User's
Manual

SMARTDAC+®

Data Acquisition System GM

Advanced Security Function (/AS) User's Manual

vigilantplant®

YOKOGAWA ◆
Yokogawa Electric Corporation

IM 04L55B01-05EN
1st Edition

Introduction

Thank you for purchasing the SMARTDAC+ Data Acquisition System GM (hereafter referred to as the GM).
This manual explains how to use the Advanced Security Function (/AS option) of the GM.
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.
- 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

- The TCP/IP software of this product and the document concerning the TCP/IP software have been developed/created by YOKOGAWA based on the BSD Networking Software, Release 1 that has been licensed from University of California.

Heimdal

The password-management function of the following products uses Heimdal source code for AES authentication key generation. In accordance with the Heimdal license agreement, the copyright notice, redistribution conditions, and license are listed below.

GM

Copyright (c) 2006 Kungliga Tekniska Högskolan (Royal Institute of Technology, Stockholm, Sweden).All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the Institute nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

1st Edition: Aug 2015 (YK)

Jsencrypt

The password encryption section of the following product’s Web application uses jsencript source code. In accordance with the MIT’s license agreement, the copyright notice, redistribution conditions, and license are listed below.

SMARTDAC+ GM10 Data Acquisition Module

Jsencrypt
https://github.com/travist/jsencrypt/blob/master/LICENSE.txt

File: src/LICENSE.txt
The MIT License (MIT)
Copyright (c) 2013 AllPlayers.com

File: lib/jsrsasign/LICENSE.txt

CONTAINS CODE FROM YUI LIBRARY SEE LICENSE @ http://yuilibrary.com/license/

The ‘jsrsasign’(RSA-Sign JavaScript Library) License

Copyright (c) 2010-2013 Kenji Urushima

File: lib/jsbn/LICENSE.txt

Licensing

This software is covered under the following copyright:

Address all questions regarding this license to:

Tom Wu
tjw@cs.Stanford.EDU

File: lib/asn1js/LICENSE.txt

ASN.1 JavaScript decoder

Revisions

August 2015	1st Edition

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 GM with release number 2 (see the STYLE S number) and style number 1 (see the STYLE H number).

What This Manual Explains

The advanced security function is a function for complying with US FDA 21 CFR Part 11.
This manual primarily explains how to use the login, audit trail, and signature functions of the advanced security function.
The advanced security function is enabled on the GM.
It is also assumed that the communication security is set to Login.

Note

You can also disable the advanced security function on the GM.
▶ For the setting procedure, see section 2.5, “Disabling the Advanced Security Function,” on page 2-19.
If the advanced security function is disabled, standard (/AS option not installed) functions will be available. Note that if disabled, compliance with US FDA 21 CFR Part 11 will no longer hold.
▶ For the operating procedure when the advanced security function is disabled, see the User’s Manual.

For details on how to use other functions, see also the User’s Manual (IM04L55B01-01EN). For details on the communication functions (general purpose communication, USB communication, Bluetooth communication), see the Communication Interface User’s Manual (IM04L51B01-17EN).
For details on signature operations, see the Universal Viewer Manual (IM 04L61B01-01EN).

The GM10 standard type and large memory type are distinguished using the following notations.

- Standard type: GM10-1
- Large memory type: GM10-2

The following terms are used for references to other manuals:

Notation	Description
User’s Manual	Data Acquisition System GM User’s Manual Refers to the IM 04L55B01-01EN.
First Step Guide	Data Acquisition System GM First Step Guide Refers to the IM 04L55B01-02EN.
Communication Command Manual	Model GX10/GX20/GP10/GP20/GM 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	GM	Release number 2 (Version 2.03)	New edition
		Style number 1	

Contents

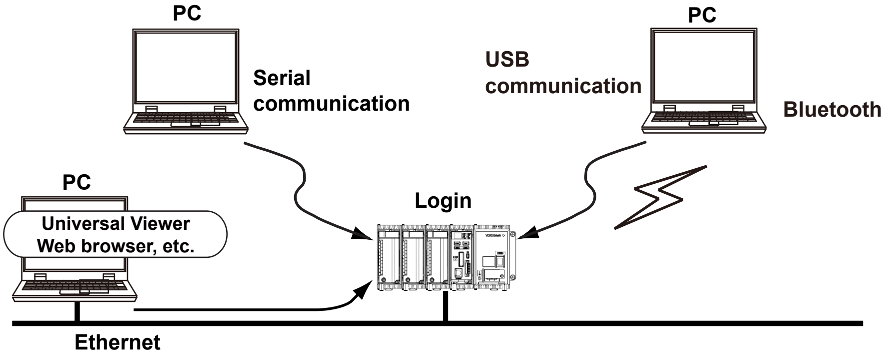
1.1 Using the Advanced Security Function

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

1.1.1 Operation Overview

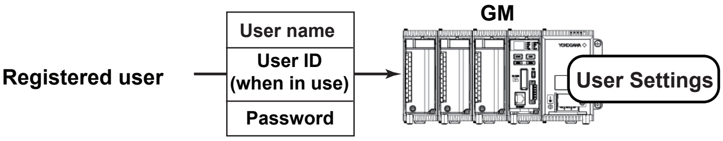
GM Operation

The GM can be configured, controlled, and monitored through the Web application (Web browser) and controlled using dedicated commands via general purpose communication (Ethernet communication, serial communication (/C3)), USB communication, Bluetooth communication (/C8).

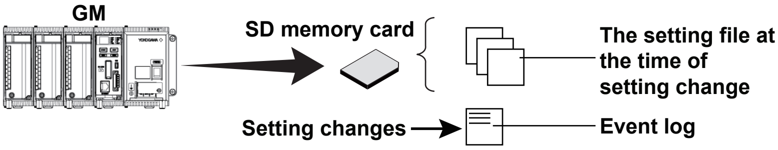


Configuring Functions

First, you need to configure the GM functions. You have to configure the measurement settings and then register GM users. After you register users, to use the GM, you will need to log in to it by entering a user name, user ID (when in use), and password. Front panel keys cannot be used.

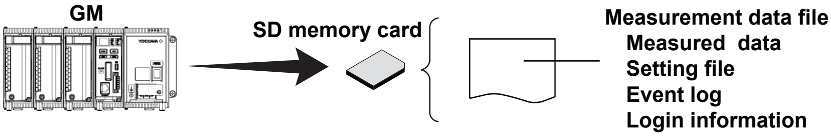


History of setting changes is recorded in an event log, and a new setting file is saved to an SD memory card. An SD memory card must be installed when settings are changed.



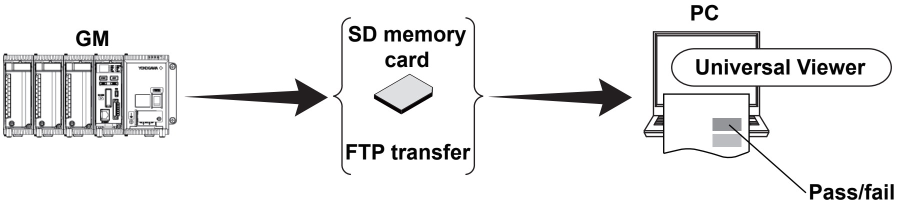
Measurement

Measured data (event or display data; see section 1.2, “Recording and Saving Data,” on page 1-4) is recorded to the GM 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. An SD memory card must be installed.



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. You can sign measurement data files using the standard PC software, Universal Viewer. Signing measurement data files is not possible from the GM.



1.1.2 GM Operation Range

The GM Manages Measured Data in Its Internal Memory

- You cannot change the measured data in the GM internal memory. The only way you can delete the measured data is by initializing the internal memory.
- Measurement data files in the GM internal memory cannot be signed.
- Measured data in the internal memory is automatically be saved to a file on an external storage medium. (When communication security is set to Login, Media save is fixed to Auto save.) During this operation, if a file with the same name exists on the external storage medium, it is overwritten unconditionally.

You Cannot Use the GM 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 GM, but you cannot change or delete it.
- The GM cannot format external storage media.

1.1.3 PC Software

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

▶ See the Universal Viewer Manual.

1.1.4 Terminology

Administrator ▶section 1.3

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

User ▶section 1.3

A type of user that can be registered on the GM. 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 GM. A monitor user can only monitor the GM 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 GM via Web application or communication (Ethernet, serial, USB communication, Bluetooth communication) 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.
Universal Viewer is used to sign measurement data files.
Signing measurement data files is not possible from the GM.

Password Management Function ▶section 1.4

A function for managing the users who can access the GM 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.
When communication security is set to Login, Media save is fixed to Auto save.

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.

1.2 Recording and Saving Data

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

1.2.1 Data Types

The types of data that the GM can store to files are listed below.

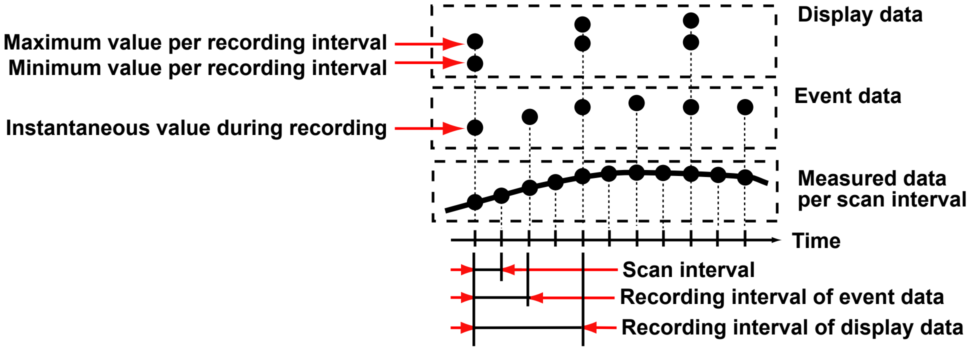
▶ For information about file name extensions, see page 1-12.

Data Type	Description
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.
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.
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.
Setting parameters	• The setting parameters of the GM. • 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.

Event data and display data

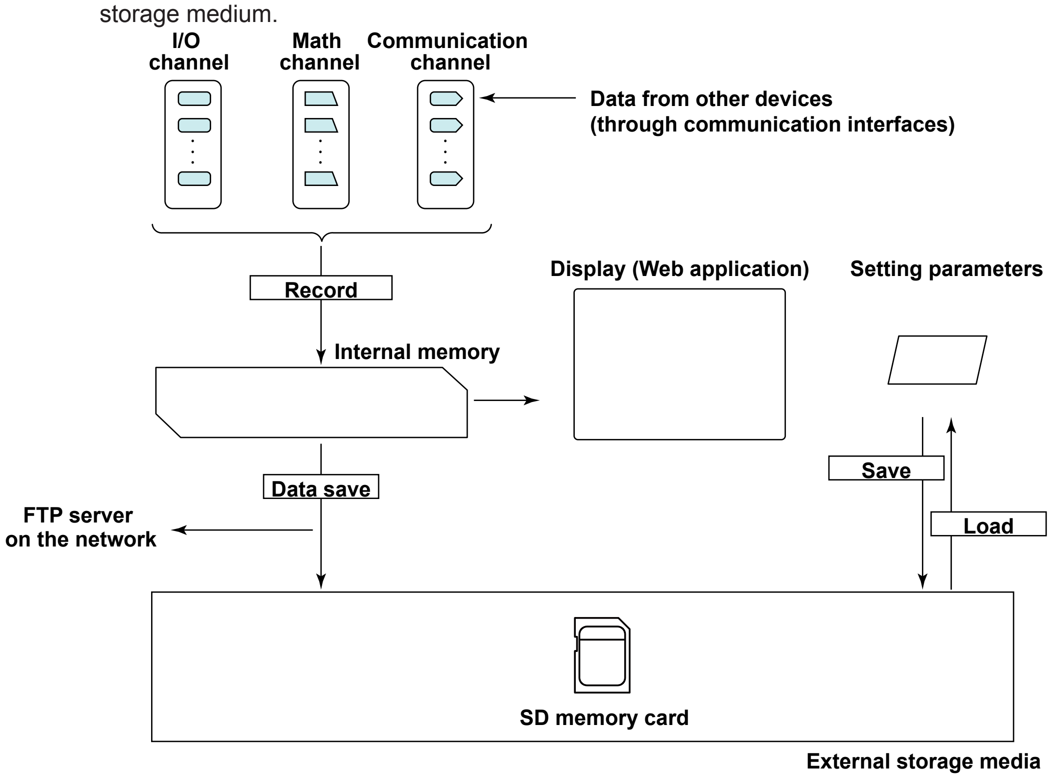
Event data is useful when you wish to record the measured data in detail.

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


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

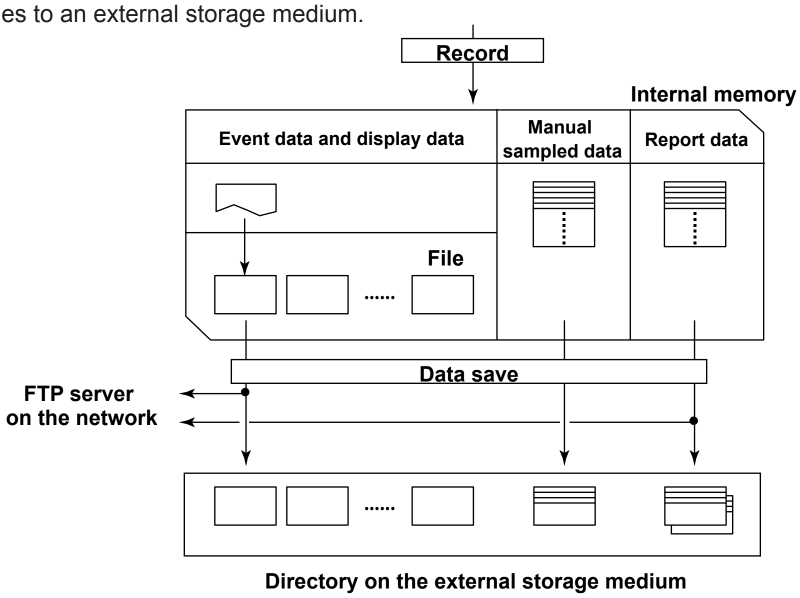
1.2.2 Data Recording and Storage Flowchart

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



Internal Memory

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


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

1.2.3 Event, Display, and Setting File Encryption

Event, display, and setting files are encrypted. You cannot change their data or delete them.

1.2.4 Event and Display Data Recording Methods

▶ For the setting procedure, see section 2.9, “Setting Recording Conditions (Recording mode, recording interval, saving interval)” and 2.8, “Setting Measurement Conditions (Scan interval, A/D integrate, etc.)” in the User’s Manual.
▶ For operating instructions, see section 3.1.1, “Starting and Stopping Recording” in the User’s Manual.

Type of Data to Record

You can choose to record event or display data.

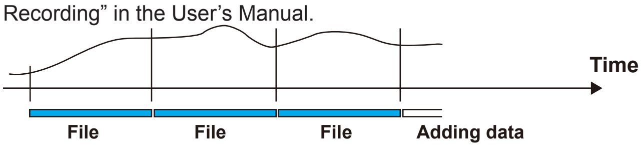
- **Choosing What Type of Data to Record**

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

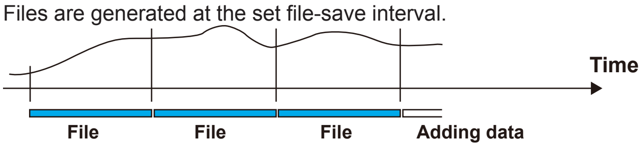
Internal Memory

The measured data is partitioned and saved to files at set intervals. If the internal memory is full or if the number of event data files and display data files exceeds 500 for GM10-1 or 1000 for GM10-2, files are overwritten from the oldest file.

Recording Conditions of Event Data

Item	Description
Channel type	You can set the channel type to measurement, computation, or communication.
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 and stop recording from the Web application. You cannot start or stop saving using the START or STOP key. For operating instructions, see section 3.1.1, “Starting and Stopping Recording” in the User’s Manual. 

Recording Conditions of Display Data

Item	Description
Channel type	Same as event data.
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 and stop recording from the Web application. You cannot start or stop saving using the START or STOP key. For operating instructions, see section 3.1.1, "Starting and Stopping Recording" in the User's Manual.

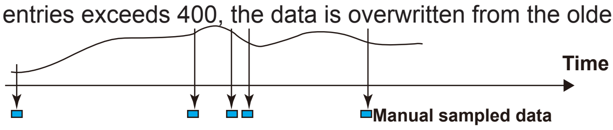
Trend Interval and Display Data Recording Interval

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.

1.2.5 Manual Sampled Data

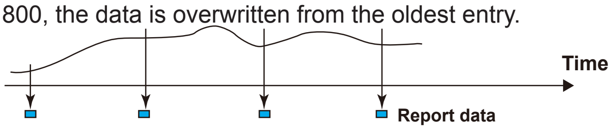
Manual sampled data is recorded to internal memory. If the number of manual sampled data entries exceeds 400, the data is overwritten from the oldest entry.



▶ For operating instructions, see "Listing and Saving Manual Sampled Data" in section 3.1.2, "Monitoring the GM Data and Controlling the GM from the Monitor Screen," 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 2.12, "Configuring 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)

SD Memory Card Directory

The directories that the GM 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 save through save operation

▶ For operating instructions, see section 2.23.1, “Saving, Loading, and Deleting GM Setting Parameters.”

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

▶ For the setting procedure, see section 2.10, “Setting the Conditions for Saving Data Files,” in the User’s Manual.

Data save destination directory using Web application operation

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

Event data, display data, manual sampled data, report data

▶ For operating instructions, see “Listing and Saving the Measured Data in the Internal Memory” in section 3.1.2, “Monitoring the GM Data and Controlling the GM from the Monitor Screen,” in the User’s Manual.

Saved Files

GMs with the advanced security option create the following types of files.

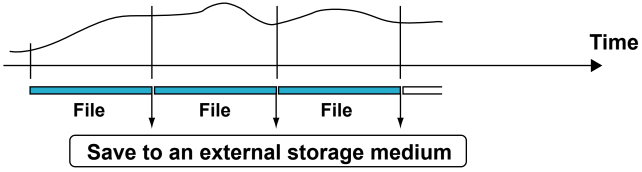
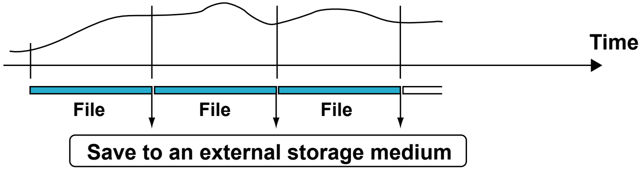
Type	Extension	Notes
Event data file	GSE	-
Display data file	GSD	-
Setting file	GSL	See page 1-12 and section 1.5.
Manual sampled data file	GMN	-
Report data file (/MT option)	GRE	-
	xlsx or xlsm	For use with the report template function
	pdf	

1.2.8 Saving Data to External Storage Medium

Auto Save

The following type of files are automatically saved: event data, display 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 (fixed to Auto save).

Auto Save Timing

Data Type	Description
Event data	The file is saved when the file is created.  Time File File File Save to an external storage medium
Display data	The file is saved when the file is created.  Time File File File Save to an external storage medium
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 the setting procedure, see “Listing and Saving Manual Sampled Data” in section 3.1.2, “Monitoring the GM Data and Controlling the GM from the Monitor Screen,” 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 2.12, “Configuring 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 Event and Display Data Files

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

Contents of the event data and display data files

- Header string (see section 2.10.1, “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 2.11, “Configuring 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

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 GM will create the directory on the SD memory card and save data to it.
▶ For the setting procedure, see section 2.10, “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)

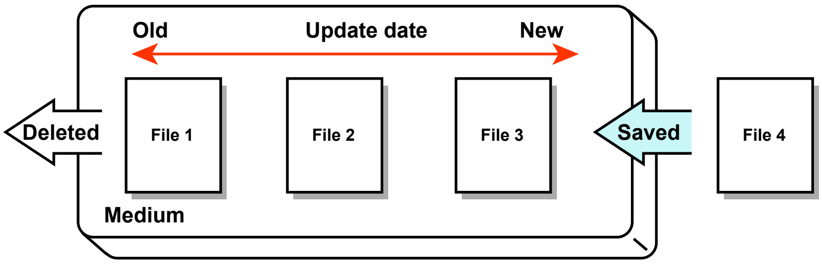
If there is not enough free space on the SD memory card, the GM cannot save the data in the internal memory to the SD memory card. Replace the SD memory card before the data in the internal memory is overwritten.

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 GM continuously without having to replace the SD memory card.

▶ For the setting procedure, see section 2.10, "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.
  Event data files, display data files, report data files (/MT option), and manual-sampled-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 GM 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.

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	Event data Display data Manual sampled 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	Event data Display data Manual sampled 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	Event data Display 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 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	**Event data : GSE Display data : GSD Manual sampled data : GMN Alarm summary data : GAL**	**Report data : GRE Report data : xlsx or xlsm (report template function) Report data : pdf (report template function)**

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 GM setting parameters to an SD memory card. 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 2.23, “Saving and Loading Settings,” 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: event data, display data, report data (/MT option), setup data when the settings are changed. You can also use the GM as an FTP server. You can access the GM from a personal computer and retrieve and store data files from both internal and external memory.
* Only monitor uses can connect to the FTP server.

Connecting from a PC via the FTP

An example of retrieving files using a browser is described below. In the URL box, enter ftp://user name@host name.domain name. Download the data you want to retrieve from the /MEM0/DATA folder in the case of internal memory data or the /DRV0 folder in the case of data on the external storage medium to the PC.
You can also use the IP address in place of the “host name.domain name.”
You will be prompted for a user name and password when you access the server. Enter a user name and password of the monitor user that is registered on the GM to connect.

- The internal memory is linked to ftp://username*@hostname/MEM0/DATA.
- [External storage medium: SD memory card] is linked to ftp://username*@hostname/DRV0/.
- You cannot retrieve data files that are being created.
- You must access using “ftps://” when SSL encryption is in use.

* username: user name of the monitor user set in user registration

▶ For the setting procedure, see section 2.17.2, “Configuring the FTP Client Function,” in the User’s Manual.
▶ For operating instructions, see section 3.3, “Accessing the Measurement Data File on the GM from a PC (FTP server function),” in the User’s Manual.

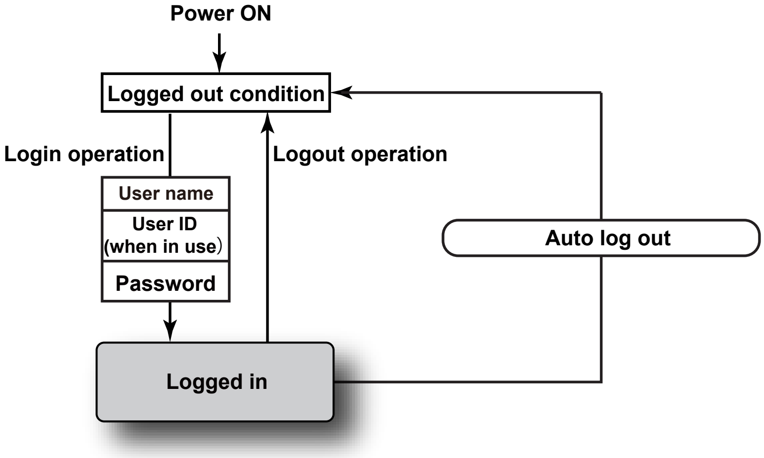
1.3 Login Function

Only registered users can control the GM by logging in by entering user identification information (user name, user ID (when in use), and password). When the login function is enabled, front panel key operations are restricted.*

* The only available operations are clearing the error display with the STOP key and turning on and off the Bluetooth function with the USER1 key.

▶ For the setting procedure, section 2.1.

▶ For operating instructions, section 2.2.



1.3.1 Logging In to and Logging Out of the Web Application

Logging In

When you access the Web application, a login window appears. Enter user identification information (user name, user ID (when in use), and password) to log in to the GM.

Logging Out

Use the logout procedure to log out from the Web application. You can also log out by closing the Web page. It is also possible to configure the GM so that a user is automatically logged out when the user does not perform any operation on the Web application for a given period.

Auto Web Logout

You can configure the GM to automatically log a user out when there is no operation from the Web application for a given period.

▶ See section 2.1.1, “Configuring the Security Function, Logout, Password Management Function, Etc.,” on page 2-1.

1.3.2 Logging In and Out through Communication

To access the GM through general purpose communication (Ethernet communication, serial communication (/C3)), USB communication, Bluetooth communication (/C8), or DARWIN compatible communication (Ethernet communication, serial communication (/C3)), you must log in as a registered user.

Logging In

Using a dedicated command, enter user identification information (user name, user ID (when in use), and password) to log in to the GM.

Logging Out

Use a dedicated command to log out. It is also possible to configure the GM so that a user is automatically logged out when there is no access for a given period.

Auto Logout

- In the case of general communication using Ethernet or FTP server, use the timeout function.
  ▶ See section 2.17.7, "Configuring the Server Function," in the User's Manual.
- In the case of general communication using serial communication, use the timeout function.
  ▶ See section 2.18.1, "Setting Basic Communication Conditions," in the User's Manual.
- In the case of general communication using USB communication, use the logout function.
  ▶ See section 2.19.1, "Turning the USB Communication Function On and Off," in the User's Manual.
- In the case of general communication using Bluetooth communication, use the communication timeout function.
  ▶ See section 2.20.1, "Turning the Bluetooth Communication Function On and Off," in the User's Manual.

▶ For details about logging in through communication, see the Communication Command Manual.

1.3.3 Logging In and Out of the FTP Server

Only the monitor users can log in to the FTP server. Administrators and users cannot log in. To use the FTP server, register a monitor user.

Logging In

Enter user identification information (user name and password) to log in.

Logging Out

It is possible to configure the GM so that a user is automatically logged out when there is no access for a given period.

Auto Logout

Use the timeout function to set the auto logout for the FTP server.
▶ See section 2.17.7, "Configuring the Server Function," in the User's Manual.

1.3.4 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 can specify the range of operations that a user can perform (user property).
Monitor user	Monitor	A monitor user can only use the monitor function. The user cannot configure or operate the GM. You can also access the GM FTP server and retrieve and store data files from both internal and external memory. There is no function for invalidating users based on password retry counts.

Administrator

Item	Description	
Login methods	Communication	Users can log in through the Web application or general purpose communication (Ethernet communication, serial communication (/C3), USB communication, Bluetooth communication (/C8)).
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 OFF, 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 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	Communication	Users can log in through the Web application or general purpose communication (Ethernet communication, serial communication (/C3), USB communication, Bluetooth communication (/C8)). For limitations on the operating range, see “User Privileges.”
Identification information	The same as for administrators.	

Monitor User

Administrators register Monitor users.

Item	Description	
Login methods	Communication	Users can log in through the Web application, general purpose communication (Ethernet communication, serial communication (/C3), USB communication, Bluetooth communication (/C8)), or FTP server. Only monitoring is possible. The user cannot configure or operate the GM except for changing the password. The password expiration cannot be changed either.
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)

Limitations on operations through the Web application or communication can be placed for each user separately. The applicable operations are shown in the following table.
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, 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; and manually recover Modbus client
Time set	Manual SNTP server time adjustment and date/time adjustment.
Setting operations	All setting operations
Calibration correction	Configure calibration correction.
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 * Includes trusted certificates
System operations	Initialize, reconfigure system, create self-signed certificates, create certificate requests, display certificates, delete certificates, install certificates, install intermediate certificates, execute unverified certificates, and activate modules
Output operations	Operate internal switches of type Manual and operate the relays of range type Manual.

Signature Privileges (Sign In Property)

The signature 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.

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 GM.

Password Expiration

You can set a password expiration period (but not for Monitor users).
▶ See section 2.1.2, “Registering Users,” on page 2-4.

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.
▶ See section 2.1.1, “Configuring the Security Function, Logout, Password Management Function, Etc.,” on page 2-1.

Reusing Setting Parameters

You can use the settings of one GM on another GM 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 default passwords.
▶ For operating instructions, see section 2.23, “Saving and Loading Settings,” 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.

1.3.5 Login Restrictions

Logging In with a Different User Name

If you open multiple Internet Explorer windows (or multiple tabs) on the same PC and access the GM through the Web application, the login procedure does not take place, and the same user that is already logged in is used to start the Web application.

This situation does not qualify as "logging in with the same user name" (explained later).

To start multiple Internet Explorer windows on the same PC and log in with different user names, click New Session on the File menu of Internet Explorer and connect through the Web application on the window that opens.

Example: When you want to regularly log in as a monitor user to monitor data and occasionally log in as an administrator to configure settings

Note

You can create a shortcut for Internet Explorer, right-click it and click Properties, and append "-nomerge" in Target box to start a new session window using the shortcut.

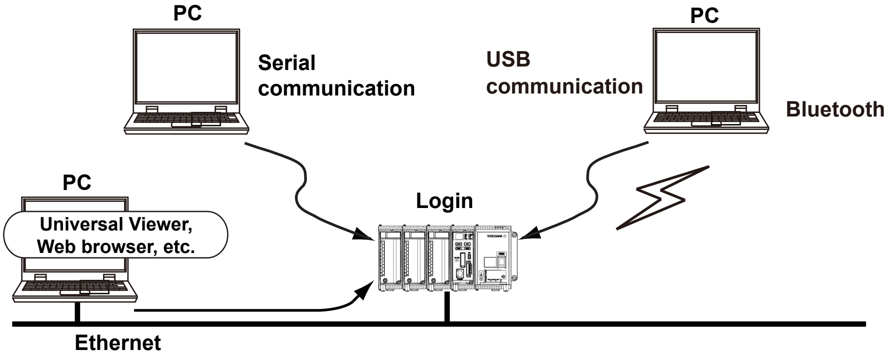
Logging In with the Same User Name

Except monitor users, users cannot log in with the same user name through the Web application.

If you try to log in with a user that is already logged in to the Web application, the connected user is logged out, and the new user is logged in.

Logging in Simultaneously

Multiple users can simultaneously log in to the GM through the Web application and communication.



Number of the simultaneous connections

Access Method	Number of Maximum Connection
General communication (Ethernet)	4
General purpose communication (serial)	1
Web application	4
USB communication	1
Bluetooth communication	1

1.3.6 How the GM Operates When the Login Function Is Not Used

The GM operates in the following manner when the login function is not used.

- There is no need to log in.
- All configuration, control, and monitor operations through the Web application are available.
- All operations using dedicated commands via general purpose communication (Ethernet communication, serial communication (/C3)), USB communication, Bluetooth communication (/C8) are available.
- START key, STOP key, and event action operations using USER1 and USER2 keys are available. Key lock is possible.
- The GM can be configured so that when an external storage medium is set, unsaved data in the internal memory is saved to files in the external storage medium.
- Saving and deleting files on the external storage medium using the FTP server are not possible.

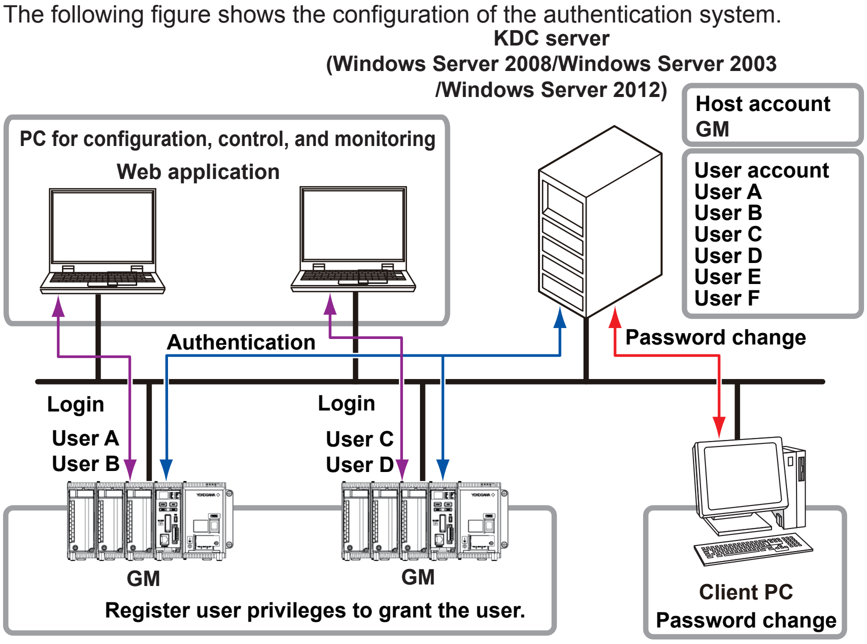
1.4 Password Management

The password management function enables you to manage access to the GM 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 GM on the network (host account) and the user accounts for accessing the GM.
- GM
  Of the user accounts on the KDC server, you can specify which accounts to use (login settings) on which GMs. You can also set different user privileges for each user on each GM.
- Client PC for maintenance
  This device is used to change user account passwords and for other maintenance. It is not explained in this manual.
- PC for configuration, control, and monitoring
  This PC is used to log in to the GM to configure, control, and monitor it.

Operation

When you log in to the GM, you will be prompted for a user name and password (the password management function does not use user IDs). The GM will then perform the communication with the KDC server that is necessary for authentication. When authentication completes successfully, you can operate the GM. The server manages the passwords and their expiration period. Monitor users (Monitor level users) are excluded from this function. Monitor users are managed on the GM (passwords can be managed on the GM).

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

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

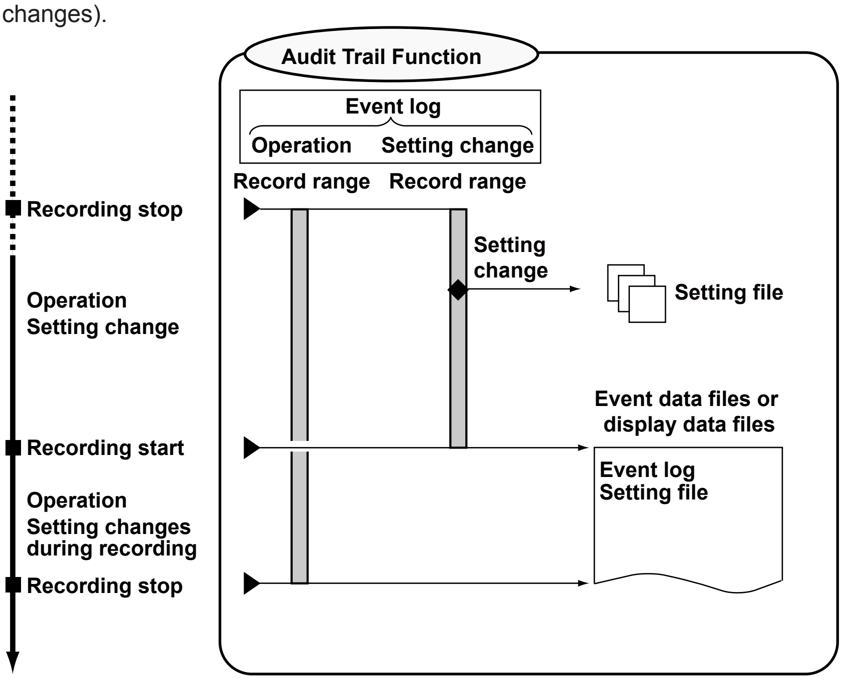
Note

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

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 (event data or display 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 GM.

1.5.2 Event Log

The event log records operations and setting changes on the GM 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.
- Operations from the Web application, operations via communication (Ethernet communication, serial communication, USB communication, Bluetooth com), operations through remote control, operations through the event action function, and auto operation by the GM (error messages and the like) can be distinguished.
  * Serial communication, USB communication, and Bluetooth communication are not distinguished.
  ▶ See appendix 1, "Event Log Contents," on page App-1.
- Operations that do not affect the measured data, such as Web application screen switching and display configuration changes, are not recorded.
  ▶ For details, see section Appendix 1.

How the Event Log Is Saved

- The GM can record up to 3000 operations per data file 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 (event or display 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 view the event logs in the internal memory on the Web application.
  The Web application can display only the most recent 2000 events from a given event log.
- You can view event logs in measurement data files on Universal Viewer.
  ▶ See the Universal Viewer Manual.

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 GM 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 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 GM to automatically write into the measured data a message indicating that the settings have changed. The GM does not save a setting file.

Logged Operations (Settings that can be changed during recording)

The following setting changes can be logged during recording.

Setup Item	
Alarm settings	On/Off
	Type
	Value
	Hysteresis
	Logging
	Output type
	Output No.
	Alarm delay
Calibration correction	Mode
	Number of set points
	Input value (1 to 12)
	Output value (1 to 12)
Data save settings	Save directory
Communication (Ethernet) settings	Recipient 1
	Recipient 2
	Sender
	Subject
User settings	User level
	User name
	User ID
	Password
	Password expiration
	User property On/Off
	Authority number
	Sign in property On/Off
	Authority of sign in

Writing Change Messages

You can configure the GM 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
	Number of set points	
	Input value (1 to 12)	
	Output value (1 to 12)	

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

Setting Changes during Recording

You can change the following settings and perform the file operations during recording. Administrators can perform all operations. Users can only perform operations that have been permitted.

Setting Changes

See “Event Log and Setting File When Recording Is in Progress.”

1.5.6 SET0 Directory Operations

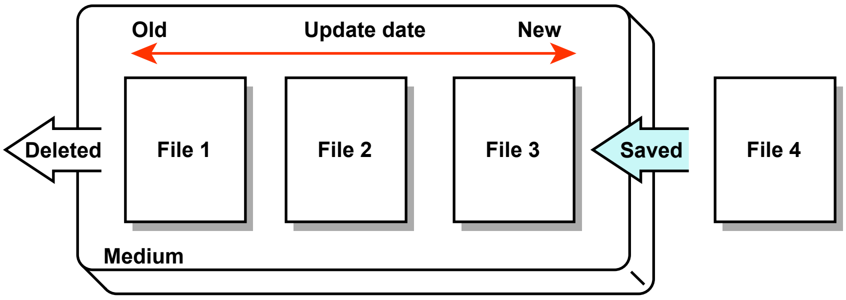
Save Operation (When not using media FIFO)

If there is not enough free space on the SD memory card, the GM 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 GM continuously without having to replace the SD memory card.
▶ For the setting procedure, see section 2.10.2, "Setting the Save Method to Media (Auto save or manual save) and Media FIFO."

- **Operation**



If there is not enough space to save a new file, the GM 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. Measurement data files created with the advanced security function contain an area for including approval information. This enables measurement data files saved in an external storage medium or the like to be signed.
Universal Viewer is used to sign measurement data files. This is not possible from the GM.
▶ Universal Viewer manual
Signature is possible only by a user with signature privileges who is registered in the login information of that measurement data file.

Approval information that can be included

- 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.

1.6.1 Signable Files

Event and display data files (.GSE and .GSD 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	Description
Batch	Measured data from when recording is started until it is stopped is managed as a batch. You cannot sign unless all the measurement data files from when recording is started until it is stopped are present. Measured data can be a single file or multiple files. If measured data is stored in multiple files, the files are linked using Universal Viewer and then signed.
File	Measured data is recorded continuously from when recording is started. You can sign each measurement data file.

“Batch” is useful when you are dealing with a process such as one in which recording starts and stops in accordance with production.
“File” is useful when you are dealing with a continuously operating process, such as the monitoring of the air conditioning temperature.

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 event or display 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.
- Monitor users cannot sign measurement data files.

Deleting and Changing Approval Information

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

1.7 Advanced Security Limitations

If the advanced security function is enabled, the following limitations are applied to the standard functions. If the advanced security function is disabled, the standard functions will be available.

Item		When Advanced Security Is Disabled (when using standard functions)	When Advanced Security Is Enabled
Number of user registrations		50	100
Number of event logs		50	3000
File type		Event data, display 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)		Yes	No
Web application		Monitor, configure, operate	Monitor, configure, operate (Monitor users can only monitor.)
FTP server feature	Output the external storage medium list	Yes	Yes (monitor users only)
	Transfer files stored in the external storage medium	Yes	Yes (monitor users only)
	Write files to the external storage medium	Yes	No
	Delete files stored on the external storage medium	Yes	No
	Output the internal memory list	Yes	Yes (monitor users only)
	Transfer files stored in the internal memory	Yes	Yes (monitor users only)
Load setting parameters		Load passwords of registered users	Except for monitor users, passwords of registered users cannot be loaded. Administrator and user passwords are set to their default passwords.
Key lock function		Available	Not available (when the communication login function is in use)
Setting changes during recording		There are limitations on the settings that you can change during recording.	There are limitations on the settings that you can change during recording. For an explanation, see section 1.5.5.
Automatic writing of messages when the settings are changed during recording		Not available	You can automatically write a message when the settings are changed during recording.
Data file format		Binary format, text format	Binary format only. The data is encrypted.
Main unit key operation		Yes	When communication security is set to Login, the following operations cannot be performed from the main unit keys. • Start recording and computation using the START key • Stop recording and computation using the STOP key • Event action operation using the USER1 and USER2 keys

2.1 Registering Users and Setting the Signature Method

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

By default, the GM is configured so that you can operate it without logging in. First, register an administrator (Admin). After you register an administrator, a user, or a monitor user and change communication security to Login, you will have to log in before you can use the GM.

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

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

Before configuring Security basic settings, configure User settings, User property, and the like. If you change the settings, the page will be reloaded, and you will have to log in.

Path

Web application: **Setting** tab > **Security settings** > **Security basic settings**
Hardware configurator: **Security settings** > **Security basic settings**

Description

Security function

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

Communication

To apply Web application and communication access security, set this to **Login**.
When you change communication security to **Login**, you will have to log in before you can use the GM.

Options	Description
Off	Disables the security function
Login	Allows only registered users to access the GM via Web application and communication

Logout

Setup Item	Selectable Range or Options	Default Value
Auto Web Logout*	Off/10min/20min/30min	Off

* This is enabled when Communication of the security function is set to Login.

Auto Web Logout

Options	Description
Off	Stays logged in until the user logs out.
10min to 30min	When you log in through the Web application, you will be automatically logged out when there is no operation for the specified duration.

- Use the Timeout function to set the auto logout for Ethernet communication and FTP server.
  ▶ See section 2.17.7, “Configuring the Server Function,” in the User’s Manual.
- Use Logout to set the auto logout for serial communication.
  ▶ See section 2.18.1, “Setting Basic Communication Conditions,” in the User’s Manual.
- Set the USB communication using auto logout.
  ▶ See “USB Communication Auto Logout [GM]” in the Communication Command Manual.
- Set the Bluetooth communication using timeout.
  ▶ See “Bluetooth Communication Timeout (/C8) [GM]” in the Communication Command Manual.

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)	-

* This is enabled when Communication of the security function is set to Login.

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 3.1.2, “Testing the KDC Server Connection”.

Note

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

If changed to On, user authentication and page reload will take place. You need to perform authentication with the KDC server to configure User settings and User property.

If the KDC server is not configured correctly, you will not be able to log in.

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 GM, 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

* This is enabled when Communication of the security function is set to Login.

Password retry

Set the total number of failed password-entry attempts that results in user invalidation.
For example, if this is set to 3, one failure on the Web application and two failures through communication will invalidate the user.

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

* This is enabled when Communication of the security function is set to Login.

On/Off

Set whether to use user IDs for users to be registered.

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.

▶ For the default user ID and password values, see section 2.2.1, “Logging In,” on page 2-11.

Web Security*

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

* This is enabled when Communication of the security function is set to Login.

Session Security

Session management is performed while logged in to the Web application.
Set whether to enhance security against session spoofing and the like
Normally, set this to On.

Options	Description
Off	Session management security is not enhanced.
On	Session management security is enhanced.

Note

Users whose user settings have changed are automatically logged out.

2.1.2 Registering Users

Path

Web browser: **Config.** tab > **Security settings** > **User settings**
Hardware configurator: **Security settings** > **User settings***

Description

User No.

Displays the user registration number (1 to 100).

User settings

Setup Item	Selectable Range or Options	Default Value
User level	Off/Admin/User/Monitor	Off
Mode	Communication	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	Initialize	—
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 Disabled when the user level is Monitor.
*3 Enabled when User property is set to On.
*4 Enabled when Sign in property is set to On.
*5 Does not appear when the user ID is disabled in Security basic settings.

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 GM.

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
Communication	You can log in to the GM via Web application and communication.

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

To initialize the password, select the **Initialize** check box. To cancel initialization, click **Cancel**.

▶ For the default value, see section 2.2.1, “Logging In”.

Note

The password is set the first time you log in.
However, for monitor users, because there is no changing of the default password, this feature is unavailable.

▶ See section 2.2.1, “Logging In,” on page 2-11.

Password expiration

Options	Description
Off	The password will not expire.
1 month, 3 month, 6 month	The GM 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 2.1.3, “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 2.1.5, “Setting Signature Restrictions”.

2.1.3 Setting User Properties

Path

Web application: **Config.** tab > **Security settings** > **Authority of user**
Hardware configurator: **Security settings** > **User property***

Description

Authority number

Displays the authority number (1 to 10) 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
Time set	Free/Lock	Free
Setting operation	Free/Lock	Free
Calibration correction	Free/Lock	Free
External media	Free/Lock	Free
System operation	Free/Lock	Free
Output operation	Free/Lock	Free

Record

Set this to **Lock** to restrict record start/stop operation.

Math

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

Operation
Math start
Math stop
Math reset
Math ACK

Data save

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

Operation
Save event data
Save display data
Manual sample
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
Printer output test
KDC test
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 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
Create self-signed certificates
Create certificate requests
Display certificates, delete certificates
Install certificates, install intermediate certificates
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.

2.1.4 Configuring the Sign in Settings

Path

Web application: **Config.** tab > **Security settings** > **Sign in settings**
Hardware configurator: **Security settings** > **Sign in settings**

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.
Use Universal Viewer to sign.

Options	Description
Batch	You can sign a collection of all the measurement data files from the start to stop of a recording.
File	You can sign each individual measurement data file.

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.

2.1.5 Setting Signature Restrictions

Path

Web application: **Config.** tab > **Security settings** > **Sign in property**
Hardware configurator: **Security settings** > **Sign in property**

Description

Authority of sign in

Displays the authority of sign in (1 to 8) 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.

2.1.6 Comment Input Function for Setting Changes

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

Path

Web application: **Config.** tab > **System settings** > **Setting file**
Hardware configurator: **System settings** > **Setting file**

Description

Setting file

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.

The Update configuration dialog box appears when you change the settings. The comment text box displays the content set in Setting file comment.
The comment that you enter is set in Setting file comment.

2.1.7 Activating Modules (for module swapping)

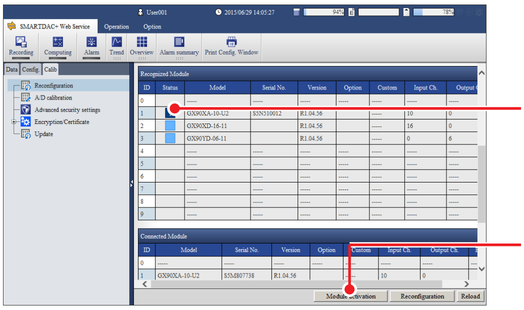
If you replace a module with another module (same type) after system reconfiguration, you need to activate the module or else the measured data will result in errors. If the identified module is different from the actual module, you can activate the module from the System reconfiguation screen.

If there are modules that need to be activated, the **Module activation** button becomes available. Only administrators and users with system operation privileges can perform this operation.

Procedure

1. Click the Config. tab and then Reconfiguration.

2. Click **Module activation**.
 The Module activation screen appears.



Recognized Module

ID	Status	Model	Serial No.	Version	Option	Custom	Input Ch.	Output
0		-----	-----	-----	-----	-----	-----	-----
1	■	GX90XA-10-U2	S5N510012	R1.04.56		-----	10	0
2	□	GX90XD-16-11		R1.04.56		-----	16	0
3	□	GX90YD-06-11		R1.04.56		-----	0	6
4		-----	-----	-----	-----	-----	-----	-----
5		-----	-----	-----	-----	-----	-----	-----
6		-----	-----	-----	-----	-----	-----	-----
7		-----	-----	-----	-----	-----	-----	-----
8		-----	-----	-----	-----	-----	-----	-----
9		-----	-----	-----	-----	-----	-----	-----

Connected Module

ID	Model	Serial No.	Version	Option	Custom	Input Ch.	Output Ch.
0	-----	-----	-----	-----	-----	-----	-----
1	GX90XA-10-U2	S5M807738	R1.04.56		-----	10	0

Icon that indicates that the module needs to be activated

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

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

4. Click **OK**.

Operation complete

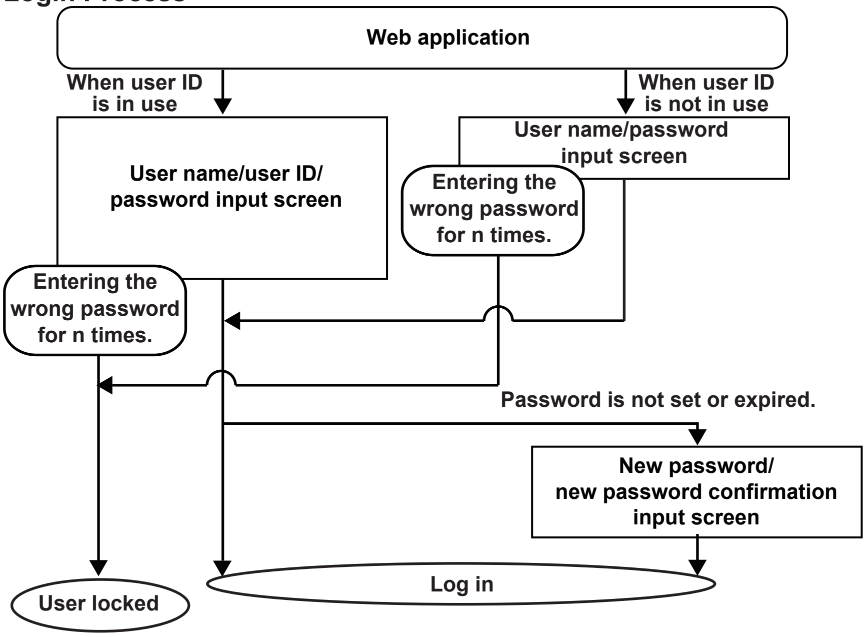
Note

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.

2.2 Logging In and Out

When you log in for the first time, you will be prompted to change the password.
When the password management function is enabled, see section 3.2.1, “Logging In and Out,” on page 3-9.
▶For information about the function, see section 1.3, “Login Function”.

Login Process


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

2.2.1 Logging In

Procedure

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

1. Start the Web application.
A login dialog box appears.

If user ID is enabled, user name, user ID, and password input boxes are displayed.
If user ID is disabled, user name and password input boxes are displayed.

2. Enter the user name, user ID (when enabled), and password (default password), and click Login.
A Password change dialog box appears (except for monitor users).

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

3. Set a new password in **New Password** and **New Password Again**, and then click **Password change**.
You will be logged in.

Operation complete

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.

When a Password Is Already Set

1. Start the Web application.
   A login dialog box appears.

   If user ID is enabled, user name, user ID, and password input boxes are displayed.
   If user ID is disabled, user name and password input boxes are displayed.

2. Enter the user name, user ID (when enabled), and password, and click **Login**.

   You will be logged in.

Operation complete

When the Password Is Expired

A Password change dialog box 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. Click the **Option** menu.
   A menu appears.

2. Click **Password change**.
   A Password change dialog box appears.

3. Enter the appropriate values in Old Password, New Password, and New Password Again, and click **Change**.

   The password will be changed.

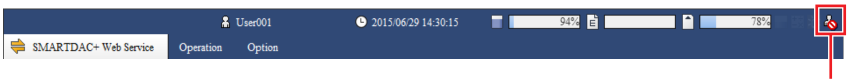
Operation complete

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.
If user lock out occurs in A/D calibration mode, key creation mode, or update mode, the user is logged out. After being logged out, the user can log back in.



User locked icon

Note

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

Icon that appears when all administrators have been locked out:	🚫

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.

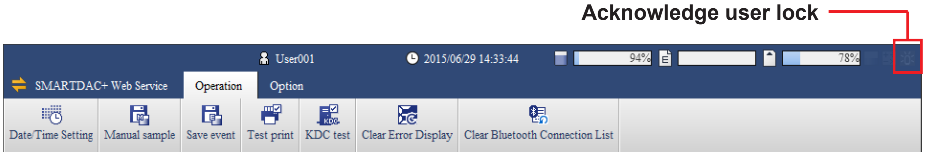
Clearing the User-Locked Icon (Only administrators can perform this operation)

1. Log in as an administrator.

2. Click the **Operation** menu.
   A tab menu appears.

3. Click **User Locked ACK** and then **Acknowledge user lock**.
   The user-locked icon is cleared.

Acknowledge user lock



Operation complete

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 2.1.2, "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.
   ▶See section 2.2.1, "Logging In," on page 2-11.

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 2.17.3, “Configuring the SMTP Client Function,” and section 2.17.4, “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 2.5, “Configuring DO Channels (Digital output channels)” in the User’s Manual.
▶ For the setting procedure, see section 2.15, “Configuring 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

Actions that cannot be triggered by a user lock out event

Event Type	Action Type
Device state “user lock out”	Adjust the time
	Start/stop recording
	Start/stop computation
	Start recording
	Stop recording
	Start computation
	Stop computation
	Reset computation
	Manual sample
	Alarm ACK
	Save display data
	Save event data
	Reset the relative timer
	Load settings
	Save settings

Logging in to A/D Calibration Mode

To switch to A/D calibration mode, the logged-in user must be authenticated.
If the communication login function is disabled, a password can be set.

▶ See section 5.1.3, “Performing A/D Calibration and Adjusting the Input Accuracy,” in the User’s Manual.

1. Click the **Config.** tab and then **A/D calibration**.
   A screen for switching to the A/D calibration mode appears.

2. Click **Next**.
   A Mode Switching dialog box appears.

3. Click **OK**.
   The GM restarts, and the Login dialog box appears.

4. The name of the user logged in appears in User Name. Enter the user ID (when enabled) and password, and click **Login**.
   The GM switches to A/D calibration mode.

Operation complete

▶ For instructions on how to use A/D calibration mode, start reading from step 4 under “Adjusting the Input Accuracy” 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.

User Invalidation (User lock out)

If a user lock out occurs while switching to A/D calibration mode, follow the procedure below to switch to A/D calibration mode again.

1. Log in using another valid user account.
   An A/D calibration mode dialog box appears.

2. Click **Exit current mode**.
   A Mode Switching dialog box appears.

3. Click **OK**.
   A Login dialog box appears.

4. Log in using another valid user account.
   A Mode Switching dialog box appears.

5. Click OK.

   Switch to calibration mode again, and perform calibration.

Operation complete

To restore a user that has been locked out, perform User Locked ACK and clear the invalid user.
Only administrators can perform these operations.

▶ For operating instructions, see “User Invalidation (User lock out) and Handling” described earlier.

Ending A/D Calibration Mode

When you end A/D calibration mode, a login dialog box appears. Enter the user ID (when enabled) and password, and click Login. The normal operation display returns, and a Mode Switching dialog box appears. If you click OK, you can resume operation.

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	Communication

Alarm Confirmation When Recording is Stopped

If Indicator in Alarm basic settings is set to **Hold** when recording is stopped, an alarm confirmation warning message appears if there are any alarms that have not be acknowledged.
Clicking **OK** will clear the message, and you will be able to stop recording.

2.2.2 Logging Out

Logging Out of the Web Application

1. On the **Option** tab, click **Logout**.
   A logout dialog box appears.

2. Click **OK**.
   A Login user changed dialog box appears.

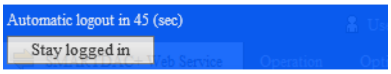
3. Click **OK**.
   The user is logged out, and a login dialog box appears.

Operation complete

Auto Logout

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

On the Web application, a logout dialog box appears about 60 seconds before the auto logout time.
Clicking **Stay logged in** continues the logged in condition.



Automatic logout in 45 (sec)

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), USB communication, Bluetooth communication, DARWIN compatible communication (Ethernet communication, serial communication)	Execute the logout communication command (Clogout).

Note

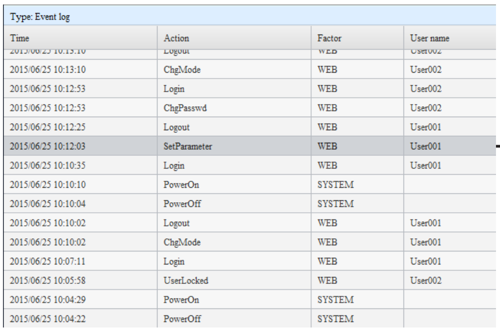
When a user is logged in through the Web application, if the communication between the GM and Web application is disconnected for 60 seconds, the GM automatically logs the user out regardless of the auto web logout function.

2.3 Viewing the Event Log

Procedure

1. Click the **Data** tab of SMARTDAC+ Web Service.

2. Click **Log** and then **Event log**.
The event log appears.
Double-click an event to display detailed information.

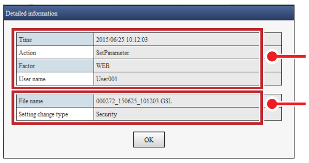


Type: Event log

Time	Action	Factor	User name
2015/06/25 10:13:10	Logout	WEB	User002
2015/06/25 10:13:10	ChgMode	WEB	User002
2015/06/25 10:12:53	Login	WEB	User002
2015/06/25 10:12:53	ChgPasswd	WEB	User002
2015/06/25 10:12:25	Logout	WEB	User001
2015/06/25 10:12:03	SetParameter	WEB	User001
2015/06/25 10:10:35	Login	WEB	User001
2015/06/25 10:10:10	PowerOn	SYSTEM	
2015/06/25 10:10:04	PowerOff	SYSTEM	
2015/06/25 10:10:02	Logout	WEB	User001
2015/06/25 10:10:02	ChgMode	WEB	User001
2015/06/25 10:07:11	Login	WEB	User001
2015/06/25 10:05:58	UserLocked	WEB	User002
2015/06/25 10:04:29	PowerOn	SYSTEM	
2015/06/25 10:04:22	PowerOff	SYSTEM	

User name
Operation method
Operation
Date and time

Double-click an event to display the details.



Detailed information

Time	2015/06/25 10:12:03
Action	SetParameter
Factor	WEB
User name	User001
File name	000272_150625_101203.GSL
Setting change type	Security

OK

Common items

Details

Common items
Time: When the event was recorded
Action: Description
Factor: Event type
User name: Name of the user operating

Details
Item of each event
Data time

For details, see the event log list in appendix 1.

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

3. Click **OK** to close the detailed information dialog box.

Operation complete

2.4 Customizing the Monitor Tree Display on the Web Page

With the advanced security function, the Monitor user level becomes available in addition to the User user level.

The Monitor user level is the same as the User user level except that Save/Load does not appear regardless of the File setting.

▶ See section 2.17.10, “Web content selection,” in the User’s Manual.

2.5 Disabling the Advanced Security Function

You can disable the advanced security function. If you disable the advanced security function, the functions that you can use on the GM are the same as those of the standard product.

Note

Note that if the advanced security function is disabled, the GM cannot comply with US FDA 21 CFR Part 11.
By factory default, the advanced security function is enabled on a GM with the advanced security function (/AS). You need to carry out the procedure explained here only if you want to use the GM as a standard product, without the advanced security function.

If you change the advanced security settings, all data including recorded data will be initialized, and the GM 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 GM).

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

Web browser: **Config.** tab > **Advanced security settings**
Hardware configurator: **System** tab > System config > **GM10** tab > **Option detail**

Description

Advanced Security Setting

Advanced security function On/Off (Hardware Configurator)

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

On/Off

Set this to **Off** to disable the advanced security function.
By factory default, the advanced security function is enabled on a GM with the advanced security function (/AS).
If you change this setting, all data including recorded data will be initialized, and the GM will restart.

Security settings cannot be changed while recording or computation is in progress.

Note

If you change the advanced security settings, all data including recorded data will be initialized. You will also need to set the IP address and measurement conditions, perform reconfiguration, and so on.

Setting a Password for the Advanced Security Settings

Click Password settings, and set On/Off to On.
Enter the old password and the new password twice, and then click Change.

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

On/Off

Set this to **On** to enable the advanced security function.
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.

Old Password

Set the old password (default value: default).

New Password

Set the new password.

New Password Again

Enter the new password again for confirmation.

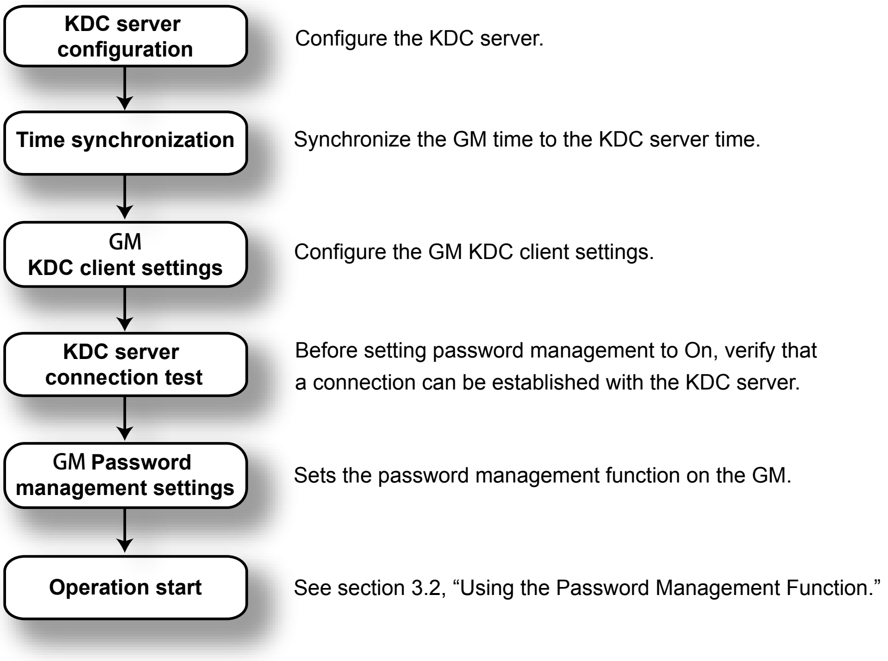
Note

- Make sure you do not forget the password. If you do, you will not be able to change the advanced security settings.
- Characters that cannot be used in passwords: SP (space) ' ; DEL (7f)

3.1 Configuring the Password Management Function

Configuration Flowchart

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


KDC server configuration
Configure the KDC server.
Time synchronization
Synchronize the GM time to the KDC server time.
GM KDC client settings
Configure the GM KDC client settings.
KDC server connection test
Before setting password management to On, verify that a connection can be established with the KDC server.
GM Password management settings
Sets the password management function on the GM.
Operation start
See section 3.2, “Using the Password Management Function.”

Terminology

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

3.1.1 GM KDC Client Settings

You need to specify the following GM KDC client settings.

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

DNS settings

Configure the DNS settings if necessary.

▶ See section 2.17.1, “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 GM must be synchronized. Configure the SNTP client function so that synchronization is maintained using an SNTP server on the network.

▶ See section 2.17.5, “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 GM and the KDC server.
- Set the DST (daylight saving time) and time zone correctly. For the setting procedure, see section 2.21.4 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

Web application: **SMARTDAC+ Web Service** tab > **Config.** > **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, Aa#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 GM 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 GM 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 GM 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 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. On the **Operation** tab, click **KDC test**.
   A KDC test dialog box appears.

2. Enter the user name and password, and click **Execute a KDC test**.
   The result of the connection test is displayed.

Operation complete

3.1.3 Setting the GM Password Management Function

Password management, root user password

Enables the password management function. Set the password of the emergency root user. Before setting password management to On, register users. If there are no users that the KDC server will manage, you will not be able to log in to the GM.
▶ See section 2.1.1, “Configuring the Security Function, Logout, Password Management Function, Etc.,” on page 2-1.

User settings

Specify operation modes, user names, and restrictions for each user.
▶ See section 2.1.2, “Registering Users,” on page 2-4.

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

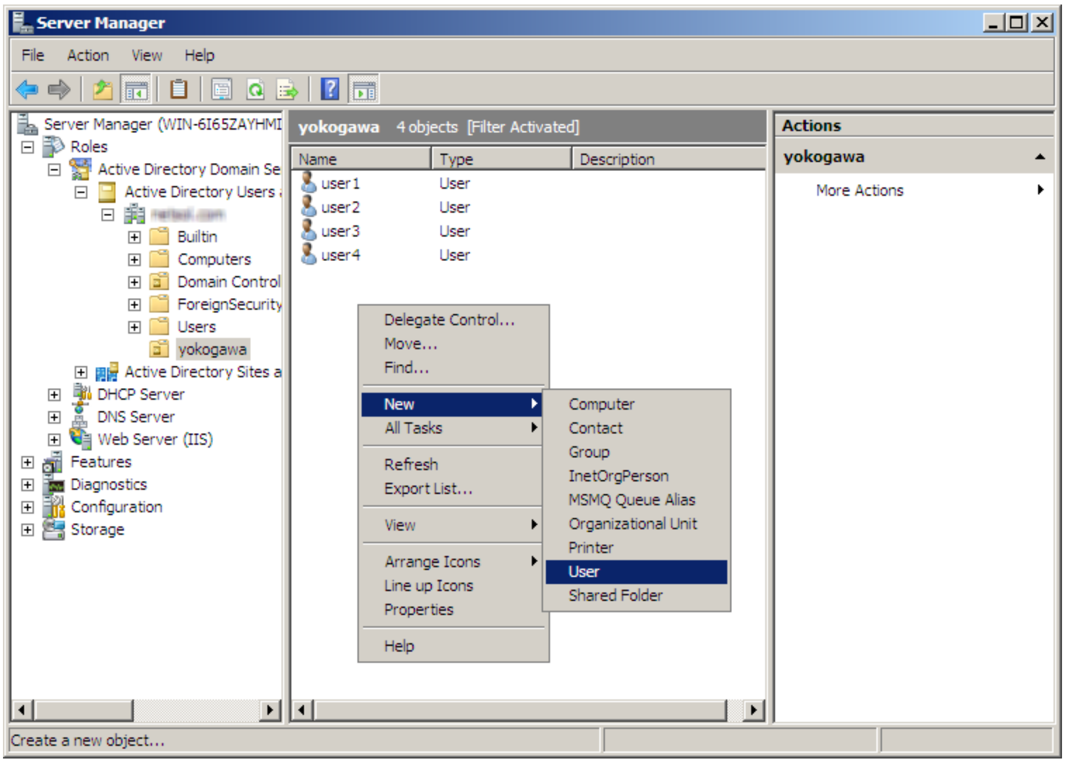
Item	Registration Name	Password
Host name	gm	record-as1

*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).

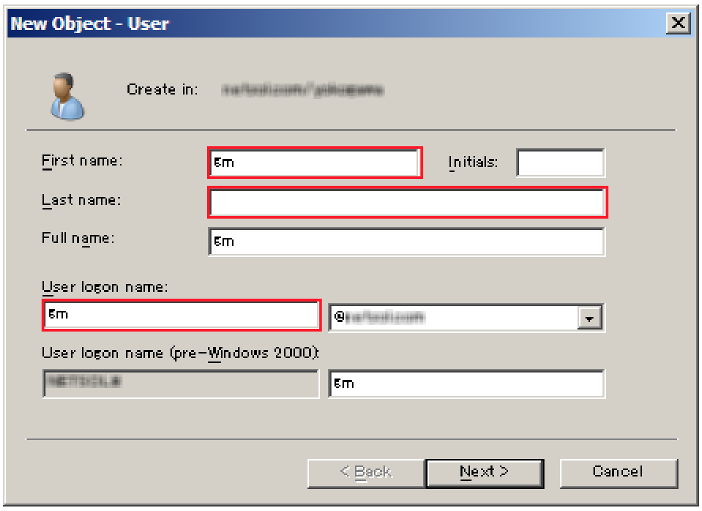
Creating a GM Host Account

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



Name	Type	Description
user1	User	
user2	User	
user3	User	
user4	User	

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



Create in: [illegible]

First name: gm

Initials:

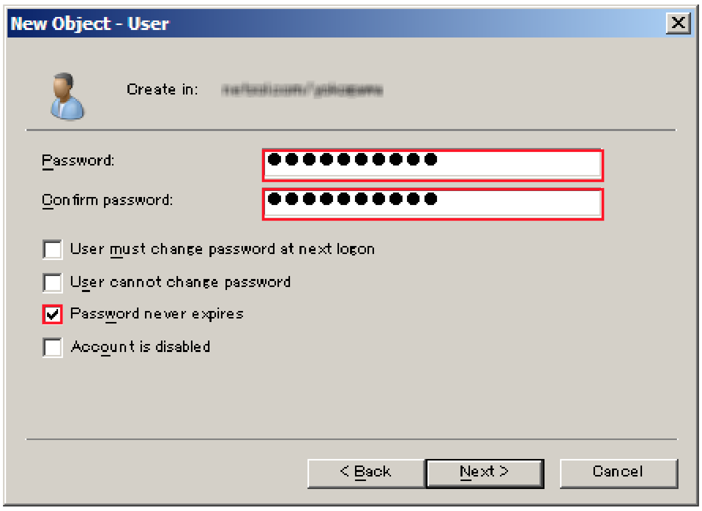
Last name:

Full name: gm

User logon name: gm @[illegible]

User logon name (pre-Windows 2000): [illegible] gm

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



Create in: [illegible]

Password: ●●●●●●●●●●

Confirm password: ●●●●●●●●●●

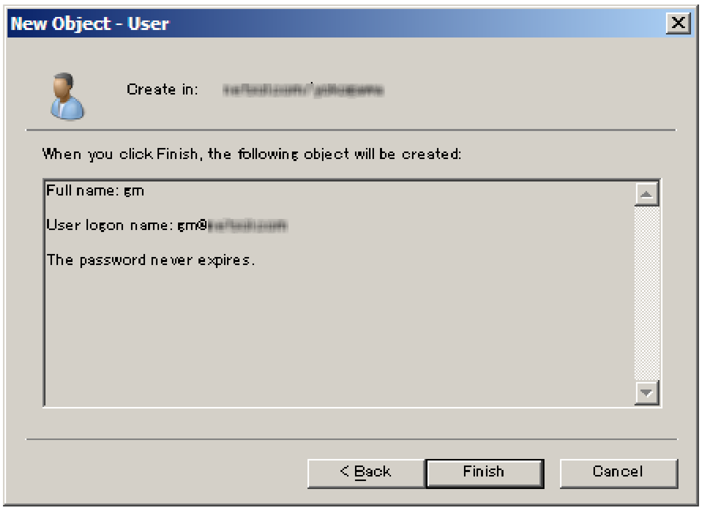
□ User must change password at next logon

□ User cannot change password

☑ Password never expires

□ Account is disabled

4. Click **Finish**.



Create in: [illegible]

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

Full name: gm

User logon name: gm@[illegible]

The password never expires.

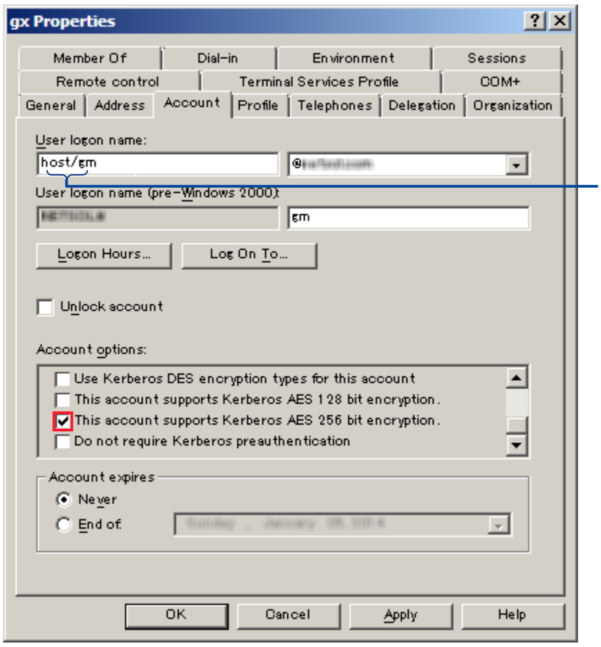
Changing the Properties of the Created Host Account

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.



gx Properties

Member Of | Dial-in | Environment | Sessions | Remote control | Terminal Services Profile | COM+ | General | Address | Account | Profile | Telephones | Delegation | Organization

User logon name:

host/gm | [redacted]

User logon name (pre-Windows 2000):

[redacted] | gm

Logon Hours... | Log On To...

□ 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

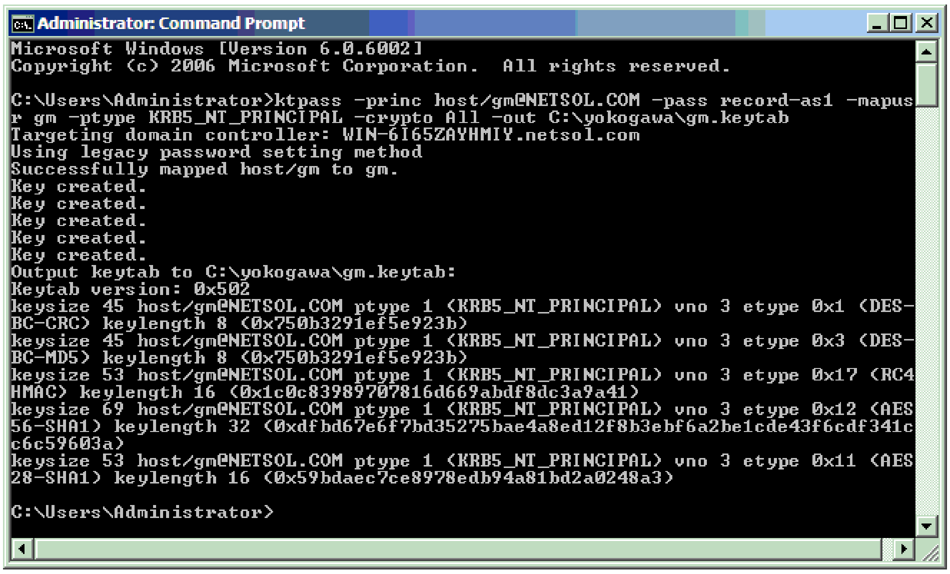
● Never
○ End of: [redacted]

OK | Cancel | Apply | Help

“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/gm@(the realm name that you are using) -pass record-as1 –mapuser gm –ptype
KRB5_NT_PRINCIPAL –crypto All –out C:\yokogawa\gm.keytab
A file named gm.keytab is created in the C:\yokogawa folder.



Administrator: Command Prompt

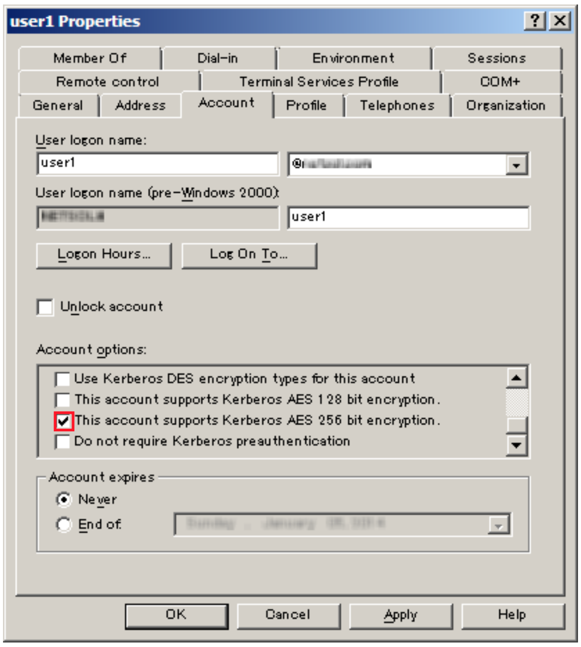
```
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>ktpass -princ host/gm@NETSOL.COM -pass record-as1 -mapus
r gm -ptype KRB5_NT_PRINCIPAL -crypto All -out C:\yokogawa\gm.keytab
Targeting domain controller: WIN-6I65ZAYHMIY.netsol.com
Using legacy password setting method
Successfully mapped host/gm to gm.
Key created.
Key created.
Key created.
Key created.
Key created.
Output keytab to C:\yokogawa\gm.keytab:
Keytab version: 0x502
keysize 45 host/gm@NETSOL.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x1 (DES-
BC-CRC) keylength 8 (0x750b3291ef5e923b)
keysize 45 host/gm@NETSOL.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x3 (DES-
BC-MD5) keylength 8 (0x750b3291ef5e923b)
keysize 53 host/gm@NETSOL.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x17 (RC4
HMAC) keylength 16 (0x1c0c83989707816d669abdf8dc3a9a41)
keysize 69 host/gm@NETSOL.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x12 (AES
56-SHA1) keylength 32 (0xdfbd67e6f7bd35275bae4a8ed12f8b3ebf6a2be1cde43f6cdf341c
c6c59603a)
keysize 53 host/gm@NETSOL.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x11 (AES
28-SHA1) keylength 16 (0x59bdaec7ce8978edb94a81bd2a0248a3)

C:\Users\Administrator>
```

Creating a User Account in Active Directory and Changing the Properties

Create a GM 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 GM 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/gm@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		gm
ptype		KRB5_NT_PRINCIPAL		KRB5_NT_PRINCIPAL
out		Output folder name\file name.keytab		c:\temp\gm.keytab

Mapping Example

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

GM Configuration

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

Item	Description
Host principal	gm
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. Start the Web application.
   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.
The root user is valid only when no users can be authenticated such as when the connection to the KDC server is broken.

Logging Out

▶ For operating instructions, see section 2.2.2, “Logging Out,” on page 2-16.

3.2.2 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 2.2.1, “Logging In,” on page 2-11.

Note

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

3.2.3 Password Expiration

Manage passwords and their expiration dates on the KDC server.
You cannot change passwords on the GM. Logging in is not possible when the password is expired.

Note

When preauthentication is not being used, users may be able to log in to the GM even after the password has expired.
We recommend that you use the preauthentication function.

Blank

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
User locked ACK	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
Snapshot	Snapshot	
Batch number setting	BatNoSet	
Lot number setting	LotNoSet	
Batch text field setting	TextFieldSet	Text field number
Display update rate change	ChgRate	Trend interval
Timer reset	TimerRST	Timer number
Match time timer reset	MTimerRST	Timer number
Communication channel writing (GM operation only)	WriteComm	Channel number/value Write type
DO channel writing (for manual operation)	WriteDO	Channel number/Status
SW writing (for manual operation) (GM, communication, serial)	WriteSW	Internal switch number/Status

Continued on next page

Operation	Display (English)	Details
Settings save	Save########	########: Report: Report template Scale: Scale image Custom: Custom display Parameter: Setting parameter Cert: Certificate All: All settings For details, see below.
Report save	SaveReport	Report format/report type
Scale image save	SaveScale	Group number
Custom display save	SaveCustom	Display number
Parameter save	SaveParameter	—
Certificate save	SaveCert	—
All settings save	SaveAll	—
Settings load	Load########	########: Report: Report template Scale: Scale image Custom: Custom display Parameter: Setting parameter Cert: Certificate All: All settings For details, see below.
Report load	LoadReport	Report format/report type
Scale image load	LoadScale	Group number
Custom display load	LoadCustom	Display number
Parameter load	LoadParameter	Setting type (security, IP address, other, communication (server settings), calibration correction settings, device information settings)
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	—
initialization	Initialize	Initialize type (security settings, settings other the security, communication (IP address), communication (server settings), calibration correction settings, device information settings, internal data)
Sign in	Sign In	Sign in level File name
Key lock	Key lock	—
Key lock release	Key lock release	—
Bluetooth function on	Bluetooth function on	—
Bluetooth function off	Bluetooth function off	—
Bluetooth connection list clear	Bluetooth connection list clear	—
Fixed IP address mode	Fixed IP address mode	—
Unsaved data save	Unsaved data save	—
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)

Continued on next page

Operation	Display (English)	Details
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)
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
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

Operation property

Factor	Description
OPERATE	GM key operation
Web	Operation through the Web application
COMMU	Operation via communication (including Web)
SERIAL	Operation via serial communication, USB communication, Bluetooth 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 GM

User Name

Factor	User Name
OPERATE	No user
Web	User logged in through the Web application
COMMU	User logged in via communication (Ethernet)
SERIAL	User logged in via serial communication, USB communication, Bluetooth communication
EXTERNAL	No user
PC	User logged in via PC
REMOTE	No user
ACTION	No user
SYSTEM	No user

Appendix 2 Error Messages and Corrective Actions

This section introduces the main error messages that occur with the advanced security function.
For other error messages, see section 5.2.1, “Messages,” in the User’s Manual.

Errors That Occur during Authentication

Code	Message	Description and Corrective Action
251	Invalid user name or password.	Enter the correct name or password.
252	The login password is incorrect.	Check the password. If the password is lost, the password must be initialized by an administrator.
261	Wrong user ID or password.	Enter the correct user ID and password.
265	Login inputs are incorrect.	Enter the correct login information.
272	This password became invalid.	On the GM, because the wrong password has been entered for more than the permissible number of times, this user is invalid.
273	Invalid user.	The account has been invalidated on the server. The account has been invalidated on the GM.
E8001	A communication error has occurred.	Unable to finish processing because Ethernet communication with the GM failed. Example: The communication is disconnected during login authentication. Check the communication environment.
E8008	Password entered is incorrect.	The passwords entered for the new password and confirmation do not match when changing the password at login. Enter the same character string for both.
E8009	This function is not possible now.	1. The GM login settings (such as the user ID on/off setting) have been changed from elsewhere. Enter the login information again. 2. Communication error. If the standby display persists, try the corrective action for 8001.
760	Invalid KDC client configuration.	Set the host principal or realm name.
763	Not supported by this machine.	Not supported by the GM.
764	Preauthentication failed.	Enter the correct password. Also, make sure that the times on the GM and the server match.
765	The encryption type is not supported by this machine.	The GM does not support the encryption type, or the encryption type settings on the GM and the server are different. Use the same encryption method on the GM and the server.
766	Failed to receive authentication from KDC server.	Check the GM and server settings. Also, make sure that the times on the GM and the server match.
767	Change the password.	Change the password. Change the password of the user account that is registered on the server.
768	The time difference with the KDC server exceeds the limit.	There is a time difference of 5 minutes or more between the GM and the server. Synchronize the GM time to the time on the server.
770	The host principal is not registered.	The host account is not registered on the server.
771	The host principal is invalid.	Check the host account that is registered on the server.
772	The host password is incorrect.	Make sure that the GM authentication-key password and the server’s host-account password match.
773	Preauthentication failed.	An internal error occurred during preauthentication. Disable the server’s preauthentication function.
774	The realm is incorrect.	Make sure that the realm name setting on the GM is correct.

Errors That Occur during Communication

Code	Message	Description and Corrective Action
761	Cannot find KDC server.	The KDC server cannot be found in the same domain.
762	KDC server connection error.	An error occurred while the GM was connecting to the KDC server. Make sure that the network connection is not broken.

Other Messages

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