OMRON

Virtual Fleet Manager

Installation Guide

I695-E-01

NOTE

Trademarks

Copyrights

Introduction

This manual is OMRON's original instructions describing the platform, infrastructure, installation, and configuration required for the operation of the Virtual Fleet Manager.
Please read this manual and ensure you understand the functionality and performance of the Virtual Fleet Manager before attempting to use it.
Keep this manual in a safe place where it will be available for reference during operation.

Intended Audience

This manual is intended for the following personnel, who must also have knowledge of factory automation (FA) systems and robotic control methods.

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

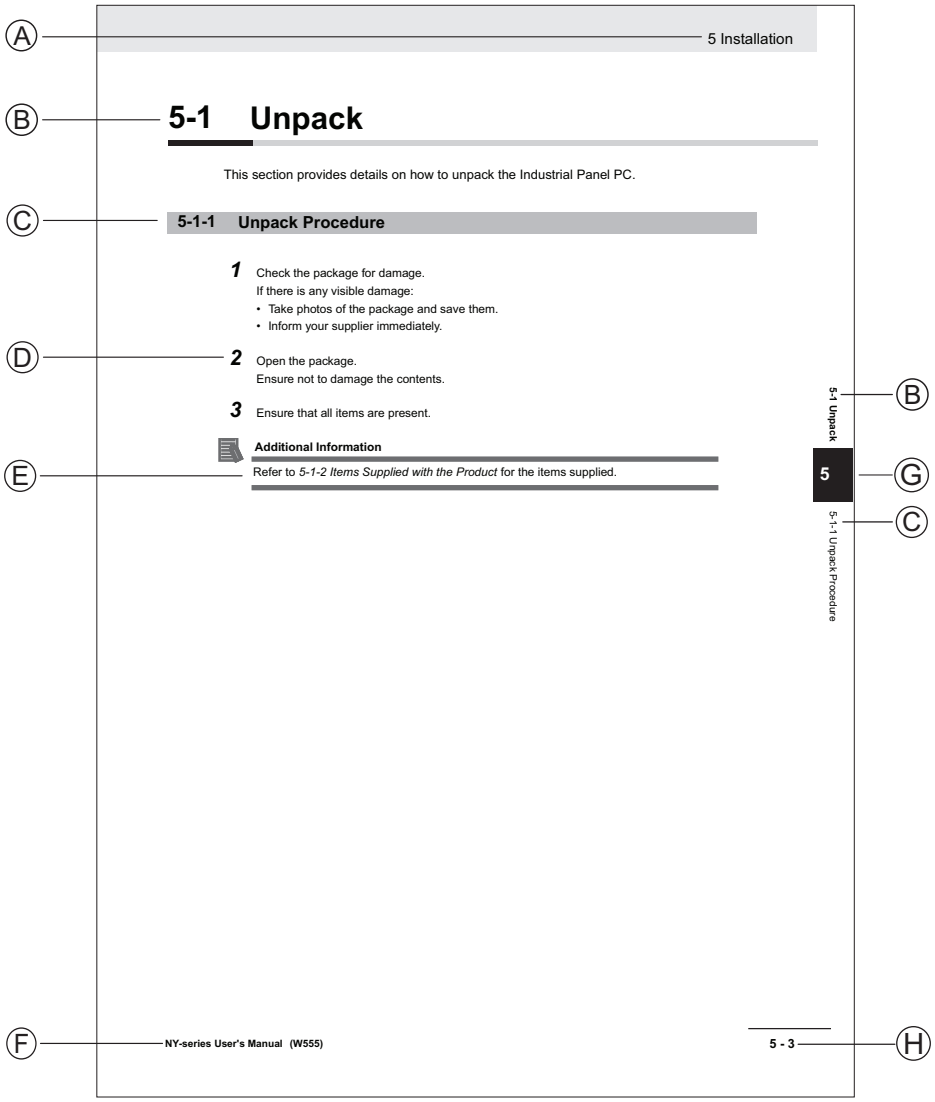
Applicable Products

This manual provides information for the Virtual Fleet Manager product.
Included procedures have been tested for FLOW Core version 4.0.

Manual Information

Page Structure

The following page structure is used in this manual.



Note: This illustration is provided as a sample. It will not literally appear in this manual.

Item	Explanation	Item	Explanation
A	Level 1 heading	E	Special Information
B	Level 2 heading	F	Manual name
C	Level 3 heading	G	Page tab with the number of the main section
D	Step in a procedure	H	Page number

Special Information

Special information in this manual is classified as follows:

Precautions for Safe Use

Precautions on what to do and what not to do to ensure safe usage of the product.

Precautions for Correct Use

Precautions on what to do and what not to do 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 different versions.

Sections in this Manual

CONTENTS

Section 1 Overview

Section 2 Virtual Machine Configuration & Creation

Section 3 Virtual Fleet Manager Installation & Configuration

Section 4 Troubleshooting

Section 5 Appendix

Terms and Conditions Agreement

Warranty and Limitations of Liability

Warranty

- **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, expressed 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 http://www.omron.com/global/ or contact your Omron representative for published information.

Limitations of Liability

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 for 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 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.
- Omron Companies shall not be responsible for the operation of the user accessible operating system (e.g. Windows, Linux), 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.

Safety Precautions

Definition of Precautionary Information

The following notation is used in this manual to provide precautions required to ensure safe usage of the Virtual Fleet Manager. The safety precautions that are provided are extremely important to safety. Always read and heed the information provided in all safety precautions.
The following notation is used.

⚠ **WARNING**	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury. Additionally, there may be severe property damage.

Symbols

	The triangle symbol indicates precautions (including warnings). The specific operation is shown in the triangle and explained in text. This example indicates a general precaution.
	The filled circle symbol indicates operations that you must do. The specific operation is shown in the circle and explained in text. This example shows a general precaution for something that you must do.

Warnings

⚠ WARNING

Cybersecurity

To maintain the security and reliability of the system, a robust cybersecurity defense program should be implemented, which may include some or all of the following:

Anti-virus protection

- Install the latest commercial-quality anti-virus software on the computer connected to the control system and keep the software and virus definitions up-to-date.
- Scan USB drives or other external storage devices before connecting them to control systems and equipment.

Security measures to prevent unauthorized network access

- 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 block unused communications ports and limit communication between systems. Limit access between control systems and systems from the IT network.
- Control remote access and adopt multifactor authentication to devices with remote access to control systems and equipment.
- Set strong password policies and monitor for compliance frequently.

Data input and output protection

- Backup data and keep the data up-to-date periodically to prepare for data loss.
- Validate backups and retention policies to cope with unintentional modification of input/output data to control systems and equipment.
- Validate the scope of data protection regularly to accommodate changes.
- Check validity of backups by scheduling test restores to ensure successful recovery from incidents.
- Safety design, such as emergency shutdown and fail-soft operations in case of data tampering and incidents.

Additional recommendations

- When using an external network environment to connect to an unauthorized terminal such as a SCADA, 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 network infrastructure, 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 devices equipped with an SD Memory Card, there is a security risk that a third party may acquire, alter, or replace the files and data in the removable media by removing or unmounting the 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 and controlling access to the installation area.
- Educate employees to help them identify phishing scams received via email on systems that will connect to the control network.

Precautions for Correct Use

- Care should be taken when deploying any configuration in a networked environment. Security and performance can be adversely affected by misconfigured networking. Suggestions in this document are provided to assist in the initial deployment of the Virtual Fleet Manager and may conflict with your site's networking infrastructure.

Related Manuals

Use the following related manuals for reference.

Manual Title	Description
Fleet Operations Workspace Core User's Manual (Cat. No. I635)	Describes Fleet management, MobilePlanner software, the SetNetGo OS, and most of the configuration procedures for an AMR.
LD-60/90 Platform User's Manual (Cat. No. I611)	Describes the installation, start-up, operation, and maintenance of the LD-60 and LD-90 AMRs.
LD-250 Platform User's Manual (Cat. No. I642)	Describes the installation, start-up, operation, and maintenance of the LD-250 AMR.
AMR (Autonomous Mobile Robot) MD-series Platform User's Manual (Cat. No. I681)	Describes the installation, start-up, operation, and maintenance of the MD-series AMRs.
HD-1500 Platform User's Manual (Cat. No. I645)	Describes the installation, start-up, operation, and maintenance of the HD-1500 AMR.

Glossary

Term / Abbreviation	Description
AMR	Autonomous Mobile Robot
Enterprise Manager	Legacy EM2100 appliance.
Fleet	Two or more AMRs operating in the same workspace controlled by a single Fleet Manager.
Fleet Operations Workspace (FLOW)	A set of mobile-robotics software applications for programming and operating one or a fleet of AMRs and the Fleet Manager.
Hypervisor	A type of computer software, firmware, or hardware which hosts and manages virtual machines.
Map	A digital representation of the AMR's operating environment.
MobilePlanner	The primary software application for configuring and monitoring AMR operations. It provides the tools for all major AMR activities, such as observing a fleet of AMRs, commanding individual AMRs to drive, creating and editing map files, goals, and tasks, and modifying AMR configurations.
SetNetGo (SNG)	The software operating system that resides on the AMR and the optional Fleet Manager appliance. It is used to configure the AMR's communication parameters, gather Debug Info Files, and upgrade the software.
Virtual Fleet Manager	The operational mode of the computing appliance that runs the FLOW Core software to control a fleet of AMRs when hosted by a hypervisor.
Virtual interface	A network interface that may not be associated with a physical interface.
Virtual machine	An emulation of a computer system that provides the functionality of a physical computer.
Virtual switch	A software program that enables one virtual machine to communicate with another.
VMware vSphere	Virtualization platform to manage virtual machines and virtual appliances, as well as hosts in a network.

1

Overview

The following sections provide an overview of the requirements and general configuration of the Virtual Fleet Manager.

1-1 Licensing

FLOW Core licenses for the Virtual Fleet Manager are bundled in tiers, based on the number of AMRs. There are three licenses pertaining to operation of the Virtual Fleet Manager and the AMR fleet:

- FLOW Core Fleet Manager License
- FLOW Core Fleet Manager Renewal License
- FLOW Core Fleet Manager Upgrade License

Each is explained in the sections that follow.

Additional Information

- Additional licensed features and functionality are available. Refer to the AMR User's Manual and *Fleet Operations Workspace Core User's Manual (Cat. No. I635)* for more information.
- Licensed products for the EM2100 are not compatible with the Virtual Fleet Manager installation.

1-1-1 FLOW Core Fleet Manager License

FLOW Core Fleet Manager License (30271-1XX) is intended for initial install. XX denotes the number of AMRs supported in a fleet, in multiples of five (up to thirty). The license for fifty may be used for an unlimited AMR fleet size. FLOW Core Fleet Manager License includes:

- Access to installable software
- Choice of number of AMRs
- Access to three years of software updates

If this license is added to an existing fleet, its expiration date will replace the existing expiration date. Any remaining time on the existing license will be lost, and the new expiration date will be based on the date of license installation. The new fleet count will be added to the existing count.

If this initial install license expires, the Virtual Fleet Manager and the fleet will still continue to operate. However, access to new software updates is limited to the major version of FLOW Core running on the Virtual Fleet Manager. For reference, the major version is determined by the first digit of the version number (e.g. 4.x.x).

1-1-2 FLOW Core Fleet Manager Renewal License

FLOW Core Fleet Manager Renewal License (30271-2XX) is intended for license renewal and provides an extension of the expiration date by one year. XX denotes the number of AMRs supported in a fleet, in multiples of five (up to thirty). The license for fifty may be used for an unlimited AMR fleet size.

If FLOW Core Fleet Manager Renewal License is added to an existing fleet, the existing expiration date will be extended by one year (based on the date of license installation). The new fleet count will fully replace the existing count as well.

If this renewal license expires, the Virtual Fleet Manager and the fleet will still continue to operate. However, access to new software updates is limited to the major version of FLOW Core running on the Virtual Fleet Manager. For reference, the major version is determined by the first digit of the version number (e.g. 4.x.x).

1-1-3 FLOW Core Fleet Manager Upgrade License

FLOW Core Fleet Manager Upgrade License (30271-001) includes the ability to add one AMR to the fleet.

If this license is added to an existing fleet, the expiration date remains the same. The new fleet count is added to the existing count.

If multiple licenses are added, the existing fleet count will increase by the order quantity (e.g. three licenses ordered adds three AMRs to the existing fleet).

For fleets without a license: The Virtual Fleet Manager requires FLOW Core Fleet Manager License to be able to run. If FLOW Core Fleet Manager Upgrade License is added, the AMR count would then be the sum of the counts of both licenses.

If FLOW Core Fleet Manager Upgrade License expires, the Virtual Fleet Manager and the fleet will still continue to operate. However, access to new software updates is limited to the major version of FLOW Core running on the Virtual Fleet Manager. For reference, the major version is determined by the first digit of the version number (e.g. 4.x.x).

1-2 Supported Platforms & Configurations

This section provides information related to hypervisors and virtual machines for the Virtual Fleet Manager.
The Virtual Fleet Manager software was validated against VMware vSphere and EXSi platform configurations. It was also validated against VMware Workstation Pro. Installing this package on a non-VMware system is not supported. Refer to *1-2-1 Virtualization Types & Scenarios* on page 1-4 for a discussion of both platforms.
There are a variety of suitable hardware configurations for operating the Virtual Fleet Manager. They are covered in *1-2-2 Required Components* on page 1-5 and *1-2-3 Map and Fleet Size Considerations* on page 1-5.

1-2-1 Virtualization Types & Scenarios

The following sections provide an overview of the different types of virtualization and describe user deployment scenarios.

Virtualization Types

Prior to virtualization, a dedicated and physical hardware configuration with an operating system is required. Virtualization allows several operating systems to coexist on one set of hardware. This provides several advantages, such as reducing the number of physical hardware components, as well as reducing time spent troubleshooting.
A hypervisor makes virtualization possible by creating a layer that separates hardware from the virtual machines that run the guest operating systems. There are two types of hypervisors:
- Type 1: Known as bare-metal or native hypervisors
- Type 2: Known as hosted hypervisors

A type 1 hypervisor is a layer of software installed on top of the set of physical hardware. No other software runs between the hypervisor and the hardware. Thus, this is why it is sometimes referred to as a bare-metal hypervisor. This type of hypervisor provides superior performance and stability, as it does not run inside any other operating system (such as Windows). This also provides higher security. VMware vSphere with ESX/ESXi is one example of a type 1 hypervisor.
A type 2 hypervisor runs inside the host machine's operating system. This is why they are known as hosted hypervisors. Unlike bare-metal hypervisors, this type has a software layer between itself and the physical hardware. This makes them easy to manage and convenient for testing, as one does not require a separate management console. VWware Workstation is an example of a type 2 hypervisor.

Deployment Scenarios

There are several factors that will determine the appropriate solution for an application, such as: Fleet size, available hardware, IT personnel, and support needs. Three different scenarios are described below.
Scenario 1:
- Small fleet (< 10 AMRs).

- IT department is remote/contracted, not well-equipped for the task, or non-existent.
- Preference to have an all-OMRON solution (Industrial PC, software), as well as OMRON support.
- Ideal for those who wish to have a low-maintenance solution.

Scenario 2:

- A central machine solution is preferred.
- Virtual Fleet Manager required to coexist on the same hardware as a guest operating system, such as Windows (type 2 hypervisor).
- Central solution carries risks: Shared resources, single point of failure.
- Ideal for sales representatives and on-site support engineers. Not recommended as a permanent solution.

Scenario 3:

- Application has a large fleet, potentially exceeding 100 AMRs.
- IT department is on-site, capable, and prefers a dedicated server rack solution (type 1 hypervisor) with higher resource limits.
- Virtual Fleet Manager is treated as mission-critical and IT prefers to deploy tools for maximum uptime, such as VMware vSphere.
- An regularly-tested, OMRON-recommended solution is preferred.

Additional Information

The number of AMRs can theoretically exceed 100 using a Virtual Fleet Manager. However, available hardware resources and bandwidth will determine the actual limit.

1-2-2 Required Components

A virtual machine will contain the installation of the Virtual Fleet Manager. The following components are required for the virtual machine:

- Two virtual disk devices
  One virtual disk is designated for the Operating System (at least 60 GB)
  One virtual disk is designated for data storage (at least 512 GB)
- One supported virtualization platform: VMware vSphere and ESXi platform software (licensed), or VMware Workstation Pro (licensed)
- Virtual Fleet Manager installer (ISO file)
- FLOW Core Fleet Manager license
- A robust wireless network (refer to *1-3 Networking Requirements & Considerations* on page 1-7 for more information)
- Four virtual network interfaces

1-2-3 Map and Fleet Size Considerations

Complex applications will demand more resources from the virtual machine. Map size and fleet size are two factors that contribute to an application's complexity. While it is not possible to cover all scenarios, the table below provides some examples for map size, fleet size, and other criteria to help determine resource requirements. Please note the storage and memory recommendations are not the minimum requirements for configuring a Virtual Fleet Manager; they are simply guidelines.

Map Size	Criteria	vCPU	vRAM	vDisk
Small	Map: <= 5000 m² AMR count: <= 5 Job Rate: • <= 5 jobs/min • One job per AMR per minute Queuing method: FIFO only	Two cores	8 GB	512 GB
Medium	Map: <= 25,000 m² AMR count: <= 15 Job Rate: • <= 30 jobs/min • Two jobs per AMR per minute Queuing method: FIFO only	Two cores	16 GB	512 GB
Large	Map: <= 75,000 m² AMR count: <= 30 Job Rate: • <= 90 jobs/min • Three jobs per AMR per minute Queuing method: FIFO or non-FIFO	Four cores	24 GB	512 GB
Extra Large	Map: <= 125,000 m² AMR count: <= 100 Job Rate: • <= 200 jobs/min • Two jobs per AMR per minute Queuing method: FIFO or non-FIFO	Four cores	32 GB	1 TB

Please note the default resolution (20) was used for the maps in the table above. Increasing the resolution will increase the complexity of the map.

1-2-4 High Availability Considerations

Adopting virtualization allows for a reduction in the amount of physical hardware. However, the main drawback to a virtual environment is that it may become the single point of failure for multiple applications, presenting a higher risk for downtime. For this reason, virtual environments require higher standards for availability.

Fault tolerance is a method of protecting against failures and interruptions in a virtual environment. It automatically detects failures and permits applications to continue running while preserving client connections. Reliability is accomplished through active redundancy.

Consider the following for high availability and fault tolerance in the application:

- VMware vSphere FT (Fault Tolerance): Provides continuous availability and fault tolerant protection by creating and maintaining a duplicate, secondary virtual machine on a separate host
- VMware vSphere HA (High Availability): Monitors and restarts virtual machines when a server outage or operating system failure is detected
- VMware vSphere vMotion: Allows for migration of the virtual machine to a new host and continued operation during maintenance activities or other planned downtime

Refer to VMware's documentation for licensing and additional information.

1-3 Networking Requirements & Considerations

A Virtual Fleet Manager running FLOW Core software is typically connected to the following items during normal operation:

- AMR wireless network
- Operator terminal(s)
- Factory equipment management systems (WES, MES)

This section provides requirements and considerations for the Virtual Fleet Manager networking environment.

1-3-1 Wireless Considerations

Network resource availability can affect Virtual Fleet Manager performance and the number of AMRs supported.

Refer to the AMR's user manuals for additional information regarding requirements for wireless networks and network access points. Be aware of the specific requirements for wireless network coverage and bandwidth.

1-3-2 Maintenance Interface

The Maintenance interface is the first to be probed and defined by the operating system. The other network interfaces, Management and Fleet, are used for fleet management (refer to *1-3-3 Fleet & Management Interfaces* on page 1-7 for more information).

Access to the Maintenance interface must be configured in one of the following ways:

- The virtual Maintenance interface can be mapped to the external network and accessed via a web browser.
- The virtual Maintenance interface can be mapped to an internal standard switch and accessed via a web browser from an independent customer-supplied virtual machine.

Refer to *3-3 Initial Access to the Maintenance Interface* on page 3-4 for more information on these procedures, as well as Introduction to vSphere Networking for more information on vSphere networking.

Once access to the Maintenance interface is gained, the IP address of the Management port must be set by accessing https://1.2.3.4 through a web browser. Additionally, SetNetGo web access must be enabled for the Management interface. Once access via the Management network is achieved, access to the Maintenance interface is no longer required.

1-3-3 Fleet & Management Interfaces

The Virtual Fleet Manager's hardware requires two static IP address assignments for the Management and Fleet networks. Each AMR in the system will also require IP address assignment via DHCP or, more commonly, a static IP address.

These virtual interfaces may be mapped to the networking infrastructure in a number of ways, using different technologies with differing performance and security consequences. The most basic configuration would place both the Management and Fleet virtual interfaces on the same subnet and map

each interface to the same standard virtual switch. This virtual switch would also be mapped to an external physical interface on the same subnet as the AMR fleet.
A different subnet may be required for the Management and Fleet networks depending on the local infrastructure. Although it is not required, using a different subnet for each network will enable isolation of Fleet data traffic from Management traffic for enhanced security.

Precautions for Correct Use

Care should be taken when deploying any configuration in a networked environment. Security and performance can be adversely affected by misconfigured networking. Suggestions in this document are provided to assist in the initial deployment of the Virtual Fleet Manager and may conflict with your site's networking infrastructure.

1-4 General Installation Overview

The steps below provide an overview of the Virtual Fleet Manager installation procedure. Details can be found in each referenced section.

1 Configure and create the virtual machine based on the chosen hypervisor type.
Refer to *Section 2 Virtual Machine Configuration & Creation* on page 2-1.

2 Install the Virtual Fleet Manager application.
Refer to *Section 3 Virtual Fleet Manager Installation & Configuration* on page 3-1.

3 Configure the Virtual Fleet Manager.
Refer to *Section 3 Virtual Fleet Manager Installation & Configuration* on page 3-1.

2

Virtual Machine Configuration & Creation

This section provides information about the creation and configuration of a virtual machine.

2-1 VMware ESXi Virtual Machine Configuration Procedure

The VMware ESXi platform should be configured as outlined in the following VMware documentation resources:

- vSphere Server virtualization software
- vCenter Server vSphere server management software
- ESXi Hardware Requirements
- Performance Best Practices for VMware vSphere 7.0

The following steps outline how to configure the virtual machine:

1 Create a new virtual machine.

2 Select a backing store for the virtual machine.
Virtual machine disks backed to NFS or SMB files systems are not recommended.

3 Configure the virtual machine's CPU and memory according to *1-2-3 Map and Fleet Size Considerations* on page 1-5.

4 Configure hard disk 1 with the following settings:

- Set disk capacity to 60 GB, at a minimum.
- Select a location.
- Set disk provisioning to **Thin**.
- Set **Unlimited** for IOPs.
- Set controller location to **SATA Controller 0**. SCSI is not supported.

5 Add a new hard disk with the following settings:

- Set disk capacity to 512 GB, at a minimum.
- Select a location.
- Set disk provisioning to **Thin**.
- Set **Unlimited** for IOPs.
- Set controller location to **SATA Controller 0**. SCSI is not supported.

6 Complete the virtual machine configuration and then modify the following settings:

- Add three additional network adapters (to equal four total for the system).
  Set adapter type of all four adapters to **E1000e**.
  The adapter assigned to the Maintenance network must be assigned to the network associated with access to the Maintenance interface (IP address 1.2.3.4).
  The adapter assigned to the Management network must be assigned to the network associated with access to the SetNetGo web interface.
  The adapter assigned to the Fleet network must be associated with the external network with fleet management.

Additional Information

The fourth adapter is planned for future use.

- Select **EFI** under *Boot Options* and ensure the UEFI secure boot option is not enabled.

7 Associate the CD/DVD with **Datastore ISO file**. Ensure the Virtual Fleet Manager's installation ISO file is uploaded to this datastore location.

8 Review the final virtual machine configuration and then complete the creation process.
After the virtual machine settings are configured, the Virtual Fleet Manager application can be installed. Refer to *Section 3 Virtual Fleet Manager Installation & Configuration* on page 3-1 for more information.

2-2 VMware Workstation Virtual Machine Configuration Procedure

VMware Workstation Pro 16 must be pre-installed before following this procedure.
VMware installation steps may limit the type and number of devices for the virtual machine. If this is the case, accept the defaults and after completing, edit the virtual machine configuration.
The Virtual Fleet Manager requires three network interfaces. To ensure the correct instantiation of the network devices on the virtual machine, they should be created in the following order:

1. Host-Only
2. Bridged
3. Bridged

The following steps outline how to configure and create the virtual machine:

1 Start VMware Workstation and create a new virtual machine.

2 Select **Custom (advanced)** for the configuration type.

3 Choose the virtual machine hardware compatibility.
For this example, choose **Workstation 16.2.x**.

4 Make a selection for the guest operating system installation.
For this example, choose to install the operating system later.

5 Select the guest operating system: **Linux Debian 8.x 64-bit**.

6 Name the virtual machine and designate a location.

7 Specify the number of processors and cores per processor.
For this example, designate 2 processors with 2 cores per processor.

8 Specify the amount of memory to allocate for the virtual machine according to *1-2-3 Map and Fleet Size Considerations* on page 1-5.

9 Add a network as host-only. This network can be used for initial configuration via the Maintenance interface (IP address 1.2.3.4).

10 Set I/O controller types as **LSI Logic (recommended)**.

11 Select **SATA** for disk type.

12 Create a new virtual disk.

13 Specify at least 60 GB as the disk capacity.

14 Specify where to store the .vmdk disk file.

15 Verify the selections and then create the virtual machine.

16 Edit the virtual machine settings to accomplish the following:

- Add a second SATA or IDE Disk and configure as 512 GB.
  If vSphere FT support is needed, use SATA disks only.
- Add the second and third network adapters as **Bridged**.
- Select **UEFI** for firmware type.
- If a Secure Boot option is enabled by default, disable it.
- Set the CD/DVD device to use the Virtual Fleet Manager's installation ISO file.

After the virtual machine settings are configured, the Virtual Fleet Manager application can be installed. Refer to *Section 3 Virtual Fleet Manager Installation & Configuration* on page 3-1 for more information.

3

Virtual Fleet Manager Installation & Configuration

This section provides information about the installation and configuration of the Virtual Fleet Manager application.

3-1 Virtual Fleet Manager Application Installation Procedure

The following items must be completed before installing the Virtual Fleet Manager application:

- VMware Workstation or VMware ESXi must be installed, configured, and running.
- The virtual machine must be configured and created.
- The ISO file for the Virtual Fleet Manager application must be uploaded to the virtual machine's file storage.

1 Power ON the virtual machine.

2 Install the Virtual Fleet Manager application by selecting *Install onto VM as EM2100* in the list displayed in the virtual machine's window.
The console shows the installation progress. Wait for the process to complete, indicated by the message *Installation successful*.

3 Reboot the virtual machine to complete this procedure.

3-2 Virtual Fleet Manager Configuration Procedure

The steps below provide an overview of the Virtual Fleet Manager configuration procedure. Details can be found in each referenced section.

1 Access the Maintenance interface based on the chosen hypervisor type.
Refer to *3-3 Initial Access to the Maintenance Interface* on page 3-4.

2 License the Virtual Fleet Manager.
Refer to *3-4 Licensing* on page 3-10.

3 Configure the system mode.
Refer to *3-5 System Mode Configuration* on page 3-11.

4 Configure the Fleet interface.
Refer to *3-6 Fleet Interface Configuration Procedure* on page 3-12.

5 Configure access control for users.
Refer to *3-7 Enable Access Control Procedure* on page 3-13.

6 Verify the system is operational.
Refer to *3-8 System Status Verification Procedure* on page 3-14.

3-3 Initial Access to the Maintenance Interface

Once the Virtual Fleet Manager application has been installed, initial configuration can be performed on the Virtual Fleet Manager's hardware. The Maintenance interface must be accessible via a web browser in the virtualized environment. The selected hypervisor type will determine which methods are applicable in the sections that follow.

Precautions for Correct Use

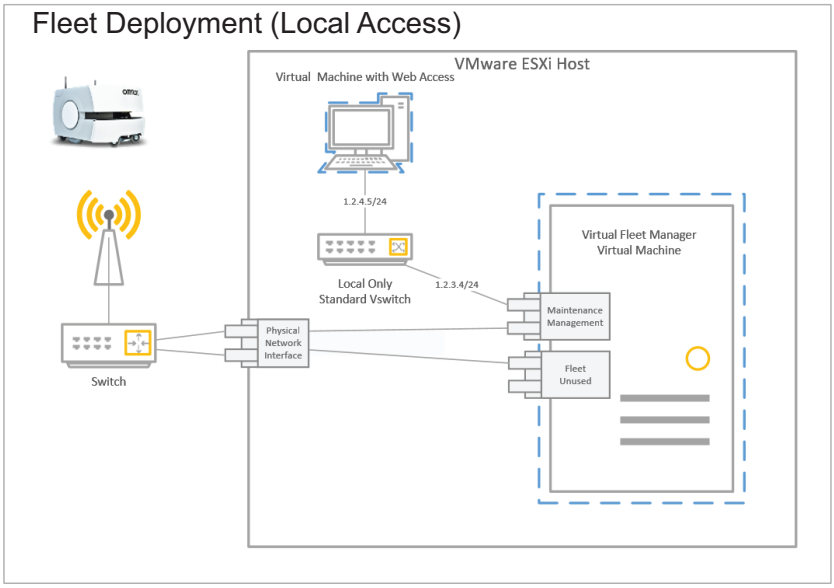
Care should be taken when deploying any configuration in a networked environment. Security and performance can be adversely affected by misconfigured networking. Suggestions in this document are provided to assist in the initial deployment of the Virtual Fleet Manager and may conflict with your site's networking infrastructure.

3-3-1 Access From VMware ESXi

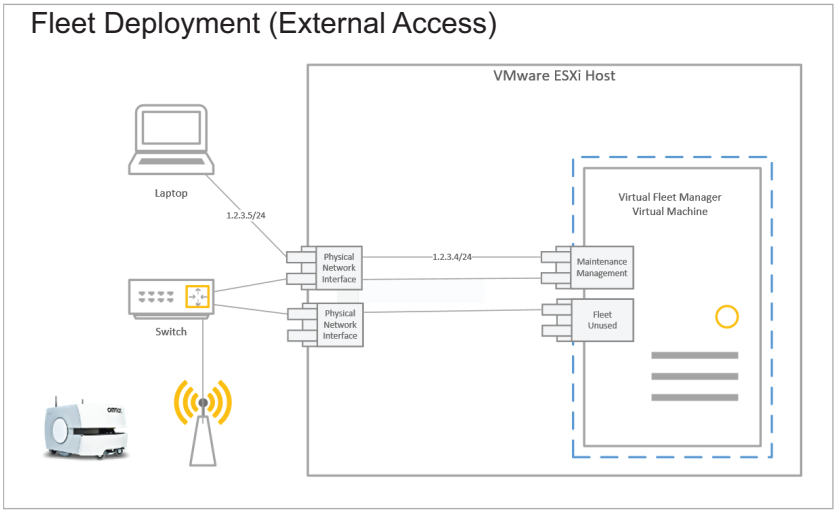
There are several methods for accessing the Maintenance interface via VMware ESXi. The table and graphics below summarize the methods, along with their advantages and disadvantages. The sections that follow provide the steps to gain access.

Method	Description	Advantage(s)	Disadvantage(s)
Local Access	The user has a non-Fleet Manager virtual machine with web access and connectivity to a local-only virtual switch.	• 1.2.3.4/24 not exposed on the corporate network • Easily done if a virtual machine is already part of virtualized environment • Less complexity on deployments with limited physical interfaces	• Must deploy and connect an independent virtual machine
External Access	The user has three physical interfaces available and maps each virtual interface to a physical interface.	• Simple deployment	• Requires 2-3 interfaces
Combined Local & External Access	The user has a single physical interface and a single virtual switch.	• Simple deployment	• Leaves 1.2.3.4/24 exposed on the corporate network

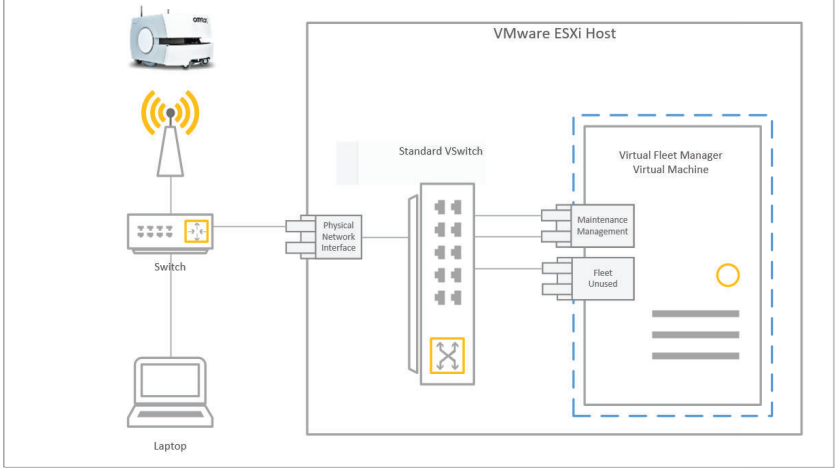
Fleet Deployment (Local Access)



Fleet Deployment (External Access)



Fleet Deployment (Combined Access)



Local Access

Follow the steps below for local access:

1. Connect the Maintenance port of the Virtual Fleet Manager to the local-only virtual switch. The Maintenance port will have an IP address of 1.2.3.4/24.
2. Connect the non-Fleet Manager virtual machine with web access and the local-only virtual switch using IP address 1.2.3.5.
3. Open a browser and access http://1.2.3.4.

External Access

Follow the steps below for external access:

1. Connect the Maintenance port of the Virtual Fleet Manager to the physical interface. The Maintenance port will have an IP address of 1.2.3.4/24.
2. Connect a PC to the physical interface associated with the Maintenance port.
3. Assign IP address 1.2.3.5 to the PC's interface.
4. Open a browser and access http://1.2.3.4.

Additional Information

A virtual switch can be used in between the virtual interfaces and physical interface. The Maintenance virtual interface should not be attached to the same virtual switch as the Management and Fleet interfaces.

Combined Local & External Access

Follow the steps below for combined access:

1. Connect the Maintenance port of the Virtual Fleet Manager to the physical interface. The Maintenance port will have an IP address of 1.2.3.4/24.
2. Connect a PC to the physical interface associated with the Maintenance port.
3. Assign IP address 1.2.3.5 to the PC's interface.
4. Open a browser and access http://1.2.3.4.
5. Configure the Management and Fleet interfaces, and allow management on the Management interface.
6. Change the IP address of the PC to the network associated with the Management interface.

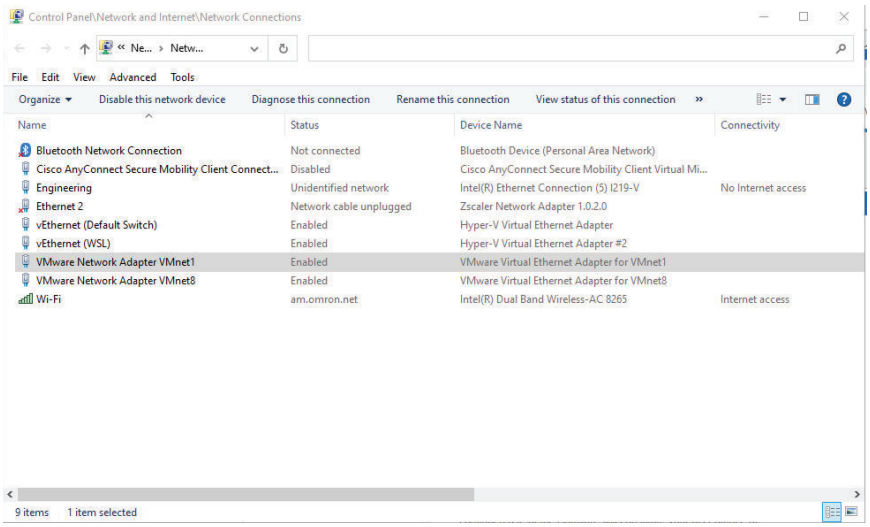
Additional Information

The Maintenance virtual interface should not be attached to the same virtual switch as the Management and Fleet interfaces.

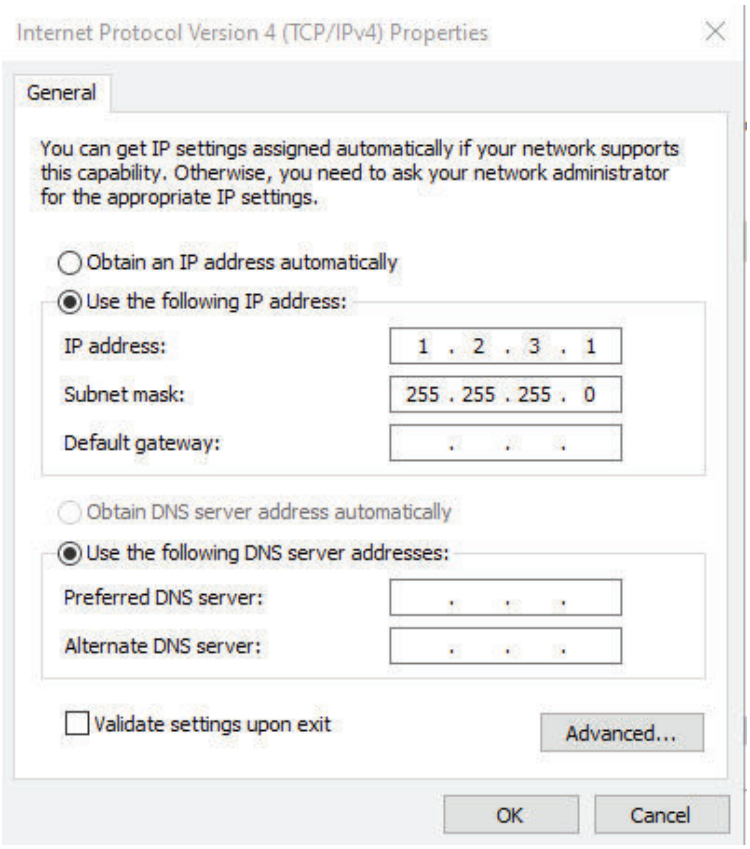
3-3-2 Access From VMware Workstation

Accessing the Maintenance interface from VMware Workstation only requires setting an IPv4 address on the host machine, as described below:

1 Configure the host network to allow connection to the Maintenance interface: Open *Control Panel / All Control Panel Items / Network Connections* and identify the host portion of the first network device on the virtual machine.



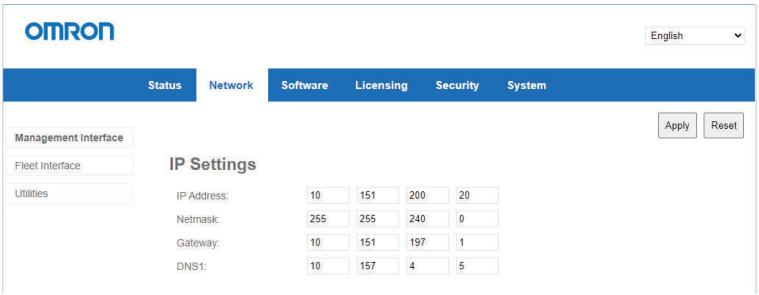
2 Add IPv4 address 1.2.3.1 to the adapter.



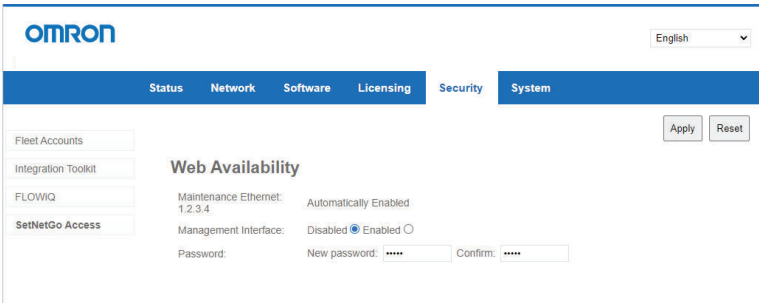
3 Open a web browser and enter the IP address: 1.2.3.4.

4 Accept the license agreement and acknowledge the pop-up.

5 Click on the **Network** tab to configure IP settings for the Management interface.



6 Click on the **Security** tab to enable SetNetGo access to the Management interface.

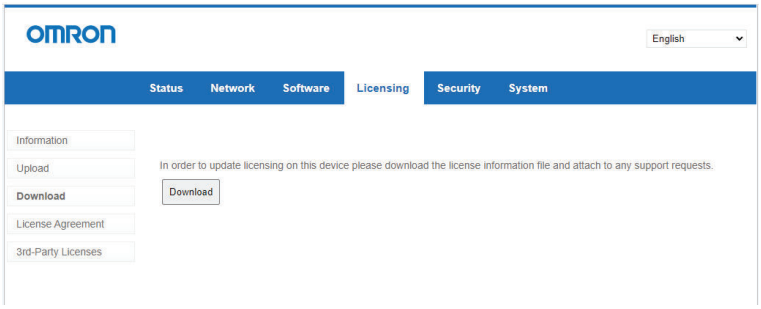


7 Access the Management interface via SetNetGo by browsing to the IP address that was set for the interface in Step 5.

3-4 Licensing

The SetNetGo licensing area provides information about license name, status, and expiration dates for the connected device. It also allows acquisition, renewal, or upgrading of any licenses on the Virtual Fleet Manager. Follow the steps below for licensing:

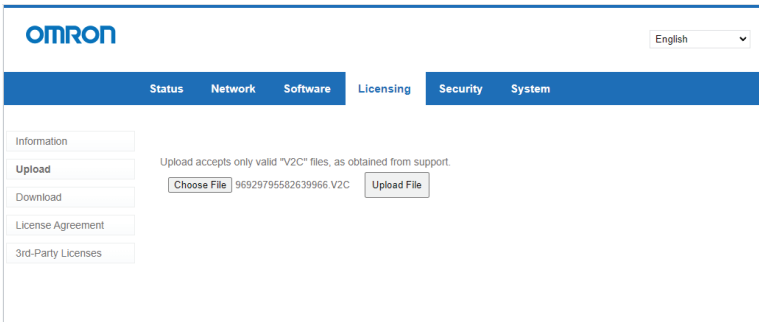
1 Access the SetNetGo web interface of the Virtual Fleet Manager and open the **Licensing** tab. Click on the **Download** option in the left pane.



2 On the download page, click the **Download** button.
This will download a .c2v file.

3 Send the downloaded file to your local OMRON representative and request the appropriate license. The corresponding .v2c file will be sent in return.

4 Upon receipt of the .v2c file, select the **Licensing** tab and choose the **Upload** option from the left pane.



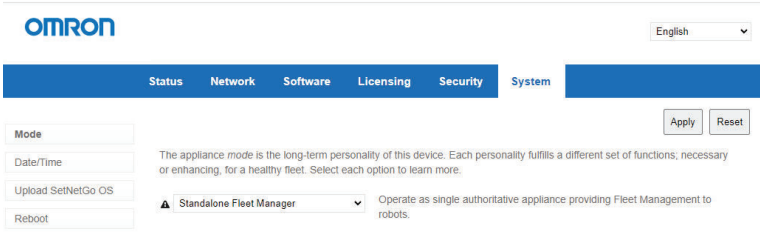
5 Click **Choose File** and select the appropriate .v2c file.

6 Click **Upload File**.
Once a valid license is activated, SetNetGo will initiate the requested mode on the Virtual Fleet Manager. Refer to *3-5 System Mode Configuration* on page 3-11 for more information on selecting the system mode.

3-5 System Mode Configuration

Configure the system mode as follows:

1 In the SetNetGo web interface, click the **System** tab.

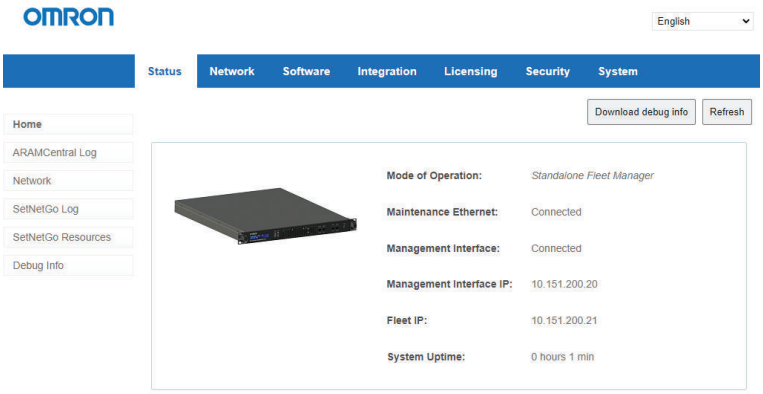


2 Click **Mode**.

3 Select **Standalone Fleet Manager** as the operating mode in the dropdown list.

4 Click **Apply**.

The Virtual Fleet Manager will reboot. The chosen system mode should then be shown by clicking on the **Status** tab, clicking the **Home** button, and viewing *Mode of Operation*. Successful completion of this procedure will allow modifications to the Fleet interface configuration.



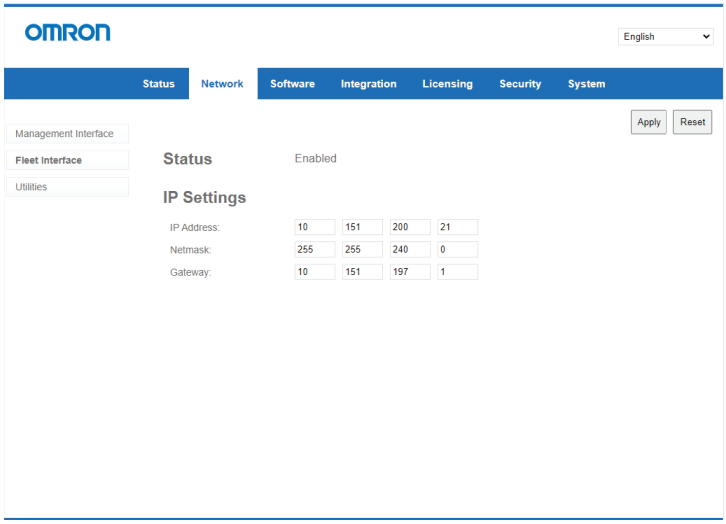
3-6 Fleet Interface Configuration Procedure

To configure the Fleet interface, the following is required:

- A dedicated static IP address to assign to the Fleet interface port
  This IP is allowed, but not required, to be on the same subnet as the Management address. Do not use 1.2.3.4; that address is permanently assigned to the Maintenance port.
- The subnet mask for the network that the fleet will use
- The IP address of the network gateway

Configure the Fleet interface network connection as follows:

1 In the SetNetGo web interface, click the **Network** tab.



2 Click **Fleet Interface** and supply entries for the following:

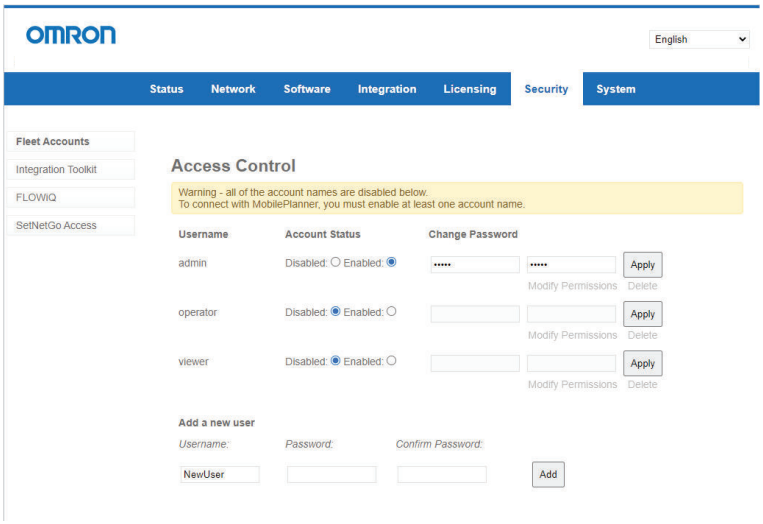
1) IP address
2) Subnet mask
3) Network Gateway IP address

3 Click **Apply** to complete this procedure.

3-7 Enable Access Control Procedure

SetNetGo's security settings allow access control for AMRs and the Virtual Fleet Manager via Mobile-Planner. This allows users to be restricted from performing specific tasks.
To configure access control:

1 Click the **Security** tab.



2 Click the associated radio button to enable or disable each account.

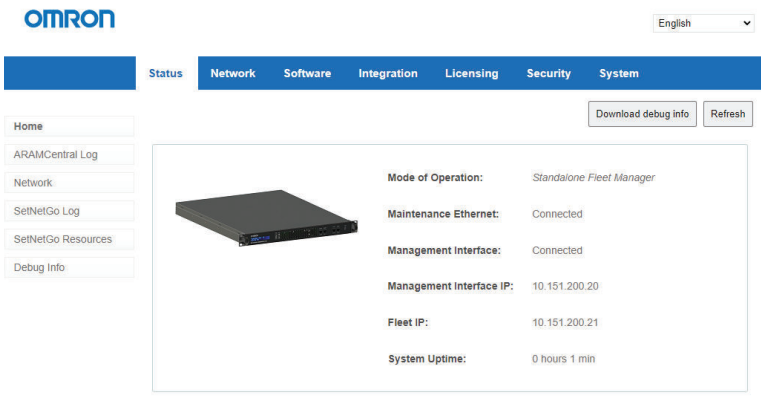
3 Supply a password for each enabled account.

4 Click **Apply** to complete this procedure .

3-8 System Status Verification Procedure

System status can now be verified by following the steps below.

1 Click the **Status** tab.



2 Verify *Mode of Operation* is the chosen mode.

3 Verify *Maintenance Ethernet* connection status.

4 Verify *Management Interface* connection status and *Management Interface IP* address.

5 Verify *Fleet IP* address.

6 Verify *System Uptime* to complete this procedure.

4

Troubleshooting

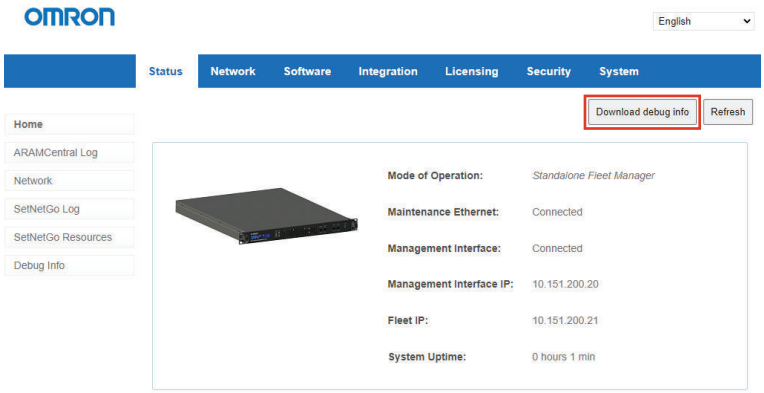
This section provides troubleshooting information.

4-1 Collecting Troubleshooting Information

Use the following procedure to retrieve the debugInfo file from SetNetGo.

1. Access the SetNetGo web interface of the Virtual Fleet Manager and open the **Status** tab. Click on the **Home** option in the left pane.

2. Click the **Download debug info** button.



3. Save the file and attach it to your support request.

Additional Information

The *Download debug info* button can also be found in SetNetGo at the Status - Debug Info area.

4-2 Failure Modes

Verifying connections and checking error logs should always be the first step in troubleshooting. If the corrective actions listed do not resolve the issue, contact OMRON support with hypervisor debug logs.

Failure Mode	Cause	Corrective Action
After install, network adapters are not reachable	Adapter type may be incorrect.	Verify virtual adapter types are E1000e. Refer to *Section 2 Virtual Machine Configuration & Creation* on page 2-1 for more information.
After install, certain features do not work.	Disk capacity may not be set high enough.	Verify hard disk has been allocated at least 512 GB. Refer to *Section 2 Virtual Machine Configuration & Creation* on page 2-1 for more information.
MobilePlanner cannot connect to Virtual Fleet Manager	Fleet Interface IP is not configured. License may have expired or is incorrectly configured.	• Ensure the network Fleet Interface IP is set. • Restart software.
Virtual Fleet Manager cannot connect to robot	Network connectivity issues may exist with the robot.	• Verify robot is powered on. • Verify IP address of robot is reachable. • Verify IP address of VFM is reachable. • Restart software.
Fleet performance degrades	Virtual CPU resources are insufficient.	• Restart software. • Increase hypervisor system resources such as CPU count or RAM. • Update software.
Fleet Manager log fills memory	Excess logs being generated by ongoing issue.	Restart software.
Fleet Manager fails to start	Configuration may have been changed recently. Hypervisor may be experiencing issues.	• Restart software. • Increase system resources such as CPU count or RAM. • Restore VM from backup or revert recent configuration change. • Update software. • Reinstall VM.
Fleet Manager stops issuing jobs	Connectivity issue between Fleet Manager and MobilePlanner	• Verify settings in hypervisor. • Restart software. • Increase system resources such as CPU count or RAM. • Restore VM from backup. • Update software. • Reinstall VM.
License failure	License may have expired.	Verify if licenses have expired and renew if necessary. Error logs will show a licensing error.
Install failure	Boot parameter set to BIOS instead of EFI.	Change boot parameter to EFI. Refer to *Section 3 Virtual Fleet Manager Installation & Configuration* on page 3-1 for more information.
VM fails to start after migration	Hypervisor may be experiencing issues.	• Restart software. • Ensure migrated VM is running. • Consult VMware documentation

5

Appendix

5-1 Network Port Allocation

Network ports are assigned as described below.

Port	Protocol	Category	Initiator to Recipient	Details
37	TCP	Intra-fleet Communications Ports. Used to broadcast configuration updates to AMRs, to dispatch job commands, and to share position and trajectory updates throughout the fleet.	AMR to Virtual Fleet Manager	Maintenance, Management and Fleet ports use this
1884	TCP			
8883	TCP			
5000	TCP/UDP			Fleet port uses this.
Range 10000 and up	UDP			For UDP Range 10000 connections and up, such as an AMR connecting to a Virtual Fleet Manager, this protocol grows with the number of robots. For best results, allocate at least twice as many UDP ports as there are AMRs in the fleet. For instance, a fleet of 20 AMRs should have an allocated range of 10000-10039.
7272	TCP/UDP			
5672	TCP	Integration Toolkit TCP Ports.	RabbitMQ AMQP	
8443	TCP		ITK REST	
5432	TCP		PostgreSQL	
443	TCP	Flow iQ External Ports (HTTPS)	Client PC to Virtual Fleet Manager	FLOW IQ is an optionally licensed monitoring and analytic tool providing information regarding fleet and AMR health and effectiveness.
	TCP	Configuration and Monitoring of Fleet. Used for MobilePlanner connections to Virtual Fleet Manager and AMRs for monitoring and configuration.	Client PC to Virtual Fleet Manager	Maintenance and Management ports use this.
Range 7272 and up	TCP/UDP		Client PC to Virtual Fleet Manager	This protocol uses as many ports as there are AMRs. Each AMR that connects uses the next available port ≥ 7272. For best results, allow a large number of ports, such as 7272-7999.
7272	TCP/UDP		Client PC to AMR	
Range 10000 and up	UDP		Virtual Fleet Manager appliance to client PC	This protocol uses as many ports as there are AMRs. Each AMR that connects uses the next available port ≥ 10000. For best results, allow a large number of ports, such as 10000-10999.
10000	UDP		AMR to Client PC	

Port	Protocol	Category	Initiator to Recipient	Details
7171	TCP	Job Monitoring and Submission (ARCL) Interface. Used for managing jobs on the Virtual Fleet Manager appliance. These are typically submitted from a Warehouse Management System (WMS) or Manufacturing Execution System (MES).	WMS/MES to Virtual Fleet Manager	ARCL Server: if enabled in the configuration, this port is open on the Virtual Fleet Manager and accepts unlimited incoming connections. The port number is configurable. (This port might be available on the AMR, depending on the application.)
Configurable port #	TCP		Virtual Fleet Manager to WMS/MES	Outgoing ARCL Connection: if enabled in the configuration, then the Virtual Fleet Manager initiates an outgoing connection to the specified hostname and TCP port number.
123	TCP	Optional.	Virtual Fleet Manager appliance to NTP server	If you enable a Network Time Protocol (NTP) client Virtual Fleet Manager Appliance, the Virtual Fleet Manager Appliance attempts to set its clock from the network time server at the specified IP address. (This function is available on the AMR, if you do not use a client Virtual Fleet Manager Appliance.)

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 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 ASIA PACIFIC PTE. LTD.
438B Alexandra Road, #08-01/02 Alexandra
Technopark, Singapore 119968
Tel: (65) 6835-3011 Fax: (65) 6835-2711

OMRON (CHINA) CO., LTD.
Room 2211, Bank of China Tower,
200 Yin Cheng Zhong Road,
PuDong New Area, Shanghai, 200120, China
Tel: (86) 21-5037-2222 Fax: (86) 21-5037-2200

Authorized Distributor:

Cat. No. I695-E-01 1023

24953-000 A