OMRON

CIDRW SYSTEM

V640 SERIES

AMPLIFIER UNITS ETHERNET TYPE

USER'S MANUAL

AMPLIFIER UNITS
V640-HAM11-ETN-V5
V640-HAM11-L-ETN-V5

CIDRW HEADS
V640-HS61
V640-HS62

NOTE

- All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, mechanical, electronic, photocopying, recording, or otherwise, without the prior written permission of OMRON.
- No patent liability is assumed with respect to the use of the information contained herein.
  Moreover, because OMRON is constantly striving to improve its high-quality products, the information contained in this manual is subject to change without notice.
- Every precaution has been taken in the preparation of this manual. Nevertheless, OMRON assumes no responsibility for errors or omissions.
  Neither is any liability assumed for damages resulting from the use of the information contained in this publication.

Trademarks

- Microsoft, Windows, Microsoft Edge, Internet Explorer are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.
- Java and other trademarks that contain “Java” are the registered trademarks of Oracle Corporation or its related companies.
- Google Chrome is trademarks or registered trademarks of Google LLC.

Other company names and product names in this document are the trademarks or registered trademarks of their respective companies.

Copyrights

Microsoft product screen shots used with permission from Microsoft.

Introduction

Thank you for purchasing the V640-series CIDRW System. This manual describes the functions, performance, and application methods needed for optimum use of the V640-series CIDRW System.
Allow the V640-series CIDRW System to be installed and operated only by qualified specialists with a sufficient knowledge of electrical systems.
Please read and understand the contents of this manual before using the system.
After reading this manual, store it in a convenient location for easy reference whenever necessary.

Intended Audience

This manual is intended for the following personnel, who must also have knowledge of electrical systems (an electrical engineer or the equivalent).

- Personnel in charge of introducing CIDRW systems.
- Personnel in charge of designing CIDRW systems.
- Personnel in charge of installing and maintaining CIDRW systems.
- Personnel in charge of managing CIDRW systems and facilities.

Applicable Products

This manual covers the following products.

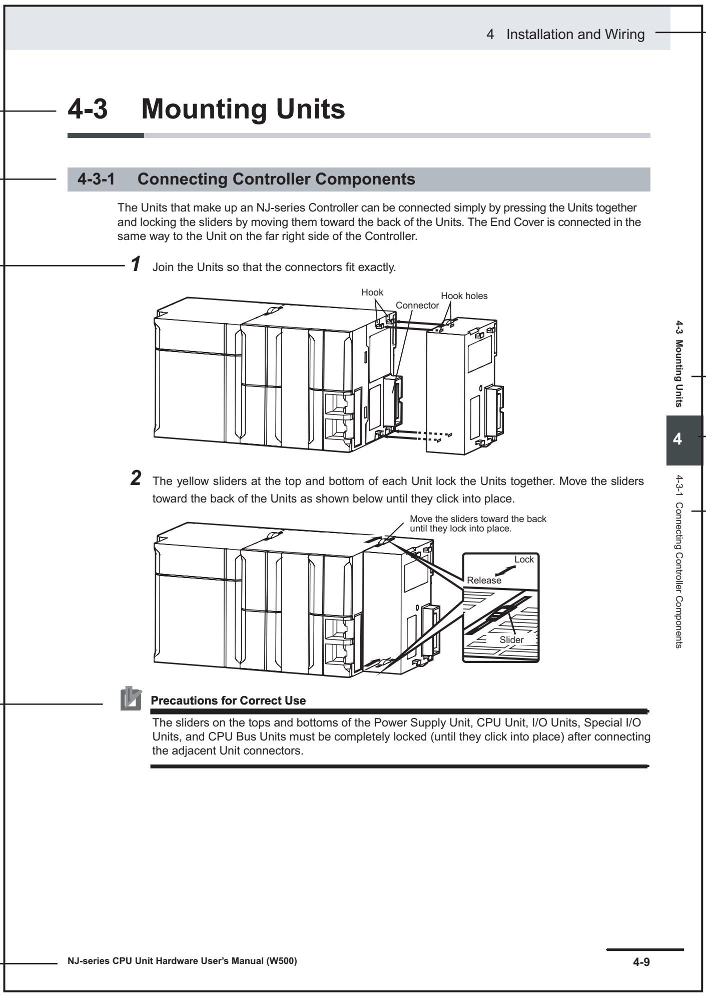
CIDRW System

V640-HAM11-ETN-V5	Amplifier Unit
V640-HAM11-L-ETN-V5	Amplifier Unit
V640-HS61	CIDRW Head
V640-HS62	CIDRW Head

Manual Structure

Page Structure

The following page structure is used in this manual.



4 Installation and Wiring

4-3 Mounting Units

4-3-1 Connecting Controller Components

The Units that make up an NJ-series Controller can be connected simply by pressing the Units together and locking the sliders by moving them toward the back of the Units. The End Cover is connected in the same way to the Unit on the far right side of the Controller.

1 Join the Units so that the connectors fit exactly.

2 The yellow sliders at the top and bottom of each Unit lock the Units together. Move the sliders toward the back of the Units as shown below until they click into place.

Move the sliders toward the back until they lock into place.
Lock
Release
Slider

Precautions for Correct Use

The sliders on the tops and bottoms of the Power Supply Unit, CPU Unit, I/O Units, Special I/O Units, and CPU Bus Units must be completely locked (until they click into place) after connecting the adjacent Unit connectors.

4-3 Mounting Units

4

4-3-1 Connecting Controller Components

NJ-series CPU Unit Hardware User's Manual (W500)

4-9

Level 1 heading

Level 2 heading

Level 3 heading

Gives the current headings.

Page tab

Gives the number of the main section.

Level 2 heading

Level 3 heading

A step in a procedure

Indicates a procedure.

Special information

Icons indicate precautions, additional information, or reference information.

Manual name

Note : This page is a sample for the purpose of describing the page structure. It differs in its actual content.

Icons

The icons used in this manual have the following meanings.

Precautions for Safe Use

Precautions on what to do and what to avoid doing to ensure the safe use of the product.

Precautions for Correct Use

Precautions on what to do and what to avoid doing to ensure proper operation and performance.

Additional Information

Additional information to read as required.
This information is provided to increase understanding or make operation easier.

Version Information

Information on differences in specifications and functionality between versions is given.

Indicator Status

The following symbols are used to show the status of the indicators on the CIDRW Controller and Amplifier Units.

● OFF

◐ Flashing

○ ON

Sections in this Manual

1 Product Outline

2 Installation and Connections/Wiring

3 Preparing for Communications

4 Reading from/Writing to ID Tags

5 Security

6 Web Browser

7 Troubleshooting

A Appendices

I Index

CONTENTS

Introduction 1

Intended Audience 1

Applicable Products 1

Manual Structure 2

Page Structure 2

Icons 3

Indicator Status 3

Sections in this Manual 5

Terms and Conditions Agreement 10

Warranty, Limitations of Liability 10

Application Considerations 11

Disclaimers 11

Statement of security responsibilities for assumed use cases and against threats 12

Safety Precautions 13

Definition of Precautionary Information 13

Meanings of Alert Symbols 13

WARNING 13

Precautions for Safe Use 15

Precautions for Correct Use 16

About installation Site 16

About depositoty Site 16

About wiring 16

About cleaning 16

Power and Ground Cables 16

About the communication range and time 17

About mounting 17

Screw Locking Adhesive 17

Startup Precaution 17

Application Precaution 17

About Transponder made by Texas Instruments Co. 17

The characteristics of the V640-HAM11-(L)-ETN-V2/V640-HAM11-(L)-ETN-V5 17

Revision History 18

Section 1 Product Outline

1-1 What Is a CIDRW System 1-2

1-2 Features 1-3

1-2-1 V640-HAM11-ETN-V5 1-3

1-2-2 V640-HAM11-L-ETN-V5 1-3

1-3 System Configuration 1-4

1-3-1 V640-HAM11-ETN-V5 1-4

1-3-2 V640-HAM11-L-ETN-V5 1-4

1-4 Component Names and Functions 1-5

1-4-1 V640-HAM11-ETN-V5 and V640-HAM11-L-ETN-V5 Amplifier Units 1-5

1-4-2 V640-HS61 and V640-HS62 CIDRW Heads 1-8

1-5 Flowchart for Getting Started 1-9

Section 2 Installation and Connections/Wiring

2-1 Installation.......................................2-2
2-1-1 Amplifier Unit.......................................2-2
2-1-2 CIDRW Head.......................................2-3

2-2 Connections and Wiring.......................................2-5
2-2-1 Amplifier Unit.......................................2-5

Section 3 Preparing for Communications

3-1 Set the IP Address on the Computer 3-2
3-1-1 Default IP Address Settings of the Amplifier Unit.......................................3-2
3-1-2 Setting the IP Address on the Computer with Windows 10/Windows 11 3-2

3-2 Setting the Communications Conditions for Amplifier Units.......................................3-3
3-2-1 Default Network Settings (IP Address and Subnet Mask).......................................3-3
3-2-2 Setting the IP Address of the Amplifier Units Using the DIP Switches.......................................3-3
3-2-3 Setting the Communications Conditions of the Amplifier Units from a Web Browser 3-4
3-2-4 Setting the Communications Conditions of the Amplifier Units for Command from the Host Device.......................................3-8

3-3 Communications Test.......................................3-9
3-3-1 Communications Test with the Host Device 3-9
3-3-2 Communications Test between ID Tags and CIDRW System.......................................3-10

Section 4 Reading from/Writing to ID Tags

4-1 Command/Response Format.......................................4-2
4-1-1 Command / Response 4-2
4-1-2 READ 4-4
4-1-3 WRITE.......................................4-6
4-1-4 SAME WRITE 4-8
4-1-5 BYTE WRITE 4-9
4-1-6 TEST 4-10
4-1-7 NAK.......................................4-11
4-1-8 GET PARAMETER.......................................4-12
4-1-9 GET LAST COMMAND.......................................4-18
4-1-10 GET COMMUNICATIONS HISTORY.......................................4-19
4-1-11 CLEAR COMMUNICATIONS HISTORY 4-20
4-1-12 NOISE MEASUREMENT 4-21
4-1-13 RESET 4-22
4-1-14 SET NETWORK.......................................4-23

Section 5 Security

5-1 Security Guide.......................................5-2
5-1-1 Necessity of Security Response 5-2
5-1-2 Purposes of Security Response.......................................5-2
5-1-3 V640-series Compliance 5-3

5-2 Security Functions.......................................5-5
5-2-1 Password Authentication Function.......................................5-6
5-2-2 Access Permission Function 5-13
5-2-3 IP Filtering Function 5-16
5-2-4 Security Log Function 5-19
5-2-5 Factory Reset Function 5-27
5-2-6 Backup Function 5-29

Section 6 Web Browser

6-1 Web Browser Overview 6-2
6-1-1 Overview 6-2
6-1-2 System Environment 6-2
6-1-3 Procedure to Display the Browser Window 6-2

6-2 Web Browser Functions 6-3
6-2-1 Windw List 6-3
6-2-2 Window Transitions 6-3
6-2-3 Window Configuration 6-4
6-2-4 Login Window 6-5
6-2-5 Status Window 6-7
6-2-6 Network Settings Window 6-8
6-2-7 Network Settings Window (TCP/IP Settings) 6-9
6-2-8 Network Settings Window (Port Setting) 6-10
6-2-9 Network Settings Window (IP Filtering Settings) 6-11
6-2-10 Network Settings Window (Permission Settings) 6-12
6-2-11 Network Settings Window (Web Password Settings) 6-13
6-2-12 Command Window 6-14
6-2-13 Command Window (CID R/W) 6-15
6-2-14 Command Window (V640 Command) 6-17
6-2-15 Noise Monitor Window 6-19
6-2-16 Log View Window 6-20
6-2-17 Log View Window (Communication Log) 6-21
6-2-18 Log View Window (Security Log) 6-22
6-2-19 Configuration Window 6-24
6-2-20 Safe-Mode Window 6-26

6-3 Root Certificate Installation Procedure 6-28

Section 7 Troubleshooting

7-1 Troubleshooting 7-2
7-1-1 Status Check with OPERATING Indicator (LED) 7-2
7-1-2 List of Error Messages 7-3
7-1-3 Operation Check Flowchart 7-4
7-1-4 Other Troubleshooting 7-10

Appendices

A-1 Specifications and Dimensions A-2
A-1-1 Amplifier Units A-2
A-1-2 CIDRW Heads A-5

A-2 Connection Examples A-7
A-2-1 V640-HAM11-ETN-V5 .... A-7
A-2-2 V640-HAM11-L-ETN-V5 .... A-7

A-3 Characteristic Data According to Conditions of Use A-8
A-3-1 Maps of Communications Areas (Reference Only) A-8
A-3-2 Mutual Interference Distances (Reference Only) A-32
A-3-3 Influence of Background Metals (Reference Only) A-34
A-3-4 Communications Time A-35
A-3-5 Communications Distance Characteristics vs. Ambient Noise A-38

A-4 ID Tag Memory Maps A-39
A-4-1 RI-TRP-DR2B(-40) A-39
A-4-2 RI-TRP-WR2B(-30) A-39

A-5 Regular Inspection A-40

A-6 ASCII Code Table A-41

A-7 Degree of Protection.. A-42

Index

Terms and Conditions Agreement

Warranty, Limitations of Liability

Warranties

- **Exclusive Warranty**

  Omron's exclusive warranty is that the Products will be free from defects in materials and workmanship for a period of twelve months from the date of sale by Omron (or such other period expressed in writing by Omron). Omron disclaims all other warranties, express or implied.

- **Limitations**

  OMRON MAKES NO WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, ABOUT NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OF THE PRODUCTS. BUYER ACKNOWLEDGES THAT IT ALONE HAS DETERMINED THAT THE PRODUCTS WILL SUITABLY MEET THE REQUIREMENTS OF THEIR INTENDED USE.

  Omron further disclaims all warranties and responsibility of any type for claims or expenses based on infringement by the Products or otherwise of any intellectual property right.

- **Buyer Remedy**

  Omron's sole obligation hereunder shall be, at Omron's election, to (i) replace (in the form originally shipped with Buyer responsible for labor charges for removal or replacement thereof) the non-complying Product, (ii) repair the non-complying Product, or (iii) repay or credit Buyer an amount equal to the purchase price of the non-complying Product; provided that in no event shall Omron be responsible for warranty, repair, indemnity or any other claims or expenses regarding the Products unless Omron's analysis confirms that the Products were properly handled, stored, installed and maintained and not subject to contamination, abuse, misuse or inappropriate modification. Return of any Products by Buyer must be approved in writing by Omron before shipment. Omron Companies shall not be liable for the suitability or unsuitability or the results from the use of Products in combination with any electrical or electronic components, circuits, system assemblies or any other materials or substances or environments. Any advice, recommendations or information given orally or in writing, are not to be construed as an amendment or addition to the above warranty.

  See https://www.omron.com/global/ or contact your Omron representative for published information.

Limitation on Liability; Etc

OMRON COMPANIES SHALL NOT BE LIABLE FOR SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, LOSS OF PROFITS OR PRODUCTION OR COMMERCIAL LOSS IN ANY

WAY CONNECTED WITH THE PRODUCTS, WHETHER SUCH CLAIM IS BASED IN CONTRACT, WARRANTY, NEGLIGENCE OR STRICT LIABILITY.

Further, in no event shall liability of Omron Companies exceed the individual price of the Product on which liability is asserted.

Application Considerations

Suitability of Use

Omron Companies shall not be responsible for conformity with any standards, codes or regulations which apply to the combination of the Product in the Buyer's application or use of the Product. At Buyer's request, Omron will provide applicable third party certification documents identifying ratings and limitations of use which apply to the Product. This information by itself is not sufficient for a complete determination of the suitability of the Product in combination with the end product, machine, system, or other application or use. Buyer shall be solely responsible for determining appropriateness of the particular Product with respect to Buyer's application, product or system. Buyer shall take application responsibility in all cases.

NEVER USE THE PRODUCT FOR AN APPLICATION INVOLVING SERIOUS RISK TO LIFE OR PROPERTY OR IN LARGE QUANTITIES WITHOUT ENSURING THAT THE SYSTEM AS A WHOLE HAS BEEN DESIGNED TO ADDRESS THE RISKS, AND THAT THE OMRON PRODUCT(S) IS PROPERLY RATED AND INSTALLED FOR THE INTENDED USE WITHIN THE OVERALL EQUIPMENT OR SYSTEM.

Programmable Products

Omron Companies shall not be responsible for the user's programming of a programmable Product, or any consequence thereof.

Disclaimers

Performance Data

Data presented in Omron Company websites, catalogs and other materials is provided as a guide for the user in determining suitability and does not constitute a warranty. It may represent the result of Omron's test conditions, and the user must correlate it to actual application requirements. Actual performance is subject to the Omron's Warranty and Limitations of Liability.

Change in Specifications

Product specifications and accessories may be changed at any time based on improvements and other reasons. It is our practice to change part numbers when published ratings or features are changed, or when significant construction changes are made. However, some specifications of the Product may be changed without any notice. When in doubt, special part numbers may be assigned to fix or establish key specifications for your application. Please consult with your Omron's representative at any time to confirm actual specifications of purchased Product.

Errors and Omissions

Information presented by Omron Companies has been checked and is believed to be accurate; however, no responsibility is assumed for clerical, typographical or proofreading errors or omissions.

Statement of security responsibilities for assumed use cases and against threats

OMRON SHALL NOT BE RESPONSIBLE AND/OR LIABLE FOR ANY LOSS, DAMAGE, OR EXPENSES DIRECTLY OR INDIRECTLY RESULTING FROM THE INFECTION OF OMRON PRODUCTS, ANY SOFTWARE INSTALLED THEREON OR ANY COMPUTER EQUIPMENT, COMPUTER PROGRAMS, NETWORKS, DATABASES OR OTHER PROPRIETARY MATERIAL CONNECTED THERETO BY DISTRIBUTED DENIAL OF SERVICE ATTACK, COMPUTER VIRUSES, OTHER TECHNOLOGICALLY HARMFUL MATERIAL AND/OR UNAUTHORIZED ACCESS.

It shall be the users sole responsibility to determine and use adequate measures and checkpoints to satisfy the users particular requirements for (i) antivirus protection, (ii) data input and output, (iii) maintaining a means for reconstruction of lost data, (iv) preventing Omron Products and/or software installed thereon from being infected with computer viruses and (v) protecting Omron Products from unauthorized access.

Safety Precautions

Definition of Precautionary Information

The following notation and alert symbols are used in this User's Manual to provide precautions required to ensure safe usage of a V640-series CIDRW System.
The safety precautions that are provided are extremely important to safety. Always read and heed the information provided in all safety precautions.
The following signal words are used in this manual.

⚠WARNING	Indicates a potentially hazardous situation which, if not avoided, will result in minor or moderate injury, or may result in serious injury or death. Additionally there may be significant property damage.

Meanings of Alert Symbols

🛇	Prohibition Indicates general prohibitions for which there is no specific symbol.
❗	Execute Indicates an action of a non-specific, general user.

WARNING

⚠ **WARNING**

Security Measures

Anti-virus protection Install the latest commercial-quality antivirus software on the computer connected to the control system and maintain to keep the software up-to-date.	❗

Security measures to prevent unauthorized access Take the following measures to prevent unauthorized access to our products. • Install physical controls so that only authorized personnel can access control systems and equipment. • Reduce connections to control systems and equipment via networks to prevent access from untrusted devices. • Install firewalls to shut down unused communications ports and limit communications hosts and isolate control systems and equipment from the IT network. • Use a virtual private network (VPN) for remote access to control systems and equipment. • Adopt multifactor authentication to devices with remote access to control systems and equipment. • Set strong passwords and change them frequently. • Scan virus to ensure safety of USB drives or other external storages before connecting them to control systems and equipment.	❗
Data input and output protection Validate backups and ranges to cope with unintentional modification of input/output data to control systems and equipment. • Checking the scope of data • Checking validity of backups and preparing data for restore in case of falsification and abnormalities • Safety design, such as emergency shutdown and fail-soft operation in case of data tampering and abnormalities	❗
Data recovery Backup data and keep the data up-to-date periodically to prepare for data loss.	❗
When using an intranet environment through a global address, connecting to a SCADA or an unauthorized terminal such as an HMI or to an unauthorized server may result in network security issues such as spoofing and tampering. You must take sufficient measures such as restricting access to the terminal, using a terminal equipped with a secure function, and locking the installation area by yourself.	❗
When constructing an intranet, communication failure may occur due to cable disconnection or the influence of unauthorized network equipment. Take adequate measures, such as restricting physical access to network devices, by means such as locking the installation area.	❗
When using a device equipped with the SD Memory Card function, there is a security risk that a third party may acquire, alter, or replace the files and data in the removable media by removing the removable media or unmounting the removable media. Please take sufficient measures, such as restricting physical access to the Controller or taking appropriate management measures for removable media, by means of locking the installation area, entrance management, etc., by yourself.	❗

Precautions for Safe Use

Please observe the following precautions for safe use of the products.

- Never use the product in an environment where combustible or explosivegas is present.
- Please separate from a high-pressure equipment and the power equipment to secure the safety of the operation and maintenance.
- In the installation, please tighten the screw surely. (Recommended 1.2N·m)
- Please do not insert foreign bodies such as water and the wires from the space of the case.
- Please do not dismantle, repair or modify this product.
- Please process as industrial waste when you abandon this product.
- When you work on wiring and put on and take off cables, CIDRW head, please perform it after switching off this product.
- Provide enough space around this product for ventilation.
- Please avoid installing this product near the machinery (a heater, a transformer, large-capacity resistance) that has high the calorific value.
- Talk to our office by any chance after you cancel use immediately when you felt abnormality to this product, and having switched it off.

Confirm the effects of radio waves on medical devices. The following guideline is from JAISA (Japan Automatic Identification Systems Association).

> This product is a reader-writer that uses radio waves for RFID equipment. The application and location of this product may affect medical devices. The following precaution must be observed in the application of the product to minimize the effects on medical devices.
>
> Any person with an implanted medical device must keep the area where the device is implanted at least 22 cm away from the antenna of a stationary or modular RFID device.

Precautions for Correct Use

Please observe the following precautions to prevent failure to operate, malfunctions, or undesirable effects on product performance.

About installation Site

Do not install this product in the locations subject to the following conditions.

- Place where direct sunshine strikes.
- Place with corroded gas, dust, metallic powder, and salinity.
- Place with condensation due to rapid temperature fluctuations.
- Place with condensation due to high humidity.
- Place where vibration and impact more than being provided by specification are transmitted directly to main body.
- Place with spray of water, oil, and chemical medicine.
- The working temperature is within the range stipulated in the specifications.

About depositoty Site

- Please follow the save ambient temperature / humidity, and keep this product.

About wiring

- Use the power supply voltage specified in this cocument.
- Ensure correct polarity when connecting to the +/- power supply terminals.
- Do not run high-voltage lines and power lines though the same conduit.
- To avoid static-induced failure, wear a wrist band or equivalent means to release a static charge before touching a terminal or a signal line within a connector.
- When you put on and take off a CIDRW head, please do not add excessive power to a connector.
- Please connect the correct CIDRW head to the amplifier unit.
- If an incorrect CIDRW head is connected, the desired communication performance may not be achieved.

About cleaning

- Use alcohol to clean this product.
- Never use an organic solvent such as thinner, benzene, acetone or kerosene, as it will attack resin components or case coating.

Power and Ground Cables

- Use an appropriate ground. An insufficient ground can affect this product operation or result in damage to this product.

About the communication range and time

- Do the communication test with Transponder in the installation environment because the metal, noise and ambient temperature around CIDRW head damage to the communication range and time.
- Install CIDRW head and ID tag in the appropriate distance because the communication range can change by the difference of ID tag specifications.

About mounting

- This product communicates with ID Tags using the 134 kHZ frequency band. Some transceivers, motors, monitoring equipment, and power supplies (power supply ICs) generate electrical waves (noise) that interfere with communications with ID Tags, If you are using the product in the vicinity of any of these devices, check the effect on communications in advance.
- In order to minimize the effects of noise, ground nearby metal bodies with a grounding resistance not exceeding 100 ohms.
- When mounting CIDRW Heads, tighten the screws tightly.(Recommended 0.6N·m)
- When multiple CIDRW Heads are mounted next to each other, communications performance could be impaired by mutual interference. Read and follow *A-3-2 Mutual Interference Distances (Reference Only)* on page A-32 on mutual interference when installing multiple heads.

Screw Locking Adhesive

- Screw locking adhesive (screw lock) may cause deterioration and cracking of resin parts; do not use it for screws in resin parts or anywhere where resin washers are used.

Startup Precaution

- Never turn OFF the power supply while the CIDRW Controller is starting, including when power is turned ON, when the mode is changed, or when the CIDRW Controller is being reset. Doing so may damage the CIDRW Controller.

Application Precaution

- Never turn OFF the power supply while setting the IP address, subnet mask, or Web password. Doing so may damage the Amplifier Unit.

About Transponder made by Texas Instruments Co.

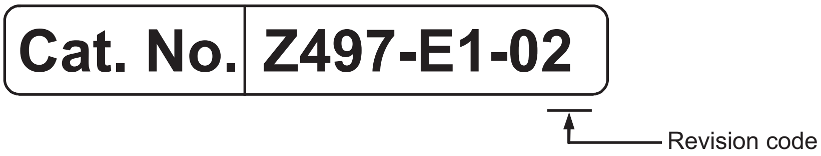
1. We can’t warrant the specifications of the communication with Transponder(RI-TRP-DR2B(-40), RI-TRP-WR2B(-30).
2. We can’t responsible for any malfunctions of Transponder.

The characteristics of the V640-HAM11-(L)-ETN-V2/V640-HAM11-(L)-ETN-V5

- It is a circuit, designed to communicate characteristics match, but because it is intended to carry out the communication with the transponder, can not be guaranteed.

Revision History

A manual revision code appears as a suffix to the catalog number on the front and back covers of the manual.



Cat. No. Z497-E1-02

Revision code

Revision code	Date	Revised content
01	August 2025	Original production
02	September 2025	Corrected mistakes

1

Product Outline

This section provides an overview of the V640-series CIDRW System, including its features, system configuration, component names and functions, and a flowchart for getting started.

1-1 What Is a CIDRW System 1-2

1-2 Features 1-3

1-2-1 V640-HAM11-ETN-V5 1-3
1-2-2 V640-HAM11-L-ETN-V5 1-3

1-3 System Configuration 1-4

1-3-1 V640-HAM11-ETN-V5 1-4
1-3-2 V640-HAM11-L-ETN-V5 1-4

1-4 Component Names and Functions 1-5

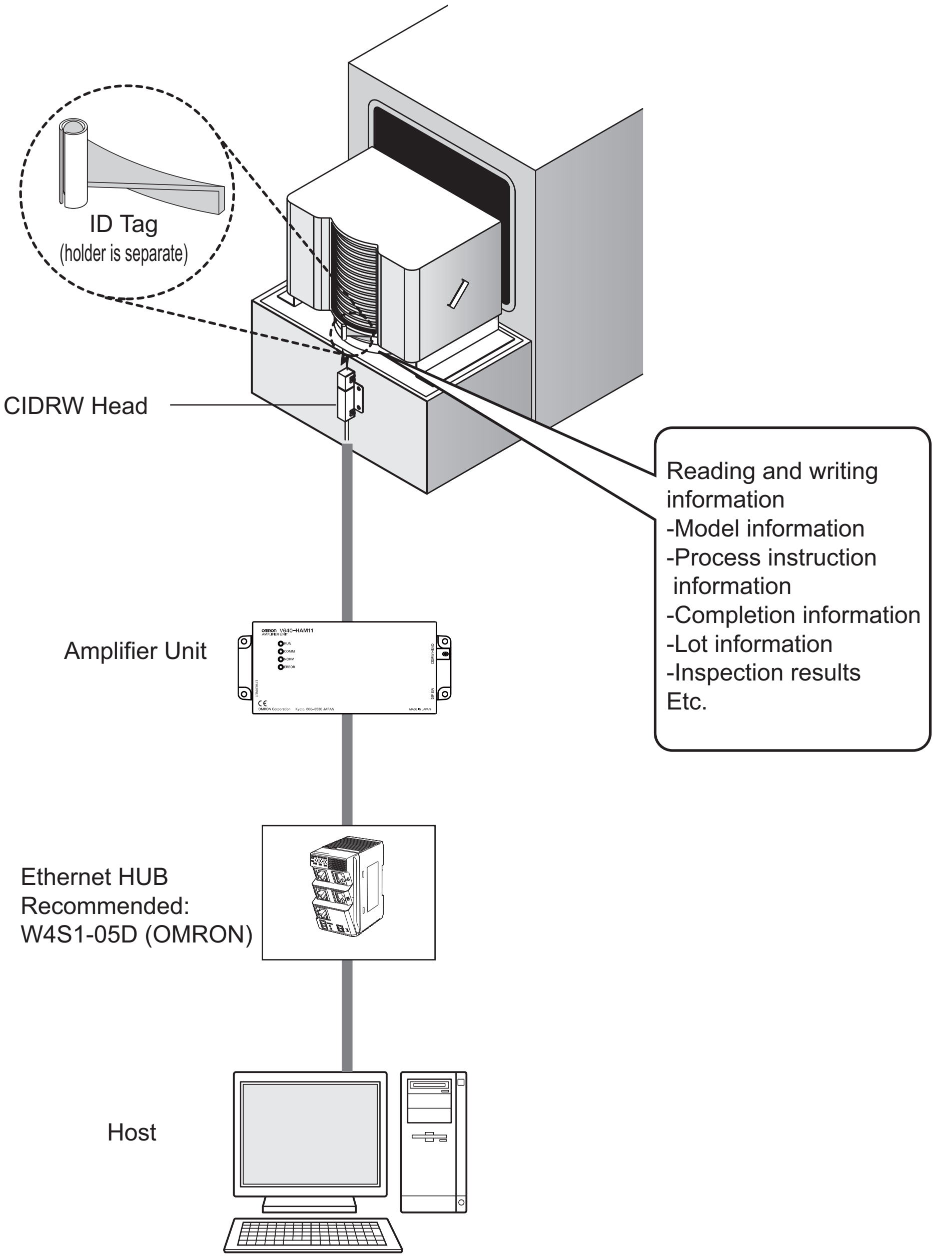
1-4-1 V640-HAM11-ETN-V5 and V640-HAM11-L-ETN-V5 Amplifier Units 1-5
1-4-2 V640-HS61 and V640-HS62 CIDRW Heads 1-8

1-5 Flowchart for Getting Started 1-9

1-1 What Is a CIDRW System

The CIDRW system writes data to, and reads data from, the carrier IDs (ID Tags) mounted on the carriers (FOUP) in semiconductor manufacturing processes without contacting these ID Tags. CIDRW is the abbreviation of Carrier ID Reader/Writer and this abbreviation is used throughout this manual. Reading and writing information such as models, process instructions, lots, and inspection results to and from ID Tags makes it possible to manage work instruction information from a host device.

Example: Management of information in semiconductor and wafer manufacturing processes



1-2 Features

A V640-series CIDRW Head can be connected to a V640-HAM11-ETN-V5 or V640-HAM11-L-ETN-V5 Amplifier Unit to read and write ID Tags manufactured by Texas Instruments (TI). Reading and writing is performed according to commands from the host device.

1-2-1 V640-HAM11-ETN-V5

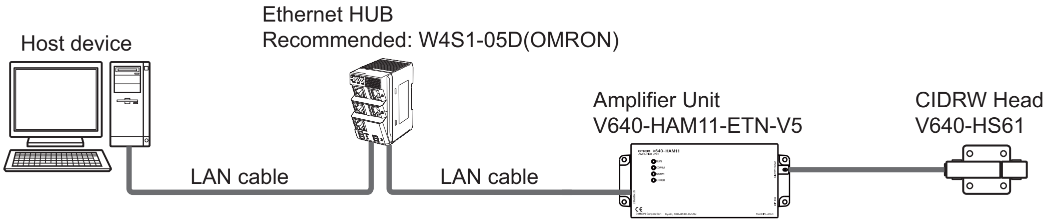
This Amplifier Unit is equipped with Ethernet. The host device is connected through a LAN cable and controls the Amplifier Units using TCP/IP. The Amplifier Units provide a Web Browser function that allows communications to be set and status to be managed using simple command communications.

1-2-2 V640-HAM11-L-ETN-V5

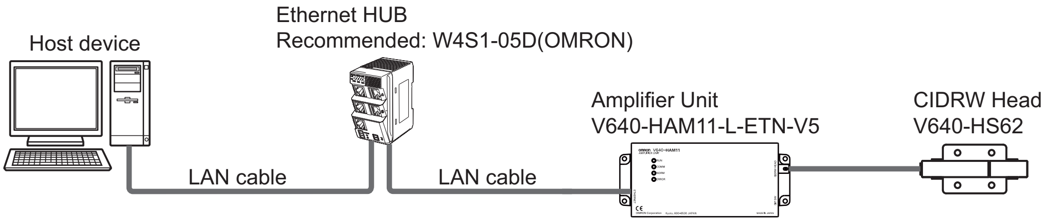
This Amplifier Unit is equipped with Ethernet and can be connected to a V640-HS62 CIDRW Head to perform long-distance communications. The functions of the V640-HAM11-L-ETN-V5 are the same as those of the V640-HAM11-ETN-V5.

1-3 System Configuration

1-3-1 V640-HAM11-ETN-V5



1-3-2 V640-HAM11-L-ETN-V5

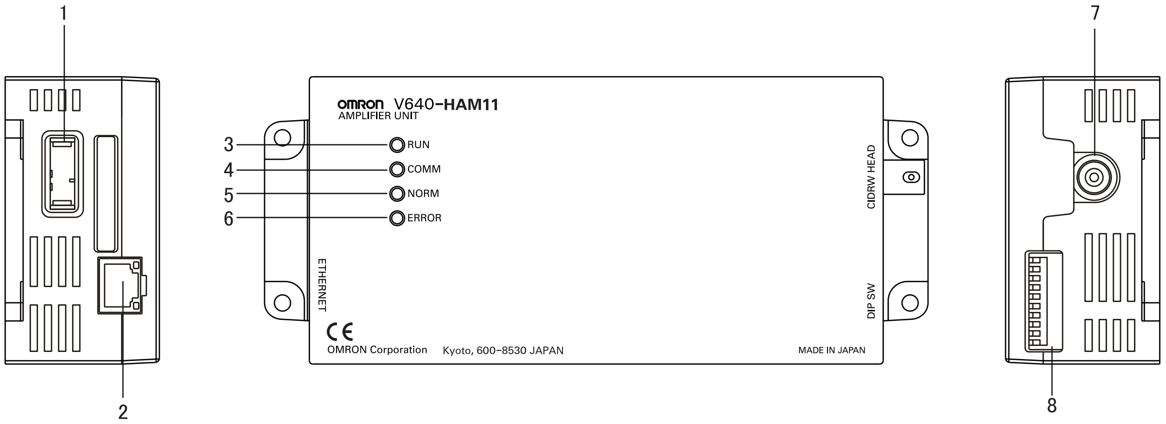


Precautions for Correct Use

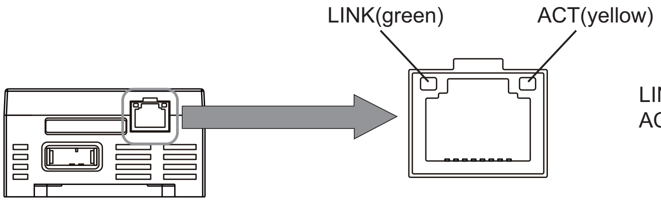
If the IP address is set on the DIP Switch, it will be in the form 192.168.1.XXX. The subnet mask is always 255.255.255.0. The IP address of the Amplifier Unit can be either set on this DIP switch or the desired IP address can be set in ROM. If pins 1 to 5 on the DIP switch are all turned OFF, the IP address that is set in ROM will be used.

1-4 Component Names and Functions

1-4-1 V640-HAM11-ETN-V5 and V640-HAM11-L-ETN-V5 Amplifier Units



No.	Name	Function
1	Dedicated power supply connector	Connect to the 24 VDC power supply.
2	Ethernet port	Connect to the host device through a LAN cable.
3	RUN indicator (green)	Turns ON when the Amplifier Unit is in normal operation.
4	COMM indicator (yellow)	Turns ON during communications with the host device or during communications with an ID Tag.
5	NORM indicator (green)	Turns ON when the communications finish with no error.
6	ERROR indicator (red)	Turns ON when an error occurs during communications with the host device, or during communications with an ID Tag.
7	CIDRW Head connection port	A CIDRW Head is connected here. The V640-HS61 CIDRW Head is used with the V640-HAM11-ETN-V5. The V640-HS62 CIDRW Head is used with the V640-HAM11-L-ETN-V5.
8	Setting DIP Switch	Set the IP address and enable/disable Test Mode and Safe-Mode with this DIP switch.



LINK---lights while linking normally.
ACT---lights when detects a carrier.

Functions

- NOISE MEASUREMENT

  The levels of noise in the vicinity of the CIDRW Head are measured and the noise level is expressed numerically in the range "00" to "99".

  For information on the NOISE MEASUREMENT command and the effect of ambient noise on communication distance, see *4-1-12 NOISE MEASUREMENT* on page 4-21, *A-3-5 Communications Distance Characteristics vs. Ambient Noise* on page A-38.

- Detecting for CIDRW Head status

  You can confirm if the CIDRW Head is connected to the Amplifier Unit correctly.

  For more information, see page 4-16.

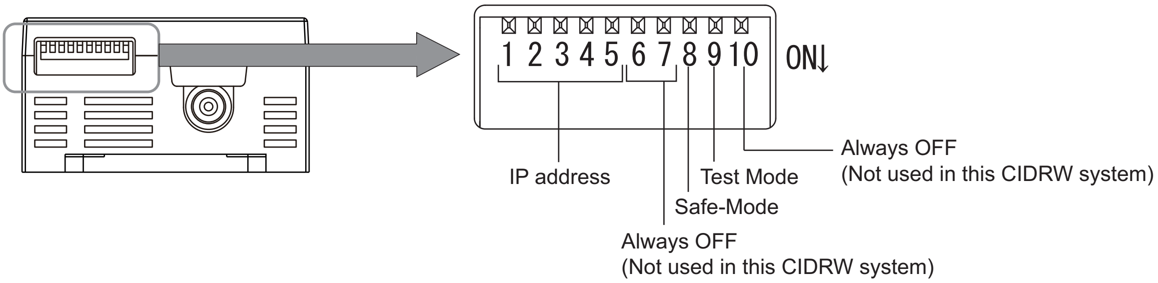
- Test Mode

  Test Mode can be used to check communications between the ID Tags and Amplifier Units without connecting a host device.

  Communications with ID Tags are automatically performed every second and the communications results are displayed on the OPERATING indicator.

  Set the Test Mode using the DIP Switch on the side face of the Amplifier Unit.

  After changing the DIP Switch settings, restart the system. The new settings will not become effective until the system is restarted.



Test Mode	DIP Switch	Description
	9	
Enabled	ON	Set the Test Mode and then restart the Amplifier Unit to make the setting effective.
Disabled	OFF	

Additional Information

- For information on the OPERATING indicator for communications result, refer to *1-4-1 V640-HAM11-ETN-V5 and V640-HAM11-L-ETN-V5 Amplifier Units* on page 1-5.
- Always connect the CIDRW Head before operating the Amplifier Unit in Test Mode.
  If Test Mode is used without connecting a CIDRW Head, the ERROR inductor will light and Amplifier Unit operation will stop.
- Commands from the host device are not accepted during operation in Test Mode. To end Test Mode, turn OFF the Test Mode pin on the DIP switch and restart the Amplifier Unit.

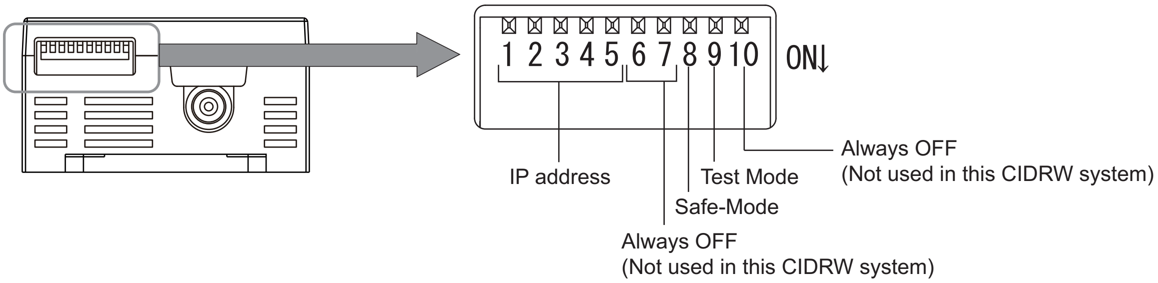
- Safe-Mode

  This mode is for maintaining the Amplifier Unit.

  If you have forgotten your Web Password or the IP Address registered with the IP Filtering function and can no longer connect using the Web Browser, you can start up in Safe-Mode and perform the Factory Reset to return to the initial state.

Set the Safe-Mode using the DIP Switch on the side face of the Amplifier Unit.

After changing the DIP Switch settings, restart the system. The new settings will not become effective until the system is restarted.



Safe-Mode	DIP Switch	Description
	8	
Enabled	ON	Set the Safe-Mode and then restart the Amplifier Unit to make the setting effective.
Disabled	OFF	

Additional Information

- When started up in safe mode, the OPERATING indicator will be in the following state.

RUN	COMM	NORM	ERROR
◐ (2 s intervals)	●	●	●

- For what to do if you have forgotten your password, refer to *What to Do If You Have Forgotten Your Password* on page 5-12 in *5-2-1 Password Authentication Function* on page 5-6.
- For information about the IP Filtering function refer to *5-2-3 IP Filtering Function* on page 5-16.

- Browser Interface

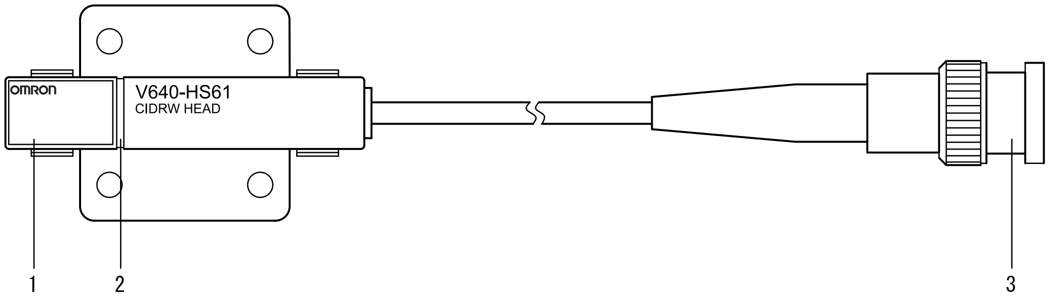
  You can confirm the status of the Amplifier Unit or control the Amplifier Unit by using the Web Browser. You can...

  - confirm the status of the Amplifier Unit
  - set the Network Settings and Web Password
  - communicate with ID tags
  - measure the levels of noise

  For information about the Web Browser, see *Section 6 Web Browser* on page 6-1.

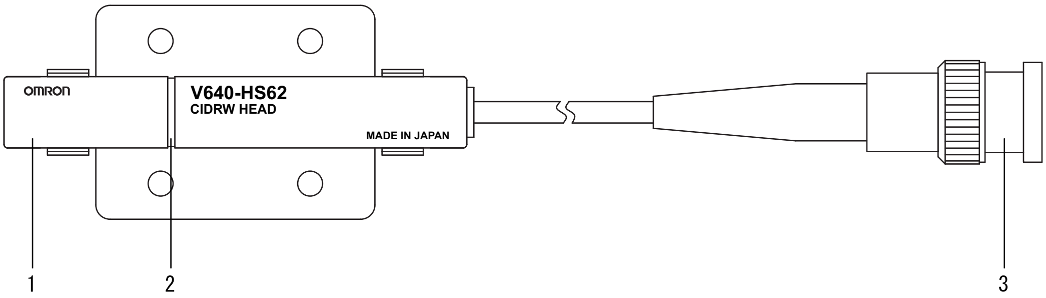
1-4-2 V640-HS61 and V640-HS62 CIDRW Heads

V640-HS61



No.	Name	Function
1	Antenna	Used to communicate with ID Tags.
2	Antenna center	This is the center of the communications area.
3	Connector	Connect to an Amplifier Unit.

V640-HS62



No.	Name	Function
1	Antenna	Used to communicate with ID Tags.
2	Antenna center	This is the center of the communications area.
3	Connector	Connect to an Amplifier Unit.

1-5 Flowchart for Getting Started

Installation and Connections	
Installation	*2-1 Installation* on page 2-2
Connection and Wiring	*2-2 Connections and Wiring* on page 2-5

↓

Preparation for Trial Operation Communications	
Setting the Communications Conditions for Amplifier Units	*3-2 Setting the Communications Conditions for Amplifier Units* on page 3-3

↓

Trial Operation	
Test for Communications with the Host Device	*3-3-1 Communications Test with the Host Device* on page 3-9
ID Tag <-> CIDRW System Communications Test	*3-3-2 Communications Test between ID Tags and CIDRW System* on page 3-10
Check the Surrounding Environment	*2-1-2 CIDRW Head* on page 2-3

↓

Communications	
Communications Test with Actual Commands	*4-1 Command/Response Format* on page 4-2

Additional Information

For Troubleshooting, please refer to the following.

- List of Error Messages: *7-1-2 List of Error Messages* on page 7-3
- Amplifier Unit Indicators: *Amplifier Unit Indicators* on page 7-2
- Operation Check Flowchart: *7-1-3 Operation Check Flowchart* on page 7-4

2

Installation and Connections/ Wiring

2-1 Installation 2-2

2-1-1 Amplifier Unit 2-2

2-1-2 CIDRW Head 2-3

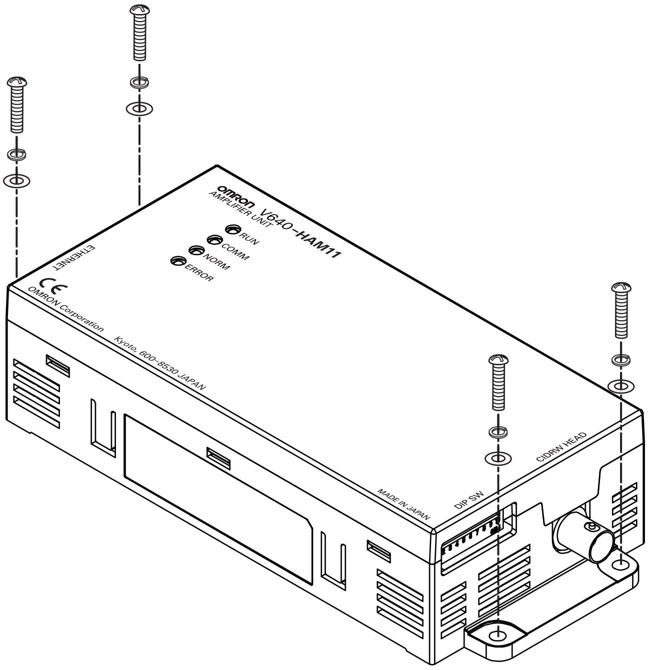
2-2 Connections and Wiring 2-5

2-2-1 Amplifier Unit 2-5

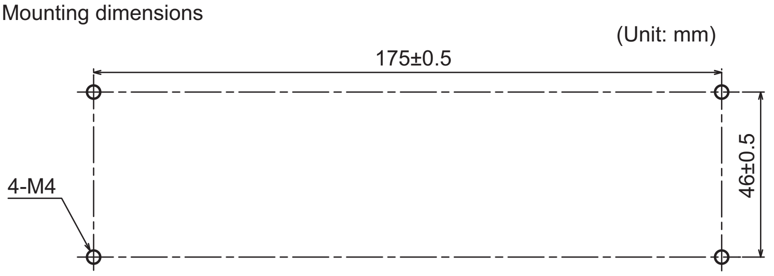
2-1 Installation

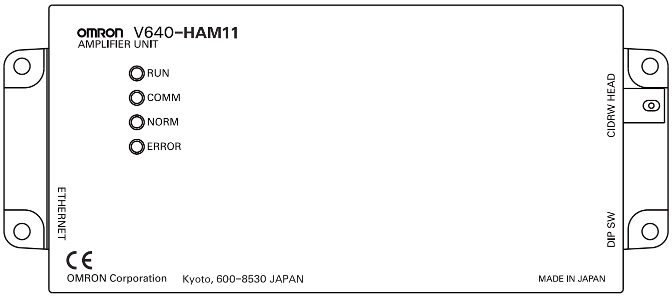
2-1-1 Amplifier Unit

Use spring washers and flat washers with the four M4 screws when mounting the Amplifier Unit.



Mounting dimensions





Precautions for Safe Use

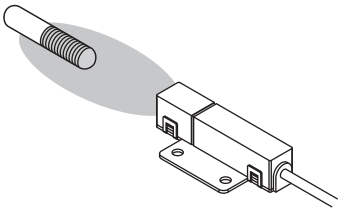
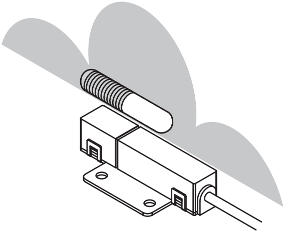
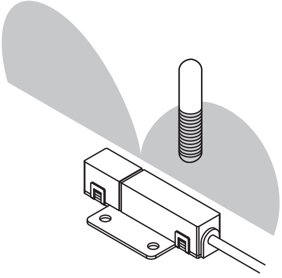
Tighten the M4 screws with a torque not exceeding 1.2 N·m.

2-1-2 CIDRW Head

The area for communications with ID Tags varies substantially according to the installation orientations and the background conditions (metals, noise, etc.). Check the communications area before deciding the installation position.
For details on actual communications distances, see *A-3 Characteristic Data According to Conditions of Use* on page A-8 in Appendix.

Positional Relationship between the CIDRW Head and the ID Tag

The communications area differs according to the positional relationship during communications.

Mounting orientation	Communications area (purely illustrative)	Explanation
Coaxial		The maximum communications area is obtained when the center lines of the CIDRW Head and the ID Tag coincide.
Parallel		The maximum communications area is obtained when the center point of the antenna on the CIDRW Controller is aligned with the center line of the ID Tag.
Vertical		When the center point of the antenna on the CIDRW Head is aligned with the center line of the ID Tag, the communications area is substantially reduced.

Data Reading and Writing

The communications distances for reading and writing are not the same; the distance is shorter for writing. Therefore, when data is to be both read and written, take the distance for writing as the reference distance when installing the CIDRW Head and the ID Tag.

Influence of Background Metal on ID Tag

Metals in the vicinity of the communications area will affect the range, making it smaller.
For more information, see *A-3-3 Influence of Background Metals (Reference Only)* on page A-34.

Influence of Noise

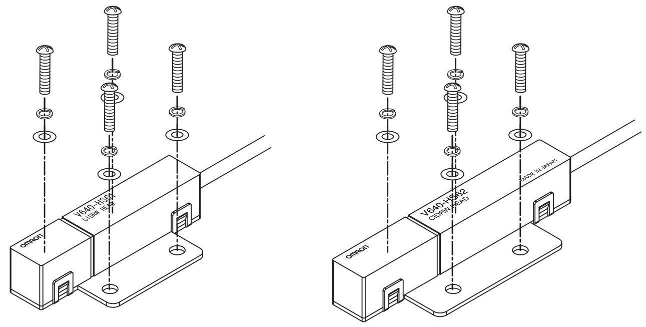
This CIDRW system uses a frequency of 134 kHz for communications with ID Tags. Equipment such as switching power supplies, inverters, servomotors, or monitors in the surrounding area will adversely affect communications, restricting the communications area.

Precautions for Correct Use

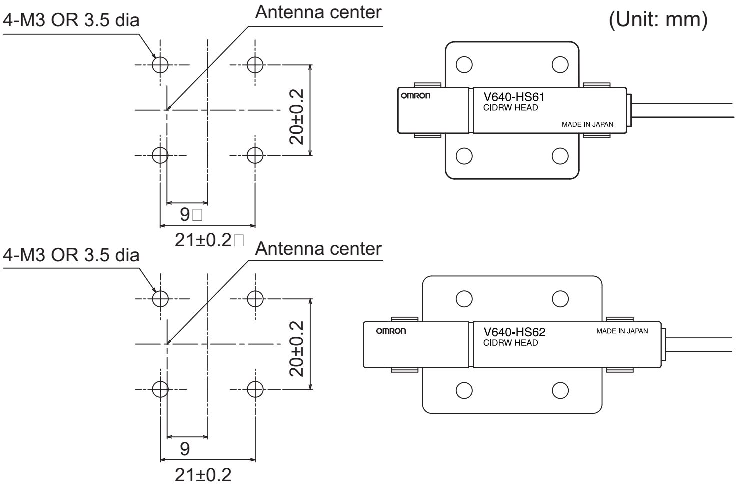
- The noise levels in the vicinity of the CIDRW Head can be determined with the environmental NOISE MEASUREMENT command.
  For more information, see *4-1-12 NOISE MEASUREMENT* on page 4-21.
- For details on the relationship between noise and communications distance, see Appendix.
  Refer to *A-3-5 Communications Distance Characteristics vs. Ambient Noise* on page A-38.

Mounting

Use spring washers and flat washers with the four M3 screws when mounting a CIDRW Head.



Mounting dimensions



*The mounting dimensions are same between V640-HS61 and V640-HS62.

Precautions for Safe Use

Tighten the M3 screws with a torque not exceeding 0.6 N·m.

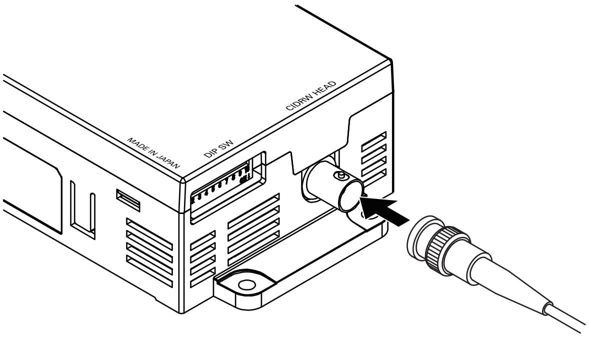
2-2 Connections and Wiring

2-2-1 Amplifier Unit

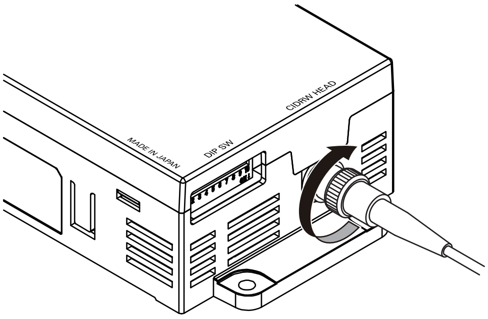
Connector for Connecting a CIDRW Head

1 Align the pin on the connector with the channel in the cable connector and insert the cable connector.

Hold the fixed part of the connector while making this insertion.



2 After inserting the connector fully home, turn the fixed part clockwise to lock it.



Precautions for Correct Use

Disconnecting the CIDRW head.

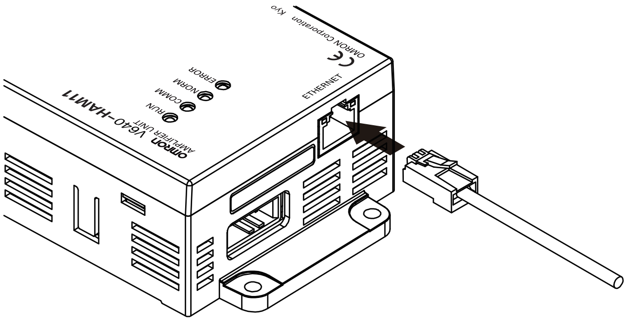
Please pull it straight out after turn a connector counterclockwise and removing a lock.

If it is difficult to pull the connector out , press down on the Amplifier Unit while pulling on the connector.

Please do not pull a cable forcibly.

Ethernet Connector

1 Hold the connector on the cable and insert it into the Ethernet connector on the Amplifier Unit.

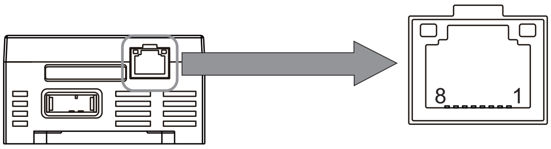


Precautions for Correct Use

Press in the connector until it locks in place when connecting the Amplifier Unit to Ethernet, including when connecting it to a hub.

● Connector

The Amplifier Unit provides an auto-MDIX function that enables communications by connecting either a cross LAN cable or straight LAN cable.



Pin No.	Signal name	Description	I/O
1	TX_D+	Send data +	Output
2	TX_D-	Send data -	Output
3	RX_D+	Receive data +	Input
4	-	-	-
5	-	-	-
6	RX_D-	Receive data -	Input
7	-	-	-
8	-	-	-

Recommended Ethernet HUB

Manufacturer	Model	Type	Port
OMRON	W4S1-05D	switching hub	5

Precautions for Correct Use

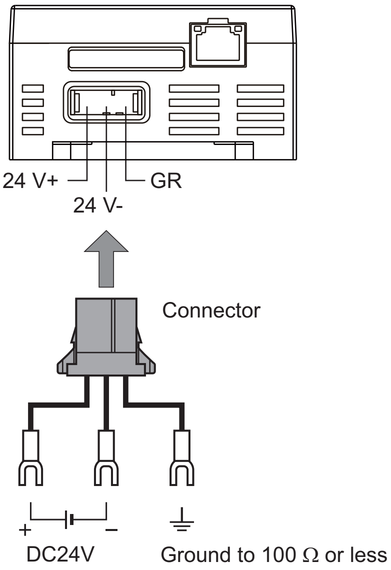
The shape and dimensions of plugs and jacks for Ethernet connectors are specified in ISO/IEC 8877:1992 (JIS X 5110:1996) To prevent faulty connections for connectors, the jack on the Amplifier Unit is designed so that non-standard plugs cannot be connected. If a commercially available plug cannot be connected, it may be non-standard.

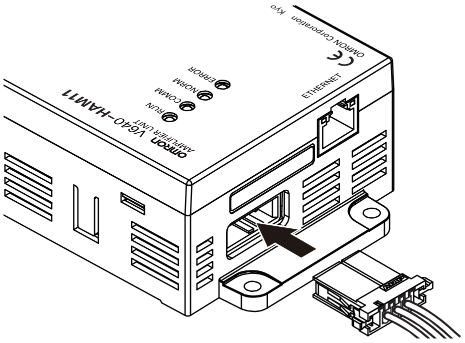
Precautions for Correct Use

If you use a Hub in your network, please choose a Switching-type Hub (Recommended: W4S1-05D (OMRON)).

Power Supply and Grounding Wires

Connect the power supply and grounding wires to the dedicated power supply connector.





Precautions for Safe Use

- The grounding wire should be connected to a ground exclusive to the Amplifier Unit. If the grounding wire is shared with another unit, or connected to a beam in a building, there may be adverse effects.
- Make the grounding point as close as possible and the length of the grounding wire used as short as possible.
- When using the Amplifier Unit in Europe, the connecting cable between the Amplifier Unit and the DC power supply must be 3 m or less.

● Dedicated Power Supply Connector

Prepare a V640-A90 (can be purchased as an accessory).

Contents of the V640-A90 set (accessory)

Name	Quantity	When procured individually	
		Manufacture	Model
Power supply connector	One	Tyco Electronics	1-178288-3
Pins for power supply connector	Three		175217-3
Connector for RS-485 port	One	Phoenix Contact	MSTB2.5/2-STF-5.08

* “Connector for RS-485 port“ is not able to use for the Amplifier Unit.

● Dedicated Power Supply Cable

Use an AWG20 to AWG24 cable.
Use a dedicated tool for crimping the cable to the connector pins.

Recommended Crimping Tool

Manufacturer	Model
Tyco Electronics	919601-1

● Power Supply

Use a power supply that satisfies the following conditions.

Manufacturer	Model	Output current	Input voltage
OMRON	S8VS-01524	24 VDC, 650 mA	100 to 240 VAC

* The maximum power consumption of the Amplifier Unit is 150 mA at 24 VDC (V640-HAM11-ETN-V5), 400 mA at 24 VDC (V640-HAM11-L-ETN-V5). The inrush current, however, must be considered when selecting the power supply capacity. A power supply with an output of 650 mA min. at 24 VDC is recommended.

3

Preparing for Communications

3-1 Set the IP Address on the Computer 3-2

3-1-1 Default IP Address Settings of the Amplifier Unit 3-2

3-1-2 Setting the IP Address on the Computer with Windows 10/Windows 11 3-2

3-2 Setting the Communications Conditions for Amplifier Units 3-3

3-2-1 Default Network Settings (IP Address and Subnet Mask) 3-3

3-2-2 Setting the IP Address of the Amplifier Units Using the DIP Switchs 3-3

3-2-3 Setting the Communications Conditions of the Amplifier Units from a Web Browser 3-4

3-2-4 Setting the Communications Conditions of the Amplifier Units for Command from the Host Device 3-8

3-3 Communications Test 3-9

3-3-1 Communications Test with the Host Device 3-9

3-3-2 Communications Test between ID Tags and CIDRW System 3-10

3-1 Set the IP Address on the Computer

The default IP addresses of the Amplifier Unit are given in the following table. Use these addresses to set the IP address on the computer.

This example changes the last part of the IP address to a value other than 200 (i.e., to 1 to 199 or 201 to 254).

Values of 0 and 255 cnnot be used.

3-1-1 Default IP Address Settings of the Amplifier Unit

Setting item	Default setting
IP address	192.168.1.200
Subnet mask	255.255.255.0

3-1-2 Setting the IP Address on the Computer with Windows 10/ Windows 11

1. Open the **Control Panel**, and select **Network and Internet** and then **Network and Sharing Center**.

2. Select **Change adapter settings** and then right-click **Ethernet**.

3. Right-click **Local Area Connection** and select **Properties**.

4. Select **Internet Protocol Version 4(TCP/IPv4)** and then click the **Properties** Button.

5. Select the **Use the following IP address Option**, make the following settings, and then click the **OK** Button.
   Change the last part of the IP address to a value other than 200 (i.e., to 1 to 199 or 201 to 254).
   Values of 0 and 255 cannot be used.

6. Click the **OK** Button to colse the **Internet Protocol Version 4(TCP/IPv4) Properties** Dialog Box.

3-2 Setting the Communications Conditions for Amplifier Units

3-2-1 Default Network Settings (IP Address and Subnet Mask)

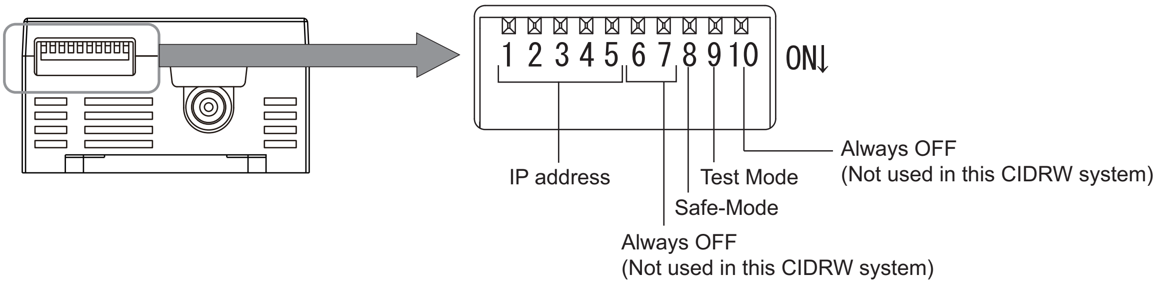
IP Address: 192.168.1.200 Subnet mask: 255.255.255.0 (Port: 7090)

The above network settings can be changed via DIP Switch or the command/browser window.

- If the IP address is set on the DIP Switch, it will be in the form 192.168.1.□□□. The subnet mask is always 255.255.255.0.
- The IP address of the Amplifier Unit can be either set on this DIP Switch or the desired IP address can be set in ROM. If pins 1 to 5 on the DIP Switch are all turned OFF, the IP address that is set in ROM will be used.

3-2-2 Setting the IP Address of the Amplifier Units Using the DIP Switchs

Set the communications conditions using the DIP Switchs on the side face of the Amplifier Unit. After changing the DIP Switch settings, turn the power off and on. The new settings will not become effective until turn the power off and on.

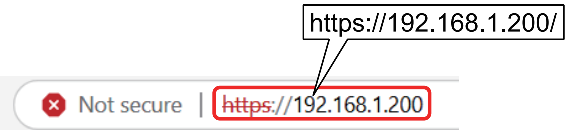


IP Address

IP address	DIP Switch				
	1	2	3	4	5
Setting in ROM	OFF	OFF	OFF	OFF	OFF
192.168.1.1	ON	OFF	OFF	OFF	OFF
192.168.1.2	OFF	ON	OFF	OFF	OFF
192.168.1.3	ON	ON	OFF	OFF	OFF
192.168.1.4	OFF	OFF	ON	OFF	OFF
192.168.1.5	ON	OFF	ON	OFF	OFF
192.168.1.6	OFF	ON	ON	OFF	OFF
192.168.1.7	ON	ON	ON	OFF	OFF
192.168.1.8	OFF	OFF	OFF	ON	OFF
192.168.1.9	ON	OFF	OFF	ON	OFF
192.168.1.10	OFF	ON	OFF	ON	OFF
192.168.1.11	ON	ON	OFF	ON	OFF
192.168.1.12	OFF	OFF	ON	ON	OFF
192.168.1.13	ON	OFF	ON	ON	OFF
192.168.1.14	OFF	ON	ON	ON	OFF
192.168.1.15	ON	ON	ON	ON	OFF
192.168.1.16	OFF	OFF	OFF	OFF	ON
192.168.1.17	ON	OFF	OFF	OFF	ON
192.168.1.18	OFF	ON	OFF	OFF	ON
192.168.1.19	ON	ON	OFF	OFF	ON
192.168.1.20	OFF	OFF	ON	OFF	ON
192.168.1.21	ON	OFF	ON	OFF	ON
192.168.1.22	OFF	ON	ON	OFF	ON
192.168.1.23	ON	ON	ON	OFF	ON
192.168.1.24	OFF	OFF	OFF	ON	ON
192.168.1.25	ON	OFF	OFF	ON	ON
192.168.1.26	OFF	ON	OFF	ON	ON
192.168.1.27	ON	ON	OFF	ON	ON
192.168.1.28	OFF	OFF	ON	ON	ON
192.168.1.29	ON	OFF	ON	ON	ON
192.168.1.30	OFF	ON	ON	ON	ON
192.168.1.31	ON	ON	ON	ON	ON

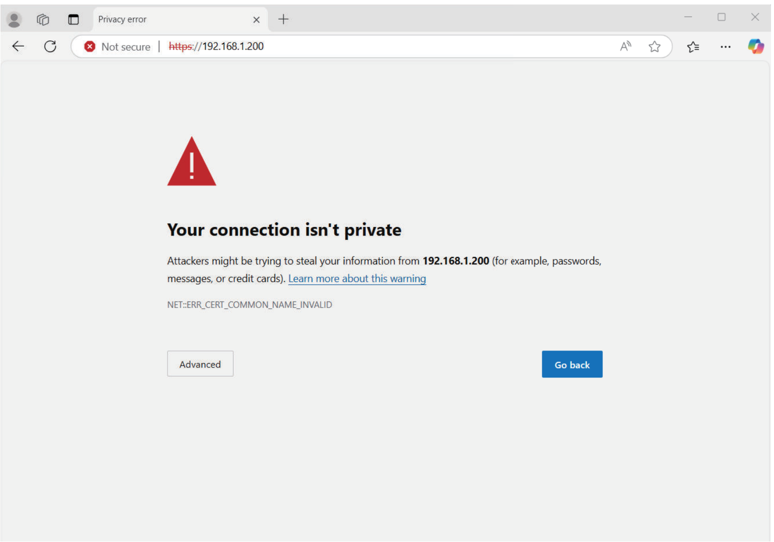
3-2-3 Setting the Communications Conditions of the Amplifier Units from a Web Browser

1 Start the Web Browser.
Enter the IP address of the Amplifier Units in the address field of the Web Browser to display the Browser Operation Window. Enter https://192.168.1.200 if you are using the default IP address.



Precautions for Correct Use

If you enter the IP address in the address field of the Web Browser, a security warning will be displayed.



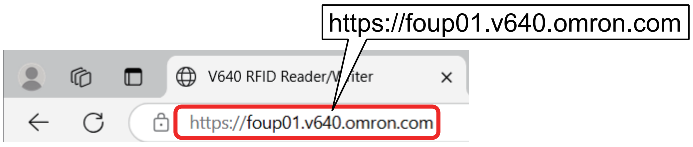
Your connection isn't private

Attackers might be trying to steal your information from **192.168.1.200** (for example, passwords, messages, or credit cards). Learn more about this warning

NET::ERR_CERT_COMMON_NAME_INVALID

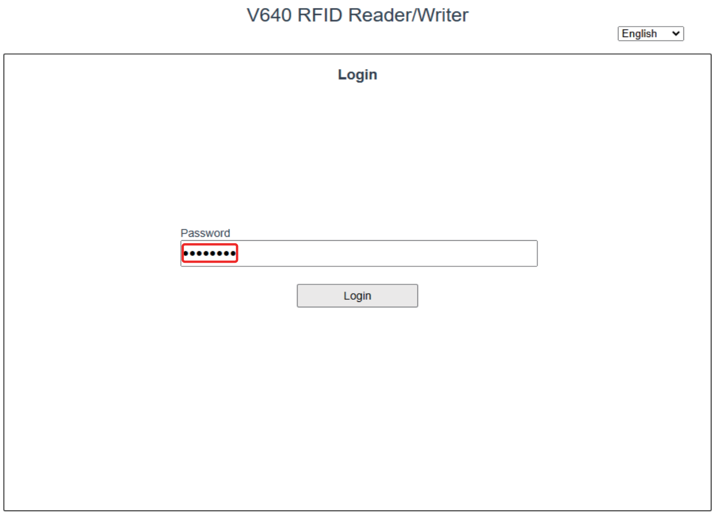
Additional Information

By installing the root certificate on your computer and setting the domain name of the Amplifier Units, you can establish a secure connection with the Amplifier Units.



For instructions on installing a root certificate, see *6-3 Root Certificate Installation Procedure* on page 6-28.

2 The Web Browser Login window will be displayed, so enter your Web Password.
In the factory default settings, an initial password is registered. The initial password is printed on the label on the Amplifier Unit itself.



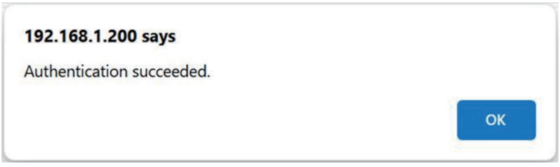
V640 RFID Reader/Writer

English

Login

Password: ••••••••

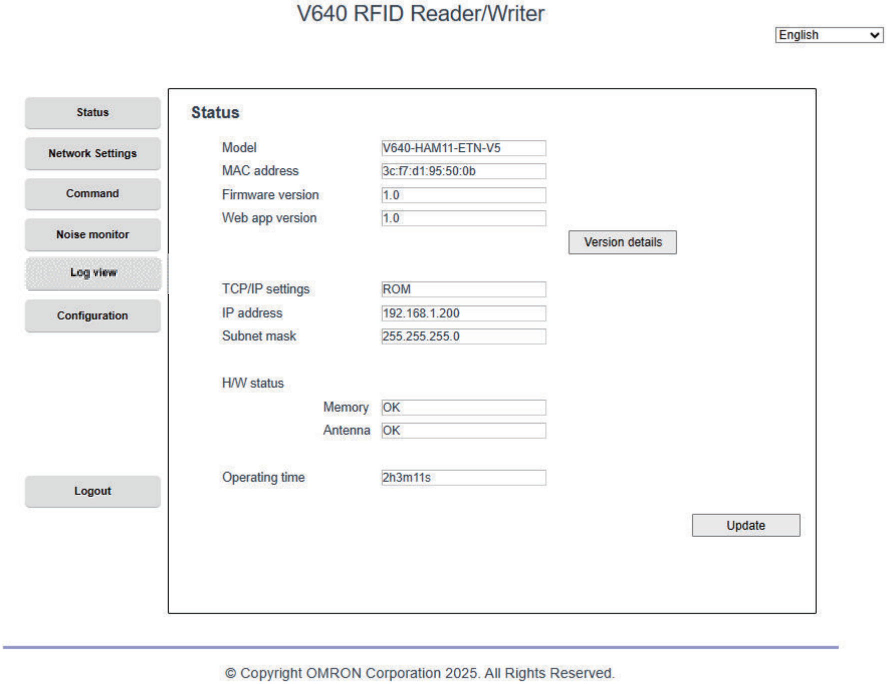
If the Web Password matches and authentication is successful, the following dialog will be displayed.



192.168.1.200 says

Authentication succeeded.

Then, the Status window will be displayed.



V640 RFID Reader/Writer

English

Status

Model: V640-HAM11-ETN-V5
MAC address: 3c:f7:d1:95:50:0b
Firmware version: 1.0
Web app version: 1.0

TCP/IP settings: ROM
IP address: 192.168.1.200
Subnet mask: 255.255.255.0

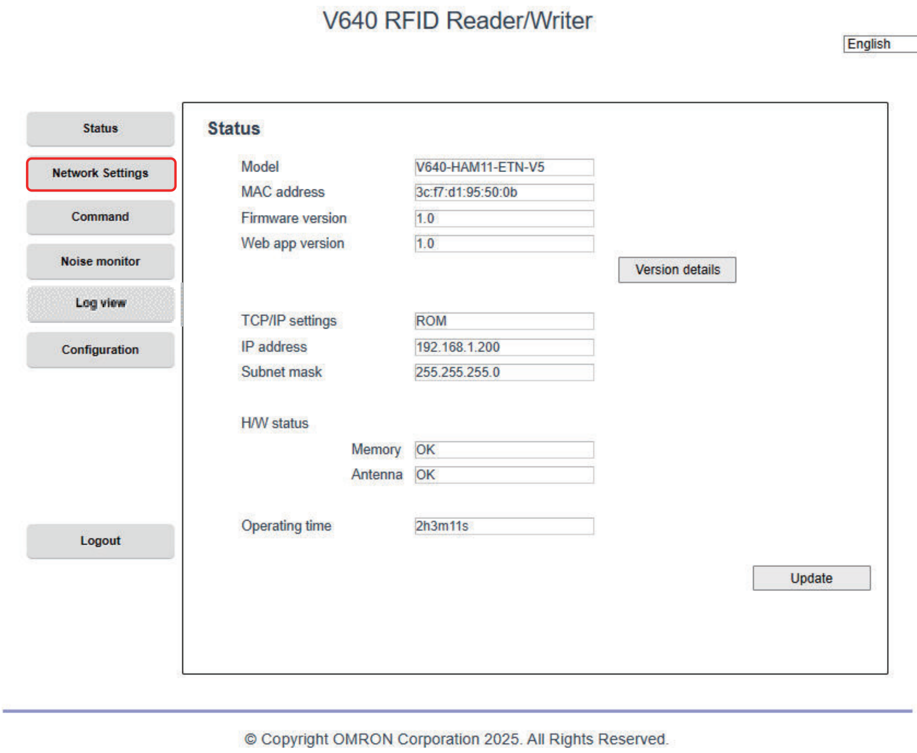
H/W status
Memory: OK
Antenna: OK

Operating time: 2h3m11s

© Copyright OMRON Corporation 2025. All Rights Reserved.

3 Displays the **TCP/IP Settings** tab.

1) Click the **Network Settings** button at the left side of the Web Browser.



V640 RFID Reader/Writer

Status

Model V640-HAM11-ETN-V5
MAC address 3c:f7:d1:95:50:0b
Firmware version 1.0
Web app version 1.0

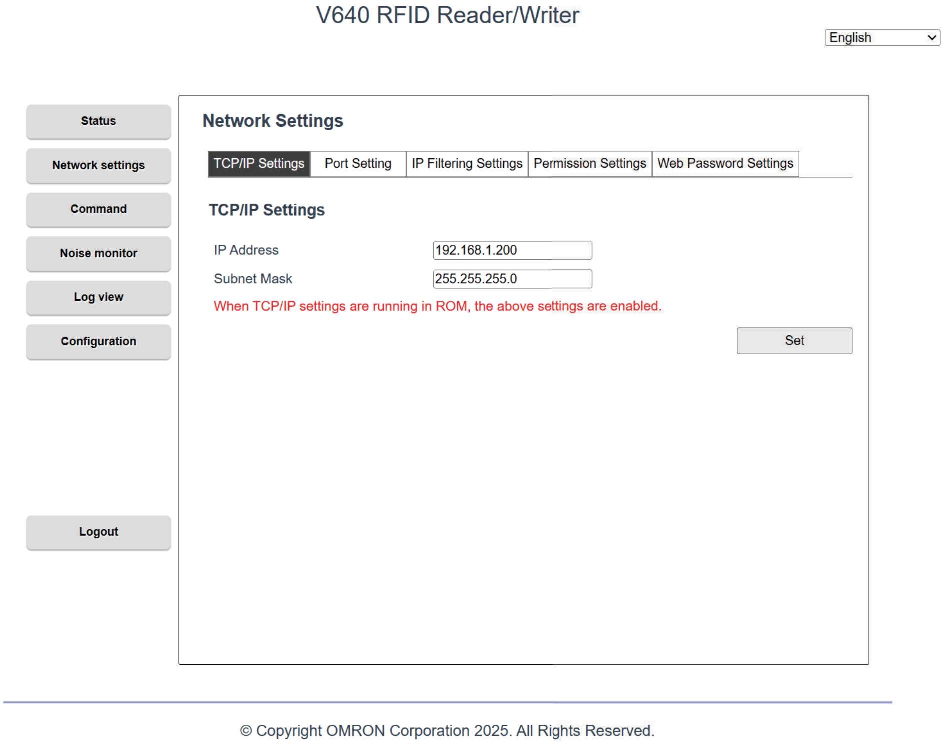
TCP/IP settings ROM
IP address 192.168.1.200
Subnet mask 255.255.255.0

H/W status
Memory OK
Antenna OK

Operating time 2h3m11s

© Copyright OMRON Corporation 2025. All Rights Reserved.

2) On the **Network Settings** window, select the **TCP/IP Settings** tab. The **TCP/IP Settings** tab will be displayed.



V640 RFID Reader/Writer

Network Settings

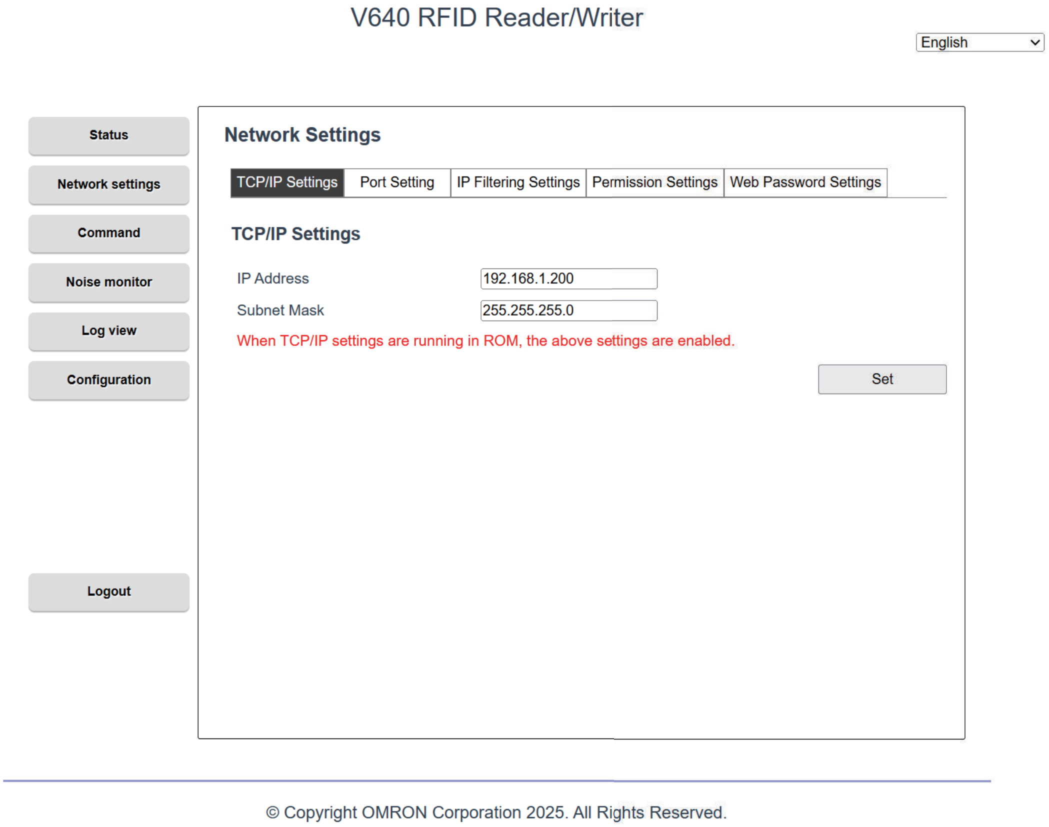
TCP/IP Settings

IP Address 192.168.1.200
Subnet Mask 255.255.255.0

When TCP/IP settings are running in ROM, the above settings are enabled.

© Copyright OMRON Corporation 2025. All Rights Reserved.

4 Set the IP address of the Amplifier Unit.
Enter the **IP address** and **subnet mask** settings on the **TCP/IP Settings** tab and click the **Set** button.



V640 RFID Reader/Writer

Network Settings

TCP/IP Settings

IP Address: 192.168.1.200

Subnet Mask: 255.255.255.0

When TCP/IP settings are running in ROM, the above settings are enabled.

© Copyright OMRON Corporation 2025. All Rights Reserved.

5 Set all DIP Switchs 1 to 5 on the Amplifier Unit to OFF.

Precautions for Correct Use

The values are enabled when the Amplifier Unit is restarted.

3-2-4 Setting the Communications Conditions of the Amplifier Units for Command from the Host Device

You can set the following items with a SET NETWORK command.

- IP address
- Subnet mask

Refer to *4-1-14 SET NETWORK* on page 4-23 for the setting method for command from the host device.

Precautions for Correct Use

When changing the Communications Conditions, restart the amplifier unit. The values are enabled when the Amplifier Unit is restarted.

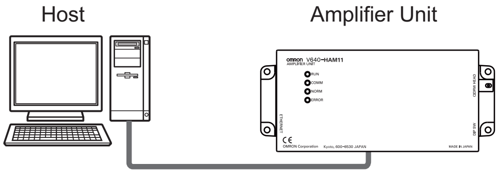
3-3 Communications Test

3-3-1 Communications Test with the Host Device

A communications test is performed to confirm that the host device and Amplifier Unit are connected correctly.

Precautions for Correct Use

For host communication specifications, see *Host Communications Specifications* on page A-3.



A test is preformed for the Amplifier Unit using the data 12345678.

Command

Command code		Test data								CR
		Data 1		Data 2		Data 3		Data 4		
1	0	1	2	3	4	5	6	7	8	0Dh

Response

If the response test data matches the command, the host device and Amplifier Unit are connected correctly.

Response code		Test data								CR
		Data 1		Data 2		Data 3		Data 4		
0	0	1	2	3	4	5	6	7	8	0Dh

3-3-2 Communications Test between ID Tags and CIDRW System

Send a command from the host device and check that normal communications with the ID Tag is possible.
Place an ID Tag in the communications area of the CIDRW Head connected to the Amplifier Unit for which communications is to be tested.

- **READ**

The data is read from pages 1 and 3 of the Amplifier Unit.

ID Tag contents

Page 1	12h	34h	56h	78h	90h	12h	34h	56h
Page 2								
Page 3	11h	22h	33h	44h	55h	66h	77h	88h
Page 4								

Command

Command code				Page designation[*1]								CR
0	1	0	0	0	0	0	0	0	0	1	4	0Dh

*1. Binary notation of *Page designation*

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0

Response

Response code		Page 1																Page 3																CR
0	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	1	1	2	2	3	3	4	4	5	5	6	6	7	7	8	8	0Dh

- **WRITE**

The data is written to pages 8 and 10 of the Amplifier Unit.

Command

Command code				Page designation[*1]								Data of page 8																Data of page 10																CR
0	2	0	0	0	0	0	0	0	A	0	0	1	1	2	2	3	3	4	4	5	5	6	6	7	7	8	8	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0Dh

*1. Binary notation of *Page designation*

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0

Response

Response code		CR
0	0	0Dh

If the command ends normally, the contents of the ID Tag will be as follows:

Page 7								
Page 8	11h	22h	33h	44h	55h	66h	77h	88h
Page 9								
Page 10	01h	23h	45h	67h	89h	ABh	CDh	EFh
Page 11								

4

Reading from/Writing to ID Tags

4-1 Command/Response Format 4-2

4-1-1 Command / Response 4-2
4-1-2 READ 4-4
4-1-3 WRITE 4-6
4-1-4 SAME WRITE 4-8
4-1-5 BYTE WRITE 4-9
4-1-6 TEST 4-10
4-1-7 NAK 4-11
4-1-8 GET PARAMETER 4-12
4-1-9 GET LAST COMMAND 4-18
4-1-10 GET COMMUNICATIONS HISTORY 4-19
4-1-11 CLEAR COMMUNICATIONS HISTORY 4-20
4-1-12 NOISE MEASUREMENT 4-21
4-1-13 RESET 4-22
4-1-14 SET NETWORK 4-23

4-1 Command/Response Format

Command

Command code				Parameter						CR
				1		· · ·		n		
										0Dh

Response

Response code		Parameter						CR
		1		· · ·		n		
								0Dh

4-1-1 Command / Response

Command Code List

Name	Value	Function	See
READ	0100	When this command is received, the system communicates with the ID Tag, and reads the specified page(s) of data. Any pages up to a maximum of 16 can be selected.	page 4-4
WRITE	0200	When this command is received, the system communicates with the ID Tag, and writes the specified page(s) of data. Any pages up to a maximum of 16 can be selected.	page 4-6
SAME WRITE	0300	When this command is received, the system communicates with the ID Tag, and writes the same data in page units to the specified pages. Up to 17 pages, which is the maximum number of pages for an ID Tag, can be specified.	page 4-8
BYTE WRITE	0400	When this command is received the system communicates with the ID Tag, and writes data to the area specified by a first address and number of bytes. A maximum of 128 bytes can be specified.	page 4-9
TEST	10	Sends received data to the host device.	page 4-10
NAK	12	Sends the response made immediately before again.	page 4-11
GET PARAMETER	14	Gets the model number, MAC address, or another parameter.	page 4-12
GET LAST COMMAND	15	Gets the command code of the last command that was executed.	page 4-18
GET COMMUNICATIONS HISTORY	16	Gets the history of communications from when the power was turned ON (total number of communications, total successful communications, and total number of failed communications).	page 4-19
CLEAR COMMUNICATIONS HISTORY	17	Clears the communications history.	page 4-20
NOISE MEASUREMENT	40	Measures the noise in the vicinity of the CIDRW Head.	page 4-21
RESET	7F	Resets the Amplifier Unit.	page 4-22
SET NETWORK	A3	Sets the network.	page 4-23

Response Code List

Type	Response code	Name	Description
Normal end	00	Normal end	Command execution is completed normally.
Host communications error	14	Format error	There is a mistake in the command format. (For example, the command code is undefined, or the page or address specification is inappropriate.)
Communications error	70	Communications error	Noise or another hindrance occurs during communications with an ID Tag, and communications cannot be completed normally.
	71	Verification error	Correct data cannot be written to an ID Tag.
	72	No Tag error	Either there is no ID Tag in front of the CIDRW Head, or the CIDRW Head is unable to detect the ID Tag due to environmental factors (e.g., noise).
	7B	Outside write area error	A write operation was not completed normally because the ID Tag was in an area in which the ID Tag could be read but not written.
	7E	ID system error (1)	The ID Tag is in a status where it cannot execute command processing.
	7F	ID system error (2)	An inapplicable ID Tag has been used.
CPU hardware error	9A	Hardware error in CPU	An error occurred when writing to EEPROM.

4-1-2 READ

Reads any pages of data from the ID Tag. The maximum number of pages that can be read at one time is 16.

Command

Command code				Page designation (8 characters)[*1]								CR
0	1	0	0									0Dh

*1. Details of *Page designation (8 characters)*

Bit	7	-	0	7	-	3	2	1	0	7	6	-	1	0	7	6	-	2	1	0
Page	Sys	-	Sys	Sys	-	Sys	17	16	15	14	13	-	8	7	6	5	-	1	Sys	Sys
Designation	0*	0*		0*	0*	0*	0/1	0/1	0/1	0/1	0/1	•••	0/1	0/1	0/1	0/1	•••	0/1	0*	0*
Value	00			00 to 07						00 to FF					00 to FC					

* Always specify 0. If you specify 1 an error (Response code: 14) will occur.

Parameter Description

Parameter	Description
Page designation	Pages are specified by setting the bits corresponding to pages that are to be read to 1 and setting the other bits to 0, then converting the result to a hexadecimal character string.

Additional Information

Refer to *A-4 ID Tag Memory Maps* on page A-39.

The response code (when normal: 00) and the data in the specified pages are returned in ascending order of page numbers.

Response

Response code		Read data														CR
		Page n						・・・		Page m (n<m)						
		Data 1		・・・		Data 8				Data 1		・・・		Data 8		
0	0															0Dh

Example: Reading Data from Pages 1 and 3 of the Amplifier Unit.

Data Content of the ID Tag

Page 1	12h	34h	56h	78h	90h	12h	34h	56h
Page 2								
Page 3	11h	22h	33h	44h	55h	66h	77h	88h
Page 4								

Command

Command code				Page designation*1								CR
0	1	0	0	0	0	0	0	0	0	1	4	0Dh

*1. Binary notation of *Page designation*

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0

Response

Response code		Page 1																Page 3																CR
0	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	1	1	2	2	3	3	4	4	5	5	6	6	7	7	8	8	0Dh

Precautions for Correct Use

If you send a “Read“ command that specified 1 to 2 page to a 1-page only ID Tag, the Amplifier Unit will response 2nd page data as all zero.

4-1-3 WRITE

Data is written in page units to the ID Tag. Any page(s) can be specified. It is possible to write to a maximum of 16 pages at one time.

Command

<table>
<tr><th colspan="4" rowspan="3">Command code</th><th colspan="8" rowspan="3">Page designation (8 characters)*1</th><th colspan="14">Write data</th><th rowspan="3">CR</th></tr>
<tr><th colspan="6">Pagen</th><th colspan="2" rowspan="2">· · ·</th><th colspan="6">Pagem(n<m)</th></tr>
<tr><th colspan="2">Data1</th><th colspan="2">· · ·</th><th colspan="2">Data8</th><th colspan="2">Data1</th><th colspan="2">· · ·</th><th colspan="2">Data8</th></tr>
<tr><td>0</td><td>2</td><td>0</td><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>0Dh</td></tr>
</table>

*1. Details of *Page designation (8 characters)*

Bit	7	-	0	7	-	3	2	1	0	7	6	-	1	0	7	6	-	2	1	0
Page	Sys	-	Sys	Sys	-	Sys	17	16	15	14	13	-	8	7	6	5	-	1	Sys	Sys
Designation	0*	0*		0*	0*	0*	0/1	0/1	0/1	0/1	0/1	•••	0/1	0/1	0/1	0/1	•••	0/1	0*	0*
Value	00			00 to 07						00 to FF					00 to FC					

* Always specify 0. If you specify 1 an error (Response code: 14) will occur.

Parameter Description

Parameter	Description
Page designation	Pages are specified by setting the bits corresponding to pages that are to be read to 1 and setting the other bits to 0, then converting the result to a hexadecimal character string.
Write data	The data to be written to the specified pages is specified in ascending order of page numbers.

Additional Information

Refer to *A-4 ID Tag Memory Maps* on page A-39.

Response

The response code (when normal: 00) is returned.

Response code		CR
0	0	0Dh

Example: Writing Data to Pages 8 and 10 of the Amplifier Unit

Command

Com-mand code				Page designation[*1]								Data of Page 8																Data of page 10																CR
0	2	0	0	0	0	0	0	0	A	0	0	1	1	2	2	3	3	4	4	5	5	6	6	7	7	8	8	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0Dh

[*1] Binary notation of *Page designation*

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0

Response

Response code		CR 9
0	0	0Dh

The ID Tag status on normal completion is as shown below.

Page 7								
Page 8	11h	22h	33h	44h	55h	66h	77h	88h
Page 9								
Page 10	01h	23h	45h	67h	89h	ABh	CDh	EFh
Page 11								

4-1-4 SAME WRITE

This command writes the same data to multiple pages of an ID Tag.
Any page(s) can be specified.

Command

Command code				Page designation (8 characters)[*1]								Write data						CR
												Data 1		• • •		Data 8		
0	3	0	0															0Dh

*1. Details of *Page designation (8 characters)*

Bit	7	-	0	7	-	3	2	1	0	7	6	-	1	0	7	6	-	2	1	0
Page	Sys	-	Sys	Sys	-	Sys	17	16	15	14	13	-	8	7	6	5	-	1	Sys	Sys
Designation	0*	0*		0*	0*	0*	0/1	0/1	0/1	0/1	0/1	•••	0/1	0/1	0/1	0/1	•••	0/1	0*	0*
Value	00			00 to 07						00 to FF					00 to FC					

* Always specify 0. If you specify 1 an error (Response code: 14) will occur.

Parameter Description

Parameter	Description
Page designation	Pages are specified by setting the bits corresponding to pages that are to be read to 1 and setting the other bits to 0, then converting the result to a hexadecimal character string.
Write data	Specify the write data.

Precautions for Correct Use

Refer to *A-4 ID Tag Memory Maps* on page A-39.

Response

The response code (when normal: 00) is returned.

Response code		CR
0	0	0Dh

Example: Clearing All Data on Pages 1 and 17 of the Amplifier Unit to 0

Command

Command code				Page designation[*1]								Write data																CR
0	3	0	0	0	0	0	7	F	F	F	C	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0Dh

*1. Binary notation of *Page designation*

0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0

Response

Response code		CR
0	0	0Dh

4-1-5 BYTE WRITE

This command writes data to any specified number of bytes starting from the address specified in the ID Tag.

The maximum number of bytes that can be written at one time is 128.

Command

Command code				First address		Write data						CR
						Data 1		・・・		Data n		
0	4	0	0									0Dh

* Data number n = number of bytes written to (2-character units)

Parameter Description

Parameter	Description
First address	Addresses can be specified in the range 00h to 87h.
Write data	Up to 128 bytes of write data, starting from the specified address, can be specified.

Additional Information

Refer to *A-4 ID Tag Memory Maps* on page A-39.

Response

The response code (when normal: 00) is returned.

Response code		CR
0	0	0Dh

Example: Writing Two Bytes of Data to Address 05h of the Amplifier Unit

Command

Command code				First address		Write data				CR
						Data 1		Data 2		
0	4	0	0	0	5	1	2	3	4	0Dh

Response

Response code		CR
0	0	0Dh

The ID Tag status on normal completion is as shown below.

Page 1						12h	34h	
Page 2								
Page 3								

4-1-6 TEST

Performs a communications test on communications between the host device and Amplifier Unit.
When an Amplifier Unit receives a test command, it sends the response code and command test data to the host device as the response.

Command

Command code		Test data						CR
		Data 1		· · ·		Data n		
1	0							0Dh

* Number of data n < 136 (2-character units)

Parameter Description

Parameter	Description
Test data	The data to be sent in the test is specified with a hexadecimal value. (270 characters max.) However, note that odd numbers of characters cannot be used.

Response

The response code (when normal: 00) and the received test data are returned.

Response code		Test data						CR
		Data 1		· · ·		Data n		
0	0							0Dh

Example: Performing a Test for the Amplifier Unit Using the Data *12345678*

Command

Command code		Test data								CR
		Data 1		Data 2		Data 3		Data 4		
1	0	1	2	3	4	5	6	7	8	0Dh

Response

Response code		Test data								CR
		Data 1		Data 2		Data 3		Data 4		
0	0	1	2	3	4	5	6	7	8	0Dh

4-1-7 NAK

Sends the response made immediately before again.

Command

Command code		CR
1	2	0Dh

Response

Sends the response made immediately before again.

Precautions for Correct Use

A response will not be returned if a NAK command is executed immediately after startup.

4-1-8 GET PARAMETER

This command gets the model number, firmware version, or another parameter.

Command

Command code		Parameter type		CR
1	4			0Dh

Parameter Description

Parameter	Value	Description
Parameter type	01	Model number
	02	Firmware version
	03	MAC address
	04	Firmware version details
	10	DIP Switch enabled/disabled status
	11	IP address on DIP Switch
	12	Subnet address on DIP Switch
	13	IP address in ROM
	14	Subnet address in ROM
	20	Memory status
	21	Antenna connection status
	F0	Hardware error

Response

The response code (00: normal) and received parameter value are returned.

Response code		Parameter value				CR
0	0					0Dh

* The contents and length of the **parameter value** depend on the parameter type that is specified for the command.

Example 1: Getting the Model Number of Amplifier Unit

Command

Command code		Parameter type		CR
1	4	0	1	0Dh

Response

The product model number is returned as an ASCII text string.

Response code		Model number														CR
0	0	V	6	4	0	-	H	A	M	1	1	-	E	T	N	0Dh

Example 2: Getting the Firmware Version of Amplifier Unit

Command

Command code		Parameter type		CR
1	4	0	2	0Dh

Response

The response code (00: normal) and firmware version are returned as a 4-digit decimal number.

Response code		Firmware version				CR
0	0	0	1	0	0	0Dh
		Major version		Minor version		

* The above response is for a firmware version of *1.00*.

Example 3: Getting the MAC Address of Amplifier Unit

Command

Command code		Parameter type		CR
1	4	0	3	0Dh

Response

The response code (00: normal) and MAC address are returned.

Response code		MAC address												CR
0	0	0	0	1	F	1	6	1	A	B	9	8	E	0Dh

* The above response is for a MAC address of *00:1F:16:1A:B9:8E*.

Example 4: Getting the Firmware Version Details of Amplifier Unit

Command

Command code		Parameter type		CR
1	4	0	4	0Dh

Response

The response code (00: normal) and firmware version details are returned as a 6-digit decimal number.

Response code		Firmware version						CR
0	0	0	1	0	2	0	3	0Dh
		Major version		Minor version		Revision		

* The above response is for a firmware version of *1.02.03*.

Example 5: Checking If Network Settings on DIP Switch on Amplifier Unit are Enabled or Disabled

Command

Command code		Parameter type		CR
1	4	1	0	0Dh

Response

The response code (00: normal) and enabled/disabled status of the DIP Switch network settings are returned.

Response code		DIP Switch enabled/disabled		CR
0	0	0	1	0Dh

* The above response is for when the DIP Switch settings are enabled. The response will show 00 for disabled status.

Example 6: Checking IP Address on DIP Switch on Amplifier Unit

Command

Command code		Parameter type		CR
1	4	1	1	0Dh

Response

The response code (00: normal) and IP address on the DIP Switch (decimal, four octets of 3 digits each) are returned.

Response code		IP address on DIP Switch												CR
0	0	1	9	2	1	6	8	0	0	1	0	2	0	0Dh
		First octet			Second octet			Third octet			Fourth octet			

* The above response is for when the IP address on the DIP Switch is *192.168.1.20*.
* The following response will be returned if the DIP Switch network settings are disabled.

Response code		IP address on DIP Switch												CR
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0Dh
		First octet			Second octet			Third octet			Fourth octet			

Example 7: Checking the Subnet Mask on the DIP Switch of Amplifier Unit

Command

Command code		Parameter type		CR
1	4	1	2	0Dh

Response

The response code (00: normal) and subnet mask (decimal, four octets of 3 digits each) are returned.

Response code		Subnet mask on DIP Switch												CR
0	0	2	5	5	2	5	5	2	5	5	0	0	0	0Dh
		First octet			Second octet			Third octet			Fourth octet			

* The subnet mask is always *255.255.255.0* regardless of whether the DIP Switch network settings are enabled or disabled.

Example 8: Checking IP Address in ROM

Command

Command code		Parameter type		CR
1	4	1	3	0Dh

Response

The response code (00: normal) and IP address in ROM (decimal, four octets of 3 digits each) are returned.

Response code		IP address on DIP Switch												CR
0	0	1	9	2	1	6	8	0	0	1	2	0	0	0Dh
		First octet			Second octet			Third octet			Fourth octet			

* The above response is for when the IP address in ROM is *192.168.1.200*.

Example 9: Checking the Subnet Mask in ROM

Command

Command code		Parameter type		CR
1	4	1	4	0Dh

Response

The response code (00: normal) and subnet mask (decimal, four octets of 3 digits each) are returned.

Response code		IP address on DIP Switch												CR
0	0	2	5	5	2	5	5	2	5	5	0	0	0	0Dh
		First octet			Second octet			Third octet			Fourth octet			

* The above response is for when the subnet mask in ROM is *255.255.255.0*.

Example 10: Getting the Memory Status of Amplifier Unit

Command

Command code		Parameter type		CR
1	4	2	0	0Dh

Response

The response code (00: normal) and memory check results for internal EEPROM are returned.

Response code		Memory status		CR
0	0	0	1	0Dh

* “Memory status” will be if the memory is normal:"01", and is error:"00".

Example 11: Getting the Antenna Connection Status of Amplifier Unit

Command

Command code		Parameter type		CR
1	4	2	1	0Dh

Response

The response code (00: normal) and Antenna connection status are returned.

Response code		Antenna connection status		CR
0	0			0Dh

* “Antenna connectionstatus” will be if the antenna is connected correctly:"01", and is not correctly:"00".

Example 12: Getting some Hardware error as System error

Command

Command code		Parameter type		CR
1	4	F	0	0Dh

Response

The response code (00: normal) and System error code are returned as a 2-digit hexadecimal number.

Response code		System error code		CR
0	0	0	0	0Dh

* “System erroe code” will be if the hardware is normal:"00".

* If the value is anything other than "00", contact your OMRON representative.

4-1-9 GET LAST COMMAND

Gets the command code of the last command that was executed.

Command

Command code		CR
1	5	0Dh

Response

This command returns the command code of the last command that was executed.

When There Is a Previously Executed Command

Response code		Command code				CR
0	0					0Dh

* The *command code* is given as two or four characters.

When There Is No Previously Executed Command

Response code		Command code		CR
0	0	0	0	0Dh

4-1-10 GET COMMUNICATIONS HISTORY

This command gets the history of communications from when the power was turned ON (total number of communications, total successful communications, and total number of failed communications).

Command

Command code		CR
1	6	0Dh

Response

This command returns the history of communications from when the power was turned ON. Four hexadecimal digits each are returned for the total number of communications, total number of successful communications, and total number of failed communications.
If the total number of communications exceeds 65,535, all data in the communications history will be reset to 0.

Response code		Total number of communications				Total number of successful communications				Total number of failed communications				CR
0	0													0Dh

Example 1: Getting the Communications History of Amplifier Unit

Command

Command code		CR
1	6	0Dh

Response

The following response is returned if there are 32,000 total communications, 30,000 successful communications, and 2,000 failed communications.

Response code		Total number of communications				Total number of successful communications				Total number of failed communications				CR
0	0	7	D	0	0	7	5	3	0	0	7	D	0	0Dh

4-1-11 CLEAR COMMUNICATIONS HISTORY

This command clears the communications history.

Command

Command code		CR
1	7	0Dh

Response

Response code		CR
0	0	0Dh

4-1-12 NOISE MEASUREMENT

The levels of noise in the vicinity of the CIDRW Head are measured and the noise level is expressed numerically in the range "00" to "99".

Command

Command code		CR
4	0	0Dh

Response

The response code (when normal: 00) and the noise level "00" to "99" are returned.

Response code		Noise level		CR
0	0			0Dh

Refer to *A-3-5 Communications Distance Characteristics vs. Ambient Noise* on page A-38.

4-1-13 RESET

All Amplifier Unit processing is stopped, and the initial status is re-established.

Command

Command code		CR
7	F	0Dh

Response

There is no response to this command.

4-1-14 SET NETWORK

This command sets the IP address and subnet mask in ROM.

Command

Command code		Parameter type		First octet			Second octet			Third octet			Fourth octet			CR
A	3															0Dh

Parameter Description

Parameter	Description
Parameter type	IP address setting: 00 Subnet mask setting: 01
First to fourth octets	The address is set in decimal in four octets of three characters each.

Response

Response code		CR
0	0	0Dh

* If an error occurs when writing to EEPROM, error 9A will be returned.

Precautions for Correct Use

- Never turn OFF the power supply to the Amplifier Unit before a response is received from the Amplifier Unit for this command. Doing so may damage the Amplifier Unit.
- The values are enabled when the Amplifier Unit is restarted.

5

Security

This section describes an overview of security for radio equipment, the need for security measures, and V640-series Ethernet type security functions.

5-1 Security Guide 5-2

5-1-1 Necessity of Security Response 5-2

5-1-2 Purposes of Security Response 5-2

5-1-3 V640-series Compliance 5-3

5-2 Security Functions 5-5

5-2-1 Password Authentication Function 5-6

5-2-2 Access Permission Function 5-13

5-2-3 IP Filtering Function 5-16

5-2-4 Security Log Function 5-19

5-2-5 Factory Reset Function 5-27

5-2-6 Backup Function 5-29

5-1 Security Guide

Lack of security is a major concern for society, especially for IoT equipment. With the ever increasing importance of product safety and quality and data in factory automation (hereinafter referred to as FA) devices, there has been an increase in the number of attacks targeting FA systems themselves, or using organizations and FA systems with inadequate security measures in the supply chain as a springboard.
Accordingly, countries are enacting cybersecurity-related laws and regulations, which cover FA system manufacturers and operators, FA systems and FA system components, whereas industries such as control system industry, semiconductor industry, and automotive industry are standardizing their security requirements. Thus, social demands for cybersecurity are increasingly growing.

The Radio Equipment Directive (RED) 2014/53/EU defines the regulations for radio equipment in Europe.
As *internet connected radio equipment*, RFID devices must comply with the essential requirements of Article 3(3)(d) of the Directive.
For Article 3(3)(d), the EN 18031-1 is applicable.

5-1-1 Necessity of Security Response

To ensure the security and safety of your FA system, in addition to the measures taken by OMRON for its FA products, you should also take security measures according to your roles.
To this end, it is important for you to correctly understand and assess the security risks involved in operations, services, and systems that you provide, and implement appropriate security measures throughout the lifecycle of the FA system.

5-1-2 Purposes of Security Response

It is important to indicate the purpose of security measures, goals, and the necessity of business security measures with clear grounds, and to proceed with agreement with management. Without these consensus, priority is given to other business requirements and it becomes difficult to get alignment and cooperation across divisions. Possible security objectives include the following.

1. Continue business and production
2. Keep the factory safe and ensure product quality
3. Ensure normal operation of FA systems
4. Protect information, know-how, and data related to products and production
5. Ensure the security quality of products and fulfill responsibilities as a manufacturer
6. Meet social demands from standards and external requirements
7. Maintain company’s brand image and prevent loss of customer trust

From these security objectives, identify threats that have a particularly high business impact, calculate the cost of countermeasures, and reach agreement on your goals.

Elements to Protect

It is easier to set goals if you clarify what will have a significant impact on your business in relation to the purpose of your security response. The objective of security measures is to ensure the three elements of security, which are *availability*, *integrity*, and *confidentiality* of operations, services, and products that your company provides.

	Ensuring Availability	Ensuring Integrity	Ensuring Confidentiality
Objective	Prevention of production equipment operation stop	Prevention of production equipment failure due to unauthorized overwriting of settings and data	Prevention of disclosure of important information such as production know-how and control programs
Impact in case of compromise	• Business suspension • Delivery delays • Increased costs	• Quality degradation • Reduced safety • Adverse impact on health • Adverse impact on environment	• Damage to social trust • Loss of business advantage • Breach of laws and regulations

The severity of the impact given by *availability*, *integrity*, and *confidentiality* differs depending on the industry, services and products that you provide, and the assets to protect. In addition, even in the same industry, it varies depending on the business role and the process. It is important to carefully consider which element your company should focus on and promote security measures.
It is important to carefully consider which element your RFID equipment should focus on and promote security measures.
For information about OMRON's product security initiatives and customer risk assessment procedures, see *Security Guideline for Factory Automation System(P162-E1)*.

5-1-3 V640-series Compliance

The V640-series complies with the EN 18031-1.
Utilizing the security element technologies required by standards increases the availability of the product itself and ensures the integrity and confidentiality of internal assets such as data and programs.
The V640-series meets the following security function requirements:

Requirements	Purpose
Prevention of Misoperation	Prevents unauthorized persons or devices from operating RFID equipments by mistake and causing damage to the RFID equipments.
Prevention of Asset Theft	Prevents leakage of user data from RFID equipments.
Non-repudiability	Records log Information to prove that an operation was performed.
Recover	Restores RFID equipments to normal status.

The V640-series protects the following assets.

Protected Assets	Contents
Device Information	• Model • MAC Address • Version • Operating Mode • Status

Protected Assets		Contents
User Settings	Network Settings	• IP Address • Subnet Mask • Port Setting
	Security Settings	• Web Password • Permission Settings • IP Filtering • Port Disable Setting
ID Tag Data[1]		• Production data stored in ID Tags
Log Information		• Communication Log (Total/Success/Error) • Security Log
System Data		• Firmware • Web Application • System Settings

[1] There is no protection function such as encryption for communication with ID Tags. Integrity is ensured by verification when writing.
When reading, check the integrity on the host device if necessary.

V640-series uses the following protocols.

Service/Protocol	Port Number	Authentication
V640 Command/TCP	TCP/7090	No[1]
Web Browser/HTTPS[2]	TCP/443	Yes

[1] There is no authentication, but security can be ensured by Permission Settings, IP Filtering Settings, etc.

[2] A secure protocol is used to connect to and operate the unit via the Web Browser.

Precautions for Correct Use

The purpose of this security guide of this document is to propose the security measures that the users of the RFID equipments should take on their own.
The recommendations we make to our customers in this document are based on the results of our analysis and study. Appropriate security measures vary with customer environment, so these recommendations do not guarantee prevention of all security breaches in customer environments. Referring to this document, please consider and implement analysis and appropriate countermeasures in line with the customer's environment on your own.

5-2 Security Functions

This section explains the security functions available for the V640-series.
The security functions can be used to protect the user programs and various data of the V640-series to protect assets. You can also restrict operations on the Web Browser to prevent misoperations.

The V640-series has the following security functions.

Security Functions	Purpose	Function Overview	Reference
Password Authentication Function	Prevention of Misoperation Prevention of Asset Theft	Authentication is performed for users when connecting to the Web Browser, and operations according to the user's authority are only possible.	*5-2-1 Password Authentication Function* on page 5-6
Access Permission Function	Prevention of Misoperation Prevention of Asset Theft	By setting access authority from the host device to the Amplifier Unit, you can restrict the commands that can be executed.	*5-2-2 Access Permission Function* on page 5-13
IP Filtering Settings Function	Prevention of Asset Theft	This function restricts access from the host device by filtering IP packets during reception processing of the Ethernet port.	*5-2-3 IP Filtering Function* on page 5-16
Security Log Function	Non-repudiability	Operations performed on the unit using the Web Browser are registered as Security Log. This allows you to check when and what operations were performed, and can be used to prevent repudiation when a problem occurs.	*5-2-4 Security Log Function* on page 5-19
Factory Reset Function	Prevention of Asset Theft Recover	Initializes various setting data in the unit to the factory settings.	*5-2-5 Factory Reset Function* on page 5-27
Backup Function	Recover	Saves various settings data in the unit as a backup file on your computer. You can also transfer the settings in the backup file to the unit to replace them.	*5-2-6 Backup Function* on page 5-29

5-2-1 Password Authentication Function

This section explains the Web Password Authentication function.

Overview

You register the Web Password Authentication settings for each Amplifier Unit. When you connect the Web Browser and Amplifier Unit with secure communication (HTTPS), you will be requested to enter a password. If the password matches, you will be authenticated and will be able to operate from the Web Browser.

If you transfer and save the authentication settings to the Amplifier Unit, operation authority can be authenticated even if you connect the Web Browser from another computer.

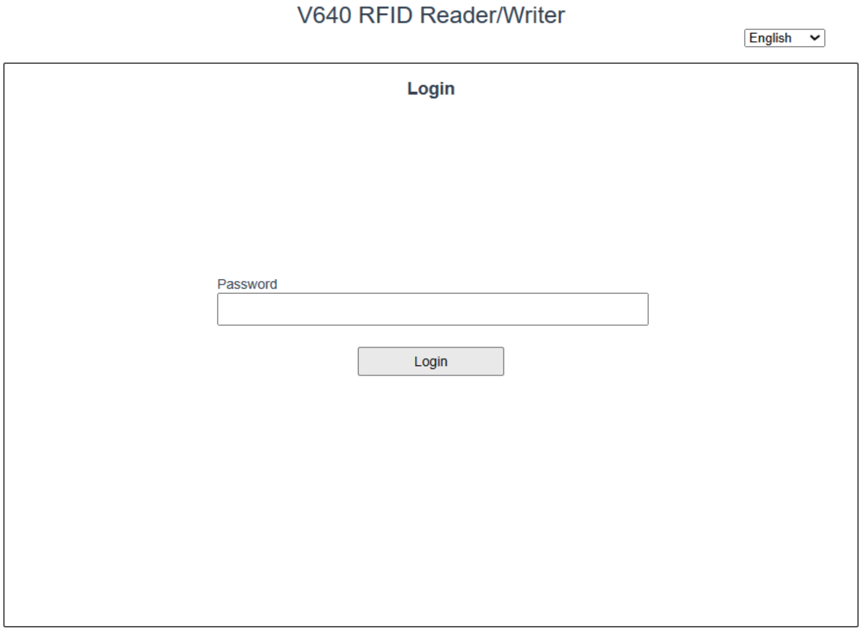
Authentication is performed by password only. User names and other information to identify the operating user are not managed. Therefore, you can only connect one Web Browser to the Amplifier Unit at a time.

The following authority is assigned by Web Password Authentication.

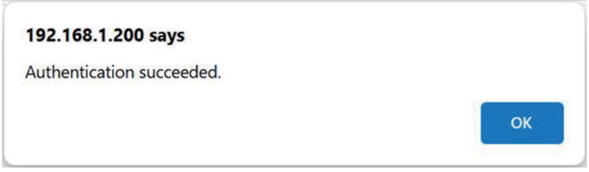
Functions	Authorization
Monitor function	Individual information
	Communication Log
	Security Log
Settings	Network settings
	Security settings
Test function	Commands
	Noise monitor
Maintenance functions	Factory Reset
	Backup (Restore)
	Reboot reset

Authentication Method

When you connect the Web Browser to the Amplifier Unit, the Login Window is displayed and the Web Password Authentication is confirmed.

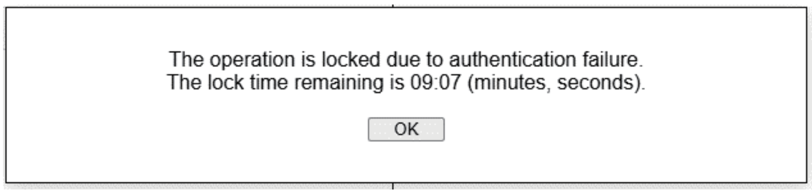


If the entered Web Password matches and authentication is successful, the following dialog is displayed and you can operate from the Web Browser.


192.168.1.200 says

Authentication succeeded.

If the Web Password does not match and authentication fails, you cannot operate from the Web Browser.

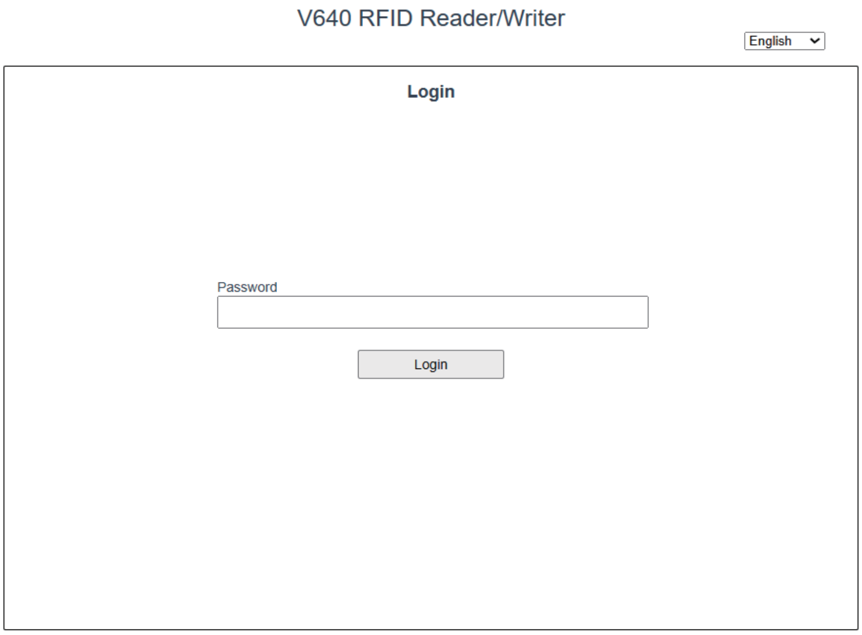

The operation is locked due to authentication failure.
The lock time remaining is 09:07 (minutes, seconds).

Web Password Setting Method

In the factory default settings, a unique initial password is set for each Amplifier Unit.
To ensure confidentiality, change the Web Password when connecting for the first time.

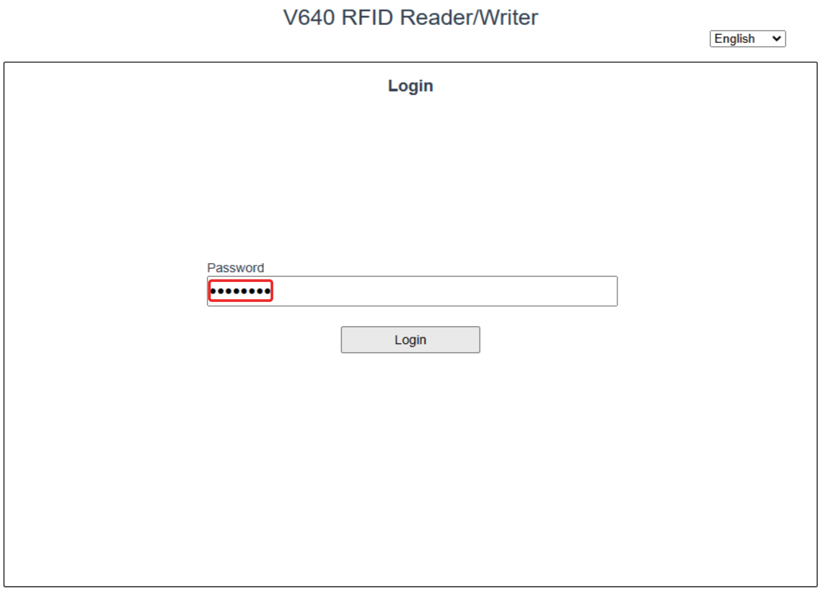
1. Start the browser.

2. Enter the IP Address of the Amplifier Unit in the browser's URL field.
   If the IP Address is the factory default, enter *https://192.168.1.200*.
   The Web Browser Login window will be displayed.



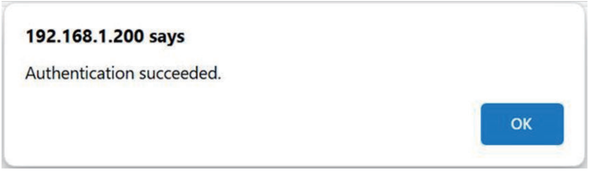
V640 RFID Reader/Writer

3 Enter the Web Password.



V640 RFID Reader/Writer

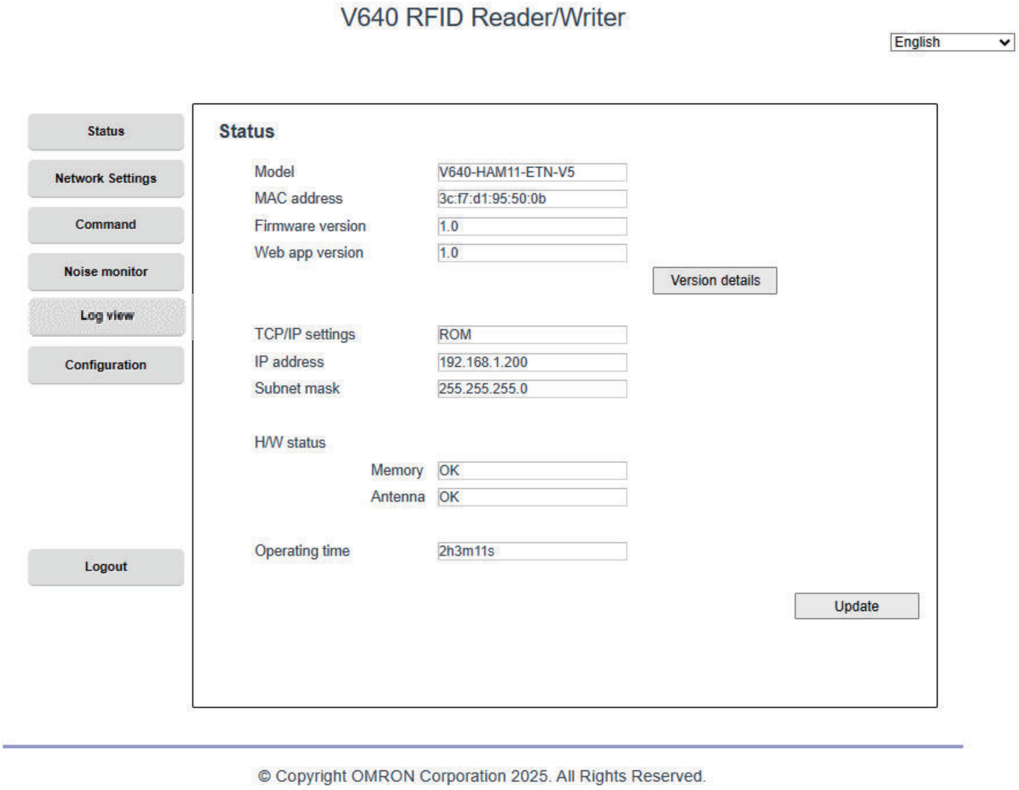
If the Web Password matches and authentication is successful, the following dialog will be displayed.



192.168.1.200 says

Authentication succeeded.

Then, the Status window will be displayed.



V640 RFID Reader/Writer

English

Status

Model	V640-HAM11-ETN-V5
MAC address	3c:f7:d1:95:50:0b
Firmware version	1.0
Web app version	1.0
TCP/IP settings	ROM
IP address	192.168.1.200
Subnet mask	255.255.255.0
H/W status	
Memory	OK
Antenna	OK
Operating time	2h3m11s

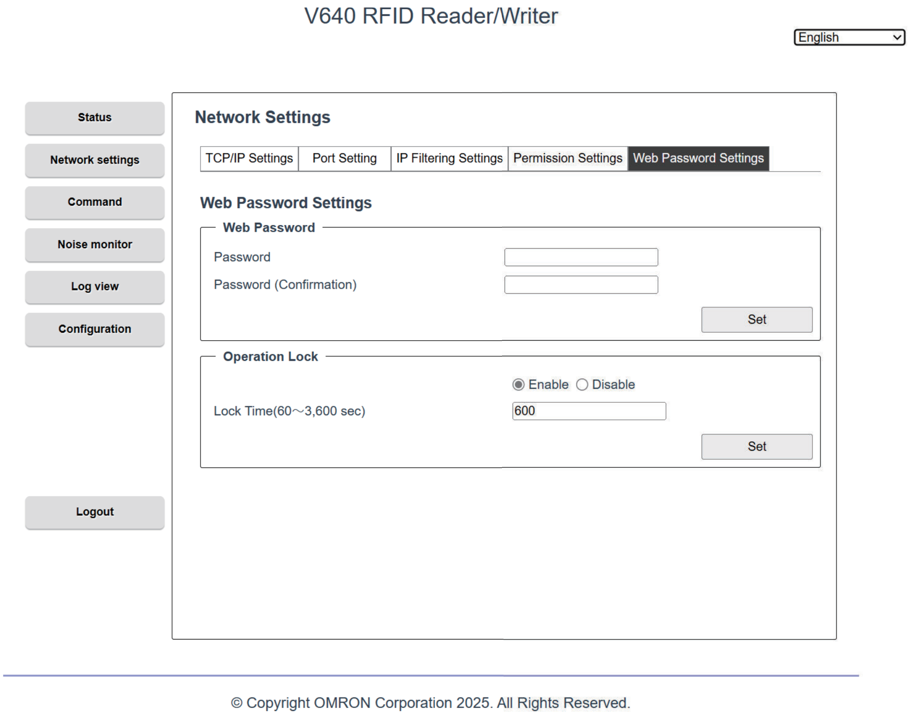
© Copyright OMRON Corporation 2025. All Rights Reserved.

Precautions for Correct Use

- In the factory default settings, an initial password is registered. The initial password is printed on the label on the Amplifier Unit itself.
- It is recommended that you change the initial password when connecting for the first time, as it may be known by a third party.
- Passwords are important information that is only for your use. Store the password properly so that it will not be known to third parties. Also, avoid setting a password that is easy for third parties to guess.
- To strengthen security, we recommend that you change your password regularly.

4 Click **Network Settings** in the Web Browser and select the **Web Password Settings** tab.

The **Web Password Settings** tab of the **Network Settings** window will be displayed.



V640 RFID Reader/Writer

English

Status | Network settings | Command | Noise monitor | Log view | Configuration | Logout

Network Settings

TCP/IP Settings | Port Setting | IP Filtering Settings | Permission Settings | Web Password Settings

Web Password Settings

Web Password

Password

Password (Confirmation)

Set

Operation Lock

● Enable ○ Disable

Lock Time(60～3,600 sec) 600

Set

© Copyright OMRON Corporation 2025. All Rights Reserved.

5 Enter the password you want to change and click the **Set** button.

6 Restart the Amplifier Unit.
The changed Web Password will be effective from the next startup.

Password Specifications

The following are the possible settings for the Web Password used in the Password Authentication function.

Item	Content
Valid number of characters	8 characters or more and 32 characters or less[*1]
Usable characters	Half-width alphanumeric characters and symbols (case-sensitive)[*2]

[*1] Any value between 8 and 32 characters can be set.

[*2] Characters that can be used are ASCII characters 0x21 to 0x7E (0-9 A-Z a-z, '-!"#$%&()*,./:;?@[]^_`{|}~+<=>).

Password Authentication Operation Range

The range of operations that can be performed with the Web Browser varies depending on the operation mode of the Amplifier Unit. The table below shows the respective operation ranges.

Web Browser Window		RUN-Mode	Safe-Mode
Status Window	Model, Version, MAC Address	○Yes	○Yes
	PowerOnTime	○Yes	×No
	TCP/IP information (DIP Switch status, IP Address, Subnet Mask)	○Yes	×No
	Status (Operation Mode, H/W Status, etc.)	○Yes	○Yes
	Reset (Reboot)	○Yes	×No
Network Settings Window	TCP/IP Settings (IP Address, Subnet Mask)	○Yes	×No
	Communication Port Settings (Port Number, Enable/Disable)	○Yes ○Yes	×No
	IP Filtering Settings	○Yes	×No
	Permission Settings	○Yes	×No
	Web Password Settings*1	○Yes	×No
Command Window	CID R/W Test	○Yes	×No
	V640 Command Test	○Yes	×No
Noise Monitor Window	Noise Monitor	○Yes	×No
Log View Window	Communication Log (Latest Communication, Total/Success/Error)	○Yes	×No
	Security Log	○Yes	×No
Configuration	Factory Reset	○Yes	○Yes
	Backup	○Yes	×No
	Restore	○Yes	×No

*1. You cannot view the Web Password.

Additional Information

While operating in Test Mode, there is no communication with the host device, so you cannot operate the unit from the Web Browser.

Lock Function

This section explains the Web Browser lock function. There are two types of lock function: Operation Lock (session timeout) and Authentication Locked.

● Operation Lock (Session Timeout)

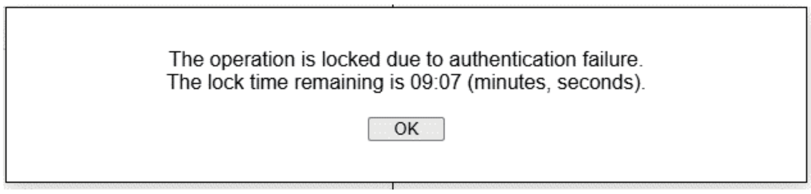
When Operation Lock is enabled, unauthorized operations from the Web Browser can be prevented. After password authentication in the Web Browser, if you do not operate the Web Browser for a certain period of time, you will need to re-enter your password.

You can set Enable/Disable and the time until lock.

Item	Content	Setting range	Initial state
Enable/Disable	Sets whether to enable or disable the Operation Lock function.	Enable, Disable	Enable
Setting time	Time until operation is locked	1 to 60 minutes	10 minutes

● Authentication Locked

Protects assets from cyber attacks such as brute force attacks. If you enter the wrong password five times on the Web Browser Login window, the following dialog box will be displayed and Web Browser operations will be locked for 10 minutes. The lock will be released when the time has passed or the Amplifier Unit is rebooted.



The operation is locked due to authentication failure.
The lock time remaining is 09:07 (minutes, seconds).

Password Handling Methods

This section explains how to erase the Web Password and what to do if you have forgotten the password.

● Password Erasure

The set Web Password can be returned to the factory default state by performing the initialization operation in the Configuration window of the Web Browser. This prevents information leakage when disposing of the Amplifier Unit.

● What to Do If You Have Forgotten Your Password

If the administrator forgets the Web Password, there is no way to check the password. In addition, the password cannot be changed unless there is operation authority after password authentication. If the administrator forgets the Web Password, please handle it as follows.

Handling method	Status after handling
Start the Amplifier Unit to be handled in Safe-Mode and connect the Web Browser. For details, see *6-2-20 Safe-Mode Window* on page 6-26.	The Web Password will be returned to the factory default state along with all the unit settings.

5-2-2 Access Permission Function

This section explains how to set access permissions for commands as protected assets.

Overview

By setting access permissions from the host device to the Amplifier Unit, you can restrict the commands that can be executed.

When setting access permissions, select the access permission to be allowed for each target command. To access a command with restricted access, you must grant access permission.

Access Permission Types

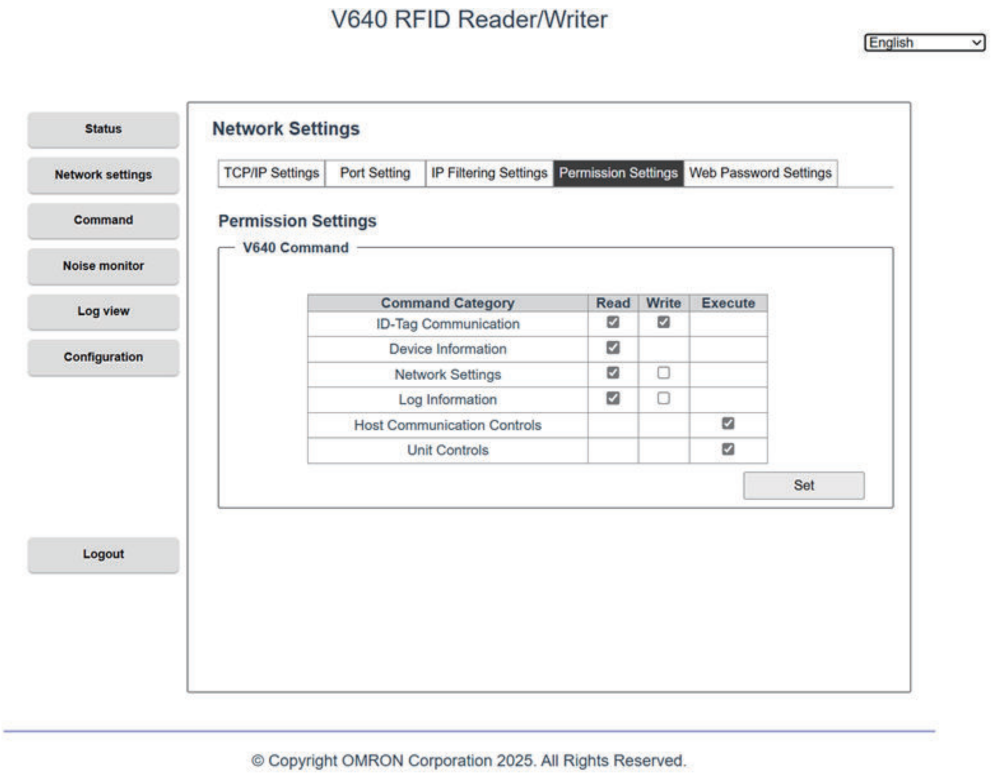
The commands that are subject to access permissions and the types of access permissions are shown below.

(○: Target ---: Not applicable)

Command Category	Access permission		
	Read	Write	Execute
ID-Tag Communication	○	○	---
Device Information	○	---	---
Network Settings	○	○	---
Log Information	○	○	---
Host Communication Controls	---	---	○
Unit Controls	---	---	○

Setting Method

After password authentication, select the Permission Settings tab on the Network Settings window of the Web Browser and set Prohibit/Permission. The settings are saved in the Amplifier Unit itself.



Permission Settings

V640 Command

Command Category	Read	Write	Execute
ID-Tag Communication	☑	☑	
Device Information	☑		
Network Settings	☑	☐	
Log Information	☑	☐	
Host Communication Controls			☑
Unit Controls			☑

Command Category	Permission	Content	Setting range	Initial state
ID-Tag Communication	Read	Access permission for RF Tag communication	Prohibit, Permission	Permission
	Write		Prohibit, Permission	Permission
Device Information	Read	Access permission for Device Information	Prohibit, Permission	Permission
Network Settings	Read	Access permission for Network Settings	Prohibit, Permission	Permission
	Write		Prohibit, Permission	Prohibit
Log Information	Read	Access permission for Log Information	Prohibit, Permission	Permission
	Write		Prohibit, Permission	Prohibit
Host Communication Controls	Execute	Access permission for Host Communication Controls	Prohibit, Permission	Permission
Unit Controls	Execute	Access permission for Unit Controls	Prohibit, Permission	Permission

Access Permission Target Commands

The commands for which access permissions can be set are shown below.

Command Category	Command name	Permission	Code value
ID-Tag Communication	READ	Read	0100
	WRITE	Write	0200
	SAME WRITE	Write	0300
	BYTE WRITE	Write	0400
Device Information	GET PARAMETER (Parameter types 01-04, 20-21, F0)	Read	14
Network Settings	GET PARAMETER (Parameter types 10-14)	Read	14
	SET NETWORK	Write	A3
Log Information	GET COMMUNICATIONS HISTORY	Read	16
	CLEAR COMMUNICATIONS HISTORY	Write	17
Host Communication Controls	TEST	Execute	10
	NAK	Execute	12
	GET LAST COMMAND	Execute	15
Unit Controls	NOISE MEASUREMENT	Execute	40
	RESET	Execute	7F

● Command Behavior without Access Permissions

If the command for which access is not permitted is issued from the host device, the "Format error" (Response code: 14) will occur.

Response

The response code (when normal: 00) is returned.

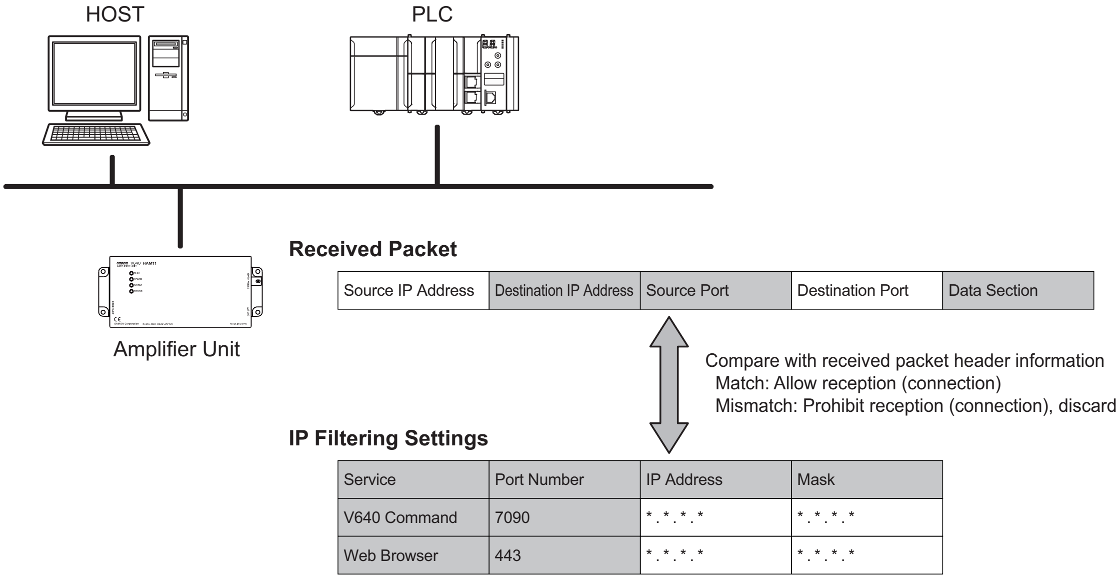
Response code		CR
1	4	0Dh

5-2-3 IP Filtering Function

This section explains the IP filtering function to prevent unauthorized access and theft of assets.

Overview

This function filters IP packets received at the Amplifier Unit's Ethernet port. IP filtering is a technology that determines whether communication is permitted or not based on IP (Internet Protocol) information.
When you enable IP filtering, only host devices with registered IP addresses can access the unit, and access from devices with unregistered IP addresses can be restricted.
The IP filtering function allows you to select packets to be permitted for each service/protocol supported by the Amplifier Unit. This allows communication only with permitted devices and prevents unnecessary packets from being received.


HOST
PLC
Amplifier Unit
Received Packet
Compare with received packet header information
Match: Allow reception (connection)
Mismatch: Prohibit reception (connection), discard
IP Filtering Settings

Received Packet

Source IP Address	Destination IP Address	Source Port	Destination Port	Data Section

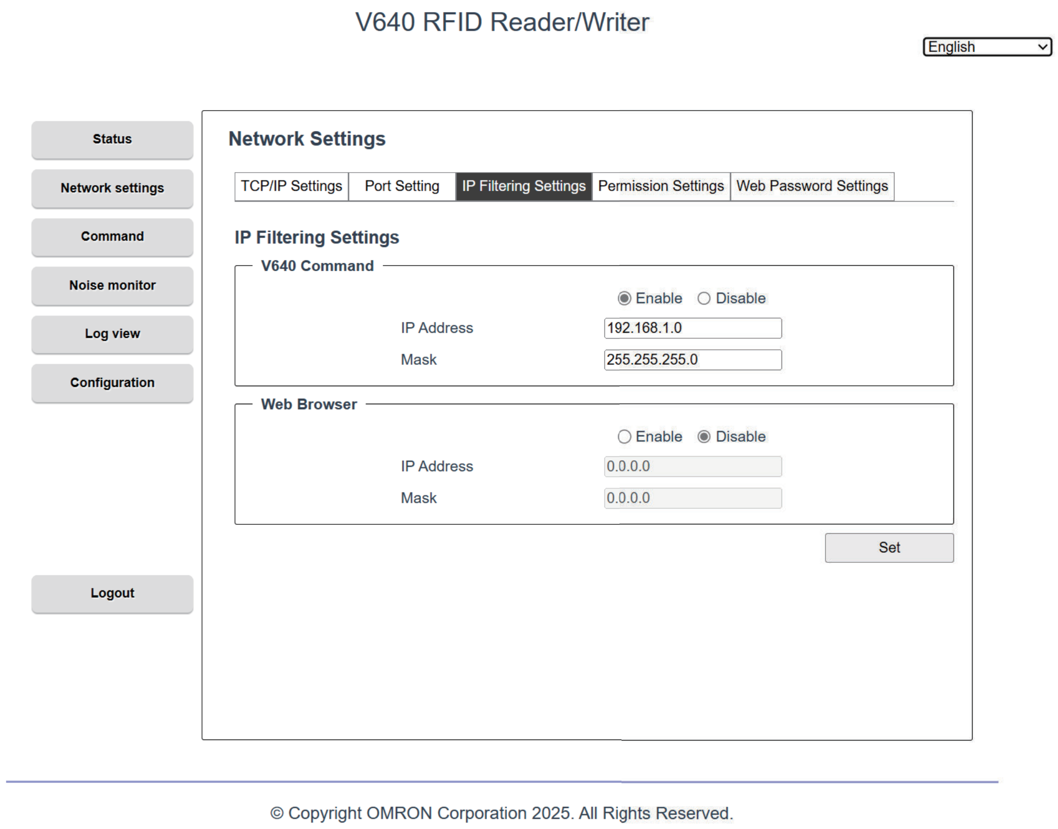
IP Filtering Settings

Service	Port Number	IP Address	Mask
V640 Command	7090	*.*.*.*	*.*.*.*
Web Browser	443	*.*.*.*	*.*.*.*

Setup Method

After password authentication, select the IP Filtering Settings tab on the Network Settings window of your Web Browser and set Enable/Disable and the IP Address. The settings are saved in the Amplifier Unit itself.

The set values are reflected after the Amplifier Unit is rebooted.



V640 RFID Reader/Writer

English

Network Settings

IP Filtering Settings

V640 Command

● Enable ○ Disable

IP Address 192.168.1.0

Mask 255.255.255.0

Web Browser

○ Enable ● Disable

IP Address 0.0.0.0

Mask 0.0.0.0

© Copyright OMRON Corporation 2025. All Rights Reserved.

Target	Item	Content	Setting range	Initial state
V640 Command	Enable/Disable	Enable/Disable IP filtering function for V640 Command	Enable, Disable	Disable
	IP Address	Setting the IP address to allow connection*1	*.*.*.*	None
	Mask	Setting the mask of the IP address to allow connection*2	*.*.*.*	None
Web Browser	Enable/Disable	Enable/Disable IP filtering function for Web Browser	Enable, Disable	Disable
	IP Address	Setting the IP address to allow connection*1	*.*.*.*	None
	Mask	Setting the mask of the IP address to allow connection*2	*.*.*.*	None

*1. The allowed IP address is calculated by the logical AND of the **IP address** and the **Mask**. If you want to allow more than one IP address, mask a part of the IP address by setting the **Mask**. In this case, set 0 to the bits to be masked in the **IP address** and **Mask**.
The following is an example of how to calculate the allowed IP addresses.

Example 1. Allowing IP address 192.168.250.1
If you want to allow one IP address, set 255.255.255.255 to the mask.

Setting	Decimal notation	Binary notation
IP address	192.168.250.1	11000000.10101000.11111010.00000001
Mask	255.255.255.255	11111111.11111111.11111111.11111111

Example 2. Allowing IP address 192.168.250.***

Set 255.255.255.0 to the mask to mask the lower 8 bits of the IP address.

Setting	Decimal notation	Binary notation
IP address	192.168.250.0	11000000.10101000.11111010.00000000
Mask	255.255.255.0	11111111.11111111.11111111.00000000

Example 3. Allowing IP address 192.168.250.1 to 192.168.250.31

Set 255.255.255.224 to the mask to mask the lower 5 bits if the IP address.

Setting	Decimal notation	Binary notation
IP address	192.168.250.0	11000000.10101000.11111010.00000000
Mask	255.255.255.224	11111111.11111111.11111111.11100000

*2. Set 0 to the bits to be masked in **Mask**. Multiple bits can be masked, but only bits from the least significant can be masked. It is not possible to mask the higher bits, such as 0.255.255.255, or the middle bits, such as 255.0.255.255.

The following are examples of setting a mask.

Example 1. Masking the lower 8 bits

Set 0 to the lower 8 bits.

Setting	Decimal notation	Binary notation
Mask	255.255.255.0	11111111.11111111.11111111.00000000

Example 2. Masking the lower 24 bits

Set 0 to the lower 24 bits.

Setting	Decimal notation	Binary notation
Mask	255.0.0.0	11111111.00000000.00000000.00000000

Precautions for Correct Use

- If you enable the IP filtering function of the Web Browser, computers with unregistered IP addresses cannot connect to the Web Browser. Please make sure that the IP addresses of the computers you want to allow connection to are registered correctly before enabling this function.
- If you forget the registered IP address and cannot connect to the Web Browser, you can return to the initial state by starting in Safe Mode and performing the Factory Reset.

5-2-4 Security Log Function

This section describes the function for registering operations performed on the Web Browser as Security Log.

Overview

Changes and controls made to the Amplifier Unit by the host device, and operations performed on the Amplifier Unit by the user using the Web Browser are registered as Security Log. In the Security Log function, these auditable matters are called events.

Events include the IP Address of the communication partner, Source (protocol/service), and PowerOn-Time. Since you can check who performed what operation, when, and what, you can prevent denial when a security problem occurs.

Precautions for Correct Use

This Security Log function does not record events that the Amplifier Unit does not recognize, such as errors on the network line. If necessary, record them on the host device.

Log Information

The following information is registered in the Security Log.

Item	Content
PowerOTime	Time information when the event occurred. The accumulated power-on time (in seconds) in the Amplifier Unit is registered.
Source	Type of the route on which the event occurred. For communication routes, the service/protocol type is registered.
Source details	Detailed information on the route on which the event occurred. For communication routes, the IP address of the communication partner is registered.
Event code	Code to identify the type of event. Defined by the event category and type.
Result	The result of the change, control, or operation that caused the event.
Additional Info 1-2	Additional information on the event result.

The following types of sources are available.

Source type	Code	Description
DIP Switch	0x10	Event caused by DIP Switch operation
Web Browser	0x20	Event caused by Web Browser
V640 Command	0x30	Event caused by V640 Command

The rules for Event codes are as follows:

First 4 digits	Last 4 digits
xxxxHex	xxxxHex
Event category	Event type

The event categories are as follows:

Event category	Code	Description
Access Control	0001Hex	Events to which access control is applied Ex.) Password Authentication, Password Change
Control System	0002Hex	Events that affect system operation Ex.) Changing Operation Mode, Reboot(Restart), etc.
Backup and Restore	0003Hex	Events that affect the overall system configuration Ex.) Factory Reset, performing Backup/Restore
Configuration Changes	0004Hex	Events that change system setting parameters
Audit Log Events	0005Hex	Events related to Security Log Ex.) Clearing Log, Changing log

Event List

The list of events detected by the Amplifier Unit is as follows:

Category	Event code	Event name	Source	See
Access Control Events	0001_0001Hex	Password Authentication	Web Browser	page 5-21
	0001_0002Hex	Password Change	Web Browser	page 5-21
	0001_0010Hex	Operation Lock Change	Web Browser	page 5-21
	0001_0020Hex	Access Permissions Change	Web Browser	page 5-22
Control System Events	0002_0001Hex	Operating Mode Change	DIP Switch	page 5-22
	0002_0002Hex	Reboot	Web Browser V640 Command	page 5-22
Backup and Restore Events	0003_0001Hex	Factory Reset	Web Browser	page 5-23
	0003_0002Hex	Backup	Web Browser	page 5-23
	0003_0003Hex	Restore	Web Browser	page 5-23
Configuration Changes Events	0004_0001Hex	TCP/IP Setting Change	Web Browser V640 Command	page 5-24
	0004_0011Hex	TCP port Change	Web Browser	page 5-24
	0004_0014Hex	WebSocket port Change	Web Browser	page 5-24
	0004_0021Hex	IP Filtering Change (TCP port)	Web Browser	page 5-24
	0004_0022Hex	IP Filtering Change (HTTPS port)	Web Browser	page 5-24
Audit Log Events	0005_FFFFHex	Security Log Clear	None	page 5-25

Event Descriptions

● How to Read the Event Descriptions

The meaning of each item in the table used in the description of each event is shown in brackets [ ].

Event name	[Event name]	**Event code**	[Event code]
Meaning	[Event content]		
Detection timing	[Event detection timing]	**Source**	[Event occurrence source]
Rresults	[Event result]		
Additional Info1-2	[Additional information on event result]		
Precautions/ Remarks	[Notes,Restrictions, Supplementary explanations, etc.]		

● Access Control Events

Event name	Password Authentication	**Event code**	0001_0001Hex
Meaning	Web Browser Password Authentication occurred		
Detection timing	At Login	**Source**	Web Browser
Rresults	Authentication Successful: 00Hex, Authentication Failed: 02Hex, Authentication Locked: 0x0F		
Additional Info1-2	None		
Precautions/ Remarks	---		

Event name	Password Change	**Event code**	0001_0002Hex
Meaning	Web Browser password changed		
Detection timing	Configuration Changes operation	**Source**	Web Browser
Rresults	Normal end: 00Hex		
Additional Info1-2	None		
Precautions/ Remarks	---		

Event name	Operation Lock Change	**Event code**	0001_0010Hex
Meaning	Web Browser Operation Lock setting changed		
Detection timing	Configuration Changes operation	**Source**	Web Browser
Rresults	Disable: 00Hex, Enable: 01Hex		
Additional Info1-2	Additional Info1: Lock Time (60 to 3,600 sec)		
Precautions/ Remarks	---		

Event name	Access Permissions Change	**Event code**	0001_0020Hex
Meaning	Access Permissions settings have been changed		
Detection timing	Configuration Changes operation	**Source**	Web Browser
Rresults	Disable: 00Hex, Enable: 01Hex		
Additional Info1-2	Allocates 1 byte for each target Command Category[*1] Readable = 0x04, Writable = 0x02, Executable = 0x01 logical OR, No permission = 0x00		
Precautions/ Remarks	---		

*1. The contents of the Additional Information are as follows.

	1st byte	2nd byte	3rd byte	4th byte
Additional Info1	ID-Tag Communication	Device Information	Network Settings	Log Information
Additional Info2	Host Communication Controls	Unit Controls	(Reserved)	(Reserved)

● Control System Events

Event name	Operating Mode Change	**Event code**	0002_0001Hex
Meaning	Unit Operation Mode has been changed		
Detection timing	At startup	**Source**	DIP Switch
Rresults	RUN-Mode: 01Hex, Safe-Mode: 02Hex		
Additional Info1-2	None		
Precautions/ Remarks	Detects if the Operation Mode has changed from the previous startup		

Event name	Reboot	**Event code**	0002_0002Hex
Meaning	Unit has been rebooted		
Detection timing	Reboot operation, Receive command	**Source**	Web Browser, V640 Command
Rresults	Normal end: 00Hex		
Additional Info1-2	None		
Precautions/ Remarks	---		

● Backup and Restore Events

Event name	Factory Reset	**Event code**	0003_0001Hex
Meaning	Factory Reset operation performed		
Detection timing	Configuration operation	**Source**	Web Browser
Rresults	Successful: 00Hex, Failed: 02Hex		
Additional Info1-2	Additional Info 1: All initialize (0x0000), Initialize without password (0x0001)		
Precautions/ Remarks	---		

Event name	Backup	**Event code**	0003_0002Hex
Meaning	Backup performed		
Detection timing	Configuration operation	**Source**	Web Browser
Rresults	Successful: 00Hex, Failed: 02Hex		
Additional Info1-2	None		
Precautions/ Remarks	---		

Event name	Restore	**Event code**	0003_0003Hex
Meaning	Restore performed		
Detection timing	Configuration operation	**Source**	Web Browser
Rresults	Successful: 00Hex, Failed: 02Hex		
Additional Info1-2	None		
Precautions/ Remarks	---		

Configuration Changes Events

Event name	TCP/IP Setting Change	Event code	0004_0001Hex
Meaning	TCP/IP Settings have been changed		
Detection timing	Configuration Changes operation, Receive command	Source	Web Browser, V640 Command
Rresults	Normal end: 00Hex		
Additional Info1-2	Additional Info 1: Changed IP Address Additional Info 2: Changed Subnet Mask		
Precautions/ Remarks	---		

Event name	TCP port change	Event code	0004_0011Hex
Meaning	TCP port (V640 Command) settings have been changed		
Detection timing	Configuration Changes operation	Source	Web Browser
Rresults	Normal end: 00Hex		
Additional Info1-2	Additional Info 1: Port Enable/Disable *Currently fixed as Enable, reserved for future expansion Additional Info 2: Port number		
Precautions/ Remarks	---		

Event name	WebSocket port change	Event code	0004_0014Hex
Meaning	WebSocket port settings have been changed		
Detection timing	Configuration Changes operation	Source	Web Browser
Rresults	Normal end: 00Hex		
Additional Info1-2	Additional Info 1: Port Enable/Disable *Currently fixed as Enable, reserved for future expansion Additional Info 2: Port number		
Precautions/ Remarks	---		

Event name	IP Filtering Change (TCP port)	Event code	0004_0021Hex
Meaning	IP Filtering Settings have been changed		
Detection timing	Configuration Changes operation	Source	Web Browser
Rresults	Normal end: 00Hex		
Additional Info1-2	Additional Info 1: Changed IP Address Additional Info 2: Changed Mask		
Precautions/ Remarks	---		

Event name	IP Filtering Change (HTTPS port)	Event code	0004_0022Hex
Meaning	IP Filtering Settings have been changed		
Detection timing	Configuration Changes operation	Source	Web Browser
Rresults	Normal end: 00Hex		
Additional Info1-2	Additional Info 1: Changed IP Address Additional Info 2: Changed Mask		
Precautions/ Remarks	---		

● Audit Log Events

Event name	Security Log Clear	**Event code**	0005_FFFFHex
Meaning	Security Log data error (tampering) detected		
Detection timing	Log data error detected	**Source**	None (0x00)
Rresults	None (0x00)		
Additional Info1-2	None		
Precautions/ Remarks	---		

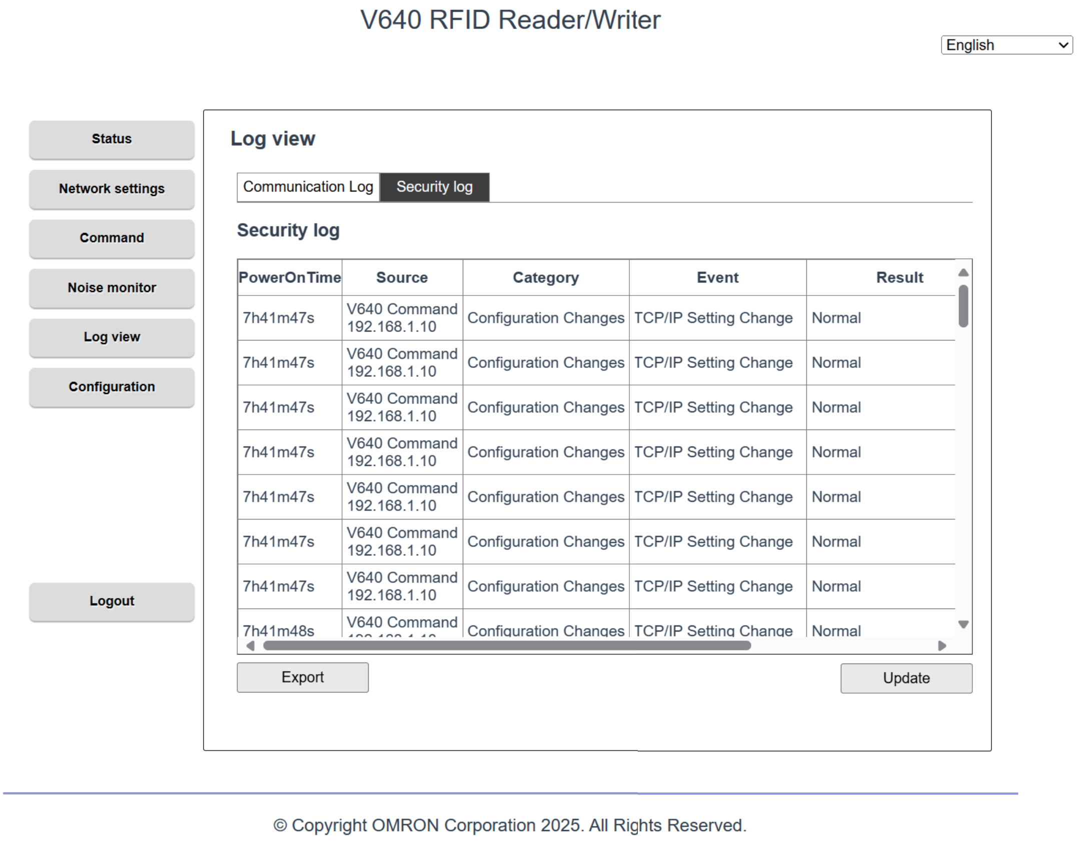
Log Capacity and Storage Conditions

The Security Log is stored in the non-volatile memory of the Amplifier Unit.

Item	Content
Number of saved items	64 items
Storage method	Ring buffer method (oldest contents are overwritten with newest contents)
Storage destination	Non-volatile memory of the Amplifier Unit

Operation Method

The Security Log can be viewed on the **Security Log** tab of the Log view window of the Web Browser. Click the **Export** button to save the Security Log to your computer as a CSV file.



Security log

PowerOnTime	Source	Category	Event	Result
7h41m47s	V640 Command 192.168.1.10	Configuration Changes	TCP/IP Setting Change	Normal
7h41m47s	V640 Command 192.168.1.10	Configuration Changes	TCP/IP Setting Change	Normal
7h41m47s	V640 Command 192.168.1.10	Configuration Changes	TCP/IP Setting Change	Normal
7h41m47s	V640 Command 192.168.1.10	Configuration Changes	TCP/IP Setting Change	Normal
7h41m47s	V640 Command 192.168.1.10	Configuration Changes	TCP/IP Setting Change	Normal
7h41m47s	V640 Command 192.168.1.10	Configuration Changes	TCP/IP Setting Change	Normal
7h41m47s	V640 Command 192.168.1.10	Configuration Changes	TCP/IP Setting Change	Normal
7h41m48s	V640 Command	Configuration Changes	TCP/IP Setting Change	Normal

PowerOnTime

The PowerOnTime registered in the Security Log is the time information accumulated while the Amplifier Unit is powered on, and is saved in the non-volatile memory of the Amplifier Unit.

The PowerOnTime is saved at the following times.

Saving timing	Content
Regular interval	Saved to non-volatile memory once an hour
When Security Log is saved	Saved to non-volatile memory according to the log registration when an event occurs

Precautions for Correct Use

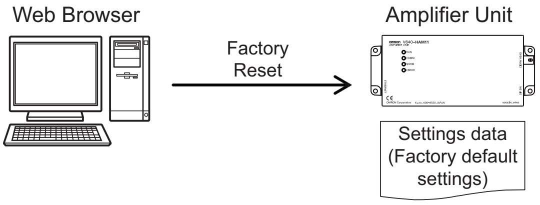
- The PowerOnTime does not represent an exact time. Please use it as a guideline for maintenance.
- Since it is saved every hour, there may be an error of up to 59 minutes and 59 seconds depending on the timing of powering off the Amplifier Unit. Also, if the Amplifier Unit is frequently turned off at intervals of less than one hour, the time may not accumulate correctly.

5-2-5 Factory Reset Function

This section describes the Factory Reset function, which is intended to prevent theft and restore assets when disposing of the Amplifier Unit.

Overview

You can use the Web Browser to reset the various setting data in the Amplifier Unit to the factory settings.



Target Data

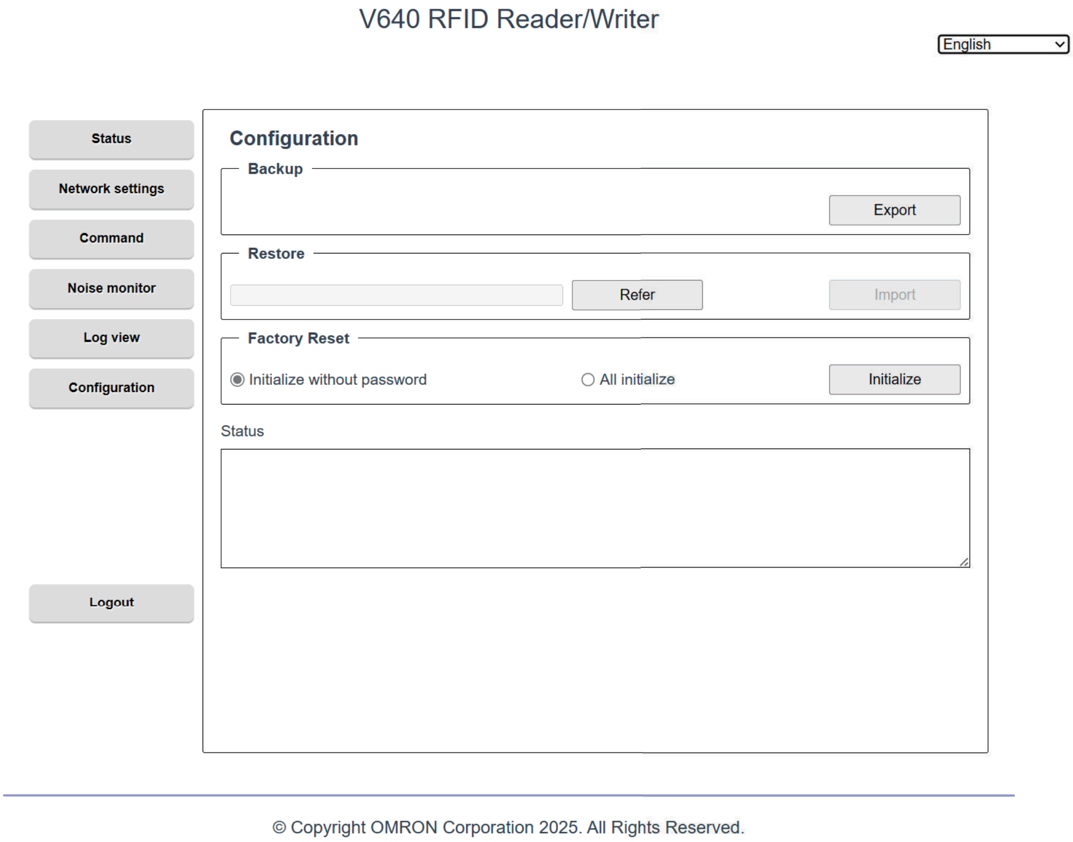
The setting data that is targeted by the Factory Reset function is shown below.

Item	Setting data	Initialize	Notes
Device Information	Model	×No	
	Firmware Version	×No	
	MAC Address	×No	
Status	Operating Mode	×No	
	Memory status	×No	
	CIDRW Head connection status	×No	
TCP/IP Settings (DIP Switch)	Enable/Disable	×No	Cannot be changed because DIP Switch
	IP Address	×No	
	Subnet Mask	×No	
TCP/IP Settings (ROM)	IP Address	○Yes	
	Subnet Mask	○Yes	
V640 Command Service settings	TCP port number	○Yes	
	IP Filtering Settings	○Yes	
	Permission Settings	○Yes	
Web Browser Service settings	TCP port availability	○Yes	
	IP Filtering Settings	○Yes	
	Web Password	○Yes	User can select whether to initialize or not
	Operation Lock	○Yes	
Log Information	Communication Log	×No	
	Security Log	×No	Not target to initialization due to security reasons

Operation Method

After password authentication, execute the operation in the Factory Reset section of the Configuration window in the Web Browser. The settings will be saved in the Amplifier Unit itself.

The settings after initialization will be reflected after rebooting the Amplifier Unit.



● Initialize without password ○ All initialize

© Copyright OMRON Corporation 2025. All Rights Reserved.

5-2-6 Backup Function

This section describes the backup function, which is used to replace the Amplifier Unit and restore various setting data in the Amplifier Unit.

Overview

You can use the Web Browser to save (export) various setting data in the Amplifier Unit as a backup file on your computer. You can also transfer (import) the settings in the backup file to the unit to replace them.

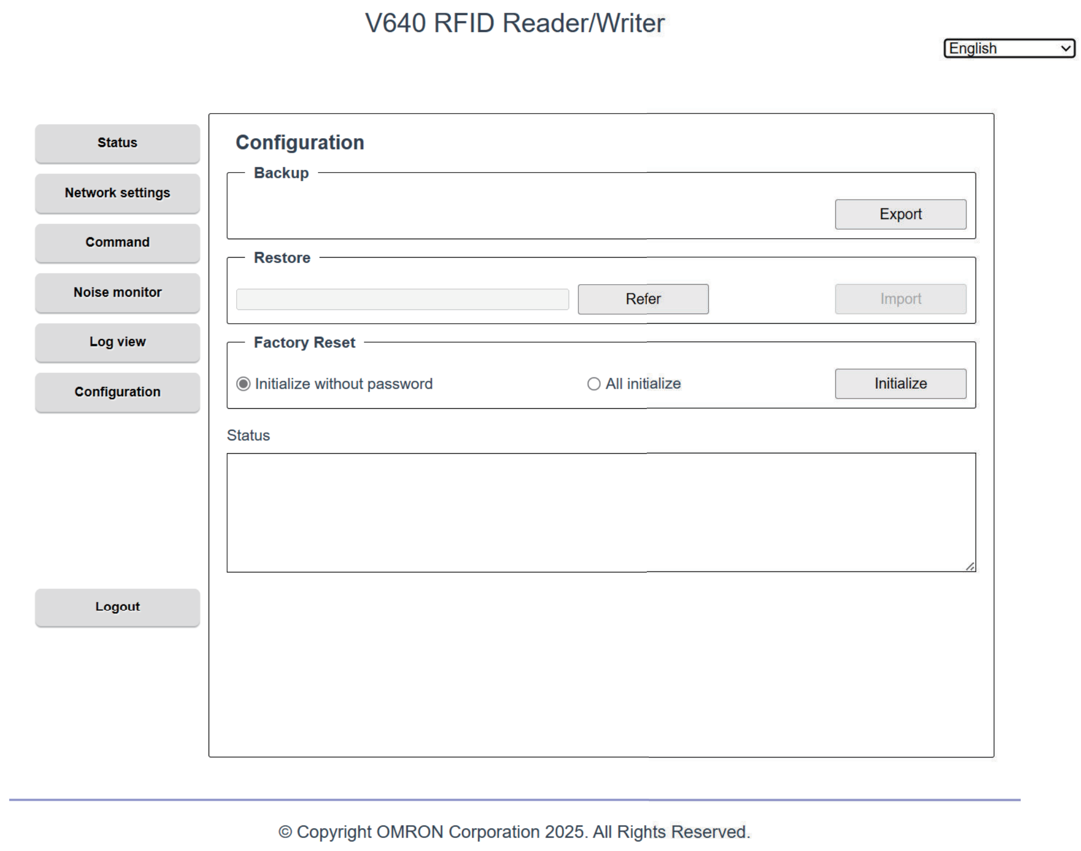
Target Data

The setting data that is targeted by the backup function is shown below.

Item	Setting data	Backup	Restore	Notes
Device Information	Model	○Yes	×No	
	Firmware Version	○Yes	×No	
	Web Application Version	○Yes	×No	
	MAC Address	○Yes	×No	
Status	Operating Mode	×No	×No	
	Memory status	×No	×No	
	CIDRW Head connection status	×No	×No	
TCP/IP Settings (DIP Switch)	Enable/Disable	○Yes	×No	Save as original information to be backed up Not applicable because restoration is not required
	IP Address	○Yes	×No	
	Subnet Mask	○Yes	×No	
TCP/IP Settings (ROM)	IP Address	○Yes	○Yes	
	Subnet Mask	○Yes	○Yes	
V640 Command Service settings	TCP port number	○Yes	○Yes	
	IP Filtering Settings	○Yes	○Yes	
	Permission Settings	○Yes	○Yes	
Web Browser Service settings	WebSocket port number	○Yes	○Yes	
	IP Filtering Settings	○Yes	○Yes	
	Web Password	×No	×No	Not applicable for security reasons
	Operation Lock	○Yes	○Yes	
Log Information	Communication Log	×No	×No	
	Security Log	×No	×No	

Operation Method

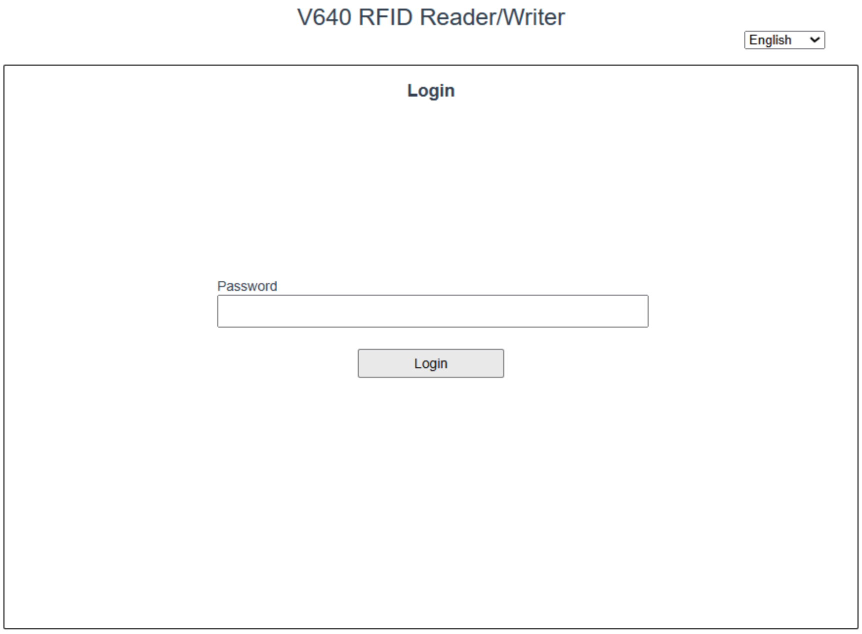
After password authentication, execute the operation in the Backup section and the Restore section of the Configuration window of the Web Browser.



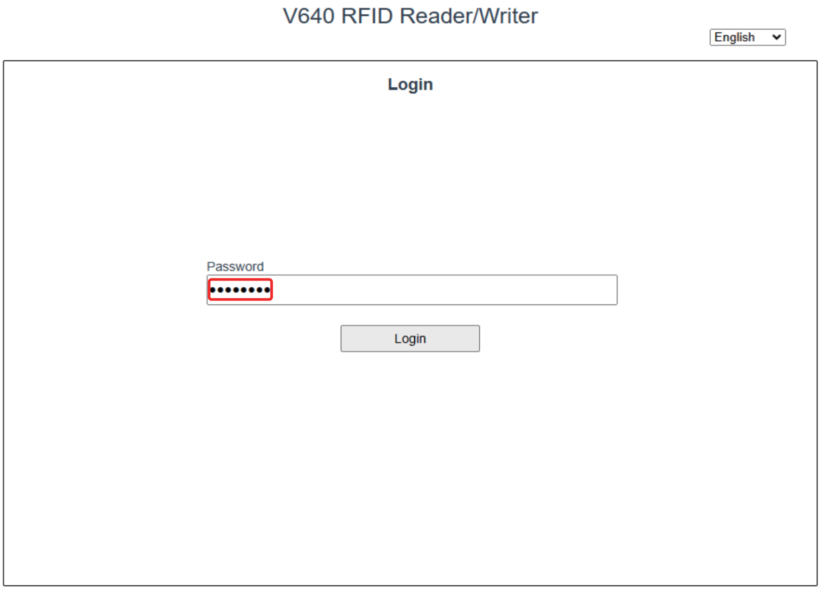
● Backup (Export) Method

1 Start the browser.

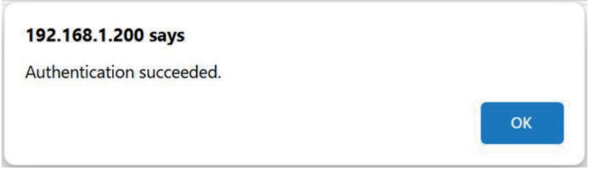
2 Enter the IP address of the Amplifier Unit in the browser's URL field.
If the IP Address is the factory default, enter *https://192.168.1.200*.
The Web Browser Login window will be displayed.



3 Enter the Web Password.



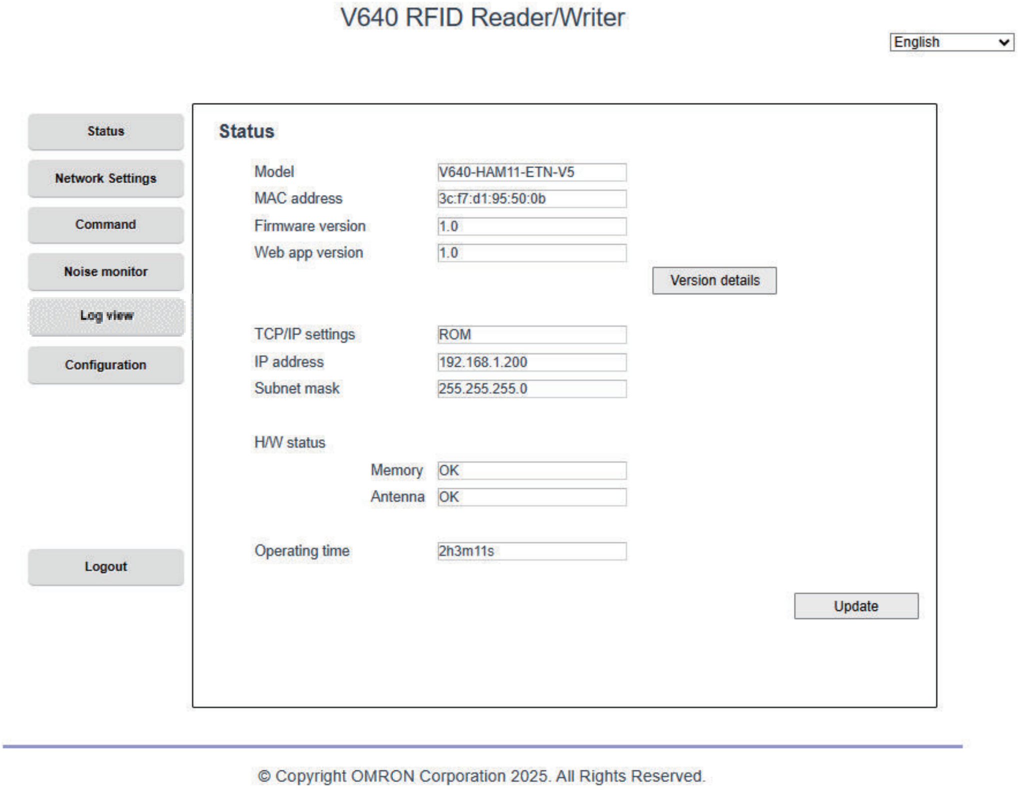
If the Web Password matches and authentication is successful, the following dialog will be displayed.



192.168.1.200 says

Authentication succeeded.

Then, the Status window will be displayed.



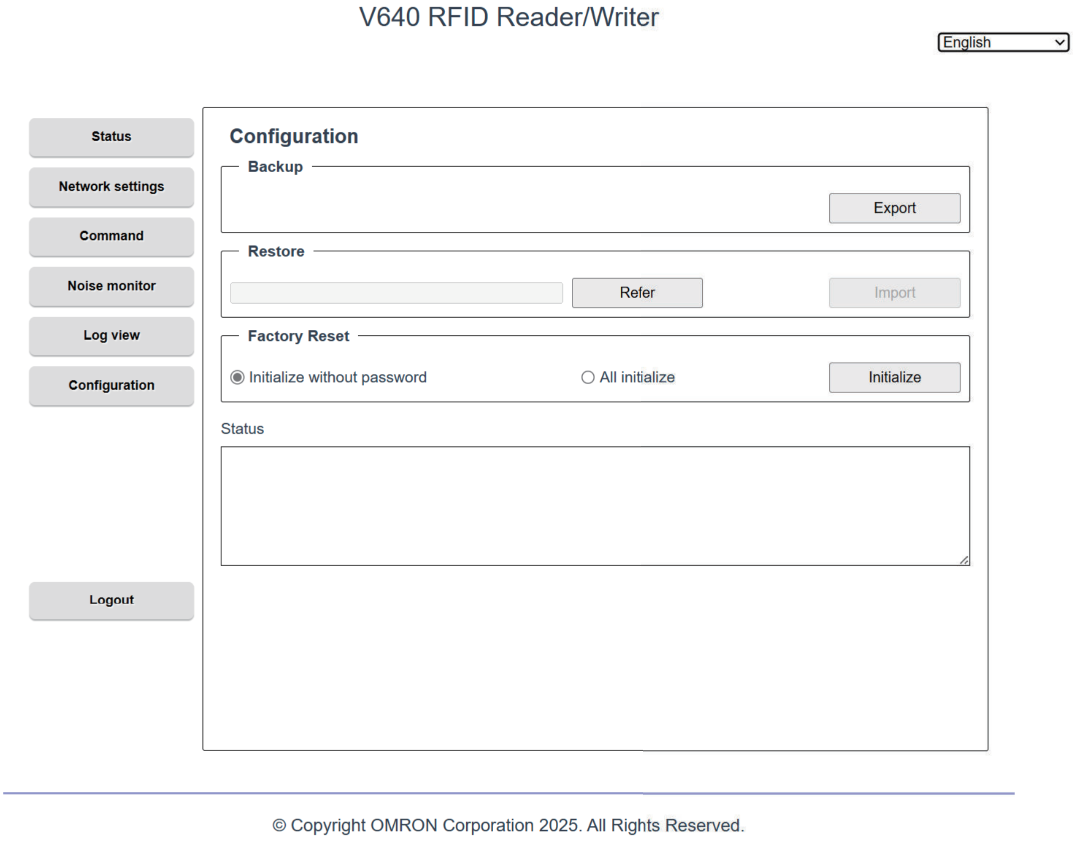
V640 RFID Reader/Writer

Status

Model	V640-HAM11-ETN-V5
MAC address	3c:f7:d1:95:50:0b
Firmware version	1.0
Web app version	1.0
TCP/IP settings	ROM
IP address	192.168.1.200
Subnet mask	255.255.255.0
H/W status	
Memory	OK
Antenna	OK
Operating time	2h3m11s

© Copyright OMRON Corporation 2025. All Rights Reserved.

4 Click **Configuration** in the Web Browser.
The Configuration window will be displayed.



V640 RFID Reader/Writer

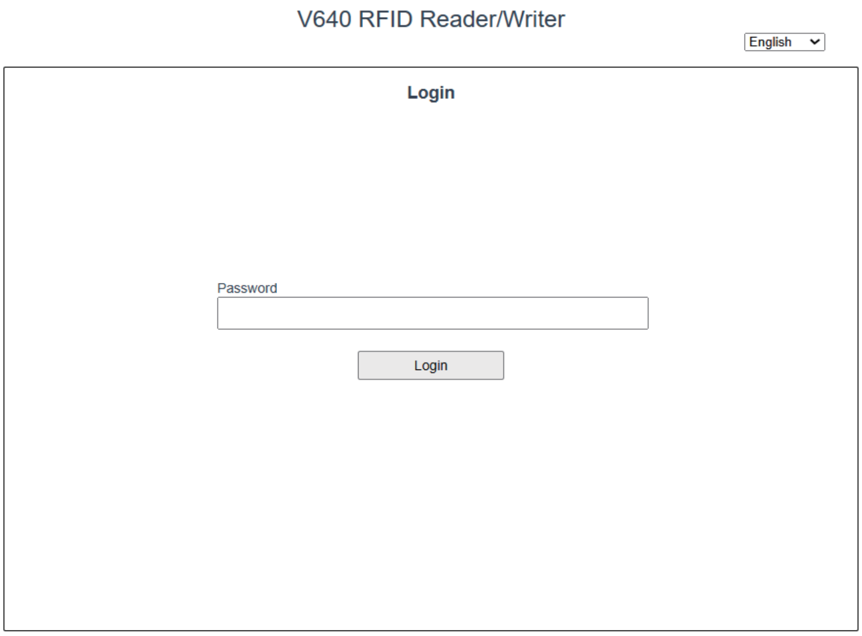
© Copyright OMRON Corporation 2025. All Rights Reserved.

5 Click the **Export** button in the Backup section.
The backup file will be saved to your computer.

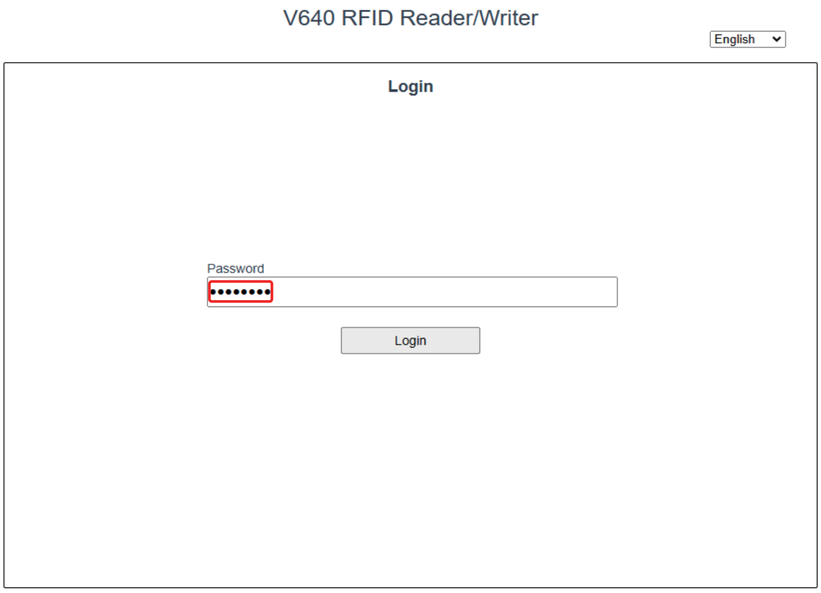
● Restore (Import) Method

1 Start the browser.

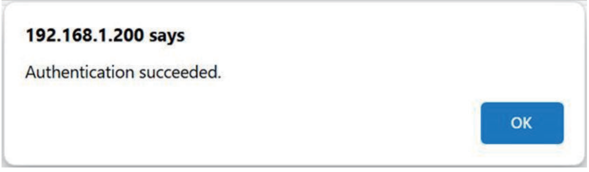
2 Enter the IP Address of the Amplifier Unit in the browser's URL field.
If the IP Address is the factory default, enter *https://192.168.1.200*.
The Web Browser Login window will be displayed.



3 Enter the Web Password.



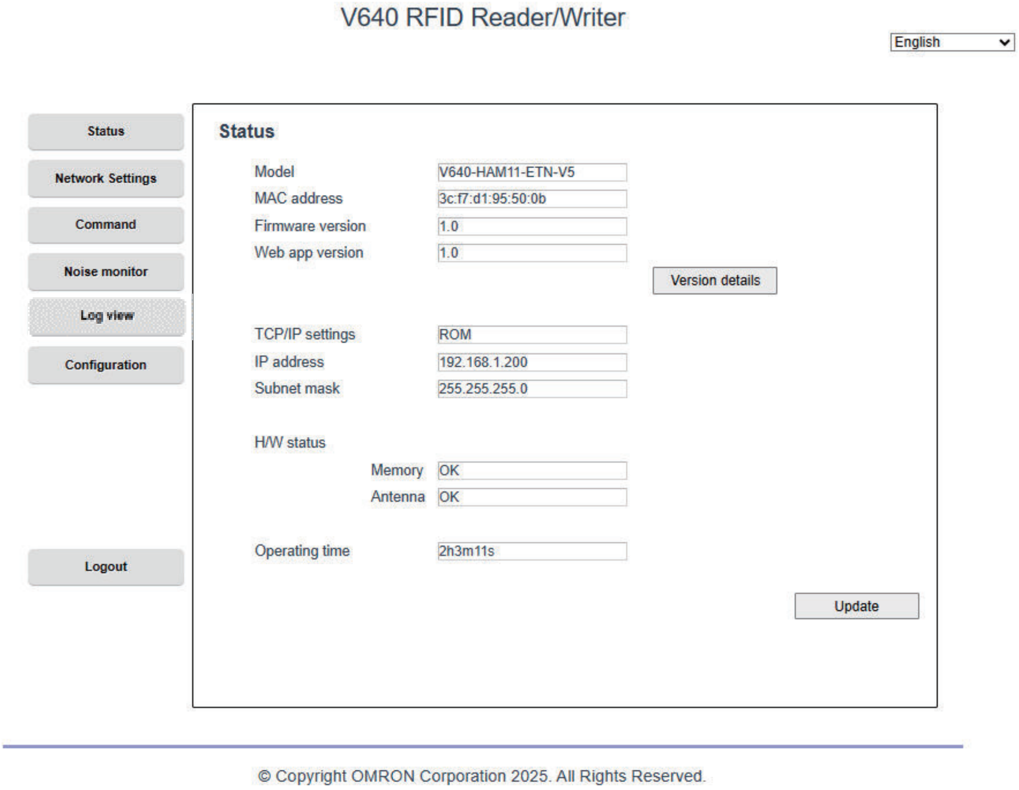
If the Web Password matches and authentication is successful, the following dialog will be displayed.



192.168.1.200 says

Authentication succeeded.

Then, the Status window will be displayed.



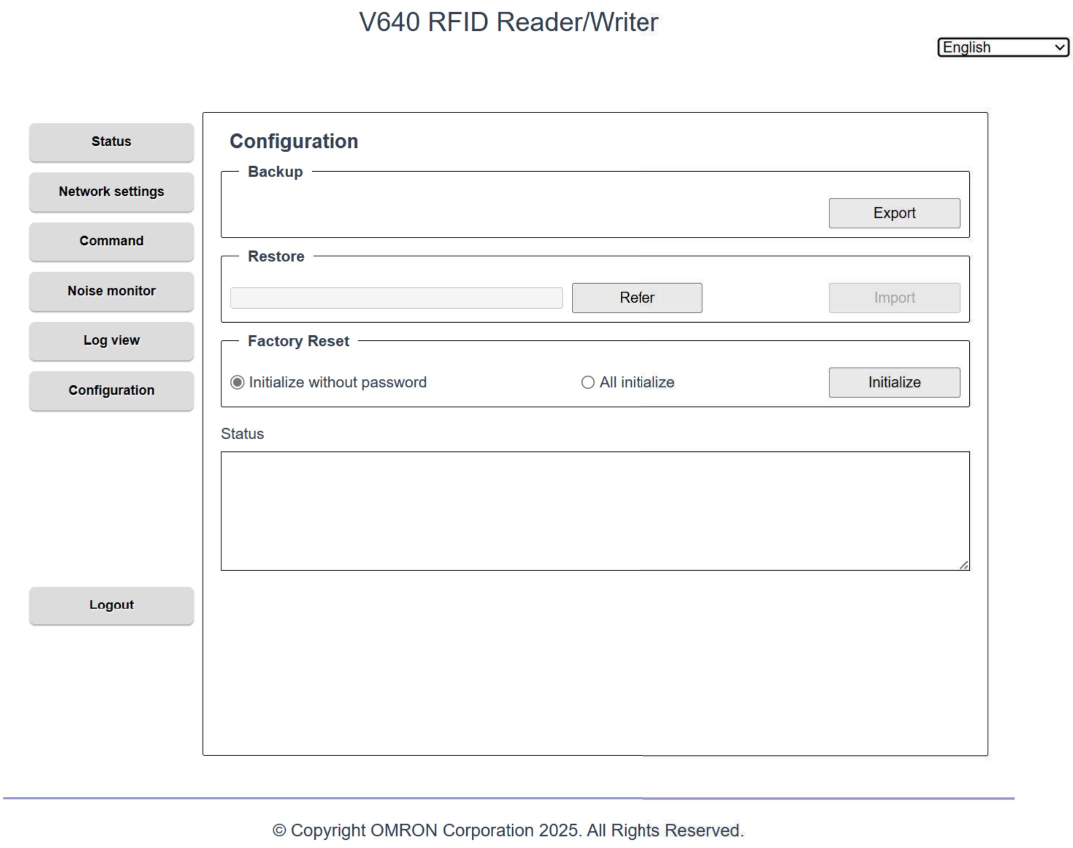
V640 RFID Reader/Writer

Status

Model	V640-HAM11-ETN-V5
MAC address	3c:f7:d1:95:50:0b
Firmware version	1.0
Web app version	1.0
TCP/IP settings	ROM
IP address	192.168.1.200
Subnet mask	255.255.255.0
H/W status	
Memory	OK
Antenna	OK
Operating time	2h3m11s

© Copyright OMRON Corporation 2025. All Rights Reserved.

4 Click **Configuration** in the Web Browser.
The Configuration window will be displayed.



V640 RFID Reader/Writer

English

Configuration

Backup

Restore

Factory Reset

● Initialize without password ○ All initialize

Status

© Copyright OMRON Corporation 2025. All Rights Reserved.

5 In the Restore section, select the backup file to be restored and click the **Import** button.
The settings in the backup file will be reflected in the Amplifier Unit.

Backup File

The backup file is in ini file format. A hash value is added to the end of the file to detect file tampering by a third party.

```
[DeviceProfile]
DeviceModel=V640-HAM11-ETN-V5
MACAddress=3c:f7:d1:95:50:14
FirmwareVersion=1.0.0
WebAppVersion=1.0.0
[NetworkSetting]
Dipsw_Enable=Disable
Dipsw_IPAddress=192.168.1.0
Dipsw_SubnetMask=255.255.255.0
IPAddress=192.168.1.200
SubnetMask=255.255.255.0
[xxxxx]
xxx
.
.
.
[Hash]
Hash=EA4D3BEB6D2F9021E04FEB74BEFC0246042D5BB94D6FC5DC45BADCF33105FF32
```

Web Browser

This section describes the Web Browser installed in the V640-series Ethernet type.

6-1 Web Browser Overview 6-2

6-1-1 Overview 6-2
6-1-2 System Environment 6-2
6-1-3 Procedure to Display the Browser Window 6-2

6-2 Web Browser Functions 6-3

6-2-1 Windw List 6-3
6-2-2 Window Transitions 6-3
6-2-3 Window Configuration 6-4
6-2-4 Login Window 6-5
6-2-5 Status Window 6-7
6-2-6 Network Settings Window 6-8
6-2-7 Network Settings Window (TCP/IP Settings) 6-9
6-2-8 Network Settings Window (Port Setting) 6-10
6-2-9 Network Settings Window (IP Filtering Settings)............................. 6-11
6-2-10 Network Settings Window (Permission Settings) 6-12
6-2-11 Network Settings Window (Web Password Settings)...................... 6-13
6-2-12 Command Window 6-14
6-2-13 Command Window (CID R/W) 6-15
6-2-14 Command Window (V640 Command)... 6-17
6-2-15 Noise Monitor Window 6-19
6-2-16 Log View Window... 6-20
6-2-17 Log View Window (Communication Log) 6-21
6-2-18 Log View Window (Security Log) 6-22
6-2-19 Configuration Window 6-24
6-2-20 Safe-Mode Window 6-26

6-3 Root Certificate Installation Procedure.. 6-28

6-1 Web Browser Overview

This section describes the overview of the Web Browser, the system environment, and the procedure to display the browser window.

6-1-1 Overview

The V640-series Amplifier Unit Ethernet type is equipped with the Web Browser.
The following functions can be easily performed without preparing special tools.

- Password Authentication
- Status View
- Network Settings
- Test Operation
- Noise Monitor
- Security Log and Communication Log View
- Backup/Restore Settings
- Factory Reset

6-1-2 System Environment

The following environment is required to use the Web Browser.

Item	Requirement
Operating System (OS)	Windows 10 32-bit or 64-bit edition Windows 11
Browser	Google Chrome Microsoft Edge
Display	XGA 1024 × 768 or higher

6-1-3 Procedure to Display the Browser Window

This section describes the procedure to display the various windows of the Web Browser.
For details, refer to the explanations in each section.

1. Connect the host device and the Amplifier Unit with a LAN cable.
2. Turn on the power of the Amplifier Unit.
3. Start the browser on the host device.
4. Enter the IP address or domain name of the Amplifier Unit in the browser's URL field.
5. The Login window will be displayed, so enter your Web Password.
6. If the Web Password matches and authentication is successful, the following dialog will be displayed.
7. Then, the Status window will be displayed.
8. Use the navigation buttons on the left side of the window to select the function you want to perform.

6-2 Web Browser Functions

This section describes the functions of the Web Browser.

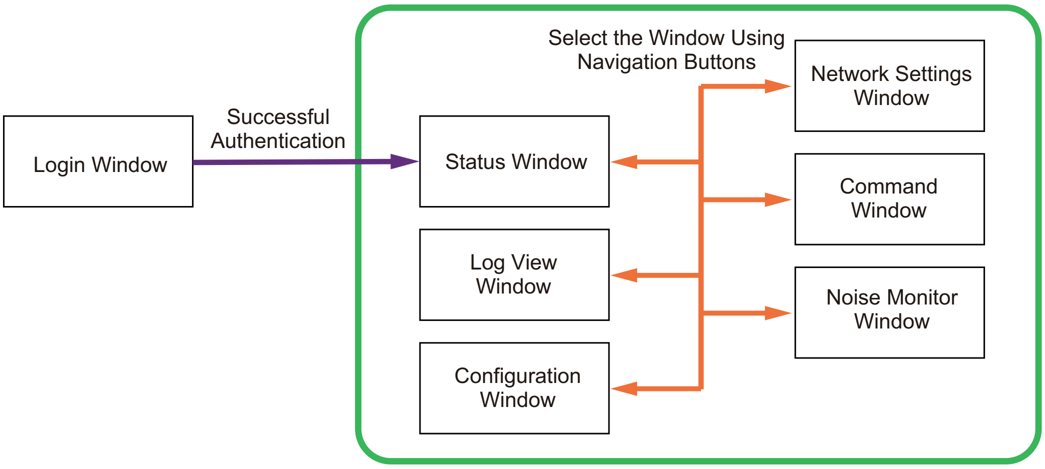
6-2-1 Windw List

The following is a list of the Web Browser windows.

Windos name	Tab name	Content	See
Login	---	Password Authentication is performed.	page 6-5
Status	---	You can check the Amplifier Unit's Device Information.	page 6-7
Network Settings	TCP/IP Settings	You can set the IP Address and subnet mask.	page 6-9
	Port Setting	You can set the Port Number and Port Enable/Disable.	page 6-10
	IP Filtering Settings	You can set IP Filtering.	page 6-11
	Permission Settings	You can change the Access Permission Settings.	page 6-12
	Web Password Settings	You can set the Web Password and Lock Time..	page 6-13
Command	CID R/W	You can communicate with ID Tags using the CID R/WCommand.	page 6-15
	V640 Command	You can communicate with ID Tags using the V640 Command.	page 6-17
Noise Monitor	---	You can use the Noise Measurement Function.	page 6-19
Log View	Communication Log	You can check the Communication Log.	page 6-21
	Security Log	You can check the Security Log.	page 6-22
Configuration	---	You can back up, restore, and performe Factory Reset.	page 6-24

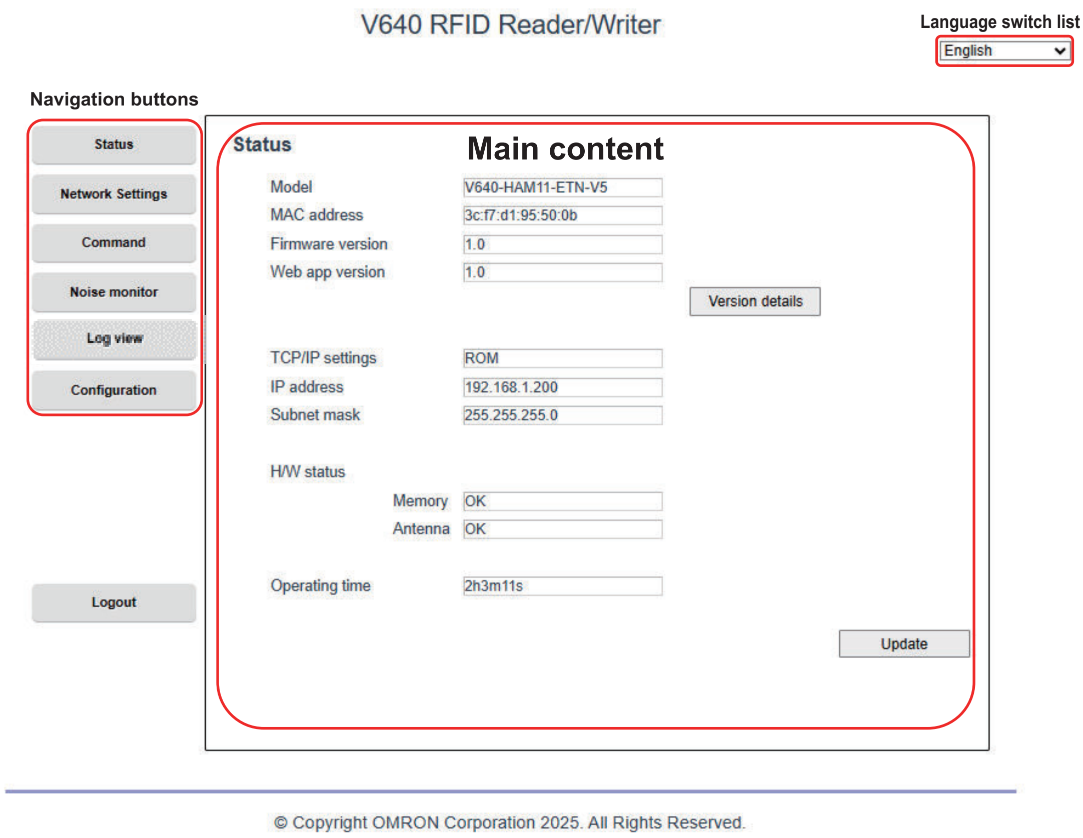
6-2-2 Window Transitions

The window transitions of the Web Browser are shown below.



6-2-3 Window Configuration

The window configuration of the Web Browser is shown below.



Status

Model: V640-HAM11-ETN-V5
MAC address: 3c:f7:d1:95:50:0b
Firmware version: 1.0
Web app version: 1.0

TCP/IP settings: ROM
IP address: 192.168.1.200
Subnet mask: 255.255.255.0

H/W status
Memory: OK
Antenna: OK

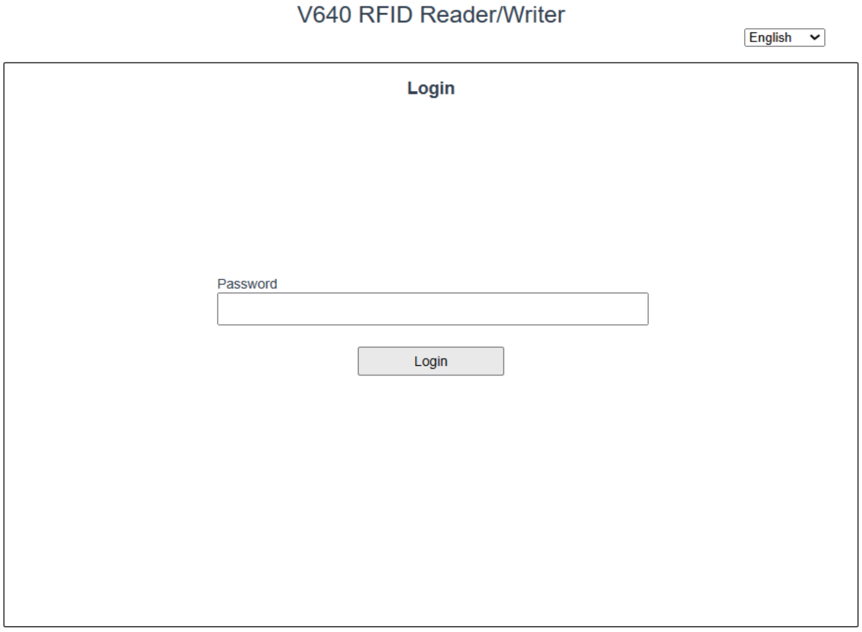
Operating time: 2h3m11s

© Copyright OMRON Corporation 2025. All Rights Reserved.

Item	Description	Notes
Language switch list	Switches the language. Select from Japanese/English.	---
Navigation buttons	Select the function to execute.	---
Logout button	Logs out.	---
Main content	This is the area where the content of each window is displayed.	---

6-2-4 Login Window

After connecting to the Amplifier Unit, the **Login** window is displayed first. The **Login** window has the Language switch list, the Password input field, and the **Login** button.
When you enter the correct Web Password and click the **Login** button, the dialog indicating successful authentication is displayed. After that, the **Status** window is displayed.



Item	Description	Notes
Language switch list	Switches the language. Select from Japanese/English.	---
Password	Enter your Web Password.	---
Login	After clicking, if the password matches, the main content is displayed.	---

Additional Information

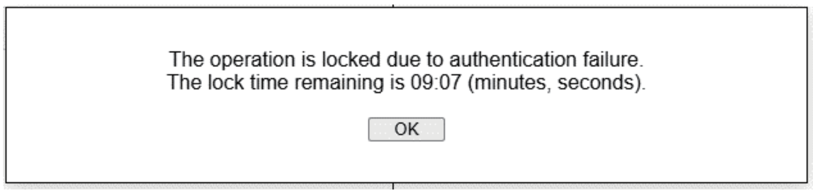
Password specifications are as follows.

Item	Content
Valid number of characters	8 characters or more and 32 characters or less[*1]
Usable characters	Half-width alphanumeric characters and symbols (case-sensitive)[*2]

*1. Any value between 8 and 32 characters can be set.

2. Characters that can be used are ASCII characters 0x21 to 0x7E (0-9 A-Z a-z, '-!"#$%&(),./:;?@[]^_`{|}~+<=>).

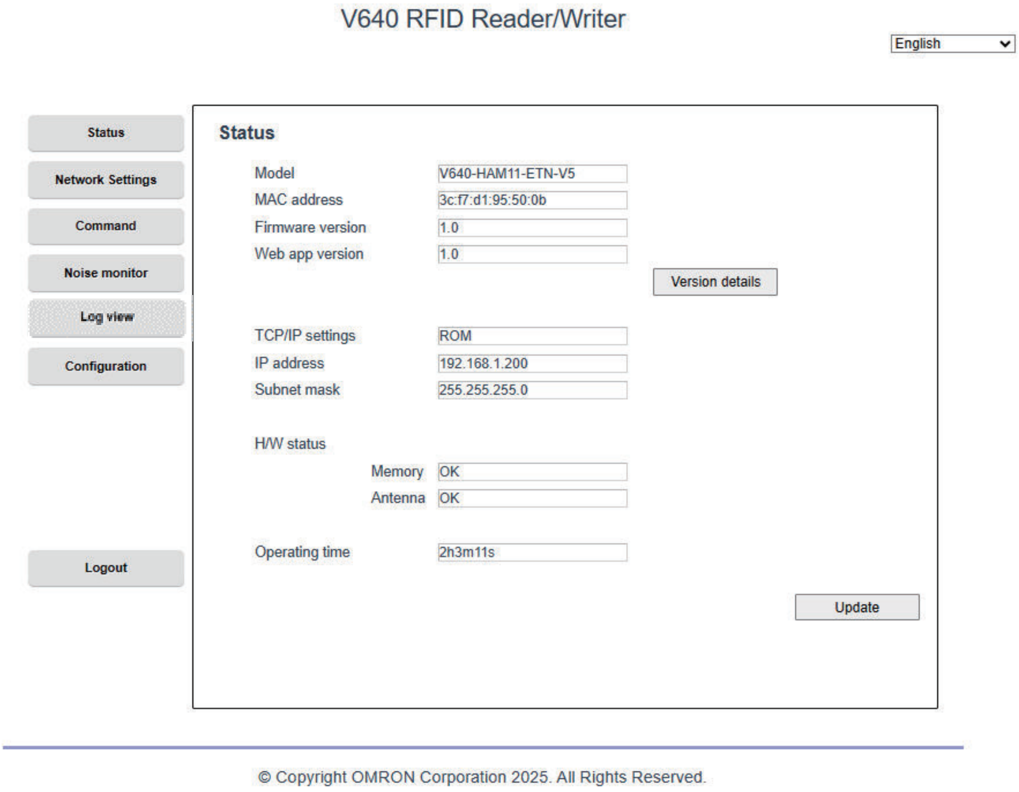
If you enter the wrong password five times, the following dialog will be displayed and the Web Browser will be locked for 10 minutes. The lock will be released after the time has elapsed or by rebooting the Amplifier Unit.



The operation is locked due to authentication failure.
The lock time remaining is 09:07 (minutes, seconds).

6-2-5 Status Window

On the window, you can check information such as the Model, MAC Address, and Firmware Version. Clicking the Update button will reload and redisplay the window.



Status

Model: V640-HAM11-ETN-V5
MAC address: 3c:f7:d1:95:50:0b
Firmware version: 1.0
Web app version: 1.0

TCP/IP settings: ROM
IP address: 192.168.1.200
Subnet mask: 255.255.255.0

H/W status
Memory: OK
Antenna: OK

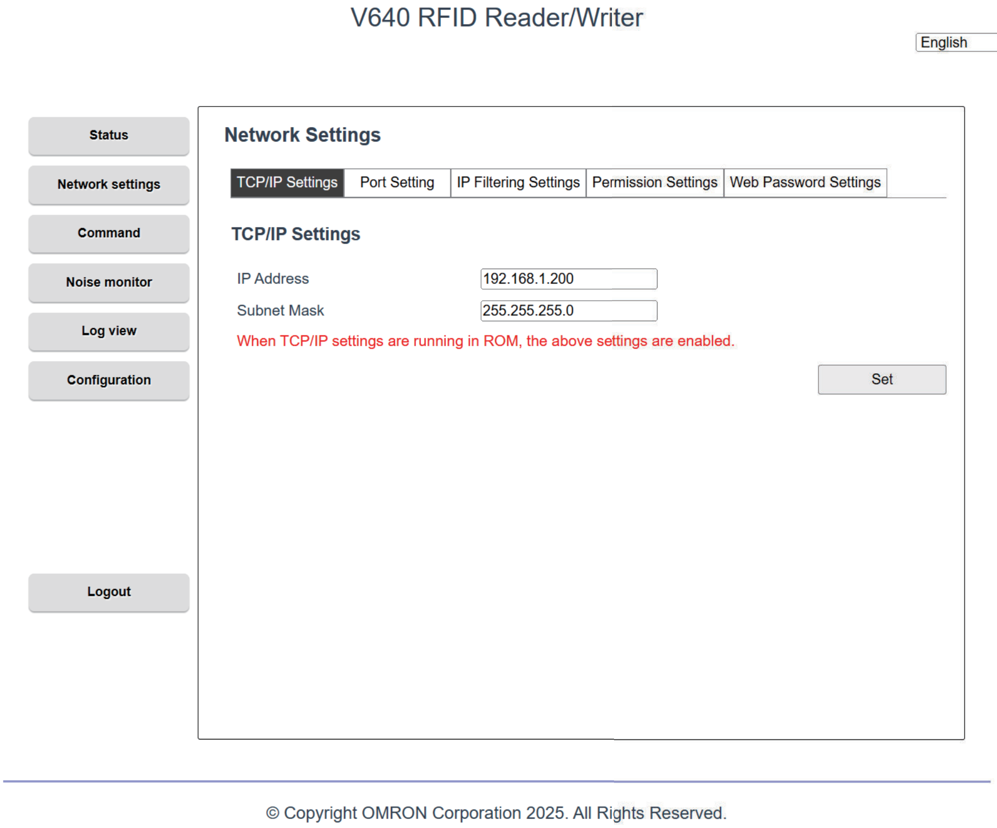
Operating time: 2h3m11s

© Copyright OMRON Corporation 2025. All Rights Reserved.

Item		Description	Notes
Model		Displays the Product Model.	You cannot enter a value.
MAC Address		Displays the MAC Address.	You cannot enter a value.
Firmware Version		Displays the Firmware Version.	You cannot enter a value.
Web Application Version		Displays the Web Application Version.	You cannot enter a value.
Version Details		Displays the Version Details in the dialog.	---
TCP/IP Settings		If the IP address is set to *DIP Switch*, **DIP Switch** is displayed, and if it is set to *ROM*, **ROM** is displayed.	You cannot enter a value.
IP Address		Displays the IP Address of the Amplifier Unit.	You cannot enter a value.
Subnet Mask		Displays the Subnet Mask of the Amplifier Unit.	You cannot enter a value.
H/W Status		Displays the hardware status.	**OK** is displayed when normal. You cannot enter a value.
	Memory	If the memory error is detected at startup, **Error** is displayed.	
	Antenna	If an error (or the head is not connected) is detected in the CID head connected to the Amplifier Unit, **Error** is displayed.	
PowerOnTime		Displays the PowerOnTime of the Amplifier Unit.	You cannot enter a value.
Update		The status information is updated.	---

6-2-6 Network Settings Window

In the **Network Settings** window, you can configure the Network Settings of the Amplifier Unit. You can set the IP Address, Subnet Mask, Port, Password, IP Filtering, and Access Permissions by selecting a tab.



TCP/IP Settings

IP Address 192.168.1.200

Subnet Mask 255.255.255.0

When TCP/IP settings are running in ROM, the above settings are enabled.

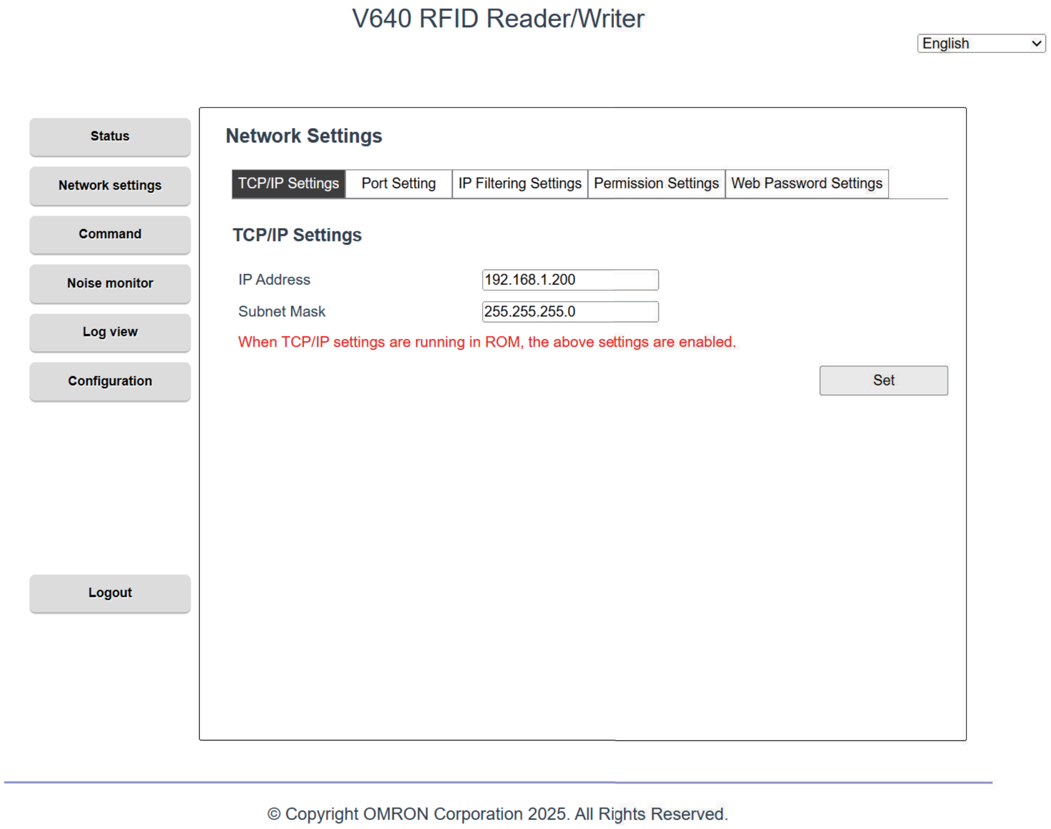
© Copyright OMRON Corporation 2025. All Rights Reserved.

Tab name	Content
TCP/IP Settings	You can set the IP Address and Subnet Mask.
Port Setting	You can set the Port number and Port Enable/Disable.
IP Filtering Settings	You can set IP Filtering.
Permission Settings	You can change the Access Permission.
Web Password Settings	You can set the Web Password and Lock Time.

6-2-7 Network Settings Window (TCP/IP Settings)

The **TCP/IP Settings** tab on the **Network Settings** window allows you to set the IP Address and Subnet Mask of the Amplifier Unit.

For information on the communication specifications of the Amplifier Unit, see *3-2 Setting the Communications Conditions for Amplifier Units* on page 3-3.



TCP/IP Settings

IP Address 192.168.1.200

Subnet Mask 255.255.255.0

When TCP/IP settings are running in ROM, the above settings are enabled.

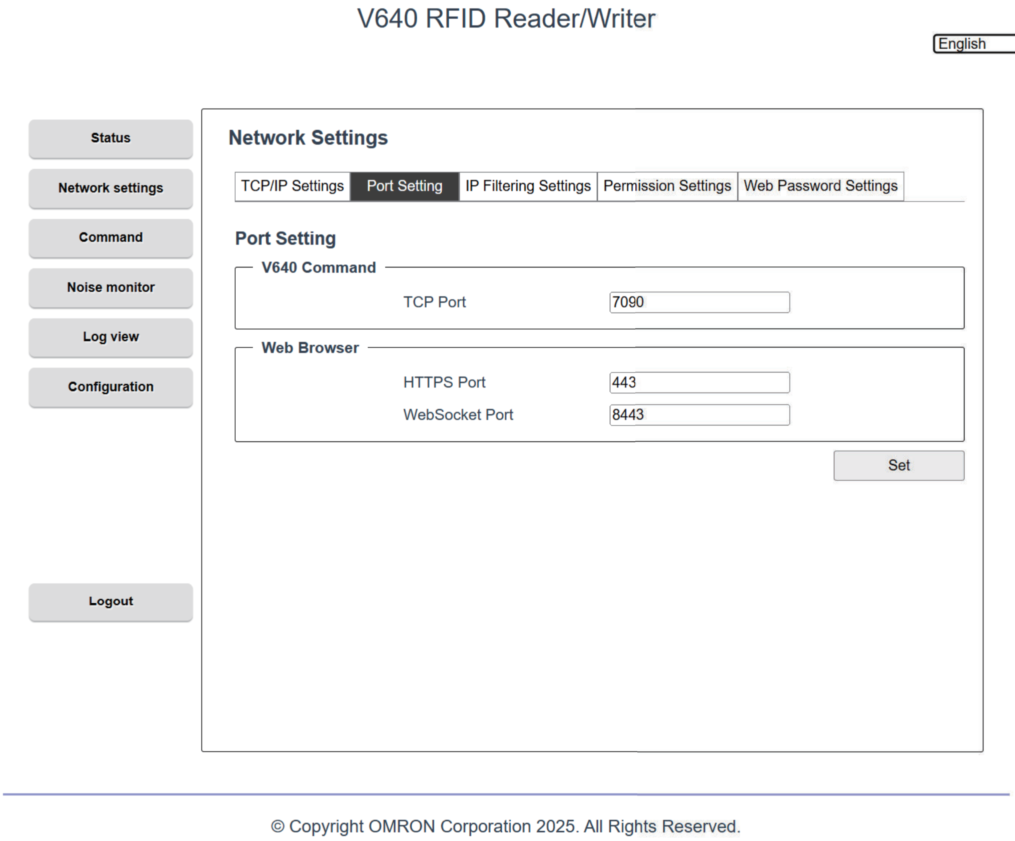
© Copyright OMRON Corporation 2025. All Rights Reserved.

Item	Description	Notes
IP Address	You can specify the IP Address of the Amplifier Unit. At startup, the IP Address value at the time of ROM is displayed.	---
Subnet Mask	You can specify the Subnet Mask of the Amplifier Unit. At startup, the Subnet Mask value at the time of ROM is displayed.	---
Set	Click to set the entered value.	If the DIP Switch setting is enabled, click to display the following. **The DIP Switch is currently enabled. The above settings will be reflected when the DIP Switch is disabled.**

6-2-8 Network Settings Window (Port Setting)

The **Port Setting** tab on the **Network Settings** window allows you to set the communication port for the Amplifier Unit.

For information on the communication specifications of the Amplifier Unit, see *3-2 Setting the Communications Conditions for Amplifier Units* on page 3-3.



Port Setting

V640 Command

TCP Port: 7090

Web Browser

HTTPS Port: 443

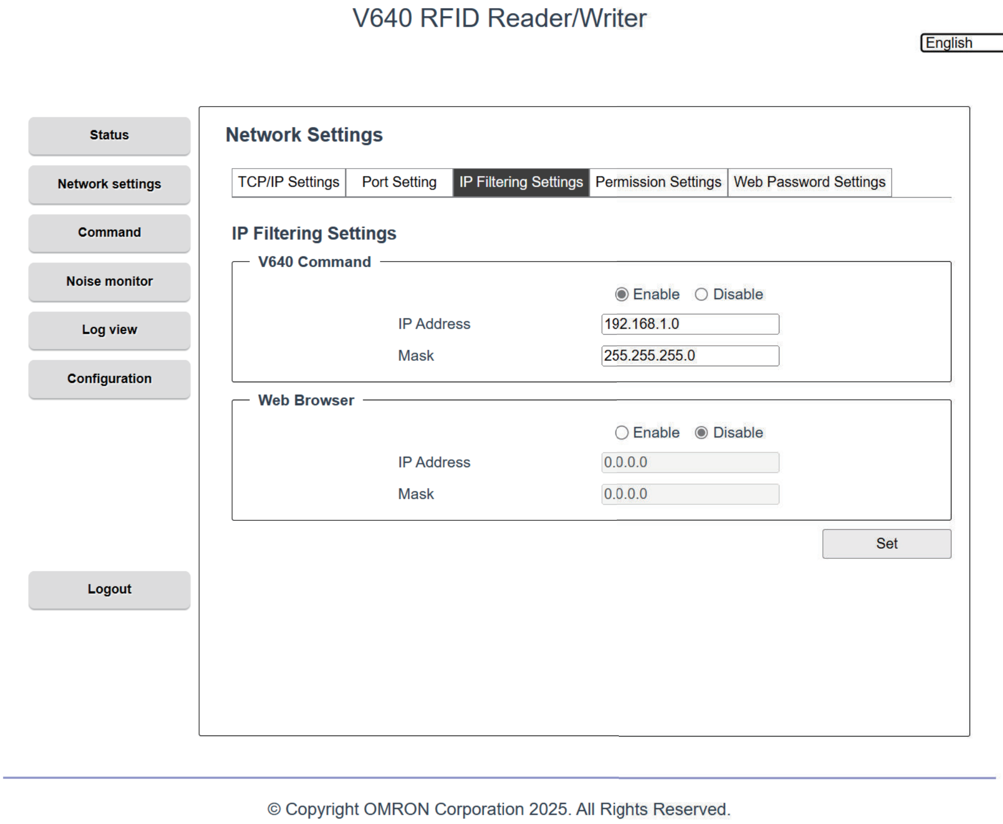
WebSocket Port: 8443

Item		Description	Notes
V640 Command			---
	TCP Port	You can specify the TCP Port number for the Amplifier Unit. At startup, the configured TCP Port number is displayed.	
Web Browser			
	HTTPS Port	The HTTPS Port number for the Amplifier Unit is displayed.	You cannot enter a value.
	WebSocket Port	You can specify the WebSocket port number for the Amplifier Unit. At startup, the configured WebSocket Port number is displayed.	---
Set		Click to set the entered value.	---

6-2-9 Network Settings Window (IP Filtering Settings)

The **IP Filtering Settings** tab on the **Network Settings** window allows you to set IP Filtering Settings for each communication.

For information on the IP Filtering function, see *5-2-3 IP Filtering Function* on page 5-16.



V640 RFID Reader/Writer

Network Settings

IP Filtering Settings

V640 Command

● Enable ○ Disable

IP Address 192.168.1.0

Mask 255.255.255.0

Web Browser

○ Enable ● Disable

IP Address 0.0.0.0

Mask 0.0.0.0

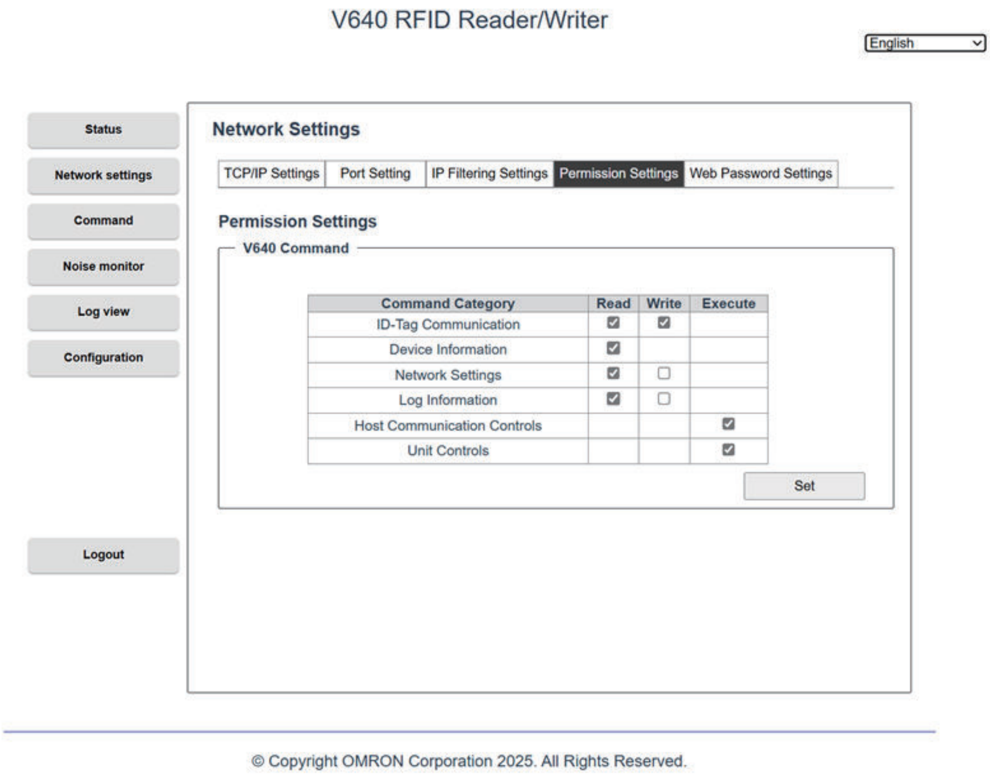
© Copyright OMRON Corporation 2025. All Rights Reserved.

Item		Description	Notes
V640 Command			---
	Enable/Disable	You can Enable/Disable the IP Filtering function for V640 Command.	
	IP Address	You can specify the IP Address that is allowed to connect.	
	Mask	You can specify the Mask for the IP Address that is allowed to connect.	
Web Browser			---
	Enable/Disable	You can Enable/Disable the IP Filtering function for Web Browser.	
	IP Address	You can specify the IP Address that is allowed to connect.	
	Mask	You can specify the Mask for the IP Address that is allowed to connect.	
Set		Click to set the entered value.	---

6-2-10 Network Settings Window (Permission Settings)

The **Permission Settings** tab on the **Network Settings** window allows you to set V640 Commands that are restricted from being executed on the Amplifier Unit.
Checked items are *Permission*. Clicking the **Set** button saves the settings to the Amplifier Unit itself.

For information on the Access Permission function, see *5-2-2 Access Permission Function* on page 5-13.



Permission Settings

V640 Command

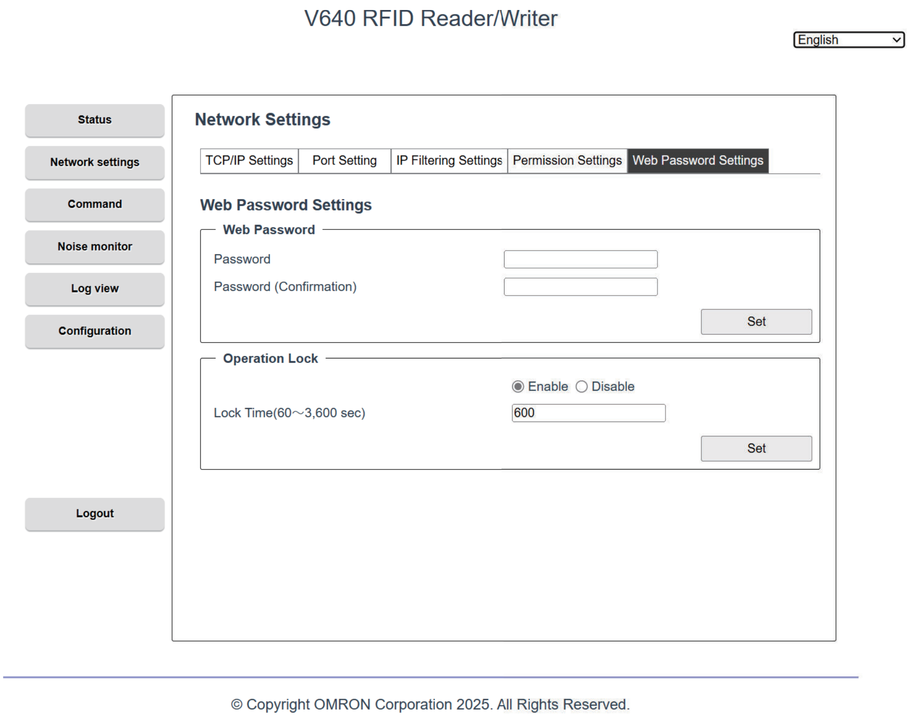
Command Category	Read	Write	Execute
ID-Tag Communication	☑	☑	
Device Information	☑		
Network Settings	☑	□	
Log Information	☑	□	
Host Communication Controls			☑
Unit Controls			☑

Target command	Permission	Content	Setting range	Initial state
ID-Tag Communication	Read	Access permission for RF Tag communication	Prohibit, Permission	Permission
	Write		Prohibit, Permission	Permission
Device Information	Read	Access permission for Device Information	Prohibit, Permission	Permission
Network Settings	Read	Access permission for Network Settings	Prohibit, Permission	Permission
	Write		Prohibit, Permission	Prohibit
Log Information	Read	Access permission for Log Information	Prohibit, Permission	Permission
	Write		Prohibit, Permission	Prohibit
Host Communication Controls	Execute	Access permission for Host Communication Controls	Prohibit, Permission	Permission
Unit Controls	Execute	Access permission for Unit Controls	Prohibit, Permission	Permission

6-2-11 Network Settings Window (Web Password Settings)

The **Web Password Settings** tab on the **Network Settings** window allows you to change the Web Password.

For details on Web Password, see *5-2-1 Password Authentication Function* on page 5-6.



Web Password Settings

Web Password

Password

Password (Confirmation)

Operation Lock

● Enable ○ Disable

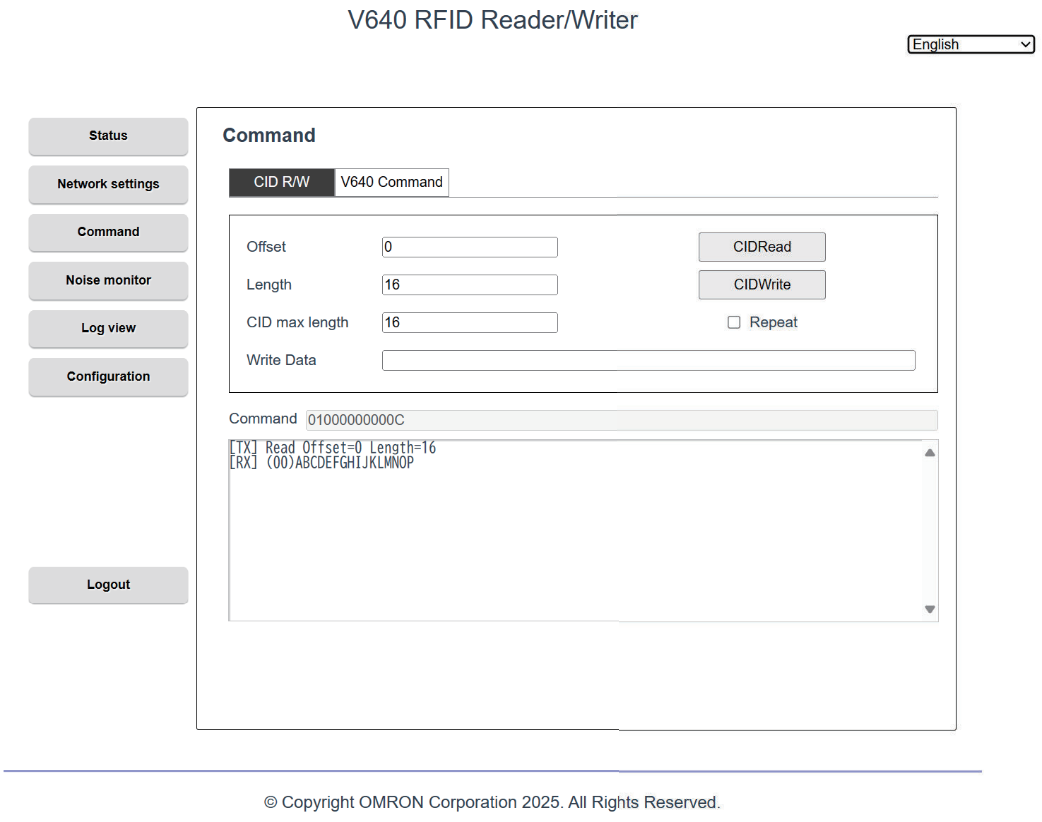
Lock Time(60～3,600 sec) 600

© Copyright OMRON Corporation 2025. All Rights Reserved.

Item		Description	Notes
Web Password			---
	Password	You can set a new password.	
	Password (Confirmation)	Re-enter the new password to confirm it.	
	Set	Click to set the entered *password*.	
Operation Lock			---
	Enable/Disable	You can choose whether to Enable or Disable the Operation Lock.	
	Lock Time (60 to 3,600 sec)	You can specify the Operation Lock Time.	
	Set	Click to set the entered *Lock Time* value.	

6-2-12 Command Window

The **Command** window allows you to communicate with ID tags. The **Command** window has two functions, **CID R/W** and **V640 Command**, which can be switched by tab.



Offset: 0

Length: 16

CID max length: 16

Write Data:

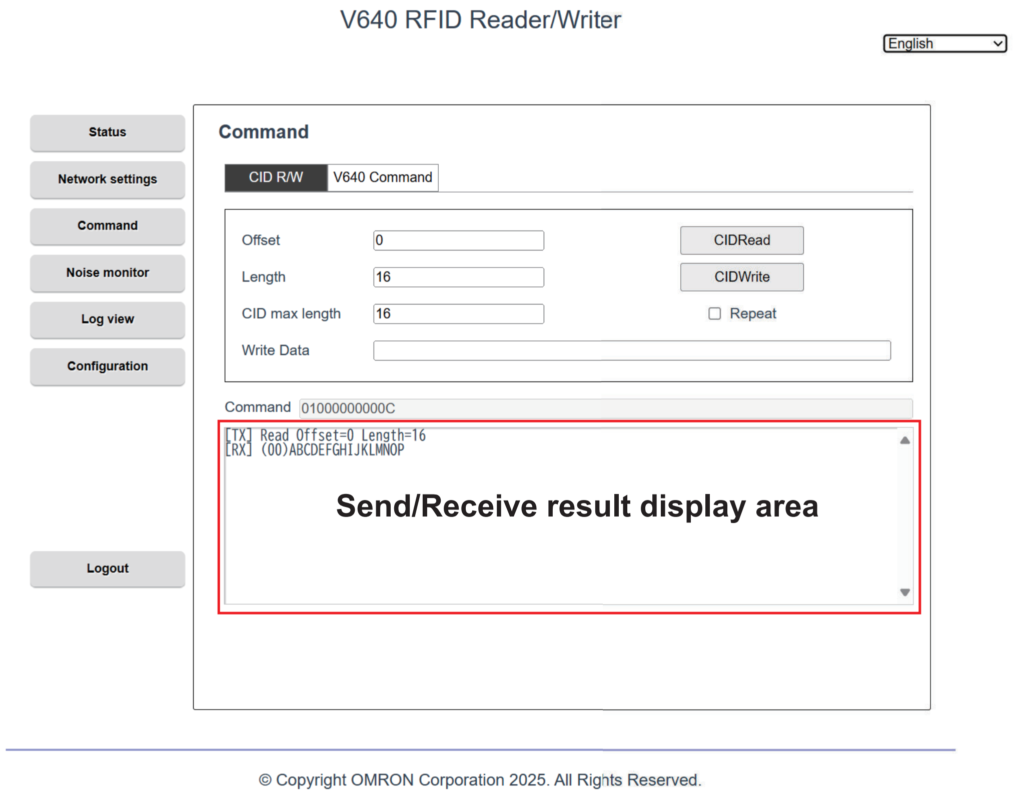
Command: 01000000000C

```
[TX] Read Offset=0 Length=16
[RX] (00)ABCDEFGHIJKLMNOP
```

Tab name	Content
CID R/W	You can communicate with ID tags with the CID R/W Command.
V640 Command	You can communicate with ID tags with the V640 Command.

6-2-13 Command Window (CID R/W)

The **CID R/W** tab on the **Command** window allows you to send communication commands.
You can specify three parameters: **Offset**, **Length**, and **Maximum byte of CID** to read/write with ID tags. When writing, you must also specify the **Write Data**.



Offset: 0
Length: 16
CID max length: 16
Write Data:
Command: 01000000000C

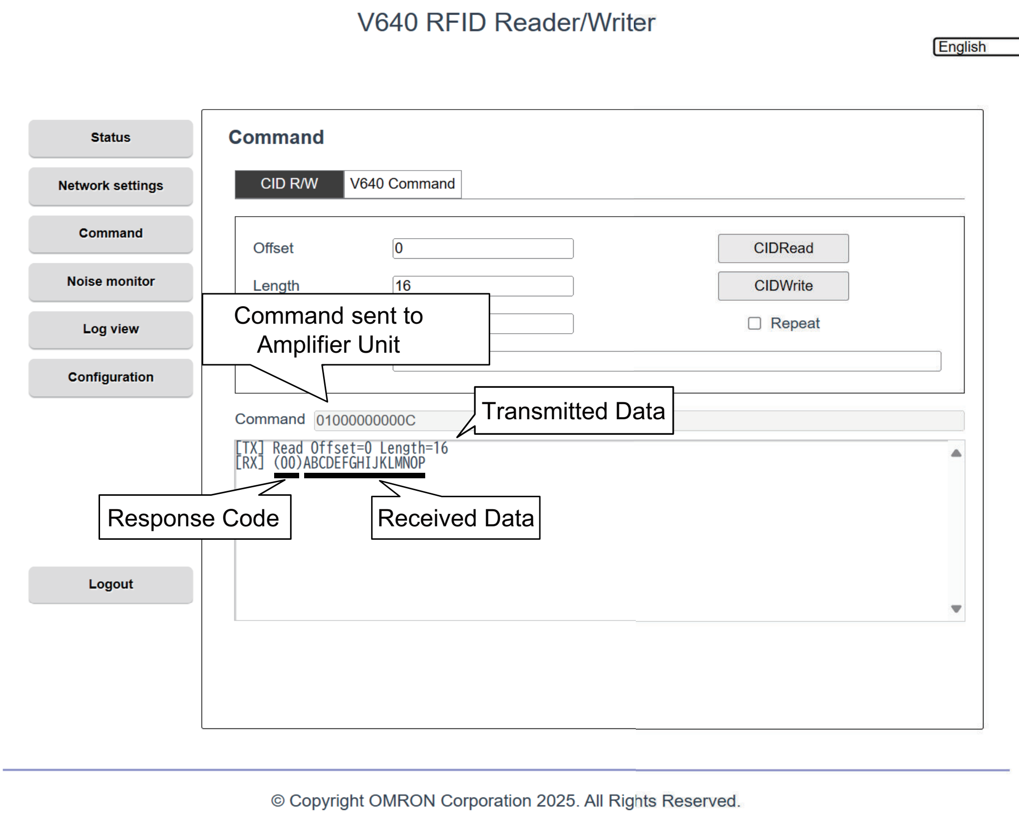
```
[TX] Read Offset=0 Length=16
[RX] (00)ABCDEFGHIJKLMNOP
```

© Copyright OMRON Corporation 2025. All Rights Reserved.

Item	Description	Notes
Offset	Specify the CID Offset value with a value of 0 to 15 bytes.	---
Length	Specify the CID Length with a value of 1 to 16 bytes.	---
Maximum byte of CID	Specify the Maximum bye of CID with a value of 1 to 16 bytes.	Specify *Offset* + *Length* ≦ *Maximum byte of CID*.
Write Data	Specify the Write Data for the number of characters specified by **Length**.	Only *Visible ASCII* characters (other than control characters) can be specified.
CID Read	Click to execute a CID Read.	---
CID Write	Click to execute a CID Write.	---
Repeat	Check if you want to execute repeatedly.	---
Command	Displays the command actually sent to the Amplifier Unit.	Displayed as a hexadecimal value.
Send/Receive result display area	Displays the data sent to the Amplifier Unit and the data received. [TX]: Displays the data sent to the Amplifier Unit. [RX]: Displays the data received from the Amplifier Unit. Since this is also used in the **V640 Command** tab, the display remains even if you switch to the **V640 Command** tab.	You cannot enter a value.

Execution Example

For example, if you execute a CID read with "Offset = 0, Length = 16, and Maximum byte of CID = 16", you will get the following results.



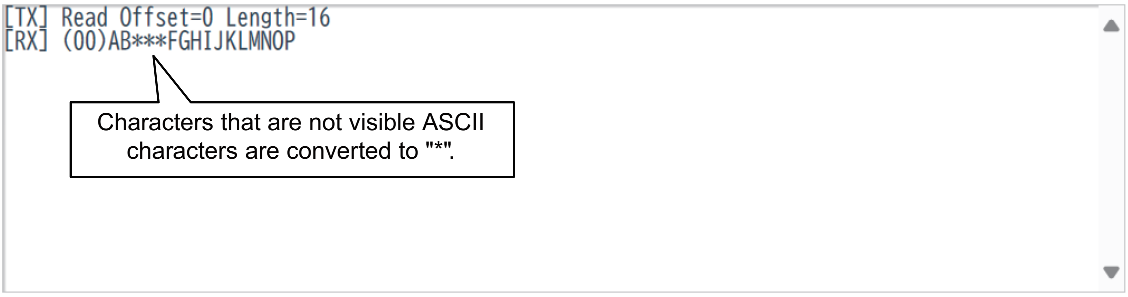
Offset: 0

Length: 16

Command: 01000000000C

```
[TX] Read Offset=0 Length=16
[RX] (00)ABCDEFGHIJKLMNOP
```

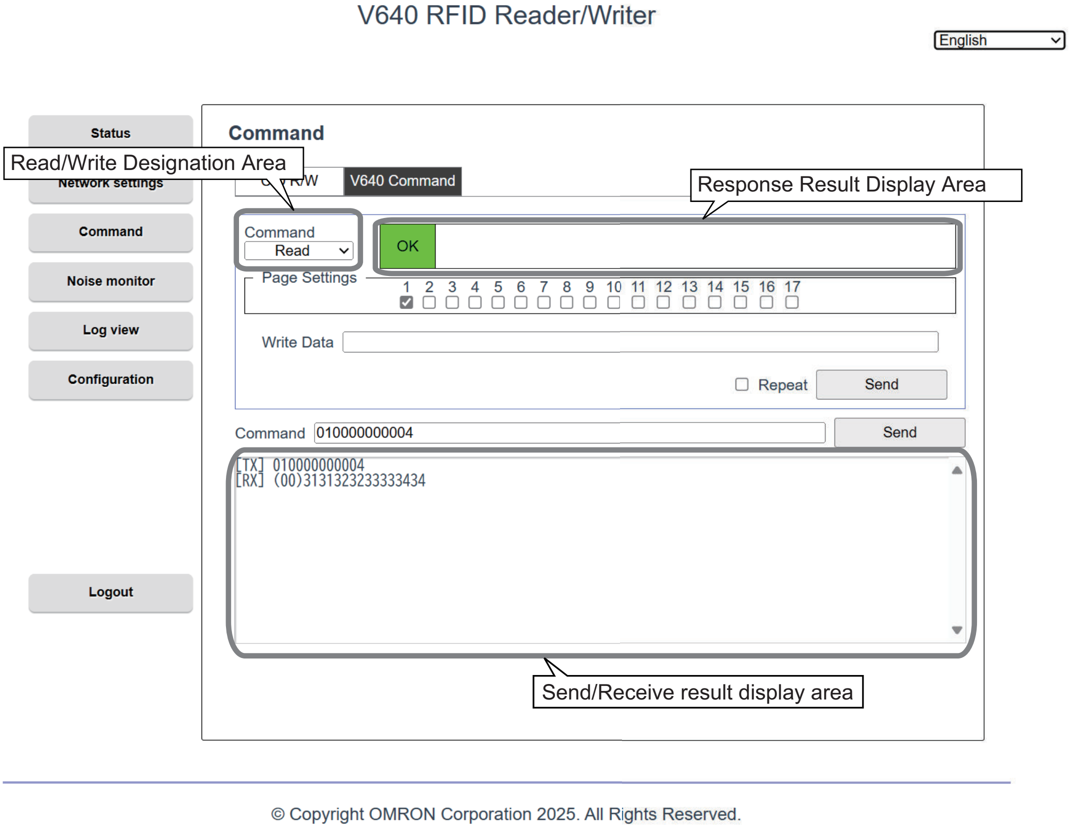
Note that **CID R/W** can only handle *Visible ASCII* as data to be read or written to ID tags, so if characters other than *Visible ASCII* are detected when executing a *CID Read*, they will be converted to "*" (asterisk) and displayed.


Characters that are not visible ASCII characters are converted to "*".

```
[TX] Read Offset=0 Length=16
[RX] (00)AB***FGHIJKLMNOP
```

6-2-14 Command Window (V640 Command)

The **V640 Command** tab on the **Command** window allows you to execute read or write according to the command format of the Amplifier Unit .



Command: 010000000004

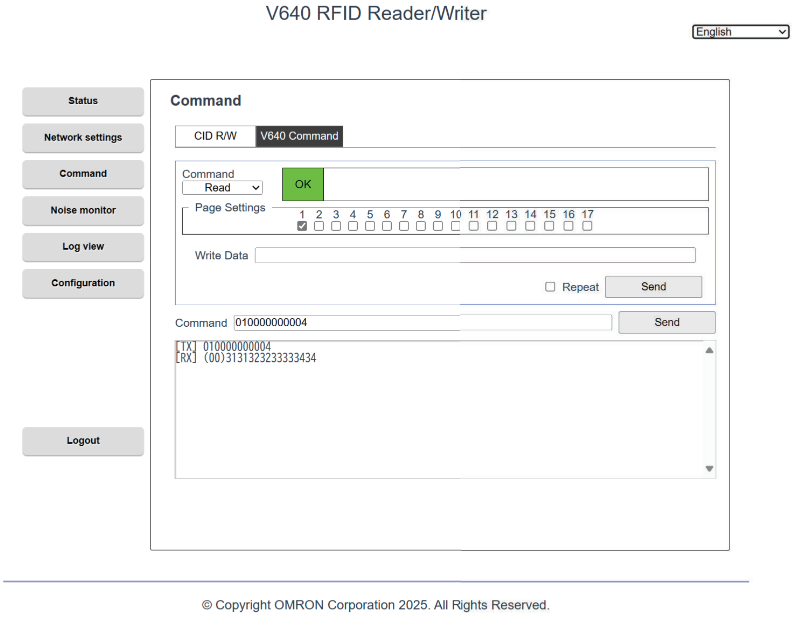
```
[TX] 010000000004
[RX] (00)3131323233333434
```

© Copyright OMRON Corporation 2025. All Rights Reserved.

Item	Description	Notes
Read/Write Designation Area	Select **Read** or **Write** from the pull-down menu.	---
Response Result Display Area	Displays the execution result of the **Read** or **Write** command as **communication success (OK)** or **communication failure (NG)**. If the result is **NG**, the details of the NG are also displayed.	You cannot enter a value.
Page Designation	Specify the page number for **Read** or **Write** processing using the checkbox.	---
Write Data	When **writing** data, specify the data to write to the ID Tag as a hexadecimal string. Specify 16 characters for each page that you specify in the **Page Designation Area**.	---
Repeat	Check this box if you want to execute repeatedly.	---
Send	Press the **Send** button to the right of **Repeat** to send the command.	---
Command	Displays the command actually sent to the Amplifier Unit. You can also execute commands by entering them in hexadecimal values in this area.	Displayed as a hexadecimal value.
Send	When you press the **Send** button to the right of the **Command**, the content displayed in the **Command** will be sent.	---
Send/Receive result display area	Displays the data sent to the Amplifier Unit and the data received. [TX]: Displays the data sent to the Amplifier Unit. [RX]: Displays the data received from the Amplifier Unit. Since this is also used in the **CID R/W** tab, the display remains even if you switch to the **CID R/W** tab.	You cannot enter a value.

Execution Example

Successful Communications



V640 RFID Reader/Writer

Command

Command: Read

OK

Page Settings: 1 ☑ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □ 10 □ 11 □ 12 □ 13 □ 14 □ 15 □ 16 □ 17 □

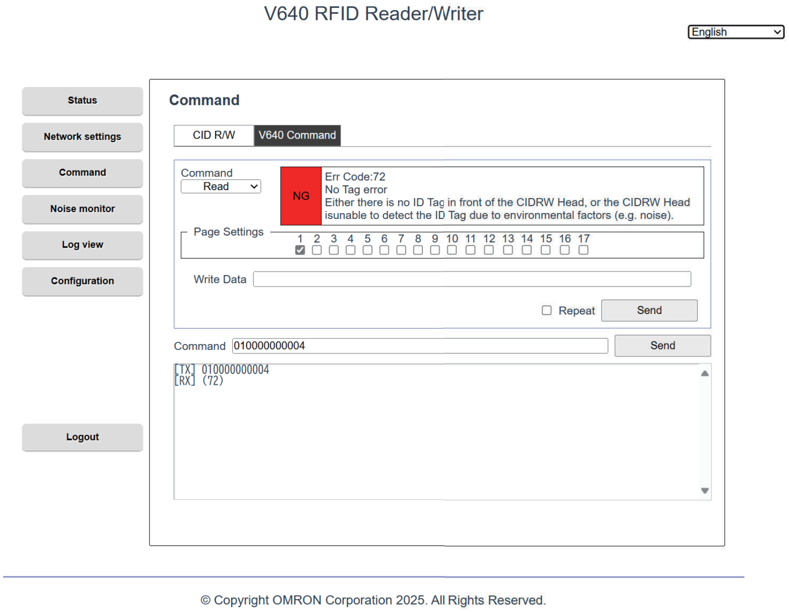
Write Data

Command 010000000004

```
[TX] 010000000004
[RX] (00)3131323233333434
```

© Copyright OMRON Corporation 2025. All Rights Reserved.

Failed Communications



V640 RFID Reader/Writer

Command

Command: Read

NG

Err Code:72
No Tag error
Either there is no ID Tag in front of the CIDRW Head, or the CIDRW Head isunable to detect the ID Tag due to environmental factors (e.g. noise).

Page Settings: 1 ☑ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □ 10 □ 11 □ 12 □ 13 □ 14 □ 15 □ 16 □ 17 □

Write Data

Command 010000000004

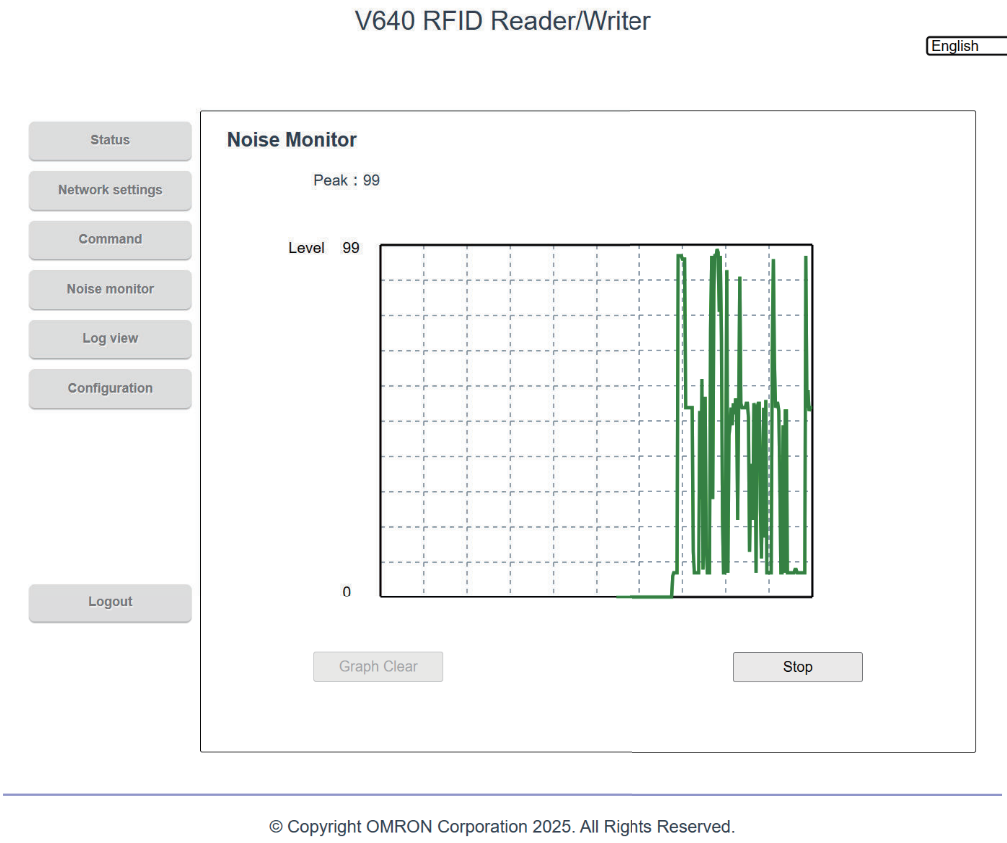
```
[TX] 010000000004
[RX] (72)
```

© Copyright OMRON Corporation 2025. All Rights Reserved.

6-2-15 Noise Monitor Window

On the **Noise Monitor** window, "NOISE MEASUREMENT" commands are continuously sent to the Amplifier Unit, and the results are displayed in a graph in real time.

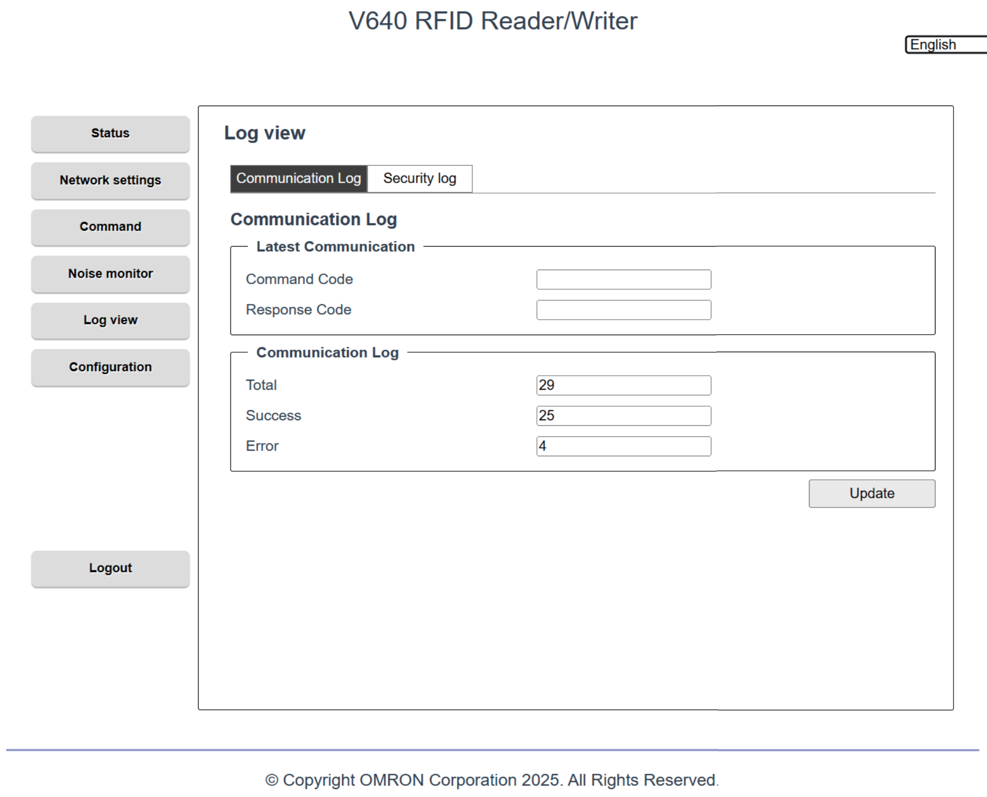
The horizontal axis gives the time and the vertical axis gives the noise level (0 to 99).



Item	Description	Notes
Start/Stop	Click to Start/Stop noise measurement.	---
Graph Clear	Click to clear the displayed graph.	---

6-2-16 Log View Window

On the **Log View** window, you can check the Communication Log and Security Log.
You can switch between them by tab.



V640 RFID Reader/Writer

Log view

Communication Log

Latest Communication

Command Code

Response Code

Communication Log

Total 29

Success 25

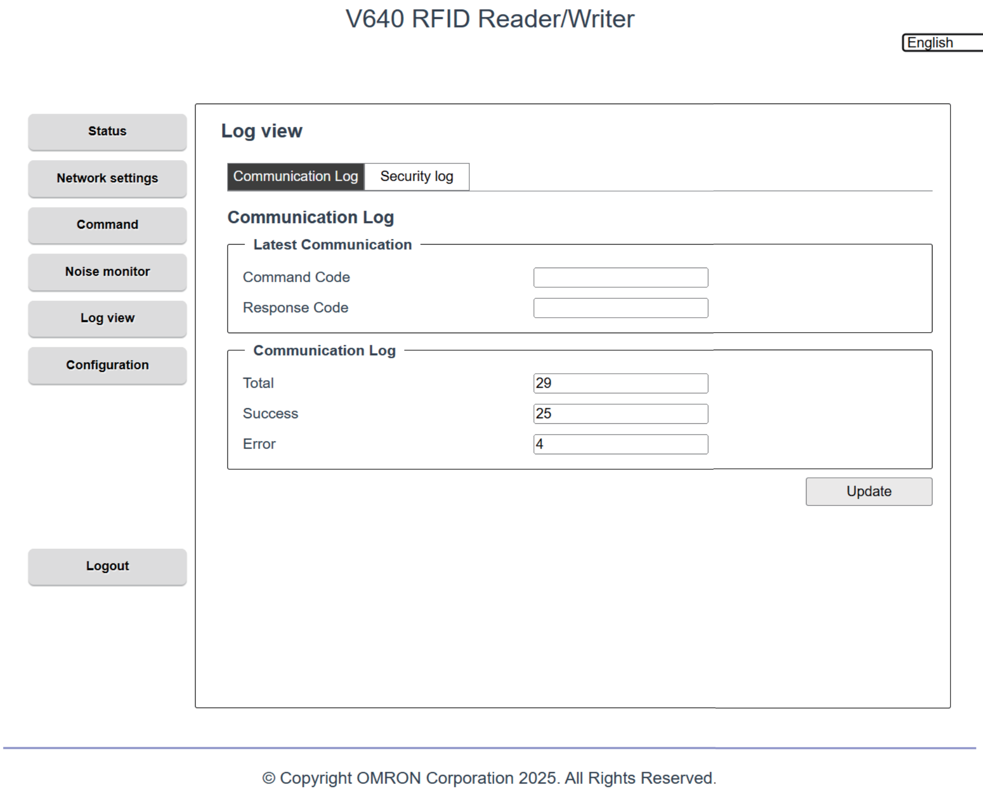
Error 4

© Copyright OMRON Corporation 2025. All Rights Reserved.

Tab name	Content
Communication Log	The Latest Communication and Communication Log with ID Tags are displayed.
Security Log	The Security Log of setting changes, control, and operations is displayed.

6-2-17 Log View Window (Communication Log)

The **Communication Log** tab on the **Log View** window allows you to check the Latest Communication and the Communication Log with ID Tags.



Communication Log

Latest Communication

Command Code

Response Code

Communication Log

Total 29

Success 25

Error 4

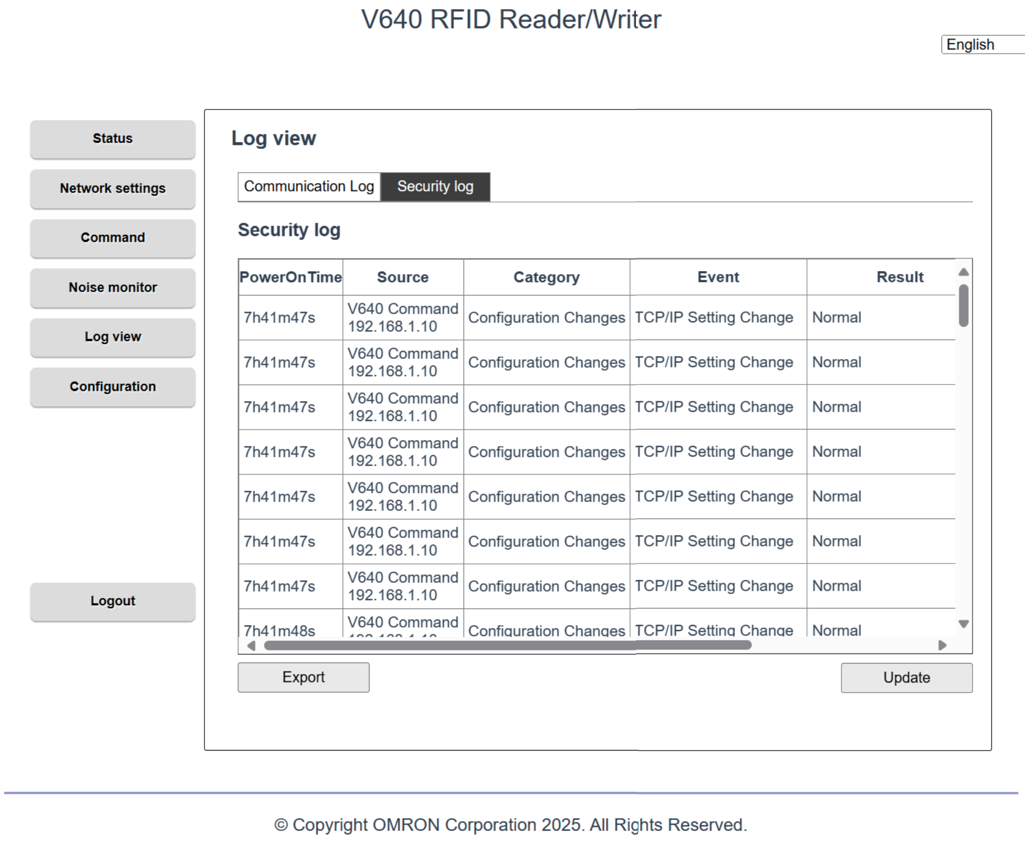
© Copyright OMRON Corporation 2025. All Rights Reserved.

Item		Description	Notes
Latest Communication		The last **Command Code** executed and the last **Response Code** to which the Amplifier Unit responded are displayed.	If no command has been executed, such as immediately after starting the Amplifier Unit, this will be blank. You cannot enter a value.
	Command Code		
	Response Code		
Communication Log		Displays the Communication Log with ID Tags.	You cannot enter a value.
	Total	Displays the total number of communications since startup.	
	Success	Displays the total number of successful communications since startup.	
	Error	Displays the total number of failed communications since startup.	
Update		Click to update the information.	---

6-2-18 Log View Window (Security Log)

The Security Log tab on the Log View window allows you to check the Log View of changes and controls made to the Amplifier Unit by the host device, and operations made to the Amplifier Unit by the user using the Web Browser.

For information on the Security Log function, see *5-2-4 Security Log Function* on page 5-19.



V640 RFID Reader/Writer

Log view

Security log

PowerOnTime	Source	Category	Event	Result
7h41m47s	V640 Command 192.168.1.10	Configuration Changes	TCP/IP Setting Change	Normal
7h41m47s	V640 Command 192.168.1.10	Configuration Changes	TCP/IP Setting Change	Normal
7h41m47s	V640 Command 192.168.1.10	Configuration Changes	TCP/IP Setting Change	Normal
7h41m47s	V640 Command 192.168.1.10	Configuration Changes	TCP/IP Setting Change	Normal
7h41m47s	V640 Command 192.168.1.10	Configuration Changes	TCP/IP Setting Change	Normal
7h41m47s	V640 Command 192.168.1.10	Configuration Changes	TCP/IP Setting Change	Normal
7h41m47s	V640 Command 192.168.1.10	Configuration Changes	TCP/IP Setting Change	Normal
7h41m48s	V640 Command	Configuration Changes	TCP/IP Setting Change	Normal

© Copyright OMRON Corporation 2025. All Rights Reserved.

Item	Description	Notes
PowerOnTime	Time information when the event occurred. The accumulated power-on time (in seconds) in the Amplifier Unit is registered.	---
Source	Type of the route on which the event occurred. For communication routes, the service/protocol type and the IP address of the communication partner are displayed.	---
Category	The event category is displayed.	--- ---
Event	The contents of the event are displayed.	---
Result	The result of the change, control, or operation that caused the event.	---
Additional Info1	Additional information on the event result.	---
Additional Info2	Additional information on the event result.	---
Export	Click to export the Security Log as a CSV file.	---
Update	Click to retrieve and redisplay the Security Log.	---

Exported File Format

This section explains the format of the CSV file that is exported when the **Export** button is clicked.

Each Security Log is separated by a "," (comma) and written on one line.

The data written is as follows.

Item	Content (format)	Example
PowerOnTime	PowerOnTime. The format is hhhh"h"mm"m"ss"s.	8765h43m21s
Source	Source type. One of three types: DIP Switch, TCP, or HTTPS. For communication routes, the source IP Address is also written.	V640Command:192.168.1.1 WebBrowser:192.168.1.1 DIPSwitch
Category	Code indicating the event category.	0010
Event	Code indicating the event type.	0000
Result	Result of the event.	00
Additional Info1	Additional information 1.	00000000
Additional Info2	Additional information 2.	00000000

● Example of Exported File

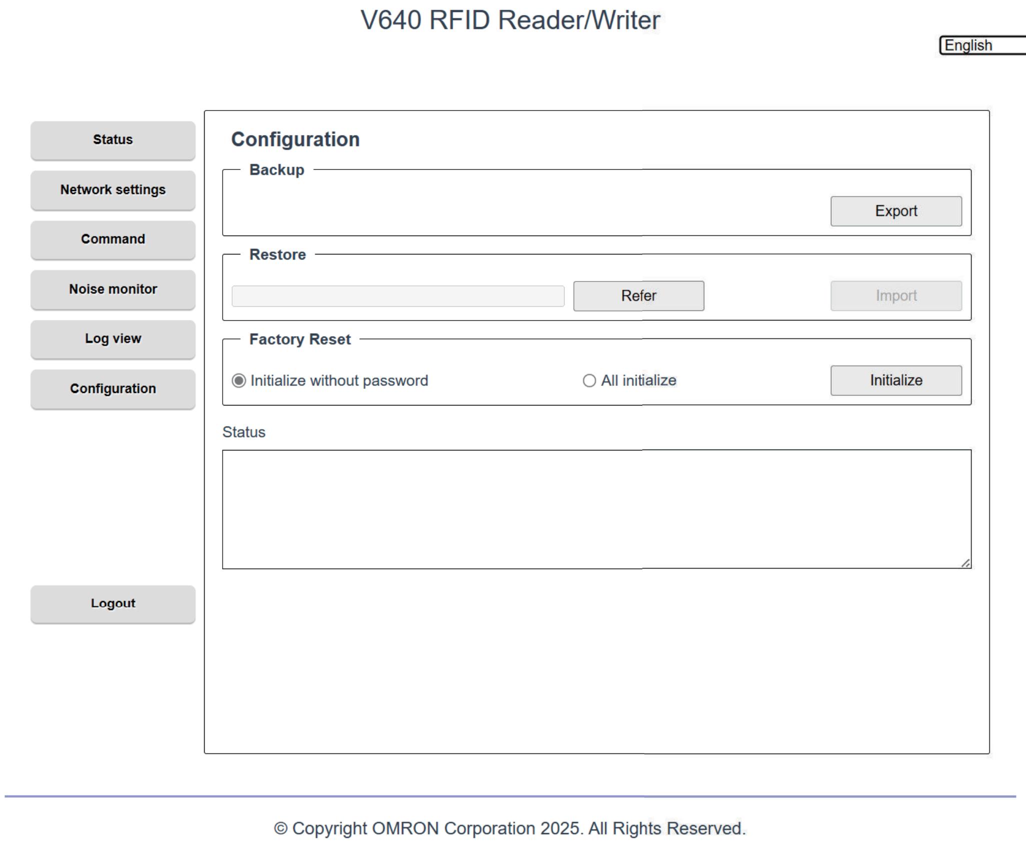
An example of an exported file.

```
PowerOnTime,Source,Category,Event,Result,Additional Info1,Additional Info2
8765h43m21s, DIPSwitch, Control System Events, Operating Mode Change, Run-Mode, 00000000, 00000000
8765h43m25s, WebBrowser:192.168.1.1, Access Control, Password Authentification, Successful, 00000000, 00000000
8765h45m59s, V640Command:192.168.1.1, Control System Events, Reboot, Normal, 00000000, 00000000
```

6-2-19 Configuration Window

The **Configuration** window allows you to perform Backup, Restore, and Factory Reset of settings.

For details on the Backup and Restore functions, see *5-2-6 Backup Function* on page 5-29.
For details on the Factory Reset, see *5-2-5 Factory Reset Function* on page 5-27.



● Initialize without password ○ All initialize

Item		Description	Notes
Backup			The file name when export is *conf.ini*.
	Export	Click to export the configuration file as a backup.	
Restore			Only ini files can be selected.
	Refer	Select the configuration file to restore.	
	Import	Click to import the configuration file to restore.	
Factory Reset			---
	Initialize without password	Select to initialize everything except the password.	
	All initialize	Select to initialize including the password.	
	Initialize	Click to perform initialization.	
Status		Displays the status of import, export, and initialization.	You cannot enter a value.

ini File Format

The format of the sections and entries in the ini file is as follows.

The text enclosed in [ ] indicates the section. Each entry is written on a separate line below it.

```
[DeviceProfile]
DeviceModel=V640-HAM11-ETN-V5
MACAddress=3c:f7:d1:95:50:14
FirmwareVersion=1.0.0
WebAppVersion=1.0.0
[NetworkSetting]
Dipsw_Enable=Disable
Dipsw_IPAddress=192.168.1.0
.
.
.
```

The section and entry names are as follows:

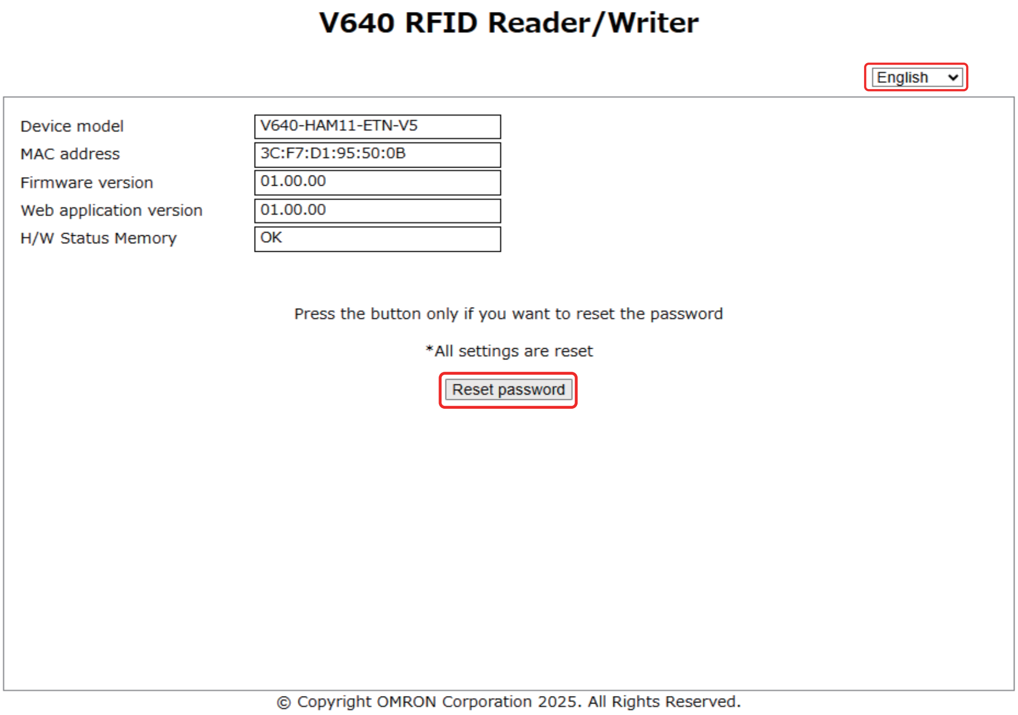
Group	Item	Section name	Entry name	A*1	B*2
Device Information	Model	[DeviceProfile]	DeviceModel	○	×
	Firmware Version		FirmwareVersion	○	×
	Web Application Version		WebAppVersion	○	×
	MAC Address		MACAddress	○	×
TCP/IP Settings (DIP Switch)	DIP Switch Enable/Disable	[NetworkSetting]	DipswEnable	○	×
	IP Address		DipswIPAddress	○	×
	Subnet Mask		DipswSubnetMask	○	×
TCP/IP Settings (ROM)	IP Address		IPAddress	○	○
	Subnet Mask		SubnetMask	○	○
Port Setting	TCP port number	[PortSetting]	TCPPort	○	○
	WebSocket port number		WebSocketPort	○	○
IP Filtering Settings	Enable/Disable (V640 Command)	[IPFilteringSetting]	TCPFilterEnable	○	○
	IP Address (V640 Command)		TCPFilterIPAddress	○	○
	Mask (V640 Command)		TCPFilterMask	○	○
	Enable/Disable (V640 Command)		WebFilterEnable	○	○
	IP Address (V640 Command)		WebFilterIPAddress	○	○
	Mask (V640 Command)		WebFilterMask	○	○
Web Interface Setting	Lock Time	[WebIFSetting]	WebLockTime	○	○
Permission Settings	ID-Tag Communication	[AccessPermissionSetting]	RFTagAccess	○	○
	Device Information		DeviceInfo	○	○
	Network Settings		NetworkSetting	○	○
	Log Information		LogPrivilege	○	○
	Host Communication Controls		CommunicationControl	○	○
	Unit Controls		UnitControl	○	○
Hash Value	Hash Value	[Hash]	Hash	○	○

*1. Export target

*2. Import target

6-2-20 Safe-Mode Window

The Safe-Mode window allows you to reset all of the unit settings, including the password, to factory default state.



V640 RFID Reader/Writer

Device model	V640-HAM11-ETN-V5
MAC address	3C:F7:D1:95:50:0B
Firmware version	01.00.00
Web application version	01.00.00
H/W Status Memory	OK

Press the button only if you want to reset the password

*All settings are reset

© Copyright OMRON Corporation 2025. All Rights Reserved.

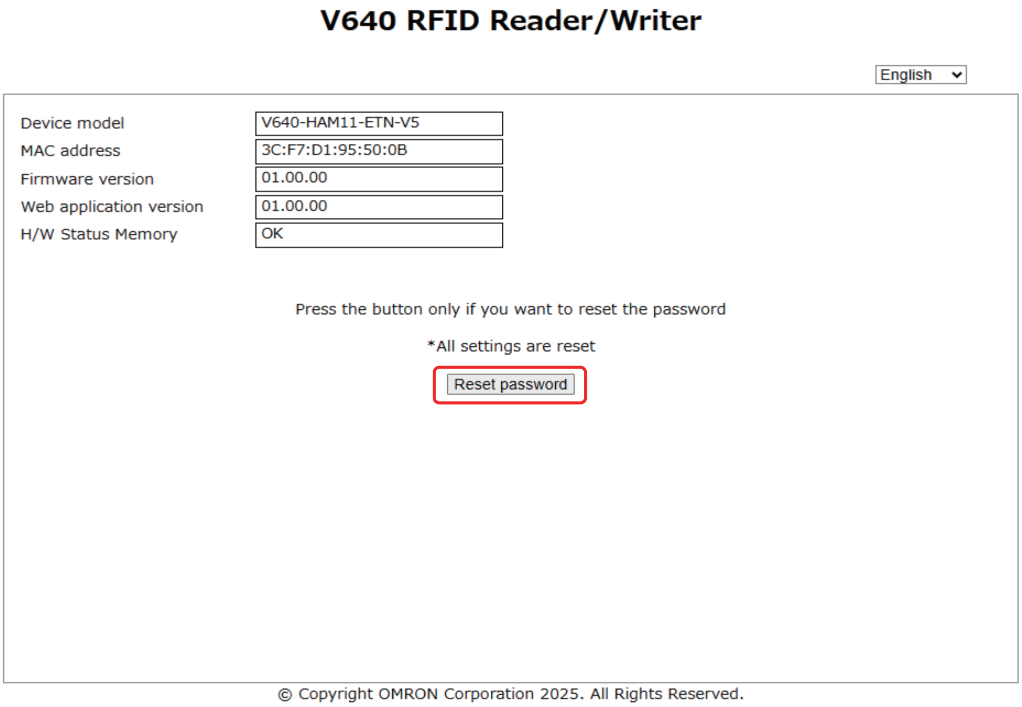
Item	Description	Notes
Language switch list	Switches the language. Select from Japanese/English.	---
Reset password	Click to perform initialization.	---

Initialization Procedure

1 Set the Amplifier Unit to Safe-Mode.
For Safe-Mode settings, refer to page 1-6.

2 Start the browser.

3 Enter the IP Address of the Amplifier Unit in the browser's URL field.
If the IP Address is the factory default, enter *https://192.168.1.200*.
The Web Browser Safe-Mode window will be displayed.



V640 RFID Reader/Writer

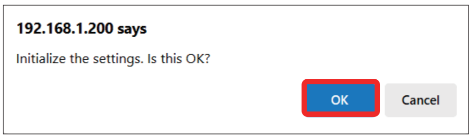
Device model	V640-HAM11-ETN-V5
MAC address	3C:F7:D1:95:50:0B
Firmware version	01.00.00
Web application version	01.00.00
H/W Status Memory	OK

Press the button only if you want to reset the password

*All settings are reset

© Copyright OMRON Corporation 2025. All Rights Reserved.

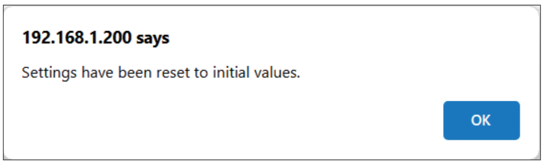
4 Click the **Reset password** button to display the following dialog. Click the **OK** button to start the initialization process.



192.168.1.200 says

Initialize the settings. Is this OK?

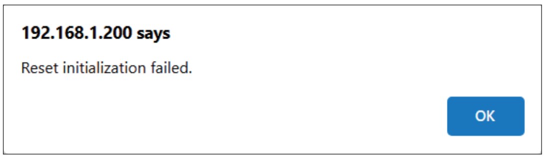
After clicking the **OK** button, you cannot cancel the initialization process.
If the initialization is successful, the following dialog will be displayed.



192.168.1.200 says

Settings have been reset to initial values.

If the initialization fails, the following dialog will be displayed. Restart the Amplifier Unit and perform the initialization again.



192.168.1.200 says

Reset initialization failed.

6-3 Root Certificate Installation Procedure

This section describes the procedure for connecting the Web Browser and the Amplifier Unit in a secure state.
Please download the root certificate *RFID_omronca.crt* from the following URL beforehand.
https://www.fa.omron.co.jp/products/family/1474/download/software.html

Precautions for Correct Use

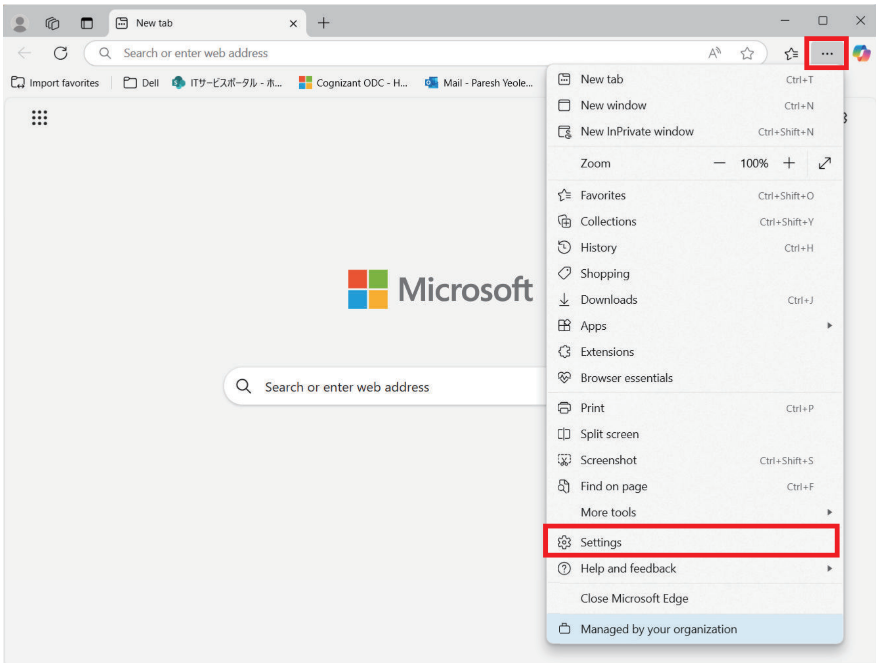
In this procedure, the hosts file (C:\windows\system32\drivers\etc\hosts) in the computer is rewritten.
If the entry is incorrect, the computer may not be able to connect.

Procedure Overview

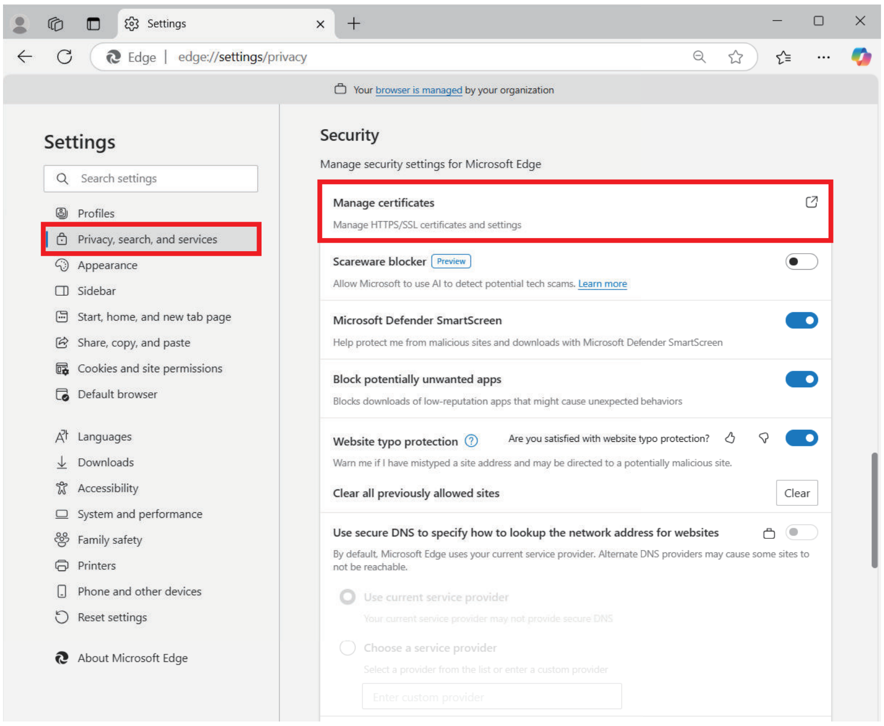
Procedure	Description
Installing the root certificate	Install the root certificate for the Amplifier Unit on the computer that uses the Web Browser.
Setting the domain name	In the hosts file in the computer, set the domain name of the Amplifier Unit to be connected with the Web Browser. If you do not set the domain name, the connection will be in "Not secure" state.
Start the Web Browser in a secure state	Enter the domain name in the address field of the Web Browser and confirm that the connection is secure.

1 Install the root certificate.
As an example, the use of Microsoft Edge is explained.

1) Click the **horizontal ellipsis** in the upper right corner of the Microsoft Edge, and then click **Settings**.



2) Click **Privacy, search, and services** – **Manage certificate**.



Security

Manage security settings for Microsoft Edge

Manage certificates

Manage HTTPS/SSL certificates and settings

Scareware blocker Preview

Allow Microsoft to use AI to detect potential tech scams. Learn more

Microsoft Defender SmartScreen

Help protect me from malicious sites and downloads with Microsoft Defender SmartScreen

Block potentially unwanted apps

Blocks downloads of low-reputation apps that might cause unexpected behaviors

Website typo protection ⓘ Are you satisfied with website typo protection?

Warn me if I have mistyped a site address and may be directed to a potentially malicious site.

Clear all previously allowed sites Clear

Use secure DNS to specify how to lookup the network address for websites

By default, Microsoft Edge uses your current service provider. Alternate DNS providers may cause some sites to not be reachable.

○ Use current service provider

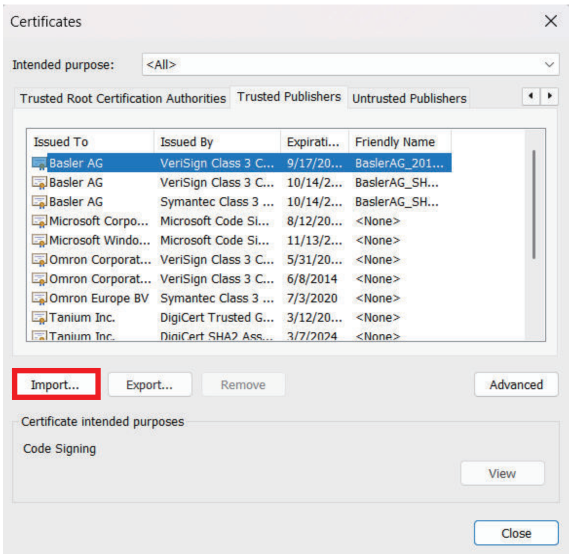
Your current service provider may not provide secure DNS

○ Choose a service provider

Select a provider from the list or enter a custom provider

Enter custom provider

3) When the certificate dialog opens, click the **Import** button.



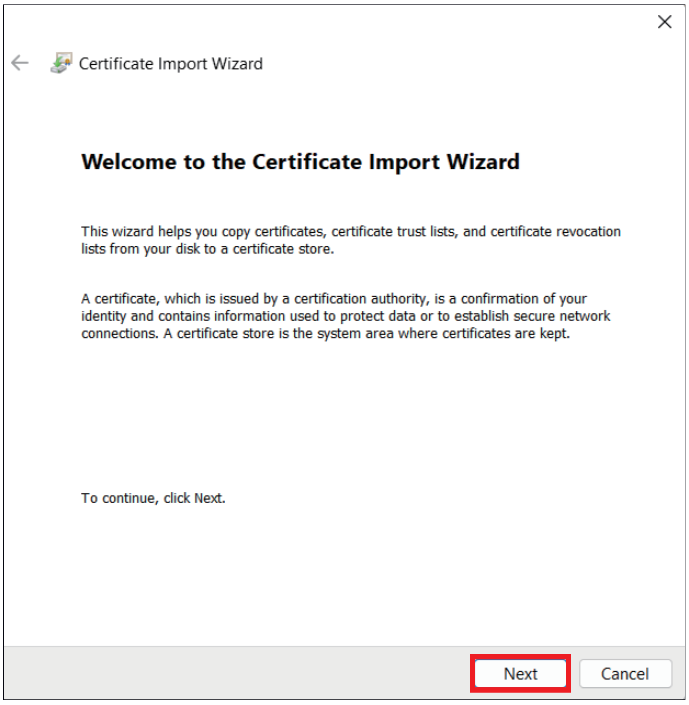
Intended purpose: <All>

Issued To	Issued By	Expirati...	Friendly Name
Basler AG	VeriSign Class 3 C...	9/17/20...	BaslerAG_201...
Basler AG	VeriSign Class 3 C...	10/14/2...	BaslerAG_SH...
Basler AG	Symantec Class 3 ...	10/14/2...	BaslerAG_SH...
Microsoft Corpo...	Microsoft Code Si...	8/12/20...	<None>
Microsoft Windo...	Microsoft Code Si...	11/13/2...	<None>
Omron Corporat...	VeriSign Class 3 C...	5/31/20...	<None>
Omron Corporat...	VeriSign Class 3 C...	6/8/2014	<None>
Omron Europe BV	Symantec Class 3 ...	7/3/2020	<None>
Tanium Inc.	DigiCert Trusted G...	3/12/20...	<None>
Tanium Inc.	DigiCert SHA2 Ass...	3/7/2024	<None>

Certificate intended purposes

Code Signing

4) When the following dialog opens, click the **Next** button.



Certificate Import Wizard

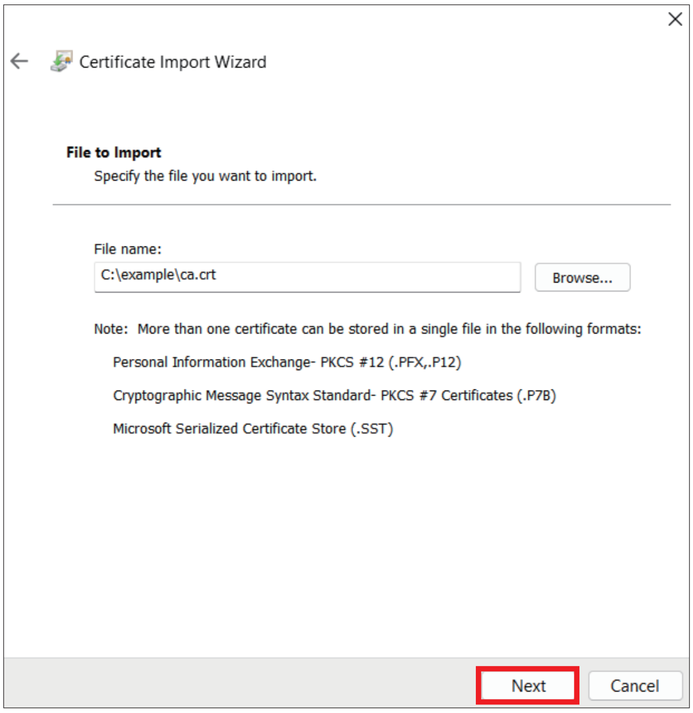
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

5) In the following dialog, select the root certificate **RFID_omronca.crt** and click the **Next** button.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\example\ca.crt

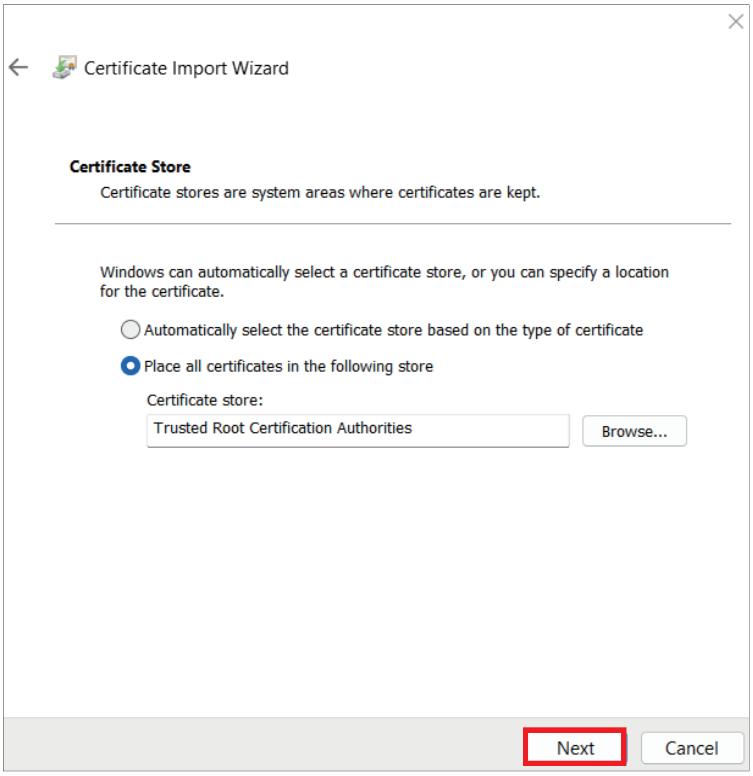
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

6) In the Certificate Store field, select **Trusted Root Certification Authorities** and click the **Next** button.



Certificate Store

Certificate stores are system areas where certificates are kept.

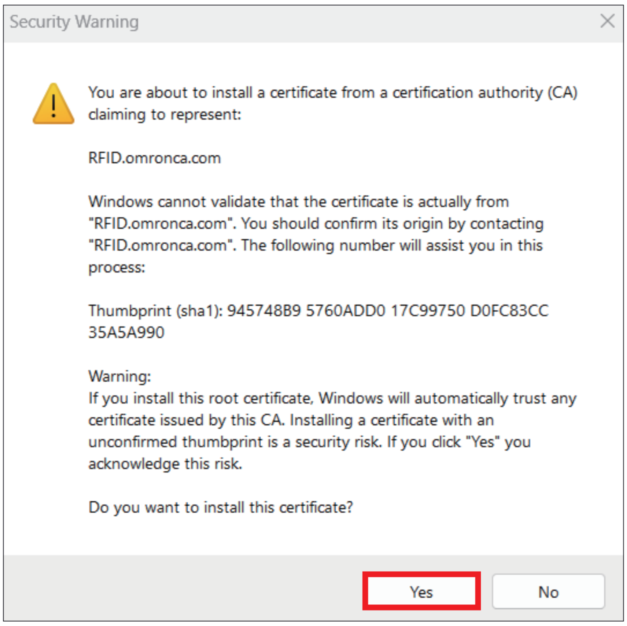
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

7) The following **security warning** dialog may be displayed. Make sure that the imported root certificate is the file provided by OMRON and click the **Yes** button.



You are about to install a certificate from a certification authority (CA) claiming to represent:

RFID.omronca.com

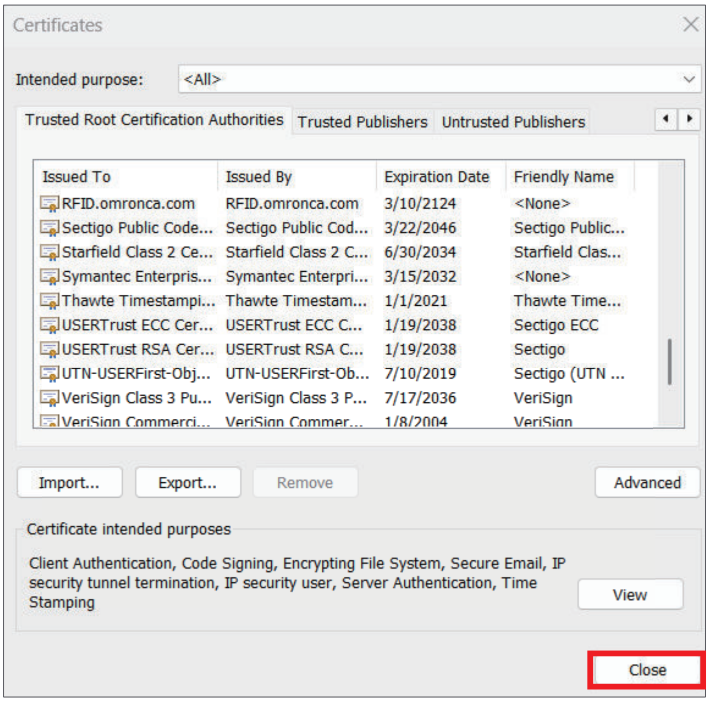
Windows cannot validate that the certificate is actually from "RFID.omronca.com". You should confirm its origin by contacting "RFID.omronca.com". The following number will assist you in this process:

Thumbprint (sha1): 945748B9 5760ADD0 17C99750 D0FC83CC 35A5A990

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

8) If **RFID_omronca.crt** is displayed in the **Trusted Root Certification Authorities** tab, installation of the root certificate is complete. Click the **Close** button to close the screen.



Issued To	Issued By	Expiration Date	Friendly Name
RFID.omronca.com	RFID.omronca.com	3/10/2124	<None>
Sectigo Public Code...	Sectigo Public Cod...	3/22/2046	Sectigo Public...
Starfield Class 2 Ce...	Starfield Class 2 C...	6/30/2034	Starfield Clas...
Symantec Enterpris...	Symantec Enterpri...	3/15/2032	<None>
Thawte Timestampi...	Thawte Timestam...	1/1/2021	Thawte Time...
USERTrust ECC Cer...	USERTrust ECC C...	1/19/2038	Sectigo ECC
USERTrust RSA Cer...	USERTrust RSA C...	1/19/2038	Sectigo
UTN-USERFirst-Obj...	UTN-USERFirst-Ob...	7/10/2019	Sectigo (UTN ...
VeriSign Class 3 Pu...	VeriSign Class 3 P...	7/17/2036	VeriSign
VeriSign Commerci...	VeriSign Commer...	1/8/2004	VeriSign

Certificate intended purposes

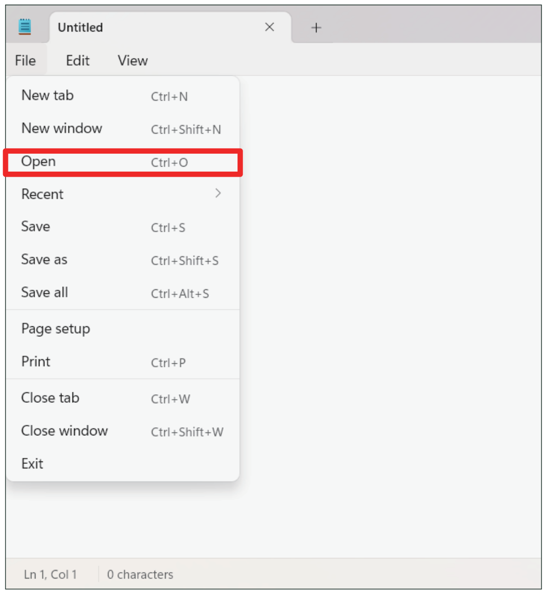
Client Authentication, Code Signing, Encrypting File System, Secure Email, IP security tunnel termination, IP security user, Server Authentication, Time Stamping

2 Next, set the domain name of the Amplifier Unit.

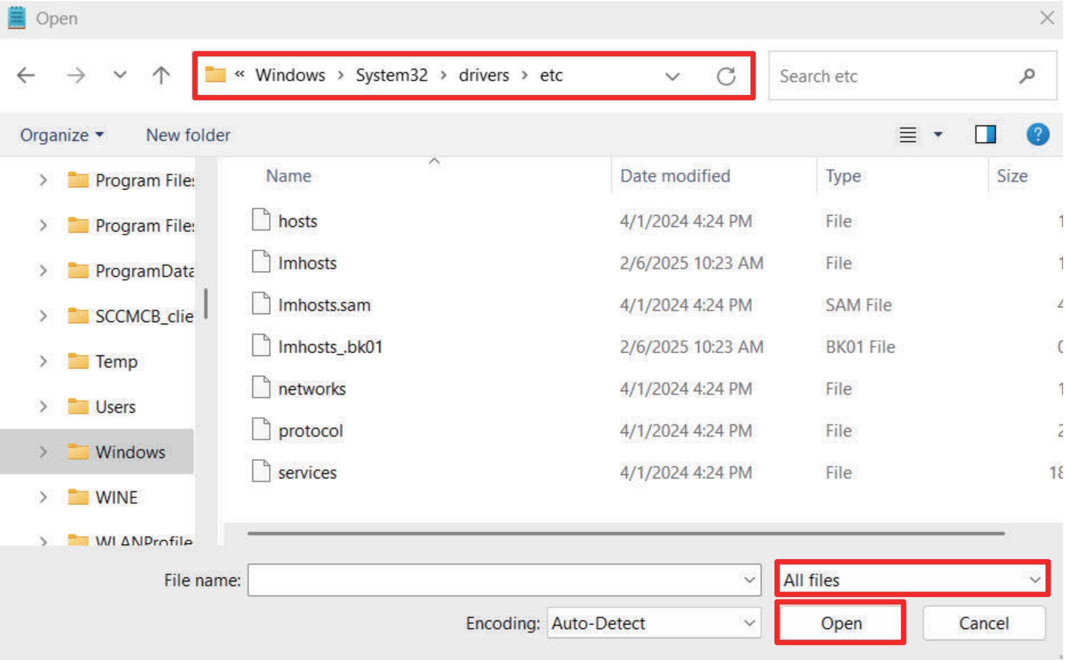
To set the domain name, write the correspondence between the Amplifier Unit's IP address and domain name in the hosts file.

1) From the Start menu, right-click Notepad in Windows Accessories and click Other - Run as administrator.

2) Click **File** - **Open**.



3) Select **All Files (*.*)** and enter *C:\Windows\System32\drivers\etc* in the address bar. Select the **hosts file** and click the **Open** button.



Address: « Windows › System32 › drivers › etc

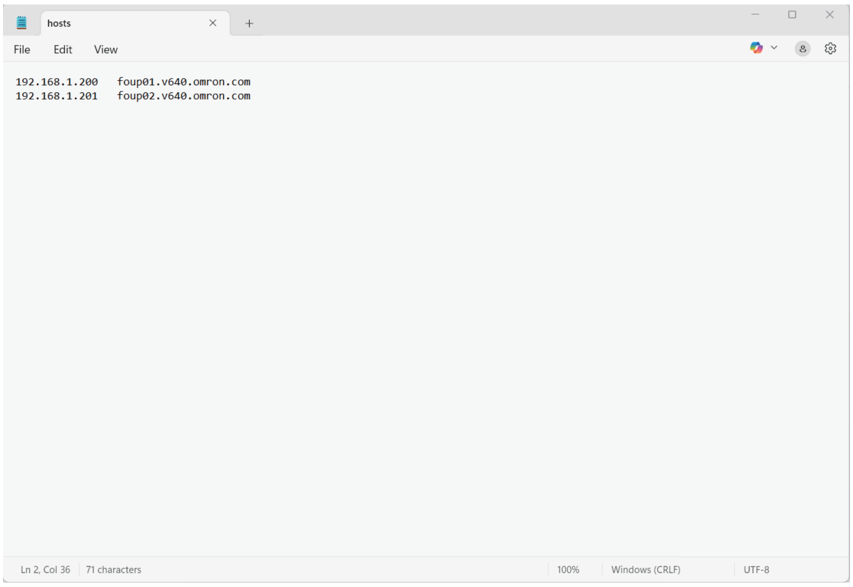
Name	Date modified	Type	Size
hosts	4/1/2024 4:24 PM	File	1
lmhosts	2/6/2025 10:23 AM	File	1
lmhosts.sam	4/1/2024 4:24 PM	SAM File	4
lmhosts_.bk01	2/6/2025 10:23 AM	BK01 File	(
networks	4/1/2024 4:24 PM	File	1
protocol	4/1/2024 4:24 PM	File	2
services	4/1/2024 4:24 PM	File	18

File name:

All files

Encoding: Auto-Detect

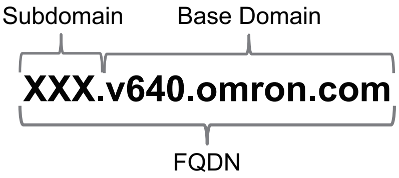
4) In the hosts file, the correspondence between IP addresses and domain names is described on each line. Add the IP address and domain name of the Amplifier Unit to be connected to the Web Browser.



```
192.168.1.200   foup01.v640.omron.com
192.168.1.201   foup02.v640.omron.com
```

Ln 2, Col 36 | 71 characters | 100% | Windows (CRLF) | UTF-8

The server certificate for the Amplifier Unit is a wildcard certificate. You can set multiple Amplifier Unit domain names by using alphanumeric characters, - (hyphen), and . (period), with 3 characters or more, and 63 characters or less, for the subdomain name.



Example: When connecting the following two Amplifier Units to the network

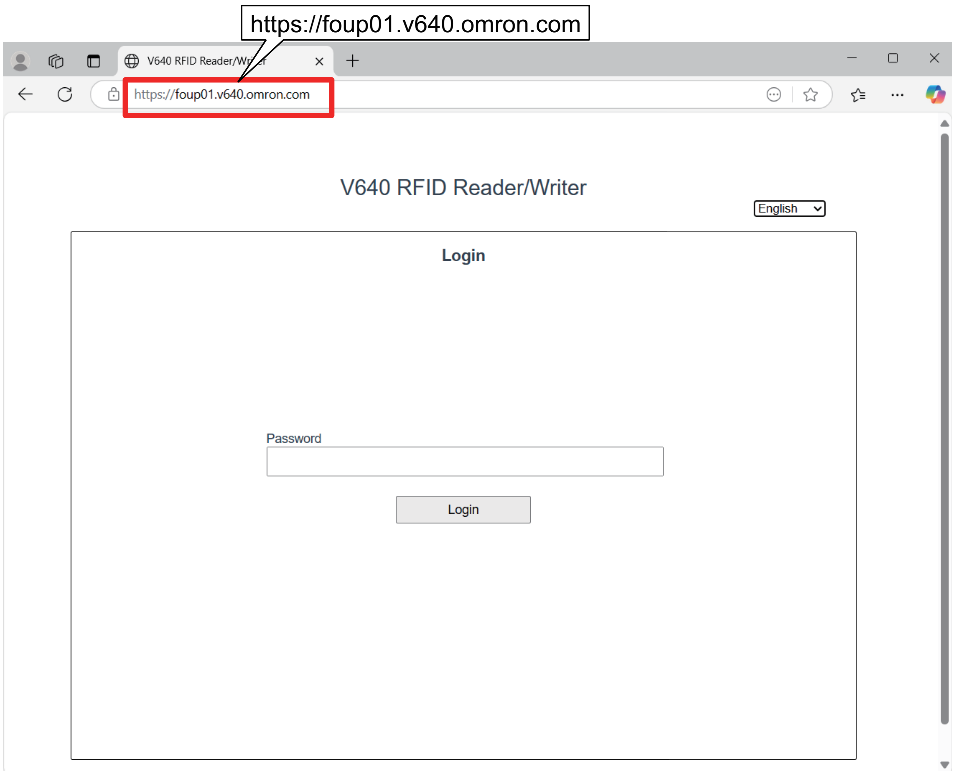
IP address	Subdomain name
192.168.1.200	foup01
192.168.1.201	foup02

Add the following to the hosts file.

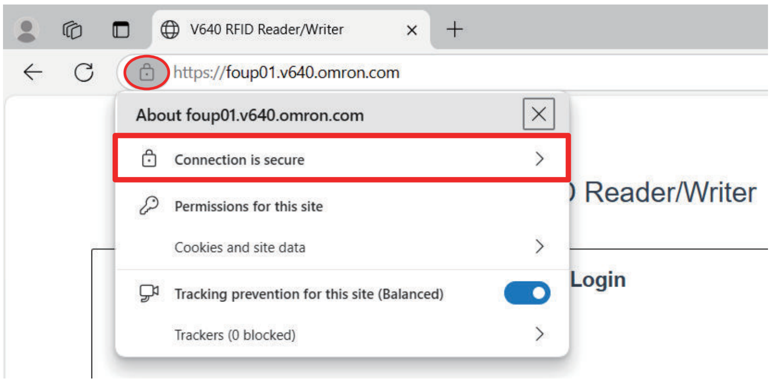
```
192.168.1.200    foup01.v640.omron.com
192.168.1.201    foup02.v640.omron.com
```

3 Connect the Web Browser and Amplifier Unit in a secure state.

1) If the subdomain name is *foup01*, enter the domain name in the address field of the Web Browser as follows.



2) Click the lock symbol to the left of the address bar and confirm that it says **The connection is secure**.



V640 RFID Reader/Writer

https://foup01.v640.omron.com

About foup01.v640.omron.com

Connection is secure

Permissions for this site

Cookies and site data

Tracking prevention for this site (Balanced)

Trackers (0 blocked)

Additional Information

If you can't connect to the Amplifier Unit

If a VPN (Virtual Private Network) connection or proxy settings are active, you may not be able to connect.

- If a VPN connection is active, disable the VPN connection by disabling Wi-Fi, for example, before connecting.
- If proxy settings are active, disable the proxy settings before connecting.

7

Troubleshooting

This section explains how to troubleshoot the V640-series.

7-1 Troubleshooting 7-2
7-1-1 Status Check with OPERATING Indicator (LED) 7-2
7-1-2 List of Error Messages 7-3
7-1-3 Operation Check Flowchart 7-4
7-1-4 Other Troubleshooting 7-10

7-1 Troubleshooting

Errors are indicated by the presence or absence of a response to an Amplifier Unit command, and by the indicators.

7-1-1 Status Check with OPERATING Indicator (LED)

The operating status of the Amplifier Unit can be checked with the OPERATING indicator (LED).

Amplifier Unit operating status		OPERATING indicator (LED)				ID tag communications	Communications with host
		RUN (green)	COMM (orange)	NORM (green)	ERROR (red)		
Startup		●	●	●	●	Not possible	Not possible
Normal operation	**RUN-Mode**	☼	●	●	●	Possible	Possible
	Safe-Mode	◐ (2 s intervals)	●	●	●	Not possible	Possible
Fatal error in Amplifier Unit	**IP address conflict error**	●	●	●	◐ (Irregularly twice)	Not possible	Not possible
	WDT error	●	●	●	☼	Not possible	Not possible
	Hardware error(9□)	☼	●	●	☼	Not possible	Not possible （Partially possible）
Non-fatal error in Amplifier Unit	**Host communications error(1□)**	☼	●	●	☼ (Lights once)	Possible	Possible
	ID tag communications error(7□)	☼	☼	●	☼ (Lights once)	Possible	Possible

Amplifier Unit Indicators

Name	Indications
RUN (green)	Turns ON when the Amplifier Unit is in normal operation.
COMM (orange)	Turns ON during communications with the host device or during communications with an ID Tag.
NORM (green)	Turns ON when the communications finish with no error.
ERROR (red)	Turns ON when an error occurs during communications with the host device, or during communications with an ID Tag.

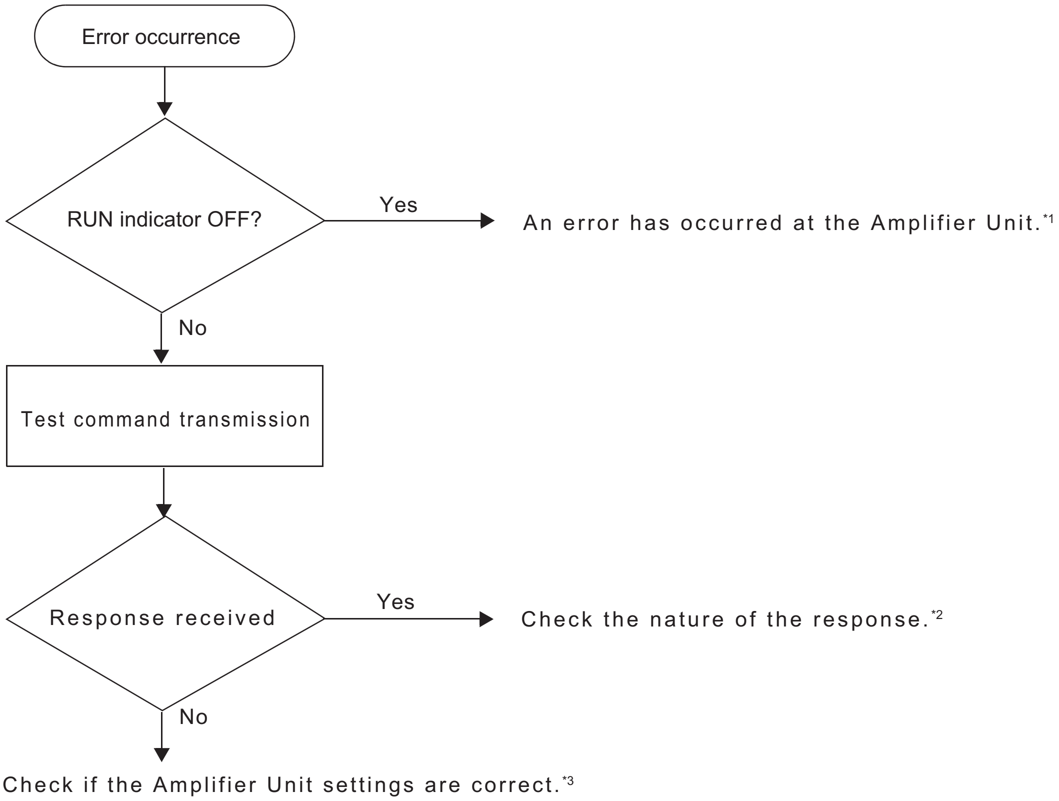
7-1-2 List of Error Messages

Type	Response code	Name	Description
Host communications error	14	Format error	There is an error in the command format. (For example, command code, page designation, address designation, or processed data volume is inappropriate.) The command received by the Amplifier Unit could not be executed.
ID tag communications error	70	Communications error	Noise or another hindrance has occurred during communications with an ID Tag, and communications cannot be completed normally.
	71	Verification error	Correct data cannot be written to an ID Tag.
	72	No Tag error	Either there is no ID Tag in front of the CIDRW Head, or the CIDRW Head is unable to detect the ID Tag due to environmental factors (e.g., noise).
	7B	Outside write area error	The ID Tag is at a position where reading is possible but writing is not, so writing does not complete normally.
	7E	ID system error (1)	The ID Tag is in a status where it cannot execute the command processing.
	7F	ID system error (2)	An inapplicable ID Tag has been used.
Hardware error	9A	Memory error	There is an error in the memory inside the Amplifier Unit. (If restarting the Amplifier Unit does not resolve the issue, please contact your OMRON representative.)

7-1-3 Operation Check Flowchart

From Installation to Trial Operation

Errors are indicated by whether or not a response to the test command is received and by the status of the Amplifier Unit indicators.


Error occurrence
RUN indicator OFF?
Yes
An error has occurred at the Amplifier Unit.*1
No
Test command transmission
Response received
Yes
Check the nature of the response.*2
No
Check if the Amplifier Unit settings are correct.*3

*1. Refer to *Amplifier Unit Error* on page 7-5.
*2. Refer to *If There Is a Response to the Command:* on page 7-5.
*3. Refer to *If There Is No Response to the Command:* on page 7-5.

- **If the Test Command Was Received Normally:**

Indicators

RUN	COMM	NORM	ERROR
☼	☼ (Lights once)	●	●

Response Code for the Response

Type	Response code	Function
Normal	00	The command was received normally.

● Amplifier Unit Error

Check the status of the indicators after transmission of the test command.

After taking appropriate corrective action, restart the Amplifier Unit, send the test command again and check again.

RUN	COMM	NORM	ERROR	Main check points
●	●	●	☼	**WDT error**[*1] • Please check for conductive objects or noise Restart the Amplifier Unit and see if that resets the error. If the error is not caused by conductive objects or noise, there is a possibility of an Amplifier Unit failure. Replace the Amplifier Unit.
●	●	●	◐ (Irregularly twice)	**IP address conflict error**[*2] • Please check the IP addresses of devices on the same network Set a different IP address and restart the system. The new settings will not become effective until the system is restarted.
●	—	—	☼	The Amplifier Unit may be damaged.
●	—	—	●	• Influence of background noise (change installation position) • Amplifier Unit power supply If the error cannot be resolved after checking, the Amplifier Unit may be damaged.

[*1.] This error can occur for an Amplifier Unit. This error occurs when the watchdog timer times out because of a hardware failure or when temporary data corruption causes the Amplifier Unit to hang.

[*2.] When the Amplifier Unit starts up, the IP address conflict detection function is activated. This error occurs when the Amplifier Unit detects devices with the same IP address on the same network.
The IP address conflict detection function will not work during operation after startup.

● If There Is a Response to the Command:

Check the status of the indicators after transmission of the test command.

After taking appropriate corrective action, restart the Amplifier Unit, send the test command again and check again.

RUN	COMM	NORM	ERROR	Main check points
☼	●	●	☼ (Lights once)	There is a mistake in the command format (number of characters, character code, etc.) .
☼	●	●	☼	By an interruption of the power supply, the memory may be damaged.

● If There Is No Response to the Command:

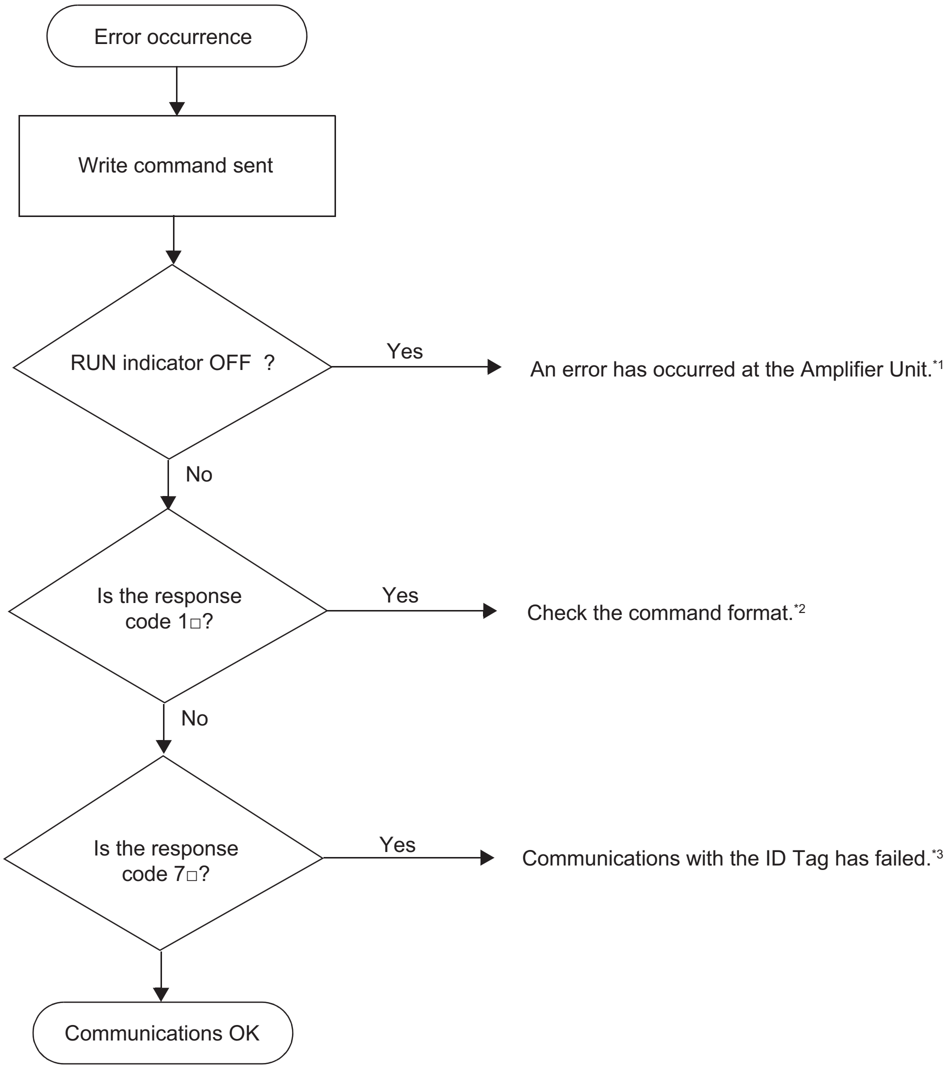
Check the status of the indicators after transmission of the test command.

After taking appropriate corrective action, restart the Amplifier Unit, send the test command again and check again.

RUN	COMM	NORM	ERROR	Main check points
☼	●	●	●	• Pleas establish the connection between the PC and the Amplifier Unit again, because the TCP/IP connection may be disconnected. • Connection and wiring of the cable between the host device and Amplifier Unit • Routing of each cable (influence of background noise) If the error cannot be resolved after checking, the Amplifier Unit may be damaged.
☼	●	●	☼ (Lights once)	• Connection and wiring of the cable between the host device and Amplifier Unit • Routing of the cables (influence of background noise) • There is a mistake in the command format (number of characters, character code, etc.)

From Trial Operation to Communications

Errors are indicated by the status of the indicators after transmission of the write command, and by the response code of the response.



*1. Refer to *Amplifier Unit Error* on page 7-8.
*2. Refer to *If the Response Code is 1□:* on page 7-8.
*3. Refer to *If the Response Code is 7□:* on page 7-9.

● If the ID Tag Was Processed Normally:

Indicators

RUN	COMM	NORM	ERROR
☼	☼ (Lights once)	☼ (Lights once)	●

Response Code for the Response

Type	Response code	Function
Normal	00	The ID Tag was processed normally.

Additional Information

If there is no response to the write command, refer to the Operation Check Flowchart of *From Installation to Trial Operation* on page 7-4.

● Amplifier Unit Error

Check the status of the indicators after transmission of the command.

After taking appropriate corrective action, send the write command again and check again.

RUN	COMM	NORM	ERROR	Main check points
●	— (If RUN is OFF, the status of the other indicators can be ignored.)			• Influence of background noise (Change installation position) • Amplifier Unit power supply If the error cannot be resolved by checking the two points above, the Amplifier Unit may be damaged.

● If the Response Code is 1□:

There is a host device communications error.

Check the status of the indicators and the response code of the response after transmission of the command.

After taking appropriate corrective action, send the write command again and check again.

RUN	COMM	NORM	ERROR
☼	●	●	☼ (Lights once)

Response code	Main check points
14	• There is an error in the command format. Please check the command format (command code, page designation, address designation, processed data volume, etc.) and resend the command. • The command received by the Amplifier Unit could not be executed. Please check the operating status and Permission Settings of the Amplifier Unit and resend the command.

● If the Response Code is 7☐:

There is a communications error in communications between the CIDRW Head and ID Tag.
Check the status of the indicators and the response code of the response after transmission of the command.
After taking appropriate corrective action, send the write command again and check again.

RUN	COMM	NORM	ERROR
☼	☼ (Lights once)	●	☼ (Lights once)

Response code	Main check points
70	• Background noise levels of the CIDRW Head (Check the surroundings with the environmental noise level measurement function) • Distance to another CIDRW Head • Influence of background noise (Change installation position) • Please check the Antenna Connection Status by using “GET PARAMETER“ command. Refer to page 4-16, *Functions* on page 1-6. If the error cannot be resolved after checking, the Amplifier Unit may be damaged.
71	• ID Tag overwrite life (Replace the ID Tag) • Environment of use of the ID Tags (ID Tag breakage due to use in unanticipated ways)
72	• Connection to the CIDRW Head • Distance between the ID Tag and CIDRW Head • CIDRW Head background noise levels (Check the surroundings with the environmental noise level measurement function) • Distance to another CIDRW Head. Please check the Antenna Connection Status by using “GET PARAMETER“ command. Refer to page 4-16, *Functions* on page 1-6.
7B	• Distance between the ID Tag and CIDRW Head • Background noise levels of the CIDRW Head (Check the surroundings with the environmental noise level measurement function) • Distance to another CIDRW Head • Influence of background noise (Change installation position)
7E	• Type/specifications of the ID Tags used • Settings of the ID Tags used (The ID Tag lock function is used. The ID Tag has a lock function, but the Amplifier Unit has no function for locking an ID Tag.) • Environment of use of the ID Tags (ID Tag breakage due to use in unanticipated ways)
7F	

7-1-4 Other Troubleshooting

Operating in Test Mode

Always connect the CIDRW Head before operating the Amplifier Unit in Test Mode. If Test Mode is used with abnormal CIDRW Head cable or without connecting a CIDRW Head, the ERROR indicator will light and Amplifier Unit operation will stop.

RUN	COMM	NORM	ERROR	Main check points
☼	●	●	☼	• Please check that the CIDRW Head is connected correctly. If the error cannot be resolved after checking, the Amplifier Unit or the CIDRW Head may be damaged.

Safe-Mode

When starting in Safe-Mode, the OPERATING indicator will be in the following state.

RUN	COMM	NORM	ERROR	Main check points
◐ (2 s intervals)	●	●	●	• Please check DIP Switch 8 on the side face of the Amplifier Unit When it is ON, it is set to Safe-Mode. Please change it to OFF and restart the system. The new settings will not become effective until the system is restarted.

A

Appendices

This section explains the specifications, dimensions, connection examples, characteristic data according to conditions of use, ID Tag memory map, and more.

A-1 Specifications and Dimensions A-2
A-1-1 Amplifier Units A-2
A-1-2 CIDRW Heads A-5

A-2 Connection Examples A-7
A-2-1 V640-HAM11-ETN-V5 .... A-7
A-2-2 V640-HAM11-L-ETN-V5 .... A-7

A-3 Characteristic Data According to Conditions of Use A-8
A-3-1 Maps of Communications Areas (Reference Only) A-8
A-3-2 Mutual Interference Distances (Reference Only) A-32
A-3-3 Influence of Background Metals (Reference Only) A-34
A-3-4 Communications Time A-35
A-3-5 Communications Distance Characteristics vs. Ambient Noise A-38

A-4 ID Tag Memory Maps A-39
A-4-1 RI-TRP-DR2B(-40) A-39
A-4-2 RI-TRP-WR2B(-30) A-39

A-5 Regular Inspection A-40

A-6 ASCII Code Table A-41

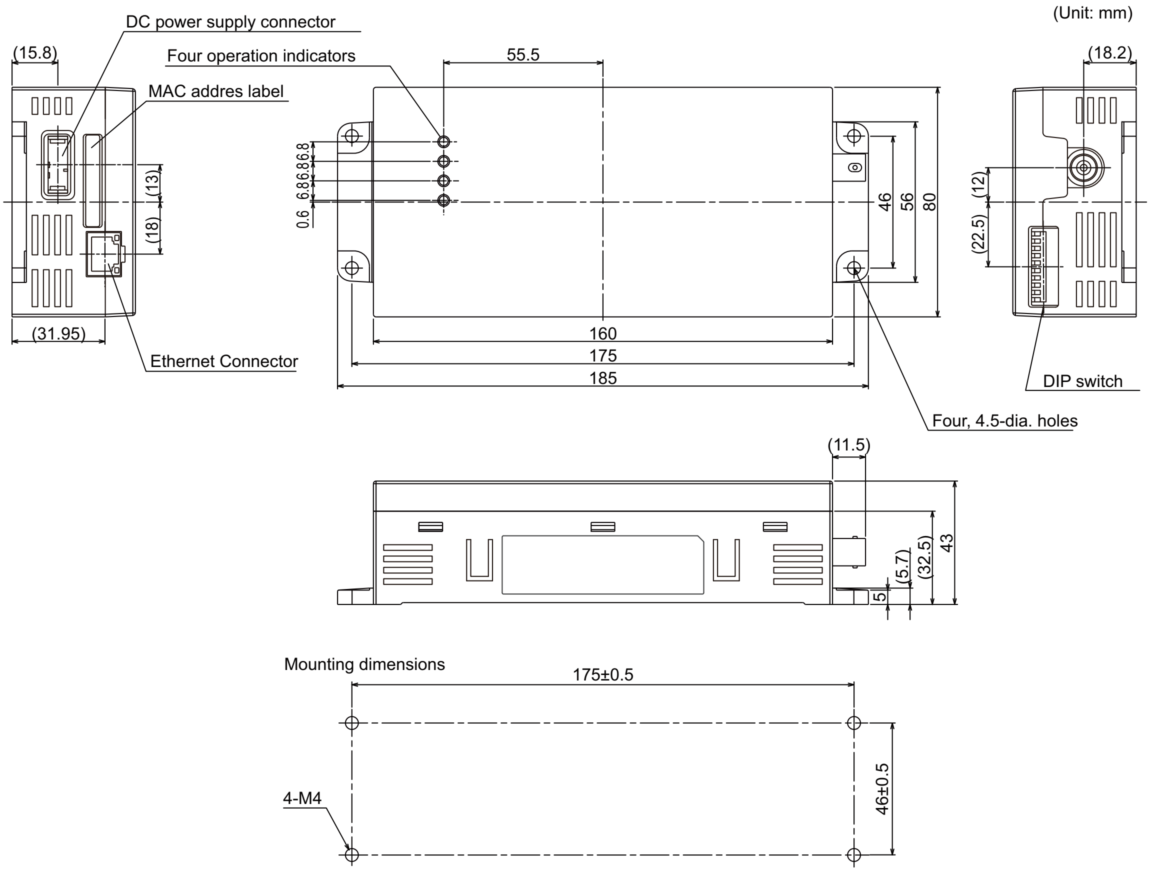
A-7 Degree of Protection A-42

A-1 Specifications and Dimensions

A-1-1 Amplifier Units

V640-HAM11-ETN-V5 and V640-HAM11-L-ETN-V5

- **Dimensions**



● Specifications

Item	Specifications	
	V640-HAM11-ETN-V5	V640-HAM11-L-ETN-V5
Power supply voltage	24 VDC +10% -15%	
Current consumption	150 mA max.	400 mA max.
Degree of protection	IP20 (IEC60529)	
Ambient temperature	Operating: 0 to +40°C Storage: -15 to +65°C (with no icing)	
Ambient humidity	Operating/Storage: 35% to 85% (with no condensation)	
Insulation resistance	20 MΩ min.(with 100 VDC megohmmeter) between power supply terminals and the frame ground terminal	
Dielectric strength	1,000 VAC (50/60 Hz for 1 min.) leak current consumption 5 mA max. between both power supply terminals and the frame ground terminal	
Vibration resistance	10 to 150 Hz, double amplitude: 0.20 mm, Max. Acceleration: 15 m/s^2 with 10 sweeps for 8 min. each in 3 directions	
Shock resistance	150 m/s^2, 3 times each in 6 directions	
Ground	Ground to 100 W or less.	
Case material	PC/ABS resin	
Dimensions	80x185x43 mm (WxDxH, excluding protruding parts)	
Mass	Approx. 250 g	
Frequency	134.2 kHz	
Rediated magnetic field strength	maximum 35 dBmA/m at 10 meters (fixed)	
Environmental pollution degree	Degree 2	
Over voltage category	Category I	
Mounting method	Secured with four M4 screws. (tightening torque: 1.2N·M)	
CIDRW Head	V640-HS61	V640-HS62

● Host Communications Specifications

Item	Description
Compliant standards	10Base-T and 100Base-TX
Protocol	TCP/IP
IP Address	The IP address of the Amplifier Unit can be either set on this DIP Switch or the desired IP address can be set in ROM. • When set by DIP Switch (any of DIP Switch1-5 is ON) If the IP address is set on the DIP Switch, it will be in the form 192.168.1.□□□. The subnet mask is always 255.255.255.0. • When set by ROM (all DIP Switch1-5 are OFF) If pins 1 to 5 on the DIP Switch are all turned OFF, the IP address that is set in ROM will be used. Refer to *3-2 Setting the Communications Conditions for Amplifier Units* on page 3-3. **Default network settings** IP Address: 192.168.1.200, Subnet mask: 255.255.255.0 (Pins 1 to 5 on the DIP Switch are all turned OFF)
Applicable port	TCP/IP: port 7090
MTU	1,500 bytes

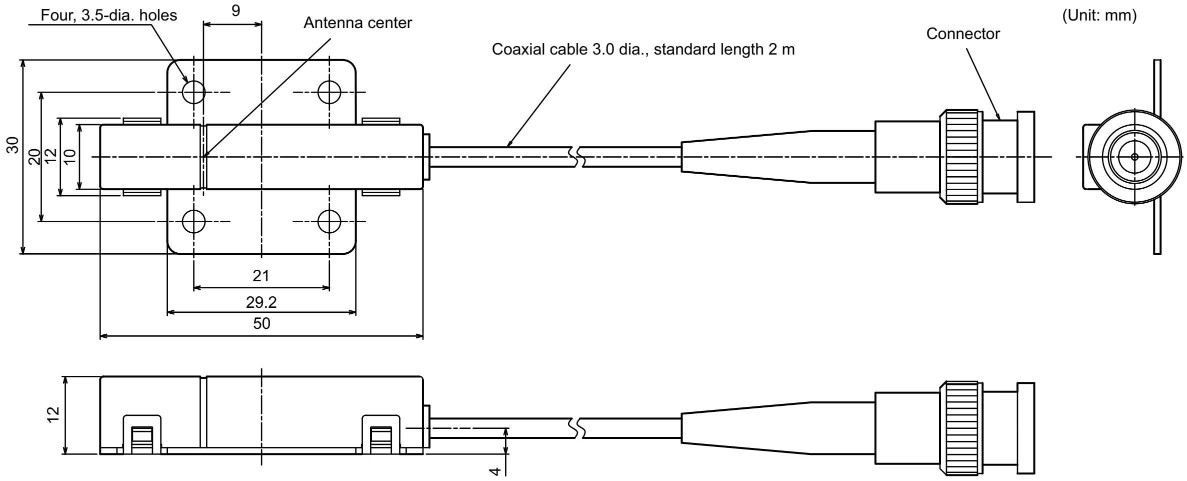
Additional Information

- Access to an Amplifier Unit is possible from only one host device at a time. If a host device (A) is connected to an Amplifier Unit and another host device (B) connects to the Amplifier Unit, the connection between host device A and the Amplifier Unit will be automatically broken and host device B will have the control right.
- When the connection between a PC and a Amplifier Units have been disconnected, an Amplifier Unit can reopen communication from a PC again by establishing a connection.
- Communications with the ID Tag will be aborted if the Ethernet cable is disconnected or the connection is broken while the Amplifier Unit is communicating with an ID Tag.

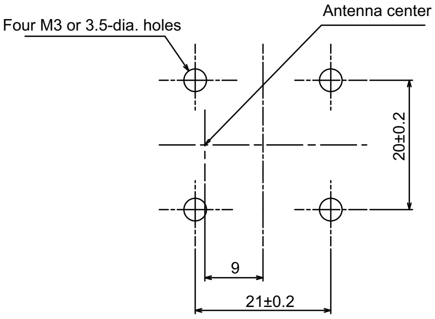
A-1-2 CIDRW Heads

V640-HS61

● Dimensions



Mounting dimensions

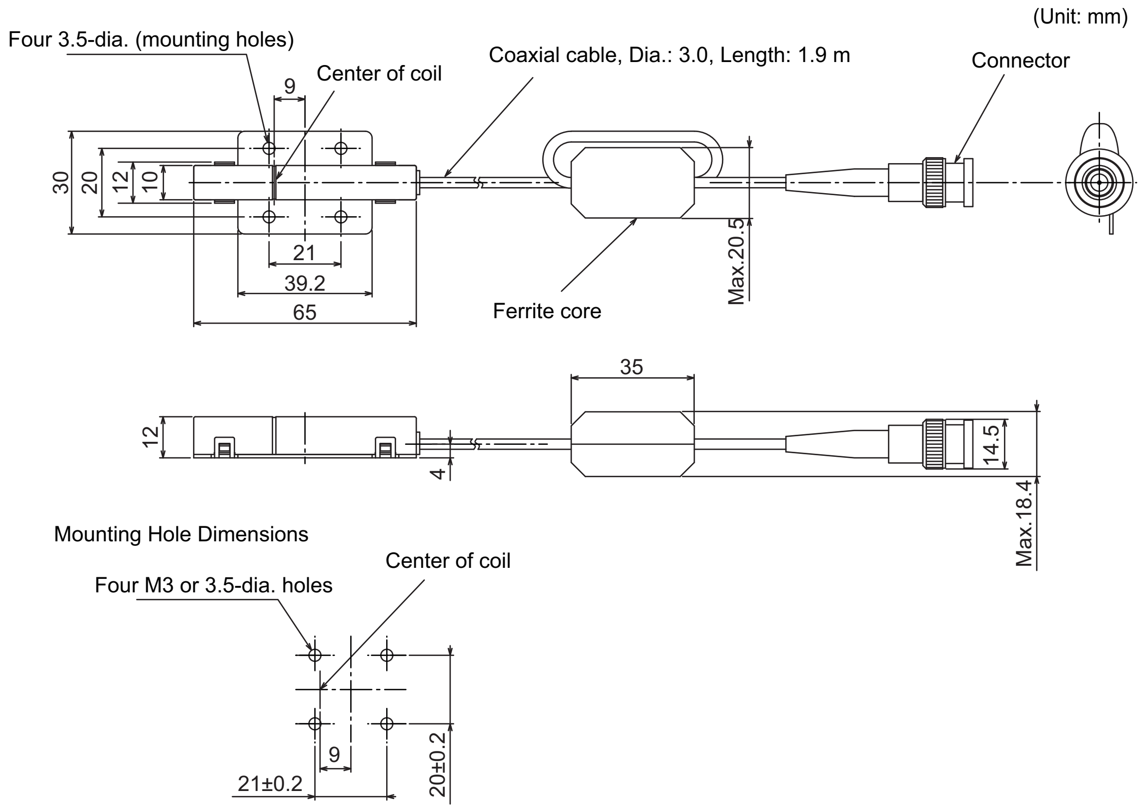


● Specifications

Item	Specifications
Transmission frequency	134 kHz
Ambient temperature	Operating: 0 to +40°C Storage: -15 to +65°C (with no icing)
Ambient humidity	Operating/Storage: 35% to 85% (with no condensation)
Degree of protection	IP20 (IEC60529)
Insulation resistance	20 MΩ min. between all terminals and the case (100 VDC M)
Dielectric strength	Leak current not to exceed 5 mA on application of 1000 VAC (50/60 Hz for 1 minute) between all terminals and the case
Vibration resistance	Frequency: 10 to 150 Hz; double amplitude: 0.20 mm; acceleration: 15 m/s2^2 for 8 minutes, 10 times each in X, Y, and Z directions
Shock resistance	Shock of 150 m/s^2 in X, Y, and Z directions, 3 times each for 18 repetitions
Casing material	ABS Stainless steel mount
Weight	Approx. 70 g
Cable length	2 m
Cable specification	3-mm-dia. coaxial cable

V640-HS62

● Dimensions



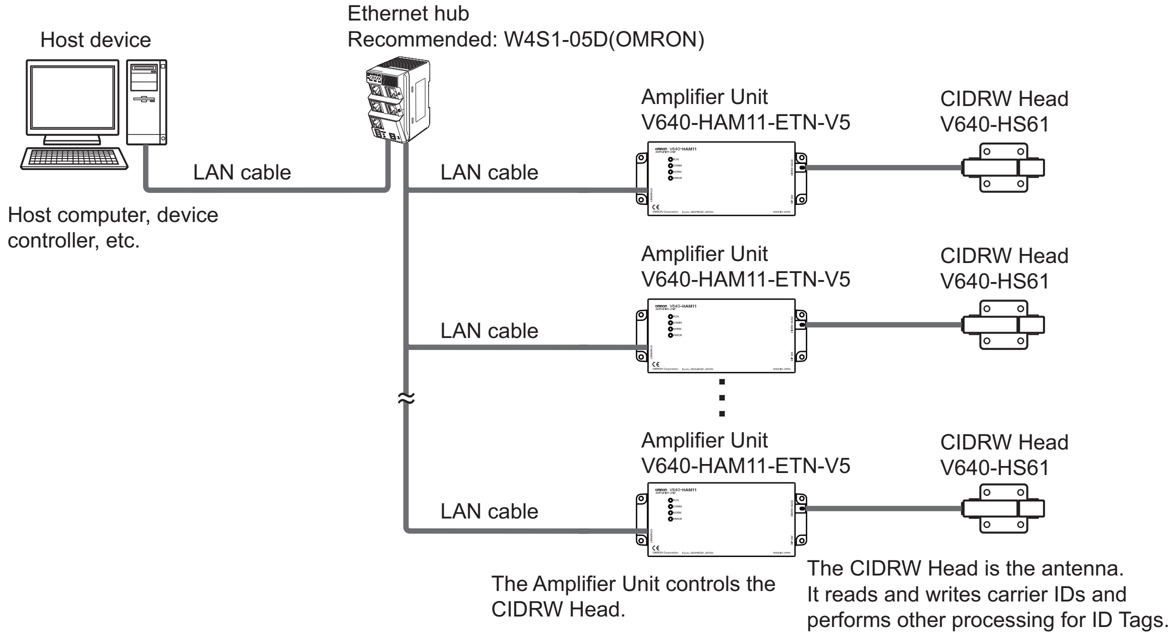
● Specifications

Item	Specifications
Transmission frequency	134 kHz
Ambient temperature	Operating: 0 to +40°C Storage: -15 to +65°C (with no icing)
Ambient humidity	Operating/Storage: 35% to 85% (with no condensation)
Degree of protection	IP20 (IEC60529)
Insulation resistance	20 MΩ min. between all terminals and the case (100 VDC M)
Dielectric strength	Leak current not to exceed 5 mA on application of 1000 VAC (50/60 Hz for 1 minute) between all terminals and the case
Vibration resistance	Frequency: 10 to 150 Hz; double amplitude: 0.20 mm; acceleration: 15 m/s^2 for 8 minutes, 10 times each in X, Y, and Z directions
Shock resistance	Shock of 150 m/s^2 in X, Y, and Z directions, 3 times each for 18 repetitions
Casing material	ABS Stainless steel mount
Weight	Approx. 100 g
Cable length	1.9 m
Cable specification	3-mm-dia. coaxial cable

A-2 Connection Examples

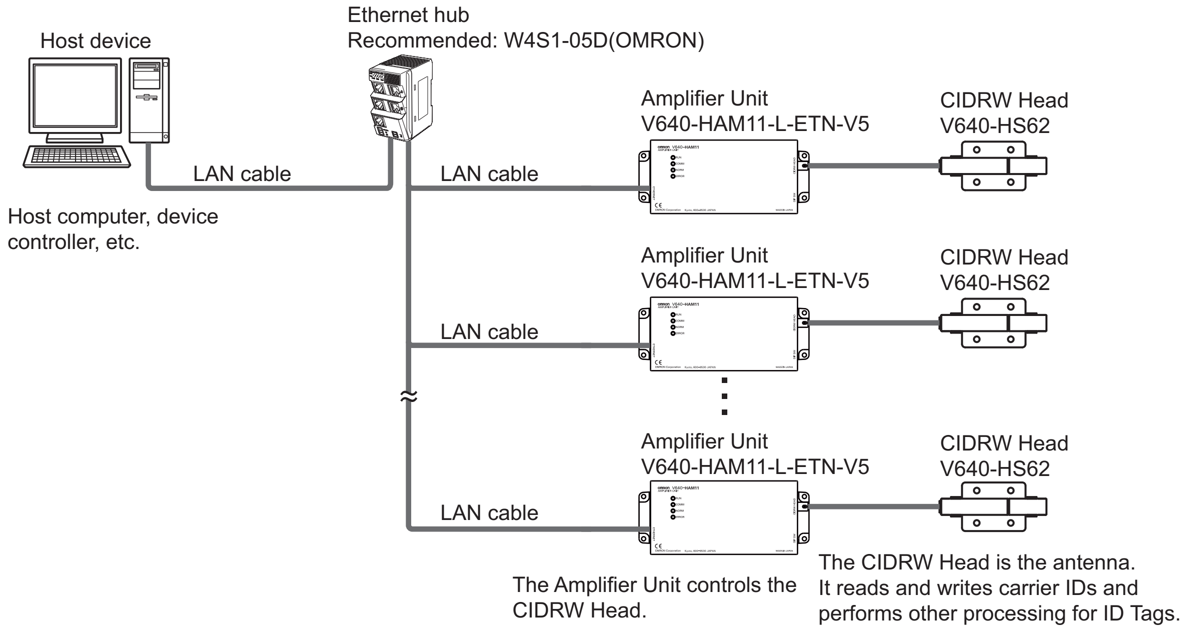
A-2-1 V640-HAM11-ETN-V5

Connect the host device and Amplifier Unit using a LAN cable.


Host device
Ethernet hub
Recommended: W4S1-05D(OMRON)
Amplifier Unit
V640-HAM11-ETN-V5
CIDRW Head
V640-HS61
LAN cable
LAN cable
Host computer, device controller, etc.
Amplifier Unit
V640-HAM11-ETN-V5
CIDRW Head
V640-HS61
LAN cable
Amplifier Unit
V640-HAM11-ETN-V5
CIDRW Head
V640-HS61
LAN cable
The Amplifier Unit controls the CIDRW Head.
The CIDRW Head is the antenna. It reads and writes carrier IDs and performs other processing for ID Tags.

A-2-2 V640-HAM11-L-ETN-V5

Connect the host device and Amplifier Unit using a LAN cable.



A-3 Characteristic Data According to Conditions of Use

A-3-1 Maps of Communications Areas (Reference Only)

The figures given below for communications areas (communications distances) are reference values only.

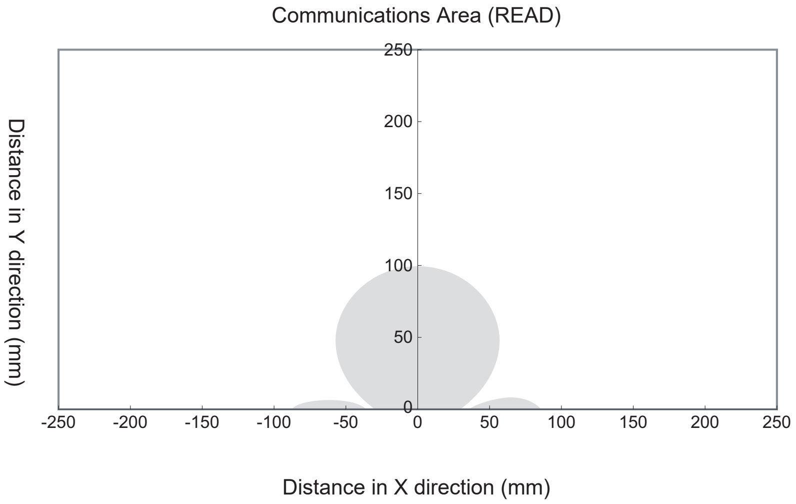
The maps of communications areas will vary according to the ID Tags that you use, the background metals, the ambient noise, the effects of temperature and so on, and should be thoroughly confirmed on installation.

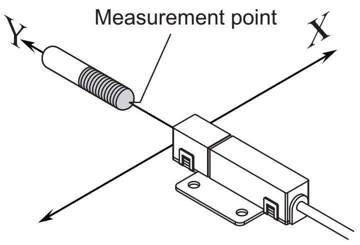
The direction of the ID Tags will affect communications performance. Check the direction of the coils in the ID Tags before using the ID Tags.

V640-HAM11-ETN-V5

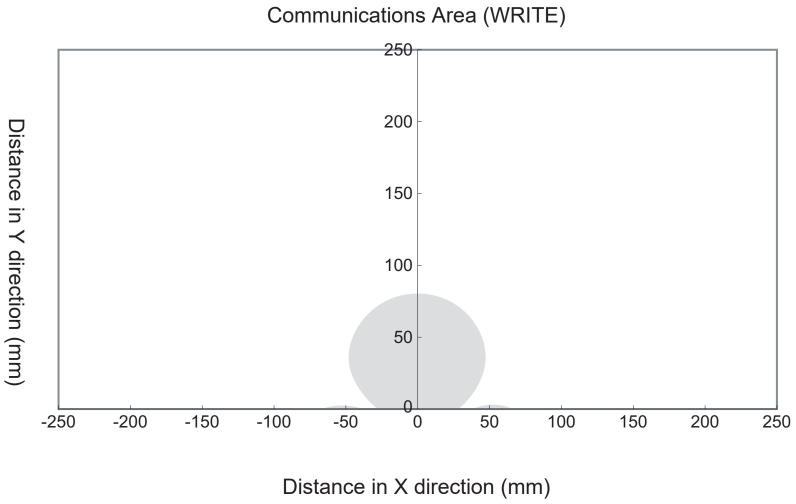
● Coaxial Mounting (RI-TRP-DR2B-40)

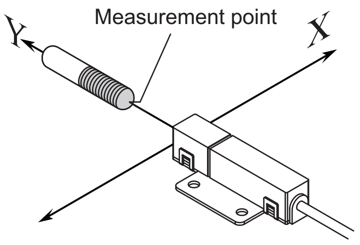
・**READ**





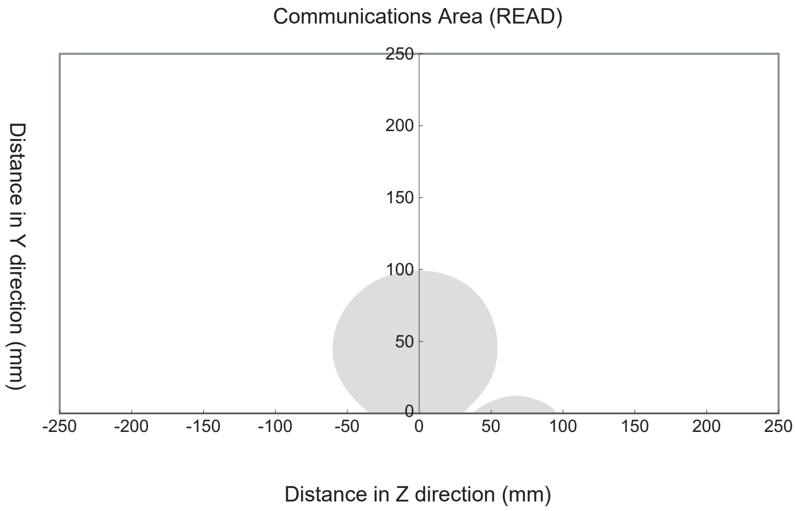
・**WRITE**

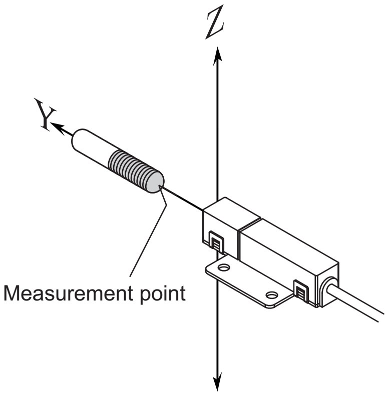




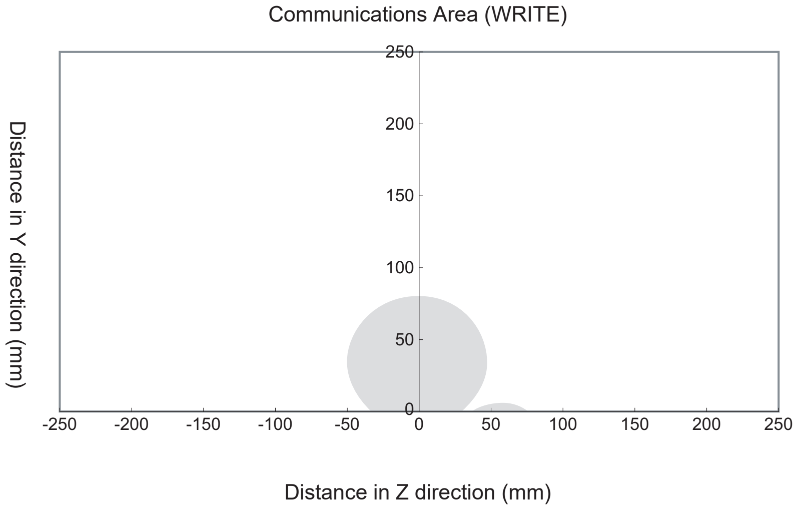
● Coaxial Mounting (RI-TRP-DR2B-40)

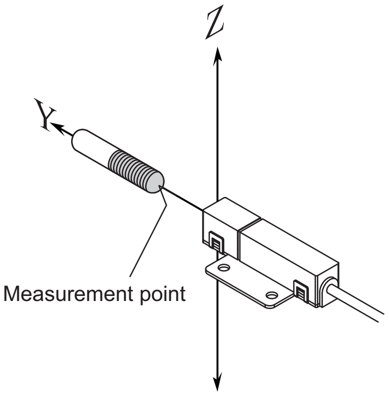
・READ





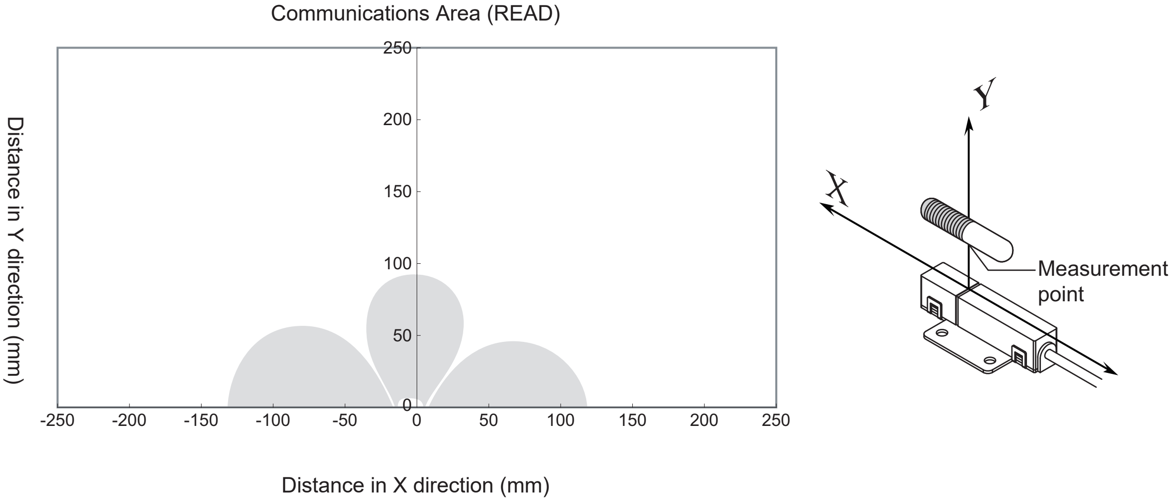
・WRITE



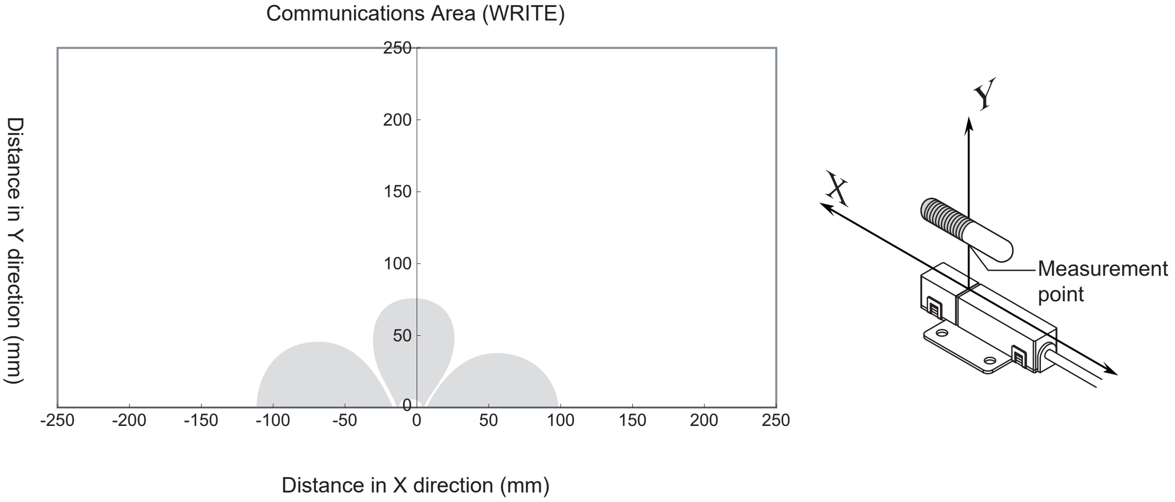


● Parallel Mounting (RI-TRP-DR2B-40)

・READ

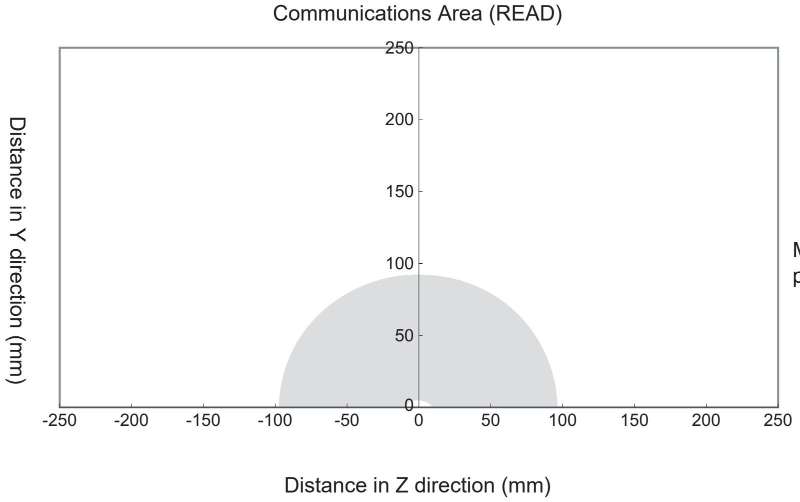


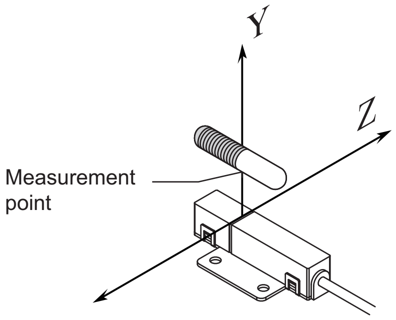
・WRITE



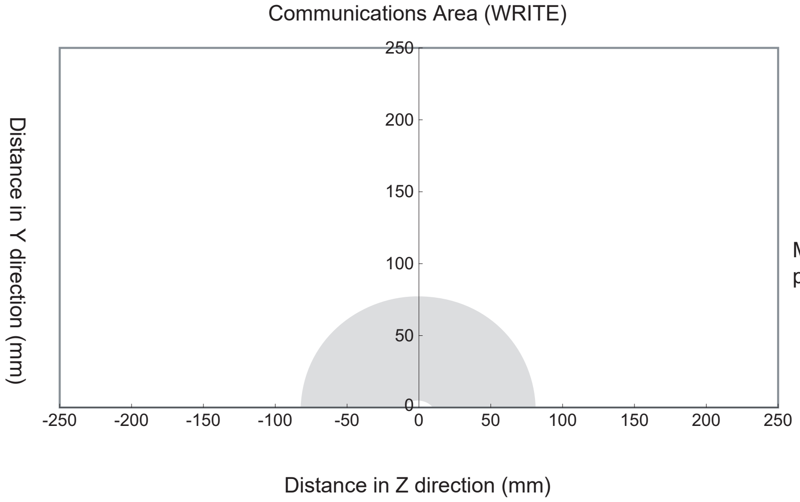
● Parallel Mounting (RI-TRP-DR2B-40)

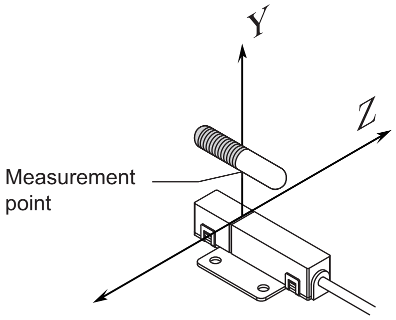
・READ





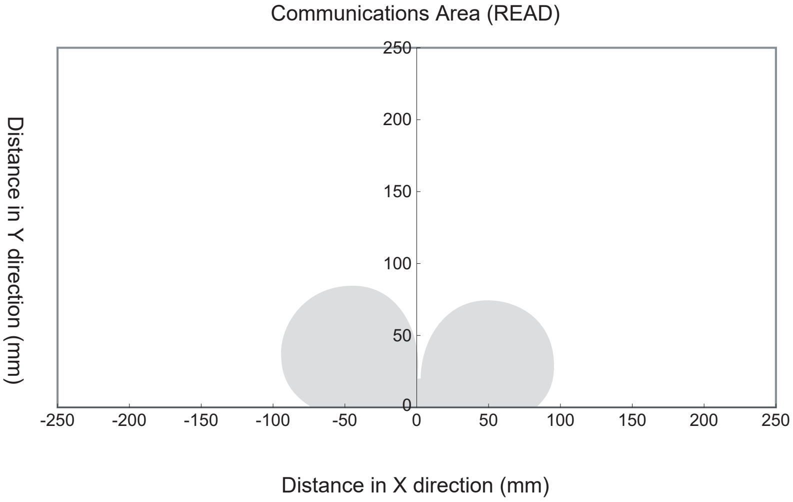
・WRITE

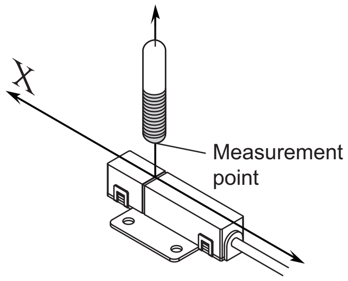




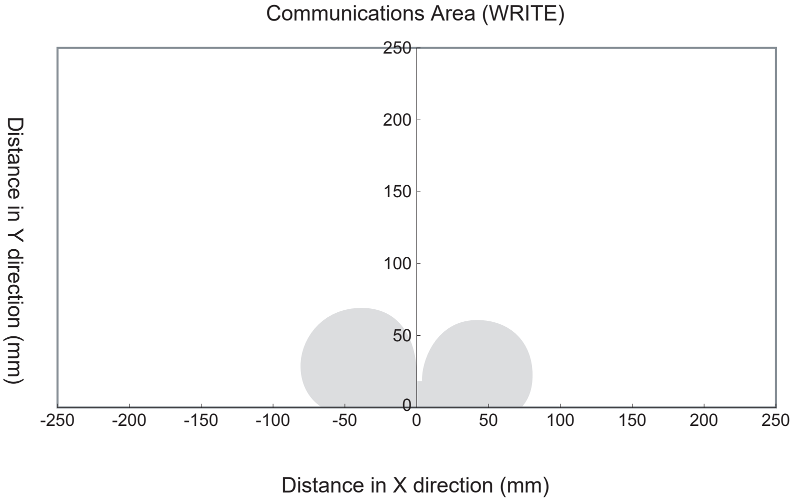
● Vertical Mounting (RI-TRP-DR2B-40)

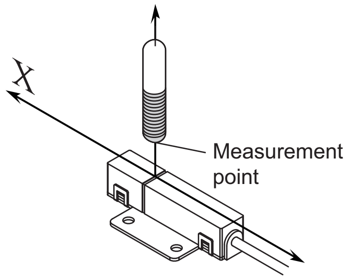
・READ





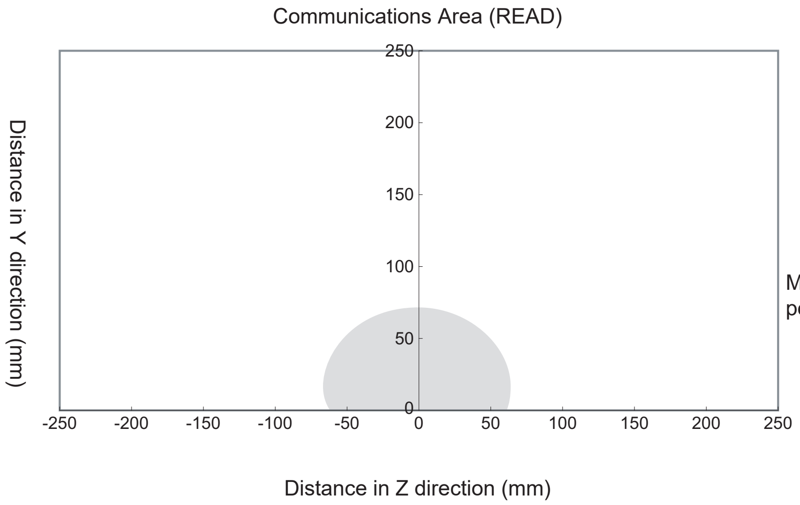
・WRITE

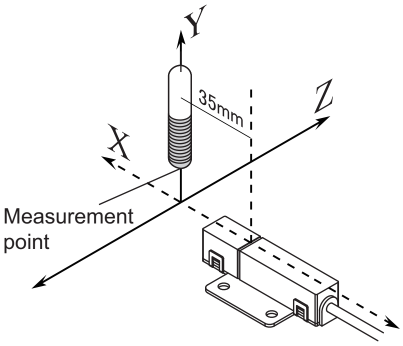




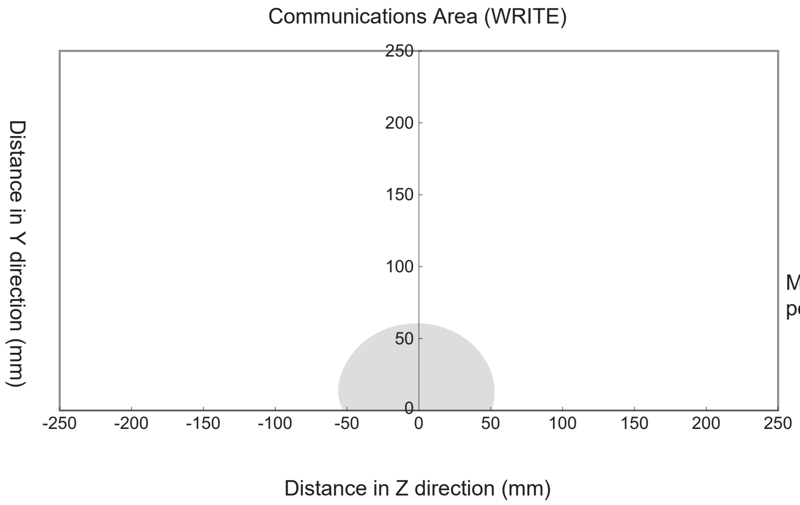
● Vertical Mounting (RI-TRP-DR2B-40)

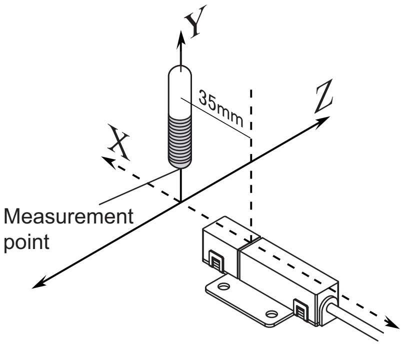
・READ





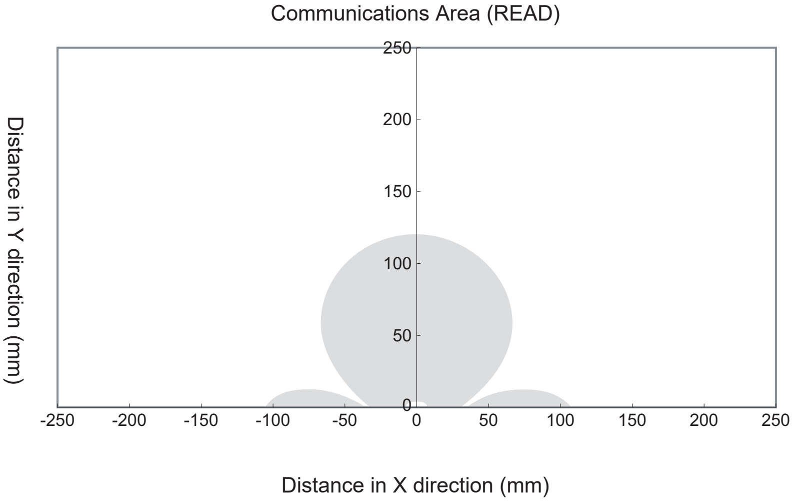
・WRITE

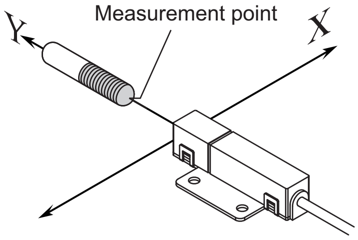




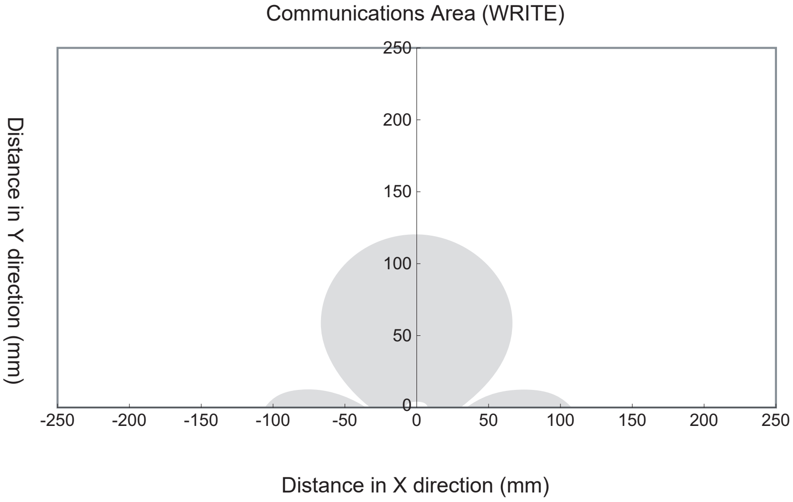
● Coaxial Mounting (RI-TRP-WR2B)

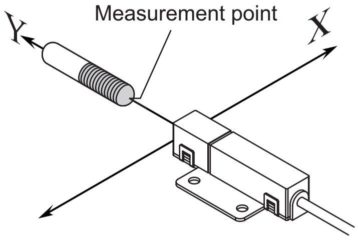
・READ





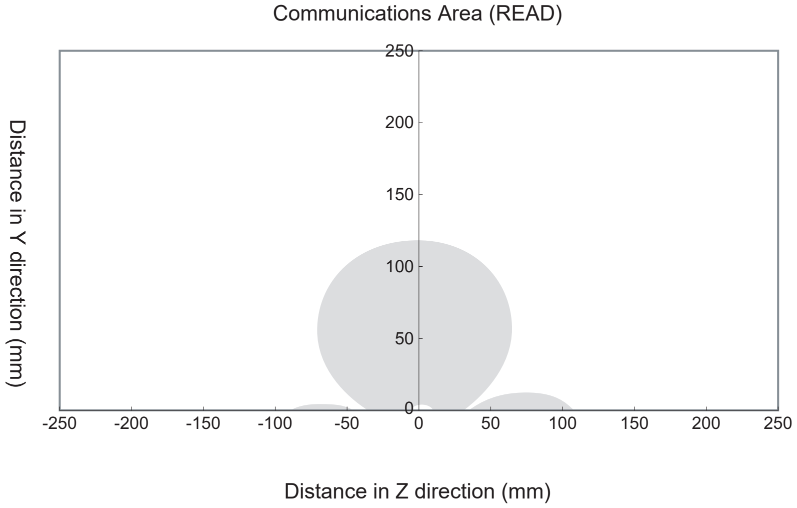
・WRITE

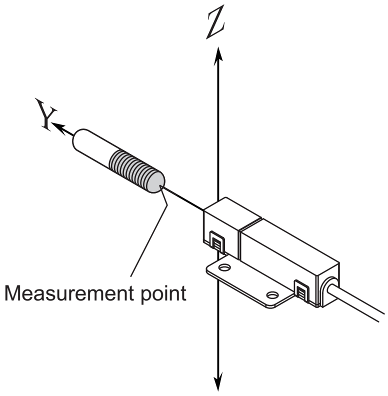




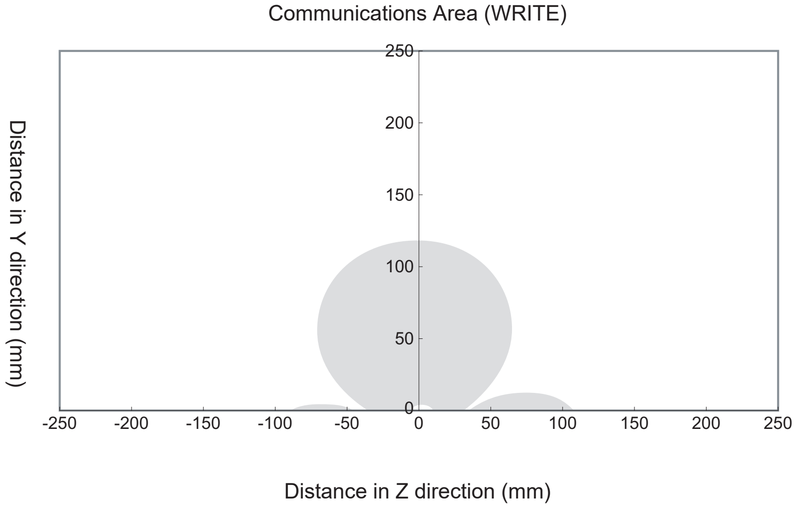
● Coaxial Mounting (RI-TRP-WR2B)

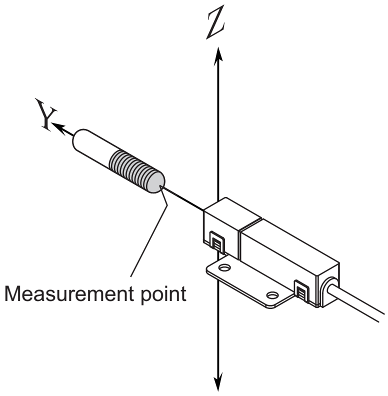
・READ





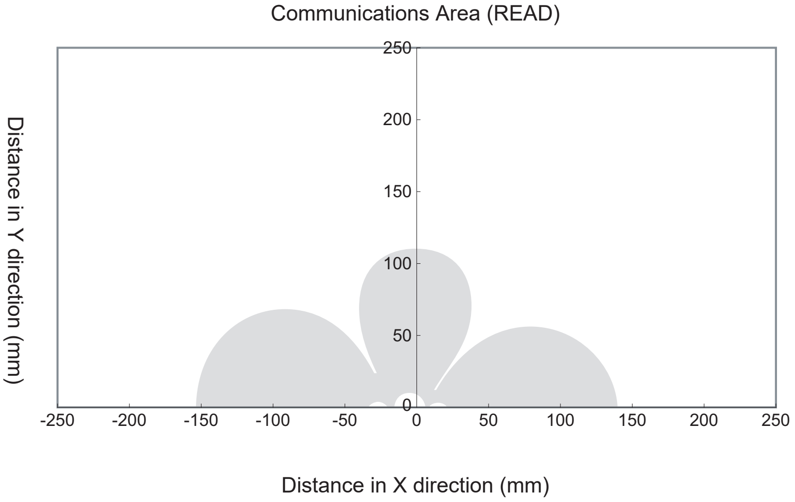
・WRITE

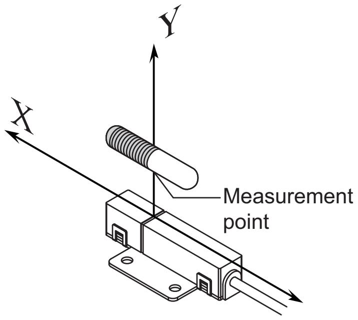




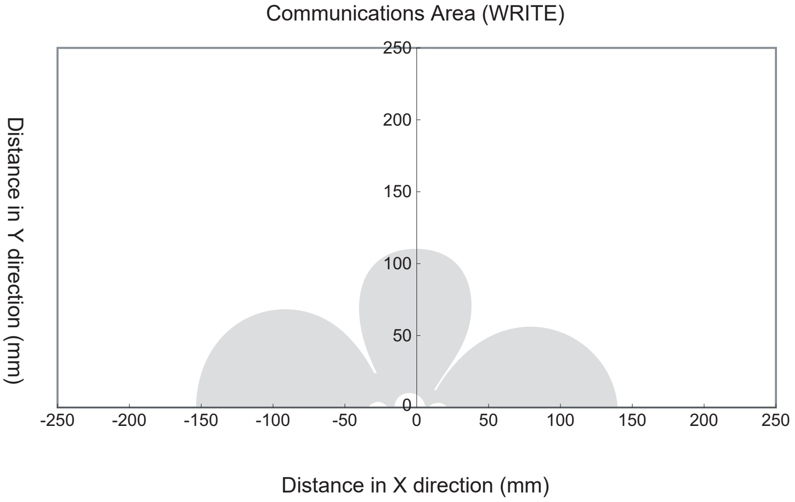
● Parallel Mounting (RI-TRP-WR2B)

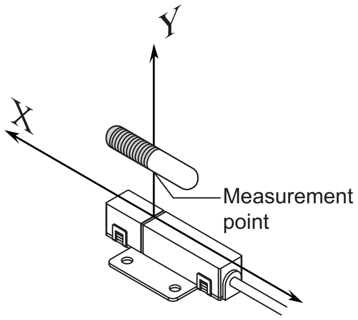
・READ





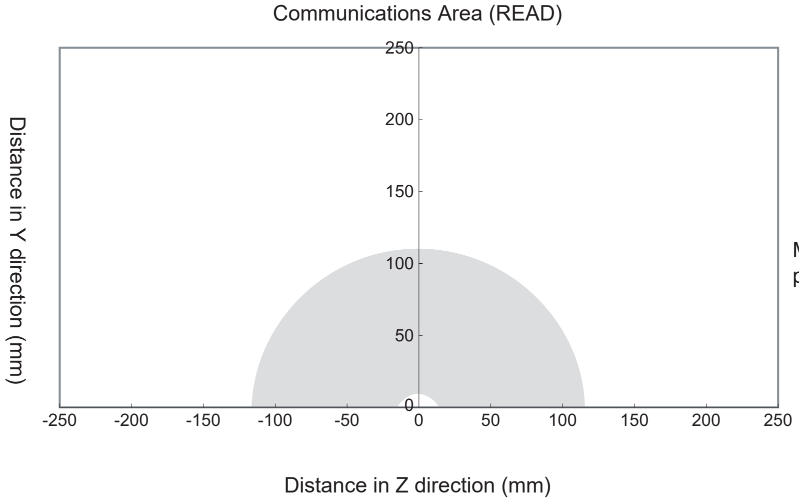
・WRITE

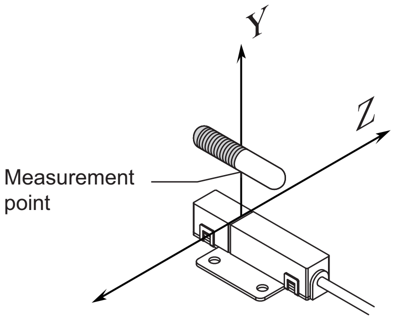




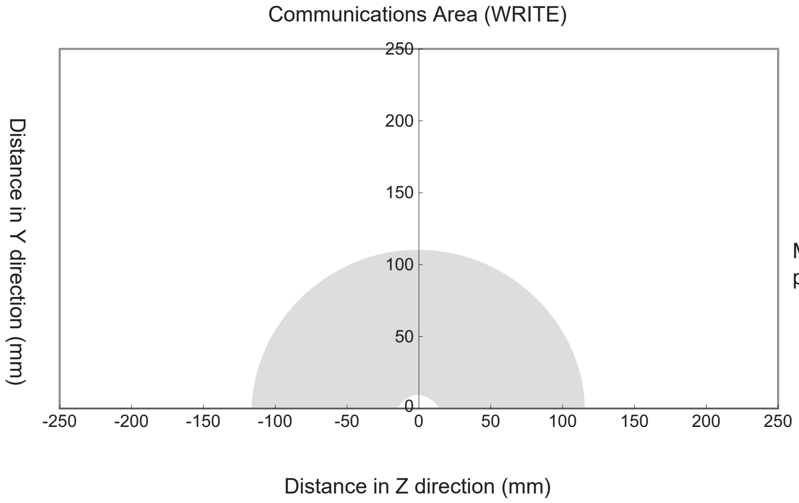
● Parallel Mounting (RI-TRP-WR2B)

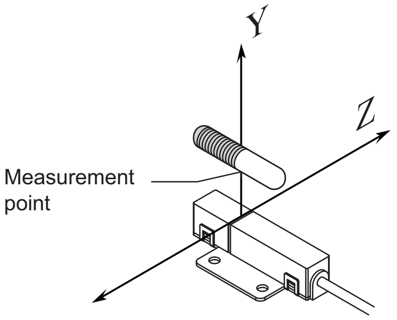
・READ





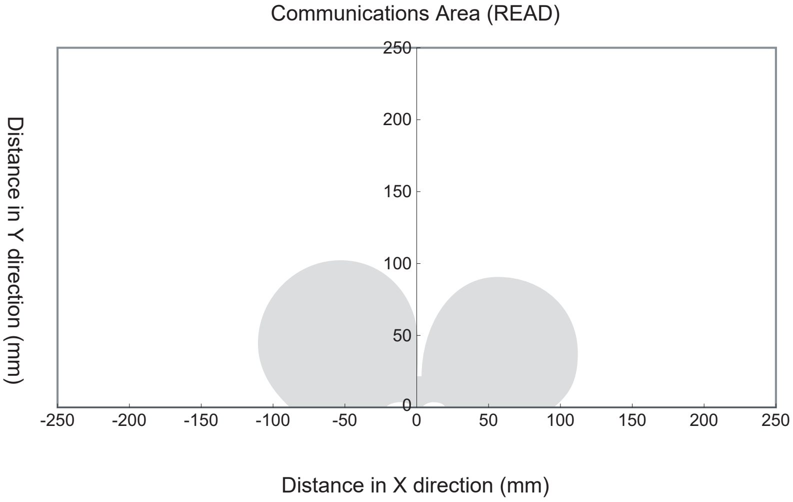
・WRITE

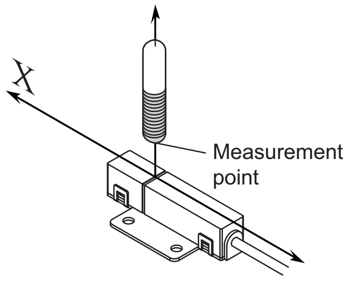




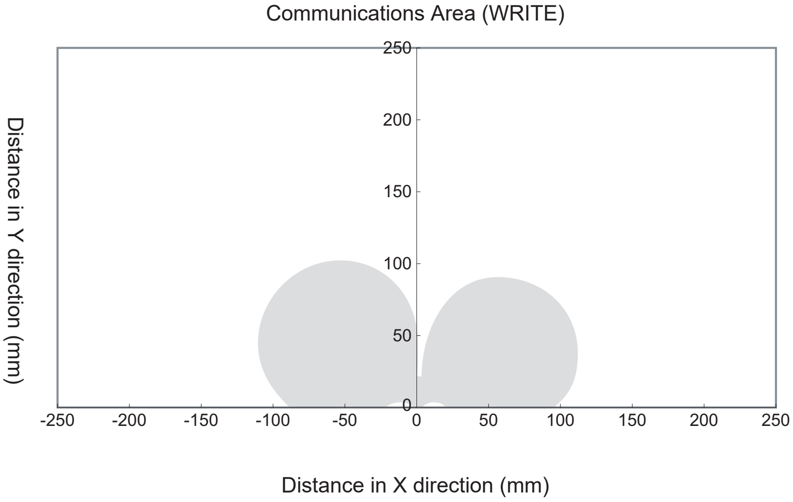
● Vertical Mounting (RI-TRP-WR2B)

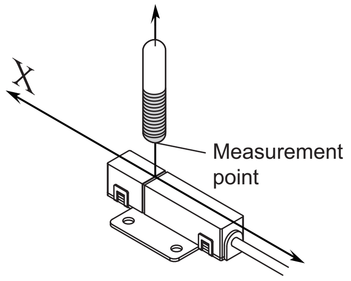
・READ





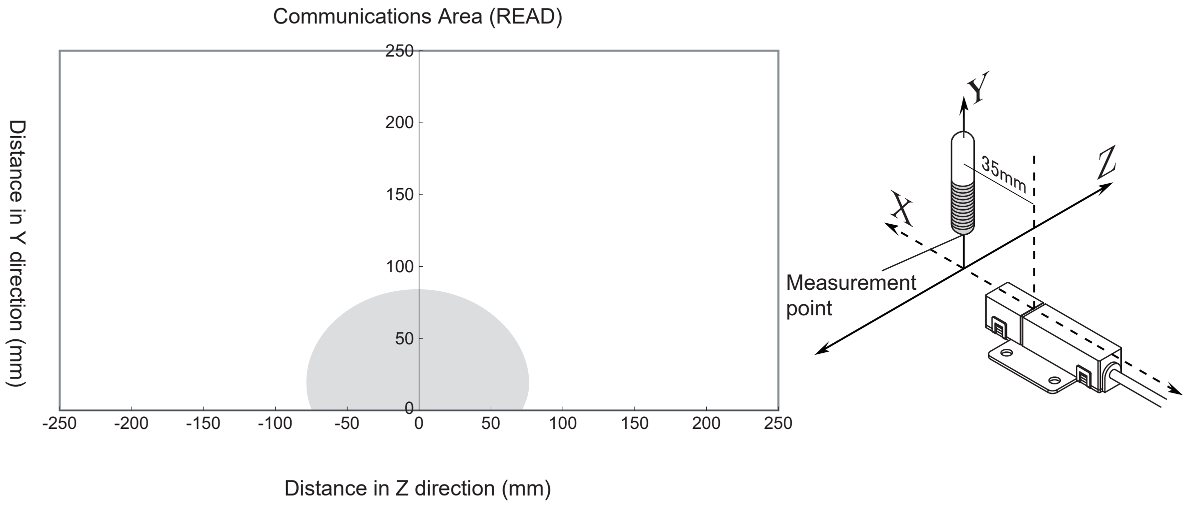
・WRITE



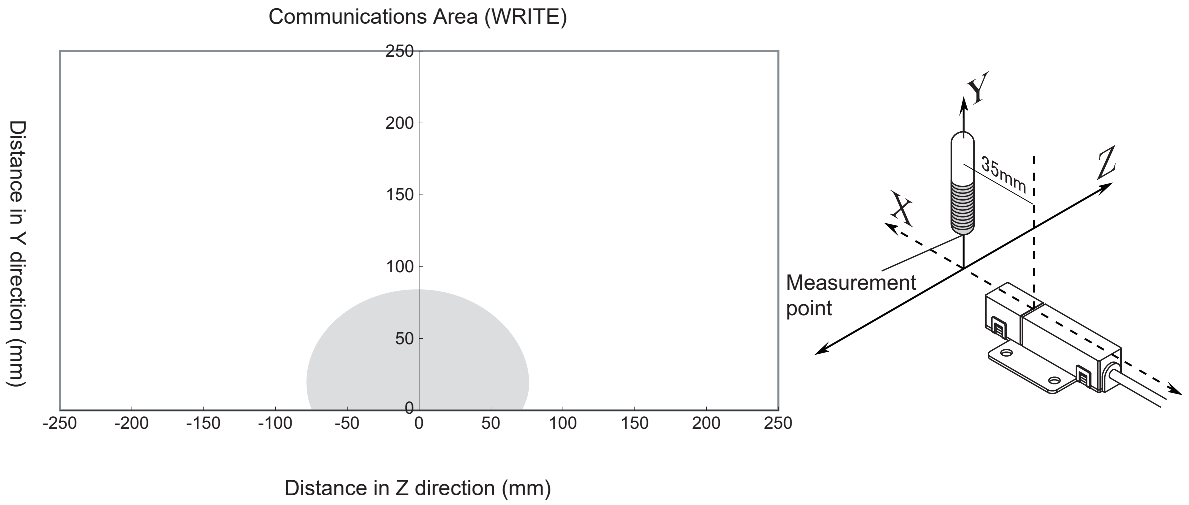


● Vertical Mounting (RI-TRP-WR2B)

・READ



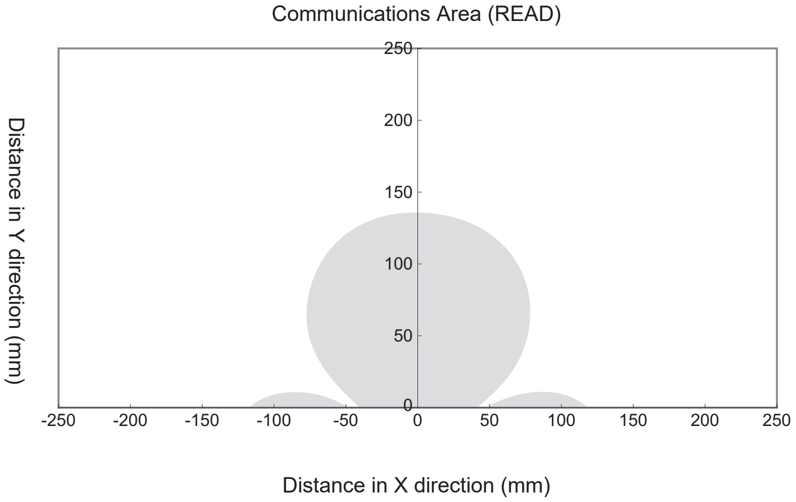
・WRITE

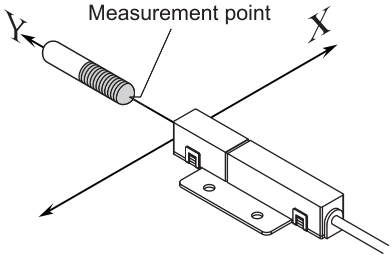


V640-HAM11-L-ETN-V5

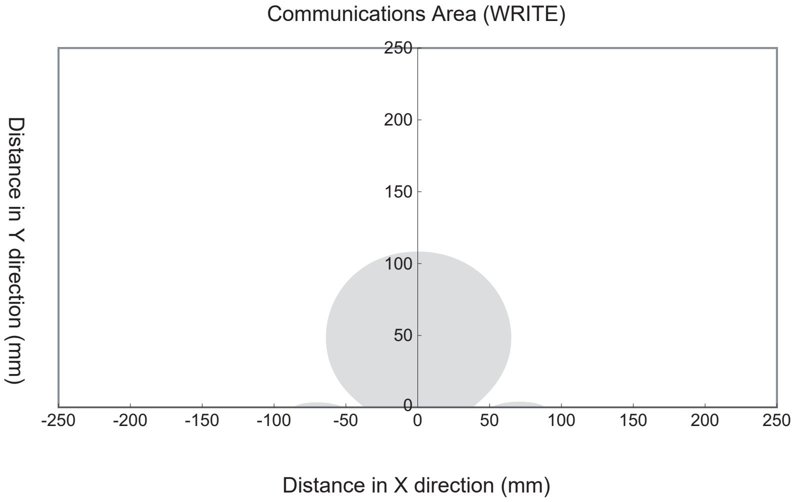
● Coaxial Mounting (RI-TRP-DR2B-40)

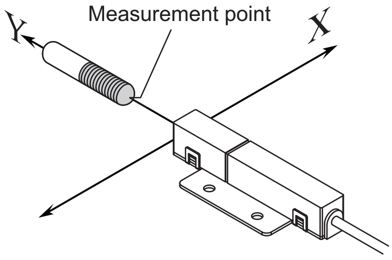
・**READ**





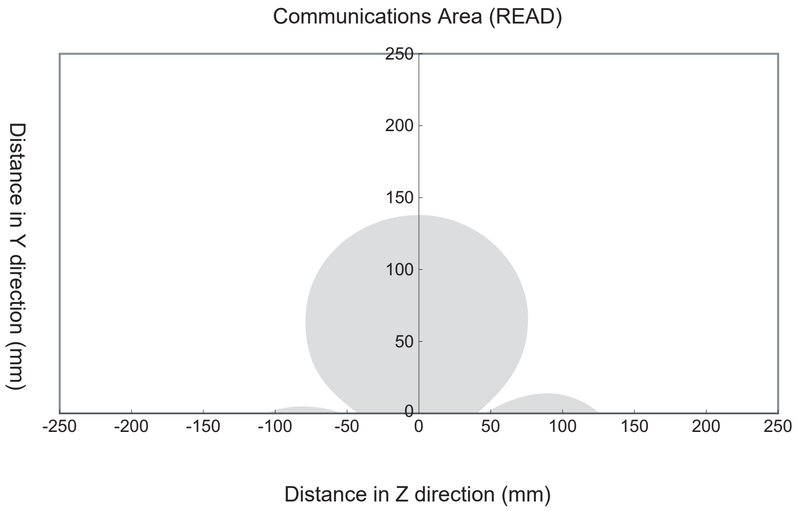
・**WRITE**

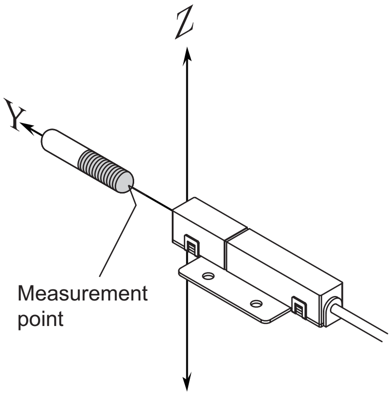




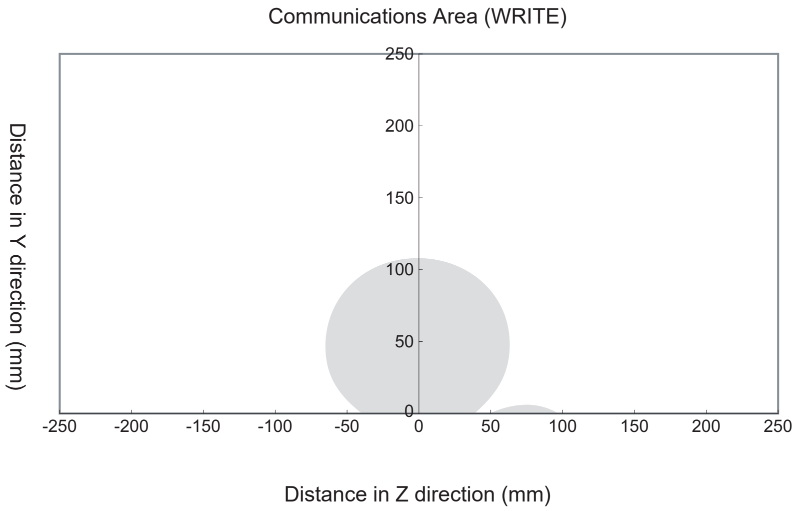
● Coaxial Mounting (RI-TRP-DR2B-40)

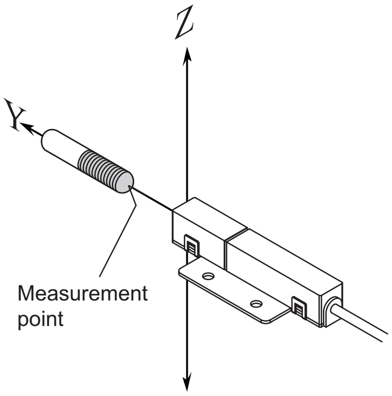
・READ





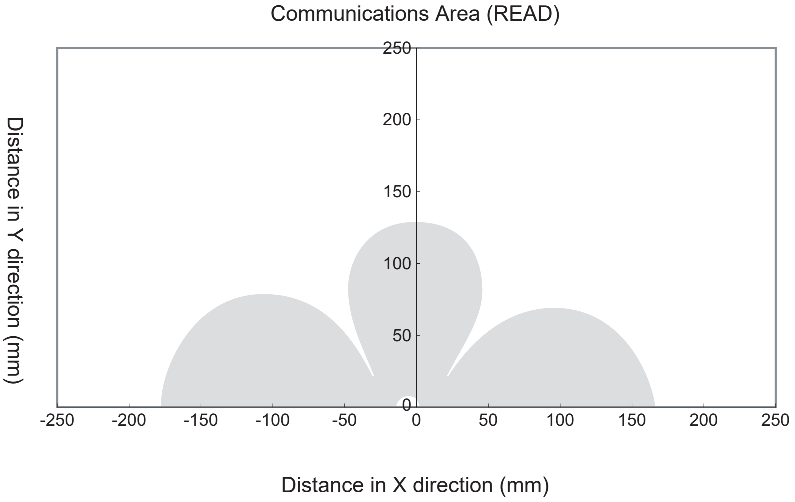
・WRITE

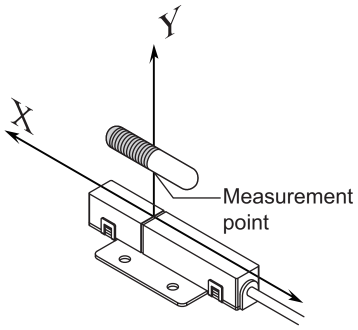




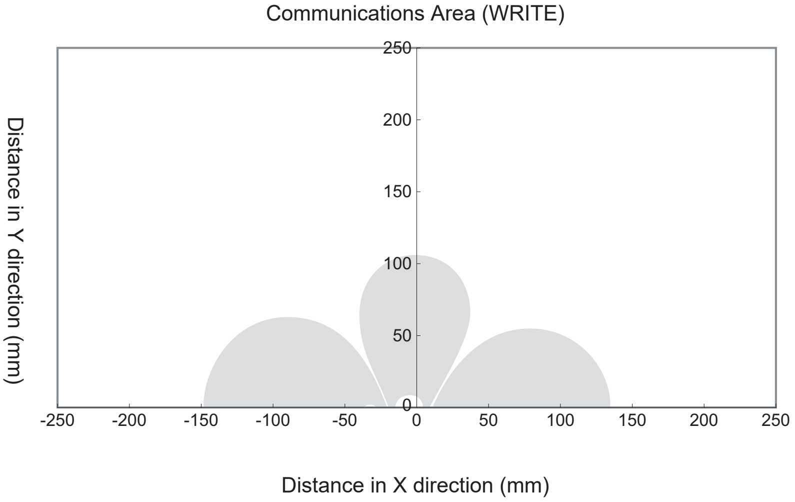
● Parallel Mounting (RI-TRP-DR2B-40)

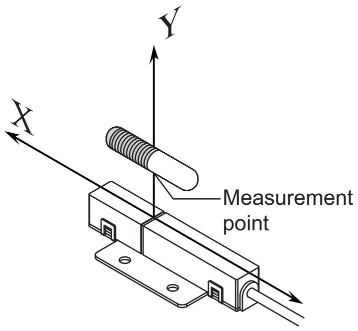
・READ





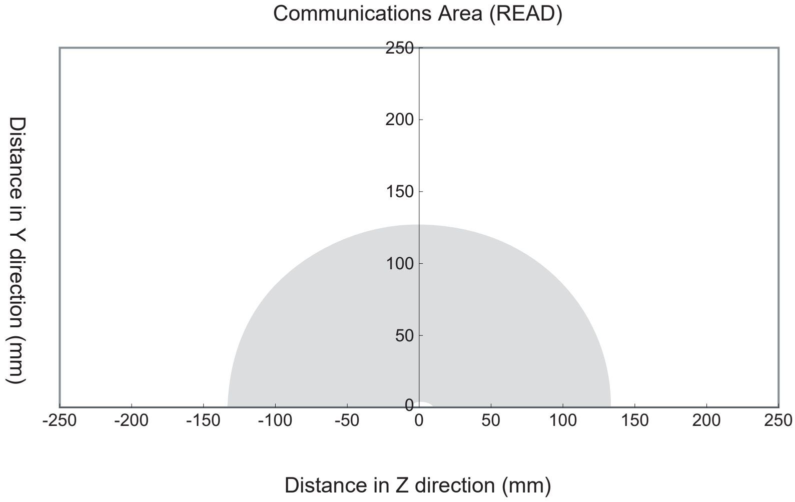
・WRITE

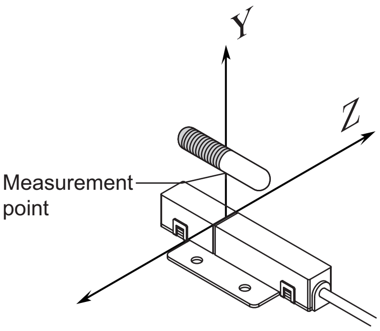




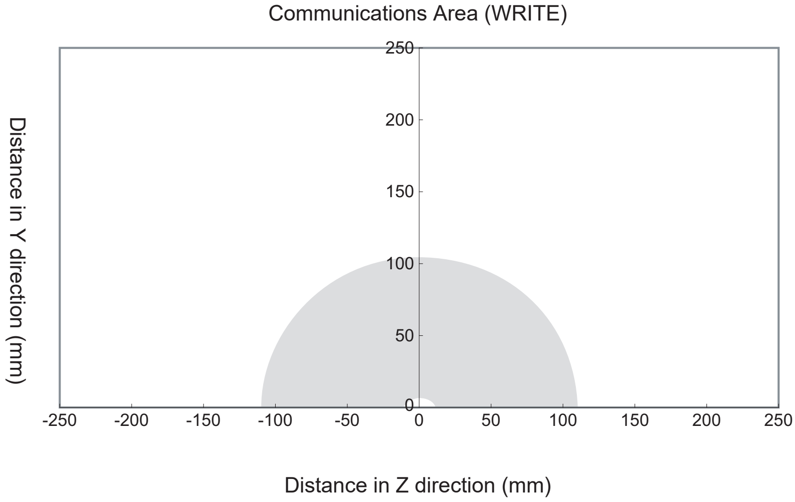
● Parallel Mounting (RI-TRP-DR2B-40)

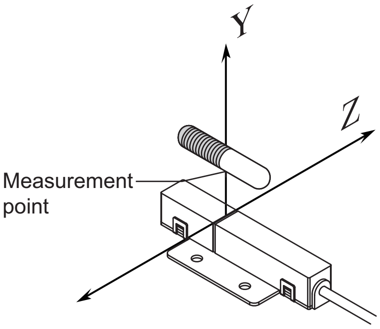
・READ





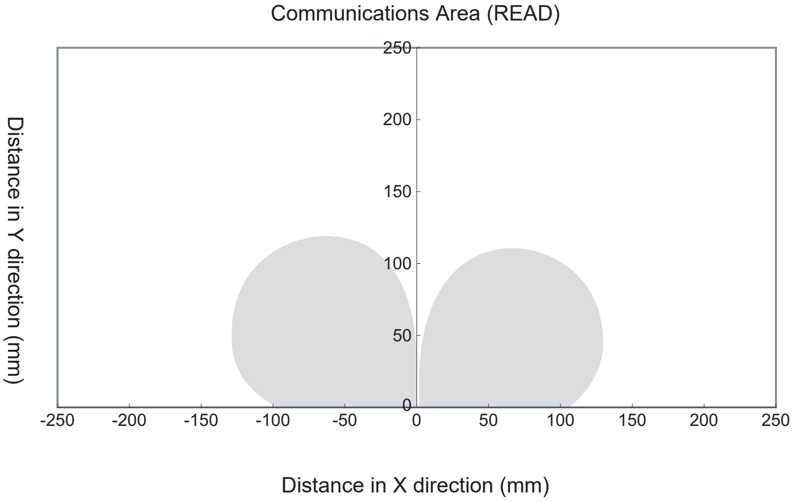
・ WRITE

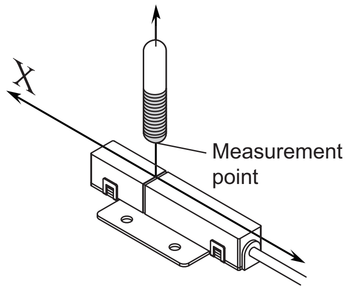




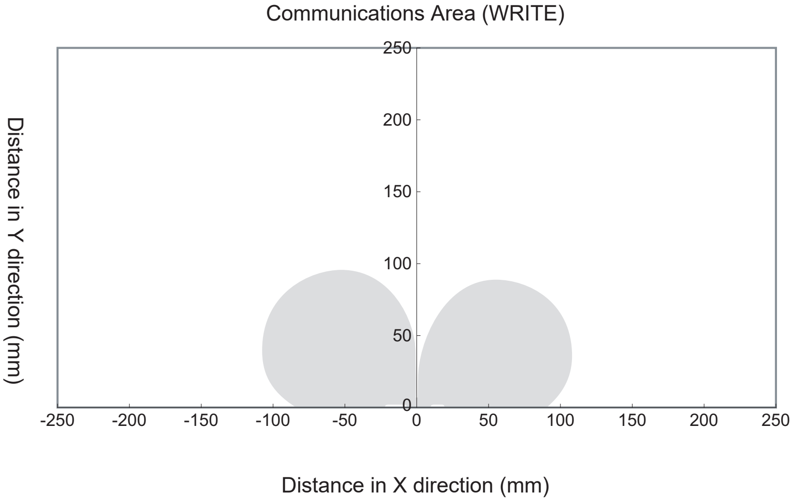
● Vertical Mounting (RI-TRP-DR2B-40)

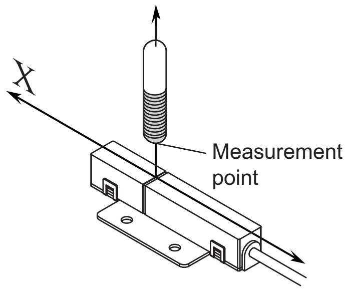
・READ





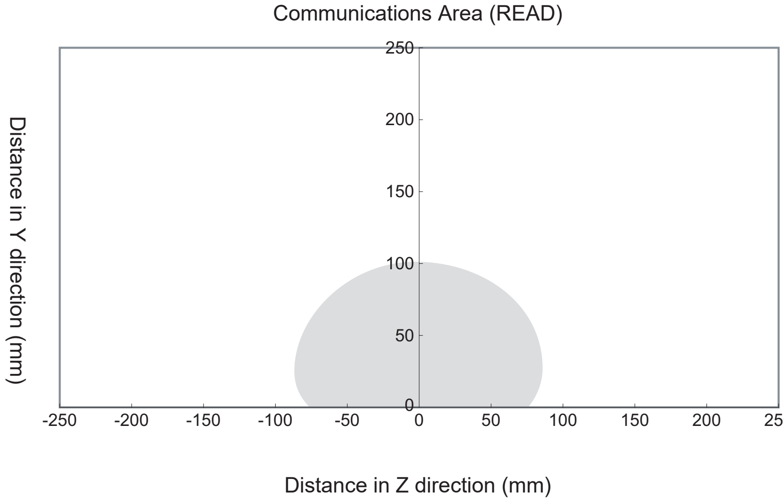
・WRITE

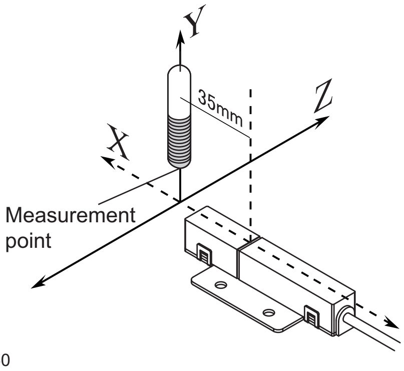




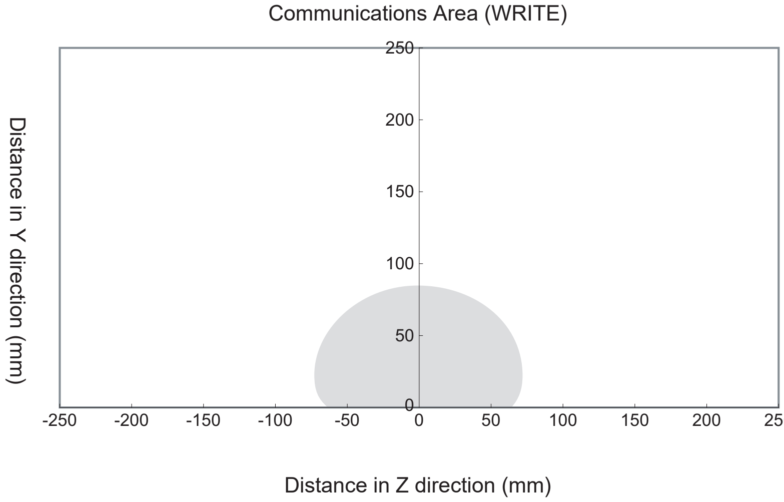
● Vertical Mounting (RI-TRP-DR2B-40)

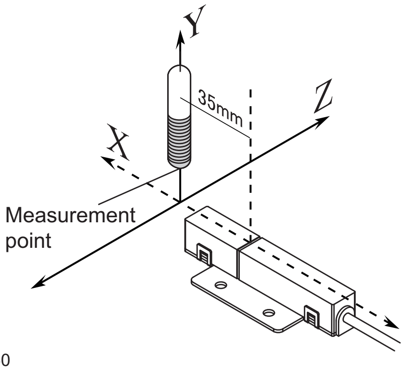
・READ





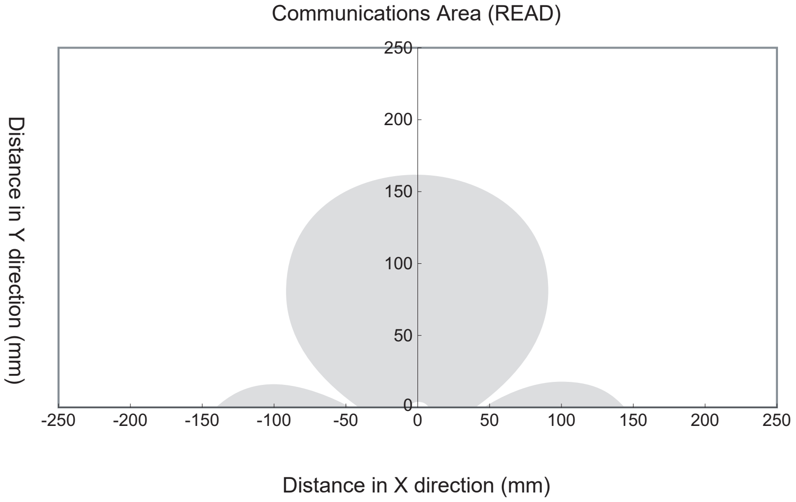
・WRITE

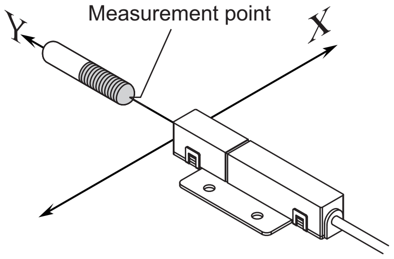




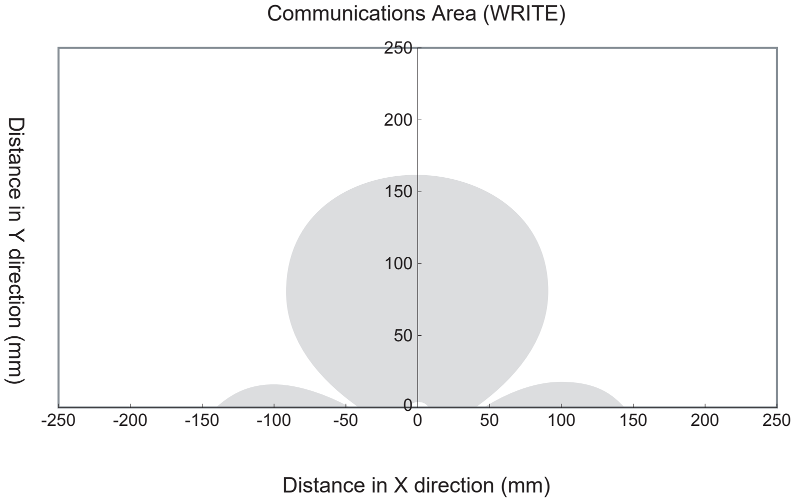
● Coaxial Mounting (RI-TRP-WR2B)

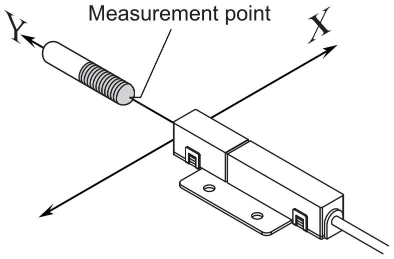
・READ





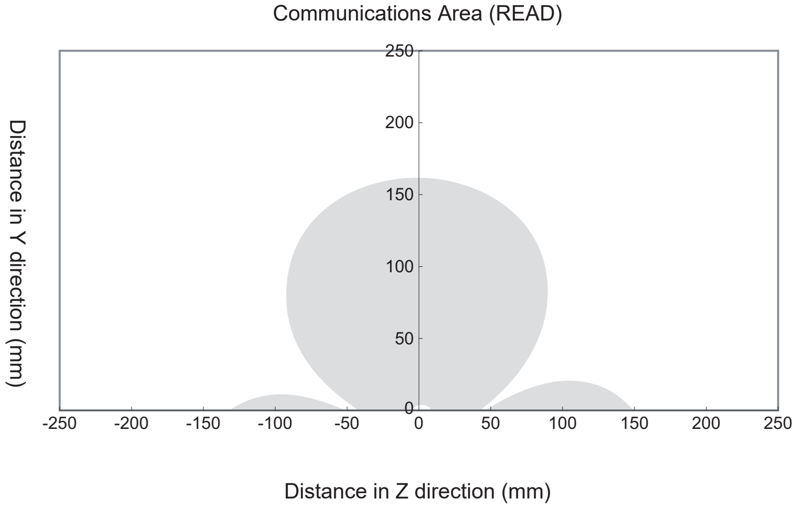
・WRITE

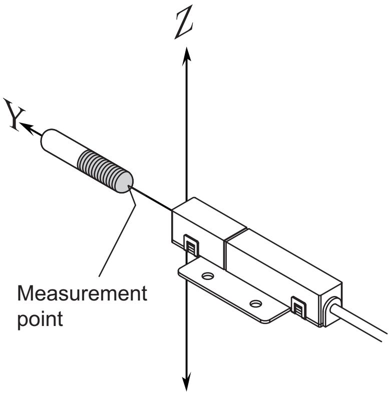




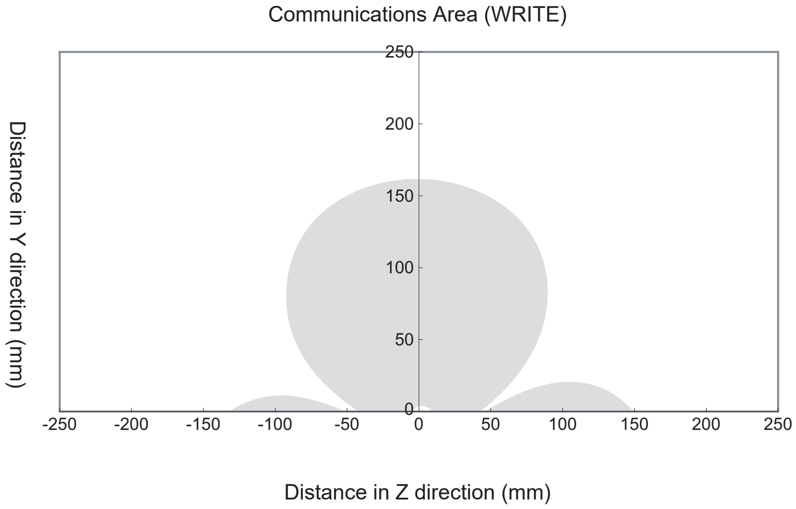
● Coaxial Mounting (RI-TRP-WR2B)

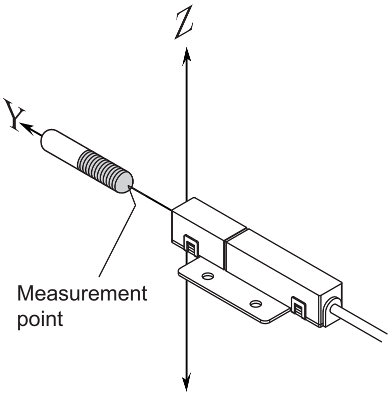
・READ





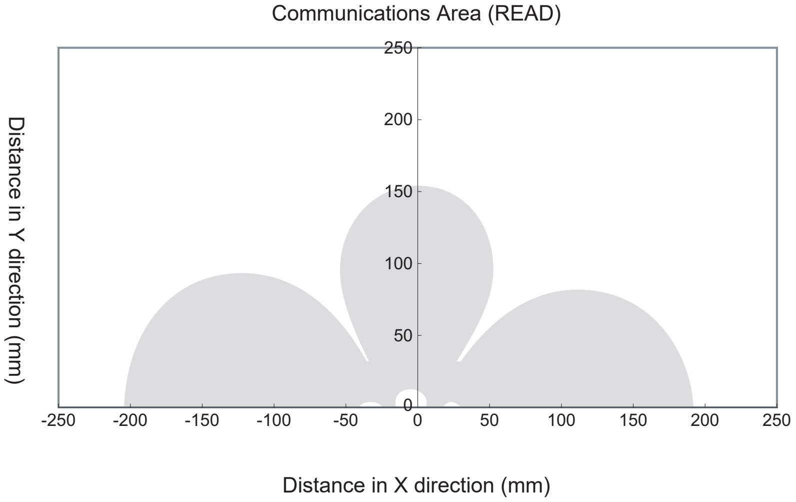
・WRITE

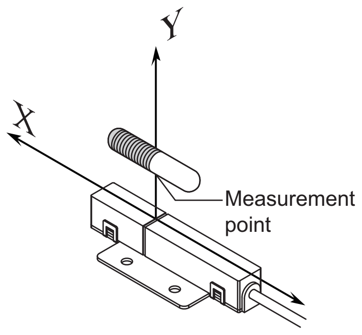




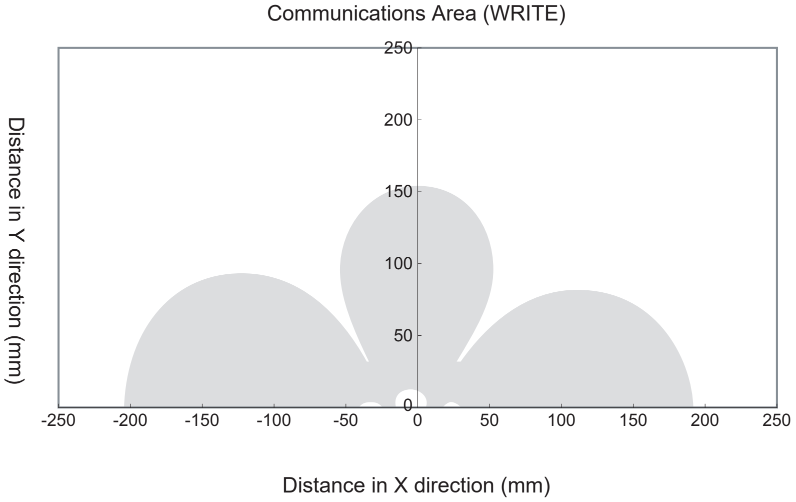
● Parallel Mounting (RI-TRP-WR2B)

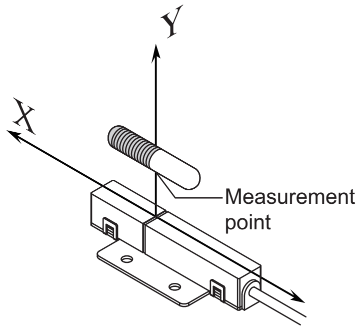
・READ





・WRITE

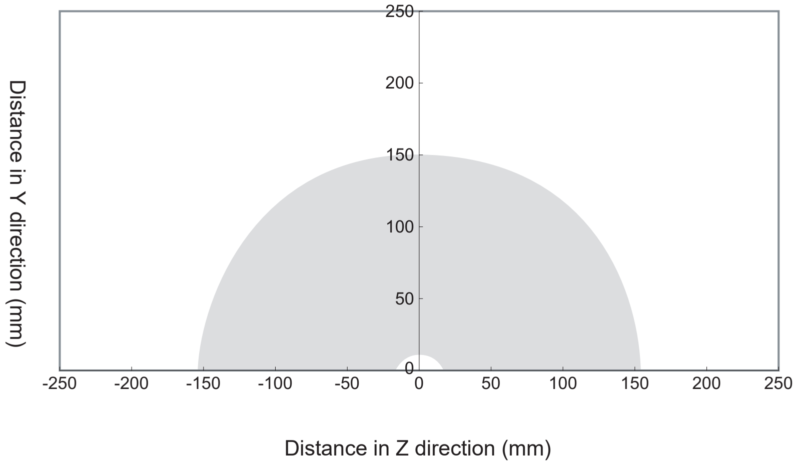


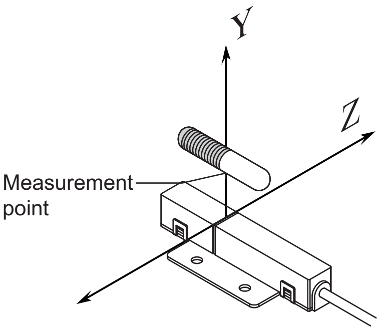


● Parallel Mounting (RI-TRP-WR2B)

・READ

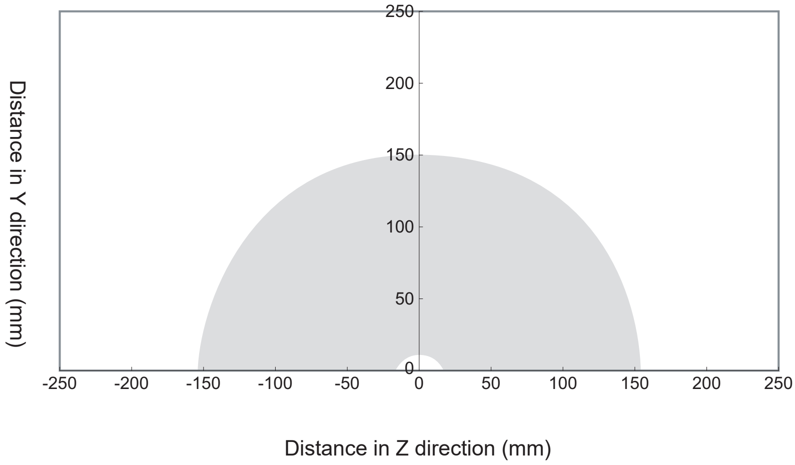
Communications Area (READ)

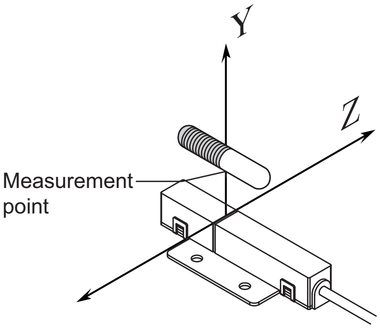




・WRITE

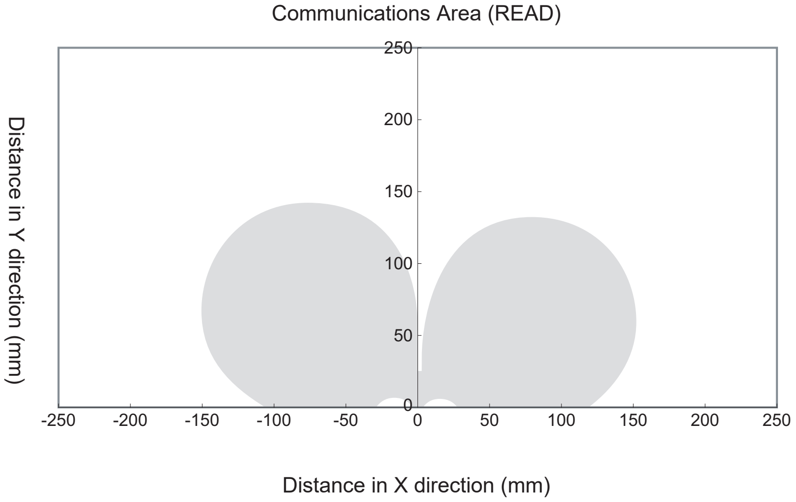
Communications Area (WRITE)

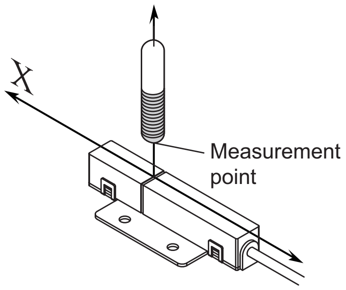




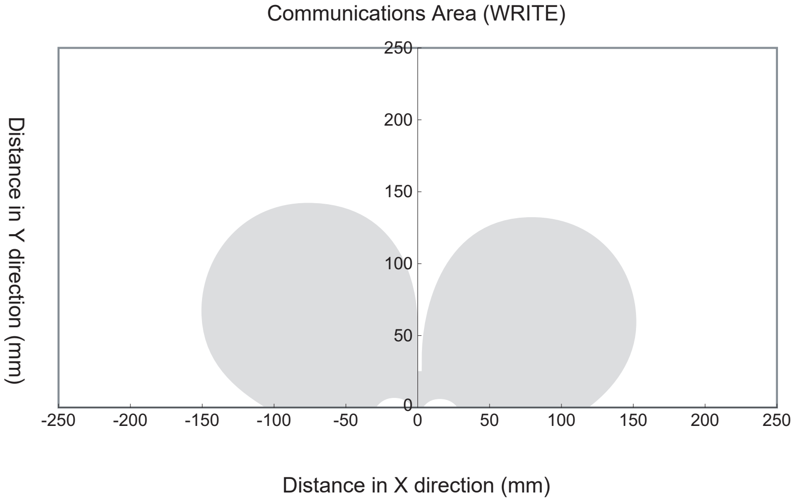
● Vertical Mounting (RI-TRP-WR2B)

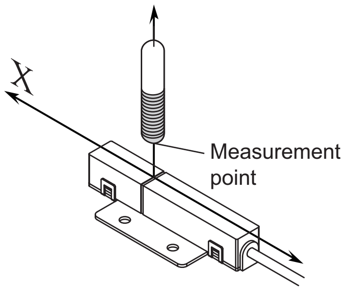
・READ





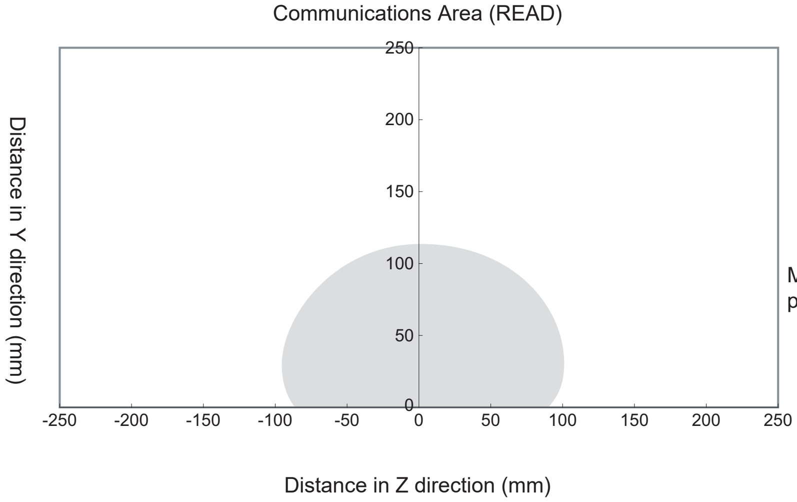
・WRITE

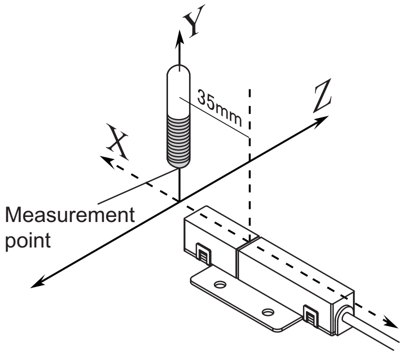




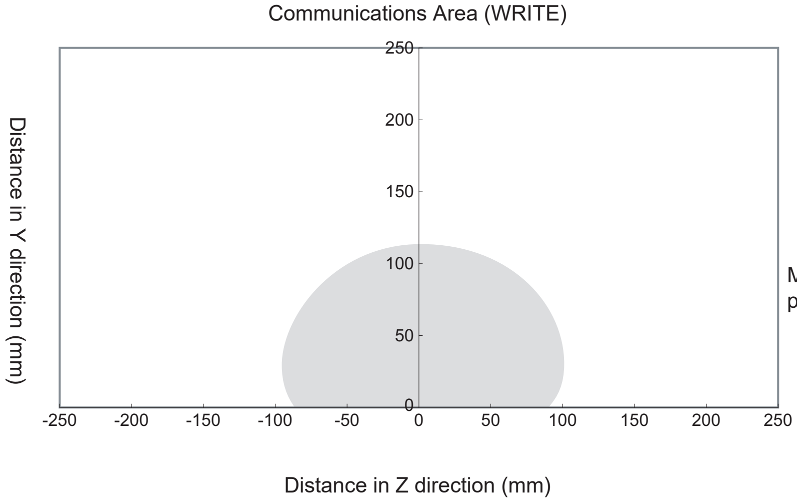
● Vertical Mounting (RI-TRP-WR2B)

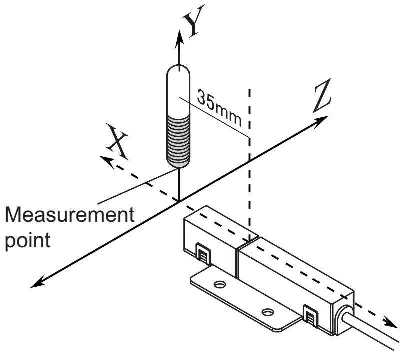
・READ





・WRITE





A-3-2 Mutual Interference Distances (Reference Only)

● When amplifier units are connected using multidrop connections and multiple CIDRW Heads are used

The CIDRW Heads will not process commands simultaneously. In this case, install the CIDRW Heads at least 0.1 m apart from each other.

● When the CIDRW Systems are installed close to each other

Distance between Antennas and Changes in Communications Distances (Reference Only)

- **V640-HS61**

Distance between Antennas	Change in communications distance
1,000 mm	100%
900 mm	100%
800 mm	100%
700 mm	99%
600 mm	90%
500 mm	74%
400 mm	55%
300 mm	40%
200 mm	15%

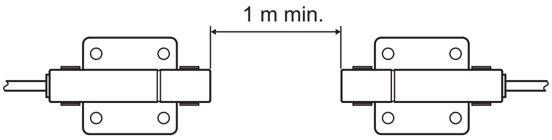
- **V640-HS62**

Distance between Antennas	Change in communications distance
2,000 mm	99%
1,600 mm	99%
1,400 mm	95%
1,200 mm	84%
1,000 mm	68%
800 mm	53%
600 mm	34%
400 mm	15%
200 mm	0%

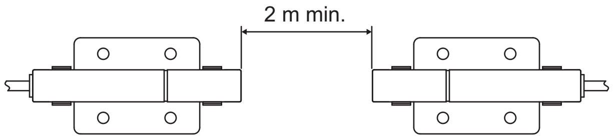
If CIDRW Heads in separate CIDRW systems process commands simultaneously, mutual interference between the Heads can result in malfunctions. If this is a problem, install the CIDRW Heads separated at least by the distances shown in the following illustrations.

- **For Coaxial Installation**

V640-HS61

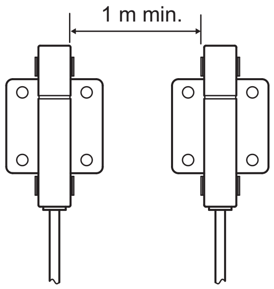


V640-HS62

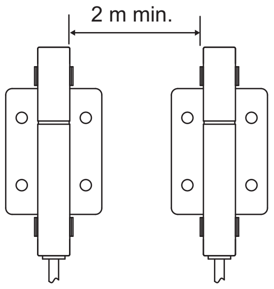


- **For Parallel Installation**

V640-HS61

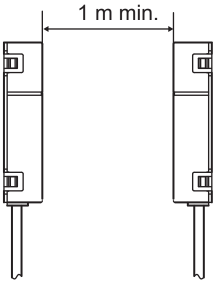


V640-HS62

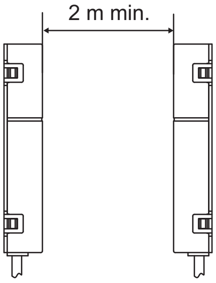


・ For Face-to-Face Installation

V640-HS61

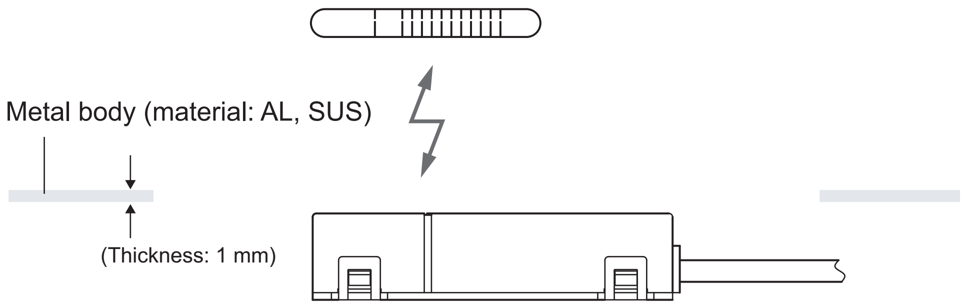


V640-HS62



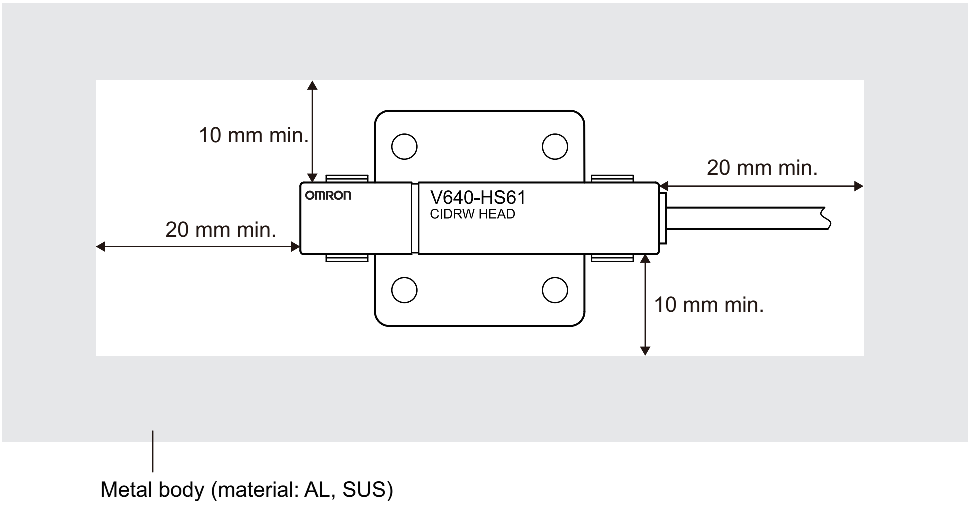
A-3-3 Influence of Background Metals (Reference Only)

The CIDRW Head can also communicate from an opening in a ceiling panel (metal body).

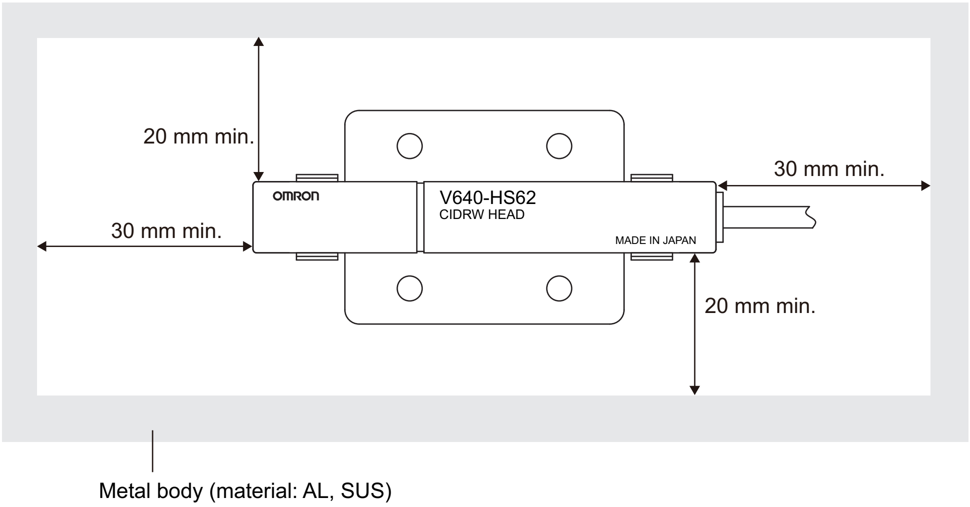


However, ensure the distances indicated below between the CIDRW Head and the metal body. If you do not ensure these distances the communications distance will be substantially shortened.

- **V640-HS61**

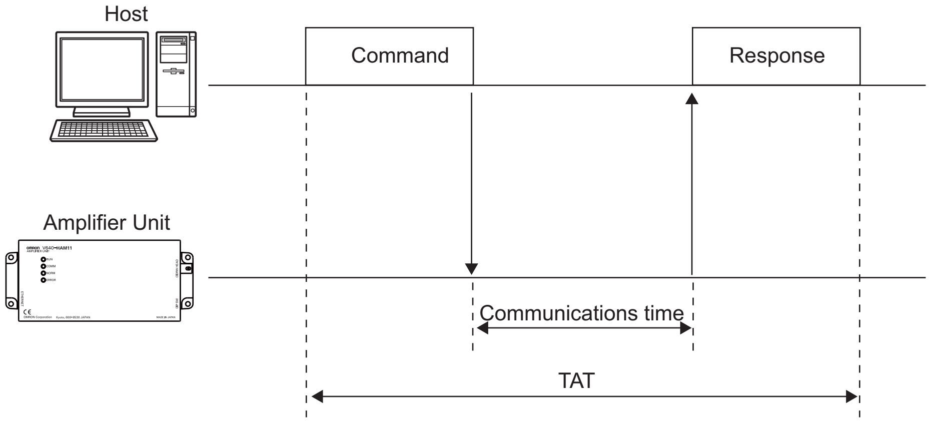


- **V640-HS62**



A-3-4 Communications Time

Take the time required for processing between the host device and Amplifier Units into account when designing the system.



Time	Description
Communications time	This is the time required for communications between an ID Tag and the CIDRW Head.
TAT	This is the time required for processing at the Amplifier Unit, seen from the host device.

Communications time calculation formula (unit: ms)

READ: 138.7 x (number of pages) + 10.0

WRITE, SAME WRITE: 379.8 x (number of pages) + 145.4

BYTE WRITE: 383.0 x (number of pages/8) + 249.0

* The result of underlined portion "number of pages/8" is rounded up.

TAT calculation formula (units: ms)

TAT = command and response transmission time + communications time

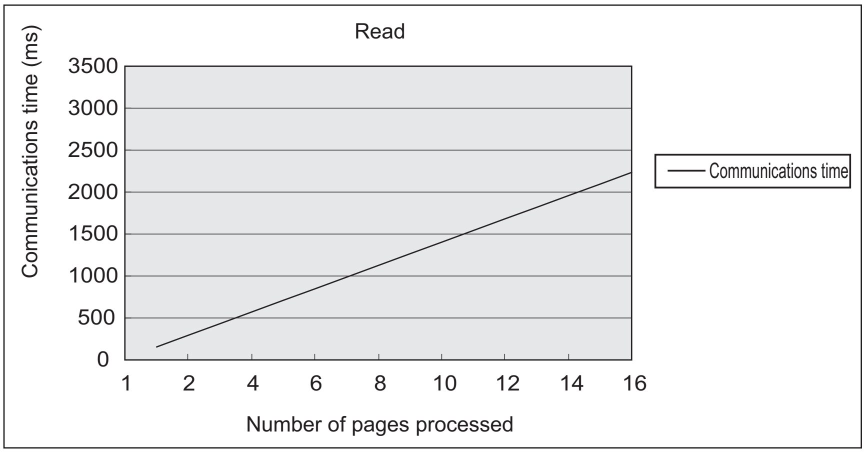
*The command and response transmission time differs depending on the network environment.

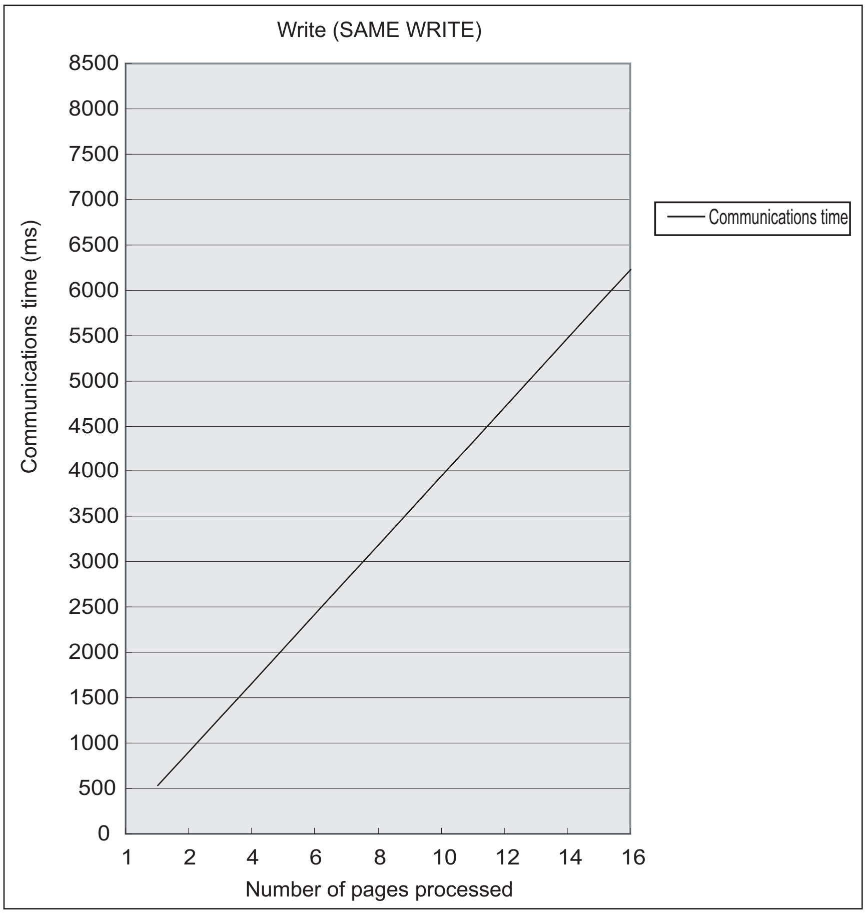
Additional Information

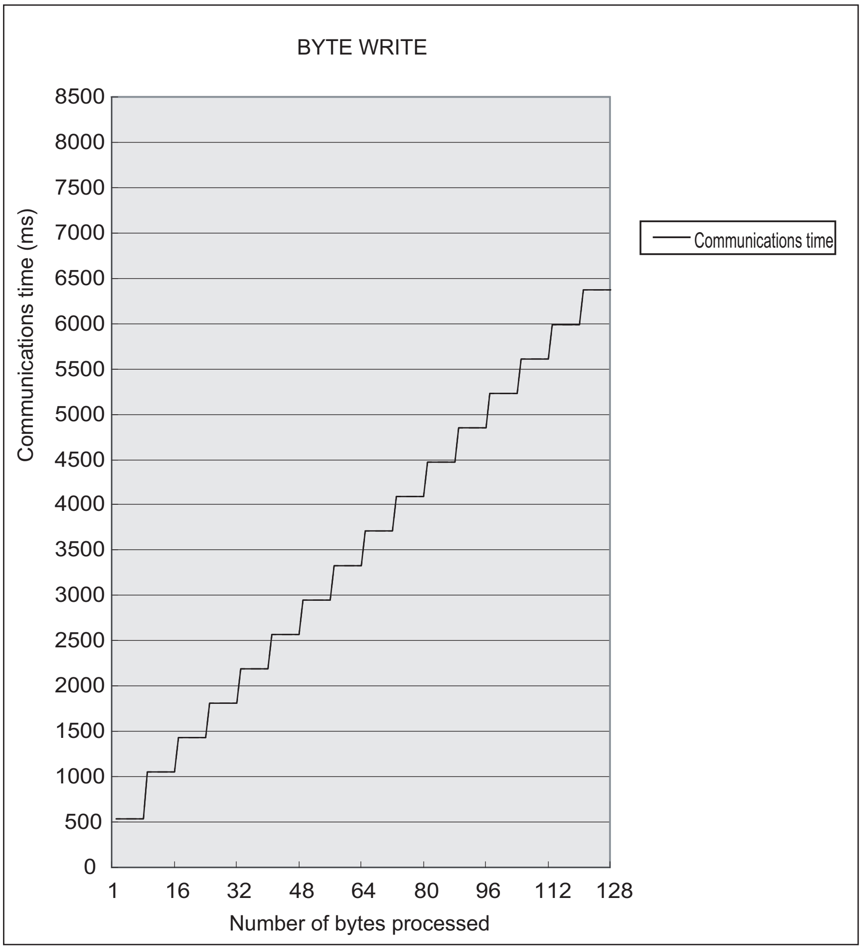
For example:
Command and response transemission time is about from 10 to 40 msec, when connect between PC and the Amplifier Unit directly by the lan cable(100M).

The graph for communications time for communications between the ID Tag and CIDRW Head, and TAT (when the baud rate is 9600 bps), is shown below.

The communications time and TAT, however, may increase substantially according to the conditions of use.







Additional Information

Please confirm beforehand, there is a difference in comparision with V640-HAM11-ETN and V640-HAM11-L-ETN in communication time.

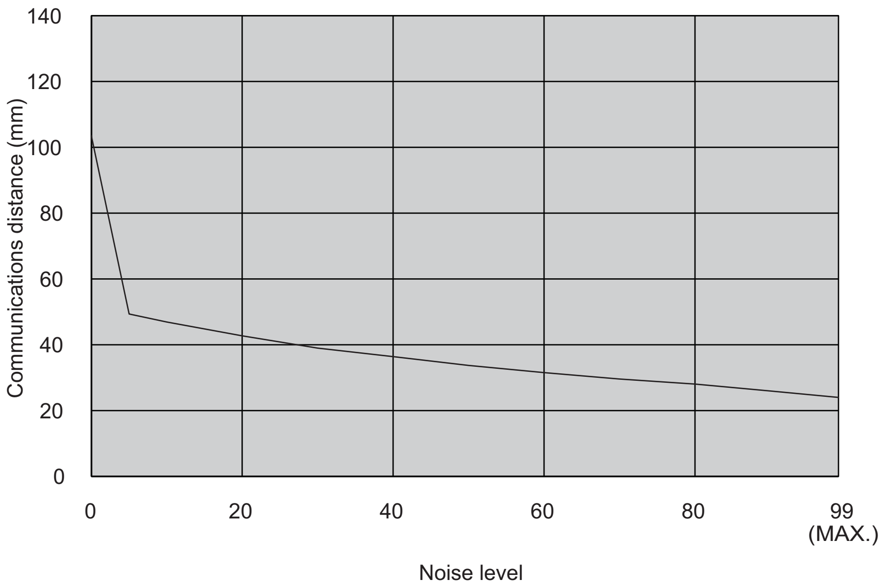
A-3-5 Communications Distance Characteristics vs. Ambient Noise

The graph below compares the results of measurement using the noise measurement function with communications distances.
At installation implement measures in regard to metal in the vicinity of the CIDRW Head, power supply noise, and atmospheric noise, to ensure that the noise level does not exceed *10*.

NOISE MEASUREMENT command (applies only when SECS is not used), refer to *4-1-12 NOISE MEASUREMENT* on page 4-21.

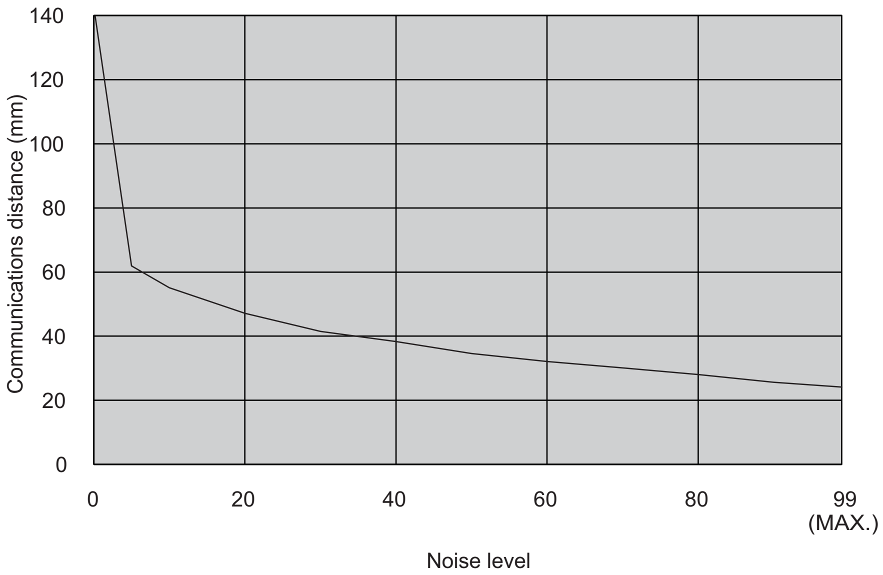
- **V640-HAM11-ETN-V5**

Relationship between noise level and communications distance (reference values)



- **V640-HAM11-L-ETN-V5**

Relationship between noise level and communications distance (reference values)



A-4 ID Tag Memory Maps

The memory maps of the RI-TRP-DR2B(-40) and RI-TRP-WR2B(-30) ID Tags are given below.

A-4-1 RI-TRP-DR2B(-40)

ID Tag Memory Map

Page	8 bytes/1 page							
1	00h	01h	02h	03h	04h	05h	06h	07h
2	08h	09h	0Ah	0Bh	0Ch	0Dh	0Eh	0Fh
3	10h	11h	12h	13h	14h	15h	16h	17h
4	18h	19h	1Ah	1Bh	1Ch	1Dh	1Eh	1Fh
5	20h	21h		•••	•••			27h
6	28h	29h		•••	•••			2Fh
7	30h	31h		•••				37h
8								
9								:
10	:							:
11	:							
12								
13								
14	68h	69h		•••	•••			6Fh
15	70h	71h		•••	•••			77h
16	78h	79h		•••	•••			7Fh
17	80h	81h		•••	•••			87h

Carrier ID (16 byte)

Data area (Total of 120 bytes)

Example of data segment settings

DATASEG	LENGTH
Carrier ID	16
"S01"	8
"S02"	8
"S03"	8
"S04"	8
"S05"	8
"S06"	8
"S07"	8
"S08"	8
"S09"	8
"S10"	8
"S11"	8
"S12"	8
"S13"	8
"S14"	8
"S15"	8

Additional Information

- The carrier ID memory area starts from page 1 (fixed).
- 00h to 87h in the table are addresses.
- The RI-TRP-DR2B(-40) has a memory capacity of 136 bytes.

A-4-2 RI-TRP-WR2B(-30)

ID Tag Memory Map

Page	8 bytes/1 page							
1	00h	01h	02h	03h	04h	05h	06h	07h

Carrier ID (8 byte)

Example of data segment settings

DATASEG	LENGTH
Carrier ID	8

Additional Information

- The RI-TRP-WR2B(-30) has a memory capacity of 8 bytes.

A-5 Regular Inspection

In order to maintain optimum performance of the functions of the CIDRW system, daily and periodic inspections are necessary.

Inspection item		Detail	Criteria	Tools required
Supply voltage fluctuation		Check that the supply voltage fluctuation at the power supply terminal block is within the permissible range.	To be within supply voltage rating.	Multimeter
		Check that there are no frequent instantaneous power failures or radical voltage drops.	To be within permissible voltage fluctuation range.	Power supply analyzer
Environment	Ambient temperature	Check that the ambient temperature and humidity are within specified range.	To be within the specified range.	Maximum and minimum thermometer Hygrometer
	Ambient humidity			
	Vibration and shock	Check that no vibration or shock is transmitted from any machines.		
	Dust	Check that the system is free of dust accumulation.	To be none.	
	Corrosive gas	Check that no metal part of the system is discolored or corroded.		
I/O power supply	Voltage fluctuation	Check on the I/O terminal block that the voltage fluctuation and ripple are within the permissible ranges.	To be within the specified range.	Multimeter Oscilloscope
	Ripple			
Mounting condition		Check that each device is securely mounted.	There must be no loose screws.	—
		Check that each connector is securely connected.	Each connector must be locked or securely tightened with screws.	
		Check that no wire is broken or nearly broken.	There must be no wire that is broken or nearly broken.	
		DCheck if grounding to 100 W or less has been done.	To be grounded to 100 Ω or less.	

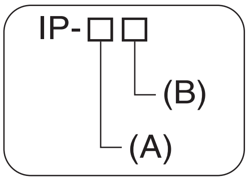
A-6 ASCII Code Table

Leftmost bits Right-most bits	b8 to b5	0000	1001	0010	0011	0100	0101	0110	0111	1000	1101	1010	1011	1100	1101	1110	1111
b4 to b1	Row Line	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0000	0	NUL	TC7(DLE)	(SP)	0	@	P	`	p	Undefined		Undefined				Undefined	
0001	1	TC1(SOH)	DC$_1$	!	1	A	Q	a	q								
0010	2	TC2(STX)	DC$_2$	"	2	B	R	b	r								
0011	3	TC3(ETX)	DC$_3$	#	3	C	S	c	s								
0100	4	TC4(EOT)	DC$_4$	$	4	D	T	d	t								
0101	5	TC5(NEQ)	TC$_8$(NAK)	%	5	E	U	e	u								
0110	6	TC6(ACK)	TC$_9$(SYN)	&	6	F	V	f	v								
0111	7	BEL	TC$_{10}$(ETB)	'	7	G	W	g	w								
1000	5	FE0(BS)	CAN	(	8	H	X	h	x								
1001	9	FE1(HT)	EM	)	9	I	Y	i	y								
1010	10	FE2(LF)	SUB	*	:	J	Z	j	z								
1011	11	FE3(VT)	ESC	+	;	K	[	k	{								
1100	12	FE4(FF)	IS$_4$(FS)	,	<	L	\	l	|								
1101	13	FE5(CR)	IS$_3$(GS)	-	=	M	]	m	}								
1110	14	S0	IS$_2$(RS)	.	>	N	^	n	ÅP								
1111	15	S1	IS$_1$(US)	/	?	O	_	o	DEL								

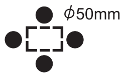
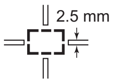
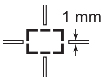
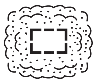
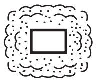
A-7 Degree of Protection

Ingress protection degrees (IP-□□) are determined by the following tests. Be sure to check the sealing capability under the actual operating environment and conditions before actual use.
IP stands for International Protection.

IEC (International Electrotechnical Commission) IEC 60529

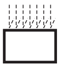
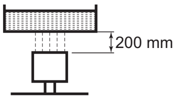
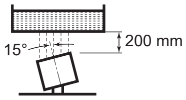
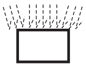
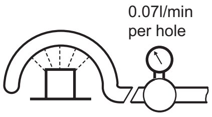
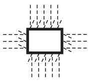
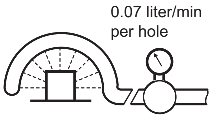
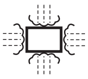
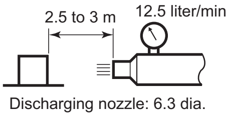
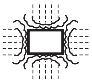
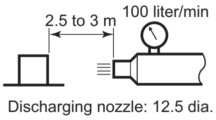
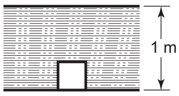
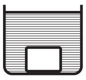


(A) First Digit: Degree of Protection from Solid Materials

Degree		Protection
0		No protection
1		Protects against penetration of any solid object such as a hand that is 50 mm or more in diameter.
2		Protects against penetration of any solid object, that is 12.5 mm or more in diameter. Even if finger or other object 12 mm in diameter penetrates, it will not reach a hazardous part.
3		Protects against penetration of any solid object, such as a wire, that is 2.5 mm or more in diameter.
4		Protects against penetration of any solid object, such as a wire, that is 1 mm or more in diameter.
5		Protects against penetration of dust of a quantity that may cause malfunction or obstruct the safe operation of the product.
6		Protects against penetration of all dust.

(B) Second Digit: Degree of Protection Against Water

Degree	Protection		Test method (with pure water)
0	No protection	Not protected against water.	No test

Degree	Protection		Test method (with pure water)
1	Protection against water drops 	Protects against vertical drops of water towards the product.	Water is dropped vertically towards the product from the test machine for 10 min. 
2	Protection against water drop	Protects against drops of water approaching at a maximum angle of 15° to the left, right, back, and front from vertical towards the product.	Water is dropped for 25 min each (i.e., 10 min in total) towards the product inclined 15° to the left, right, back, and front from the test machine. 
3	Protection against sprinkled water 	Protects against sprinkled water approaching at a maximum angle of 60° from vertical towards the product.	Water is sprinkled for 10 min at a maximum angle of 60° to the left and right from vertical from the test machine. 
4	Protection against water spray 	Protects against water spray approaching at any angle towards the product.	Water is sprayed at any angle towards the product for 10 min from the test machine. 
5	Protection against water jet spray 	Protects against water jet spray approaching at any angle towards the product.	Water is jet sprayed at any angle towards the product for 1 min per square meter for at least 3 min in total from the test machine.  2.5 to 3 m 12.5 liter/min Discharging nozzle: 6.3 dia.
6	Protection against high pressure water jet spray 	Protects against high-pressure water jet spray approaching at any angle towards the product.	Water is jet sprayed at any angle towards the product for 1 min per square meter for at least 3 min in total from the test machine.  2.5 to 3 m 100 liter/min Discharging nozzle: 12.5 dia.
7	Protection against limited immersion in water	Resists the penetration of water when the product is placed underwater at specified pressure for a specified time.	The product is placed 1 m deep in water (if the product is 850 mm max. in height) for 30 min. 
8 (See note.)	Protection against long-term immersion in water 	Can be used continuously underwater.	The test method is determined by the manufacturer and user.

Note: OMRON Test Method

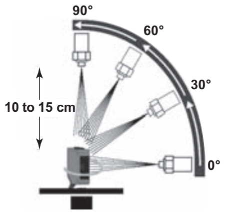
Usage condition: 10 m or less under water in natural conditions

1. No water ingress after 1 hour under water at 2 atmospheres of pressure.

2. Sensing distance and insulation resistance specifications must be met after 100 repetitions of half hour in 5°C water and half hour in 85°C water.

About IPX9K

IPX9K is a protection standard regarding high temperature and high-pressure water which is defined by the German standard (DIN 40050 PART9).
Water is sprayed on 80 °C hot water with the water pressure of 80 to 100BAR from a nozzle to the test piece.
Amount of water is 14 to 16 liters/minute.
The distance between the test piece and a nozzle is 10 to 15 cm, and the directions of water-drainage are 0 degrees, 30 degrees, 60 degrees, and 90 degrees horizontally.
They are evaluated with the test piece is rotating on a horizontal plane by 30 seconds in each direction.



Oil Resistance (OMRON in-house standard)

Protection	
Oil-resistant	No adverse affect from oil drops or oil spray approaching from any direction.
Oil-proof	Protects against penetration of oil drops or oil spray approaching from any direction.

Note. Oil resistance has been tested using a specific oil as defined in the OMRON test method. (JIS C 0920:2003, Appendix 1)

Index

Index

A

Amplifier Unit....2-2, 2-5
Amplifier Unit Indicators....7-2
Amplifier Unit operating status....7-2
Amplifier Units V640-HAM11-ETN-V5....1-5
Amplifier Units V640-HAM11-L-ETN-V5....1-5
ASCII Code Table....A-41

B

BYTE WRITE....4-9

C

Characteristic Data According to Conditions of Use....A-8
CIDRW Head....2-3
CIDRW Heads V640-HS61....1-8
CIDRW Heads V640-HS62....1-8
CLEAR COMMUNICATIONS HISTORY....4-20
Command / Response....4-2
Command Window....6-14
Command Window (CID R/W)....6-15
Command Window (V640 Command)....6-17
Command/Response Format....4-2
Communications Distance Characteristics vs. Ambient Noise....A-38
Communications Test....3-9
Communications Test between ID Tags and CIDRW System.....3-10
Communications Time....A-35
Component Names and Functions....1-5
Configuration Window....6-24
Connection Examples....A-7
Connections and Wiring....2-5
Connector for Connecting a CIDRW Head....2-5

D

Data Reading and Writing....2-3
Degree of Protection....A-42

E

Ethernet Connector....2-6

F

Features....1-3
Flowchart for Getting Started....1-9
For Coaxial Installation....A-32
For Face-to-Face Installation....A-33
For Parallel Installation....A-32

G

GET LAST COMMAND....4-18
GET PARAMETER....4-12

I

ID Tag Memory Maps....A-39
IEC (International Electrotechnical Commission) IEC 60529.....A-42
Influence of Background Metal on ID Tag....2-3
Influence of Noise....2-4
Installation....2-2

L

List of Error Messages....7-3
Log View Window....6-20
Login Window....6-5

M

Maps of Communications Areas (Reference Only)....A-8
Mounting....2-4
Mutual Interference Distances (Reference Only)....A-32

N

NAK....4-11
Network Settings Window....6-8
NOISE MEASUREMENT....4-21
Noise Monitor Window....6-19

O

Oil Resistance (OMRON in-house standard)....A-44
Operation Check Flowchart....7-4

P

Positional Relationship between the CIDRW Head and the ID Tag....2-3
Power Supply and Grounding Wires....2-7

R

READ....4-4
Regular Inspection....A-40
RESET....4-22
Root Certificate Installation Procedure....6-28

S

Safe-Mode Window....6-26
SAME WRITE....4-8
SET NETWORK....4-23
Set the IP Address on the Computer....3-2
Specifications and Dimensions....A-2
Status Window....6-7

System Configuration.. 1-4

T

TEST.. 4-10
Troubleshooting...7-2

W

What Is a CIDRW System... 1-2
Window Configuration... 6-4
WRITE...4-6

OMRON Corporation **Industrial Automation Company**

Kyoto, JAPAN **Contact : www.ia.omron.com**

Regional Headquarters

OMRON EUROPE B.V.
Wegalaan 67-69, 2132 JD Hoofddorp
The Netherlands
Tel: (31) 2356-81-300 Fax: (31) 2356-81-388

OMRON ASIA PACIFIC PTE. LTD.
438B Alexandra Road, #08-01/02 Alexandra
Technopark, Singapore 119968
Tel: (65) 6835-3011 Fax: (65) 6835-3011

OMRON ELECTRONICS LLC
2895 Greenspoint Parkway, Suite 200
Hoffman Estates, IL 60169 U.S.A.
Tel: (1) 847-843-7900 Fax: (1) 847-843-7787

OMRON (CHINA) CO., LTD.
Room 2211, Bank of China Tower,
200 Yin Cheng Zhong Road,
PuDong New Area, Shanghai, 200120, China
Tel: (86) 21-6023-0333 Fax: (86) 21-5037-2388

Authorized Distributor:

Cat. No. Z497-E1-02 0925