

---

# **M2M Gateway ARM600**

## User Manual







Document ID: 1MRS758861

Issued: 2022-02-09

Revision: K

Product version: 5.0.1

© Copyright 2022 ABB. All rights reserved

# Copyright

This document and parts thereof must not be reproduced or copied without written permission from ABB, and the contents thereof must not be imparted to a third party, nor used for any unauthorized purpose.

The software or hardware described in this document is furnished under a license and may be used, copied, or disclosed only in accordance with the terms of such license.

## Trademarks

ABB is a registered trademark of the ABB Group. All other brand or product names mentioned in this document may be trademarks or registered trademarks of their respective holders.

## Warranty

Please inquire about the terms of warranty from your nearest ABB representative.

[abb.com/mediumvoltage](http://abb.com/mediumvoltage)

# Disclaimer

The data, examples and diagrams in this manual are included solely for the concept or product description and are not to be deemed as a statement of guaranteed properties. All persons responsible for applying the equipment addressed in this manual must satisfy themselves that each intended application is suitable and acceptable, including that any applicable safety or other operational requirements are complied with. In particular, any risks in applications where a system failure and/or product failure would create a risk for harm to property or persons (including but not limited to personal injuries or death) shall be the sole responsibility of the person or entity applying the equipment, and those so responsible are hereby requested to ensure that all measures are taken to exclude or mitigate such risks.

This product has been designed to be connected and communicate data and information via a network interface which should be connected to a secure network. It is the sole responsibility of the person or entity responsible for network administration to ensure a secure connection to the network and to take the necessary measures (such as, but not limited to, installation of firewalls, application of authentication measures, encryption of data, installation of anti virus programs, etc.) to protect the product and the network, its system and interface included, against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB is not liable for any such damages and/or losses.

This document has been carefully checked by ABB but deviations cannot be completely ruled out. In case any errors are detected, the reader is kindly requested to notify the manufacturer. Other than under explicit contractual commitments, in no event shall ABB be responsible or liable for any loss or damage resulting from the use of this manual or the application of the equipment. In case of discrepancies between the English and any other language version, the wording of the English version shall prevail.

## Conformity

This product complies with the directive of the Council of the European Communities on the approximation of the laws of the Member States relating to electromagnetic compatibility (EMC Directive 2014/30/EU) and concerning electrical equipment for use within specified voltage limits (Low-voltage directive 2014/35/EU). This conformity is the result of tests conducted by ABB in accordance with the product standard EN 60255-26 for the EMC directive, and with the product standards EN 60255-1 and EN 60255-27 for the low voltage directive. The product is designed in accordance with the international standards of the IEC 60255 series.

# End user license agreement

This End User License Agreement is a legal agreement between you and ABB for the Product identified below.

BY INSTALLING, COPYING, OR OTHERWISE USING THE PRODUCT YOU AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE, YOU ARE NOT ENTITLED TO INSTALL OR USE THE PRODUCT.

## 1. The product

For the purposes of this agreement, the term “Product” shall mean all software and related information provided by ABB under this agreement including but not limited to ABB proprietary module for Arctic Patrol (m2msys, viola-m2mgw-base, viola-centos-configuration, viola-m2mgw, viola-php-common).

The Product includes computer software and may include a License Key, associated media printed materials, and online or electronic documentation.

Product software can delivered as such or as a part of hardware product (ARM600). The form of delivery is agreed between the Parties.

The term “System of Computers” shall mean a system of one or more interconnected computers on which the Product software is installed and configured such that the computers cooperate as a system to perform the functions of the Product.

The Product may include software, which is owned by a third party. For such software separate license terms and conditions may apply which you agree to comply with.

## 2. Grant of license

ABB grants you the following non-exclusive and restricted rights, provided that you comply with all the terms and conditions of this agreement.

### 2.1 Installation and use

You may install and run the Product on one System of Computers, and use, access, and display the functional options that are specified in the License Certificate, for their intended use as defined in the product documentation, and within the configuration and capacity limits that are specified in the License Certificate.

You may not use, access or display functions that are not specified in the License Certificate.

You may not exceed the configuration and capacity limits that are specified in the License Certificate.

A License for the Product may not be shared or used concurrently on different Systems of Computers.

## **2.2 Storage and network use**

You may copy the Product for safekeeping. All copies must carry the same copyright notice as the original product.

You may store a copy of the Product on a storage device, such as a network server, for use for installing the Product over an internal network onto the System of Computers.

You may store a copy of the Product on a storage device, such as a network server, for use for installing the Product over an internal network onto the System of Computers.

## **2.3 Network connection and Internet based functions**

The Product is intended for use on a system of one or more computers that are interconnected by means of a computer communication network. The Product contains functions that can be configured to allow network access to/from other computer systems on the same or other networks. Further, the Product contains functions that can be configured to utilize Internet based services. You acknowledge and agree that you are responsible for the safe and secure configuration and use of these functions and network connections.

## **2.4 Limitations in use**

You may not use the product for planning, construction, maintenance, or operation, directly or indirectly, of nuclear facilities, flight navigation, aircraft control, air traffic control and ground support equipment, missile technology, and facilities for weapons of mass destruction, unless this use is explicitly approved by ABB in writing in each and every case. Such approval shall be granted only if ABB's liability for damage to property, personal injury and death, damage to plant as well as property located there or in its vicinity, and all consequential and incidental costs and losses connected with any of the aforesaid is excluded by law and by contract to the satisfaction of ABB.

For the purposes of this agreement the term "nuclear facilities" shall mean any nuclear facility, including, but not limited to, nuclear power plants, nuclear fuel manufacturing plants, uranium enrichment plants, uranium conversion plants, spent nuclear fuel conversion plants, spent nuclear fuel storage plants, and research reactors. The term "facilities for weapons of mass destruction" shall mean any facility for design, manufacturing, storage, transportation, controlling, dispatching, and destruction of weapons of mass destruction, including, but not limited to, nuclear, chemical, and biological weapons.

## **2.5 Reservation of rights**

ABB reserves all rights not expressly granted to you in this agreement.



### **3. Upgrades**

To use a Product identified as an upgrade, you must first be licensed for the product identified by ABB as eligible for the upgrade. After upgrading, you may no longer use the product that formed the basis for your upgrade eligibility.

### **4. Additional software**

This agreement applies to updates or supplements to the original Product provided by ABB, unless other terms are provided along with the update or supplement.

### **5. Transfer of rights**

#### **5.1 Internal**

You may move the Product to a different System of Computers. This may require that the License Key be substituted for a new License Key that is tied to the new set of computer hardware.

#### **5.2 Transfer to third party**

You may not transfer the rights granted through this agreement to another end user without prior written approval from ABB. Such approval shall not be unreasonably withheld. The transfer must include the License Certificate, the License Key (if any) and all component parts, media, printed materials, and this agreement. The transfer may not be an indirect transfer, such as a consignment. Prior to the transfer, the end user receiving the transferred rights must agree to all the terms of this agreement.

#### **5.3 No rental**

You may not rent, lease or lend the Product.

#### **5.4 Third party software**

You acknowledge that the Product contains certain proprietary software licensed to ABB by third parties. You agree to such third party software license agreements provided by the said third parties. Such third parties may enforce this Agreement and their own license terms directly against You to the extent of such third party's interest in the Software.

### **6. Limitation on reverse engineering, de-compilation, and disassembly**

You may not reverse engineer, de-compile, or disassemble the Product, except and only to the extent that it is expressly permitted by applicable law notwithstanding this limitation.

### **7 Demonstration and evaluation software**

If the License is identified as "Temporary" or "Internal Use", the Product must not be transferred or used for any purpose other than demonstration, test, or evaluation.

## **8 Export restrictions**

You acknowledge that the Product in part is of U.S. origin and may be subject to U.S. export restrictions. You agree to comply with all applicable international and national laws that apply to the Product, including the U.S. Export Administration Regulations, as well as end-user, end-use, and destination restrictions issued by U.S. and other governments. For additional information contact your ABB representative.

## **9 Intellectual property rights**

The Product is protected by copyright and other intellectual property rights, including but not limited to patents. ABB or its suppliers own the title, copyright, and other intellectual property rights in the Product. The Product is licensed, not sold. You may not disclose to any third party the software or any information of commercial or technical nature provided by ABB as part of or in association with the Product.

You agree to not disclose benchmark test results related to the Product to any third party.

## **10 Entire agreement**

This agreement, including any addendum or amendment to this agreement that is included with the Product, is the entire agreement between you and ABB relating to the Product and related support services (if any) and they supersede all prior or contemporaneous oral or written communications, proposals, and representations, with respect to the Product or any other subject matter covered by this agreement. To the extent the terms of any ABB policies or programs for support services conflict with the terms of this agreement, the terms of this agreement shall control.

## **11 Termination**

Without prejudice to any other rights, ABB may cancel this agreement if you do not abide by the terms and conditions of this agreement, in which case you must return all copies of the Product and all of its component parts to ABB.

## **12 Applicable law**

This Agreement shall be governed by and construed in accordance with the substantive laws of Finland.

All disputes, differences or questions between the Parties with respect to any matter arising out of or relating to the Agreement shall be finally determined in arbitration in accordance with the rules of International Chamber of Commerce. The Place of arbitration shall be Helsinki, Finland and the language shall be English.

## **13 Indemnification**

13.1 ABB will indemnify you against any third party claim that the Product infringes upon intellectual property rights of any third party, provided that (i) you promptly notify ABB in writing of the claim; (ii) ABB shall have the sole control

of the defense and all related settlement negotiations; and (iii) you provide ABB with the assistance, information and authority necessary for ABB to perform its obligations under this section. ABB shall have no liability towards you in respect of an actual or alleged intellectual property right infringement if this results from any breach by you of (i) your obligations under these license terms or (ii) of any other agreement between you and ABB.

13.2 If the Product is held to constitute an intellectual property rights infringement, or such is considered by ABB to constitute such infringement, ABB shall have the option, at its own expense, to: (i) modify the Product so that it no longer constitutes an infringement; (ii) obtain a license for you to continue using the Product notwithstanding such infringement; or (iii) replace the Software Product with substitutes which do not constitute infringements, provided that such substitutes do not entail a material diminution in performance or function.

## 14. Warranty

Provided that you have a valid license to use the Product, ABB warrants that a) for a period of 90 days from the date of shipment of your license (the "Warranty Period") that it will perform substantially in accordance with the written materials that accompany the Product; and b) any related support services provided by ABB shall be substantially as described in applicable written materials provided to you by ABB, and ABB support engineers will use commercially reasonable efforts, care and skill to remedy by repair or replacement or supply a temporary fix, or make an emergency bypass, if the Product yields incorrect results. In the event that the Product fails to comply within the warranty period, ABB will either a) repair or replace the Product or b) return the price you paid for the Product.

The foregoing warranty shall not apply to defects resulting from unauthorized modification. ABB does not warrant that the functions contained in the software will operate in combinations which may be selected for use by You or that the software products are free from errors in the nature of what is commonly categorized by the computer industry as "bugs."

The foregoing warranties shall not apply to Software which (1) have been improperly modified or altered; (2) have been subjected to misuse, negligence or accident; (3) have been used in a manner contrary to ABB's instructions, including instructions concerning appropriate environmental specifications; (4) are used in combination with equipment, components or products not specified by ABB; and/or (5) where the damage is attributable to external factors, including, without limitation, failure or fluctuation of electrical power or air conditioning.

The foregoing warranties shall not apply to Software which (1) have been improperly modified or altered; (2) have been subjected to misuse, negligence or accident; (3) have been used in a manner contrary to ABB's instructions, including instructions concerning appropriate environmental specifications; (4) are used in combination with equipment, components or products not specified by ABB; and/or (5) where the damage is attributable to external factors, including, without limitation, failure or fluctuation of electrical power or air conditioning. **TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND**

**SUBJECT TO THE WARRANTY ABOVE, ABB DISCLAIMS ALL WARRANTIES, CONDITIONS AND OTHER TERMS, EITHER EXPRESS OR IMPLIED (WHETHER BY STATUTE, COMMON LAW, COLLATERALLY OR OTHERWISE) INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF SATISFACTORY QUALITY AND FITNESS FOR PARTICULAR PURPOSE WITH RESPECT TO THE PRODUCT AND THE WRITTEN MATERIALS THAT ACCOMPANY THE PRODUCT. ANY IMPLIED WARRANTIES THAT CANNOT BE EXCLUDED ARE LIMITED TO ONE YEAR OR TO THE SHORTEST PERIOD PERMITTED BY APPLICABLE LAW, WHICHEVER PERIOD IS GREATER. THE REMEDIES STATED HEREIN CONSTITUTE YOUR EXCLUSIVE REMEDIES AND ABB'S ENTIRE LIABILITY FOR ANY BREACH OF WARRANTY.**

### **15 Exclusion of liability**

To the maximum extent permitted by applicable law, ABB and its suppliers shall not be liable for any damages whatsoever resulting from this agreement, the granted license, or the use of the Product. Without limiting the applicability of the above exclusion, it is explicitly agreed that ABB shall under no circumstance be liable for loss of income or profits, business interruption, loss of data, loss of business information or other pecuniary loss as well as for any special, indirect or consequential losses or damages, arising out of the use or inability to use the Product, even if ABB or any of its suppliers has been advised of the possibility of such damages. In any case ABB's entire liability under any provision of this Agreement shall be limited to the amount actually paid by you for the Product.

ABB or its suppliers shall not be liable towards any party for consequential costs as result of upgrading from one software version to another, such as, but not limited to, the need for newer or other versions of third party software, or the need for higher capacity or performance hardware.

## Safety information



Dangerous voltages can occur on the connectors, even though the auxiliary voltage has been disconnected.



Non-observance can result in death, personal injury or substantial property damage.



National and local electrical safety regulations must always be followed.



This product is not fault-tolerant and is not designed, manufactured or intended for use or resale as on-line control equipment or as part of such equipment in any hazardous environment requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of the hardware or software described in this manual could lead directly to death, personal injury, or severe physical or environmental damage.



To prevent damage both the product and any terminal devices must always be switched off before connecting or disconnecting any cables. It should be ascertained that different devices used have the same ground potential. The output voltage of the power supply should be checked before connecting any power cables.



The devices mentioned in this manual are to be used only according to the instructions described in this manual. Faultless and safe operation of the devices can be guaranteed only if the transport, storage, operation and handling of the devices is appropriate. This also applies to the maintenance of the products.



---

## Table of contents

<b>Section 1</b>	<b>Introduction.....</b>	<b>5</b>
	This manual.....	5
	Intended audience.....	5
	Product documentation.....	5
	Product documentation set.....	5
	Document revision history.....	5
	Related documentation.....	6
	Symbols and conventions.....	6
	Symbols.....	6
	Document conventions.....	7
<b>Section 2</b>	<b>ARM600 overview.....</b>	<b>9</b>
	Overview.....	9
	Key features.....	10
	Physical interfaces (only for ARM600 hardware variants).....	11
	Standard edition.....	11
	Front panel.....	11
	Back panel.....	12
	Health indicators.....	12
	Enterprise edition.....	13
	Front panel.....	13
	Back panel.....	14
	LCD panel.....	14
	Deployment scenarios.....	14
<b>Section 3</b>	<b>Cybersecurity.....</b>	<b>17</b>
	Cybersecurity definition.....	17
	Configuring firewall and services.....	17
	Software updates.....	18
<b>Section 4</b>	<b>Getting started.....</b>	<b>19</b>
	Configuring ARM600 (only for ARM600 hardware variants).....	19
	Rack mounting ARM600 (only for ARM600 hardware variants).....	19
	Connecting cables (only for ARM600 hardware variants).....	20
	Setting up virtual machine environment (only for ARM600SW).....	20
	Creating users for ARM600.....	20
	Logging in.....	21
<b>Section 5</b>	<b>Web HMI.....</b>	<b>23</b>
	Menu structure.....	23

---

System menu.....	23
Status.....	23
Statistics.....	24
Time.....	24
Network menu.....	24
Network configuration.....	24
Static routing.....	24
VPN menu.....	25
L2TP-VPN.....	25
SSH-VPN.....	25
OpenVPN.....	25
OpenVPN with firewall.....	26
Firewall menu.....	26
General.....	26
Filter incoming.....	27
Filter forwarded.....	27
Filter outgoing.....	27
D-NAT.....	27
S-NAT.....	27
Custom rules.....	27
Arctic Patrol menu.....	28
Overview.....	29
Devices.....	29
Management.....	29
Details.....	29
Statistics.....	29
Registration.....	29
Configuration.....	29
Profiles.....	30
Device firmware.....	30
Tools menu.....	30
User Administration.....	30
Adding users.....	30
Setting password history.....	31
Changing password and setting password lifetime.....	31
Editing groups.....	31
Backup and Auto backup.....	31
Support Log.....	32
Release Notes.....	32
Reboot.....	32
<b>Section 6 Network configuration.....</b>	<b>33</b>
Configuring Ethernet interfaces.....	33
Ethernet interface setup parameters.....	35



---

<b>Section 7</b>	<b>Arctic Patrol.....</b>	<b>37</b>
	Overview.....	37
	Registering Arctic devices to Patrol.....	37
	Allowing Arctic devices to scan local networks.....	41
	Asset management.....	42
	Selecting devices for device management.....	43
	Arctic device management .....	44
	Updating Arctic device firmware via ARM600 (only for ARM600 hardware variants).....	44
	Updating Arctic device firmware via ARM600SW.....	45
	Updating RTU configuration.....	47
	Updating device XML configuration.....	48
	Rebooting Arctic devices.....	51
	RIO600 device management .....	52
	Updating RIO600 configuration.....	52
	Updating RIO600 firmware.....	54
	Exporting RIO600 configurations from PCM600.....	56
	OpenVPN certificate management.....	58
	Renewing certificates for an OpenVPN server.....	59
	Sending renewed certificates to Arctic devices.....	60
	Checking certificate status on Arctic wireless devices.....	63
<b>Section 8</b>	<b>SSH mode selection and key update.....</b>	<b>65</b>
	SSH legacy mode.....	65
	Legacy mode effects on the system.....	65
	Legacy mode activation.....	66
	Manually deactivating and activating SSH legacy mode.....	66
	SSH-VPN key update tool.....	67
	Comparison of SSH versions.....	67
	Checking SSH version.....	68
	Using SSH key update tool.....	69
<b>Section 9</b>	<b>Additional administrative features.....</b>	<b>71</b>
	Updating ARM600 system (ARM600 hardware variants).....	71
	Updating ARM600SW system.....	72
	Local software repository mirror.....	74
	Updating firmware for Arctic Wireless Gateways using ARM600SW.....	74
<b>Section 10</b>	<b>Troubleshooting.....</b>	<b>77</b>
	Common problems and solutions.....	77
	Questions and answers.....	78
<b>Section 11</b>	<b>Technical data (ARM600 hardware variants).....</b>	<b>79</b>

---

Section 12 Glossary.....81

---

## Section 1 Introduction

### 1.1 This manual

The user manual provides introductory information as well as detailed instructions on how to set up and manage the device as part of a network environment.

### 1.2 Intended audience

This manual addresses the personnel, such as security administrators, who manage the company's IT Infrastructure consisting of the network or security systems and applications running in the company's environment.

The personnel involved in installing and managing the Arctic devices are expected to be experienced in secure network practices.

### 1.3 Product documentation

#### 1.3.1 Product documentation set

Product series- and product-specific manuals can be downloaded from the ABB Web site [abb.com/mediumvoltage](http://abb.com/mediumvoltage).

#### 1.3.2 Document revision history

Document revision/date	Product version	History
A/2017-09-29	4.3	First release
B/2018-06-29	4.4.1	Content updated to correspond to the product version
C/2019-04-24	4.5.1	Content updated to correspond to the product version
D/2020-06-30	4.5.3	Content updated to correspond to the product version
E/2021-01-19	4.5.3	Content updated
F/2021-03-18	4.5.3	Content updated
G/2021-06-28	5.0.1	Content updated to correspond to the product version
H/2021-12-20	5.0.1	Content updated
K/2022-02-09	5.0.1	Content updated



Download the latest documents from the ABB Web site  
[abb.com/mediumvoltage](http://abb.com/mediumvoltage).

### 1.3.3 Related documentation

Name of the document	Description	Document ID
Arctic Cyber Security Deployment Guideline		1MRS758860
3G/LTE configuration guide Technical Note	Configuring Wireless Gateways, Controllers and M2M Gateway	1MRS758449

Product series- and product-specific manuals can be downloaded from the ABB Web site [abb.com/mediumvoltage](http://abb.com/mediumvoltage).

## 1.4 Symbols and conventions

### 1.4.1 Symbols



The electrical warning icon indicates the presence of a hazard which could result in electrical shock.



The warning icon indicates the presence of a hazard which could result in personal injury.



The caution icon indicates important information or warning related to the concept discussed in the text. It might indicate the presence of a hazard which could result in corruption of software or damage to equipment or property.



The information icon alerts the reader of important facts and conditions.



The tip icon indicates advice on, for example, how to design your project or how to use a certain function.

---

Although warning hazards are related to personal injury, it is necessary to understand that under certain operational conditions, operation of damaged equipment may result in degraded process performance leading to personal injury or death. Therefore, comply fully with all warning and caution notices.

## 1.4.2

### Document conventions

A particular convention may not be used in this manual.

- Abbreviations and acronyms are spelled out in the glossary. The glossary also contains definitions of important terms.
- Menu paths are presented in bold.  
Select **Main menu/Settings**.
- Parameter names are shown in italics.  
The function can be enabled and disabled with the *Operation* setting.
- Parameter values are indicated with quotation marks.  
The corresponding parameter values are "On" and "Off".



---

## Section 2      ARM600 overview

### 2.1              Overview

M2M Gateway ARM600 is a member of ABB's Arctic product family. ARM600 is a communication server, a VPN concentrator and firewall and is typically placed in the same location as the central control and monitoring system, such as SCADA.

ARM600SW is a software-only version of ARM600 with additional features such as a faster update cycle via a dedicated software repository and capability to be run in virtual machine environment.

ARM600 manages all Arctic 600 series wireless gateway connections and is the main interface between the field devices and the central control and monitoring system. ARM600 includes the Arctic Patrol application for condition monitoring and centralized device management. Centralized device management is essential to ensure the network operability in large-scale or geographically dispersed communication systems.

ARM600 provides static IP addressing for the central control and monitoring system. This means that the Arctic 600 series wireless gateways in remote locations can use normal SIM cards with dynamic IP addresses from any operator. Thus different operators can be used depending on the coverage and pricing. Both standard (public) and private APN type SIM cards can be used in this communication system.

ARM600 is typically part of a complete communication system which consists of Arctic 600 series wireless gateways and a central Arctic M2M Gateway ARM600 communication server. ARM600 is an essential part of the total communication solution. The communication solution is application independent, that is, any type of remote application can be connected to any type of centralized control and monitoring application.

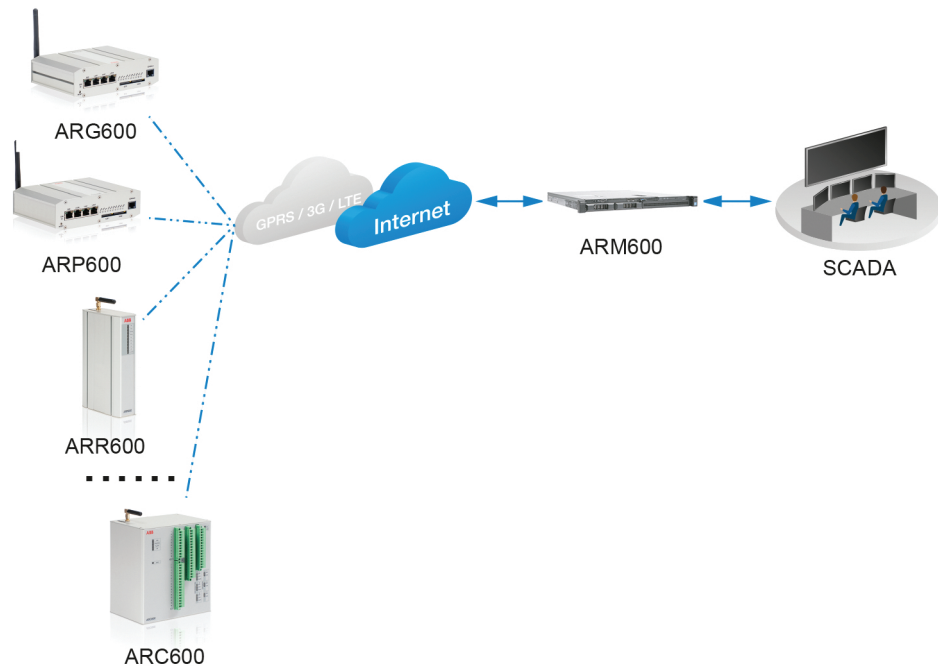


Figure 1: Communication system overview

## 2.2 Key features

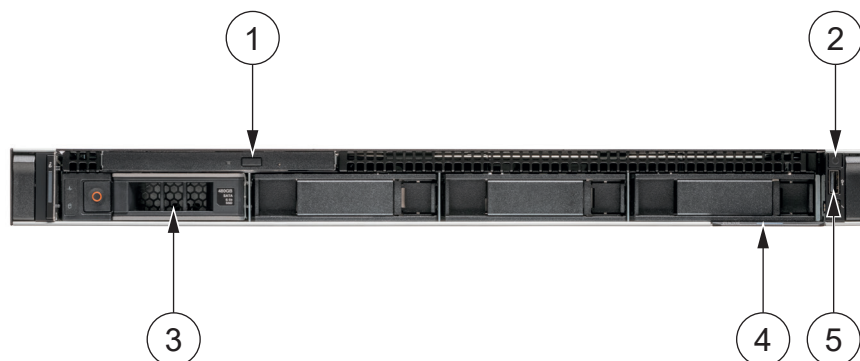
- VPN concentrator manages VPN tunnels to Arctic 600 series wireless gateways
  - Supports OpenVPN, L2TP and SSH-VPN tunnels
  - OpenVPN bridging
  - Connection to ARM600 with a PC from any location via VPN
- Firewall to restrict unauthorized access
- Provides static IP addressing of Arctic 600 series wireless gateways for SCADA
- Full routing capability allows integrating remote LAN into a central LAN
- Configuration via Web UI and command line (SSH) access
- Arctic Patrol offers condition monitoring and centralized device management application that supervises the cellular connections to the connected Arctic 600 series wireless gateways and enables advanced remote management of all connected Arctic gateways and ABB's RIO600 devices
- Supports virtual machine environment, for example, VMware vSphere ESXi 6.7 or later (only applies to ARM600SW)
- Software updates via a repository (only applies to ARM600SW)
- 19" rack mountable design (only applies to ARM600 hardware variants)



## 2.3 Physical interfaces (only for ARM600 hardware variants)

### 2.3.1 Standard edition

#### 2.3.1.1 Front panel



*Figure 2: Front panel*

- 1 Optical drive
- 2 Power on indicator, power button
- 3 Hard drive
- 4 Service tag (EST)
- 5 USB 2.0 port

2.3.1.2 Back panel



Figure 3: Back panel

- 1 Ethernet port eth0 (Gb1)
- 2 Ethernet port eth1 (Gb2)
- 3 Power supply health/activity indicators
- 4 Video (VGA) port
- 5 iDRAC
- 6 Two USB 3.0 ports
- 7 Power supply unit (PSU)

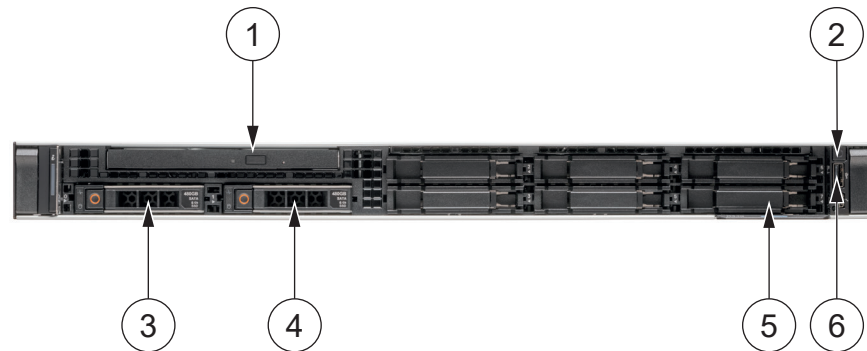
2.3.1.3 Health indicators

Table 1: System health indicator codes (on the left side of the front panel)

Status and color	Description
Solid blue	Indicates that the system is turned on and healthy System ID mode is not active. Press the system health and system ID button to toggle between system ID mode and system health mode.
Flashing blue	Indicates that the system ID mode is active
Solid amber	Indicates that the system is in fail-safe mode
Flashing amber	Indicates that the system is experiencing a fault Check the System Event Log for more specific error messages. For more information on the event and error messages, see the Error Code Lookup page at <a href="https://www.dell.com">Dell.com</a> .

## 2.3.2 Enterprise edition

### 2.3.2.1 Front panel



*Figure 4: Front panel*

- 1 Optical drive
- 2 Power on indicator, power button
- 3 Hard drive 1
- 4 Hard drive 2
- 5 Service tag (EST)
- 6 USB 2.0 port

### 2.3.2.2

## Back panel

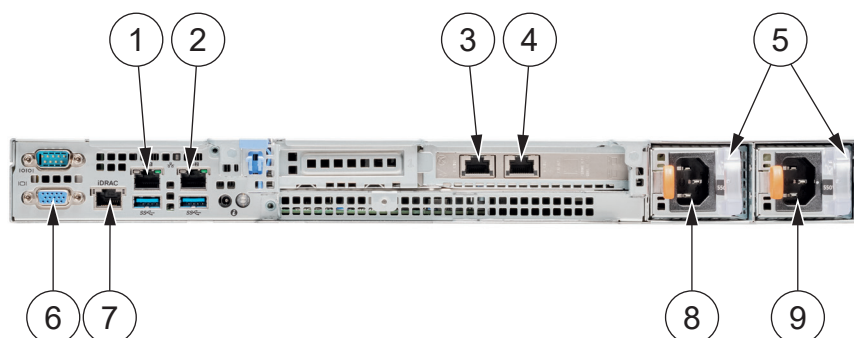


Figure 5: Back panel

- 1 Ethernet port eth2
- 2 Ethernet port eth3
- 3 Ethernet port eth1
- 4 Ethernet port eth0
- 5 Power supply health/activity indicators
- 6 Video (VGA) port
- 7 iDRAC
- 8 Power supply bay 1
- 9 Power supply bay 2

### 2.3.3

## LCD panel

For a detailed description of the LCD panel functions, visit [Dell.com](http://Dell.com).

## 2.4

## Deployment scenarios

ARM600 is typically installed in the same location as the central control and monitoring system.

When typical SIM cards are used, ARM600 requires a fixed line Internet connection with a public and static IP address. The public IP address is required for the data from the connected Arctic 600 series wireless gateways to be routed to ARM600 via the public Internet. The fixed IP address is required because the data connection between the Arctic 600 series wireless gateways and ARM600 is initiated by the wireless gateways.

Use of a private APN is recommended. The cellular operator's access router provides routing between the IP addresses of the SIM cards and the M2M gateway.

The added value of ARM600 in a private APN use case comes from the added security, end-to-end routing from central LAN to remote LAN and centralized device management.

### ARM600 in the company's DMZ

The DMZ is a safe subnet, separated by firewalls from the company LAN and from the Internet. The servers requiring accessibility from the Internet are placed in the DMZ. The company's border router/firewall forwards the VPN port from the public IP to ARM600, which has a private IP address and uses the border router as a default gateway.

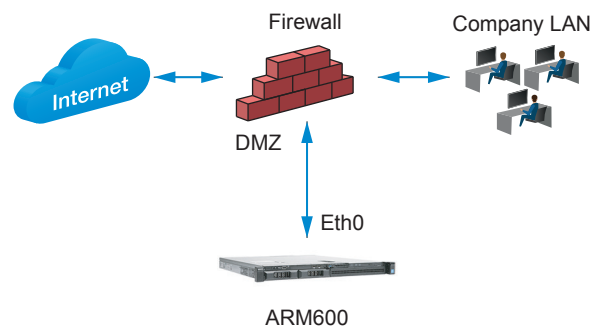


Figure 6: DMZ installation



ARM600SW should only be installed behind the company firewall according to [Figure 7](#).

### ARM600 behind the company's firewall

In this setup ARM600 is directly connected to the company's LAN. ARM600 has a private IP address and the border router/firewall forwards packets from a public, static IP address to ARM600.

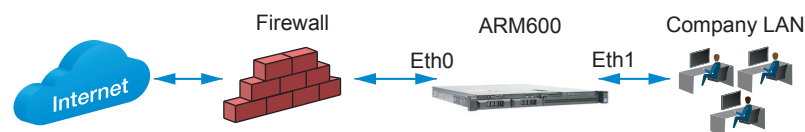


Figure 7: Border firewall installation

### ARM600 directly connected to the Internet

In the simplest scenario, ARM600 is directly connected to the Internet, that is, the public, static IP is configured to the WAN interface of ARM600. ARM600 itself works as a firewall and border router in this case.



*Figure 8: Directly connected to internet installation*



ARM600SW should only be installed behind the company firewall according to [Figure 7](#).

---

## Section 3      Cybersecurity

### 3.1      Cybersecurity definition

Cybersecurity aims to secure the properties of the organization against security risks. To strengthen the system and increase the security level towards any cybersecurity attacks from the Internet, certain actions are recommended while configuring the device.

- The device should be installed physically secure, for example, in a locked cabinet.
- The latest security updates need to be installed for all network devices.
- The network inventory needs to be documented and kept up to date.
- Unused services and interfaces should always be disabled.
- Only VPN connections should be used to access remote networks.

### 3.2      Configuring firewall and services

Enable the firewall and disable the unused services and interfaces in the device. To start, disallow traffic and allow only the needed traffic. Use the default policy to drop connections.

- Check that the firewall is enabled.
- For incoming connections, always filter (drop) all unused ports which may include DNS, L2TP-VPN, SNMP and so on.
- Check that the default action is “drop” in firewalls and allow only the needed ports.
- Set unique passwords for each device.
- Keep passwords stored in a safe place, for example, Encrypted password management tool.
- Check that all unused services are disabled.
- If possible, allow IP connections only via VPN.
- Back up the configuration.

---

## 3.3 Software updates

ARM600SW is updated using the product's official software repository which offers a fast update cycle making the product up-to-date all the time. Software repository access requires a valid SSL certificate file installed in the system. This certificate is supplied with the ARM600SW software ISO file.



---

## Section 4      Getting started

### 4.1      Configuring ARM600 (only for ARM600 hardware variants)

ARM600 is delivered with factory pre-installed software. As the configuration is performed with a Web browser, no additional software is needed. Follow the recommended configuration order.



Do not use any install media possibly delivered with the server.

1. Rack mount ARM600.
2. Connect the cables.
3. Log in to ARM600 using the WHML.
4. Enable and configure the eth1 interface.
5. Configure the eth0 interface.
6. Configure the VPN, firewall and time settings.

### 4.2      Rack mounting ARM600 (only for ARM600 hardware variants)

- To install ARM600 to 19" computer rack, follow the instructions provided with the ARM600 server.



Some racks require specific mounting kits and power cords. See the rack's documentation for details.

---

## 4.3 Connecting cables (only for ARM600 hardware variants)

1. Verify that the available AC operating voltage complies with the hardware specifications.
2. Insert the AC power cord to ARM600 and connect the other end to the AC socket or rack's power rail.
3. Connect the Ethernet cable between the PC and the ARM600 Ethernet port eth0 (located on the back panel).  
VGA display and USB keyboard are not needed for configuring ARM600. They can be used if a local console access is needed.

## 4.4 Setting up virtual machine environment (only for ARM600SW)

ARM600SW supports running in virtual machine environment such as VMware vSphere ESXi 6.7 or later.

1. Select the VMware settings.
  - For ARM600SW and max. 200 Arctic connections
    - 2 or more vCPUs
    - 8 GB or more RAM
    - 32 GB or more hard disk space
  - For ARM600SW and max. 2000 Arctic connections
    - 8 or more vCPUs
    - 32 GB or more RAM
    - 32 GB or more hard disk space

For detailed VMware vSphere setup instructions, see the official VMware documentation at <https://www.vmware.com>.

## 4.5 Creating users for ARM600

ARM600 has root login disabled and there are no default users in the system.



The first created user gets admin privileges by default. Create the first user immediately after connecting the system to the network.

1. Configure your PC to use the same IP address space as ARM600.  
The default IP address of ARM600 is 10.10.10.10.  
Example: Laptop IP is 10.10.10.11 with netmask 255.255.255.0.
2. In a Web browser, connect to **https://10.10.10.10:10000/create\_user.php**.
3. Create usernames and passwords as needed.

## 4.6

### Logging in

1. In a Web browser, connect to the ARM600 WHMI on port 10000 using the HTTPS protocol.

- **https://ARM600\_ip\_address:10000**

The WHMI uses self-signed certificates. Click the **Add an exception** button to add a security policy exception or click the **Continue to this Website** text during login, depending on the browser in use.

2. Enter the username and password.



# Section 5 Web HMI

## 5.1 Menu structure

The WHMI menu structure contains six main menus and the related submenus. The menu structure is always visible on the left pane.

- System
- Network
- VPN
- Firewall
- Arctic Patrol
- Tools

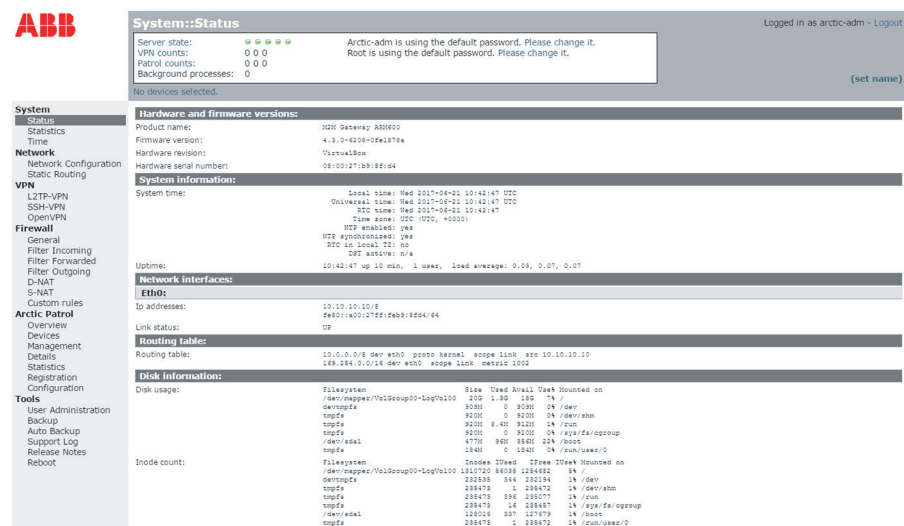


Figure 9: Menu structure

## 5.2 System menu

The system menu contains the system overview and time settings.

### 5.2.1 Status

This submenu is shown after login. It displays details of the hardware, network interfaces and firewall status.

---

## 5.2.2 Statistics

This submenu presents performance indicator graphs for a quick summary of the ARM600 server historical performance statistics.

- Graphically illustrated system load, free memory, number of processes, swap and root file system usage, log disk slice size, number of connected Arctic Patrol clients and VPN connections and RX/TX traffic figures of the network interfaces
- Pre-defined warning levels of KPIs, such as system load, process count, memory usage, swap usage, hard disk space and hard disk nodes

## 5.2.3 Time

This submenu is used to control time settings. There are two options.

- Manual time setting
- Using NTP server to acquire and keep the correct time

ARM600 can work as a time server to provide time to the LAN or VPN connected devices.

By default, the time setting is configured as NTP client using the NTP pool servers. If another NTP server is required, the NTP server's name or IP address can be entered and the availability tested by clicking the Test NTP servers button.



Configure the DNS server's IP address if DNS names are used for the NTP server.

## 5.3 Network menu

The network menu contains the network interface configuration and static routing settings.

### 5.3.1 Network configuration

This submenu is used to configure IP addresses, netmask and other network interface related settings.

### 5.3.2 Static routing

This submenu is used to configure static routing. Static routing is needed if LAN subnets beyond the ARM600's LAN need to be reached via a router in the

ARM600's LAN. A typical example is a separated SCADA LAN when the ARM600's LAN interface is in the DMZ.

A new static route can be configured by selecting the network interface from the drop-down menu and entering the network, netmask and gateway values.

## 5.4 VPN menu

Three types of VPN can be configured in the VPN menu. L2TP-VPN and SSH-VPN are vendor-specific implementations, whereas OpenVPN is an open implementation.



OpenVPN is the only recommended option.



Active SSH-VPN connections are not disconnected automatically after an SSH-VPN server restart.

### 5.4.1 L2TP-VPN

This submenu is used to configure L2TP-VPN. Because of the lack of encryption, it is recommended to use L2TP-VPN only in installations where an additional security layer is present.

If L2TP-VPN is used, the peer name in ARM600 must match the hostname of the Arctic wireless gateway/controller.

### 5.4.2 SSH-VPN

This submenu is used to configure SSH-VPN.

By default, SSH-VPN only supports the SSH v2 protocol. If needed for legacy devices, SSH v1 support can be enabled with legacy support as described in [SSH legacy mode](#). SSH-VPN works on top of the TCP protocol.

If SSH-VPN is used, the peer name in ARM600 must match the hostname of the Arctic wireless gateway/controller. The public SSH keys must be interchanged between ARM600 and Arctic wireless gateways/controllers.

### 5.4.3 OpenVPN

This submenu is used to configure OpenVPN.

OpenVPN uses UDP protocol by default. There are two operating modes.

- Layer 3 is a routed solution meaning that ARM600 and the Arctic wireless gateways work as routers. ARM600 and each Arctic device have unique LAN subnets.
- Layer 2 is a bridged solution where all the devices belong to the same LAN subnet (to the same Ethernet broadcast domain) and all Ethernet broadcast traffic is sent over VPN tunnels to all devices.

In most cases, the recommended operation mode is Layer 3 VPN.

### 5.4.3.1

#### OpenVPN with firewall

The built-in firewall in ARM600 affects the IP packets routed through an OpenVPN server because they belong to the same IP layer of the host ARM600. The *Client to client* setting of the OpenVPN server alters this behavior.

The default setting is that *Client to client* is enabled which means that the VPN tunnel is not affected by the firewall rules.

If the *Client to client* setting is enabled, the packets sent over that particular VPN tunnel from one client to another on the same VPN network never reach the host ARM600 network stack which is, therefore, not affected by the firewall settings by default. This simplifies the scenario that clients need to be able to connect to each other over an OpenVPN tunnel.



A disabled *Client to client* setting does not mean that the traffic from one client to another is blocked; that traffic is just not routed directly through the VPN tunnel. If clients need to be isolated, add a firewall forwarding rule for the VPN tunnel network interface which drops that traffic.

## 5.5

### Firewall menu

ARM600 has a built-in stateful firewall. In addition to the firewall settings, the firewall menu contains D-NAT and S-NAT settings that control pre- and post-routing packet forwarding (network address translation).

### 5.5.1

#### General

This submenu contains general settings of using the firewall, using network address translations and default actions for incoming, forwarded and outgoing packets.



---

## 5.5.2 Filter incoming

This submenu is used to configure the incoming packets that arrive at ARM600 and are not forwarded, that is, the packets are related to using the M2M services like WHMI or the VPN tunnel creation.

The default action is “drop” meaning that only packets matching the rules (white-listed) are accepted, and the others are dropped.

## 5.5.3 Filter forwarded

This submenu is used to configure the forwarded packets coming to ARM600 from one interface and leaving from another.

The default action is “pass”, which allows packets to be forwarded from an interface to another.

By default, there is one “drop” rule which drops packets that come from eth0 (WAN interface) and leave from any interface. This prohibits packets from the Internet from accessing any internal network.

## 5.5.4 Filter outgoing

This submenu is used to configure the outgoing packets leaving from ARM600 for other network elements. By default, all outgoing packets are allowed.

## 5.5.5 D-NAT

This submenu is used to adjust forwarding packets based on their destination address or port. Usually the port forwarding is not needed in ARM600.

## 5.5.6 S-NAT

This submenu is used to adjust the packets’ source addresses. S-NAT is needed, for example, when ARM600 is used as a border router to Internet.

## 5.5.7 Custom rules

The custom rules are for the experienced user who has knowledge of iptables configuration. When custom rules are used, the rule set must contain all needed tables (incoming, forwarded, outgoing, D-NAT and S-NAT).

## 5.6 Arctic Patrol menu

The Arctic Patrol centralized monitoring and administration tool is used via this menu.

ARM600 includes the Arctic Patrol centralized device management application. Arctic Patrol provides condition monitoring of the cellular connections, statistical data of network usage, direct access to the connected Arctic 600 series wireless gateway user interfaces, automatic backup of Arctic 600 series wireless gateway configurations and alarms from any faults in the availability of the Arctic 600 series wireless gateways. The Arctic Patrol interface can be accessed via ARM600. It offers information about the entire communication system status at a glance.

- Pre-installed in M2M Gateway ARM600
- Condition monitoring of cellular connections
- Statistical data of network usage
- Direct access to the connected Arctic 600 series wireless gateway user interfaces
- Automatic backup of Arctic 600 series wireless gateway configurations
- Communication network faults generate alarms
- Individual or mass updates of all connected Arctic 600 series gateway firmware
- Individual or mass updates of all connected RIO600 firmware

Status (total 10):

Errors 0

Warnings 0

OK 10

VPN (total 11):

Never connected 0

Down 0

Up 10

VPN Type:

All

Filter:

Off

Page refresh:

Reset all filters

#	Accept devices	Status	VPN	Name	Location	Serial number	Firmware	Connection	Signal Level	IP Address	Uptime	Last Patrol Connection	VPN Status	VPN RX	VPN TX	Actions
#1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ATF116	1VHB71028431		3.4.9	Mobile WAN, SIM1	Very good SIM1	10.10.116.116/24 fe80::206:70ff:fe05:529/64	1 month	5 mins ago	Up 2 days OpenVPN	55.9 MB	53.3 MB	<a href="#">Web UI</a>
#2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ATF128	1VHB71010011		3.4.9	Mobile WAN, SIM1	Very good SIM1	10.10.128.128/24 fe80::206:70ff:fe04:14/64	8 months	37 secs ago	Up 7 days OpenVPN	190.5 MB	188.1 MB	<a href="#">Web UI</a>
#3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ATF130	1VHB71010007		3.4.9	192.168.130.2		fe80::206:70ff:fe04:c/64 10.10.130.130/24	8 months	1 min ago	Up 15 days OpenVPN	349.5 MB	329.8 MB	<a href="#">Web UI</a>
#4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ATF132	1VHB71010025		3.4.9	Mobile WAN, SIM1	Good SIM1	10.10.132.132/24 fe80::206:70ff:fe04:26/64	8 months	2 mins ago	Up 10 hours OpenVPN	12.2 MB	11.7 MB	<a href="#">Web UI</a>
#5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ATF134	1VHB71010022		3.4.9	Mobile WAN, SIM1	Normal SIM1	10.10.134.134/24 fe80::206:70ff:fe04:1a/64	6 months	4 mins ago	Up 10 hours OpenVPN	12.3 MB	11.6 MB	<a href="#">Web UI</a>
#6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ATF136	1VHB91000000		3.4.9	192.168.136.2		fe80::206:70ff:fe04:1/64 10.10.136.136/24	8 months	2 mins ago	Up 10 hours OpenVPN	6.7 MB	6.2 MB	<a href="#">Web UI</a>
#7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ATF138	1VHB91200003		3.4.9	Mobile WAN, SIM1	Very good SIM1	10.10.138.138/24 fe80::206:70ff:fe02:10/64	8 months	59 secs ago	Up 1 day OpenVPN	33.3 MB	33.6 MB	<a href="#">Web UI</a>
#8	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ATF140	ARCHX28-454-128-029388		3.4.9	192.168.140.2		fe80::206:70ff:fe02:9388/64 10.10.140.140/24	8 months	9 secs ago	Up 15 days OpenVPN	343.9 MB	324.6 MB	<a href="#">Web UI</a>
#9	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ATF142	AUG6248-400-328-022BE9		3.4.9	Ethernet WAN		10.10.142.142/24 fe80::206:70ff:fe02:2bea/64	8 months	4 mins ago	Up 15 days OpenVPN	211.2 MB	207.2 MB	<a href="#">Web UI</a>
#10	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ATF144	AUG6248-400-328-0304CA		3.4.9	Ethernet WAN		10.10.144.144/24 fe80::206:70ff:fe03:4cb/64	8 months	3 mins ago	Up 15 days OpenVPN	117.3 MB	93.0 MB	<a href="#">Web UI</a>

Figure 10: Arctic Patrol user interface

---

### 5.6.1 Overview

This submenu shows the number of VPN tunnels and Patrol clients. It also shows how many are up/down, how many have never connected and what are the reported signal levels.

### 5.6.2 Devices

This submenu shows the most important details of the Arctic wireless devices, such as VPN and Patrol connections, hostnames, firmware versions, signal levels, IP addresses, uptimes and data amounts of VPN tunnels.

The WHMI of the Arctic device can be accessed by clicking the Web UI button.

### 5.6.3 Management

This submenu provides fleet management functions for upgrading the firmware or rebooting multiple devices as a batch run. The devices need to be selected from the Devices submenu before a batch run can be done.

### 5.6.4 Details

This submenu shows device-specific details that are useful for troubleshooting. The device's configuration can also be viewed.

### 5.6.5 Statistics

This submenu shows historical statistics of the devices and is also useful for troubleshooting.

### 5.6.6 Registration

This submenu provides a method for pre-registering the Arctic wireless devices to ARM600. The connection mode (HTTPS or SSH) is selected and the wireless device's serial number is entered. If the SSH mode is used, the client configuration (including SSH keys) is copied to the Arctic wireless device.

### 5.6.7 Configuration

This submenu contains a registration password, which needs to be copied to Arctic cellular devices. It is used only for the initial Patrol connection. ARM600 provides a strong unique password for each Arctic cellular device once Arctic is accepted from the device screen.

---

The other configurable parameters consist of alert from and to email addresses, mailing intervals and statuses, time intervals for status changes and whether to store historical data or not.

## 5.6.8 Profiles

This submenu shows RTU configuration files and allows configuring multiple Arctic devices using XML configuration profile templates.

## 5.6.9 Device firmware

This submenu shows Arctic and RIO600 firmware packages that are stored on ARM600. It also provides functionality to list and download the latest published Arctic wireless device firmware packages to ARM600 if ARM600 is connected to the Internet.

## 5.7 Tools menu

The tools menu is used to configure users and backups, take snapshots of log files for technical support purposes, view release notes and reboot the ARM600 server.

### 5.7.1 User Administration

This submenu is used for defining user rights, changing passwords, setting password lifetime and adding new users.

#### 5.7.1.1 Adding users

1. Click **Add user** to add a new user to the ARM600 system.
2. On the **Add user** page, enter a username and click **Add**.  
A password is automatically generated for the new user.



Copy the password as it cannot be recovered after leaving the **Add user** page. This password must be changed before logging in for the first time.

3. Add the new user to the appropriate user groups as instructed in [Editing groups](#).

### 5.7.1.2 Setting password history

1. Under **Password history settings**, enable or disable the password history functionality.
2. Set the number of remembered passwords.  
With this functionality the users cannot use the same password repeatedly making the system more cyber secure.

### 5.7.1.3 Changing password and setting password lifetime

1. Select a user and click **Change password**.
2. Under **Password expiration**, set the password's minimum and maximum lifetime.  
With this functionality the users are forced to change their password periodically making the system more cyber secure.
3. Click **Set password expiration**.

### 5.7.1.4 Editing groups

1. Select a user.
2. Under **Group(s)**, click **Edit groups**.
3. Assign a group from the **Selected groups** area to the new user.

**Table 2:** *User groups and functions*

User groups	Functions
admin-ssh	User gets access to SSH port 10022.
admin-web	User gets full access to ARM600 WHMI.
users	Default group for all users in the ARM600 system
wheel	User gets super user rights.

## 5.7.2 Backup and Auto backup



During the system backup and restore or update it is possible that the user home directories are deleted and recreated. Any information stored in the user home directories is erased during the process.

This submenu is used for performing backup and auto backup functions.

Backup is used to create and restore backups and upload/download them from/to a PC. ARM600 contains a factory backup that can be used for reverting to the factory configuration. However, the IP addresses of network interfaces are not reverted to factory defaults. Both standard backup and full backup are configuration backups and they cannot be used for full disaster recovery.

Auto backup is used to configure ARM600 to back up the configuration to an additional standby ARM600. The data transfer method is rsync over SSH.



Starting from version 5.0.1, backups use a dedicated service user account for improved cybersecurity.

**Table 3:** *Compatibility between source and target systems in auto backups*

Source system	Target system	Compatibility
4.5.3 or older	Fresh installation of 5.0.1	Incompatible Starting from 5.0.1, there is no default user anymore, which prevents using older auto backup targets.
4.5.3 or older	4.5.3 first updated to 5.0.1 with the "update installer" script	Incompatible Starting from 5.0.1, there is no default user anymore, which prevents using older auto backup targets.
5.0.1	4.5.3	Compatible Target address for the auto backup requires the username, for example, "arctic-adm@10.10.10.10".

### 5.7.3

## Support Log

This submenu is used to download the system log and ARM600 configuration collection to a PC. The support log is used for troubleshooting purposes.

### 5.7.4

## Release Notes

This submenu contains the release notes for the currently running ARM600 firmware version.

### 5.7.5

## Reboot

This submenu is used to reboot the ARM600 server. A verification dialog box opens after the reboot button is clicked.

## Section 6 Network configuration

### 6.1 Configuring Ethernet interfaces

The Ethernet interfaces are configured using the WHMI.

1. Log in to the ARM600 WHMI.
2. On the left pane, under **Network**, click **Network Configuration**.
3. Click the **Network Interfaces** icon.  
The **Network Interfaces** pane opens.
4. Click **Edit interface eth1** and configure the eth1 parameters.



It is recommended to configure the eth1 interface first if applicable, as the PC is usually connected to ARM600 via the eth0 interface (applies only to ARM600 hardware variants).



Change the IP address and netmask according to the required setup. Either set the netmask or the prefix (number of bytes in netmask), not both.

**Table 4:** *Eth1 settings*

Parameter	Value
Device	eth1
BOOTPROTO	none
IPADDR	<IP address>
NETMASK <sup>1)</sup>	<netmask>
PREFIX <sup>1)</sup>	<prefix>
DEFROUTE	No
IPV6_DEFROUTE	No

1) Set either the netmask or the prefix

5. Click **Save**.
6. Click **Restart interface eth1**.
7. Click **Edit interface eth0** and configure the eth0 parameters based on the information received from the Internet Service Provider or from the ICT department.



As the public IP address of ARM600 is case dependent, it is not possible to define an example. If ARM600 is located in

DMZ, the eth0 IP address can be a private IP address. In that case the specific ports are forwarded to ARM600 by the border router.

**Table 5:** *Eth0 settings*

Parameter	Value
Device	eth0
BOOTPROTO	none
IPADDR	<IP address>
NETMASK <sup>1)</sup>	<netmask>
PREFIX <sup>1)</sup>	<prefix>
GATEWAY	<gateway IP>
DNS1, DNS2	Set the DNS servers, if needed.
DEFROUTE	Yes
IPV6_DEFROUTE	Yes

1) Set either the netmask or the prefix



The default route is usually set pointing to the router in the ARM600's eth0 subnet. The Arctic devices usually connect from unknown (dynamic) IP addresses via the eth0 interface, which is by default the WAN interface in ARM600.

8. Click **Save**.
9. Click **Restart interface eth0**.



The IP address of the eth0 interface used for the current connection to ARM600 has now been changed. After the changes to the eth0 IP address have been applied, the browser is not able to connect to ARM600 using the address `https://10.10.10.10:10000`.

10. Switch the Ethernet cable from the ARM600's eth0 port to the eth1 port (applies only to ARM600 hardware variants).

At this point, there is usually no need for adding static routes. If the SCADA or other control entity is in a different subnet than the ARM600 LAN, define a static route to that subnet. Do not define static routes over dynamic VPN tunnels.



## 6.2 Ethernet interface setup parameters

**Table 6:** *Ethernet interface configuration parameters*

Parameter	Description
DEVICE	Network interface device name
BOOTPROTO	"None" is used for static IP addressing; "DHCP" is used for dynamic addressing.
IPADDR	IP address allocated for this interface
NETMASK	Netmask in dotted notation, for example, 255.255.255.0
PREFIX	Netmask bits, for example, 24 (either NETMASK or PREFIX needed)
GATEWAY	IP gateway's address for this interface
DNS1, DNS2	Domain name servers for this interface
ONBOOT	Interface enabled/disabled in boot up
IPADDR0	First additional IP address associated to this interface
PREFIX0	Number of netmask bits for the first additional IP address
IPADDR1	Second additional IP address associated to this interface
PREFIX1	Number of netmask bits for the second additional IP address
IPADDR2	Third additional IP address associated to this interface
PREFIX2	Number of netmask bits for the third additional IP address
IPV6INIT	Enable/disable IPv6 for this interface
DEFROUTE	Use this interface as IPV4 default route
IPV4_FAILURE_FATAL	Consider interface failed if IPV4 configuration fails
IPV6_AUTOCONF	Control IPv6 autoconfiguration
IPV6_DEFROUTE	Use this interface as IPV6 default route
IPV6_FAILURE_FATAL	Consider interface failed if IPV6 configuration fails
IPV6_PEERDNS	Allow the resolv.conf to be modified according to DHCP server
IPV6_PEERROUTES	Allow the default gateway to be modified according to DHCP server
UUID	Universal unique identifier for the interface
TYPE	Interface type
NAME	Name of the interface as displayed in the Network Connections



---

## Section 7 Arctic Patrol

### 7.1 Overview

The Arctic Patrol application runs on ARM600 and provides a Web-based HMI interface. The Arctic Patrol application is used for condition monitoring and centralized management of field devices. The centralized management enables, for example, remote updating of the Arctic wireless devices' firmware in larger batches as opposed to device-by-device. The asset management in Patrol is a feature of the ABB Arctic product line, but it also supports other ABB products that have been connected to a remote Arctic wireless device.

The available actions shown in Arctic Patrol depend on the features and devices that the Arctic wireless devices have reported. The Arctic wireless devices' local network is scanned for supported ABB products only, if the feature has been enabled in the Arctic wireless device.

### 7.2 Registering Arctic devices to Patrol

The registration page in Arctic Patrol allows creating a configuration that can be imported into an Arctic device during the configuration phase.

1. Log in to ARM600's WHMI.
2. On the left pane under the **Arctic Patrol** menu, select **Registration**.
3. Select the Patrol protocol to be used.

The Patrol main functionality is the same regardless of the chosen communication protocol. The SSH protocol is selected as an example in this instruction.

- SSH
- HTTPS



The border firewall must allow the use of TCP 22 (default) or TCP 10000 port in order to get the Patrol working.

**Table 7:** *Protocol comparison*

Feature	SSH	HTTPS
Response time	Quicker	Slower
Connection type	"Always on"	Interval-based
Protocol port (TCP)	22	10000

4. Click **No** to confirm that there is no existing SSH public key.
5. Define the device information and click **Register device**.
  - Arctic device's serial number
  - ARM600's IP address (usually public)
  - Connection mode
  - Connection interval

patrol -> registration -> ssh -> generate

**Device information for SSH Patrol protocol**

Device serial number:  ⓘ

Host IP and port:   ⓘ

Connection mode: Continuous ☒ Polling ☐ ⓘ

Connection interval (seconds):  ⓘ

**Figure 11:** *Defining device information*

The next screen shows the ready-made configuration content that needs to be copied to the Arctic device.

```
patrol -> registration -> ssh -> generate
```

Copy this to your Arctic device to complete registration.

```
{
  "serialnumber": "1VHB91201361",
  "protocol": "ssh",
  "connectionmode": "continuous",
  "connectioninterval": "1500",
  "host": "10.10.10.5",
  "port": "22",
  "sshpublickey": "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDdcqXaZNJwcv
z/qyBnLehCr2ALNEnXrfBcU7UQ7uX3g2Ul8nC6corep8YL
Rbc0A2FbLAXQ3IAaV6l77kwp2SldlSxgBBi5LTEjfPIvX2kz
K3fjimRGJV9PMcsr5IgfWxafq0ypidJXFyZ6BwHhSt8UlrW
  "sshprivatekey": "-----BEGIN RSA PRIVATE KEY-----
\pMIEFowIBAAKCAQEA3YKl2mTScHMNvFim+d8eWz7xd
```

Figure 12: Configuration content

6. Log in to the Arctic device as the arctic-adm user.
7. Click **Arctic Patrol** and select **Import New**.
8. Paste the configuration content to the **Patrol configuration file** box and click **Submit**.

Arctic Patrol configuration (easy setup)

Patrol configuration file

```
{
  "serialnumber": "1VHB91201361",
  "protocol": "ssh",
  "connectionmode": "continuous",
  "connectioninterval": "1500",
  "host": "10.10.10.5",
  "port": "22",
  "sshpublickey": "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQBAQDdcqXaZNJwcw28WOb53x5Zr
vF3kHfhTZFZ8HIWOJFbNrGC3tj7F8bj
9rlnmoqYLvzmsANnTu0lz/qyBnLehCr
2ALNEhXrfBcU7UQ7uX3g2UI8nC6cor
ep8YLV9T6rLPQ7WzrylXm89AXjJVc6
7ALGtX4YE+ca52XL7dHFAAT3BEV7
RF+T/bD1Rbc0A2FbLAXQ3IAaV6I77k
wp2SldlSxgBBi5LTEjPlvX2kZQ3XpJC
StSfc2AwMUukPKp5gRhE2JNz/rPJ38
K3tmMegOGS1QG/sDBYB3nfnjK3fjm
RGJV9PMcsr5lqfWxafq0ypidJXFyZ6B
```



Submit

Reset

Figure 13: Pasting configuration content

Once the configuration is submitted, the Arctic Patrol connections are shown. The configuration can be edited by clicking the pen and paper icon or deleted by clicking the trash can icon.

The configured Arctic Patrol connection(s).  
Click edit to show details.

Arctic Patrol connection(s)						
Enabled	Name	Protocol	Server IP	Server Port	Remote management	
Yes	10.10.10.12:22	SSH	10.10.10.10	22	Yes	 

Create new

Import new

Figure 14: Editing configuration

9. Reboot the Arctic device.
10. Log in to ARM600's WHMI, click **Arctic Patrol** and select **Devices**.
11. Select the check box of the new Arctic device, select **Accept devices** from the drop-down list and click **Do action**.

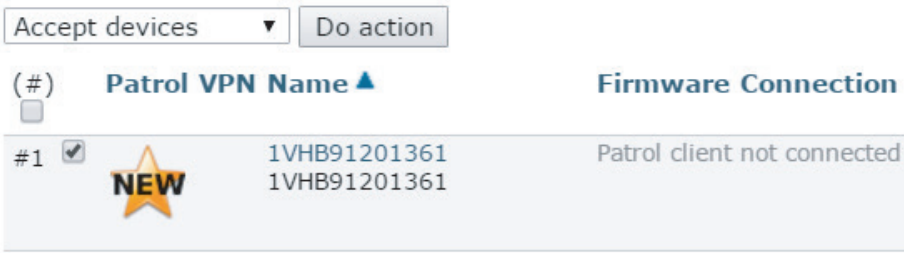


Figure 15: Accepting devices

12. Click **OK** in the verification dialog box.

When the Arctic device is rebooted and accepted in ARM600’s Patrol, the device details and configuration file are transferred to ARM600. The device details are shown in the ARM600’s Patrol view.

(#)	Patrol VPN Name ▲	Firmware Connection	Signal Level	IP Address	Uptime	Last Patrol Connection	VPN Status	VPN TX	VPN Actions
#1	testclient1 1VHB91201361	3.3.1		10.10.10.10/24 fe80::206:70ff:fe02:a068/64	2 mins	3 mins ago	No VPN configured		<a href="#">Web UI</a>

Figure 16: Device details

7.2.1

Allowing Arctic devices to scan local networks

Arctic devices are able to scan their local networks for supported devices such as RIO600.

1. Log in to the Arctic device as the arctic-adm user.
2. To edit the Patrol connection in the Arctic device’s WHMI, click **Services**, select **Arctic Patrol** and click the pen and paper icon next to the Patrol connection.
3. In the **Allow LAN device SCAN** drop-down list, select **Yes** to enable scanning for the supported devices.

Options	
Backup active configuration to server	<div>Yes</div> <div>Copy encrypted version of XML configuration file to server. Can be used for device replacement in case of a broken device.</div>
Allow remote management	<div>Yes</div> <div>Enable Patrol remote management</div>
Allow LAN device scan	<div>No</div> <div>Yes</div> <div>Allow this device to periodically scan its local network for ABB devices. Currently supported devices: RIO600</div>

Submit

Reset

Figure 17: Allowing LAN device scan

4. Click **Submit**.
5. Reboot the device for the changes to take effect.



The Arctic device's local network is scanned for new devices about twice per hour at the most. If a non-continuous Patrol connection is configured, the scanning is limited to the chosen connection interval. Only networks with a netmask of 255.255.255.\* are scanned to avoid excessive scanning time.

## 7.3 Asset management

With the asset management features in the Arctic Patrol application, it is possible to remotely batch update the Arctic wireless devices. Additionally, RIO600 update actions can also be performed from a remote Arctic wireless device through the ARM600's WHMI. The asset management functionality is developed on top of the Arctic Patrol application, which is a centralized management system running in ARM600 (server) and Arctic wireless devices (clients).

When one or more devices have been selected in the device list via **Arctic Patrol/Devices**, these devices can be managed using the actions available via **Arctic Patrol/Management**. The available actions depend on the selected device types. Arctic wireless devices report a list of the supported API commands to the Arctic Patrol application. These management commands can be executed remotely from the Arctic Patrol application interface for one or several devices.

In addition to the API commands, a list of more advanced management tools may be available via **Arctic Patrol/Management** depending on the type of device that has been selected via **Arctic Patrol/Devices**. These tools typically use the more simple API commands in the background.

[Figure 18](#) illustrates the API commands and tools available when both an Arctic wireless device and a RIO600 device have been selected in the device list.



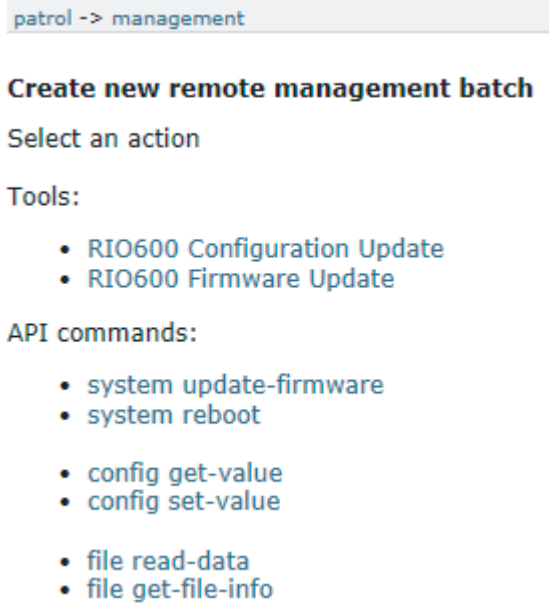


Figure 18: Available API commands



Asset management is available from ARM600 Ver.4.2.1 onwards.

### 7.3.1

## Selecting devices for device management

To manage devices through the ARM600's Arctic Patrol application, they have to be first selected from the Patrol device list. When the Arctic device has been set to scan local networks, the detected devices are visible in the Arctic Patrol application's device list. The devices are listed as a sub-device below the Arctic device that found the device on its local network.

1. Log in to the ARM600's WHMI as the arctic-adm user.
2. On the left pane under the **Arctic Patrol** menu, select **Devices**.
3. Choose one or more devices to be managed by selecting the check box next to the device.  
The selected devices are listed in the top part of the ARM600's WHMI.
4. Perform an action on the selected devices in one of the alternative ways.
  - Select **Manage devices** from the drop-down menu and click **Do action**.
  - On the left pane under the **Arctic Patrol** menu, select **Management**.


Manage devices ▼		Do action	
(#)	<input type="checkbox"/>	Patrol VPN	Name ▲ Firmware
#1	<input checked="" type="checkbox"/>		arctic-0288fa AUG8248-400-328-0238E7 3.3.1

Figure 19: Managing devices



For optimal performance, it is recommended to perform actions on 100 devices at the maximum at a time.

## 7.3.2 Arctic device management

The Arctic wireless devices can be managed using the API commands from the ARM600's WHMI Arctic Patrol application. The management commands can be executed remotely from the Arctic Patrol application interface for one or several Arctic devices as part of the asset management functionality.

### 7.3.2.1 Updating Arctic device firmware via ARM600 (only for ARM600 hardware variants)

The asset management functionality enables a batch update possibility. First the firmware file is uploaded to ARM600 via the WHMI and then ARM600 performs the batch update as a background process. This requires Arctic devices with firmware Ver.3.3.1 or later.

Arctic and RIO600 firmware packages that are stored on ARM600 can be viewed via **Arctic Patrol/Device Firmware**. The **Arctic Patrol/Device Firmware** page provides functionality to list and download the latest published Arctic wireless device firmware packages to ARM600 if ARM600 is connected to the Internet. When there are new Arctic firmware versions available, notifications are visible on the upper pane of the ARM600's WHMI if ARM600 is connected to the Internet.



For the ARM600's automatic fetching of the Arctic device firmware, allow TCP connections on port 443 (HTTPS) to the host [arcticupdate.abb.com](https://arcticupdate.abb.com).

1. Select the Arctic devices to be managed.
2. On the left pane under the **Arctic Patrol** menu, select **Management**.
3. Verify that the hostnames of the selected devices are correct and select **system update-firmware** under **API commands**.
4. Click **Choose File** and select the firmware file to be uploaded from PC to ARM600.

- 5. Click **Upload** and use the **Firmware** drop-down menu to verify that the firmware is correct.
- 6. When the file has been uploaded to ARM600, verify that all the devices are compatible with the firmware update action.
- 7. Click **Run this action for all selected devices** to run the batch update.

**New batch for remote devices**

**Action:** update-firmware

**Compatible devices for this action:**  
- AUG8248-400-328-0238E7

**Incompatible devices for this action:**  
- All devices are compatible

Fill required parameters:

firmware = 

[ Choose firmware ]

or upload new firmware: 

Choose File

 No file chosen

Back

Run this action to all selected devices

Figure 20: Updating Arctic firmware

The **Running and old batches list** shows the started batch update. The **Status** column indicates how many of the total number of firmware update tasks have been finished.

The Arctic device’s system log file records the starting and finishing of the firmware update.

```
Sep 14 15:45:32 arctic-0288fa user.info fwupdate.sh: Starting firmware update
...
Sep 14 15:47:25 arctic-0288fa user.info fwupdate.sh: Firmware update OK
```

When all update tasks are finished, the duration of the batch update is shown in the Status column.

**Running and old batches**

[ Select an action ] Do action

ID	Title	Status	Start time	Created by
<input type="checkbox"/> 13	system update-firmware firmware=firmware_arctic2_3.3.1-4937.bin	0 / 1 completed	a few seconds ago	arctic-adm
<input type="checkbox"/> 12	file get-file-info filename=/opt/viola/rw/s.txt	1 / 1 completed, duration 0:00:02	33 minutes ago	arctic-adm
<input type="checkbox"/> 11	Copy /opt/viola/rw/configuration-Last_Boot.xml from device AUG8248-400-328-0238E7	1 / 1 completed, duration 0:04:50	3 hours ago	AUG8248-400-328-0238E7

Figure 21: Running and old batches list for firmware update

7.3.2.2 Updating Arctic device firmware via ARM600SW

The asset management functionality enables a batch update via the WHMI. ARM600 performs the batch update as a background process. This requires Arctic devices with firmware Ver.3.3.1 or later.

Before starting the firmware update process, download the latest firmware updates to ARM600 as described in chapter [Updating firmware for Arctic Wireless Gateways using ARM600SW](#) or using

ARM600  
User Manual

45

the local repository mirror described in chapter [Local software repository mirror](#).

1. Select the Arctic devices to be managed.
2. On the left pane under the **Arctic Patrol** menu, select **Management**.
3. Verify that the hostnames of the selected devices are correct and select **system update-firmware** under **API commands**.
4. Click **Choose File** and select the firmware file to be uploaded from PC to ARM600.
5. Click **Upload** and use the **Firmware** drop-down menu to verify that the firmware is correct.
6. When the file has been uploaded to ARM600, verify that all the devices are compatible with the firmware update action.
7. Click **Run this action for all selected devices** to run the batch update.

New batch for remote devices

Action: update-firmware

Compatible devices for this action:  
- AUG8248-400-328-0238E7

Incompatible devices for this action:  
- All devices are compatible

Fill required parameters:

firmware = 

[ Choose firm Ware ]

or upload new firmware: 

Choose File

 No file chosen

Back

Run this action to all selected devices

Figure 22: Updating Arctic firmware

The **Running and old batches list** shows the started batch update. The **Status** column indicates how many of the total number of firmware update tasks have been finished.

The Arctic device’s system log file records the starting and finishing of the firmware update.

```
Sep 14 15:45:32 arctic-0288fa user.info fwupdate.sh: Starting firmware update
...
Sep 14 15:47:25 arctic-0288fa user.info fwupdate.sh: Firmware update OK
```

When all update tasks are finished, the duration of the batch update is shown in the Status column.

Running and old batches

[ Select an action ]

Do action

ID	Title	Status	Start time	Created by
<input type="checkbox"/>	13 system update-firmware firmware=firmware_arctic2_3.3.1-4937.bin	0 / 1 completed	a few seconds ago	arctic-adm
<input type="checkbox"/>	12 file get-file-info filename=/opt/viola/rw/s.txt	1 / 1 completed, duration 0:00:02	33 minutes ago	arctic-adm
<input type="checkbox"/>	11 Copy /opt/viola/rw/configuration-Last_Boot.xml from device AUG8248-400-328-0238E7	1 / 1 completed, duration 0:04:50	3 hours ago	AUG8248-400-328-0238E7

Figure 23: Running and old batches list for firmware update

46

ARM600  
User Manual

## 7.3.2.3

## Updating RTU configuration

The RTU configuration in Arctic devices can be updated with Arctic Patrol. ARM600 can keep multiple revisions of an RTU configuration with a specific name. Any old revision can be restored.

1. On the left pane of ARM600's WHMI, under the **Arctic Patrol** menu, select **Profiles**.  
The RTU section on the **Profiles** page shows how many RTU configurations are available.
2. Click **Edit** to proceed.  
The following page lists the RTU configurations available in ARM600.

The screenshot shows the Arctic Patrol web interface. On the left is a navigation menu with categories: System, Network, VPN, Firewall, Arctic Patrol, and Tools. The 'Arctic Patrol' section is expanded, showing 'Overview', 'Devices', 'Management', 'Details', 'Statistics', 'Registration', 'Configuration', and 'Profiles'. The 'Profiles' option is selected. The main content area displays a table of RTU configurations. Above the table, there are status indicators for Server state, VPN counts, Patrol counts, and Background processes. A message box indicates that Arctic-adm and Root are using default passwords and should be changed. The table has columns for Name, Revision, and Checksum. There are four rows of configurations, each with an 'Add new' button next to it.

Name	Revision	Checksum
acd00-nu	4 (3 older)	270d6a741b9306dc13244d8b9be2
acd00-nu	3	4b833b261006a7d54604a6b9c7e272
acd00-nu	2	e14299224610e038186a6537801ade
acd00-nu	1	e826a79d8c65315d95c523c5d08da4a

Figure 24: Available RTU configurations

3. Update the configurations in one of the alternative ways.
  - Add a configuration by clicking the **Add new** button on the page with the available RTU configurations.  
Give a name to the configuration and save it in INI file format by clicking **Save**.



Only the following characters are accepted in the name of an RTU configuration.

- Numbers 0-9
- Letters a-z, A-Z
- Special characters .-

- Click the notepad icon on the right to edit the latest configuration revision.  
A new revision is saved. Every revision has an MD5 checksum so that it can be verified.



If a configuration with the specified name is not found, a new configuration with that name is created with revision 1.

- Edit an older configuration revision by clicking the link **n older** (n being the number of older revisions available) in the column **Revision**. This displays all the revisions of the configuration.
  - Delete the latest configuration revision.  
In the list of RTU configurations, click the trashcan icon.
  - Delete the whole configuration by clicking the trashcan icon for each revision.
4. Send the finished RTU configuration to the Arctic device(s).



When updating the RTU configuration of an Arctic device using Patrol, all the available RTU configurations on the device will be overwritten.

- 4.1. On the left pane under the **Arctic Patrol** menu, select **Management**.
- 4.2. Select **RTU Configuration Update** under **Tools**.
- 4.3. On the next page, review the compatible devices selected and click **Next**.
- 4.4. Select the appropriate RTU configuration from the list displayed and click **Next**.
- 4.5. Select the revision of the RTU configuration and click the **Send configuration** button.
- 4.6. Reboot the Arctic device to activate the RTU configuration.

#### 7.3.2.4

#### Updating device XML configuration

Arctic field devices have their full configuration stored in XML format. ARM600 product Ver.4.5.1 and newer include support for updating the full XML configuration using Arctic Patrol.

The configurations use a template mechanism on ARM600. In each XML configuration file, device-specific parts of the configuration file must be marked using special markers in the XML file. The files must be named as configuration-

xxx.xml where the xxx part can contain the letters a-z and A-Z, 0-9 and hyphens (-).

The tags that mark the device-specific values are of the form `_PRECONFIG_XXX` where XXX is the label/name of a specific setting. The marker tags are always inside html tags since the markers mark a single configuration value in the configuration file. It is important to make sure that all device-specific parts of the configuration have been properly defined in the template using `_PRECONFIG_XXX` tags inside the XML template.

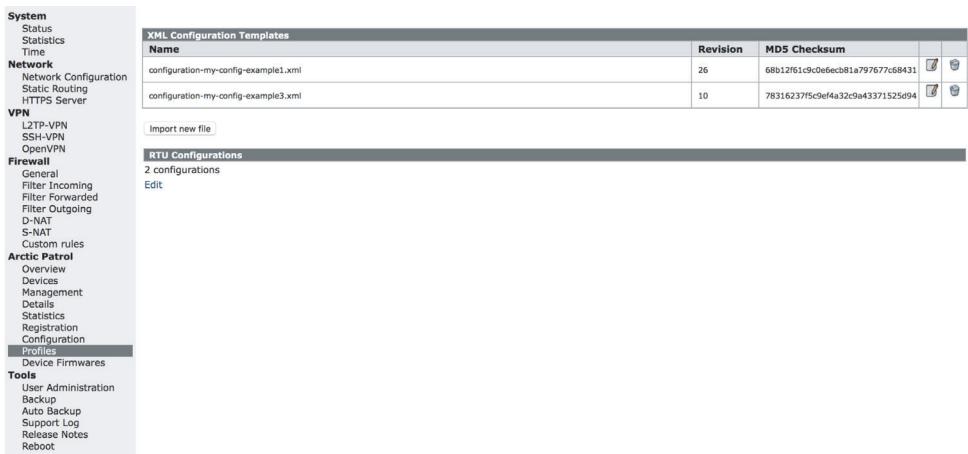


Figure 25: List of XML configuration templates

It is recommended not to use any production field devices for the initial setup but have at least two Arctic devices in a laboratory type of setup so that if any problems arise, the devices can be easily reset to a factory default state.

The typical workflow of using the XML configuration templates is described below.

1. Manually configure a single Arctic device to work as planned in the production system.  
This configuration includes at least Patrol configuration, possibly a VPN configuration and any other configuration that the field devices must have to work as intended.
2. Take the working XML configuration file from the Arctic device and use this as a base for creating a configuration template.
3. Edit the XML configuration file and mark all the device-specific parts of the XML with `_PRECONFIG_XXX` marker tags.
4. Upload the configuration template to ARM600.  
XML files can be imported to ARM600 under the **Arctic Patrol** menu **Profiles** page. The first version of the XML template becomes revision 1 on ARM600. Any changes made and updated after this increase the revision counter automatically.

5. Take a second Arctic device and update its XML configuration using the Patrol Management XML Configuration Update tool.
6. Reboot the second Arctic device to make sure it does not lose any important parts of the configuration file as part of the XML configuration update process.  
If the XML configuration template works as intended, after the reboot the second Arctic device should be able to connect to ARM600 using Arctic Patrol and work as intended.
7. If there are any issues, repeat steps 3 through 6 until the XML configuration template works as intended.  
When the second Arctic is proven to be working as wanted, any other Arctic field devices can be mass-updated at a time.

Typically the following parts of the XML configuration should be marked with `_PRECONFIG_XXX` tags:

- `system.general.hostname: <hostname> _PRECONFIG_HOSTNAME </hostname>`
- `system.user.shadow: <shadow> _PRECONFIG_SHADOW </shadow>`
- `system.console_access.shadow: <shadow> _PRECONFIG_ROOTSHADOW </shadow>`
- `system.cli.password: <password> _PRECONFIG_CLIPASSWORD </password>`
- `network.lans.iface.address: <address> _PRECONFIG_LANIP </address>`
- `network.lans.iface.mask: <mask> _PRECONFIG_LANMASK </mask>`
- `certificates.local_ssh_keys.key.public_key_data: <public_key_data> _PRECONFIG_PATROLSSHPUBLICKEY </public_key_data>`
- `certificates.local_ssh_keys.key.private_key_data: <private_key_data> _PRECONFIG_PATROLSSHPUBLICKEY </private_key_data>`
- `certificates.remote_ssh_keys.key.public_key_data: <public_key_data> _PRECONFIG_PATROLSSHHOSTKEY </public_key_data>`
- `certificates.trusted_cas.key.public_key_data: <public_key_data> _PRECONFIG_VPNCA </public_key_data>`
- `certificates.local_identity.key.name: <name> _PRECONFIG_VPNNAME </name>`
- `vpn.openvpn_client.client.loc_cert <loc_cert> _PRECONFIG_VPNNAME </loc_cert>`
- `certificates.local_identity.key.private_key_data: <private_key_data> _PRECONFIG_VPNKEYDATA </private_key_data>`
- `certificates.local_identity.key.public_key_data: <public_key_data> _PRECONFIG_VPNCRTDATA </public_key_data>`
- `vpn.openvpn_client.client.name: <name> _PRECONFIG_VPNSERVER </name>`
- `vpn.openvpn_client.client.remote_port: <remote_port> _PRECONFIG_VPNPORT </remote_port>`

The tag names described above use the same naming conventions as the ARM600 command line operations *viola patrol create-ssh-clients* and *viola openvpn export-*



*clients*. This way if the field device Patrol configurations and OpenVPN configuration have been mass-created on ARM600 using command line utilities, the field names in the generated CSV files match the XML template's `_PRECONFIG_` tags.

When a working configuration has been set up and tested, multiple field devices can be updated at a time using the XML Configuration Update tool under the Arctic Patrol Management menu.

7.3.2.5                      **Rebooting Arctic devices**

The system reboot enables rebooting a batch of Arctic devices. This is required for example after the firmware has been updated to take the new firmware version into use.

- 1.    Select the Arctic devices to be managed.
- 2.    Verify the **Selected devices** shown on the upper part of the pane.
- 3.    On the left pane under the **Arctic Patrol** menu, select **Management**.
- 4.    In the management actions list, verify that the correct devices are selected and select **system reboot** under **API commands**.
- 5.    Click **Run this action for all selected devices** to reboot the devices.

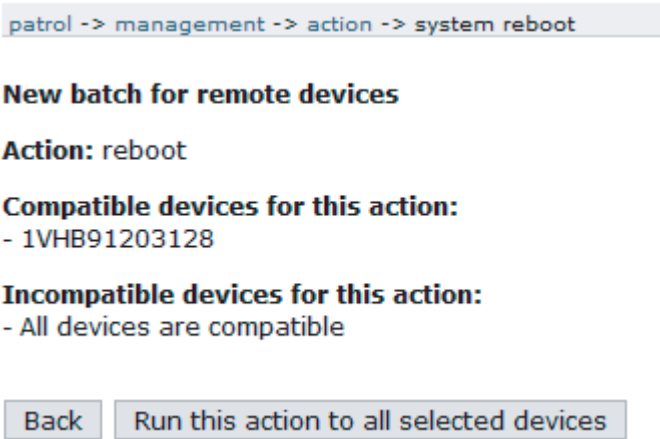


Figure 26:            *Rebooting Arctic device*

The **Running and old batches list** shows the started batch update. The **Status** column indicates how many of the total number of reboot tasks have been finished.  
When all update tasks are finished, the duration of the batch update is shown in the **Status** column.

	ID	Title	Status	Start time	Created by
<input type="checkbox"/>	14	system reboot	1 / 1 completed, duration 0:00:02	11 minutes ago	arctic-adm

Figure 27:            *Running and old batches list for rebooting*

### 7.3.3 RIO600 device management

Remote RIO600 devices connected to an Arctic device can be updated using the tools available in ARM600 WHMI's Arctic Patrol application. It is possible to transfer a new configuration as well as firmware to the RIO600 devices. However, the RIO600 device configuration and maintenance is always handled with PCM600.

If enabled in the Arctic wireless devices' configurations, the Arctic wireless devices scan their local networks for RIO600 devices and report them to the ARM600's Patrol view. The RIO600 devices are separately listed under each Arctic device the way they were found on the network. Although the ARM600's asset management features do not have any knowledge of the RIO600 device composition, software or configuration, it attempts to show this information whenever available.

Asset management actions may be performed on the RIO600 devices by selecting them from the device list in the same way as the Arctic devices.

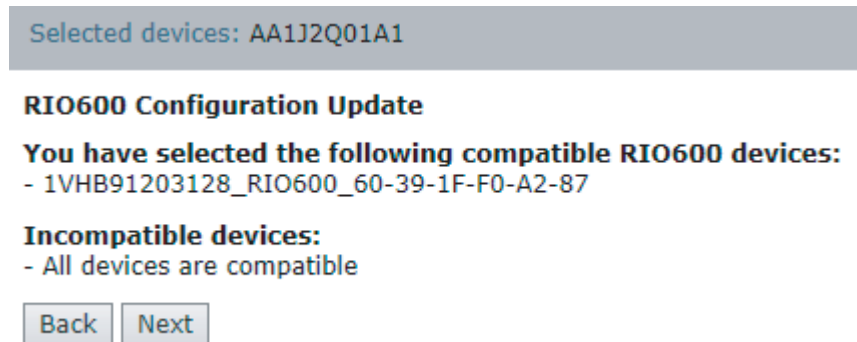


The asset management functionality for RIO600 is available from ARM600 Ver.4.3.1 onwards and with Arctic devices' firmware Ver.3.4.1 onwards.

#### 7.3.3.1 Updating RIO600 configuration

With the M2M Gateway ARM600 Patrol application it is possible to write new configurations in batch to many RIO600 devices connected to one or many Arctic devices. The RIO600 configurations to be written to RIO600 devices has to first be exported from PCM600.

1. Select the Arctic devices to be managed.
2. Verify the **Selected devices** shown on the upper part of the pane.
3. On the left pane under the **Arctic Patrol** menu, select **Management**.
4. In the management actions list, verify that the correct devices are selected and select **RIO600 Configuration Update** under **Tools**.
5. In the management actions list, select **RIO600 Configuration Update** and click **Next**.



Selected devices: AA1J2Q01A1

### RIO600 Configuration Update

**You have selected the following compatible RIO600 devices:**

- 1VHB91203128\_RIO600\_60-39-1F-F0-A2-87

**Incompatible devices:**

- All devices are compatible

[Back](#) [Next](#)

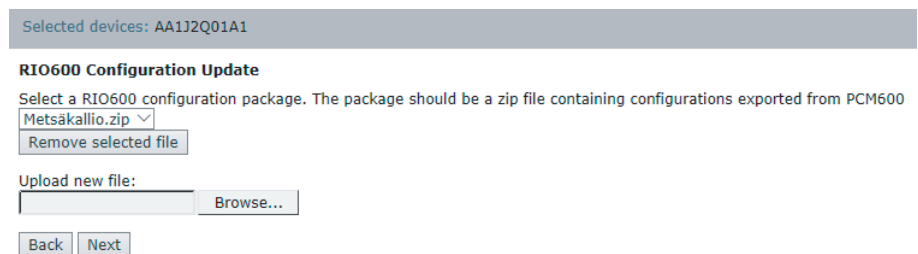
Figure 28: Selecting RIO600 configuration update

- Click **Browse** to select the firmware file and then click **Upload file**. The uploaded configuration packages appear in the drop-down list.



RIO600 configuration packages are exported from PCM600.

- Select an uploaded RIO600 configuration package file from the **Choose File** drop-down list and click **Next**.



Selected devices: AA1J2Q01A1

### RIO600 Configuration Update

Select a RIO600 configuration package. The package should be a zip file containing configurations exported from PCM600

Metsäkallio.zip

Upload new file:

[Browse...](#)

[Back](#) [Next](#)

Figure 29: Selecting RIO600 configuration package

- ARM600 asset management tries to automatically associate uploaded configurations to the found devices. However, if this is not possible, create the association manually.
  - Select a configuration from the left side under **Configurations**.
  - Select a RIO600 device from the right side under **Devices**.
  - Click the blue arrow to create the association.

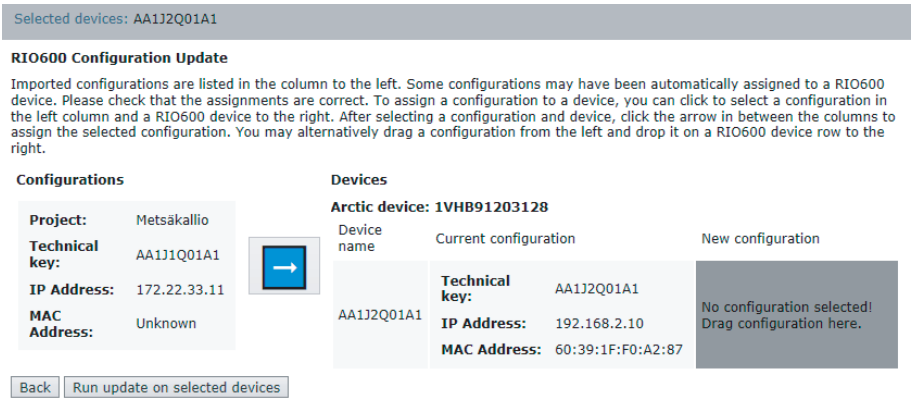


Figure 30: Creating associations manually



Ensure that each configuration is compatible and intended for the selected RIO600 device.

9. Click **Run update on selected devices** to add the task to the batch.

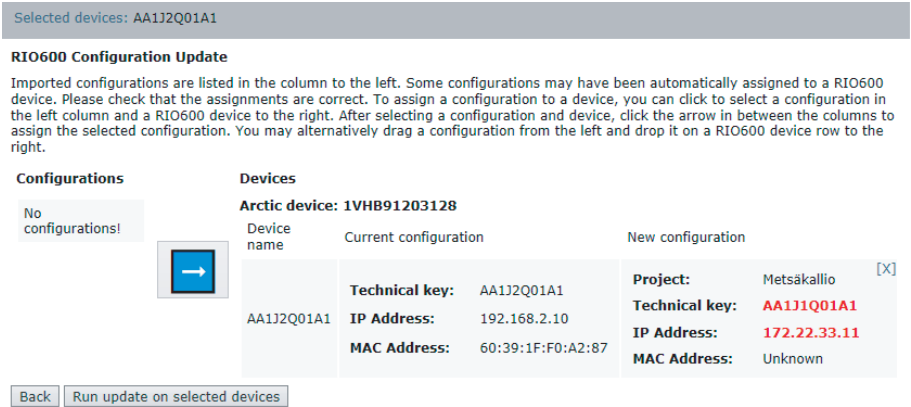


Figure 31: Updating RIO600 configuration



Ensure that the RIO600 device has a firmware version compatible with the uploaded configuration.

7.3.3.2

Updating RIO600 firmware

The ARM600 Patrol application enables the writing of firmware as a batch to several RIO600 devices connected to one or several Arctic devices. However, all RIO600 modules and firmware versions cannot be updated. The firmware packages supported by the Patrol application contain one or many firmware files for the

RIO600 modules and are distributed in zip files, for example, `RIO600V1.7.3_FIRMWARE.zip`. The Arctic and RIO600 firmware packages that are stored on ARM600 can be viewed via **Arctic Patrol/Device Firmware**.



LECM module firmware Ver.1.7 or later supports firmware upgrade.



SIM8F module firmware Ver.1.2 or later supports firmware upgrade.

1. Select the Arctic devices to be managed.
2. Verify the **Selected devices** shown on the upper part of the pane.
3. On the left pane under the **Arctic Patrol** menu, select **Management**.
4. In the management actions list, verify that the correct devices are selected and select **RIO600 Firmware Update** under **Tools**.
5. In the management actions list, select **RIO600 Configuration Update** and click **Next**.

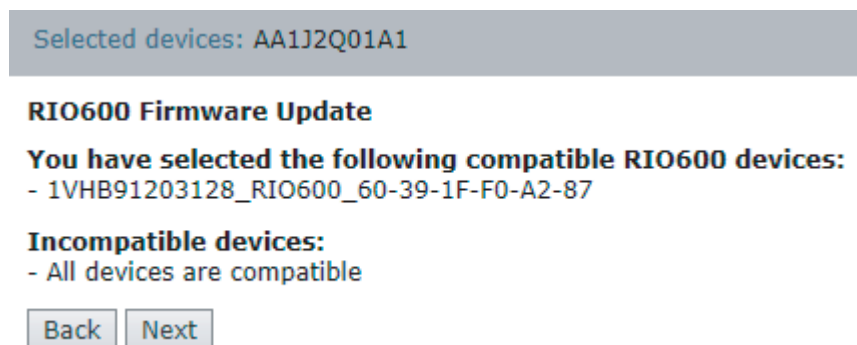


Figure 32: Selecting RIO600 firmware update

6. Click **Browse** to select the firmware file and then click **Upload file**. The uploaded firmware packages appear in the drop-down list.
7. Select an uploaded RIO600 firmware package file from the **Choose File** drop-down list and click **Next**. The contents of the firmware package are shown. One firmware package can contain one or many files for one or many modules on the RIO600 stack. The update process updates all modules available on the RIO600 stack.
8. Click **Run update on selected devices** to add the task to the batch.

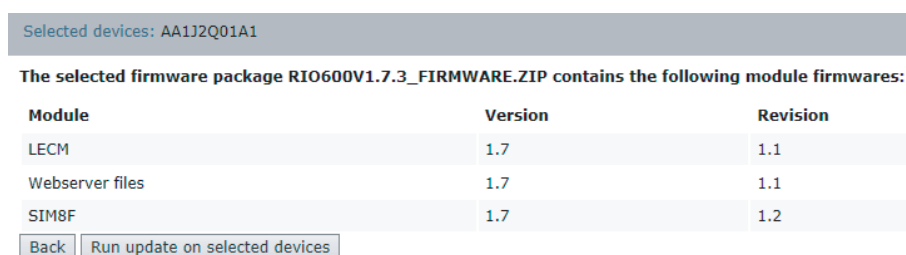


Figure 33: Updating RIO600 firmware



Ensure that the firmware package is intended and compatible with the selected RIO600 devices.

### 7.3.3.3

## Exporting RIO600 configurations from PCM600

RIO600 configurations are always maintained and stored within a PCM600 project. This requires that the RIO600 connectivity package is installed in PCM600. Every RIO600 device must have their own unique configuration within a PCM600 project.



See the PCM600 documentation for information on how to install and work with connectivity packages.

RIO600 configurations have to be exported from PCM600 into a format supported by the ARM600 asset management actions. Normally the configuration is written directly to a RIO600 device using the Write to IED option in PCM600. Instead of writing to a RIO600 device, the operation can be overridden by enabling the export configuration in Write to IED option. When this is enabled for one or more RIO600 devices and the Write to IED command is executed, the configuration is exported to a zip file instead of being directly written to a RIO600 device. The exported zip file can be uploaded into ARM600's Patrol WHMI for transfer as a batch to the RIO600 devices connected to the Arctic devices.

1. Open or create a new project in PCM600 with any number of RIO600 devices.
2. In the **Plant Structure**, right-click a device and select **Export Configuration in Write to IED**.

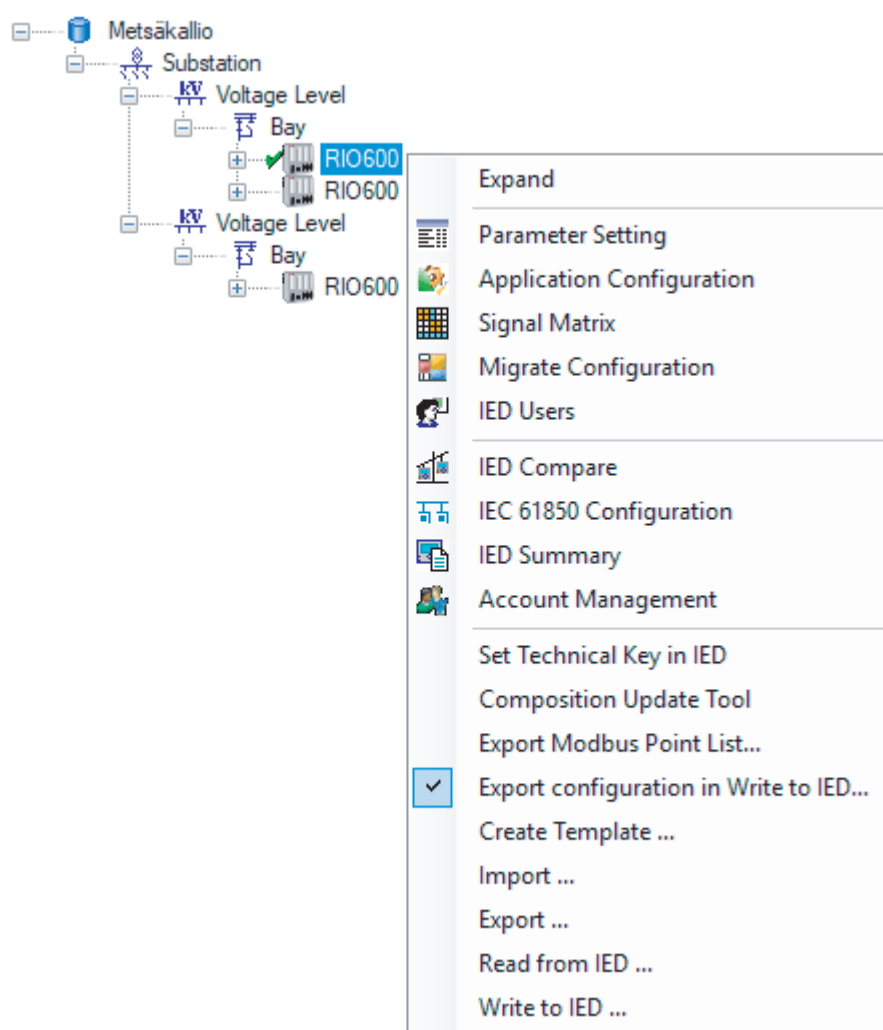


Figure 34: Selecting Export Configuration in Write to IED

3. In the **ExportConfigurationWindow** dialog, select each of the RIO600 devices from which the configuration should be exported, click **Browse** to set the **Export Path** and click **OK**.

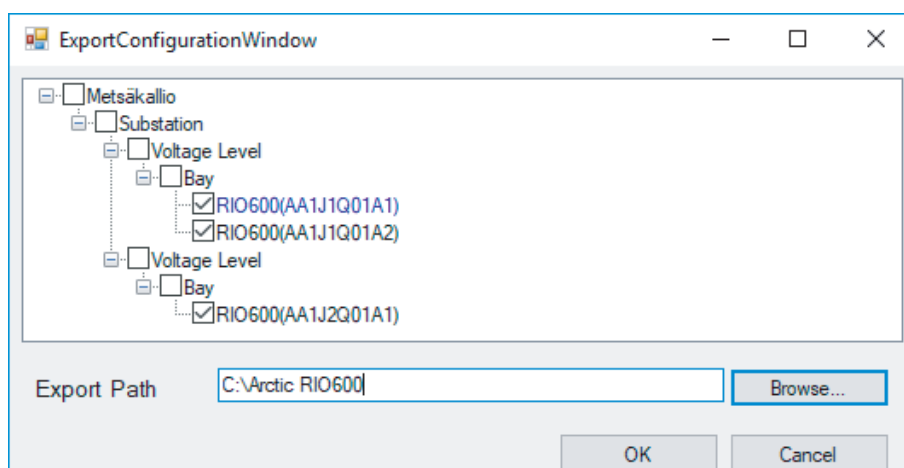


Figure 35: Selecting devices

4. Right click any RIO600 and choose **Write to IED** option.  
As **Export Configuration in Write to IED** is active, the normal action that would write directly to the RIO600 device is overwritten. A file called <project name>.zip is instead generated to the selected export path. The file <project name>.zip that was exported to the chosen export path is now ready to be uploaded to ARM600's WHMI.



RIO600 export for ARM600 is available in ABB IED Connectivity Package for RIO600 Ver.1.7.2 or later.

### 7.3.4

## OpenVPN certificate management

The server and client certificates that OpenVPN uses are always valid for a limited time. ARM600's WHMI shows a warning about expiring certificates when there is less than 6 months left until some OpenVPN certificates expire. It is recommended to take action well in advance before the certificates expire, since expired certificates cause VPN connections to fail.

If the OpenVPN clients are Arctic wireless devices that are also connected to the ARM600 server using Arctic Patrol with asset management enabled, the OpenVPN certificate can be renewed using ARM600's WHMI. This is a two-step process:

1. Renewing certificates for the server and clients on ARM600
2. Sending the new certificates to the Arctic wireless devices through Arctic Patrol. There are certain prerequisites for this step.



- Clients must be configured with Arctic Patrol for asset management. See the [Asset management](#) section in this manual for information on how to set this up.
- OpenVPN client names and Arctic hostnames must match, otherwise ARM600 is not able to match Patrol connections with VPN connections and is not able to transfer the new certificates.



### 7.3.4.1

### Renewing certificates for an OpenVPN server

1. Log in to ARM600's WHMI as the arctic-adm user.
2. On the left pane under the **VPN** menu, select **OpenVPN**.
3. Click the **Renew certificates** link.

**server1**

Status:	running
Tunnel type:	normal (layer 3)
Key type:	certificates
Bridged network interface:	none
Port:	1194
Protocol:	udp
Tunnel IPs network:	10.23.0.0 255.255.0.0
Comp LZO:	yes
Key size:	2048
Route:	
Client to client:	yes
Certificate is not valid before:	2018-05-18 11:05:01
+0000	
Certificate is not valid after:	2018-08-16 11:05:01
+0000	
Certificate is valid still:	2 months 🕒
Configured clients:	10



[Add clients »](#)  
[Edit server »](#)  
[Show server log »](#)  
[Renew certificates »](#)  
[Check certificate status »](#)

Figure 36: Renew certificates link

4. Choose the new expiration time.
5. Click **Continue**.  
The certificates have now been renewed. Clients that are not using the new certificates can connect to the OpenVPN server using the old certificates until they expire.
6. Restart the OpenVPN server to take into use the new certificates.
  - 6.1. Click **Edit server**.
  - 6.2. On the next page, click **Stop server**.
  - 6.3. Click the same button, now named **Start server**, to start the server again.



All clients are disconnected, and have to connect again when the server is restarted. This causes a brief loss of communication through VPN tunnels.



The server does not need to be restarted immediately. As long as the old certificates have not expired, the Arctic wireless devices are able to connect to ARM600.

#### 7.3.4.2


#### Sending renewed certificates to Arctic devices

Once the certificates for a server and its clients have been renewed, the new certificates need to be sent to all clients, and activated.

1. Log in to ARM600's WHMI as the arctic-adm user.
2. On the left pane under the **VPN** menu, select **OpenVPN**.
3. Go to the OpenVPN Certificate Update tool in one of the alternative ways.
  - Click the upload icon as shown in [Figure 37](#).

**server1**

Status:	running
Tunnel type:	normal (layer 3)
Key type:	certificates
Bridged network interface:	none
Port:	1194
Protocol:	udp
Tunnel IPs network:	10.23.0.0 255.255.0.0
Comp LZO:	yes
Key size:	2048
Route:	
Client to client:	yes
Certificate is not valid before:	2018-05-18 11:05:01
+0000	
Certificate is not valid after:	2018-08-16 11:05:01
+0000	
Certificate is valid still:	2 months 🌐
Configured clients:	10



[Add clients »](#)  
[Edit server »](#)  
[Show server log »](#)  
[Renew certificates »](#)  
[Check certificate status »](#)

Figure 37: Certificate upload icon

- Click the upload icon next to one OpenVPN client to transfer new certificates only to a specific client.

The tool now shows a list of clients for the chosen OpenVPN server as shown in [Figure 38](#).

**OpenVPN Certificate Update**

Certificates for OpenVPN server **server1** will be uploaded to the following clients:

Select devices that have not been updated

<input checked="" type="checkbox"/>	Name	Certificate on device expires	Last checked
<input checked="" type="checkbox"/>	arctic-1	unknown (unknown, <b>not updated</b> )	never
<input checked="" type="checkbox"/>	arctic-2	unknown (unknown, <b>not updated</b> )	never
<input checked="" type="checkbox"/>	arctic-3	unknown (unknown, <b>not updated</b> )	never
<input checked="" type="checkbox"/>	arctic-4	unknown (unknown, <b>not updated</b> )	never
<input checked="" type="checkbox"/>	arctic-5	unknown (unknown, <b>not updated</b> )	never
<input checked="" type="checkbox"/>	arctic-6	unknown (unknown, <b>not updated</b> )	never
<input checked="" type="checkbox"/>	arctic-7	unknown (unknown, <b>not updated</b> )	never
<input checked="" type="checkbox"/>	arctic-8	unknown (unknown, <b>not updated</b> )	never
<input checked="" type="checkbox"/>	arctic-9	unknown (unknown, <b>not updated</b> )	never
<input checked="" type="checkbox"/>	arctic-10	unknown (unknown, <b>not updated</b> )	never

Continue

Check certificate status

Figure 38: OpenVPN peers and certificate status

Column **Certificate on device expires** shows when the certificate installed on the device expires. Since ARM600 might not know how the device is configured, this column might contain "unknown" values. The device status can be queried with the Check certificate status tool.

4. Click the check boxes on the left of the **Name** column to select the devices that should be updated.  
Usually all devices should be updated, unless some devices were already updated.
5. Click **Continue** to start the update process.
6. Check the progress of the certificate transfer in one of the alternative ways.
  - Click the **Return to Management page** button.
  - Navigate to **Management** under the **Arctic Patrol** menu on the left pane.
7. On the **Patrol Management** page, near the top of the **running and old batches** list, click the title **Update client certificate** to see the progress of the certificate update.

**Batch #4 details**

Title: Update client certificate  
 Start time: a minute ago, 2018-05-21 13:19:02+03:00  
 Created by: arctic-adm  
 Completed: 5 / 5

**Results:**

1VHB91202021  Done

**Tasks:**

	Device	Accept time	Cancel time	Ready time	Result
1.	1VHB91202021	2018-05-21 13:19:02+03:00	-	2018-05-21 13:19:04+03:00	{ "openvpn_client": { "client":
2.	1VHB91202021	2018-05-21 13:19:04+03:00	-	2018-05-21 13:19:15+03:00	true
3.	1VHB91202021	2018-05-21 13:19:15+03:00	-	2018-05-21 13:19:27+03:00	true
4.	1VHB91202021	2018-05-21 13:19:27+03:00	-	2018-05-21 13:19:28+03:00	{ "key": { { "onoff": "1", "na
5.	1VHB91202021	2018-05-21 13:19:28+03:00	-	2018-05-21 13:19:40+03:00	{ "name": "arctic-1", "prot

Figure 39: Certificate update batch details

On this page, under **Results**, the status of the update for each device is shown. For these changes to take effect, the Arctic wireless devices that have been updated need to be rebooted separately. This can be done as described in the [Rebooting Arctic devices](#) section in this manual.

### 7.3.4.3

### Checking certificate status on Arctic wireless devices

It may be useful to check the expiration times of OpenVPN certificates on individual Arctic wireless devices, since the configuration of the device might have been changed manually. ARM600 might not then have access to the latest status of the OpenVPN certificates on all devices.

1. Log in to ARM600's WHMI as the arctic-adm user.
2. On the left pane under the **VPN** menu, select **OpenVPN**.
3. Click the **Check certificate status** link.
4. Select all devices whose status you wish to check.  
By default, all devices are selected.
5. Click **Continue** to proceed.
6. Click **Return to Management page** to go to the Arctic Patrol Management page.
7. Click the batch title **Check client certificates** at, or near, the top of the **Running and old batches** list to see the progress and results of the certificate status check.

When the status check is completed, the certificate expiration times for each device are listed on the batch details page under **Results**.



---

## Section 8 SSH mode selection and key update

### 8.1 SSH legacy mode

The recent OpenSSH software versions no longer support the deprecated SSH protocol version 1 (SSHv1). OpenSSH is used for SSH-VPN, SSH Patrol and console access on ARM600. While the SSHv1 protocol is no longer supported for new connections, the SSHv1 protocol might be in use, especially for SSH-VPN connections in older installations. Arctic devices using the A1 platform, that is, devices with firmware versions A1 5.x.x cannot be upgraded to support the newer, more secure SSH protocol version 2 (SSHv2). Other Arctic devices support SSH protocol version 2 and should be updated if they are still configured to use protocol version 1.

### 8.2 Legacy mode effects on the system

To keep backward compatibility with devices configured to use SSHv1, *SSH legacy mode* was introduced as an option in the ARM600's SSH-VPN settings. When *SSH legacy mode* is enabled, ARM600 uses the last version of OpenSSH with SSHv1 support included in the CentOS Linux distribution for all SSH-VPN and SSH Patrol connections. This means that if the SSH legacy mode is active, no updates are applied to the OpenSSH server responsible for SSH-VPN and SSH Patrol connections. When the legacy mode is disabled, an up-to-date OpenSSH version is used for all SSH connections. The legacy mode does not affect the SSH console access on port 10022 of ARM600.

Due to the lack of security updates when using this mode, it is highly recommended to avoid using the SSH legacy mode if possible. This is done by:

1. Updating any SSH-VPN peers using SSH protocol version 1 to use protocol version 2
2. Disabling the SSH legacy mode in ARM600

In Arctic wireless devices, SSH protocol version 2 is used when the private and public keys used for authentication are set to SSH2 RSA keys.

## 8.3 Legacy mode activation

*SSH legacy mode* replaces the earlier "Enable SSH Protocol 1" SSH-VPN server setting. *SSH legacy mode* is disabled by default in new installations, but it is automatically activated when upgrading the ARM600 software or restoring a backup of an installation where the following two criteria are met:

1. SSH protocol version 1 is enabled.
2. Any of the following is true:
  - At least one enabled SSH-VPN peer requires SSHv1 support.
  - At least one SSH Patrol peer requires SSHv1 support.

If these criteria are not met during upgrade or backup restore - for example, if the SSHv1 protocol was previously enabled, but no peer requires SSHv1 - the legacy mode is disabled.

### 8.3.1 Manually deactivating and activating SSH legacy mode

1. Log in to ARM600's WHMI as the arctic-adm user.
2. On the left pane under the **VPN** menu, select **SSH-VPN**.  
Under **Global Settings**, the current state of the SSH legacy mode is shown.

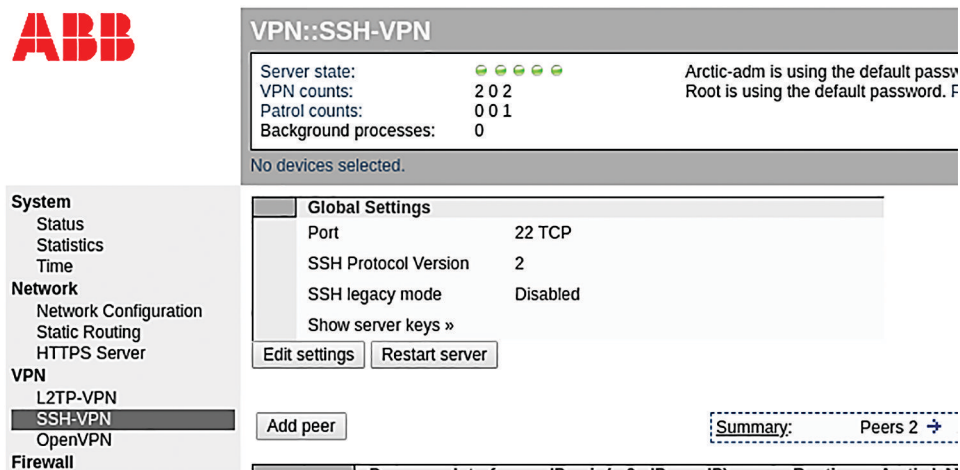


Figure 40: SSH legacy mode status

3. Click **Edit settings** to enable or disable the mode.
4. Clear the check box next to **Enable SSH legacy mode** to disable the SSH legacy mode. Click the check box to enable the legacy mode.
5. Click **Confirm settings** to confirm the changes.
6. For the changes to take effect, restart the SSH-VPN server by pressing **Restart server** on the SSH-VPN page.



Due to the security risk inherent in the SSH legacy mode, a notification is shown at the top of ARM600's WHMI when it is active. The notification can be dismissed by clicking the link to the right of the notification and confirming it permanently by selecting the **Do not show this again** check box followed by clicking **Confirm**.



Restarting the SSH-VPN server does not immediately affect already connected peers. For example, after disabling the SSH legacy mode, already connected peers use the legacy SSH server until the connection is broken. The next time they connect, the peers use the non-legacy OpenSSH server. It is possible to force peers to re-connect by, for example, disabling and re-enabling each peer individually by clicking the **Disable** button, followed by clicking **Enable** on the **SSH-VPN** page in the list of peers.



After disabling the SSH legacy mode, any peers with an SSH1 RSA key are no longer able to connect to ARM600. The key type of each peer is listed on the SSH-VPN page.

## 8.4 SSH-VPN key update tool

In the Arctic product line, SSH-VPN is a vendor-specific VPN which uses SSH public-key cryptography for securing the VPN traffic. The current product portfolio of ABB Arctic devices supports SSH v.2 which is considered safe within the contemporary cybersecurity standards.

The earlier versions of Arctic devices used SSH version 1 keys. Since several vulnerabilities were found in SSH v.1, the protocol is nowadays considered unsafe from the cybersecurity point of view. Thus, it is recommended to use the SSH key update tool for ABB ARM600 M2M Gateway to update any existing SSH-VPN v.1 key to v.2. The tool can also be used to update an existing SSH v.2 key to a new one, for example, by changing the key size from 2048 to 4096.

### 8.4.1 Comparison of SSH versions

The following table lists the details of SSH v.1 and SSH v.2 in ABB Arctic products. The larger key size in SSH v.2 improves security against brute-force attacks. The supported firmware versions are also listed.

Table 8: SSH versions

Description	SSH v.1 VPN	SSH v.2 VPN
Considered safe	No	Yes
Key size	1024	Min. 2048
Support for wireless gateways, firmware	Max. FW 3.3.6	Min. FW 2.0.10
Support for 2G legacy wireless gateways	All	None
Support for M2M gateway, firmware	Max. 4.5.3 (current version)	Min. 4.1.2

All currently sold ABB Arctic devices support SSH v.2. However, the older ABB or Viola models may not do so. The discontinued ABB REC/RER601/603 products, Viola Arctic 2G products and Viola M2M Gateway products (except for version 3.5.2) do not support SSH v.2. In case of these products, it is recommended to replace them with devices from the new ABB Arctic product line that support SSH v.2.

## 8.4.2

## Checking SSH version

- Identify the SSH version. The following indicate that ARM600 uses the old SSH v.1 key type.
  - *SSH legacy mode* is activated in ARM600.
  - On the SSH-VPN page, the enabled SSH Protocol Version is 1.
  - The key type column in the peer list shows "SSH1 RSA".
  - The key size column shows "1024" in red color.

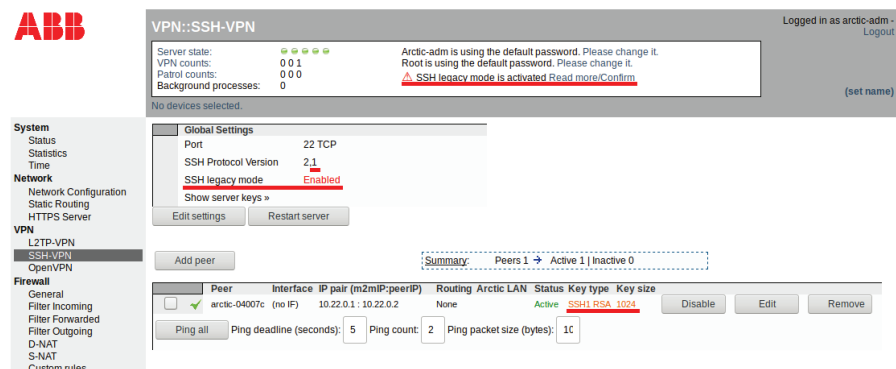


Figure 41: Indication of active SSH v.1

### 8.4.3 Using SSH key update tool

Verify that the following pre-requisites are met before using the SSH key update tool.

- Arctic wireless devices use firmware Ver.3.4.8 or newer.
- ARM600 M2M Gateway uses firmware Ver.4.5.3 or newer.
- Arctic Patrol is configured and enabled in all devices to be updated.

The firmware version is shown in the Status screen of the Arctic wireless gateways and ARM600 M2M Gateway. Once the firmware versions and Arctic Patrol functionality have been verified, the following update process can be used.

1. Log in to ARM600's WHMI, click **Arctic Patrol** and select **Devices**.
2. Select the Arctic wireless devices to be updated from the device list by selecting the check-box in the beginning of each device's information row.
3. Click **Arctic Patrol** and select **Management**.
4. Click **Update SSH-VPN public key**.  
The tool checks that all the selected devices have the correct firmware version to perform the update.
5. Click **Next** and select the key size.
6. Click **Start**.

A Patrol batch run is created and the update process begins.

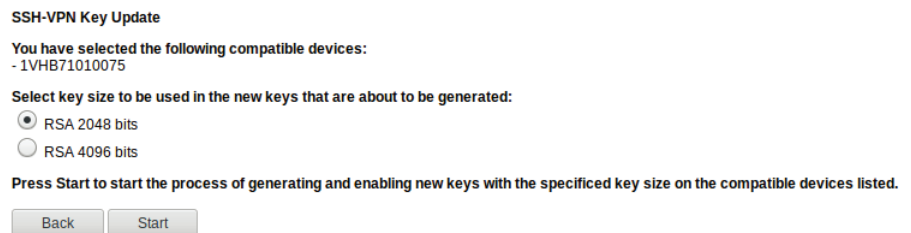


Figure 42: Updating SSH-VPN key

The SSH key update tool creates a new SSH key pair for every device, stores the public part of the key in ARM600 and takes the new key into use on ARM600 and the Arctic wireless device.



If Arctic Patrol is configured to be connected via the SSH protocol and Patrol uses the same SSH key as SSH-VPN, the SSH key update tool also updates the key for Patrol.



If Arctic Patrol is configured to be connected via the SSH-VPN tunnel and the key update batch fails for any reason, the Patrol connection may end up in an unusable state.



The Arctic devices must be rebooted to take the new SSH keys in use.

## Section 9 Additional administrative features

ARM600 has several administrative features which can be run from shell with administrator privileges.

**Table 9:** Additional administrative features

Feature	Description
ARM600 system update	See chapters <a href="#">Updating ARM600 system (ARM600 hardware variants)</a> and <a href="#">Updating ARM600SW system</a> in this manual.
Firmware update for Arctic Wireless Gateways using ARM600SW	See chapter <a href="#">Updating firmware for Arctic Wireless Gateways using ARM600SW</a> in this manual.
Antivirus software (ClamAV antivirus engine)	See the official ClamAV documentation for further instructions at <a href="https://www.clamav.net">https://www.clamav.net</a> .
File and directory integrity checker (AIDE storage integrity software)	See the official AIDE documentation for further instructions at <a href="https://aide.github.io">https://aide.github.io</a> .
Duplicate MAC address detection (Arpwatch)	Contact technical support for further instructions.
Syslog retention	Contact technical support for further instructions.

### 9.1 Updating ARM600 system (ARM600 hardware variants)



The default system software configuration has passed the ABB quality assurance process. Installing any third-party software may cause the system to malfunction.

The ARM600 system can be updated via shell with administrator privileges. Before updating the system, take a backup using the backup functionality described in [Backup and Auto backup](#).

It is highly recommended to download the generated backup file to another computer as a precaution.

1. Download the latest updates for the ARM600 system from the download server.
  - 1.1. In a Web browser, go to <https://arcticupdate.abb.com/m2mgw>.
  - 1.2. Click the required software version directory.
  - 1.3. Select file **m2mgw-repository-(version-number)-x86\_64.tar.gz**.
  - 1.4. Save the file on your computer.
2. Install the latest updates for the ARM600 system.

- 2.1. Use an SSH-capable file browser (for instance, free WinSCP).
- 2.2. Log in to ARM600 using the WinSCP client to port 10022 as a user of the wheel group.  
Users of the wheel group have administrator privileges.
- 2.3. Transfer the downloaded system update file from your computer to ARM600 by dragging the file to the right-side window of WinSCP.  
The system update file is transferred to the home directory of the logged in user.
- 2.4. Log in to the ARM600 system with an SSH terminal client, such as PuTTY.
- 2.5. Type the following command and press ENTER.  

```
# sudo /opt/viola/bin/system-update.sh [system  
update file name]
```



Replace [system update file name] with the name of the system update file, without the brackets.

The system checks the integrity of the package and unpacks it before running the update procedure. After the update, the system notifies if a reboot is necessary.

## 9.2 Updating ARM600SW system



The default system software configuration has passed the ABB quality assurance process. Installing any third-party software may cause the system to malfunction.

The ARM600SW system can be updated via shell with administrator privileges. Updating the system requires a system update file available in the ARM600SW software repository. Software repository access requires a valid SSL certificate file installed in the system accessing the repository. This certificate is supplied with the ARM600SW software ISO file. The easiest way to get the system update file is to use a standard Web browser which has the certificate installed and configured.

Before updating the system, take a backup using one of the procedures listed below in order of preference.

1. Use the snapshot feature of the virtual machine environment. For detailed VMware vSphere snapshot instructions, see the official VMware documentation at <https://www.vmware.com>.
2. Use the backup functionality described in [Backup and Auto backup](#). It is highly recommended to download the generated back up file to another computer as a precaution.

1. Configure the Web browser for accessing the software repository (Microsoft Edge used as an example).
  - 1.1. In Microsoft Edge, click the three dots in the upper right corner and select **Settings**.
  - 1.2. Select **Privacy, search and services** and click **Manage certificates**.
  - 1.3. On the **Certificates** dialog box, click **Import**.
  - 1.4. Click **Next** and then **Browse**.
  - 1.5. Select the .p12 file supplied with your ARM600SW software and click **Next**.
  - 1.6. When prompted for a password, leave it blank and press ENTER.
  - 1.7. Click **Next** and select **Personal**.
  - 1.8. Click **Next** and then **Finish**.  
You can now access the ARM600SW software repository with your Web browser.
2. Download the latest updates for the ARM600SW system from the software repository.
  - 2.1. Open your Web browser configured with the .p12 certificate.
  - 2.2. Go to <https://arcticupdate.abb.com/repo/5/centosrepo>.
  - 2.3. Select file **m2mgw-repository-(version-number)-x86\_64.tar.gz**.
  - 2.4. Save the file on your computer.
3. Install the latest updates for the ARM600SW system.
  - 3.1. Use an SSH-capable file browser (for instance, free WinSCP).
  - 3.2. Log in to ARM600(SW) using WinSCP client to port 10022 as a user of the wheel group.  
Users of the wheel group have administrator privileges.
  - 3.3. Transfer the downloaded system update file from your computer to ARM600SW by dragging the file to the right-side window of WinSCP.  
The system update file is transferred to the home directory of the logged in user.
  - 3.4. Log in to the ARM600SW system with an SSH terminal client, such as PuTTY.
  - 3.5. Type the following command and press ENTER.  

```
# sudo /opt/viola/bin/system-update.sh [system
update file name]
```



Replace [system update file name] with the name of the system update file, without the brackets.

The system checks the integrity of the package and unpacks it before running the update procedure. After the update, the system notifies if a reboot is necessary.

## 9.2.1 Local software repository mirror



Do not use the official CentOS software repositories or other third-party repositories. Updating the RPM packages using other repositories than the one described in the user manual or its local mirror can cause system malfunctioning.

ARM600SW features a possibility to set up a local software repository mirror in LAN. This can be done via shell with administrator privileges. The mirror can be synchronized with the official software repository to offer the latest updates for the ARM600SW system and Arctic Wireless Gateways. Thus the system can be updated via LAN rather than using a local portable media, such as a USB hard drive. The local software repository mirror requires a PC running Linux operating system (CentOS 8 Stream recommended). Contact technical support for further instructions.

## 9.3 Updating firmware for Arctic Wireless Gateways using ARM600SW

The firmware of Arctic Wireless Gateways can be updated using ARM600SW via shell with administrator privileges. Updating the firmware requires an update file available at the software repository. Software repository access requires a valid SSL certificate file installed in the system accessing the repository. This certificate is supplied with ARM600SW software. The easiest way to get the latest firmware is to use a standard Web browser which has the certificate installed and configured.

1. Download the latest firmware for Arctic Wireless Gateways from the software repository.
  - 1.1. Start your Web browser configured with the .p12 certificate (see the [Updating ARM600SW system](#) chapter in this manual).
  - 1.2. Go to <https://arcticupdate.abb.com/repo/arcticfw>.
  - 1.3. Select the firmware file.
  - 1.4. Save the file on your computer.
2. Install the latest firmware for the Arctic Wireless Gateways.
  - 2.1. Use an SSH-capable file browser (for instance, free WinSCP).
  - 2.2. Log in to ARM600(SW) using the WinSCP client to port 10022 as a user of the wheel group.

Users of the wheel group have administrator privileges.
  - 2.3. Transfer the downloaded Arctic Wireless Gateway update file from your computer to ARM600(SW) by dragging the file to the right-side window of WinSCP.

The system update file is transferred to the home directory of the logged in user.



- 
- 2.4. Log in to the ARM600(SW) system with an SSH terminal client, such as PuTTY.
  - 2.5. Type the following command and press ENTER.  

```
# sudo /opt/viola/bin/system-update.sh [update  
file name]
```



Replace [update file name] with the name of the Arctic Wireless Gateway update file, without the brackets.

The system checks the integrity of the package and unpacks the firmware.

- 2.6. Update the Arctic Wireless Gateway firmware according to the instructions in the [Updating Arctic device firmware via ARM600SW](#) chapter in this manual.



## Section 10 Troubleshooting

### 10.1 Common problems and solutions

**Table 10:** *Common problems and solutions*

Problem	Suggested solution
Cannot establish a VPN tunnel	<ul style="list-style-type: none"> <li>• Check that ARM600 has a default gateway configured for the eth0 interface.</li> <li>• ARM600 needs a public, static IP address. Provided that ICMP ping is allowed in the firewalls, check that ARM600 can be pinged from the Internet.</li> <li>• Verify that the OpenVPN ciphers in ARM600 and in Arctic Wireless Gateway/Controller are the same.</li> <li>• Check that the border firewall does not block the traffic and that there is a port forwarding to ARM600, if the public IP is associated to the border router. At least the VPN port must be open (UDP 1194 for first OpenVPN server instance).</li> </ul>
Cannot connect to the Arctic device's Patrol	<ul style="list-style-type: none"> <li>• Check that the registration password has been copied to Arctic Wireless Gateway/Controller.</li> <li>• Check that the Arctic Wireless Gateway's/Controller's hostname is the same as the OpenVPN peer name in ARM600.</li> <li>• Check that the port TCP 10000 is open in the border firewall.</li> </ul>
Cannot ping the devices connected to Arctic devices	<ul style="list-style-type: none"> <li>• Verify the routing settings, both in ARM600's VPN settings and in Arctic Wireless Gateways/Controllers.</li> <li>• Check that the ARM600's firewall allows the ICMP ping in the forward table.</li> <li>• If the ping target is a PC, disable the firewall of the PC or allow ICMP messages.</li> </ul>
SCADA server is unable to connect the field devices through ARM600	<ul style="list-style-type: none"> <li>• The SCADA needs to be aware of the routing; define a static route in SCADA so that the field devices' IP address range is routed through ARM600.</li> <li>• If the SCADA is in a dedicated LAN subnet outside ARM600's LAN subnet, define a static route in ARM600 so that it is aware of the SCADA LAN subnet.</li> <li>• Verify that Arctic Wireless Gateways/Controllers have a route in the VPN settings (<b>OpenVPN/Routing and Addressing</b>) so that they are able to send reply packets through the VPN tunnel. Usually, the default route can be used.</li> <li>• Check that the field devices connected to Arctic Wireless Gateways/Controllers are configured to use the Arctic as a default gateway.</li> </ul>
Cannot access the asset management features	<ul style="list-style-type: none"> <li>• Check that the device firmware versions are correct. <ul style="list-style-type: none"> <li>• Arctic device Ver.3.3.1 or later</li> <li>• ARM600 Ver.4.2.1 or later</li> </ul> </li> </ul>

## 10.2 Questions and answers

**Table 11:** *Questions and answers*

Question	Answer
Do I need a public, static IP address for ARM600?	When using standard “off the shelf” public cellular network SIM cards in the Arctic field devices, they are routed over the Internet. ARM600 is a server equipment and it requires a public, static IP address when public networks are used. The public IP address may be associated to the company’s border router and VPN packets can be port forwarded to ARM600. Thus, the public IP address does not need to be associated directly to ARM600’s Ethernet interface.
Why is there no SIM card inside ARM600?	ARM600 requires more bandwidth than a SIM card can provide, especially when there is a large number of connected wireless gateways.
Can IEC 61850 GOOSE be transferred over this system?	Yes, with Layer 2 OpenVPN tunnels. However, note that the contemporary cellular networks are not capable of providing the required latency and speed for higher speed GOOSE message classes.
Our company has a private APN in cellular network. Do we need ARM600?	Arctic Gateways/Controllers can be used without ARM600, if a private APN is available. However, ARM600 is still highly recommended because of the Patrol centralized management functionality, secure VPN tunnels, firewall and for not needing complex D-NAT configurations in the field devices.

## Section 11 Technical data (ARM600 hardware variants)

**Table 12:** *Dimensions*

Description	Standard edition	Enterprise edition
Height × Width × Depth	4x 3.5" chassis <ul style="list-style-type: none"> <li>42.8 × 434.0 × 596 mm (without bezel)</li> <li>1.67 × 17.09 × 23.5 in</li> </ul>	8x 2.5" chassis <ul style="list-style-type: none"> <li>42.8 × 434.0 × 545 mm (without bezel)</li> <li>1.67 × 17.09 × 21.5 in</li> </ul>

**Table 13:** *Hardware*

Description		Standard edition	Enterprise edition
Processor environment	Processor	Intel Pentium	Intel Xeon
	Memory	8 GB UDIMM	32 GB UDIMM
HDD		480 GB SSD SATA 6Gbps 2.5in hot-plug	Dual, 480 GB SSD SATA 6Gbps 2.5in hot-plug
Power supply		Single power supply 350 W	Dual, hot-plug, redundant power supply (2 ×), 550 W
Casing		Metal, 19" rack mountable (1U)	Metal, 19" rack mountable (1U)
Approvals		Global CB Scheme, CE, FCC	Global CB Scheme, CE, FCC
Environmental conditions	Temperature: Continuous operation (for altitude less than 950 m or 3117 ft)	10...35°C (50...95°F)	10...35°C (50...95°F)
	Relative humidity: operating	10...80% relative humidity with 29°C (84.2°F) maximum dew point	10...80% relative humidity with 29°C (84.2°F) maximum dew point

**Table 14:** *Standard and Enterprise editions*

Description		Value
Operating voltage <sup>1)</sup>		100...240 V AC, autoranging, 50/60 Hz
Temperature	Continuous operation (for altitudes less than 950 m or 3,117 ft)	10...35°C (50...95°F) with no direct sunlight on the equipment
	Storage	-40...65°C (-40...149°F)
Table continues on next page		

Description		Value
Relative humidity	Operating	10...80% relative humidity with 29°C (84.2°F) maximum dew point
	Storage	5...95% relative humidity with 33°C (91°F) maximum dew point The atmosphere must be non-condensing at all times.
Maximum vibration	Operating	0.26 Grms at 5...350 Hz (operation orientation)
	Storage	1.88 Grms at 10...500 Hz for 15 min (all six sides tested)
Maximum shock	Operating	One pulse on each side of the system of 71 G for up to 2 ms
	Storage	Six consecutively executed shock pulses in the positive and negative x, y, and z axes (one pulse on each side of the system) of 71 G for up to 2 ms
Maximum altitude	Operating	30,482,000 m (100,006,560 ft)
	Storage	12,000 m (39,370 ft)
Operating altitude de-rating		Maximum temperature is reduced by 1°C/300 m (1°F/547 ft) above 950 m (3,117 ft)

- 1) Also designed to be connected to IT power systems with a phase-to-phase voltage that does not exceed 230 V

**Table 15:** *Ordering data*

Description	Standard edition ARM600C2500NA	Enterprise edition ARM600C2505NA
Ethernet ports	2	4
Power supply	single	dual
HDD	single	dual
RAID	no	yes
CPU type	Intel Pentium	Intel Xeon
RAM	8 GB	32 GB
Max Arctic connections	300	2000 <sup>1)</sup>
Size	1U 19"	1U 19"

- 1) With the hardware listed in [Table 13](#)

---

## Section 12      Glossary

<b>AC</b>	Alternating current
<b>API</b>	Application programming interface
<b>APN</b>	Access Point Name
<b>D-NAT</b>	Destination network address translation
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>DMZ</b>	De-militarized zone
<b>DNS</b>	Domain Name System
<b>EMC</b>	Electromagnetic compatibility
<b>Ethernet</b>	A standard for connecting a family of frame-based computer networking technologies into a LAN
<b>GOOSE</b>	Generic Object-Oriented Substation Event
<b>HMI</b>	Human-machine interface
<b>HTTPS</b>	Hypertext Transfer Protocol Secure
<b>ICMP</b>	Internet Control Message Protocol
<b>IEC</b>	International Electrotechnical Commission
<b>IEC 61850</b>	International standard for substation communication and modeling
<b>IP</b>	Internet protocol
<b>IP address</b>	A set of four numbers between 0 and 255, separated by periods. Each server connected to the Internet is assigned a unique IP address that specifies the location for the TCP/IP protocol.
<b>L2TP</b>	Layer 2 tunneling protocol
<b>LAN</b>	Local area network
<b>LCD</b>	Liquid crystal display
<b>M2M</b>	Machine to machine
<b>MD5</b>	Message digest algorithm 5
<b>NTP</b>	Network time protocol
<b>PC</b>	1. Personal computer 2. Polycarbonate
<b>PCM600</b>	Protection and Control IED Manager
<b>PSU</b>	Power supply unit

---

<b>RAM</b>	Random access memory
<b>RIO600</b>	Remote I/O unit
<b>RTU</b>	Remote terminal unit
<b>Rx</b>	Receive/Received
<b>S-NAT</b>	Source network address translation
<b>SCADA</b>	Supervision, control and data acquisition
<b>SIM</b>	Subscriber identity module
<b>SNMP</b>	Simple Network Management Protocol
<b>SSH</b>	Secure shell
<b>TCP</b>	Transmission Control Protocol
<b>Tx</b>	Transmit/Transmitted
<b>UDP</b>	User datagram protocol
<b>USB</b>	Universal serial bus
<b>VGA</b>	Video graphics array
<b>VPN</b>	Virtual Private Network
<b>WAN</b>	Wide area network
<b>WHMI</b>	Web human-machine interface
<b>XML</b>	Extensible markup language











---

**ABB Distribution Solutions**

P.O. Box 699

FI-65101 VAASA, Finland

Phone +358 10 22 11

**[abb.com/mediumvoltage](https://abb.com/mediumvoltage)**