setting the invalidated user’s password to the default password.

Reusing Setting Parameters

You can use the settings of one GX/GP on another GX/GP by loading the setting file.
You can specify whether to load all settings or specific settings (security, IP address, or other).
However, the passwords are not loaded except for Monitor users. All administrator and user passwords are set to their defaults.
▶ For operating instructions, see section 1.21.1, “Loading Setting Parameters” in the User’s Manual.

The following tables show the settings that can be loaded for different user levels when the user is logged in depending on the recording status (recording or recording stopped).

Recording

User Level		**Admin**	**User**	**Login Function Not Used**
Setup Item	Security	✓		✓
	IP address			
	Other*	✓	✓	✓

* Only settings that can be changed during recording

Recording stopped

User Level		**Admin**	**User**	**Login Function Not Used**
Setup Item	Security	✓		✓
	IP address	✓	✓	✓
	Other	✓	✓	✓

Loading Setting Files Using Event Action

Security settings are not loaded.

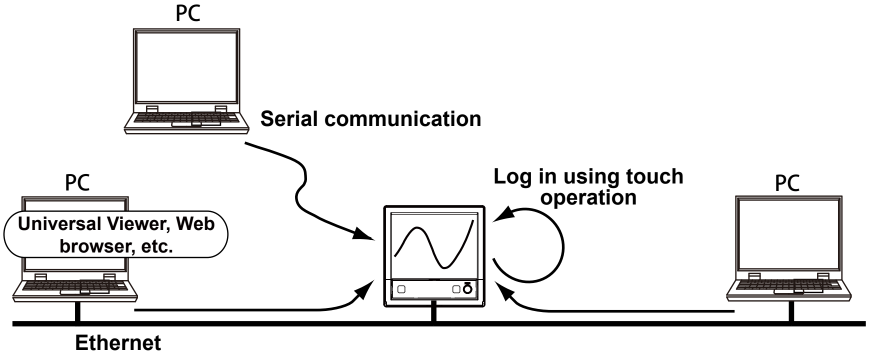
1.3.4 Login Restrictions

Logging In with the Same User Name

Simultaneous login is possible by the same user from multiple PCs.

Logging in Simultaneously

Multiple users can simultaneously log in to the GX/GP through touch operation and communication.


PC
Serial communication
PC
Universal Viewer, Web browser, etc.
Log in using touch operation
PC
Ethernet

Number of the simultaneous connection

Access Method	Number of Maximum Connection
General communication	4
Web application	4

When Not Using Communication Login

The following table shows the available operations through communication depending on the touch-operation security settings.

Access Method	Touch-Operation Security Settings	
	Off	Login
Using general communication (Ethernet or serial communication)	No login. All operations available.	No login. Monitor function only.
Web application	No login. Monitor function only.	No login. Monitor function only.
FTP server		

1.3.5 How the GX/GP Operates When the Login Function Is Not Used

The GX/GP operates in the following manner when the login function is not used.

- There is no need to log in.
- The signature function is not available.
- You can connect and execute commands using general communication (Ethernet or serial communication) in the same way as on a standard model.
- Only the monitor function is available over a Web application connection.

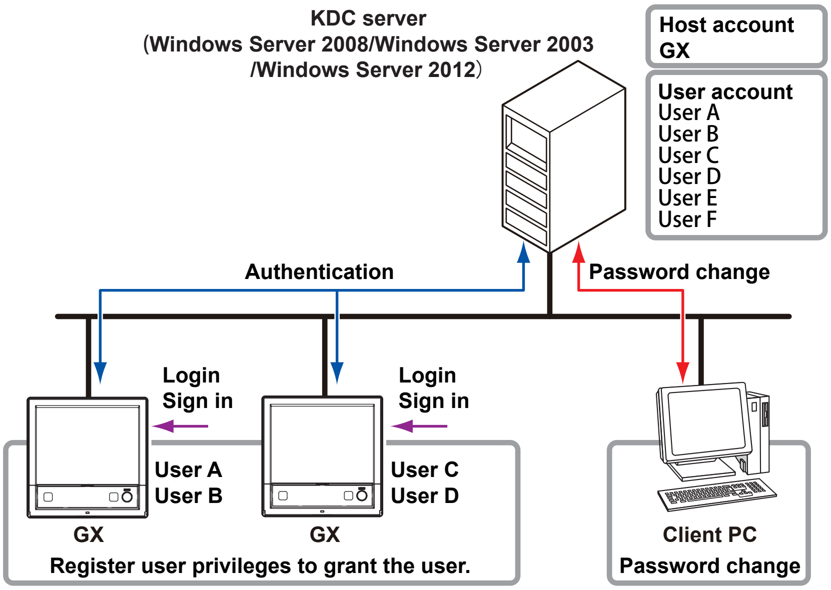
1.4 Password Management

The password management function enables you to manage access to the GX/GP by using the Kerberos v5 authentication protocol.

▶ For the setting procedure and operating instructions, see section Chapter 3, “Password Management”.

System Configuration

The following figure shows the configuration of the authentication system.



The authentication system consists of the devices listed below connected on an Ethernet.

- KDC server
  Windows Server 2008, Windows Server 2003, or Windows Server 2012. Manages the account of a GX/GP on the network (host account) and the user accounts for accessing the GX/GP.
- GX/GP
  Of the user accounts on the KDC server, you can specify which accounts to use (login settings) on which GX/GPs. You can also set different user privileges for each user on each GX/GP.
- Client PC for maintenance
  This device is used to change user account passwords and for other maintenance. It is not explained in this manual.

Operation

When you log in to the GX/GP or use the signature function, you will be prompted for a user name and password (the password management function does not use user IDs). The GX/GP will then perform the communication with the KDC server that is necessary for authentication. When authentication completes successfully, you can operate the GX/GP.

The server manages the passwords and their expiration period. Monitor users (Monitor level users) are excluded from this function.

If the connection to the KDC server is broken, or if no users can be authenticated for some other reason, you can operate the GX/GP using a special user account (root).

▶ See Note in section 3.2.1, “Logging In and Out”.

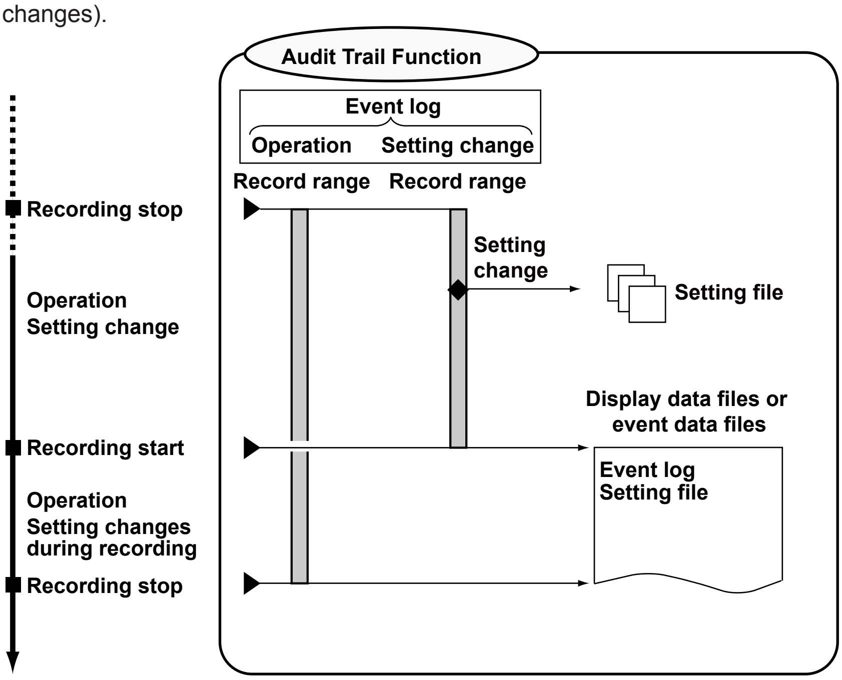
Note

- Cross-realm authentication (authentication of different domain names) is not supported.
- You cannot change user account passwords from the GX/GP.

1.5 Audit Trail Function

The audit trail function records histories of operations. It saves event logs and also setup files when the settings change. You do not need to perform any special settings to use this function.

The figure below indicates what items are recorded to the event log (operations and setting changes).



1.5.1 Information That Is Saved to Measurement Data Files

When measurement data files (display data or event data files) are saved, in addition to the measured data, a setup file and event log are also saved.

Setting File

A file that contains the settings that were in use when recording started. If the settings are changed during recording, you can view the changes in the event log.

Event Log

A history of operations and setting changes.
The event log is saved in the measurement data file.

Login Information

Information about the users who can operate the GX/GP.

1.5.2 Event Log

The event log records operations and setting changes on the GX/GP in chronological order. The event log is saved in the measurement data file.

▶ For information about the display, see section 2.5.

▶ Description: section Appendix 1

Recorded Operations

- Operations that affect the measured data, such as record start and message writing, are recorded. Error messages are also recorded.
- Touch operations and START/STOP key operations, communication operations, remote-control operations, event-action operations, and automatic GX/GP operations (e.g., error messages) can be distinguished from each other.
- Operations that do not affect the measured data, such as screen switching and display configuration changes, are not recorded.
  ▶ For details, see section Appendix 1.

How the Event Log Is Saved

- The GX/GP can record up to 3000 operations and setting changes (log entries) in its internal memory. When the number of log entries exceeds 3000, the oldest log entries are overwritten.
- The log of events that occurred since the previous record stop to the current record stop is stored in the measurement data file (display or event data file). If the measurement data file is divided, each time a file is created, the event log up to that point is saved in the file.

Viewing the Event Log

- You can display the event logs in the internal memory on the GX/GP screen.
  The GX/GP can display only the most recent 2000 events from a given event log.
- You can view event logs in measurement data files on the GX/GP screen or Universal Viewer (standard software).

How to Clear the Event Log

- The event logs in the internal memory are cleared if you execute Initialize all. However, you cannot execute initialization (clearing event logs) while recording is in progress.
- You cannot clear the event log in a measurement data file.

1.5.3 Login Information

A user’s password may change during operation. The login information is the user name, user ID (when in use), and the password at the time that the measurement data file was created. To sign a measurement data file using the standard software (Universal Viewer), you must log in as a user that is registered in the login information in that file. You cannot view the login information.

▶ For information about the display, see the Universal Viewer Manual.

1.5.4 Event Log and Setting File When Recording Is Not in Progress

When you change the settings, the changes are logged in the event log. At the same time, a setting file is saved to the SET0 directory (fixed) on the SD memory card.

▶ For information about the display, see section 2.5.

Note

- Make sure that the SD memory card is inserted when you change the settings. If the GX/GP is unable to save a setting file, it will display an error message, and you will not be able to finish changing the settings.
- Do not place a file named “SET0” in the SD card.

Logged Operations

Changes to the settings are logged. Setting file loading and setting initialization are also logged.

How Setting Files Are Saved

- A setting file is saved to the SD memory card when the settings are changed. If an SD memory card is not inserted at such an instant, an error occurs.
- The directory “SET0” is automatically created on the SD memory card, and a setting file (.GSL extension) is saved in the directory.
- The file name is generated automatically.

Structure
7-digit Date, time . Extension
Example: 000123_131231_174633.GSL

Item	Description	
7-digit	**Consists of** 6-digit number + 1-character delimiter	
	6-digit number	A sequence number in chronological order. The number ranges from 000001 to 999999. If the number reaches 999999, it returns to 000000.
	1-character delimiter	Starts with '_' and takes on the following values: A to Z and 0 to 9. If a file with the same name exists in the specified directory, the file is saved by changing the delimiter to prevent overwriting. Example: If a file named “000123_131231_174633.GSL” already exists, the file is saved to the name “000123A131231_174633.GSL.”
Date	YYMMDD_hhmmss	**YY: Year (lower two digits), MM: Month, DD: Day** **hh: Hour, mm: Minute, ss: Second**
Extension	GSL	

Viewing a Setting File

You can use the standard software (Universal Viewer) to view the setting file contents that correspond to the relevant event log.

▶ For operating instructions, see the Universal Viewer Manual.

How the Event Log Is Saved

▶ See section 1.5.2, “Event Log”.

1.5.5 Event Log and Setting File When Recording Is in Progress

The setting changes are recorded in the event log. You can configure the GX/GP to automatically write into the measured data a message indicating that the settings have changed. The GX/GP does not save a setting file.

▶ For the setting procedure, see section 1.7.4, “Setting Trend Display Conditions,” in the User’s Manual.

Logged Operations (Settings that can be changed during recording)

The following setting changes can be logged during recording.
However, the following limitations apply.

- The maximum number of settings that can be changed simultaneously is 100.
  If this limit is exceeded, the setting changes cannot be saved.
  If this limit is exceeded, you can either cancel the setting changes or stop recording to apply the setting changes. Save the setting changes before the number of changed settings exceeds 100.
- You cannot set multiple consecutive channels. (Only the first channel will be selected.)

Setup Item	
Alarm settings	On/Off
	Type
	Value
	Hysteresis
	Logging
	Output type
	Output No.
	Alarm delay
Calibration correction	Mode: Linearizer Approximation/Linearizer/ Correction factor *2
	Number of set points
	Input value (1 to 12)
	Output value (1 to 12)
	Uncorrected value (1 to 12)*1 *2
	Instrument correction factor (1 to 12)*1 *2
	Sensor correction factor (1 to 12)*1 *2
Data save settings	Save directory
Communication (Ethernet) settings	Recipient 1
	Recipient 2
	Sender
	Subject
User settings	User level
	Mode
	User name
	User ID
	Password
	Password expiration
	User property On/Off
	Authority number
	Sign in property On/Off
	Authority of sign in
Calibration reminder settings*2	On/Off
	Due date
	Daily reminder
	Re-notification cycle
	Buzzer
	Calibration correction setting
	Title
	Notification message 1
	Notification message 2

*1 When the mode is set to correction factor.
*2 To use the correction factor, the aerospace heat treatment (/AH option) must be installed in the GX/GP.

Writing Change Messages

You can configure the GX/GP so that a message is written automatically when any of the following settings are changed during recording.

Setup Item		Message
Alarm	On/Off	Alarm settings
	Type	
	Value	
	Hysteresis	
	Logging	
	Output type	
	Output No.	
Alarm delay	Alarm delay (hour/minute/second)	Alarm delay setting
Calibration correction	Mode	Calibration correction setting
	Number of set points	
	Input value (1 to 12)	
	Output value (1 to 12)	
	Uncorrected value (1 to 12)*	
	Instrument correction factor (1 to 12)*	
	Sensor correction factor (1 to 12)*	

* When the mode is set to correction factor. To use the correction factor, the aerospace heat treatment (/AH option) must be installed in the GX/GP.

To do so, in **Display settings**, under **Trend settings**, you need to set **Message**’s **Change message** to **On**.

▶ For the setting procedure, see section 1.7.4, “Setting Trend Display Conditions,” in the User’s Manual.

Setting Changes during Recording

You can change the following settings and perform the following file operations during recording. Administrators can perform all operations. Users can only perform operations that have been permitted. The setting menu that appears varies depending on the operations that can be performed.

Setting Changes

See section 1.5.5, “Event Log and Setting File When Recording Is in Progress” (described earlier).

File Operations

The file operations that you can perform during recording are shown below.

Load/Save Function	
Load display data	
Load event data	
Load settings	Setting parameters (only those that can be changed during recording)
	Scale image
	Report templates (when the /MT computation option is installed)
	Load trusted certificates (when the encryption function is enabled)
	Custom display (when the /CG custom display option is installed)
Save settings	Setting parameters (only those that can be changed during recording)
	Scale image
	Report templates (when the /MT computation option is installed)
	Trusted certificates (when the encryption function is enabled)
	Custom display (when the /CG custom display option is installed)
File list	

1.5.6 SET0 Directory Operations

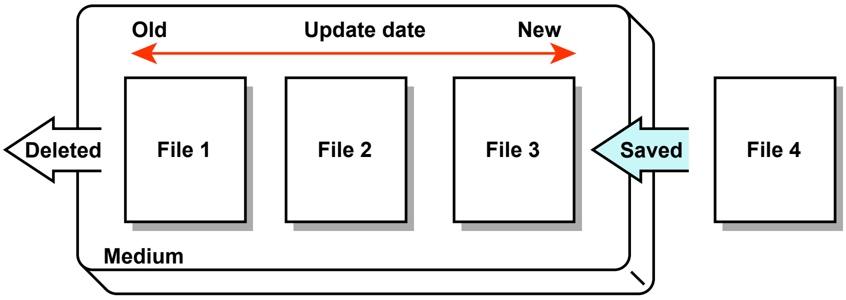
Save Operation (When not using media FIFO)

If there is not enough free space on the SD memory card, the GX/GP cannot save the setting parameters in the internal memory to the SD memory card. When this happens, an error occurs, and the setting parameters cannot be changed. Use another SD memory card to save the data.

Save Operation (Always retain most recent data file/media FIFO)

The newest setting files can always be saved on the SD memory card. This method allows you to use the GX/GP continuously without having to replace the SD memory card.
▶ For the setting procedure, see section 1.10.2, "Setting the Save Method to Media (Auto save or manual save) and Media FIFO," in the User's Manual.

- **Operation**



If there is not enough space to save a new file, the GX/GP deletes the oldest files and then saves the new file. This operation is referred to as FIFO (first in first out).

- FIFO is used only when the following files are saved automatically. When files are saved using other methods, FIFO is not used.
  Setting File
- Files subject to deletion
  All files in the destination directory, except for the ones listed below, are subject to deletion. Files not subject to deletion:
  Hidden files, read-only files, files in the subdirectory within the save destination directory
- Up to the most recent 100 files are retained. If the number of files in the save destination directory exceeds 100, the number of files is held at 100 by deleting old files even if there is enough free space.
- If there are more than 100 files already in the save destination directory, one or more files are always deleted before saving the new file. The number of files does not remain at or below 100 in this case.

1.6 Signature Function

Signing is the act of attaching the following approval information to a measurement data file.

- Pass or fail judgment
- Comment
- Name of the user who attached the information and time when the information was attached

▶ For the setting procedure, see section 2.2.
▶ For operating instructions, see section 2.4.

1.6.1 Signable Files

Display and event data files (.GSD and .GSE extensions) can be signed.

Two Sign In Type

Set the sign in type to choose what types of measurement data files can be signed.

Sign In Type	Signable Data	
	When signing from the GX/GP	When signing from Universal Viewer
Batch	When the measured data from the start to stop of recording is contained in a single file.	When all the measurement data files from the start to stop of a recording are present. You can specify one file or multiple files.
Continuous	Each measurement data file.	Each measurement data file.

The “continuous” process type is useful when you are dealing with a continuously operating process, such as the monitoring of the air conditioning temperature. You can sign each measurement data file.
On the other hand, the “batch” process type is useful when you are dealing with a process such as one in which recording starts and stops in accordance with production. You cannot sign a unit of data unless all the files from the start to the stop of the recording are present.
On the GX/GP, data files whose Sign in type is set to Batch and are divided from the start to stop of recording cannot be signed.
Such files need to be signed using the standard software (Universal Viewer).

1.6.2 Signature Privileges and Signatures

Users and Signature Privileges

- You can attach three signatures (Sign in 1, Sign in 2, and Sign in 3), each with different privileges, to a single display or event data file. For example, you could reserve Sign in 1 for the operator, Sign in 2 for the quality control supervisor, and Sign in 3 for the general supervisor.
- An administrator can attach signatures with any privilege.
- A user can only attach a signature that they have been given permission to attach.
- A signature with the same privilege can only be attached once. You cannot overwrite a signature.

Deleting and Changing Approval Information

You cannot delete or change the approval information that has been attached to a file.

1.6.3 Signing from the GX/GP

From the GX/GP, you can only sign measurement data files in the internal memory.

- You can show display or event data on the signature screen (historical trend screen) and sign it.
- You can configure the settings so that the signature screen (historical trend screen) appears automatically when recording stops.
- Viewing the data
  When you sign a file, you can view the following information from the signature screen (historical trend screen).
  - Measured value
  - Data information (information about the displayed measurement data file)
  - Event log (a history of the operations)
  - Alarm summary
  - Message summary

1.6.4 Signing Using the Standard PC Software (Universal Viewer)

You can sign measurement data files using Universal Viewer. A measurement data file can only be signed by a user with signature privileges who is registered in the login information of that measurement data file.

▶ For operating instructions, see the Universal Viewer Manual.

1.7 Unique Specifications of GX/GP with Advanced Security

1.7.1 Functions That Differ from Those of GX/GPs without Advanced Security or GX/GPs Whose Advanced Security Is Disabled

The main functions that have not been explained thus far in this manual that differ with the functions of GX/GPs without advanced security or GX/GPs whose advanced security is disabled are explained in the table below.

Item	Specification for GX/GPs with Advanced Security	Reference
Recording of display and event data	Display and event data cannot be recorded simultaneously.	For the setting procedure, see section 1.9 in the User’s Manual.
Event data modes	You can only record event data at all times (free mode).	For the setting procedure, see section 1.9 in the User’s Manual.
Event action function	Action cannot be set to Event trigger.	For the setting procedure, see section 1.15 in the User’s Manual.
Operation lock function	Not available	—
Setting changes during recording	There are limitations on the settings that you can change during recording.	For an explanation, see section section 1.5.5.
Automatic writing of messages when the settings are changed during recording	You can automatically write a message when the settings are changed during recording.	For the setting procedure, see section 1.7.4 in the User’s Manual.
Data file format	Binary format only. The data is encrypted.	
Operations performed on external storage media	Formatting and file deletion cannot be performed.	—
Loading of setting files	When you load a setting file onto the GX/GP from an external storage medium, the settings that can be loaded vary depending on the user level and recording status.	For the operating procedure, see section 1.21 in the User’s Manual.
Web application	Monitor function only. The user cannot configure or operate the GX/GP.	—

1.7.2 Functions That Differ from Those of the DX1000/DX1000N/DX2000

The main differences between the GX/GP advanced security function and the DX1000/DX1000N/DX2000 advanced security function are explained in the table below.

Item	Specification for DXs with Advanced Security	Specification for GX/GPs with Advanced Security	Reference
Setting modes	There are two modes: *Setting mode*, which is a mode for configuring settings, such as the input range and the measurement method, and *Basic setting mode*, which is a mode for configuring basic settings, such as the scan interval and the measured data save method.	There is no distinctions by modes.	—
Number of failed password entry attempts	You can select the number of failed password entry attempts that will result in a user being invalidated.	Same as the DX.	For the setting procedure, see section 2.2.
Signature privilege settings	You can give or deny a user signature privileges for each signature level (Sign in 1, 2, and 3).	Same as the DX.	For the setting procedure, see section 2.2.
Multi login	You can log in simultaneously through key operations and communication.	Same as the DX.	
Selecting a user name when logging in	When user IDs are being used, you can select the user name from a list when you log in (you do not have to enter the user name directly).	Same as the DX.	For operating instructions, see section 2.3.
KDC server password management	You can manage user accounts and passwords from a KDC server on the network.	Same as the DX.	For the setting procedure and operating instructions, see Chapter 3.
Signature function	You can only sign files in the internal memory. You cannot sign files that have been loaded from the external memory.	Same as the DX.	For operating instructions, see section 2.4.
	You can sign files from the historical trend display.	You can sign files from the signature screen (historical trend screen).	For operating instructions, see section 2.4.
Saving files	If the same file already exists in the save destination, it is overwritten.	Same as the DX.	For an explanation, see section 1.1.
Settings that can be changed during recording	Alarm settings can be changed during recording.	Same as the DX.	For an explanation, see section 1.5.5.
Logging of setting changes during recording	Setting changes are recorded in the operation log.	Setting changes are recorded in the event log.	For an explanation, see section 1.5.
Alarm ACK	You can perform the alarm acknowledge operation using the FUNC key.	You can perform the alarm acknowledge operation by touching the screen.	For the operating procedure, see section 2.4 in the User's Manual.
Alarm delay time	Can be set to up to 24 hours.	Same as the DX.	For the setting procedure, see sections 1.2, 1.3, and 1.5 in the User's Manual.
Batch text fields	You can enter a text field at the start of recording.	Same as the DX.	For the operating procedure, see section 1.11 in the User's Manual.
Alarm ACK summary	There is no alarm acknowledge summary. Alarm acknowledge operations are recorded in the alarm summary and the operation log.	There is no alarm acknowledge summary. Alarm acknowledge operations are recorded in the event log and alarm summary.	
The "batch" process type (sign in type)	You can freely select the display-data file-save interval or the event-data data length from the listed options.	Same as the DX.	For the setting procedure, see section 2.2.

1.8 Advanced Security Limitations

If you install the /AS option and enable advanced security, the following limitations are applied to the standard functions.

Item	When Advanced Security Is Disabled	When Advanced Security Is Enabled
Number of user registrations	50	100
Number of event logs	50	3000
Touch-operation security	Off, Login, Operation Lock	Off, Login
File type	Display data, event data, display data + event data	Display data, event data
Event data recording modes	Free, Single, Repeat	Free
Data save settings, file format	Binary, Text	Binary
Event action setting > Action	Event trigger action available	Event trigger action not available
Delete files on the external storage medium (SD memory card or USB memory card)	Yes	No
Format the external storage medium (SD memory card or USB memory card).	Yes	No
Web application	Monitor, configure, operate	Monitor
FTP server feature	Output the external storage medium list	Output the external storage medium list
	Transfer files stored in the external storage medium	Transfer files stored in the external storage medium
	Write files to the external storage medium	—
	Delete files stored on the external storage medium	—
	Output the internal memory list	Output the internal memory list
	Transfer files stored in the internal memory	Transfer files stored in the internal memory
Load setting parameters	Load passwords of registered users	Cannot load passwords of registered users

Blank

2.1 Enabling the Advanced Security Function

You can enable and disable the advanced security function as you like. If you disable the advanced security function, the functions that you can use on the GX/GP are the same as those of the standard product.
If you change the advanced security settings, all data including recorded data will be initialized, and the GX/GP will restart.
You can set a password on the advanced security settings so that they cannot be changed without permission (only for operations performed from the GX/GP).

Data Subject to Initialization

- **All internal data**
- **All setting parameters including security settings (Contents*1 of certificates are excluded)**
- **System configuration data*2**

*1 Loading certificates or installing certificates/intermediate certificates
*2 You must reconfigure the system.

Path

GX/GP: **MENU** key > **Browse** tab > **Init/Calib** > Setting menu **Advanced security settings**
Hardware configurator: **System** tab > System config > **Option detail**

Description

Password settings

Setup Item	Selectable Range or Options	Default Value
On/Off	Off/On	Off
Password	Character string (up to 16 characters, Aa#1)	—

On/Off

Set this to **On** to set a password on the advanced security settings.
If you set the password setting to On, the next time you want to change the advanced security settings, you will be prompted to enter the password.

Password

Set the password for the advanced security settings.
Characters that cannot be used in passwords: SP (space) ' ; DEL (7f)

Note

Be careful not to forget the password. If you do, you will not be able to change the advanced security settings.
Default password: default

Advanced security function

Setup Item	Selectable Range or Options	Default Value
On/Off	Off/On	On

On/Off

Set this to **On** to enable the advanced security function.
If you change this setting, all data including recorded data will be initialized, and the GX/GP will restart.

Execute

Enables the advanced security function
Tapping **Execute** displays a confirmation screen. If you tap **OK**, the GX/GP will restart, and the advanced security function will be enabled.
You cannot change the advanced security settings during recording or computation.

2.2 Registering Users and Setting the Signature Method

Procedure for Configuring the Login and Signature Features for the First Time

When the advanced security function is enabled, the GX/GP is configured so that you can operate it without logging in. First, register an administrator. After you register an administrator, a user, or a monitor user, you will have to log in before you can use the GX/GP.

▶ For an explanation of this function, see section 1.3, "Login Function" and section 1.6, "Signature Function".

2.2.1 Configuring the Security Function, Logout, Password Management Function, Etc.

Path

GX/GP: **MENU** key > **Browse** tab > **Setting** > Setting menu **Security settings** > **Basic settings**

Hardware configurator: **Security settings** > **Security basic settings**

Description

Security function

Setup Item	Selectable Range or Options	Default Value
Touch operation	Off, Login	Off
Communication	Off, Login	Off

Touch operation

Set the type of touch screen security to apply.

Options	Description
Off	Disables the security function
Login	Enables the login function

Communication

To apply communication access security, set this to **Login**.

Options	Description
Off	Disables the security function
Login	Allows only registered users to access the GX/GP via communication

Note

If Touch operation is set to Login, configure User settings and User property and then save the settings. If you save immediately after setting Login, you will exit from the setup menu and be logged out. You must log in to configure User settings and User property.

Logout*

Setup Item	Selectable Range or Options	Default Value
Auto logout	Off/1min/2min/5min/10min	Off
Operation without Login	Off/On	Off

* Appears when Touch operation in Security settings is set to Login.

Auto logout

Options	Description
Off	Stays logged in until the user logs out.
1min to 10min	When you log in through touch operation, you will be automatically logged out when there is no activity for the specified duration.

This does not work for FTP server or Web application.
Use Timeout function to set the auto logout for Ethernet communication .

▶ See section 1.17.7, "Configuring the Server Function" in the User's Manual.

Operation without Login

Set the operations that users can carry out without being logged in.

Options	Description
Off	Allows only login operation.
On	Allows login operation and switching the operation screen

Password management

Setup Item	Selectable Range or Options	Default Value
On/Off	Off/On	Off
Root user password	Character string (between 6 and 20 characters, Aa#1)	root123

On/Off

To perform password management using a KDC server on the Ethernet, select **On**.

Options	Description
Off	Disables KDC server password management
On	Enables KDC server password management

If you change the password management on/off setting, the user ID enable/disable setting is changed to Off. Also, the user IDs and passwords of all users will be initialized.

Before setting password management to On, we recommend that you perform a KDC server connection test to verify that a connection can be established with the KDC server.

▶ See section 3.1.3, “Testing the KDC Server Connection”.

Note

Before setting password management to On, configure User settings, User property, and KDC client.

If you set password management to On, configure User settings, User property, and KDC client, and then save the settings. If you save immediately after specifying On, you will exit from the setup menu and be logged out. You need to perform authentication with the KDC server to configure User settings and User property.

Root user password

Set the password of the root user (this user name is fixed to “root”).
The default password is “root123.”

The root user is an emergency user account that you can use when users cannot log in to the GX/GP, such as when the KDC server is inaccessible.

Password retry

Setup Item	Selectable Range or Options	Default Value
Password retry	Off, 3 times, 5 times	3 times

Password retry

Set a total number of failed password-entry attempts that results in user invalidation.

Options	Description
3, 5	Three or five failed password entry attempts result in user invalidation.
Off	Users are never invalidated, no matter how many times they enter the wrong password.

Note

If you set the password retry, be careful not to forget the password or mistype the password repetitively causing the user to be invalidated (user lock out).

User ID

Setup Item	Selectable Range or Options	Default Value
On/Off	Off/On	On

On/Off

Set whether to use user IDs for user registration.

Options	Description
Off	User IDs are not used to register users.
On	User IDs are used to register users.

If you change the user ID enable/disable setting, the user IDs and passwords of all users will be initialized.

Note

Users whose user settings have changed are automatically logged out.

2.2.2 Registering Users

Path

GX/GP: **MENU** key > **Browse** tab > **Setting** > Setting menu **Security settings** > **User settings***
Hardware configurator: **Security settings** > **User settings***

* Appears when, in Basic settings, Touch operation or Communication of the security function is set to Login

Description

Setup Item	Selectable Range or Options	Default Value
User No.	1 to 100	Off

User No.

Select the user number to register.

User settings

Setup Item	Selectable Range or Options	Default Value
User level	Off/Admin/User/Monitor	Off
Mode	Touch operation, Communication, Touch operation + Communication	Touch operation + Communication
User name	Character string (between 1 to 20 characters, Aa#1)	—
User ID*5	Character string (up to 20 characters, Aa#1)	—
Initialize password	Back, Initialize password	—
Password expiration*2	Off, 1 month, 3 month, 6 month	Off
User property*1	Off/On	Off
Authority number*3	1 to 10	1
Sign in property*1	Off/On	Off
Authority of sign in*4	1 to 8	1

*1 Appears when the user level is set to User.
*2 Does not appear when the user level is set to Monitor.
*3 Appears when the User property is set to On.
*4 Appears when the Sign in property is set to On.
*5 Does not appear when the user ID is disabled.

When password management is enabled, the user settings vary depending on the user level as shown below.

User level	Admin	User	Monitor
Setup Item	User No.	User No.	User No.
	User level	User level	User level
	Mode	Mode	Mode
	User name	User name	User name
		User property	Initialize password
		Authority number	
		Sign in property	
		Authority of sign in	

User level

Set the user level.
The user level of User number 1 is fixed to Admin.

Options	Description
Admin	The system administrator. An administrator has access to all operations.
User	A common user. A user cannot access security settings. Nor can a user perform A/D calibration, enable the advanced security function, set encryption, encryption of certificate, or key creation, or upload I/O module firmware. Limitations can be applied to the operations that a user can perform.
Monitor	A type of user that has access only to the monitor function. A monitor user can only change the password; the user cannot change settings or operate the GX/GP.

Note

We recommend that you register several administrators.
If there is only a single administrator and this administrator becomes locked as a result of forgetting the password or entering the password multiple times, there will be no way of unlocking the user.

Mode

Options	Description
Touch operation	You can log in to the GX/GP through touch operation.
Communication*	You can log in to the GX/GP via communication.
Touch operation + Communication	You can log in to the GX/GP through touch operation and communication.

* Communication cannot be specified for user number 1.

User name

Set the user name. Duplicate user names are not allowed.
User names cannot contain spaces. User names cannot be set to “PowerUser” or “root.”

User ID

Set the user ID. You cannot set the user ID if password management is enabled.
User IDs cannot contain spaces.

Initialize password

Select **Initialize password** to initialize a password. To cancel the initialization, select **Back**.
▶ For the default value, see section 2.3.1, “Logging In”.

Note

The password is set the first time you log in.

Password expiration

Options	Description
Off	The password will not expire.
1 month, 3 month, 6 month	The GX/GP will prompt the user to change the password after the specified period of time passes.

This item cannot be set when:

- Password management is enabled.
- When the user level is Monitor.

User property

Set this to **On** to restrict the functions that users can use.

Authority number

Select the authority number to apply restrictions to functions.
▶For details on how to set the user property, see section 2.2.3, “Setting User Properties”.

Sign in property

Set this to **On** to restrict the sign in level that a user can use to sign at.

Authority of sign in

Set the authority of sign in to restrict the signature.
▶For details on how to set the “Sign in property,” see section 2.2.5, “Setting Signature Restrictions”.

2.2.3 Setting User Properties

Path

GX/GP: **MENU** key > **Browse** tab > **Setting** > Setting menu **Security settings** > **User property***
Hardware configurator: **Security settings** > **User property***

* Appears when, in Basic settings, Touch operation or Communication of the security function is set to Login

Description

Setup Item	Selectable Range or Options	Default Value
Authority number	1 to 10	Off

Authority number

Select the authority number to apply user restrictions.

User property

Setup Item	Selectable Range or Options	Default Value
Record	Free/Lock	Free
Math	Free/Lock	Free
Data save	Free/Lock	Free
Message	Free/Lock	Free
Batch	Free/Lock	Free
AlarmACK	Free/Lock	Free
Communication	Free/Lock	Free
Touch operation	Free/Lock	Free
Time set	Free/Lock	Free
Setting operation	Free/Lock	Free
External media	Free/Lock	Free
System operation	Free/Lock	Free
Output operation	Free/Lock	Free
Calibration correction	Free/Lock	Free

* Release number 2 (version 2.02) and later

Record

Set this to **Lock** to restrict record start/stop operation.
This also applies to the corresponding operation using **START/STOP** key.

Math

Set this to **Lock** to restrict the math operations below.
This also applies to the corresponding operations using the **START/STOP** key.

Operation
Math start
Math stop
Math reset
Math ACK

Data save

Set this to **Lock** to restrict the data save operations below.

Operation
Save display data
Save event data
Manual sample
Snapshot
Timer reset
Match time timer reset

Message

Set this to **Lock** to restrict message writing operation.

Batch

Set this to **Lock** to restrict the batch operations below.

Operation
Write batch numbers
Write lot numbers
Write comments
Write in text fields

AlarmACK

Set this to **Lock** to restrict alarm acknowledge operation (including individual alarm acknowledge operation).

Communication

Set this to **Lock** to restrict the communication operations below.

Operation
Start, stop, test E-Mail
FTP test
Obtain, release network Information
Printer output test
Manually recover Modbus master;
Manually recover Modbus client
Manually recover SLMP

Touch operation

Set this to **Lock** to restrict the touch operations below.

Operation
Register the standard display
Register favorites
Switch screen content
Switch the display rate
Manually recover Modbus master
Manually recover Modbus client

Time set

Set this to **Lock** to restrict manual SNTP server time adjustment and date/time adjustment.

Setting operation

Set this to **Lock** to restrict all setting operations.
However, even if Setting operation is set to Lock, if calibration correction is set to Free and an AI module is present, it will still be possible to set calibration correction and calibration reminder settings (/AH option) items.

External media

Set this to **Lock** to restrict the external media operations below.

Operation
Save and load files
Display a list of files
Manually save data
Manual save
Alarm save
Save stop
Create certificate signature request
Install certificate
Install intermediate certificates

System operation

Set this to **Lock** to restrict the system operations below.

Operation
Initialize
System reconfiguration
Encryption/Certificate
Execute unverified certificate
Activate module

Output operation

Set this to **Lock** to restrict the internal switch operations whose type is Manual and relay operations whose range type is Manual.

Calibration correction

Set this to **Lock** to restrict the calibration correction of AI channel settings and calibration reminder settings (/AH option).

2.2.4 Configuring the Sign in Settings

Path

GX/GP: **MENU** key > **Browse** tab > **Setting** > Setting menu **Security settings** > **Sign in settings**

Hardware configurator: **Security settings** > **Sign in settings***

* Appears when, in Basic settings, Touch operation or Communication of the security function is set to Login

Description

Sign in type

Setup Item	Selectable Range or Options	Default Value
Type	Batch, File	Batch

Type

Choose what types of measurement data files can be signed.

Options	Description
Batch	You can sign a collection of all the measurement data files from the start to stop of a recording. However, you can only sign a file from the GX/GP when the file covers the measured data of an entire recording, from start to stop.
File	You can sign each individual measurement data file.

Recording stop action

Setup Item	Selectable Range or Options	Default Value
Sign in	Off/On	Off

Sign in

Set this to **On** to display a signature screen (historical trend screen) for signing in when recording is stopped through touch operation or the **START/STOP** key.
However, the following conditions apply.

- When the data file contains all the data from record start to record end
- When Sign in type is set to Batch
- When the user that stopped recording is allowed to sign
- When the screen is not displaying Setting, Save load, or Init/Calib.

Options	Description
On	The signature screen (historical trend display) appears automatically when recording is stopped.
Off	The screen does not change when recording is stopped.

Note

When the multi-batch function (/BT option) is enabled, the signature screen (historical trend display) does not appear automatically when recording is stopped in batch overview mode.

Data file transfer

Setup Item	Selectable Range or Options	Default Value
FTP transfer timing	Sign in, Data save	Data save

FTP transfer timing

Set whether to transfer data files via FTP when files are signed or when data is saved. The FTP client function must be configured for the FTP transfer to work.
▶ For the setting procedure, see section 1.17.2, “Setting the FTP Client Function.” in the User’s Manual

Options	Description
Sign in	Data files are transferred to the FTP server only when they are signed. Display data and event data are not transferred to the FTP server when data is saved. Other types of data are transferred. Also, the Transfer wait time settings are invalid; transfer is executed immediately.
Data save	Data files are transferred to the FTP server when the data is saved. The files are not transferred when they are signed.

Sign in title*

Setup Item	Selectable Range or Options	Default Value
Sign in 1	Character string (up to 16 characters, Aa#1)	Signature1
Sign in 2		Signature2
Sign in 3		Signature3

Sign in 1 to 3

You can set titles for Sign in 1 to 3.

2.2.5 Setting Signature Restrictions

Path

GX/GP: **MENU** key > **Browse** tab > **Setting** > Setting menu **Security settings** > **Sign in property***
Hardware configurator: **Security settings** > **Sign in property***

* Appears when, in Basic settings, Touch operation or Communication of the security function is set to Login

Description

Setup Item	Selectable Range or Options	Default Value
Authority of sign in	1 to 8	1

Authority of sign in

Select the authority of sign in to restrict the signature.

Sign in property*

Setup Item	Selectable Range or Options	Default Value
Sign in 1	Free/Lock	Free
Sign in 2	Free/Lock	Free
Sign in 3	Free/Lock	Free

Sign in 1 to 3

For Sign in 1 to 3, you can choose whether or not to give users signature privileges.

Options	Description
Free	The operation is enabled.
Lock	The operation is disabled.

2.2.6 Comment Input Function for Setting Changes

You can enter comments to setting files that are saved when settings are changed.

Path

GX/GP: **MENU** key > **Browse** tab > **Setting** > Setting menu **System settings** > **Setting file**
Hardware configurator: **System settings** > **Setting file**

Description

Setup Item	Selectable Range or Options	Default Value
Setting file comment	Character string (up to 50 characters, Aa#1)	—

Setting file comment

Set the comment to attach to the setup file.

Configuration changes comment

Setup Item	Selectable Range or Options	Default Value
Input comment	Off/On	Off

Input comment

Set this to **On** to enter comments in setting files when settings are changed.

Tapping **Save** displays a screen for setting and saving a comment.
The comment that you enter is set in Setting file comment.

2.2.7 Activating Modules (for module swapping)

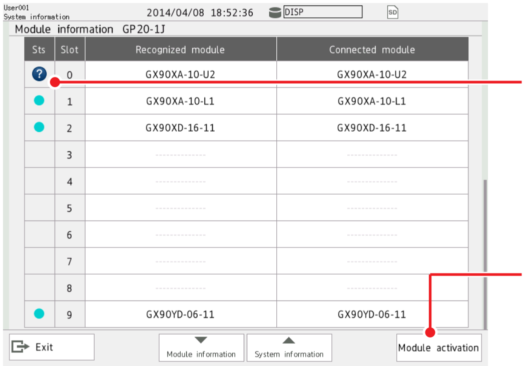
If you replace a module with another module (same type) after system reconfiguration, you need to activate the module or else the measured data will result in errors. If the identified module is different from the actual module, you can activate the module from the System information screen.

Only administrators and users with system operation privileges can perform this operation.

Procedure

1. Press **MENU**.
   The menu screen appears.

2. Tap the **Browse** tab and then **System information**.
   The system information screen appears.



User001
System information

2014/04/08 18:52:36 DISP

Module information GP20-1J

Sts	Slot	Recognized module	Connected module
?	0	GX90XA-10-U2	GX90XA-10-U2
●	1	GX90XA-10-L1	GX90XA-10-L1
●	2	GX90XD-16-11	GX90XD-16-11
	3	-------------	-------------
	4	-------------	-------------
	5	-------------	-------------
	6	-------------	-------------
	7	-------------	-------------
	8	-------------	-------------
●	9	GX90YD-06-11	GX90YD-06-11

Icon that indicates that the module needs to be activated

Module Activation
This becomes available when the module needs to be activated.

3. Tap **Activate module**.
   The module will be activated.

Operation complete

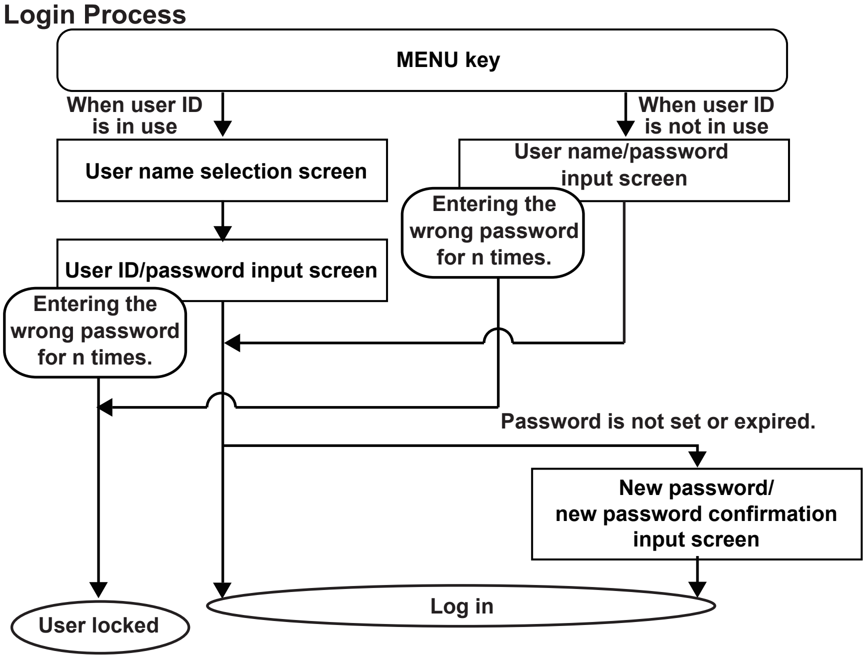
Note

Be sure to turn off the power when removing or inserting modules. Removing or inserting modules with the power turned on may lead to malfunction.

2.3 Logging In and Out

When you log in for the first time, you will be prompted to change the password.
▶For information about the function, see section 1.3, “Login Function”.

Login Process


MENU key
When user ID is in use
When user ID is not in use
User name selection screen
User name/password input screen
Entering the wrong password for n times.
User ID/password input screen
Entering the wrong password for n times.
Password is not set or expired.
New password/ new password confirmation input screen
User locked
Log in

2.3.1 Logging In

Procedure

Logging In for the First Time (logging in before the password has been set)

1. Press **MENU**.
   If the GX/GP is configured to use user IDs, a screen for selecting the user name opens.
   If the GX/GP is configured to not use user IDs, a login screen (for entering the user name and password) appears.
   Proceed to step 3.

2. Tap a user name.
   A login screen (for entering the user ID and password) appears.

3. If the GX/GP is configured to use user IDs, set the user ID and default password, and tap **OK**.

   If the GX/GP is configured to not use user IDs, set the user name and default password, and tap **OK**.
   A screen with the default password appears.

User No.	Default User Name	Default User ID	Default Password
1	User001	Blank (no setting)	User001
2	User002	Blank (no setting)	User002
:	:	:	:
100	User100	Blank (no setting)	User100

4. Set a new password in New Password and New Password Again, and then tap **OK**.
   You will be logged in.

Note

- You cannot use the same combination of user ID and password as another user.
- Enter the password using 6 to 20 characters, A a # 1 .
- You cannot use a character string that contains the following characters: SP (space) ' ; DEL (7f)
- You cannot specify the same password as the current password.

Operation complete

When a Password Has Been Set

1. Press **MENU**.
If the GX/GP is configured to use user IDs, a screen for selecting the user name opens.
If the GX/GP is configured to not use user IDs, a login screen (for entering the user name and password) appears.
Proceed to step 3.

2. Tap a user name.
A login screen (for entering the user ID and password) appears.

3. If the GX/GP is configured to use user IDs, set the user ID and password, and tap **OK**.

If the GX/GP is configured to not use user IDs, set the user name and password, and tap **OK**.
You will be logged in.

Operation complete

When the Password Is Expired

A password expiration screen appears. Change the password (between 6 to 20 characters, A a # 1). You will be logged in.

Changing the Password (voluntary change)

After logging in, perform the procedure below.

1. Press **MENU**.
The menu screen appears.

2. Tap the **Universal** tab and then **Password change**.
The screen for changing the password appears.

3. Enter the appropriate values in Old Password, New Password, and New Password Again, and tap **OK**.
The password will be changed.

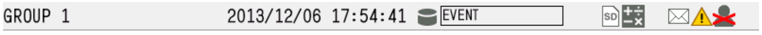
Operation complete

Note

- If a password is set successfully, the password expiration will be updated.
- If password management is enabled, the screen for changing the password does not appear.

User Invalidation (User lock out) and Handling

If a user enters the wrong password for the specified number of times (Password retry), that user is invalidated and can no longer log in. The user-locked icon appears in the status area. To restore the user, you need to perform User Locked ACK and clear the invalid user. Only administrators can perform these operations.



Note

If all the registered administrators are invalidated, administrators will no longer be able to log in (registered users can still log in).

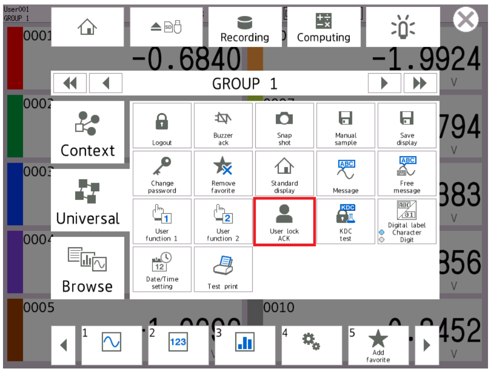
Icon that appears when all administrators have been invalidated:	☒

Be sure to manage the passwords to prevent this from happening. If you become unable to log in as an administrator, contact your nearest Yokogawa dealer.

Clearing the User-Locked Icon (Only administrators can perform this operation)

1. Log in as an administrator.

2. Press **MENU**, and tap the **Universal** tab and then **User Locked ACK**.
   The user-locked icon is cleared.



Operation complete

Note

The User-locked ACK icon appears when a user is invalidated, and an administrator logs in to the GX/GP.
If the Touch operation of the security function is set to Off, the User-locked ACK icon appears without logging in when a user is invalidated.

Releasing the Invalid User Status and Logging in as an Invalidated User

1. An administrator has to initialize the invalidated user's password to its default.
   ▶For the setting procedure, see section 2.2.2, "Registering Users".

2. The invalidated user must then follow the procedure under "Logging In for the First Time (logging in before the password has been set)" to log in.

Operation complete

Notification When a User Lock Out Condition Occurs

E-mail Notification

An e-mail notification can be sent when a user lock out condition occurs.
The following settings are necessary:

- SMTP client settings
- E-mail settings

▶ For the setting procedure, see section 1.17.3, “Configuring the SMTP Client Function,” and section 1.17.4, “Setting E-mail Transmission Conditions (When the SMTP client function is on),” in the User’s Manual.
For details on e-mail contents, see section 3.2.5, “E-mail Format,” in the User’s Manual.

DO Output

A signal can be output from a DO channel using the event action function when a user lock out condition occurs.
The following settings are necessary:

- DO channel range type
- Event action function

▶ For the setting procedure, see section 1.5, “Configuring DO Channels (Digital output channels)” in the User’s Manual.
▶ For the setting procedure, see section 1.15, “Setting the Event Action Function” in the User’s Manual.

Setting example: Output to DO channel 0201

DO channel (0201) setting

- Range
  Type: Manual

Event action settings

- Event action number: 1
- Event action
  On/Off: On
- Event
  Type: Status
  Event details: User lock out
  Operation mode: Rising / Falling edge
- Action
  Type: DO On/Off
  NO: 0201

Status Output

A signal can be output from a DO channel using the event action function to indicate whether there are users that are logged in.
The following settings are necessary:
- DO channel range setting
- Event action function

▶ For the setting procedure, see section 1.5, "Configuring DO Channels (Digital output channels)" in the User's Manual.
▶ For the setting procedure, see section 1.15, "Setting the Event Action Function" in the User's Manual.

Setting example: Output to DO channel 0202

DO channel (0202) setting

- Range
  Type: Manual

Event action settings

- Event action number: 2
- Event action
  On/Off: On
- Event
  Type: Status
  Event details: Under login
  Operation mode: Rising / Falling edge
- Action
  Type: DO On/Off
  NO: 0202

Logging in to A/D Calibration Mode

To switch to A/D calibration mode, the logged-in user must be authenticated.
There is no password protection for A/D calibration.

1. Press **MENU**.
   The menu screen appears.

2. Tap the **Browse** tab, **Init/Calib**, and on the menu **A/D calibration** > **Execute**.
   The user authentication screen appears.

3. Enter the user name or user ID (when in use) of the logged-in user, and tap **OK**.
   A screen appears for you to confirm the switch to A/D calibration mode.

4. Tap **OK**.
   The GX/GP restarts and enters A/D calibration mode.

Operation complete

▶ For instructions on how to use A/D calibration mode, start reading from step 4 in section 5.1.3, "Performing A/D Calibration and Adjusting the Input Accuracy," in the User's Manual.

Password Expiration

See the earlier description.

Logging in to the Web Application

When you access the Web application, a login window appears.
Log in by entering the user name and password.
Even when password management is enabled, log in by entering the user name and password.
Only the users whose LoginSet settings are set as follows can log in to the Web application.

Item	Description
User level	Monitor
Mode	Touch operation + Communication or Communication

Logging into the FTP Server

Only the users whose LoginSet settings are set as follows can log in to the FTP server.

Item	Description
User level	Monitor
Mode	Touch operation + Communication or Communication

Alarm Confirmation When Recording is Stopped

If there are alarms that have not been acknowledged when recording is stopped using touch operation or the **START/STOP** key, an alarm confirmation warning message appears. Tapping the Close icon for the warning message will clear the message, and you will be able to stop recording.

The warning message that appears when the **START/STOP** key is used appears only when the Confirmation screen under Record confirmation action is set to On.▶ See section 1.9.1, “Setting the Type of Data to Record (Display or event data) and Recording Conditions,” in the User’s Manual.
A warning message does not appear if recording is stopped by means other than touch operation or the **START/STOP** key.

2.3.2 Logging Out

Logging Out Using Touch Operation

1. Press **MENU**.
   The menu screen appears.

2. Tap **Universal** and then **Logout**.
   You will be logged out.

Operation complete

Auto Logout

When auto logout is enabled, users are logged out automatically if there are no touch operations for the specified period of time.

Other Methods of Logging Out

Item	Logout
Web application	Close the browser.
FTP server	Disconnect the FTP client connection.
General communication (Ethernet or serial communication)	Execute the logout communication command (Clogout).

2.4 Signing Display and Event Data

You can sign display and event data from the signature screen (historical trend display).

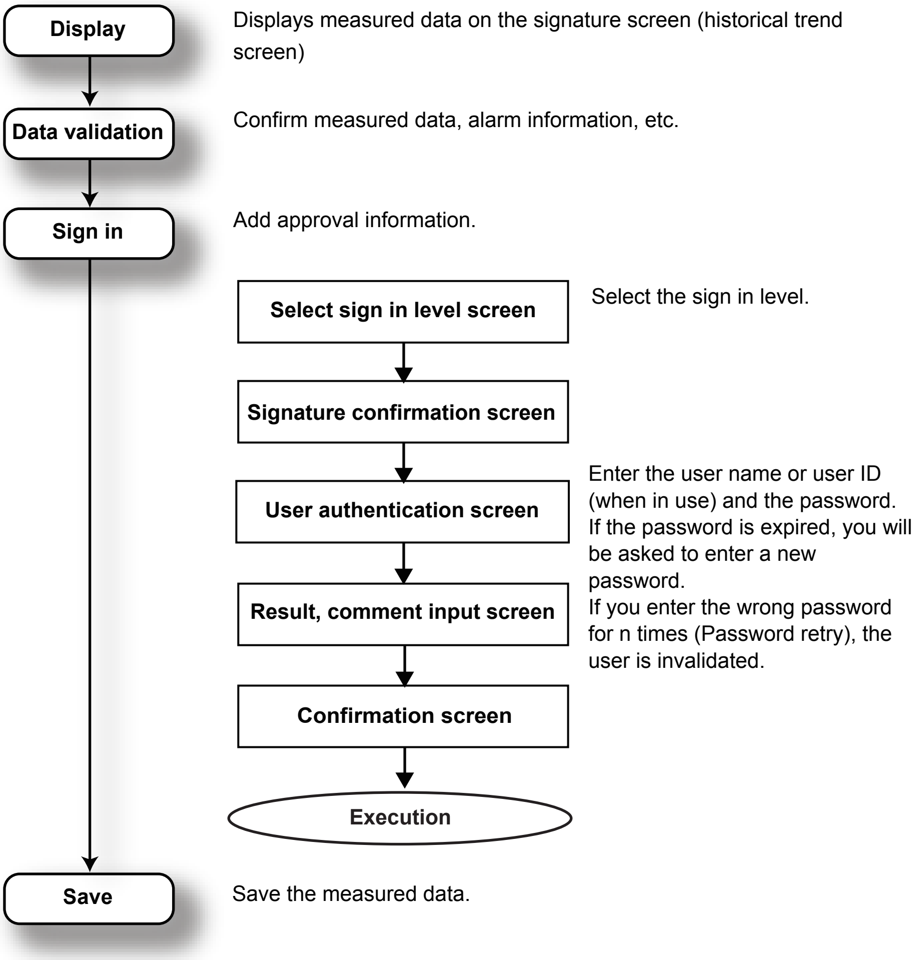
You can sign a unit of data when:

- You are logged in as a user with signature privileges.
- The files are in the internal memory (even if the data is in the internal memory, you cannot sign it unless it has been saved to files).
- The data has not already been signed in the same place.
- All the data that you want to sign can be displayed.
  For example, the GX/GP can display up to 1000 alarms. You cannot sign a file that has more than 1000 alarms. In such a case, use the standard software (Universal Viewer) to sign.

Item	Condition
Alarm information	1000 or less
Event log information	2000 or less

- When Sign in type is set to Batch and the measured data from the start to stop of recording is contained in a single file. You cannot sign files that are divided from the start to stop of recording.

2.4.1 Signing Process


Display
Data validation
Sign in
Select sign in level screen
Signature confirmation screen
User authentication screen
Result, comment input screen
Confirmation screen
Execution
Save

Display: Displays measured data on the signature screen (historical trend screen)

Data validation: Confirm measured data, alarm information, etc.

Sign in: Add approval information.

Select sign in level screen: Select the sign in level.

User authentication screen: Enter the user name or user ID (when in use) and the password. If the password is expired, you will be asked to enter a new password. If you enter the wrong password for n times (Password retry), the user is invalidated.

Save: Save the measured data.

▶For information about the function, see section 1.6, “Signature Function”.

2.4.2 Signing In

Procedure

Showing the Signature Screen

1. Press **MENU**.
   The menu screen appears.

2. Tap the **Browse** tab and then **Memory summary/Data save**.
   The memory summary appears.

3. Tap the data you want to sign.
   The memory information screen appears.

4. Tap **Go to Sign in**. The signature screen (historical trend display) appears.
   Tap the Sign in information to display it.

Operation complete

Go to Sign in is not displayed

- Data not saved to a file yet
- When Sign in type is set to Batch and the measured data from the start to stop of recording is divided into files.

Automatically Showing the Signature Screen (historical trend screen) When Recording Is Stopped

When Sign in for Recording stop action is set to On, the signature screen (historical trend screen) will appear when recording is stopped if the conditions are met.

▶ For the setting procedure, section 2.2.4, “Configuring the Sign in Settings”.

Viewing Information

On the signature screen (historical trend screen), perform the procedure below.

1. Press **MENU**.
   The menu screen appears.

2. Tap the **Context** tab and then the information screen icon to display.
   The screen that you selected appears.
   - Alarm summary
   - Message summary
   - Event log
   - Data information

   ▶ For details on the displayed information, see section 2.3, “Displaying Various Types of Information,” in the User’s Manual.

Operation complete

Data Display Range on the Signature Screen

Only the recorded data in the selected data file is displayed.

Display Item	Display Range
Trend	Data in the data file
Alarm summary	The most recent 1000 data entries in the data file
Message summary	The most recent 450 data entries and 50 added entries in the data file
Event log	Contents of the event log

Signing Data (Attaching approval information)

On the signature screen (historical trend screen), perform the procedure below.

1. Press **MENU**.
   The menu screen appears.

2. Tap **Context** and then **Go to Sign in**.
   The Select sign in level screen appears.
   You can also use the shortcut that appears when you tap the screen to switch to the Select sign in level screen.

3. Tap a sign in level. A sign in confirmation screen will appear. Tap **Yes**.
   The user authentication screen appears.

4. Enter the user name or user ID (when in use) and the password, and tap **OK**.

Note

- If a user enters the wrong password for the specified number of times (Password retry), that user is invalidated and logged out. If this occurs, this user can no longer log in. The invalidated user must have an administrator reset their password to the default, and then the user must follow the procedure under “Logging In for the First Time (logging in before the password has been set)” in section 2.2, “Logging In and Out,” to set a new password.
- If the entered password is expired, a password change screen will appear.
  You will not be able to sign until you change the password.

5. Set the Sign in information (Result, Comment), and tap **OK**.
   The Confirm sign in screen appears.

   For the comment, enter up to 32 characters.

6. Tap **Execute**.
   The data is signed.

   Tap Exit on the menu screen to exit from the signature screen (historical trend screen).

Operation complete

Signature Data Written in Data Files

Item	Description
Result	Pass or fail judgment
Comment	Comment
User name	Name of the user that wrote the information
Signature time	Date and time when the information was written

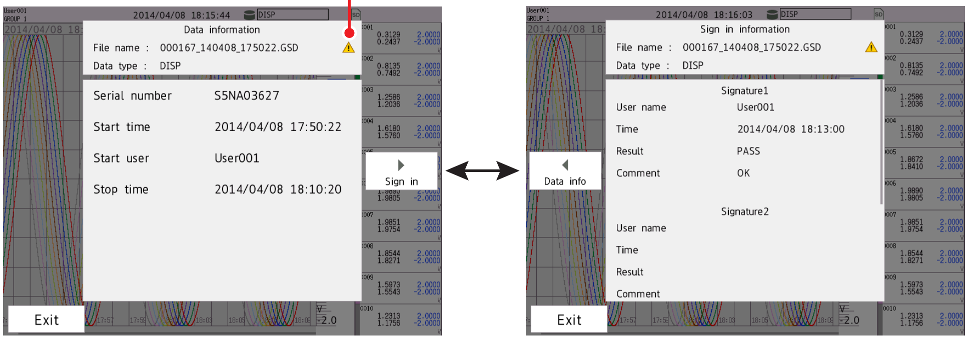
Note

Added messages cannot be written in signed data files.

Viewing Signature Information (Sign In Information)

You can view signature information in data files on the Data information screen.
You can verify whether the data file loaded into the GX/GP is abnormal (changed by some means). If the file condition is abnormal, an icon indicating this condition appears in the File name line on the Data information screen.
You can display data information from the following context menus.

Screen
Historical trend screen
Historical trend screen > Alarm summary
Historical trend screen > Message summary
Historical trend screen > Event log
Signature screen
Signature screen > Alarm summary
Signature screen > Message summary
Signature screen > Event log



Abnormal file icon

User001
GROUP 1
2014/04/08 18:15:44 DISP

Data information
File name : 000167_140408_175022.GSD ⚠
Data type : DISP

Serial number S5NA03627
Start time 2014/04/08 17:50:22
Start user User001
Stop time 2014/04/08 18:10:20

User001
GROUP 1
2014/04/08 18:16:03 DISP

Sign in information
File name : 000167_140408_175022.GSD ⚠
Data type : DISP

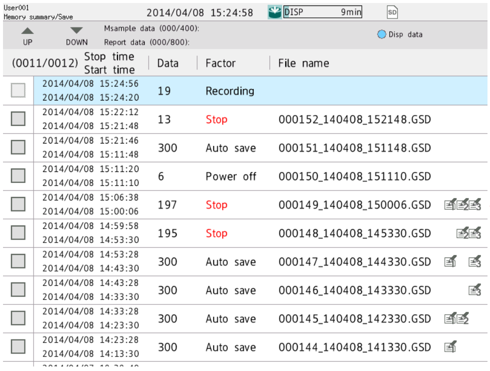
Signature1
User name User001
Time 2014/04/08 18:13:00
Result PASS
Comment OK

Signature2
User name
Time
Result
Comment

Sign in information

Viewing the Signature Status on the Memory Summary Screen

You can verify whether data files have been signed on the memory summary screen.
An icon indicating the signature status is displayed for each data file.



User001
Memory summary/Save
2014/04/08 15:24:58 DISP 9min

Msample data (000/400):
Report data (000/800):

(0011/0012)	Stop time Start time	Data	Factor	File name	
☐	2014/04/08 15:24:56 2014/04/08 15:24:20	19	Recording		
☐	2014/04/08 15:22:12 2014/04/08 15:21:48	13	Stop	000152_140408_152148.GSD	
☐	2014/04/08 15:21:46 2014/04/08 15:11:48	300	Auto save	000151_140408_151148.GSD	
☐	2014/04/08 15:11:20 2014/04/08 15:11:10	6	Power off	000150_140408_151110.GSD	
☐	2014/04/08 15:06:38 2014/04/08 15:00:06	197	Stop	000149_140408_150006.GSD	1 2 3
☐	2014/04/08 14:59:58 2014/04/08 14:53:30	195	Stop	000148_140408_145330.GSD	2 3
☐	2014/04/08 14:53:28 2014/04/08 14:43:30	300	Auto save	000147_140408_144330.GSD	1 3
☐	2014/04/08 14:43:28 2014/04/08 14:33:30	300	Auto save	000146_140408_143330.GSD	3
☐	2014/04/08 14:33:28 2014/04/08 14:23:30	300	Auto save	000145_140408_142330.GSD	1 2
☐	2014/04/08 14:23:28 2014/04/08 14:13:30	300	Auto save	000144_140408_141330.GSD	1

Signature status
(Sign in 1 to 3)

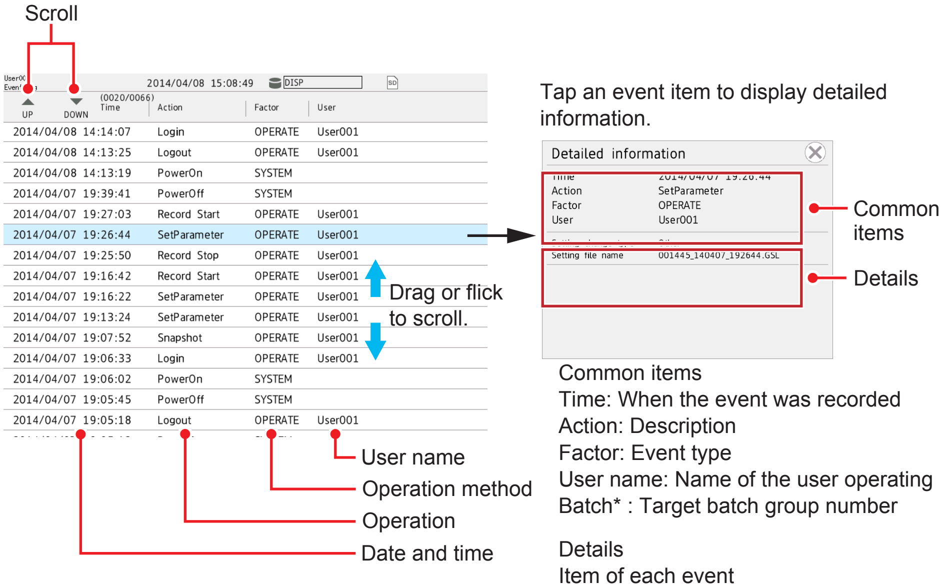
2.5 Viewing the Event Log

Procedure

1. Press **MENU**.
   The menu screen appears.

2. Tap the **Browse** tab and then **Log**.
   The log select screen appears.

3. Tap **Event**.
   The event log appears.
   Tap an entry to display detailed information.



User00
2014/04/08 15:08:49 DISP
(0020/0066)

Time	Action	Factor	User
2014/04/08 14:14:07	Login	OPERATE	User001
2014/04/08 14:13:25	Logout	OPERATE	User001
2014/04/08 14:13:19	PowerOn	SYSTEM	
2014/04/07 19:39:41	PowerOff	SYSTEM	
2014/04/07 19:27:03	Record Start	OPERATE	User001
2014/04/07 19:26:44	SetParameter	OPERATE	User001
2014/04/07 19:25:50	Record Stop	OPERATE	User001
2014/04/07 19:16:42	Record Start	OPERATE	User001
2014/04/07 19:16:22	SetParameter	OPERATE	User001
2014/04/07 19:13:24	SetParameter	OPERATE	User001
2014/04/07 19:07:52	Snapshot	OPERATE	User001
2014/04/07 19:06:33	Login	OPERATE	User001
2014/04/07 19:06:02	PowerOn	SYSTEM	
2014/04/07 19:05:45	PowerOff	SYSTEM	
2014/04/07 19:05:18	Logout	OPERATE	User001

Tap an event item to display detailed information.

Detailed information

Time	2014/04/07 19:26:44
Action	SetParameter
Factor	OPERATE
User	User001
Setting change type	Other
Setting file name	001445_140407_192644.GSL

Common items
Time: When the event was recorded
Action: Description
Factor: Event type
User name: Name of the user operating
Batch* : Target batch group number

Details
Item of each event
For details, see the event log list in appendix 1.

▶ For details on the event log, see section Appendix 1, "Event Log Contents".

* A Batch column is displayed when the multi batch function (/BT option) is enabled.

Operation complete

You can display event logs from the following context menus.

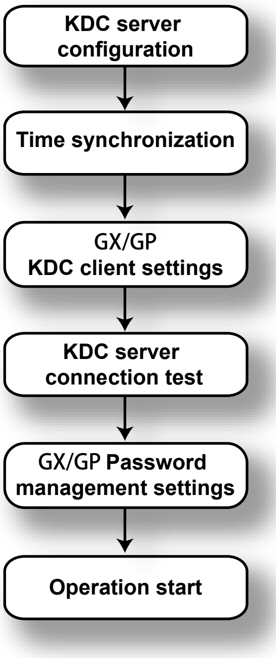
Screen	
Historical trend screen	Trend
	Alarm summary
	Message summary
Signature screen	Trend
	Alarm summary
	Message summary

Blank

3.1 Configuring the Password Management Function

Configuration Flowchart

To use the password management function, you must configure the KDC server and GX/GP. First configure the KDC server and then the GX/GP.


KDC server configuration
Time synchronization
GX/GP KDC client settings
KDC server connection test
GX/GP Password management settings
Operation start

Configure the KDC server.

Synchronize the GX/GP time to the KDC server time.

Configure the GX/GP KDC client settings.

Before setting password management to On, verify that a connection can be established with the KDC server.

Sets the password management function on the GX/GP.

See section 3.2, “Using the Password Management Function.”

Terminology

- KDC server (Key Distribution Center)
  Manages the GX/GP account (host account) and the user accounts for operating the GX/GP.
- Encryption type
  The type of encryption applied to the data for authentication.
- Authentication
  The task of verifying whether the user operating the GX/GP is valid.
- Host account
  The GX/GP user account on the KDC server.
- Host principal
  The name of the GX/GP on the application.
- User account
  The user account for operating the GX/GP.
- Mapping
  The association between the host principal and host account.
- Realm name
  The domain name that the KDC server and GX/GP belong to.

3.1.1 GX/GP KDC Client Settings

You need to specify the following GX/GP KDC client settings.

▶ For information about the function, see section 1.4, “Password Management”.

DNS settings

Configure the DNS settings if necessary.

▶ See section 1.17.1, “Setting Basic Communication Conditions,” in the User’s Manual.

SNTP client settings

For the password management function to work, the times on the KDC server and the GX/GP must be synchronized. Configure the SNTP client function so that synchronization is maintained using an SNTP server on the network.

▶ See section 1.17.5, “Setting the SNTP Client Function,” in the User’s Manual.

Note

- The password management function will not work if there is a difference of ±5 minutes or more between the GX/GP and the KDC server.
- Set the DST (daylight saving time) and time zone correctly. For the setting procedure, see sections 2.1 and 2.2, respectively, in the User’s Manual.

KDC client settings

Set the server information, the encryption type, etc. You can select the encryption type from AES128, AES256, and ARC4.

Path

GX/GP: **MENU** key > **Browse** tab > **Setting** > Setting menu **Communication (Ethernet) settings** > **KDC client settings**

Hardware configurator: **Communication (Ethernet) settings** > **KDC client settings**

Description

KDC connection Primary

Setup Item	Selectable Range or Options	Default Value
Server name	Character string (up to 64 characters, A a # 1)	—
Port number	Numeric value (1 to 65535)	88

Server name

Set the host name or IP address of the KDC server.

Port number

Set the port number.

KDC access point Secondary

Configure the secondary KDC server.

The settings are the same as those for “KDC connection Primary.”

Certification key

Setup Item	Selectable Range or Options	Default Value
Host principal	Character string (up to 20 characters, Aa#1)	—
Realm name	Character string (up to 64 characters, Aa#1)	—
Password	Character string (up to 20 characters, Aa#1)	—
Encryption type	ARC4, AES128, AES256	ARC4

Host principal

Set the name of the GX/GP that will be registered as a user of the KDC server.
You cannot use these characters: @/

Realm name

Set the realm name.
You cannot use these characters: @/

Password

Set the password of the GX/GP that will be registered as a user of the KDC server.

Encryption type

Set the same encryption as the server.

Note

- Host principal is converted in the GX/GP as follows:
  host/host principal@realm name
- Cross-realm authentication (authentication of different domain names) is not supported.
- ARC4 (ARCFOUR) is an encryption algorithm that is compatible with RC4.

3.1.2 GX/GP Password Management Settings

Password management, root user password

Enables the password management function. Set the password of the emergency root user.
▶ See section 2.2.1, “Configuring the Security Function, Logout, Password Management Function, Etc.”

User settings

Specify operation modes, user names, and restrictions for each user.
▶ See section 2.2.2, “Registering Users”.

3.1.3 Testing the KDC Server Connection

You can perform a KDC server connection test.
You can use this test when password management is set to Off.
Before setting password management to On, perform a KDC server connection test.

Procedure

1. Press **MENU**.
   The menu screen appears.

2. Tap the **Universal** tab and then **KDC test**.
   The KDC test screen appears.

3. Enter the user name and password, and then tap **OK**.
   The result of the connection test is displayed.

Operation complete

KDC Server Configuration Example

This section provides a KDC server configuration example. This example assumes that the KDC server is running on an English version of Windows Server 2008, and Active Directory is enabled.

Overview

The steps necessary in Active Directory of Windows Server 2008 are creating a host account, changing the properties, mapping*1 the host principal to the host account, and creating a keytab file (can be omitted). The following conditions will be used.

Item	Description
Domain name	The domain name that you are using
Realm	The realm name that you are using*2
Encryption type	AES256
Port number	88
Preauthentication	Enabled

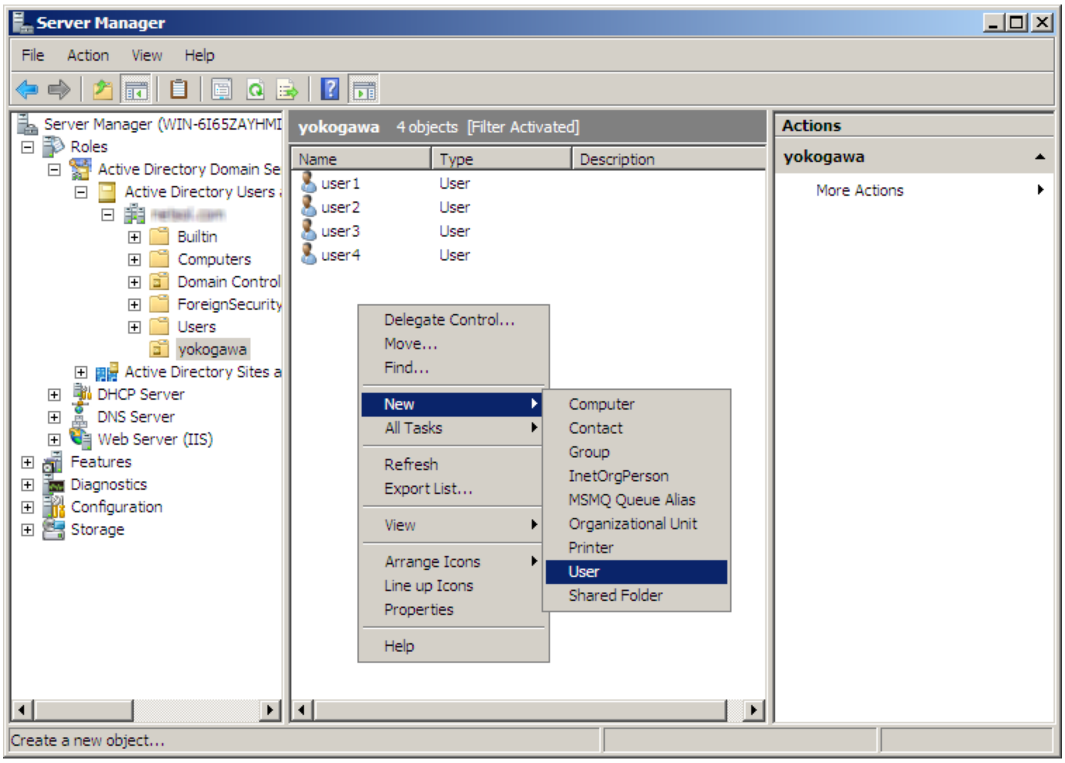
Item	Registration Name	Password
Host name	gx	record-as1

*1 Mapping is necessary when performing a user registration of a non-Windows device in Active Directory.

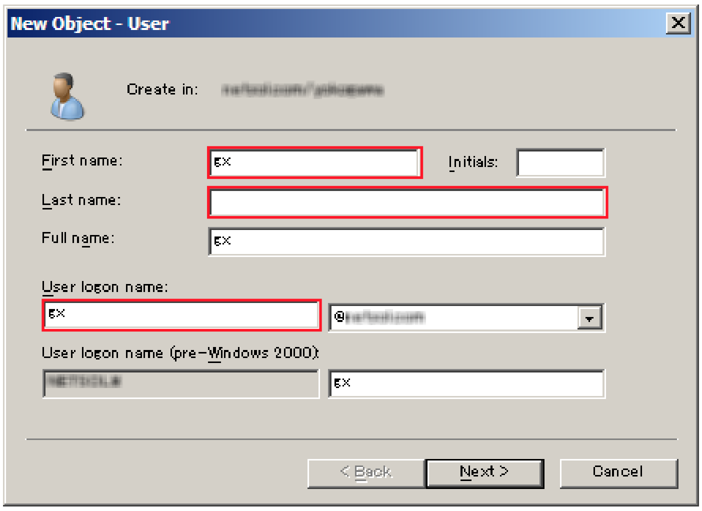
*2 The realm name will be the domain name (uppercase letters).

Creating a GX/GP Host Account

1. Start Server Manager, and choose New and then User.



2. Type “gx” in the **First name**, **Full name**, and **User logon name** boxes.



New Object - User

Create in: [redacted]

First name: gx Initials:

Last name:

Full name: gx

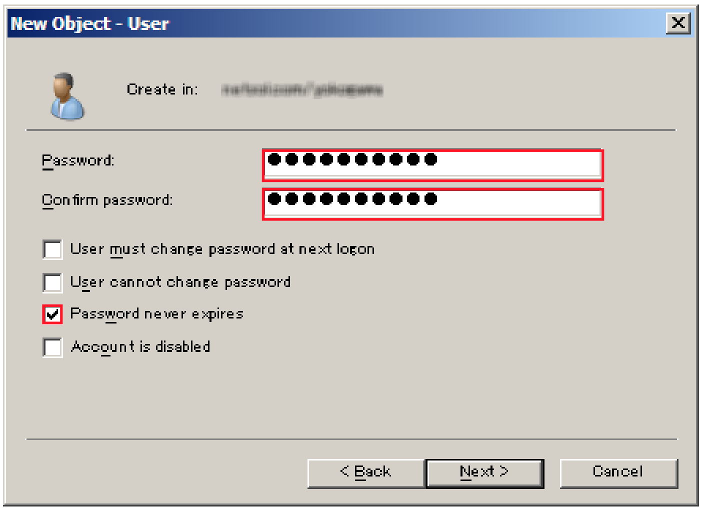
User logon name:

gx @[redacted]

User logon name (pre-Windows 2000):

[redacted] gx

3. Type “record-as1” in the **Password** box. Select the **Password never expires** check box.



New Object - User

Create in: [redacted]

Password: ●●●●●●●●●●

Confirm password: ●●●●●●●●●●

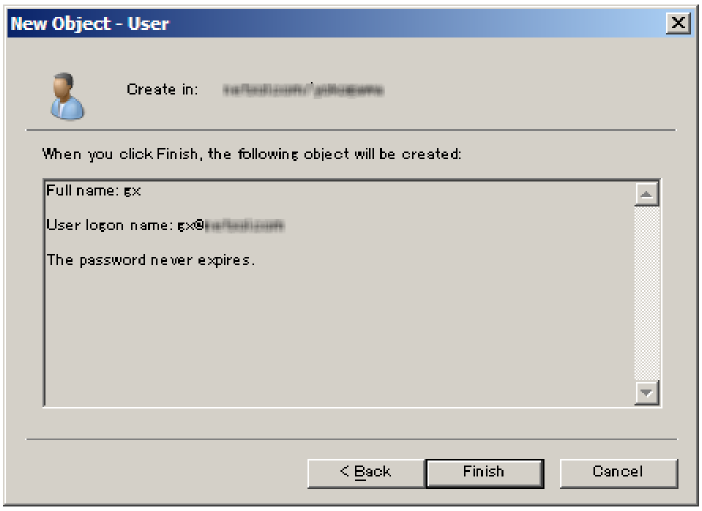
□ User must change password at next logon

□ User cannot change password

☑ Password never expires

□ Account is disabled

4. Click **Finish**.



New Object - User

Create in: [redacted]

When you click Finish, the following object will be created:

Full name: gx

User logon name: gx@[redacted]

The password never expires.

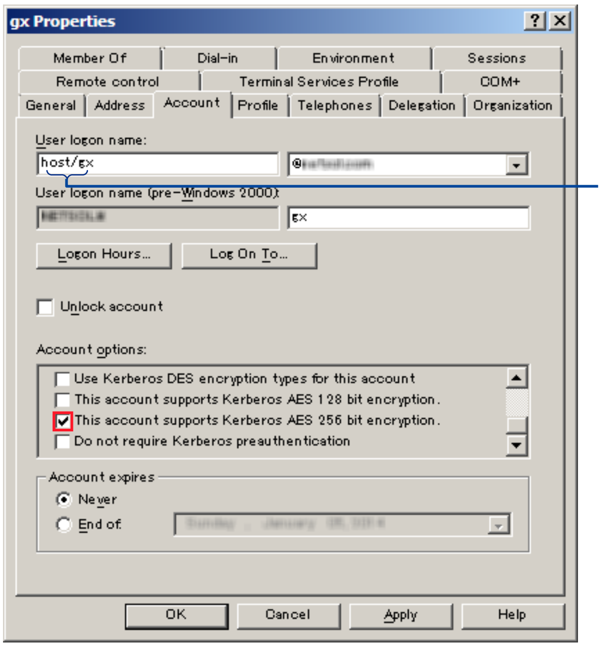
Changing the Properties of the Created Host Account

Select the following check boxes. Clear all other check boxes.

This account supports Kerberos AES 256 bit encryption

Password never expires

- The Password never expires check box was already selected in step 3, so it is selected in this dialog box.
- Clearing all the encryption check boxes is equivalent to selecting RC4.



User logon name: host/gx @[redacted]

User logon name (pre-Windows 2000): [redacted] gx

□ Unlock account

Account options:

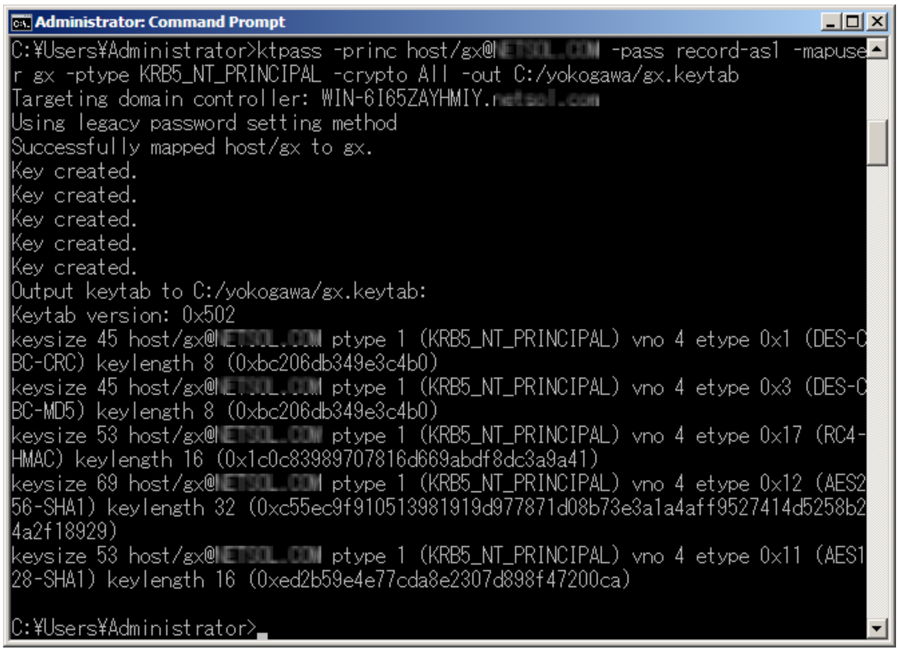
□ Use Kerberos DES encryption types for this account
□ This account supports Kerberos AES 128 bit encryption.
☑ This account supports Kerberos AES 256 bit encryption.
□ Do not require Kerberos preauthentication

Account expires
● Never
○ End of: [redacted]

“host” is not included before mapping. It is included after a successful mapping.

Mapping the Host Principal to the Host Account

Open a Command Prompt window, and execute the following command.
ktpass –princ host/gx@(the realm name that you are using) -pass record-as1 –mapuser gx –ptype
KRB5_NT_PRINCIPAL –crypto All –out C:\yokogawa\gx.keytab
A file named gx.keytab is created in the C:\yokogawa folder.



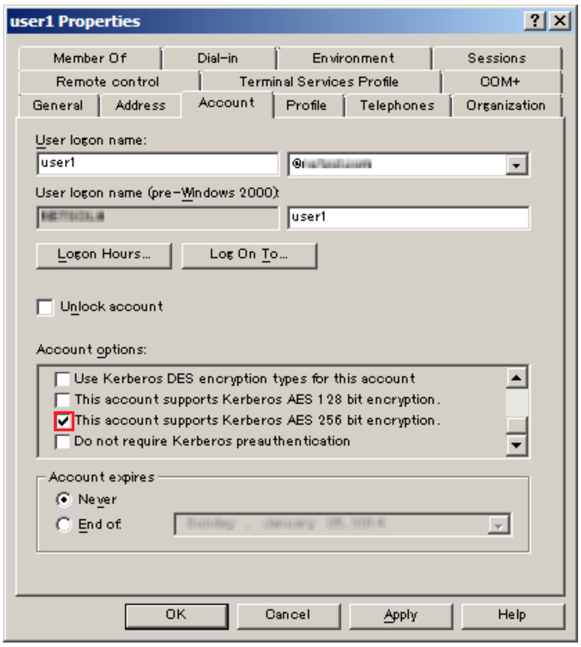
Administrator: Command Prompt

```
C:¥Users¥Administrator>ktpass -princ host/gx@[redacted] -pass record-as1 -mapuse
r gx -ptype KRB5_NT_PRINCIPAL -crypto All -out C:/yokogawa/gx.keytab
Targeting domain controller: WIN-6I65ZAYHMIY.[redacted]
Using legacy password setting method
Successfully mapped host/gx to gx.
Key created.
Key created.
Key created.
Key created.
Key created.
Output keytab to C:/yokogawa/gx.keytab:
Keytab version: 0x502
keysize 45 host/gx@[redacted] ptype 1 (KRB5_NT_PRINCIPAL) vno 4 etype 0x1 (DES-C
BC-CRC) keylength 8 (0xbc206db349e3c4b0)
keysize 45 host/gx@[redacted] ptype 1 (KRB5_NT_PRINCIPAL) vno 4 etype 0x3 (DES-C
BC-MD5) keylength 8 (0xbc206db349e3c4b0)
keysize 53 host/gx@[redacted] ptype 1 (KRB5_NT_PRINCIPAL) vno 4 etype 0x17 (RC4-
HMAC) keylength 16 (0x1c0c83989707816d669abdf8dc3a9a41)
keysize 69 host/gx@[redacted] ptype 1 (KRB5_NT_PRINCIPAL) vno 4 etype 0x12 (AES2
56-SHA1) keylength 32 (0xc55ec9f910513981919d977871d08b73e3a1a4aff9527414d5258b2
4a2f18929)
keysize 53 host/gx@[redacted] ptype 1 (KRB5_NT_PRINCIPAL) vno 4 etype 0x11 (AES1
28-SHA1) keylength 16 (0xed2b59e4e77cda8e2307d898f47200ca)

C:¥Users¥Administrator>_
```

Creating a User Account in Active Directory and Changing the Properties

Create a GX/GP user in Active Directory. Change the user account properties to match those of the host account.
In this example, select the
This account supports Kerberos AES 256 bit encryption
check box. Be sure to set the same encryption as the GX/GP host account.



user1 Properties

User logon name: user1 @[redacted]

User logon name (pre-Windows 2000): [redacted] user1

□ Unlock account

Account options:

□ Use Kerberos DES encryption types for this account
□ This account supports Kerberos AES 128 bit encryption.
☑ This account supports Kerberos AES 256 bit encryption.
□ Do not require Kerberos preauthentication

Account expires

● Never
○ End of: [redacted]

About Mapping

Mapping is the association between the host principal and host account. In the example below, setup item “princ” is associated with setup item “mapuser.” This is done using the ktpass tool.

- Open a Command Prompt window, and enter the ktpass command.

ktpass Settings

Setup Item		Windows Server 2003	Windows Server 2008, Windows Server 2012	Example
princ		host/host principal@realm name		host/gx@EXAMPLE.COM
pass		Password		record-as1
crypto	**ARC4**	RC4-HMAC-NT	RC4-HMAC-NT	RC4-HMAC-NT
	AES128		AES128-SHA1	
	AES256		AES256-SHA1	
mapuser		Host account		gx
ptype		KRB5_NT_PRINCIPAL		KRB5_NT_PRINCIPAL
out		Output folder name\file name.keytab		c:\temp\gx.keytab

Mapping Example

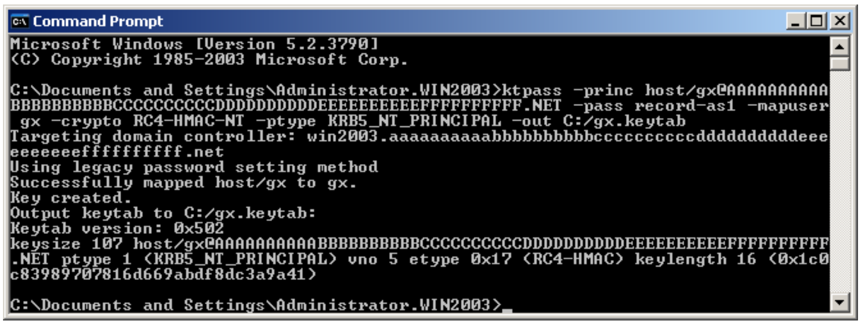
ktpass -princ host/gx@EXAMPLE.COM -pass record-as1 -crypto RC4-HMAC-NT -mapuser gx -ptype KRB5_NT_PRINCIPAL -out c:\temp\gx.keytab

Note

- Run the ktpass tool after installing the support tool provided by the server.
- Be sure to use uppercase letters for the realm name.
- On Windows Server 2008 and Windows Server 2012, you can set crypto to All.
- Set the same encryption for the user account and host account.
- ARC4 (ARCFOUR) is an encryption algorithm that is compatible with RC4.
- out can be omitted.

ktpass execution example (Windows Server 2003)

This execution example is different from what is shown in “ktpass Settings.”



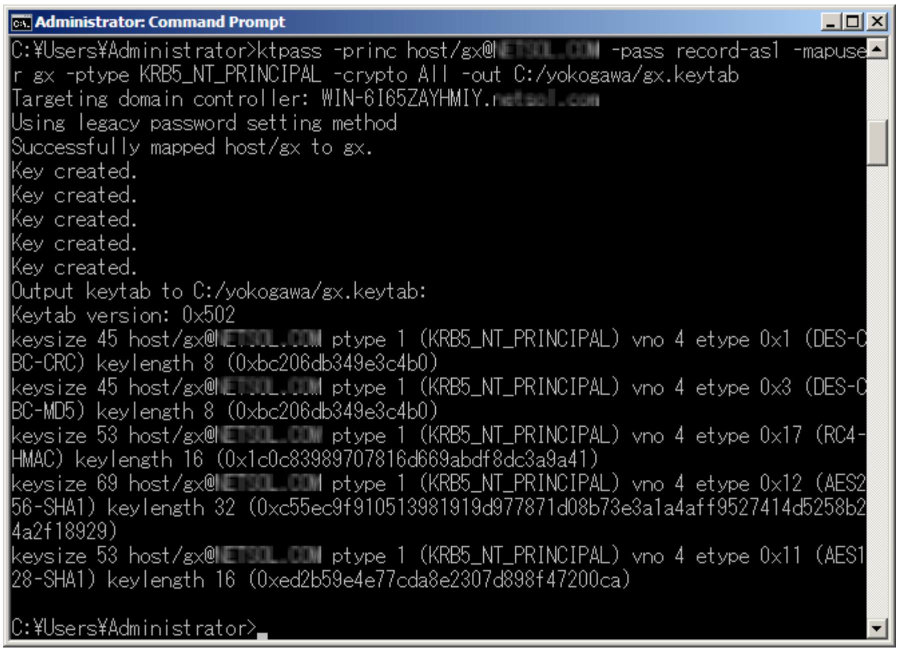
```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator.WIN2003>ktpass -princ host/gx@AAAAAAAAAA
BBBBBBBBBBCCCCCCCCCCDDDDDDDDDDEEEEEEEEEEFFFFFFFFFF.NET -pass record-as1 -mapuser
 gx -crypto RC4-HMAC-NT -ptype KRB5_NT_PRINCIPAL -out C:/gx.keytab
Targeting domain controller: win2003.aaaaaaaaaabbbbbbbbbbccccccccccddddddddddeee
eeeeeeeffffffffff.net
Using legacy password setting method
Successfully mapped host/gx to gx.
Key created.
Output keytab to C:/gx.keytab:
Keytab version: 0x502
keysize 107 host/gx@AAAAAAAAAABBBBBBBBBBCCCCCCCCCCDDDDDDDDDDEEEEEEEEEEFFFFFFFFFF
.NET ptype 1 (KRB5_NT_PRINCIPAL) vno 5 etype 0x17 (RC4-HMAC) keylength 16 (0x1c0
c83989707816d669abdf8dc3a9a41)

C:\Documents and Settings\Administrator.WIN2003>_
```

ktpass execution example (Windows Server 2008)

This execution example is different from what is shown in “ktpass Settings” on the previous page.



```
C:¥Users¥Administrator>ktpass -princ host/gx@[redacted] -pass record-as1 -mapuse
r gx -ptype KRB5_NT_PRINCIPAL -crypto All -out C:/yokogawa/gx.keytab
Targeting domain controller: WIN-6I65ZAYHMIY.[redacted]
Using legacy password setting method
Successfully mapped host/gx to gx.
Key created.
Key created.
Key created.
Key created.
Key created.
Output keytab to C:/yokogawa/gx.keytab:
Keytab version: 0x502
keysize 45 host/gx@[redacted] ptype 1 (KRB5_NT_PRINCIPAL) vno 4 etype 0x1 (DES-C
BC-CRC) keylength 8 (0xbc206db349e3c4b0)
keysize 45 host/gx@[redacted] ptype 1 (KRB5_NT_PRINCIPAL) vno 4 etype 0x3 (DES-C
BC-MD5) keylength 8 (0xbc206db349e3c4b0)
keysize 53 host/gx@[redacted] ptype 1 (KRB5_NT_PRINCIPAL) vno 4 etype 0x17 (RC4-
HMAC) keylength 16 (0x1c0c83989707816d669abdf8dc3a9a41)
keysize 69 host/gx@[redacted] ptype 1 (KRB5_NT_PRINCIPAL) vno 4 etype 0x12 (AES2
56-SHA1) keylength 32 (0xc55ec9f910513981919d977871d08b73e3a1a4aff9527414d5258b2
4a2f18929)
keysize 53 host/gx@[redacted] ptype 1 (KRB5_NT_PRINCIPAL) vno 4 etype 0x11 (AES1
28-SHA1) keylength 16 (0xed2b59e4e77cda8e2307d898f47200ca)

C:¥Users¥Administrator>
```

GX/GP Configuration

Configure the GX/GP as follows. For the configuration procedure, see section 3.1.1, “GX/GP KDC Client Settings”

Item	Description
Host principal	gx
Realm name	Set the realm name.
Password	record-as1
Encryption type	AES256
KDC server	Set the KDC server name.
Port number	88

Note

The realm name will be the domain name in uppercase letters.

3.2 Using the Password Management Function

3.2.1 Logging In and Out

Logging In

Log in by entering the user name and password.

Procedure

1. Press **MENU**.
   The login screen appears.

2. Enter the user name and password, and then tap **OK**.
   You will be logged in.

Operation complete

Note

Even if you enter a password, you may not be able to log in because of a network error or a problem with the settings. An error message will appear if this is the case. Perform the operation described below to log in as the root user.

Set the user name to “root” and the password to the root password, and tap **OK**.
You will be logged in as the root user. The default password for the root user is root123.

Logging Out

▶ For operating instructions, section 2.3.

3.2.2 Signing In

When you sign in, you will be prompted for a user name and password.
▶ For operating instructions, section 2.4.

3.2.3 Dealing with the “Invalid User” Status

If a user enters the wrong password for the specified number of times (Password retry), that user is invalidated. The user-locked icon appears in the status area. The user can log in again after a system administrator performs the locked-ACK operation (and the user-locked icon disappears).
▶ To clear the user locked icon, see section 2.3.

Note

The “Invalid user” status is only applicable on the GX/GP being operated. The user account on the server is not invalidated.

3.2.4 Password Expiration

Manage passwords and their expiration dates on the KDC server.

Note

When preauthentication is not being used, users may be able to log in to the GX/GP even after the password has expired.

3.3 Error Messages and Corrective Actions

Errors That Occur during Authentication

Code	Message	Description and Corrective Action
E004	Incorrect input character string.	Enter a proper character string.
E251	Invalid user name or password.	Enter the correct name or password.
E252	The login password is incorrect.	Check the password. If the password is lost, the password must be initialized by an administrator.
E261	Wrong user ID or password.	Enter the correct user ID and password.
E265	Login inputs are incorrect.	Enter the correct login information.
E272	This password became invalid.	On the GX/GP, because the wrong password has been entered for more than the permissible number of times, this user is invalid.
E273	Invalid user.	The account has been invalidated on the server. The account has been invalidated on the GX/GP.
E760	Invalid KDC client configuration.	Set the host principal or realm name.
E763	Not supported by this machine.	Not supported by the GX/GP.
E764	Preauthentication failed.	Enter the correct password. Also, make sure that the times on the GX/GP and the server match.
E765	The encryption type is not supported by this machine.	The GX/GP does not support the encryption type, or the encryption type settings on the GX/GP and the server are different. Use the same encryption method on the GX/GP and the server.
E766	Failed to receive authentication from KDC server.	Check the GX/GP and server settings. Also, make sure that the times on the GX/GP and the server match.
E767	Change the password.	Change the password. Change the password of the user account that is registered on the server.
E768	The time difference with the KDC server exceeds the limit.	There is a time difference of 5 minutes or more between the GX/GP and the server. Synchronize the GX/GP time to the time on the server.
E770	The host principal is not registered.	The host account is not registered on the server.
E771	The host principal is invalid.	Check the host account that is registered on the server.
E772	The host password is incorrect.	Make sure that the GX/GP authentication-key password and the server's host-account password match.
E773	Preauthentication failed.	An internal error occurred during preauthentication. Disable the server's preauthentication function.
E774	The realm is incorrect.	Make sure that the realm name setting on the GX/GP is correct.

Errors That Occur during Communication

Code	Message	Description and Corrective Action
E651	IP address is not set or ethernet function is not available.	The GX/GP IP address not set. Check the IP address.
E657	Ethernet cable is not connected.	Check the cable connection.
E761	Cannot find KDC server.	The KDC server cannot be found in the same domain.
E762	KDC server connection error.	An error occurred while the GX/GP was connecting to the KDC server. Make sure that the network connection is not broken.

Other Messages

Code	Message	Description and Corrective Action
E836	KDC test connection succeeded.	—
E837	Login may be impossible in incorrect KDC client settings.	—

Appendix 1 Event Log Contents

Event Log

Operation	Display	Details
Error log		
Error	Error###	Error code Message ###: Error code
A/D calibration operation		
A/D calibration	A/DCalExec	Unit/slot
Login operations		
Power off	PowerOff	
Power on	PowerOn	
Login	Login	
Logout	Logout	
User invalidation	UserLocked	User number
Control operations		
Mode change	ModeChg	Mode
Time change	TimeChg	
New time	NewTime	
Time adjustment start	TRevStart	Difference
Time adjustment stop	TRevEnd	
SNTP time change	SNTPtimeset	
Daylight saving time start	DSTStart	
Daylight saving time end	DSTEnd	
Password change	ChgPasswd	User number
Unauthorized access acknowledge	UserLockedACK	
Alarm acknowledge	AlarmACK	Channel number Alarm level
Message writing*	Message###	Message number (excluding freehand message) Message type Data timestamp (for additions) ###: Number (normal) F##: Number (free) Hnd: (freehand)
Recording start*	MemStart	
Recording stop*	MemStop	
Manual sample	ManualSample	
Math start	MathStart	
Math stop	MathStop	
Math reset*	MathRST	
Computation data dropout acknowledgment	MathACK	
Mail start	MailStart	
Mail stop	MailStop	
Modbus manual recovery	RefModbus	Type
Display data save*	DispSave	
Event data save*	EventSave	
Manual data save	ManualSave	Data type
SaveManual	SaveManual	
Snapshot	Snapshot	
Batch number setting*	BatNoSet	
Lot number setting*	LotNoSet	
Batch text field setting*	TextFieldSet	Text field number
Multi batch setting change	Multi Batch	On/Off atch operation qty
Display update rate change	ChgRate	Trend interval
Timer reset	TimerRST	Timer number
Match time timer reset	MTimerRST	Timer number
Communication channel writing (GX/GP operation only)	WriteComm	Channel number/value Write type
DO channel writing (for manual operation)	WriteDO	Channel number/Status
SW writing (for manual operation) (GX/GP, communication, serial)	WriteSW	Internal switch number/Status
Report save	SaveReport	Report format/report type

Continued on next page

Operation	Display (English)	Details
Scale image save*	SaveScale	Group number
Custom display save	SaveCustom	Display number
Parameter save	SaveParameter	
Certificate save	SaveCert	
All settings save	SaveAll	
Report load	LoadReport	Report format/report type
Scale image load*	LoadScale	Group number
Custom display load	LoadCustom	Display number
Parameter load	LoadParameter	Setting type
Certificate load	LoadCert	
All settings load	LoadAll	
Key creation	GeneKey######	######: Start: Start creation Cancel: Cancel creation Done: Creation completed
Installation of certificate	InstallServCert	Certification type/purpose
Certificate creation	CreateCert	
Touch screen adjustment	ExecTouchCal	
initialization	Initialize	Initialize type
Sign in	Sign In	Sign in level File name
Reminder expiration	Expiration####	Schedule number Title ####: Schedule number
Manually recover SLMP communication	RefSLMP	
Setting changes while recording is in progress or is stopped		
Schedule setting change	SetSchedule####	Schedule number On/Off (before and after change) Due date (before and after change) Daily reminder (before and after change) Re-notification cycle (before and after change) Title (after change) Notification contents (Changed notification content number) Buzzer (before and after change) CC Setting ####: Schedule number
Setting changes while recording is stopped		
Setting change	SetParameter	Setting change type Setting file name
Setting changes during recording		
Alarm setting change	SetAlarm	Channel number /Alarm level On/Off (before and after change) Type (before and after change) Alarm value (before and after change) Hysteresis (before and after change) Logging (before and after change) Output type (before and after change) Output destination (before and after change)
Alarm delay setting change	SetAlmDelay	Channel number Delay hour (before and after change) Delay minute (before and after change) Delay second (before and after change)
Calibration correction/set point change	CCModePntSet	Channel number Mode (before and after change) Number of set points (before and after change)

Continued on next page

Operation	Display (English)	Details
Calibration correction value change	SetCCValue	Channel number Set number Calibration correction value (before and after change) Output calibration value (before and after change)
Save directory change	SetDirectory	Folder name (before and after change)
Send address change	SendAddressSet	Recipient number (1/2)
Login change	LoginSet	User number
Correction factor setting change	SetCFactor	Channel No. Set number Uncorrected value (before and after change) Inst correction factor (before and after change) Sensor correction factor (before and after change)
Module		
Module update	UpdateModule	Unit/slot
Module disconnection	RemoveModule	Unit/slot Module name Serial number Version number
Modules installed	AttachModule	Unit/slot Module name Serial number Version number
Module information	InfoModule	Unit Slot Calibration date Calibration user
Module activation	ApplyModule	
Reconfiguration	ConfigModule	
Updating		
Updating of other settings	Update####	Update type ####: Web: Web application

* Batch group numbers are displayed in the Batch column when the multi batch function (/BT option) is enabled.

Operation property

Factor	Description
OPERATE	GX/GP key operation, touch operation (including bar-code)
COMMU	Operation via communication (including Web)
SERIAL	Operation via serial communication
EXTERNAL	Operation from Modbus and the like
PC	Only when the user accessing from the PC is invalidated
REMOTE	Remote control operation
ACTION	Event action operation
SYSTEM	Auto operation by the GX/GP

User Name

Factor	User Name
OPERATE	User logged in from the GX/GP panel
COMMU	User logged in via communication
SERIAL	User logged in via serial interface
EXTERNAL	No user
PC	User logged in via PC
REMOTE	User logged in from the GX/GP panel
ACTION	No user
SYSTEM	No user