



Software manual
moneo|vAppliance
QVA200

GB

incl. appliance management system (AMS)
V1.13 or higher

Contents

1	Preliminary note	5
1.1	Legal and copyright information	5
1.2	Open source information	5
1.3	Purpose of the document	6
1.4	Symbols used	6
1.5	Warnings	6
2	Safety instructions	7
3	Intended use	8
4	Installation	9
4.1	Licensing	9
4.1.1	Impact of licensing on the AMS	9
4.2	Setup of vAppliance	9
4.2.1	Requirements / Preparation	9
4.2.2	Import to VMware ESXi	10
4.2.3	Import to VMware vCenter	10
4.2.4	Import to Microsoft Hyper-V	11
4.2.5	Set-up of moneo vAppliance	12
4.2.5.1	Adapting the hostname	12
4.2.5.2	Adapting the IP address - Ethernet interface 2	13
4.2.5.3	Set-up completed	13
4.2.6	Opening the appliance management system (AMS)	13
4.2.6.1	Requirements	13
4.2.6.2	Initial login via the browser	13
4.2.7	Opening moneo	14
4.3	Standard IP addresses	14
4.4	Default host name	14
4.5	Standard network communication	15
5	Function	16
5.1	Access options	16
6	Web interface	17
6.1	Open guest view	17
6.2	Login to AMS	17
6.2.1	First-time login	17
6.2.2	Login	17
6.2.3	Logout	17
6.2.4	Changing the password	18
6.2.5	Resetting the password	18
6.2.6	Password requirements	18
6.2.7	Protection against brute-force attacks	18
6.3	System status	19
6.3.1	Display system load	19
6.3.2	Managing moneo services	19
6.3.3	Managing System Services	19
6.3.4	Displaying system information	20
6.4	Configuration	20
6.4.1	Changing the network settings	20
6.4.2	Setting DHCP	21
6.4.3	Changing the hostname	21
6.4.4	Setting up FQDN for access to moneo	21
6.4.5	Activating proxy servers	21
6.4.6	Adding proxy exclusions	21
6.4.7	Removing proxy exceptions	22
6.4.8	Deactivating proxy servers	22
6.4.9	Enabling and setting the time server	22
6.4.10	Deleting the time server	23
6.4.11	Disabling the a time server	23
6.4.12	Setting the time zone	23

6.4.13	Setting date and time	24
6.4.14	Adding a USB memory device	24
6.4.15	Denying a USB memory device	24
6.4.16	Removing a USB memory device	24
6.4.17	HTTPS/TLS certificates	25
6.4.17.1	Adding your own HTTPS/TLS certificate	25
6.4.17.2	Removing your own HTTPS/TLS certificate	26
6.4.17.3	Displaying information about the used HTTPS/TLS certificate	26
6.4.18	Shutting down / rebooting the device	26
6.5	Update	27
6.5.1	Enabling automatic checks for updates	27
6.5.2	Disabling automatic checks for updates	27
6.5.3	Manual search for available updates	27
6.5.4	Installing online updates	27
6.5.5	Installing offline updates	28
6.6	Saving and restoring	28
6.6.1	Creating a manual backup	28
6.6.2	Copying backup files to a USB memory device	29
6.6.3	Configuring a backup target	29
6.6.4	Downloading backup passwords	29
6.6.5	Restoring a backup from the backup destination	30
6.6.6	Restoring a backup copied manually to USB	30
6.6.7	Deleting a backup	31
6.6.8	Enable automatic backup	31
6.6.9	Disable automatic backup	31
6.7	Maintenance	31
6.7.1	Determining support-related information	31
6.7.2	Enabling remote access (SSH)	32
6.7.3	Disabling remote access (SSH)	32
6.7.4	Enabling ifm remote support	32
6.7.5	Disabling ifm remote support	32
6.7.6	Download logfiles	33
6.7.7	Show logfiles	33
6.7.8	Show live log	33
7	AMS console	34
7.1	Local access	34
7.1.1	Requirements	34
7.1.2	Logging in for the first time	34
7.1.3	Login	34
7.2	Remote access	34
7.2.1	ifm service account	35
7.2.2	Requirements	35
7.2.3	Accessing the AMS console via SSH	35
7.2.4	Login	35
7.3	Displaying system information	35
7.3.1	Display host information	35
7.3.2	Display network information	36
7.3.3	Showing moneo service information	36
7.4	System configuration	36
7.4.1	Adapting the host name	36
7.4.2	Changing the password	37
7.4.3	Changing the keyboard layout	37
7.4.4	Enabling Remote Support (SSH)	37
7.4.5	Disabling Remote Support (SSH)	38
7.4.6	Adjust network settings	38
7.4.7	Upgrading the virtual hard disk	39
7.5	Restart the required moneo service	39
7.6	Resetting the AMS administrator password	39
7.7	Reset the system to factory settings	40
7.8	Reboot the system	40
7.9	Shut down the system	40

7.10 Logout.....	40
------------------	----

1 Preliminary note

1.1 Legal and copyright information

© All rights reserved by ifm electronic gmbh. No part of these instructions may be reproduced and used without the consent of ifm electronic gmbh.

All product names, pictures, companies or other brands used are the property of the respective rights owners.

- Microsoft® is the property of Microsoft Corporation, USA
- Windows® is the property of Microsoft Corporation, USA
- Linux® is the registered trademark of Linus Torvalds in the USA and in other countries.
- VMware ESXi is the property of VMware, Inc., USA
- VMware is the property of VMware, Inc., USA
- Microsoft Hyper-V is the property of Microsoft Corporation, USA
- IO-Link® is the property of PROFIBUS Nutzerorganisation e.V., Germany
- PHOENIX CONTACT is the property of Phoenix Contact GmbH, Germany
- autosen is the property of autosen GmbH, Germany
- Google Chrome is a registered trademark of Google LLC, USA.
- Mozilla Firefox is a registered trademark of the Mozilla Foundation, USA.
- Microsoft Edge is a registered trademark of Microsoft Corporation, USA.

1.2 Open source information

This product can contain Free Software or Open Source Software from various software developers which is subject to the following licenses: General Public License version 1, version 2 and version 3 (General Public License version 3 in conjunction with the GNU Compiler Collection Runtime Library Exception version 3.1), Lesser General Public License version 2.1, Lesser General Public License version 3, Berkeley Software Distribution (BSD-2-Clause, BSD-3-Clause, BSD-4-Clause), MIT-License (MIT), Python Software Foundation License 2.0, Pearl Artistic License and Artistic License 2.0, Microsoft Public License, Apache Software License Version 1.0, 1.1 und 2.0, ISC License, libpng License, zlib License, the Academic Free License version 2.1, Mozilla Public License 2.0.

For the components subject to the General Public License in their respective versions the following applies:

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation. If version 1 applies to the software: either version 1 of the License or (at your option) any later version; if version 2 (or 2.1) applies to the software: either version 2 (or 2.1) of the License or (at your option) any later version; if version 3 applies to the software: either version 3 of the License or (at your option) any later version. The following disclaimer of the software developers applies to the software components that are subject to the General Public License or the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License and the GNU Lesser General Public License for more details.

The responsibility of ifm electronic gmbh for ifm products, in the case of product-specific software, remains unaffected by the above disclaimer. Please note that the firmware for the ifm products is in some cases provided free of charge. The price of the ifm products has then to be paid for the respective device itself (hardware) and not for the firmware. For the latest information on the license agreement for your product please visit www.ifm.com

For binaries that are licensed under any version of the GNU General Public License (GPL) or the GNU LGPL or Mozilla Public License 2.0 you may obtain the complete corresponding source code of the GPL software from us by sending a written request to: opensource@ifm.com or to ifm electronic gmbh, Friedrichstraße 1, 45128 Essen, Germany.

We charge €30 for each request. Please write “source for product Y” in the memo line of your payment. Your request should include (i) the name of the covered binary, (ii) the name and the version number of the ifm product, (iii) your name and (iv) your return address.

The following applies to components covered by the General Public License in their respective versions. This offer is valid to anyone in receipt of this information. This offer is valid for at least three years (from the date you received the GPL/LGPL covered code).

1.3 Purpose of the document

This software manual describes the moneo|appliance management system (AMS) within a virtual appliance and the setup process of a virtual appliance for moneo (moneo|vAppliance).

► For better understanding, use this manual along with the opened software.

1.4 Symbols used

- ✓ Requirement
- Instructions
- ▷ Reaction, result
- [...] Designation of keys, buttons or indications
- Cross-reference
-  Important note
Non-compliance may result in malfunction or interference.
-  Information
Supplementary note

1.5 Warnings

Warnings indicate the possibility of personal injury and damage to property. This enables safe product handling. Warnings are graded as follows:



WARNING

Warning of serious personal injury

▷ If the warning is not observed, fatal and serious injuries are possible.



CAUTION

Warning of minor to moderate personal injury

▷ If the warning is not observed, minor to moderate injuries are possible.

ATTENTION

Warning of damage to property

▷ If the warning is not observed, damage to property is possible.

2 Safety instructions

- Read this document before setting up the product and keep it during the entire service life.
- The product must be suitable for the corresponding applications without any restrictions.
- Only use the product for its intended purpose (→ Intended use).
- If the operating instructions or the technical data are not adhered to, personal injury and/or damage to property may occur.
- The manufacturer assumes no liability or warranty for any consequences caused by tampering with the product or incorrect use by the operator.
- There is an encrypted ifm service account that is used for assistance in the event of support/errors.
(→ [ifm service account](#)  35)

3 Intended use

The moneo|appliance management system (AMS) is used for maintenance and configuration of the moneo|vAppliance.

The vAppliance is used for the operation of moneo in a virtualisation environment.

4 Installation

4.1 Licensing



You can find further information on licensing in the moneo installation instructions.

4.1.1 Impact of licensing on the AMS

Licence “vAppliance (FREE)”

The vAppliance is operated without a licence and used with up to 25 info points:

- The AMS can be used without restrictions.

The vAppliance is operated without a licence and used with more than 25 info points:

- A 30-day trial period begins, during which a “vAppliance (QVA200)” licence must be purchased in order to continue using all functions.
 - The AMS can be used without restrictions during the trial period.
- If the trial period expires before installation of a licence, the AMS can be used with restrictions:
 - The “Backup and restore” functions can no longer be used in the AMS.
 - The function for updating the system can no longer be used in the AMS.
- After installing the “vAppliance (QVA200)” licence, the AMS can be used without restrictions.

Licence “vAppliance (QVA200)”

The vAppliance is operated with licence “vAppliance (QVA200)”:

- The AMS can be used without restrictions, regardless of the number of info points used.

4.2 Setup of vAppliance

4.2.1 Requirements / Preparation

- ✓ A virtualisation environment is available.
Supported:
 - VMware ESXi version 7.0 or higher
 - Microsoft Hyper-V
- ✓ The following system resources must be available for the operation of the vAppliance:

In general

- Graphics resolution (min.): 1920 x 1080
- Network cards: 2x Ethernet 1 Gbit/s
- Hard disk (min.): 128 GB

- ✓ For the operation of the vAppliance, the following system resources must be available depending on the performance class:

Performance class S

- CPU clock rate (min.): 2.3 GHz
- Number of CPU cores (min.): 4
- RAM (min.): 8 GB

Performance class L

- CPU clock rate (min.): 3.0 GHz
- Number of CPU cores (min.): 8
- RAM (min.): 32 GB

► Download the vAppliance template (zip file) from www.ifm.com.



Ideally, the installation is done by or with the help of the IT department or an IT administrator.

4.2.2 Import to VMware ESXi

- Unzip the vAppliance template (zip file).
- Log into the ESXi web interface at `https://<ESXi-IP or host name>/ui/`
- Click on the [Virtual machine] tab in the [Navigator].
- Then click on [Create/Register VM].
 - ▷ The window [New virtual machine] appears.
- Select the item [Deploy a virtual machine from an OVF or OVA file] under [Select creation type] and confirm with [Next].
- Enter a name for the virtual machine under [Select OVF and VMDK files] and import the unzipped files (.ovf .vmdk .nvram). Then confirm with [Next].
- Select the storage location for the vAppliance under [Select storage] and confirm with [Next].
- Assign the network cards for `ETH1` and `ETH2` and select [Disk Provisioning] under [Deployment options] and confirm with [Next].



Provisioning is possible in "Thin" and "Thick". "Thick provisioned" is recommended.

- Check the settings under [Ready to complete]. If everything is correct, confirm with [Finish].
 - ▷ The VM of the vAppliance is imported.
 - ▷ The status is displayed below.
- After successful import select the vAppliance and start it with [Power on].
- Click on [Console] to open the vAppliance console.
 - ▷ A window with the AMS console of the vAppliance appears.
- Then continue with the steps in section [Set-up of moneo/vAppliance \(→ 12\)](#).

4.2.3 Import to VMware vCenter

- Unzip the vAppliance template (zip file).
- Log into the vSphere Client at `https://<vSphere IP or hostname>/ui/`
- For installation on a specific host/cluster: In the overview on the left, switch to the host view and select the required host/cluster.
 - or-
 - For installation in a specific folder: In the overview on the left, switch to the folder view and select the required folder.
- Click on [Deploy OVF Template...].
- Select the field [Local file] and click on [Upload files].
- In the new window, select the downloaded and unzipped files (.ovf .mf .vmdk .nvram) and import them.
- Continue by clicking on [Next].
- Assign a name for the VM and allocate a storage space.



Provisioning is possible in "Thin" and "Thick". "Thick provisioned" is recommended.

- ▶ Confirm by clicking on [Next].
- ▶ Select the host/cluster that is to provide the computing power for the vAppliance.
- ▶ Continue by clicking on [Next].
- ▶ Check the details and then confirm with [Next].
- ▶ On the next page, select a storage location and confirm with [Next].



Only storage locations that have the status [Compatible] in the column [Storage Compatibility] can be selected.

- ▶ For `ETH1_sensor-network` at [Destination Network], assign the appropriate network.
- ▶ For `ETH2_it-network` at [Destination Network], assign the appropriate network.
- ▶ Continue by clicking on [Next].
- ▶ On the last page, all settings can be checked. Then click on [Finish] to import the vAppliance.
- ▶ The current import status can be tracked below.
- ▶ When the import is complete, select the created VM and switch it on by clicking on [Start].
- ▶ Open the console of the vAppliance with [Launch remote console].
- ▶ Then continue with the steps in section [Set-up of moneo/vAppliance \(→ 12\)](#).

4.2.4 Import to Microsoft Hyper-V

- ▶ Unzip the vAppliance template (zip file).
- ▶ Open the Hyper-V Manager.
- ▶ Select the required machine on which vAppliance is to be operated in the topology of the Hyper-V Manager and click on it with the right mouse button.
- ▶ Select [Import Virtual Machine...] in the context menu.
- ▶ Select the vAppliance template in the new window. Select the entire folder in which the vAppliance files are located for this purpose.
- ▶ Confirm the selection and go to the next page with [Next] .
- ▶ Select the vAppliance template under [Select Virtual Machine] and confirm with [Next].
- ▶ Select the required import type under [Choose Import Type] and confirm with [Next].
- ▶ The folders in which to store the VM can be selected under [Choose Destination]:
For the default folders: confirm the page with [Next].
-or-
Use custom folders: select the [Store the virtual machine in a different location] field and enter the required folders. Confirm by clicking on [Next].
- ▶ Enter the required storage location for the vAppliance under [Choose Storage Folders] and confirm with [Next].
- ▶ The previously selected settings are displayed for you to check under [Summary]. If they are correct, confirm with [Finish] and the VM is created.
- ▶ After the import, select the VM you have just created in the [Virtual Machines] table and start it by clicking on [Start] in the [Actions] table.
- ▶ Click on [Connect...] in the [Actions] table to open the window with the vAppliance console.
- ▶ Then continue with the steps in the section [Set-up of moneo/vAppliance \(→ 12\)](#).

4.2.5 Set-up of moneo|vAppliance



The different menu items in the appliance management system can be selected using the keyboard. Example: The keyboard shortcut [C] opens [C) Configure the system].

- ▶ Enter the login details and confirm with [Enter].



User name: administrator
Password: vAppliance1969!

- ▷ If the login details are correct, the [Simple keyboard configuration menu] appears.
- ▶ Select the corresponding keyboard layout and confirm by clicking on [OK].
- ▶ Confirm the successful change by clicking on [OK].
 - ▷ Prompt to change the password appears.
- ▶ Change the password when signing in for the first time.

Password requirements:

- At least 8 characters
- Must contain:
 - at least one upper case letter
 - at least one lower case letter
 - at least one number
 - at least one special character
- ▶ Repeat the password and confirm by clicking on [OK].
- ▶ After assigning the new password, log in again with new login data.
- ▷ The [Main menu] of moneo|vAppliance is displayed.

4.2.5.1 Adapting the hostname

The default host name of the moneo|vAppliance is: moneo-vappliance-XXXXXXX.

When the user has logged in, the default host name can be viewed at: [System status] > [System information]



The last 7 digits of the host name are generated during the import of vAppliance.



The host name can be adapted when signing in for the first time or later by following the below steps.

- ▶ Note that the entry is case sensitive.
- ▶ Open the [Main menu].
- ▶ Select [C) Configure the system].
 - ▷ The [Configuration menu] opens.
- ▶ Select [H) Change the hostname].
 - ▷ [Hostname change] opens.
 - ▷ The current host name is displayed in the field [Specify the new hostname].
- ▶ Change the host name using the keyboard and select [<Ok>].
- ▷ The host name is saved and the interface [Host name change] is closed.
- ▶ Select [R) Return to the previous menu] to go back to the previous menu environment.

4.2.5.2 Adapting the IP address - Ethernet interface 2

- ▶ Open the [Main menu].
- ▶ Select [C) Configure the system].
 - ▷ [Configuration menu] opens.
- ▶ Select [N) Configure the network].
 - ▷ [Network configuration] opens.
- ▶ Select [I) IT network (ETH 2)].
- ▶ Select [U) Use DHCP].
- ▶ Click on [Enter] to change the entry from [yes] to [no].
- ▶ Select [I) Set the IP address].
 - ▷ [Network (ip)] opens.
- ▶ Enter the new IP address using the keyboard and select [Ok].
 - ▷ [Network configuration] opens.



Now the settings must also be made for the network mask, gateway and the DNS servers. Once all settings have been made, they must be permanently saved.

- ▶ Select [S) Save the configuration].
 - ▷ The message [The network configuration was successfully changed] is displayed.
- ▶ Confirm the message with [Ok].
- ▶ Select [R) Return to the previous menu] several times to return to the [Main menu].
 - ▷ The system is configured and available via web interface.

4.2.5.3 Set-up completed

- ▶ Select [X) Exit].
 - ▷ The [Main menu] is closed.

The following systems are available via the web browser:

- appliance management system: [Opening the appliance management system \(AMS\) \(→ 13\)](#)
- moneo: [Opening moneo \(→ 14\)](#)

4.2.6 Opening the appliance management system (AMS)

4.2.6.1 Requirements

Device (e.g. PC) connection to the moneo|vAppliance. This device must be connected to the same network as the Ethernet interface (ETH 2) of the moneo|vAppliance.

For access to the appliance management system (AMS), a suitable web browser must be installed on the user's own PC.

- ▶ Use a recommended browser: Google Chrome (version 93 or higher), Mozilla Firefox (version 78 or higher), Microsoft Edge (version 93 or higher).

4.2.6.2 Initial login via the browser

- ▶ Open the URL of the appliance management system in your browser.
 - `https://<IP or hostname>/ams`
 - ▷ General status information is displayed.

- ▶ Click on the symbol .
- ▶ Log in as administrator with the login details assigned in the AMS console.



If the user has not previously logged in to the AMS console, use the following login details:

User: administrator
Password: vAppliance1969!

- ▶ Enter the login details and confirm with [Login].
 - ▷ Prompt to change the password appears.
- ▶ Change password according to the requirements below.
- ▷ The appliance management system with its entire functional scope is displayed.

Password requirements:

- At least 8 characters
- Must contain:
 - at least one upper case letter
 - at least one lower case letter
 - at least one number
 - at least one special character



After set-up:

- ▶ Download the backup passwords as soon as possible and store them securely. [Downloading backup passwords](#) (→  29)

4.2.7 Opening moneo

- ▶ Open moneo in your browser.
`https://<IP or hostname>`
- ▷ The licencing wizard is displayed.



You can find further information on licensing in the moneo installation instructions.

4.3 Standard IP addresses

moneo|vAppliance (standard)

Ethernet interface	Description	Standard IP address	Subnet mask
Eth1	OT interface (sensor network)	192.168.0.100	255.255.255.0
Eth2	IT interface	DHCP	DHCP

4.4 Default host name

The default host name of the moneo|vAppliance is: moneo-vappliance-XXXXXXX.

When the user has logged in, the default host name can be viewed at: [System status] > [System information]



The last 7 digits of the host name are generated during the import of vAppliance.

4.5 Standard network communication

For communication in the network, the AMS needs access to various addresses in the network. More detailed information can be found in the "Security Whitepaper" document.

5 Function

The AMS allows the user to carry out basic maintenance tasks for the moneo|vAppliance, e.g.:

- Reading status information for hardware and software
- Setting the network configuration and hostnames
- Setting the date and time
- Rebooting or shutting down the moneo|vAppliance
- Monitoring and restarting services
- Importing software updates
- Displaying contact details for technical support.
- Setting the access for remote support
- Reading log files
- Data backup

5.1 Access options

The AMS offers the following access options with different functionalities:

1. Web interface: Offers the full range of functions and can be used via a browser.
2. Console: Offers basic functions for interfaces, accesses, etc. that are required for initial setup as well as subsequent administrative activities.

6 Web interface

The web interface offers the following access options:

1. Guest view:
 - Restricted access; Limited to status information and system information
2. Registered with AMS:
 - Unrestricted access to all status and system information
 - Unrestricted access to all settings of the system

6.1 Open guest view

- ✓ The installation and connection of the moneo|vAppliance are completed.
- ✓ Use a recommended browser: Google Chrome (version 93 or higher), Mozilla Firefox (version 78 or higher), Microsoft Edge (version 93 or higher).
- ✓ The device with the browser (e.g. PC) is connected to the same network as the Ethernet interface `eth2` of the moneo|vAppliance.

► Open the URL of the moneo|vAppliance in the browser: `https://<IP or host name>/ams`



Please observe the following when opening it for the first time:

IP address It was assigned during setup or automatically assigned by the DHCP server.

Host name: → Chapter [Default host name](#) (→ [14](#))

▷ The guest view is open.

6.2 Login to AMS

6.2.1 First-time login

- ✓ The guest view is open. (→ [Open guest view](#) [17](#))
- ✓ Standard login data:
 - User: administrator
 - Default password: vAppliance1969!
- Click on the ☺ icon (top left) to log in as `administrator` with the above standard login details.
 - ▷ The user is prompted to change the default password.
- Change the password according to the [Password requirements](#) (→ [18](#)).
- ▷ The password has been changed.
- ▷ The AMS offers the full range of functions.

6.2.2 Login

- ✓ The guest view is open. (→ [Open guest view](#) [17](#))
- Click on the ☺ icon (top left) to log in as administrator.
- ▷ The AMS offers the full range of functions.

6.2.3 Logout

- ✓ The user is logged in to the AMS. (→ [Login to AMS](#) [17](#))

- ▶ Click on the  icon (top left)
- ▶ Log out by clicking on  [Logout].
- ▷ The guest view is open.

6.2.4 Changing the password

- ✓ The user is logged in to the AMS. ([→ Login to AMS](#)  17)
- ▶ Click on the  icon (top left)
- ▶ Click on  [Change password] to change the password. [Password requirements](#) ([→](#)  18)
- ▷ The password has been changed.

6.2.5 Resetting the password

- ✓ The guest view is open. ([→ Open guest view](#)  17)
- ▶ Click on the  icon (top left)
 - ▷ The input mask for the login appears.
 - ▷ The button [Forgot password?] is below the input mask.
- ▶ Click on the [Forgot password?] button.
- ▶ In the input field [Username], enter the user name `administrator`.
- ▶ Enter the new password in the input field [New password]. [Password requirements](#) ([→](#)  18)
- ▶ In the input field [Serialnumber], enter the serial number of the moneo|vAppliance.
 The serial number can be viewed on the console's start screen or, if logged in, at [System information]. ([Displaying system information](#) ([→](#)  20))
- ▶ Click on the [Change password] button.
- ▷ The new password will be immediately active.

6.2.6 Password requirements

- Minimum length: 8 characters
- Must contain:
 - at least one upper case letter
 - at least one lower case letter
 - At least one number
 - At least one special character

6.2.7 Protection against brute-force attacks

To protect against brute-force attacks, the AMS implements a function that fends off potential attackers. Attempts by an attacker to gain access with guessed user data are blocked after 5 attempts. Afterwards, no user login to the AMS is possible for 5 minutes, even with correct user data. A display informs the user about the blockade and the remaining blockade duration.

6.3 System status

6.3.1 Display system load

- ✓ The user is logged in to the AMS. ([→ Login to AMS](#)  17)
- ▶ In the [System status] section, show the system load for various system components on the [Resource monitoring] tab:
 - CPU utilisation in %
 - Total and used RAM in % and GB
 - Network load in Mbit
 - Total and used hard disk space in % and GB for all partitions



The displayed values for system load are read and displayed statically at the time of page setup.

An update is only performed when the page is reloaded, e.g. by pressing the key [F5].

6.3.2 Managing moneo services

- ✓ The user is logged in to the AMS. ([→ Login to AMS](#)  17)
- ✓ In the [System status] section, the [moneo services] tab shows the moneo services in their individual states.
- ▶ Clicking on  opens a menu with the following options:
 - [Restart all services]
 - [Start all services]
 - [Stop all services]
- ▶ Click on one of the menu items to start, stop or restart all moneo services simultaneously.
- ▶ Click on one of the buttons in the [Actions] column next to the respective moneo service to perform the following individual actions:
 - Display the memory usage of the service with .
 - Start the service with .
 - Stop the service with .
 - Restart the service with .

ATTENTION

Starting and stopping services

- ▷ Influence on the proper functioning of the running system.
- ▷ Data loss is possible.
- ▶ Recommendation: Only start and stop services after consultation with the ifm service.

6.3.3 Managing System Services

- ✓ The user is logged in to the AMS. ([→ Login to AMS](#)  17)
- ✓ In the [System status] section, the [System services] tab shows the moneo services in their individual states.

► Click on one of the buttons in the [Actions] column to perform the following actions:

- Start the service with ►.
- Stop the service with ■.
- Restart the service with ↺.

ATTENTION

Starting and stopping services

- ▷ Influence on the proper functioning of the running system.
- ▷ Data loss is possible.
- Recommendation: Only start and stop services after consultation with the ifm service.

6.3.4 Displaying system information

► In the [System status] area, select the [System information] tab.

▷ General status information is displayed:

- System type
- Serial number
- Installed version of the moneo software
- Installed version of the AMS
- Installed version of the moneo|vAppliance
- Installed version of the License Gateway



If you have to reset a password:

- Find the serial number on the console's start screen.

6.4 Configuration

6.4.1 Changing the network settings

✓ The user is logged in to the AMS. (→ [Login to AMS](#) 17)

► In the section [Configuration] > [Network], enter the following network settings for the network interfaces `Eth1` and `Eth2` separately.

Input box	Description
[IP address]	IP address
[Netmask]	Subnet mask
[Gateway]	Standard gateway
[DNS]	DNS server (separate multiple servers with commas)

► Click on [Save] to save the changes.

▷ The network settings will be stored.



► Adjust the DNS alias according to the set IP address to `Eth1` and the set host name.



Interference with the function of the current system when the network settings are changed.

► Assign the IP address and host name in a network (subnet) only once.

6.4.2 Setting DHCP

- ✓ The user is logged in to the AMS. ([→ Login to AMS](#)  17)
- ▶ Configure the following network settings for the network interfaces `Eth1` and `Eth2` separately.
- ▶ Click on the [DHCP] button under [Configuration] > [Network] in the section of the required network interface.
- ▶ Click on [Save] to save the changes.
- ▷ The interface has been changed to DHCP mode.

6.4.3 Changing the hostname

- ✓ The user is logged in to the AMS. ([→ Login to AMS](#)  17)
- ▶ Change the host name under [Configuration] > [Network] in the [HOSTNAME] section.
- ▶ Click on the [Save] button.
- ▷ The hostname has been changed.
-  ▶ Adjust the DNS alias according to the set IP address to `Eth1` and the set host name.
-  Interference with the function of the current system when the network settings are changed.
- ▶ Assign the IP address and host name in a network (subnet) only once.

6.4.4 Setting up FQDN for access to moneo

-  The use of FQDN is optional.
- Domain and alias do not have to be entered.
- ✓ The user is logged in to the AMS. ([→ Login to AMS](#)  17)
- ▶ At [Configuration] > [Network] enter the domain in the [Domain] field.
- ▶ Enter the required aliases in the table [Alias name].
- ▶ If necessary, add further aliases by clicking on the [+] icon.
- ▶ Click [Save] to save the settings.
- ▷ Access to moneo is now possible via the assigned aliases.

6.4.5 Activating proxy servers

- ✓ The user is logged in to the AMS. ([→ Login to AMS](#)  17)
- ▶ Under [Configuration] > [Proxy settings] enable [Use proxy].
- ▶ Enter the proxy data for the respective protocol ([http] and [https]) or activate [Use same proxy server for all protocols] to use the same proxy server for all protocols.
- ▶ If a user name and password are required for the proxy server: Enable [Use authentication] and enter the user information [User name] and [Password].
- ▶ If no user name and password are required for the proxy server: Disable [Use authentication].
- ▶ Click [Save] to save and apply the proxy server settings.

6.4.6 Adding proxy exclusions

- ✓ The user is logged in to the AMS. ([→ Login to AMS](#)  17)

- ▶ Under [Configuration] > [Proxy settings] in the section [Proxy exclusions], click on the + icon.
- ▶ Enter the proxy exceptions and click [Save].
- ▷ The proxy will no longer be applied to the added addresses.

6.4.7 Removing proxy exceptions

- ✓ The user is logged in to the AMS. ([→ Login to AMS](#)  17)
- ▶ Under [Configuration] > [Proxy settings] in the section [Proxy exclusions], remove the desired addresses by clicking on the  icon.
- ▶ Click [Save] to save the settings.

6.4.8 Deactivating proxy servers

- ✓ The user is logged in to the AMS. ([→ Login to AMS](#)  17)
- ▶ Under [Configuration] > [Proxy settings] disable [Use proxy].
- ▶ Click [Save] to save the settings.
- ▷ No proxy is used.

6.4.9 Enabling and setting the time server



The current time of an internal or external time server can be adopted using the Network Time Protocol (NTP).

ATTENTION

The moneo services are restarted when the settings are saved. During this process, moneo and the moneo|appliance management system are unavailable for some time.

- ▷ No data is recorded during the restart.
- ▷ Data loss is possible.
- ▶ Restart the moneo services at an uncritical moment, e.g. during a standstill.

- ✓ The user is logged in to the AMS. ([→ Login to AMS](#)  17)
- ▶ Under [Configuration] > [Date & Time] select the option [Synchronise with NTP-Server].
- ▶ In the [NTP-Server] section under [Enter NTP server address] enter the IP address of the requested NTP server.
- ▶ If there are several NTP servers, click on + to add and configure an additional NTP server.
- ▶ Click on [Save].
 - ▷ The window [Time changes require restart] appears.
- ▶ Click [Save and restart] to apply the settings and restart the moneo services.
- ▷ The NTP servers are set.

6.4.10 Deleting the time server

ATTENTION

The moneo services are restarted when the settings are saved. During this process, moneo and the moneo|appliance management system are unavailable for some time.

- ▷ No data is recorded during the restart.
- ▷ Data loss is possible.
- ▶ Restart the moneo services at an uncritical moment, e.g. during a standstill.

- ✓ The user is logged in to the AMS. ([→ Login to AMS](#)  17)
- ✓ The section [Configuration] > [Date & Time] is open.
- ▶ In the [NTP-Server] section, click on  in the [Actions] column to delete the corresponding NTP server.
- ▶ Click on [Save].
 - ▷ The window [Time changes require restart] appears.
- ▶ Click [Save and restart] to apply the settings and restart the moneo services.
- ▷ The corresponding NTP server will be deleted.

6.4.11 Disabling the a time server

- ▶ To disable an NTP server, set the date and time manually. [Setting date and time](#) ([→](#)  24)

6.4.12 Setting the time zone

ATTENTION

The moneo services are restarted when the settings are saved. During this process, moneo and the moneo|appliance management system are unavailable for some time.

- ▷ No data is recorded during the restart.
- ▷ Data loss is possible.
- ▶ Restart the moneo services at an uncritical moment, e.g. during a standstill.

- ✓ The user is logged in to the AMS. ([→ Login to AMS](#)  17)
- ✓ The currently set time zone is indicated under [Configuration] > [Date & Time].
- ▶ Under [Configuration] > [Date & Time], select the required time zone from the list.
- ▶ Click on [Save].
 - ▷ The window [Time changes require restart] appears.
- ▶ Click [Save and restart] to apply the settings and restart the moneo services.
- ▷ The time zone has been set.

6.4.13 Setting date and time

ATTENTION

The moneo services are restarted when the settings are saved. During this process, moneo and the moneo|appliance management system are unavailable for some time.

- ▷ No data is recorded during the restart.
- ▷ Data loss is possible.
- ▶ Restart the moneo services at an uncritical moment, e.g. during a standstill.

✓ The user is logged in to the AMS. ([→ Login to AMS](#)  17)

- ▶ Under [Configuration] > [Date & Time] select the option [Manual time setting].
- ▶ Set the date and time.
- ▶ Click on [Save].
 - ▷ The window [Time changes require restart] appears.
- ▶ Click [Save and restart] to apply the settings and restart the moneo services.
- ▷ The date and time are set.

6.4.14 Adding a USB memory device

- ▶ Connect the USB memory device to the USB port of moneo|vAppliance.



- ▶ Use a USB memory device with at least 4 GB storage capacity.

- ▶ Under [Configuration] > [USB devices], select the requested device from the table.
- ▶ In the [Actions] column, click on ∨ [Allow device].
- ▶ The message [Formatting of the USB device necessary] appears.

ATTENTION

Formatting the USB memory device.

- ▷ Data stored on the USB memory device will be deleted.
- ▷ Data loss is possible.
- ▶ Create a backup of data you want to keep.

- ▶ Click on [Delete Data & Format].
- ▷ The USB memory device is formatted. Data stored on the USB memory device will be deleted.
- ▷ The USB memory can now be used in moneo|vAppliance.

6.4.15 Denying a USB memory device

- ▶ Under [Configuration] > [USB devices], select the requested device from the table.
- ▶ In the [Actions] column, click on ⊗ [Deny device].
- ▷ The USB memory can no longer be used in moneo|vAppliance.

6.4.16 Removing a USB memory device

- ▶ Under [Configuration] > [USB devices], select the requested device from the table.
- ▶ In the [Actions] column, click on  [Delete device].

▷ The USB memory device is removed.

6.4.17 HTTPS/TLS certificates



The provision of corporate TLS web server certificates requires in-depth IT knowledge as well as a public key infrastructure (PKI).

Certificates in the AMS are used to verify the system identity and to encrypt client-server communication. The configured certificate is stored on the system's web server and is used to secure system identity for the accessing system (client's web browser).

2 different types of certificates can be used on the moneo|vAppliance:

1. Self-signed certificate:

- Active on delivery.
- Signed by the AMS itself and therefore not verifiable by the browser.
- A warning is displayed in the browser.
- Ensures that the communication between browser and web server is encrypted.
- Contains the following information:
 - IP addresses: 127.0.0.1 <system_ips>
 - DNS names: localhost <hostname> [<hostname>.<domain>] [<aliases>]

2. Custom certificate:

- Signed by a trustworthy certification body in the customer network.
- No warning is displayed in the browser.
- Ensures that the communication between browser and web server is encrypted.
- Checks the web server's identity if a PKI is available.



For further information on TLS encryption please refer to: → IT security whitepaper

To create a custom certificate, the following steps are required:

1. Requesting the certificate with the properties specified below from the client's internal IT department.
2. Integrating the certificate in the moneo|vAppliance.



The certificate must be combined into a p12 container together with all intermediate CA certificates of the PKI and the private key of the web server.

The list of intermediate CA certificates (chain file) must be in pem format (not p7b format).

The p12 file must not be protected by an import password.

6.4.17.1 Adding your own HTTPS/TLS certificate



When importing the p12 file, the following is checked:

- Whether the p12 file is complete (certificate plus chain file).
- Whether one of the included SANs (Subject Alternative Names) corresponds to one of the hostnames of the appliance, or whether one of the included IPs (IPv4) corresponds to one of the current IPs of the appliance.
- Whether the chain of intermediate certificates can be traced from the appliance back to the issuing root CA. Each intermediate CA (up to the root CA) indicated in the p12 file must be accessible from the appliance via the network.

✓ A certificate in p12 file format has been created and is available on the used device.

✓ The user is logged in to the AMS. (→ [Login to AMS](#) 17)

- ▶ Under [Configuration] > [TLS certificates], click on the button [Add new certificate].
- ▶ Select the required certificate and confirm by clicking [APPLY].
- ▷ When uploading the certificate, the moneo|vAppliance automatically checks the plausibility of the certificate information for validity.
- ▷ The interface is automatically reloaded.
- ▷ The certificate is used.



If the AMS is no longer accessible or the page fails to reload:

- ▶ Reload the interface manually, e.g. by pressing [F5].

6.4.17.2 Removing your own HTTPS/TLS certificate

- ✓ Your own certificate has already been added. (→ [Adding your own HTTPS/TLS certificate](#) 25)
- ✓ The user is logged in to the AMS. (→ [Login to AMS](#) 17)
- ▶ Click on  under [Configuration] > [TLS certificates].
- ▶ Click on [DELETE] to confirm the deletion.
- ▷ The interface is automatically reloaded.
- ▷ The certificate is overwritten with a self-signed certificate.
- ▷ Your self-created certificate is no longer used.



If the AMS is no longer accessible or the page fails to reload:

- ▶ Reload the interface manually, e.g. by pressing [F5].

6.4.17.3 Displaying information about the used HTTPS/TLS certificate

- ✓ The user is logged in to the AMS. (→ [Login to AMS](#) 17)
- ▶ The [Configuration] > [TLS certificates] section is open.
 - ▷ The [Certification path] field displays the certification path.
- ▶ Select the required certificate details in the [Details field].
 - ▷ The corresponding details values are displayed in the [Details value] field.

6.4.18 Shutting down / rebooting the device

- ✓ The user is logged in to the AMS. (→ [Login to AMS](#) 17)
- ▶ Click on  [SHUTDOWN].
- ▶ Restart the moneo|vAppliance by clicking on [Neustart]

or

- ▶ Shut down by clicking on [SHUTDOWN].



- ▷ If the system is shut down using the [SHUTDOWN] function, it can only be switched on again on the device.

6.5 Update

6.5.1 Enabling automatic checks for updates

- ✓ The user is logged in to the AMS. ([→ Login to AMS](#)  17)
- ▶ Under [Update] enable the option [Automatic update check daily at 05:00].
- ▷ The system checks daily at 5:00 am whether updates are available.
- ▷ If an update is available, the status [Update available.] is displayed.

6.5.2 Disabling automatic checks for updates

- ✓ The user is logged in to the AMS. ([→ Login to AMS](#)  17)
- ▶ Under [Update] disable the option [Automatic update check daily at 05:00].
- ▷ The system no longer checks automatically whether updates are available.

6.5.3 Manual search for available updates

- ✓ The user is logged in to the AMS. ([→ Login to AMS](#)  17)
- ▶ Click on the  icon under [Update].
- ▷ A check for updates is run.
- ▷ If an update is available, the status [Update available.] is displayed.

6.5.4 Installing online updates

ATTENTION

Changes to the system during the update process.

- ▷ Influence on the proper functioning of the system.
- ▷ Data loss is possible.
- ▶ Do not make any changes to the system during the update procedure.
- ▶ Follow the instructions during the update procedure.



No version may be skipped!

An update is only possible from the previous version!



Please note that when updating a non-licensed system, licensing will no longer be possible once the update has been completed.

- ▶ License the system before updating.

- ✓ The user is logged in to the AMS. ([→ Login to AMS](#)  17)
- ✓ An update is available.
[Enabling automatic checks for updates](#) ([→](#)  27)
[Manual search for available updates](#) ([→](#)  27)
- ✓ Under [Update] the status [Update available.] is displayed.
- ▶ Click on  to download the update.
- ▶ Optional, if the update download is to be cancelled: Click on the symbol  and then confirm to cancel the download.
- ▷ Once the update is downloaded, information about the available update is displayed in the [Local update version] column.

- ▶ Click on [Start Update] to install the update.

6.5.5 Installing offline updates

ATTENTION

Changes to the system during the update process.

- ▷ Influence on the proper functioning of the system.
- ▷ Data loss is possible.
- ▶ Do not make any changes to the system during the update procedure.
- ▶ Follow the instructions during the update procedure.



No version may be skipped!

An update is only possible from the previous version!



Please note that when updating a non-licensed system, licensing will no longer be possible once the update has been completed.

- ▶ License the system before updating.

- ✓ The user is logged in to the AMS. (→ [Login to AMS](#) □ 17)
- ✓ A more recent version than the one currently installed is available.
- ▶ Download the update file from www.ifm.com.
- ▶ Under [Update], click on the  icon and select an update file.
- ▶ Click on [Start Update] to install the update.

6.6 Saving and restoring

This menu item offers the following options:

- Manually creating and externally saving a backup of the existing system
- Activating/deactivating an automatic daily backup in the memory of the moneo|vAppliance.
- Restoring backup files that were created manually or automatically.

The generated backup file contains all system-relevant information to ensure a smooth system recovery.

6.6.1 Creating a manual backup

- ✓ The user is logged in to the AMS. (→ [Login to AMS](#) □ 17)
- ✓ TheBackup & Restore section is open.
- ▶ Click on the [Create backup] button.
- ▷ The backup will be created.
- ▷ The backup is encrypted with an automatically generated password.
- ▷ The newly created backup appears in the table.
- ▷ The backup is stored to the required destination. (→ [Configuring a backup target](#) □ 29)



Keep the backup file in a different location than moneo|vAppliance, taking into account fire protection and access regulations.

6.6.2 Copying backup files to a USB memory device

- ✓ The user is logged in to the AMS. ([→ Login to AMS](#)  17)
 - ✓ A backup file was previously created and is available in the AMS.
 - ✓ The [Backup & Restore] section is open
 - ✓ The required USB memory has already been added to the AMS. ([→ Adding a USB memory device](#)  24)
 - ▶ In the [Actions] column, click on the  icon of the required backup.
 - ▷ All available USB memories are displayed.
 - ▶ Select the required USB memory and click on [OK].
 - ▷ The selected backup will be copied to the USB memory.
-  There is not enough free space on USB storage devices marked in red to copy the backup file to them.

6.6.3 Configuring a backup target

- ▶ Open the [Backup & Restore] section.
- ▶ Click the button [Configure backup target].
 - ▷ The [Configure backup target] window opens.
- ▶ Select the requested backup destination in the selection field.

To save backups locally:

- ▶ Select [Local Storage] as the destination and confirm with [OK].
- ▷ Backups will now be stored locally.

To save backups on a USB memory device:

-  ▶ First allow USB memory devices ([→ Adding a USB memory device](#)  24).
- ▶ Select [USB storage] as the destination.
 - ▶ Click  to refresh the USB memories.
 - ▶ Select the desired USB memory device from the table and confirm with [OK].
 - ▷ Backups will be stored on the selected USB memory device.

To save backups on a network storage:

- ▶ Select [Network storage] as the destination.
- ▶ Select the required protocol type: SMB, SFTP or NFS.
- ▶ Enter the required parameters and confirm with [OK].
- ▷ Backups will be stored on the selected network storage.

6.6.4 Downloading backup passwords

- ▶ Open the [Backup & Restore] section.

- ▶ Click the button [Download backup passwords].
- ▷ A PDF file with all backup targets and the corresponding MasterKey is downloaded.
- ▷ The red key is the backup key used to encrypt the backups.



The local MasterKey is not output.

6.6.5 Restoring a backup from the backup destination



If the backup is to be restored on another moneo|vAppliance, assistance from the ifm support is required.

A backup can only be restored if it has been created in the same moneo version with which the system is operated.

- ✓ At least one backup file was previously created and is located on the previously set up backup destination (→ [Configuring a backup target](#)  29).
- ✓ The backup file is in the archive of moneo|vAppliance.
- ✓ The user is logged in to the AMS. (→ [Login to AMS](#)  17)
- ✓ The [Backup & Restore] section is open.
- ✓ Available backup files are displayed in tabular form with a timestamp.
- ▶ In the line of the required backup: Click on the  icon in the [Actions] column to start restoring the backup file.
- ▷ The backup file will be restored.
- ▷ Once started, the recovery of a backup file cannot be aborted.
- ▷ System settings, data, etc. of the moneo|vAppliance are reset to the status of the backup file that was imported.

6.6.6 Restoring a backup copied manually to USB



If the backup is to be restored on another moneo|vAppliance, assistance from the ifm support is required.

A backup can only be restored if it has been created in the same moneo version with which the system is operated.

- ✓ A backup was created and then copied to a USB memory device.
- ✓ The USB memory device on which the backup is located has been plugged in and added to the AMS (→ [Adding a USB memory device](#)  24).
- ▶ Set up the USB memory device as a backup destination to be able to see the backups in the AMS. (→ [Configuring a backup target](#)  29)
- ▶ Open the [Backup & Restore] section.
- ▶ In the line of the required backup: click on the  icon in the [Actions] column to start restoring the backup file.
- ▷ The backup file will be restored.
- ▷ Once started, the recovery of a backup file cannot be aborted.
- ▷ System settings, data, etc. of the moneo|vAppliance are reset to the status of the backup file that was imported.

6.6.7 Deleting a backup

- ✓ At least one backup file has been previously created and/or uploaded from an external data carrier.
- ✓ The backup file is in the archive of moneo|vAppliance.
- ✓ The user is logged in to the AMS. (→ [Login to AMS](#) 17)
- ✓ The section [Backup & Restore] is open.
- ✓ Available backup files are displayed in tabular form with a timestamp.
- ▶ In the line of the required backup: Click on the  icon in the [Actions] column to delete the backup file.

6.6.8 Enable automatic backup

- ✓ The user is logged in to the AMS. (→ [Login to AMS](#) 17)
- ✓ The [Backup & Restore] section is open.
- ▶ Enable the option field [Automatic daily backup at 02:50:00].
- ▷ The automatic backup is active.
- ▷ Every day at 2:50 am, a backup file will be created automatically in the moneo|vAppliance archive.



The automatically generated backup file is overwritten every day with the new backup file.

6.6.9 Disable automatic backup

- ✓ The user is logged in to the AMS. (→ [Login to AMS](#) 17)
- ✓ The [Backup & Restore] section is open.
- ▶ Disable the option field [Automatic daily backup at 02:50:00].
- ▷ Automatic backup is disabled.

6.7 Maintenance

6.7.1 Determining support-related information

- ✓ The user is logged in to the AMS. (→ [Login to AMS](#) 17)
- ▶ Look up the ifm contact information in the section [Support] > [Contact information].
- ▶ Look up the information relevant for support in the section [System status] > [System information]:
 - [System type]
 - [Serialnumber]
 - [Installed software]

6.7.2 Enabling remote access (SSH)

ATTENTION

SSH for remote access is enabled.

- ▷ Unauthorised data access (read or write) is possible.
- ▷ Unauthorised manipulation of the device function is possible.
- ▶ Recommendation: Enable SSH access only if prompted by the ifm service.
- ▶ Recommendation: Enable SSH access only temporarily and disable it after use.

- ✓ The user is logged in to the AMS. ([→ Login to AMS](#) 17)
- ▶ In the section [Support] > [Remote access], click on [Enable SSH access] to enable the SSH service for remote access to the console.
- ▷ The SSH service is enabled.
- ▷ Access via SSH is possible.

6.7.3 Disabling remote access (SSH)

- ✓ The user is logged in to the AMS. ([→ Login to AMS](#) 17)
- ▶ In the section [Support] > [Remote access], click on [Enable SSH access] to disable the SSH service for remote access to the console.
- ▷ The SSH service is disabled.
- ▷ Access via SSH is no longer possible.

6.7.4 Enabling ifm remote support



Please note the information on the ifm-Serviceaccount ([→ ifm service account](#) 35).

- ✓ The user is logged in to the AMS. ([→ Login to AMS](#) 17)
- ✓ Remote access is enabled. ([→ Enabling remote access \(SSH\)](#) 32)
- ▶ In the section [Support] > [Remote access], click on [Enable ifm remote support] to enable remote access for ifm.
- ▷ The connection to the ifm VPN gateway is established.
- ▷ ifm's support can access the system.



▶ If the ifm remote support is to be used via a proxy server, make sure that the proxy server address is configured as IP address and not as FQDN.

6.7.5 Disabling ifm remote support

- ✓ The user is logged in to the AMS. ([→ Login to AMS](#) 17)
- ▶ In the section [Support] > [Remote access], click on [Enable ifm remote support] to disable remote access for ifm.
- ▷ The connection to the ifm VPN gateway is disconnected.
- ▷ ifm's support can no longer access the system.



Recommendation: Also disable SSH access. ([→ Disabling remote access \(SSH\)](#) 32)

6.7.6 Download logfiles

- ✓ The user is logged in to the AMS. ([→ Login to AMS](#)  17)
- ▶ Click on [Download all logs] under [Support] > [Logging] to download all log files as a ZIP archive.

6.7.7 Show logfiles

- ✓ The user is logged in to the AMS. ([→ Login to AMS](#)  17)
- ▶ Click on ► under [Support] > [Logging] to show all log files.
- ▷ The individual log files are displayed one below the other.

6.7.8 Show live log

- ✓ The user is logged in to the AMS. ([→ Login to AMS](#)  17)
- ▶ Display the log files under [Support] > [Logging]. [Show logfiles](#) ([→](#)  33)
- ▶ In the line of the required log file: Click on the  icon in the [Actions] column to show the selected log file.

7 AMS console

The following options are available to access the console:

- Access via the web interface of the virtualisation environment.
- Remote access via IP/SSH. This access requires administrative clearing.
Web interface: [Enabling remote access \(SSH\)](#) (→ [32](#)),
Console: [Enabling Remote Support \(SSH\)](#) (→ [37](#))

After logging in and establishing the connection to the AMS console, the operation and range of functions is identical in both cases.

The different menu items in the appliance management system can be selected using the keyboard.
Example: The keyboard shortcut [C] opens [C) Configure the system].

7.1 Local access

In the following, local access to the AMS console is described.

7.1.1 Requirements

- ✓ The installation and connection of the moneo|vAppliance are completed.
- ▶ Start the moneo|vAppliance.
- ▷ The AMS console will be started.

7.1.2 Logging in for the first time

- ✓ The login prompt is displayed.
- ✓ Standard login data:
User: administrator
Default password: vAppliance1969!
- ▶ Enter the login details and confirm with [Enter].
 - ▷ If the login details are correct, the [Simple keyboard configuration menu] appears. [Changing the keyboard layout](#) (→ [37](#))
- ▶ Select the corresponding keyboard layout and confirm by clicking on [OK].
- ▶ Confirm the successful change by clicking [OK].
 - ▷ The prompt to change the password appears.
- ▶ Change the password according to the requirements and confirm by clicking [OK].
- ▶ Repeat the password and confirm by clicking [OK].
- ▷ When the change was successful, the [Main menu] appears.

7.1.3 Login

- ✓ Login prompt is displayed.
- ▶ Enter the login details and confirm with [Enter].
- ▷ If the login data is correct, the [Main menu] will appear.

7.2 Remote access

The following describes remote access to the AMS console via IP/SSH.

7.2.1 ifm service account



- There is an ifm service account that has full access to the system. This can be used for assistance in the event of support/error.
- The ifm service account can only be used if the customer allows SSH access / remote support and ifm is also granted access to the customer network.
- The password is unique for each appliance.
- The password is documented in encrypted form and can only be accessed by ifm support staff.

7.2.2 Requirements

- ✓ The installation and connection of the moneo|vAppliance are completed.
- ✓ Remote access via IP/SSH is enabled.
Web interface: [Enabling remote access \(SSH\)](#) (→ [32](#))
Console: [Enabling Remote Support \(SSH\)](#) (→ [37](#))
- ✓ The device (e.g. PC) for connection is connected to the same network as the Ethernet interface eth2 of the moneo|vAppliance.
- ✓ A suitable SSH client is installed on the device, e.g. Putty or Microsoft Powershell.
- ✓ The login data for the system that is assigned during initial setup is known.
- ▶ Check the above-mentioned conditions.

7.2.3 Accessing the AMS console via SSH

- ▶ Start the SSH client on the accessing device.
- ▶ Enter the IP address of the moneo|vAppliance.
- ▶ Optional: Enter the SSH port 22.
- ▷ Connection to the moneo|vAppliance console is established.
- ▷ The AMS console login is displayed.

7.2.4 Login

- ✓ AMS console is started.
- ✓ Login prompt is displayed.
- ▶ Enter the login details and confirm with [Enter].
- ▷ If the login data is correct, the [Main menu] will appear.

7.3 Displaying system information

7.3.1 Display host information

- ▶ Open the [Main menu].
- ▶ Select [I) Show system information].
 - ▷ The [Info menu] opens.
- ▶ Select [H) Show host information].
- ▷ [Show host information] with the following information:

- Host name
- Uptime
- Serial number
- Version
- Hard disk utilisation

7.3.2 Display network information

- ▶ Open the [Main menu].
- ▶ Select [I) Show system information].
 - ▷ The [Info menu] opens.
- ▶ Select [N) Show network information].
 - ▷ [Show network information] with the configurations of the Ethernet interfaces appears.

7.3.3 Showing moneo service information

- ▶ Open the [Main menu].
- ▶ Select [I) Show system information].
 - ▷ The [Info menu] opens.
- ▶ Select [S) Show moneo services information].
 - ▷ [moneo services status] appears with status information of the moneo services.

7.4 System configuration

7.4.1 Adapting the host name

The default host name of the moneo|vAppliance is: moneo-vappliance-XXXXXXX.

When the user has logged in, the default host name can be viewed at: [System status] > [System information]



The last 7 digits of the host name are generated during the import of vAppliance.

- ▶ Note that the entry is case sensitive.
- The host name can be adapted when signing in for the first time or later by following the below steps.
- ▶ Open the [Main menu].
 - ▶ Select [C) Configure the system].
 - ▷ The [Configuration menu] opens.
 - ▶ Select [H) Change the hostname].
 - ▷ [Host name change] opens.
 - ▷ The current host name is displayed in the field [Specify the new hostname].
 - ▶ Change the host name using the keyboard and select [Ok].
 - ▷ The host name is saved and the interface [Host name change] is closed.
 - ▶ Select [R) Return to the previous menu] to go back to the previous menu environment.

7.4.2 Changing the password

- ▶ Open the [Main menu].
- ▶ Select [C) Configure the system].
 - ▷ The [Configuration menu] opens.
- ▶ Select [P) Change the password].
 - ▷ [Password change] opens.
- ▶ Enter password and acknowledge with [OK].
- ▶ Enter the identical password again and acknowledge with [OK].
- ▷ Password is saved and the interface [Password change] is closed.
- ▶ Select [R) Return to the previous menu] to go back to the previous menu environment.

7.4.3 Changing the keyboard layout

- ▶ Open the [Main menu].
- ▶ Select [C) Configure the system].
 - ▷ The [Configuration menu] opens.
- ▶ Select [K) Change the keyboard layout].
 - ▷ The [Keyboard configuration menu] opens.
- ▶ Select
 - Simple: [S) Simple keyboard configuration] - or - Advanced: [A) Advanced keyboard configuration]
 - ▷ The [Simple keyboard configuration menu] - or - the [Configuring keyboard-configuration] menu opens.
- ▶ Select the drequired keyboard layout.
- ▶ Confirm by clicking [OK].

7.4.4 Enabling Remote Support (SSH)



The SSH service can be enabled only with local access.

Enabling the SSH service is necessary for subsequent remote access.

The current status of the SSH service is displayed in brackets after the menu item.



Please note the information on the ifm-Serviceaccount ([→ ifm service account](#) [□ 35](#)).

ATTENTION

SSH for remote access is enabled.

- ▷ Unauthorised data access (read or write) is possible.
- ▷ Unauthorised manipulation of the device function is possible.
- ▶ Recommendation: Enable SSH access only if prompted by the ifm service.
- ▶ Recommendation: Enable SSH access only temporarily and disable it after use.

✓ [Local access.]

- ▶ Open the [Main menu].
- ▶ Select [C) Configure the system].
 - ▷ The [Configuration menu] opens.
- ▶ Select the menu item [S) Toggle SSH access (disabled)].
 - ▷ Access via SSH will be enabled.
 - ▷ The menu item [S) Toggle SSH access (enabled)] is shown.
- ▶ Select [R) Return to the previous menu] to go back to the previous menu environment.

7.4.5 Disabling Remote Support (SSH)



Risk of connection failure and loss of access:

- ▶ Disable the SSH service only with local access.



The current status of the SSH service is displayed in brackets after the menu item.

- ✓ [Local access]
- ▶ Open the [Main menu].
- ▶ Select [C) Configure the system].
 - ▷ The [Configuration menu] opens.
- ▶ Select the menu item [S) Toggle SSH access (enabled)].
 - ▷ Access via SSH is blocked.
 - ▷ The menu item [S) Toggle SSH access (disabled)] is displayed.
- ▶ Select [R) Return to the previous menu] to go back to the previous menu environment.

7.4.6 Adjust network settings

- ▶ Open the [Main menu].
- ▶ Select [C) Configure the system].
 - ▷ The [Configuration menu] opens.
- ▶ Select [N) Configure the network].
 - ▷ [Network configuration] opens.
- ▶ Select the required interface: [S) Sensor network (ETH 1)] or [I) IT network (ETH 2)].
- ▶ Select [U) Use DHCP].
- ▶ Change the entry [yes] / [no] as required.

With DHCP deactivated:

- ▶ Select [I) Set the IP address].
 - ▷ [Network (ip)] opens.
- ▶ Enter the new IP address using the keyboard and select [Ok].
 - ▷ [Network configuration] opens.
- ▶ Carry out the settings for the network mask, the gateway and the DNS servers.
- ▶ Select [S) Save the configuration].
 - ▷ The message [The network configuration was successfully changed] is displayed.
- ▶ Select [Ok].

- ▶ Select [R) Return to the previous menu] to go back to the previous menu environment.
- ▷ The system is configured and available via web interface.

7.4.7 Upgrading the virtual hard disk

- ▶ Switch off moneo|vAppliance before expanding the virtual hard disk.
- ▶ Set the hard disk size of the VM in the hypervisor as required.



The hard disk must be expanded by at least 1 GB, otherwise expansion is not possible.



When the virtual hard disk is expanded, the ring buffer size for the process value archive is set to 50% of the free space available after expansion, minus the space required for the ring buffer, its backups and a 1 GiB buffer.

- ▶ Start moneo|vAppliance.
- ▶ Open the AMS console.
- ▶ Open the [Main menu].
- ▶ Select [C) Configure the system].
 - ▷ The [Configuration menu] opens.
- ▶ Select [X) Expand storage...].
 - ▷ A security prompt appears.
- ▶ Click on [OK] to confirm the expansion of the virtual hard disk. Then restart the VM to apply the expansion.
 - or -
 - Click on [ESC] to cancel the expansion of the virtual hard disk.

7.5 Restart the required moneo service.

- ▶ Open the [Main menu].
- ▶ Select [R) Restart the moneo services].
 - ▷ [Restart the moneo services] opens.
- ▶ Restart the required service.
- ▶ Select [R) Return to the previous menu] to go back to the previous menu environment.

7.6 Resetting the AMS administrator password

- ▶ Open the [Main menu].
- ▶ Select [A) Reset the AMS 'administrator' password].
 - ▷ The administrator password is reset to: vAppliance1969!

7.7 Reset the system to factory settings

ATTENTION

When resetting the system, all data is deleted and reset to the factory settings. This also includes the databases and backups.

▷ Data loss is possible.

▶ Export backups you want to keep before resetting the system. (→ [Saving and restoring](#) [□ 28](#))

- ▶ Open the [Main menu].
- ▶ Select [F) Factory-reset the system].
- ▶ Click [OK] to confirm the factory reset
-or-
Click [ESC] to abort the factory reset.



At this point, the factory reset can be aborted with [ESC].

After confirming with [OK], the factory reset can no longer be aborted!

- ▷ The system will be reset to the factory settings:
- ▷ The host name will be reset to: moneo-vappliance-XXXXXXX



The last 7 digits of the host name are randomly generated.

- ▷ The admin password will be reset to: vAppliance1969!
- ▷ The AMS password will be reset to: vAppliance1969!
- ▷ The IP addresses will be reset to the factory settings.
- ▷ The moneo databases will be deleted.
- ▷ The licences will be deleted.

7.8 Reboot the system

- ▶ Open the [Main menu].
- ▶ Select [B) Reboot the system].
- ▶ Acknowledge with [OK].
- ▷ The system will then be restarted

7.9 Shut down the system

- ▶ Open the [Main menu].
- ▶ Select [D) Shutdown the system].
- ▶ Acknowledge with [OK].
- ▷ The system will be shut down.

7.10 Logout

- ✓ Logging in to the console was successful.
- ✓ The [Main menu] is displayed.

- ▶ Use the menu [X) Exit] the console.
- ▷ The user will be logged out.
- ▷ Local access: The login prompt is displayed.
- ▷ Remote access: The SSH connection is terminated.