M2M Gateway
ARM600
User Manual
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.

www.abb.com/substationautomation
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.
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.
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

Using OpenVPN with firewall .......................................................... 21
Firewall menu .................................................................................. 22
Arctic Patrol menu ......................................................................... 23
Tools menu ....................................................................................... 25

Section 6 Network configuration ...................................................... 27
Configuring Ethernet interfaces ........................................................ 27
Ethernet interface setup parameters ............................................... 29

Section 7 Arctic Patrol .................................................................... 31
Overview ........................................................................................ 31
Registering Arctic devices to Patrol .................................................. 31
Allowing Arctic devices to scan local networks .................................. 35
Asset management ......................................................................... 36
Selecting devices for device management ........................................ 37
Arctic device management ............................................................... 38
  Updating Arctic device firmware ................................................ 38
  Updating RTU configuration ....................................................... 39
  Updating device XML configuration ........................................... 41
  Rebooting Arctic devices ......................................................... 43
RIO600 device management ........................................................... 44
  Updating RIO600 configuration ................................................. 45
  Updating RIO600 firmware ...................................................... 47
Exporting RIO600 configurations from PCM600 ......................... 48
OpenVPN certificate management ............................................... 51
  Renewing certificates for an OpenVPN server ......................... 52
  Sending renewed certificates to Arctic devices ......................... 53
  Checking certificate status on Arctic wireless devices .............. 56

Section 8 Legacy features ............................................................... 57
SSH legacy mode .......................................................................... 57
Legacy mode effects on the system ............................................... 57
Legacy mode activation .................................................................. 58
  Manually deactivating and activating SSH legacy mode ........ 58

Section 9 Troubleshooting ............................................................. 61
Common problems and solutions .................................................. 61
Questions and answers .................................................................. 62

Section 10 Technical data ............................................................... 63

Section 11 Glossary ........................................................................ 67
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


1.3.2 Document revision history

<table>
<thead>
<tr>
<th>Document revision/date</th>
<th>Product version</th>
<th>History</th>
</tr>
</thead>
<tbody>
<tr>
<td>A/2017-09-29</td>
<td>4.3</td>
<td>First release</td>
</tr>
<tr>
<td>B/2018-06-29</td>
<td>4.4.1</td>
<td>Content updated to correspond to the product version</td>
</tr>
<tr>
<td>C/2019-04-24</td>
<td>4.5.1</td>
<td>Content updated to correspond to the product version</td>
</tr>
</tbody>
</table>

Download the latest documents from the ABB Web site http://www.abb.com/substationautomation.
1.3.3 Related documentation

<table>
<thead>
<tr>
<th>Name of the document</th>
<th>Description</th>
<th>Document ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arctic Cyber Security Deployment Guideline</td>
<td></td>
<td>1MRS758860</td>
</tr>
<tr>
<td>3G/LTE configuration guide Technical Note</td>
<td>Configuring Wireless Gateways, Controllers and M2M Gateway</td>
<td>1MRS758449</td>
</tr>
</tbody>
</table>


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. ARM600 manages all Arctic 600 series wireless gateway connections and is the main interface between the field devices and 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 utilize normal SIM cards with dynamic IP addresses from any operator. This allows the user to utilize different operators 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.
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 console (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
- 19” rack mountable design
2.3 Physical interfaces

2.3.1 Standard edition

2.3.1.1 Front panel

Figure 2: Front panel

1 Power on indicator, power button
2 Video (VGA) connector
3 LCD menu buttons
4 LCD panel
5 Two USB 2.0 connectors
6 Service tag (EST)
7 Optical drive
8 Hard drive
2.3.1.2 Back panel

Figure 3: Back panel

1. Two USB 3.0 connectors
2. Power supply unit (PSU)
3. Video (VGA) connector
4. Ethernet connector for WAN #1 (Gb1)
5. Ethernet connector for LAN #2 (Gb2)

2.3.1.3 Health indicators

Table 1: Health indicators

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Status and color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health indicator</td>
<td>Solid blue</td>
<td>System is on and in good health</td>
</tr>
<tr>
<td></td>
<td>Flashing amber</td>
<td>Error condition, for example, a failed fan or hard drive</td>
</tr>
<tr>
<td>Hard drive indicator</td>
<td>Flashing amber</td>
<td>Hard drive error</td>
</tr>
<tr>
<td>Electrical indicator</td>
<td>Flashing amber</td>
<td>Electrical error, for example, voltage out of range or a failed power supply</td>
</tr>
<tr>
<td>Temperature indicator</td>
<td>Flashing amber</td>
<td>Thermal error, for example, temperature out of range or fan failure</td>
</tr>
<tr>
<td>Memory indicator</td>
<td>Flashing amber</td>
<td>Memory error</td>
</tr>
</tbody>
</table>
2.3.2 Enterprise edition

2.3.2.1 Front panel

Figure 4: Front panel

1. Two USB connectors
2. Optical drive
3. Service tag (EST)
4. LCD panel
5. Hard drive 1
6. Hard drive 2
2.3.2.2 Back panel

Figure 5: Back panel

1 Ethernet connector for LAN #1 (eth0)
2 iDRAC
3 Power supply health/activity indicators
4 Video (VGA) connector
5 Ethernet connector for WAN #2 (eth1)
6 Ethernet connector #3 (eth2)
7 Ethernet connector #4 (eth3)
8 Power supply bay 1
9 Power supply bay 2

2.3.3 LCD panel

The system’s LCD panel provides system information and status and error messages to indicate, if the system is operating correctly or if the system needs attention.

Table 2: LCD backlight statuses

<table>
<thead>
<tr>
<th>Status</th>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ON</td>
<td>Blue</td>
<td>Normal operation</td>
</tr>
<tr>
<td></td>
<td>Amber</td>
<td>Error condition</td>
</tr>
<tr>
<td>OFF</td>
<td>-</td>
<td>Standby mode</td>
</tr>
</tbody>
</table>

The LCD backlight can be turned on by pressing either the Select, Left, or Right button on the LCD panel. The LCD backlight remains off if the LCD messaging is turned off through the iDRAC utility, the LCD panel, or other tools.
2.4 Deployment scenarios

ARM600 is typically installed in the same location as the central control and monitoring system. ARM600 can be installed, for example, in the company DMZ (demilitarized zone) between the company LAN and the public Internet or directly behind the company firewall.

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.

If a private APN is used, ARM600 does not need a public IP address. Instead, a private static IP address can be used. The cellular operator’s access router provides routing between IP addresses of the SIM cards and 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 border router as a default gateway.
ARM600 behind the company’s firewall

There is no DMZ in this setup as ARM600 is directly connected to the company’s LAN. As in the DMZ scenario, ARM600 has a private IP address and the border router/firewall forwards packets from a public, static IP address to ARM600.

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.
Section 3 Cyber security

3.1 Cyber security definition

Cyber security aims to secure the properties of the organization against security risks. To strengthen the system and increase the security level towards any cyber security 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.
- Disable all unused services, for example, Dial-in, SMSconfig, serial and SNMP.
- Back up the configuration.
Section 4 Getting started

4.1 Configuring ARM600

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 WHMI.
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

- 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

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. Insert the Ethernet cables.
### Table 3: Operating system interface names and physical Ethernet connectors

<table>
<thead>
<tr>
<th>ARM600 version</th>
<th>Eth0 interface (WAN)</th>
<th>Eth1 interface (LAN)</th>
<th>Eth2 interface (spare)</th>
<th>Eth3 interface (spare)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard edition</td>
<td>Gb1 connector</td>
<td>Gb2 connector</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Enterprise edition</td>
<td>Ethernet 1 connector</td>
<td>Ethernet 2 connector</td>
<td>Ethernet 3 connector</td>
<td>Ethernet 4 connector</td>
</tr>
</tbody>
</table>

3.1. **Standard edition**: The default firewall configuration expects that the Gb1 port is the WAN port and Gb2 is the LAN port. In factory configuration, only the Gb1 port is enabled. Insert first the Ethernet cable to the “Gb1” port. This port is seen in ARM600’s WHMI as the eth0 port.

3.2. **Enterprise edition**: Insert first the Ethernet cable to the port marked with “1”. This port is seen in ARM600’s WHMI as the eth0 port.

The VGA display and USB keyboard are not needed for configuring ARM600. They can be used, if a local console access is needed.

### 4.4 Logging in

1. Configure the computer to use the same IP address space as the device. Example: Laptop IP is 10.10.10.11 with netmask 255.255.255.0.
2. In a Web browser, connect to the ARM600 WHMI on port 10000 using the HTTPS protocol.
   - `https://10.10.10.10:10000`

   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.
3. Enter the username and password.
   - Change the default "arctic-adm" and "root" user passwords before connecting ARM600 to public networks.
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

![Menu structure diagram]

Figure 10: Menu structure

5.2 System menu

The system menu contains the system overview and time settings.
Table 4: System submenus

<table>
<thead>
<tr>
<th>Menu</th>
<th>Description</th>
</tr>
</thead>
</table>
| Status | Shown after login.  
  - Details of the hardware and firmware versions, system time, network interfaces, routing table, disk information and firewall status |
| Statistics | 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 filesystem 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 |
| Time | Used to control the time settings. There are two options.  
  - Manual time setting  
  - Using NTP server for acquiring and keeping the correct time  
  ARM600 can work as a time server for providing 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.

Table 5: Network submenus

<table>
<thead>
<tr>
<th>Menu</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Configuration</td>
<td>Used to configure IP addresses, netmask and other network interface related settings.</td>
</tr>
</tbody>
</table>
| Static routing | Used to configure the static routing.  
  Static routing is needed, if LAN subnets beyond the ARM600’s LAN need to be reached via a certain 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.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2TP-VPN</td>
<td>Used to configure L2TP-VPN. It is not recommended to use L2TP-VPN, because of the lack of encryption, except 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.</td>
</tr>
<tr>
<td>SSH-VPN</td>
<td>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.</td>
</tr>
</tbody>
</table>
| OpenVPN | Used to configure OpenVPN. OpenVPN utilizes 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 has 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. |

5.4.1 Using 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).

### Table 7: Firewall submenus

<table>
<thead>
<tr>
<th>Menu</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Contains general settings of using the firewall, using network address translations and default actions for incoming, forwarded and outgoing packets.</td>
</tr>
<tr>
<td>Filter incoming</td>
<td>Used to configure the incoming packets that arrive to 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”, which means that only packets matching the rules (white-listed) are accepted, others are dropped.</td>
</tr>
<tr>
<td>Filter forwarded</td>
<td>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 interface to another. As a 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.</td>
</tr>
<tr>
<td>Filter outgoing</td>
<td>Used to configure the outgoing packets leaving from ARM600 to other network elements. By default, all outgoing packets are allowed.</td>
</tr>
<tr>
<td>Menu</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>D-NAT</td>
<td>Used to adjust forwarding packets based on their destination address/port. Usually the port forwarding is not needed in ARM600.</td>
</tr>
<tr>
<td>S-NAT</td>
<td>Used to adjust the source addresses of packets. The S-NAT is needed, for example, when ARM600 is used as a border router to Internet.</td>
</tr>
<tr>
<td>Custom rules</td>
<td>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).</td>
</tr>
</tbody>
</table>

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
Table 8: Arctic Patrol submenus

<table>
<thead>
<tr>
<th>Menu</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>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.</td>
</tr>
<tr>
<td>Devices</td>
<td>Shows most important details of the Arctic wireless devices like 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.</td>
</tr>
<tr>
<td>Management</td>
<td>Provides fleet management functions for upgrading the firmware or rebooting of multiple devices as a batch run. The devices need to be selected from the &quot;Devices&quot; submenu before a batch run can be done.</td>
</tr>
<tr>
<td>Details</td>
<td>Shows device-specific details that are useful for troubleshooting. The device’s configuration can also be viewed.</td>
</tr>
<tr>
<td>Statistics</td>
<td>Shows historical statistics of the devices and is also useful for troubleshooting.</td>
</tr>
<tr>
<td>Registration</td>
<td>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.</td>
</tr>
</tbody>
</table>

Table continues on next page
### Menu Description

**Configuration**
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 the Arctic is accepted from the device screen. The other configurable parameters consist of alert from/to email addresses, mailing intervals and statuses, time intervals for status changes and whether to store historical data or not.

**Profiles**
Shows RTU configuration files and allows configuring multiple Arctic devices using XML configuration profile templates.

**Device Firmware**
Shows Arctic and RIO600 firmware packages that are stored on ARM600. 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.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Administration</strong></td>
<td>Used to define user rights, change passwords and add new users.</td>
</tr>
<tr>
<td></td>
<td>• The default users are arctic-adm and root.</td>
</tr>
<tr>
<td></td>
<td>• The root user logging is allowed from console only. As for the other users, they can be granted WHMI access, SSH command line access, or both.</td>
</tr>
<tr>
<td></td>
<td>• The enabled Patrol users, that is, Arctic wireless gateways with Patrol enabled, are also seen in the user administration page. Do not delete the Patrol user unless the Patrol client is disabled in the Arctic wireless gateway.</td>
</tr>
<tr>
<td></td>
<td>Change the default “arctic-adm” and “root” user passwords before connecting ARM600 to public networks.</td>
</tr>
<tr>
<td><strong>Backup</strong></td>
<td>Used to create and restore backups and upload/download them from/into 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.</td>
</tr>
<tr>
<td><strong>Auto Backup</strong></td>
<td>Used to configure ARM600 to backup the configuration to an additional standby ARM600. The data transfer method is rsync over SSH.</td>
</tr>
<tr>
<td><strong>Support Log</strong></td>
<td>Used to download the system log and ARM600 configuration collection to a PC. The support log is used for troubleshooting purposes.</td>
</tr>
<tr>
<td><strong>Release Notes</strong></td>
<td>Contains the release notes for the currently running ARM600 firmware version.</td>
</tr>
<tr>
<td><strong>Reboot</strong></td>
<td>Used to reboot the ARM600 server. A verification dialog opens after the reboot button is clicked.</td>
</tr>
</tbody>
</table>
Section 6  Network configuration

6.1 Configuring Ethernet interfaces

The Ethernet interfaces are configured using the WHMI.

1. Connect the PC to ARM600’s eth0 port.
2. Log in to the ARM600 WHMI.
3. On the left pane, under Network, click Network Configuration.
4. Click the Network Interfaces icon.
   The Network Interfaces pane opens.
5. Click Edit interface eth1 and configure the eth1 parameters.

   It is recommended to configure the eth1 interface (LAN) first, as the PC is now connected to ARM600 via the eth0 interface (WAN).

   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>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>eth1</td>
</tr>
<tr>
<td>BOOTPROTO</td>
<td>none</td>
</tr>
<tr>
<td>IPADDR</td>
<td>&lt;IP address&gt;</td>
</tr>
<tr>
<td>NETMASK</td>
<td>&lt;netmask&gt;</td>
</tr>
<tr>
<td>PREFIX</td>
<td>&lt;prefix&gt;</td>
</tr>
<tr>
<td>DEFRUTE</td>
<td>No</td>
</tr>
<tr>
<td>IPV6.DEFRUTE</td>
<td>No</td>
</tr>
</tbody>
</table>

1) Set either the netmask or the prefix

6. Click Save.
7. Click Restart interface eth1.
8. 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 border router.

### Table 11: Eth0 settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>eth0</td>
</tr>
<tr>
<td>BOOTPROTO</td>
<td>none</td>
</tr>
<tr>
<td>IPADDR</td>
<td>&lt;IP address&gt;</td>
</tr>
<tr>
<td>NETMASK</td>
<td>&lt;netmask&gt;</td>
</tr>
<tr>
<td>PREFIX&lt;sup&gt;1)&lt;/sup&gt;</td>
<td>&lt;prefix&gt;</td>
</tr>
<tr>
<td>GATEWAY</td>
<td>&lt;gateway IP&gt;</td>
</tr>
<tr>
<td>DNS1, DNS2</td>
<td>Set the DNS servers, if needed.</td>
</tr>
<tr>
<td>DFRROUTE</td>
<td>Yes</td>
</tr>
<tr>
<td>IPV6_DFRROUTE</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<sup>1)</sup> Set either the netmask or the prefix

The default route is usually set pointing the router in 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.

9. Click **Save**.
10. 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 will not be able to connect to ARM600 using the address https://10.10.10.10:10000.

11. Switch the Ethernet cable from ARM600’s WAN interface to the LAN interface.
   - In the standard edition, switch the Ethernet cable to the Gb2 interface.
   - In the Enterprise edition, switch the Ethernet cable to port 2.

If the eth1 interface has been configured according to this example, use the address https://192.168.0.1:10000 to access ARM600 via its eth1 (LAN) port. Remember to change the PC’s IP address accordingly. For example, use the IP address 192.168.0.2 in the PC with netmask 255.255.255.0.
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>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEVICE</td>
<td>Network interface device name</td>
</tr>
<tr>
<td>BOOTPROTO</td>
<td>“None” is used for static IP addressing; “DHCP” is used for dynamic addressing.</td>
</tr>
<tr>
<td>IPADDR</td>
<td>IP address allocated for this interface</td>
</tr>
<tr>
<td>NETMASK</td>
<td>Netmask in dotted notation, for example, 255.255.255.0</td>
</tr>
<tr>
<td>PREFIX</td>
<td>Netmask bits, for example, 24 (either NETMASK or PREFIX needed)</td>
</tr>
<tr>
<td>GATEWAY</td>
<td>IP gateway’s address for this interface</td>
</tr>
<tr>
<td>DNS1, DNS2</td>
<td>Domain name servers for this interface</td>
</tr>
<tr>
<td>ONBOOT</td>
<td>Interface enabled/disabled in boot up</td>
</tr>
<tr>
<td>IPADDR0</td>
<td>First additional IP address associated to this interface</td>
</tr>
<tr>
<td>PREFIX0</td>
<td>Number of netmask bits for the first additional IP address</td>
</tr>
<tr>
<td>IPADDR1</td>
<td>Second additional IP address associated to this interface</td>
</tr>
<tr>
<td>PREFIX1</td>
<td>Number of netmask bits for the second additional IP address</td>
</tr>
<tr>
<td>IPADDR2</td>
<td>Third additional IP address associated to this interface</td>
</tr>
<tr>
<td>PREFIX2</td>
<td>Number of netmask bits for the third additional IP address</td>
</tr>
<tr>
<td>IPV6INIT</td>
<td>Enable/disable IPv6 for this interface</td>
</tr>
<tr>
<td>DEFRoute</td>
<td>Use this interface as IPv4 default route</td>
</tr>
<tr>
<td>IPV4_FAILSAFE_FATAL</td>
<td>Consider interface failed if IPv4 configuration fails</td>
</tr>
<tr>
<td>IPV6_AUTOCONF</td>
<td>Control IPv6 autoconfiguration</td>
</tr>
<tr>
<td>IPV6_DEFRoute</td>
<td>Use this interface as IPv6 default route</td>
</tr>
<tr>
<td>IPV6_FAILSAFE_FATAL</td>
<td>Consider interface failed if IPv6 configuration fails</td>
</tr>
<tr>
<td>IPV6_PEERDNS</td>
<td>Allow the resolv.conf to be modified according to DHCP server</td>
</tr>
<tr>
<td>IPV6_PEERROUTES</td>
<td>Allow the default gateway to be modified according to DHCP server</td>
</tr>
<tr>
<td>UUID</td>
<td>Universal unique identifier for the interface</td>
</tr>
<tr>
<td>TYPE</td>
<td>Interface type</td>
</tr>
<tr>
<td>NAME</td>
<td>Name of the interface as displayed in the Network Connections</td>
</tr>
</tbody>
</table>
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 as the arctic-adm user.
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 13: Protocol comparison

<table>
<thead>
<tr>
<th>Feature</th>
<th>SSH</th>
<th>HTTPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response time</td>
<td>Quicker</td>
<td>Slower</td>
</tr>
<tr>
<td>Connection type</td>
<td>&quot;Always on&quot;</td>
<td>Interval-based</td>
</tr>
<tr>
<td>Protocol port (TCP)</td>
<td>22</td>
<td>10000</td>
</tr>
</tbody>
</table>

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: 1VHB91201361
- Host IP and port: 10.10.10.5, 22
- Connection mode: Continuous, Polling
- Connection interval (seconds): 1500

**Figure 12: Defining device information**

The next screen shows the ready-made configuration content that needs to be copied to the Arctic device.
Copy this to your Arctic device to complete registration.

```json
{
    "serialnumber": "1VHB91201361",
    "protocol": "ssh",
    "connectionmode": "continuous",
    "connectioninterval": "1500",
    "host": "10.10.10.5",
    "port": "22",
    "sshpublickey": "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAADcqXaZNJwcwz/qyBnLehCr2ALNEnXrfBcU7UQ7uX3g2Ul8nC6corep8YL
Rbc0A2FbLAXQ3lAaV6l77kwp2SIdlSxgBBi5LTEjP1vX2k;
K3fjimRGJv9PMcsr51gfWxafq0ypidJXFyZ68wHHSt8UlW
"sshprivatekey": "-----BEGIN RSA PRIVATE KEY-----

Figure 13: 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.
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.

Reboot the Arctic device.

Log in to ARM600's WHMI, click Arctic Patrol and select Devices.

Select the check box of the new Arctic device, select Accept devices from the drop-down list and click Do action.
12. Click **OK** in the verification dialog.

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

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.
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 19 illustrates the API commands and tools available when both an Arctic wireless device and a RIO600 device have been selected in the device list.
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.
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

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.

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

8. **Back** | **Run this action to all selected devices**

**Figure 21: 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.

**Figure 22: Running and old batches list for firmware update**

### 7.3.2.2 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.

   ![Available RTU configurations](image)

   **Figure 23: 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).

   ![Warning]

   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.

### 7.3.2.3 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.
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_PATROLSSHPRIVATEKEY </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.

### 7.3.2.4 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.

```
patrol -> management -> action -> system reboot
```

**New batch for remote devices**

**Action:** reboot

**Compatible devices for this action:**
- 1VHB91203128

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

![Running and old batches list for rebooting](image)

**Figure 25: 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.

```

<table>
<thead>
<tr>
<th>ID</th>
<th>Title</th>
<th>Status</th>
<th>Start time</th>
<th>Created by</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>system reboot</td>
<td>13/1 completed, duration 0:00:02</td>
<td>11 minutes ago</td>
<td>arm600</td>
</tr>
</tbody>
</table>
```

**Figure 26: 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.

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

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

RIO600 configuration packages are exported from PCM600.
8. ARM600 asset management tries to automatically associate uploaded configurations to the found devices. However, if this is not possible, create the association manually.

8.1. Select a configuration from the left side under **Configurations**.

8.2. Select a RIO600 device from the right side under **Devices**.

8.3. Click the blue arrow to create the association.

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.
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.

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.
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.

---

**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.

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

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.
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**.
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]

Figure 35: 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.

![Warning]

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

![Info]

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 36].
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 37.
OpenVPN Certificate Update

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Certificate on device expires</th>
<th>Last checked</th>
</tr>
</thead>
<tbody>
<tr>
<td>arctic-1</td>
<td>unknown (unknown, not updated)</td>
<td>never</td>
</tr>
<tr>
<td>arctic-2</td>
<td>unknown (unknown, not updated)</td>
<td>never</td>
</tr>
<tr>
<td>arctic-3</td>
<td>unknown (unknown, not updated)</td>
<td>never</td>
</tr>
<tr>
<td>arctic-4</td>
<td>unknown (unknown, not updated)</td>
<td>never</td>
</tr>
<tr>
<td>arctic-5</td>
<td>unknown (unknown, not updated)</td>
<td>never</td>
</tr>
<tr>
<td>arctic-6</td>
<td>unknown (unknown, not updated)</td>
<td>never</td>
</tr>
<tr>
<td>arctic-7</td>
<td>unknown (unknown, not updated)</td>
<td>never</td>
</tr>
<tr>
<td>arctic-8</td>
<td>unknown (unknown, not updated)</td>
<td>never</td>
</tr>
<tr>
<td>arctic-9</td>
<td>unknown (unknown, not updated)</td>
<td>never</td>
</tr>
<tr>
<td>arctic-10</td>
<td>unknown (unknown, not updated)</td>
<td>never</td>
</tr>
</tbody>
</table>

Select devices that have not been updated

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.

Figure 37: 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.
Figure 38: 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  Legacy features

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.

![SSH legacy mode status](image)

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.
Section 9 Troubleshooting

9.1 Common problems and solutions

Table 14: Common problems and solutions

<table>
<thead>
<tr>
<th>Problem</th>
<th>Suggested solution</th>
</tr>
</thead>
</table>
| Cannot establish a VPN tunnel               | • Check that ARM600 has a default gateway configured for the eth0 interface.  
• 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.  
• Verify that the OpenVPN ciphers in ARM600 and in Arctic Wireless Gateway/Controller are the same.  
• 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). |
| Cannot connect to the Arctic device's Patrol | • Check that the registration password has been copied to Arctic Wireless Gateway/Controller.  
• Check that the Arctic Wireless Gateway’s/Controller’s hostname is the same as the OpenVPN peer name in ARM600.  
• Check that the port TCP 10000 is open in the border firewall. |
| Cannot ping the devices connected to Arctic devices | • Verify the routing settings, both in ARM600’s VPN settings and in Arctic Wireless Gateways/Controllers.  
• Check that the ARM600’s firewall allows the ICMP ping in the forward table.  
• If the ping target is a PC, disable the firewall of the PC or allow ICMP messages. |
| SCADA server is unable to connect the field devices through ARM600 | • 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.  
• 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.  
• Verify that Arctic Wireless Gateways/Controllers have a route in the VPN settings (OpenVPN/Routing and Addressing) so that they are able to send reply packets through the VPN tunnel. Usually, the default route can be used.  
• Check that the field devices connected to Arctic Wireless Gateways/Controllers are configured to use the Arctic as a default gateway. |
| Cannot access the asset management features | • Check that the device firmware versions are correct.  
• Arctic device Ver.3.3.1 or later  
• ARM600 Ver.4.2.1 or later |
## 9.2 Questions and answers

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do I need a public, static IP address for ARM600?</td>
<td>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.</td>
</tr>
<tr>
<td>Why is there no SIM card inside ARM600?</td>
<td>Depending on the model, ARM600 is designed to support 300…3000 Arctic Wireless Gateways/Controllers. One cellular network connection on the ARM600 side is not able to provide the required bandwidth for hundreds or thousands of Arctic field devices.</td>
</tr>
<tr>
<td>Can IEC 61850 GOOSE be transferred over this system?</td>
<td>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.</td>
</tr>
<tr>
<td>Our company has a private APN in cellular network. Do we need ARM600?</td>
<td>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.</td>
</tr>
</tbody>
</table>
## Section 10  Technical data

### Table 16: Dimensions

<table>
<thead>
<tr>
<th>Description</th>
<th>Standard edition</th>
<th>Enterprise edition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Height × Width × Depth</td>
<td>42.8 × 434.0 × 495.0 mm</td>
<td>42.8 × 434.0 × 607.0 mm</td>
</tr>
<tr>
<td></td>
<td>1.69 × 17.09 × 19.49 in</td>
<td>1.69 × 17.09 × 23.90 in</td>
</tr>
</tbody>
</table>

### Table 17: Hardware

<table>
<thead>
<tr>
<th>Description</th>
<th>Standard edition</th>
<th>Enterprise edition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor environment</td>
<td>Intel Pentium G4500, 3M Cache, 3.50 GHz, 2C/2T, 51W</td>
<td>Intel Xeon E5-2620 v4, 20M Cache, 2.10 GHz, 8C/16T, 85 W</td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB UDIMM</td>
<td>32 GB RDIMM</td>
</tr>
<tr>
<td>HDD</td>
<td>500 GB 7.2 RPM SATA 3 Gbps 3.5&quot;</td>
<td>300 GB 10K RPM SAS 12 Gbps 2.5in hot-plug</td>
</tr>
<tr>
<td>Power supply</td>
<td>Single power supply 250 W</td>
<td>Dual, hot-plug, redundant power supply (2 ×), 550 W</td>
</tr>
<tr>
<td>Casing</td>
<td>Metal, 19&quot; rack mountable (1U)</td>
<td>Metal, 19&quot; rack mountable (1U)</td>
</tr>
<tr>
<td>Approvals</td>
<td>Global CB Scheme, CE, FCC</td>
<td>Global CB Scheme, CE, FCC</td>
</tr>
<tr>
<td>Environmental conditions</td>
<td>Operational temperature 5...35°C at 5...85% relative humidity with 29°C dew point</td>
<td>Operational temperature 5...40°C at 5...85% relative humidity with 29°C dew point</td>
</tr>
<tr>
<td></td>
<td>Humidity 5...85% (noncondensing) at a maximum wet bulb temperature of 29°C (84.2°F)</td>
<td>Humidity 5...85% (noncondensing) at a maximum wet bulb temperature of 29°C (84.2°F)</td>
</tr>
</tbody>
</table>

### Table 18: Standard edition

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating voltage</td>
<td>100...240 V AC, autoranging, 50/60 Hz</td>
</tr>
<tr>
<td>Temperature (for altitude less than 950 m or 3117 ft)</td>
<td>10...35°C (50...95°F) with no direct sunlight on the equipment</td>
</tr>
<tr>
<td>Storage</td>
<td>20°C/h (36°F/h)</td>
</tr>
<tr>
<td>Maximum temperature (gradient and operating)</td>
<td>20°C/h (36°F/h)</td>
</tr>
</tbody>
</table>

Table continues on next page
### Technical data

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relative humidity</td>
<td>Operating 5...85% (noncondensing) at a maximum wet bulb temperature of 29°C (84.2°F).</td>
</tr>
<tr>
<td></td>
<td>Storage 5...95% relative humidity with 33°C (91°F) maximum dew point. Atmosphere must be non-condensing at all times.</td>
</tr>
<tr>
<td>Maximum vibration</td>
<td>Operating 0.26 Grms at 5...350 Hz (operation orientation)</td>
</tr>
<tr>
<td></td>
<td>Storage 1.88 Grms at 10...500 Hz for 15 min (all six sides tested)</td>
</tr>
<tr>
<td>Maximum shock</td>
<td>Operating Six consecutively executed shock pulses in the positive and negative x, y, and z axes of 40 G for up to 2.3 ms.</td>
</tr>
<tr>
<td></td>
<td>Storage One pulse on each side of the system of 71 G up to 2 ms</td>
</tr>
<tr>
<td>Maximum altitude</td>
<td>Operating 3.048 m (10,000 ft)</td>
</tr>
<tr>
<td></td>
<td>Storage -15.2...10,668 m (-50...35,000 ft)</td>
</tr>
<tr>
<td>Operating altitude de-rating</td>
<td>Up to 35°C (95°F) Maximum temperature is reduced by 1°C/300 m (1°F/547 ft) above 900 m (3,117 ft).</td>
</tr>
</tbody>
</table>

1) This system is also designed to be connected to IT power systems with a phase-to-phase voltage not exceeding 230 V

### Table 19: Enterprise edition

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating voltage</td>
<td>100...240 V AC, autoranging, 50/60 Hz</td>
</tr>
<tr>
<td>Temperature</td>
<td>Continuous operation (for altitudes less than 950 m or 3117 ft)</td>
</tr>
<tr>
<td></td>
<td>5...40°C at 10...80% relative humidity with 29°C max dew point</td>
</tr>
<tr>
<td></td>
<td>De-rate maximum allowable dry bulb temperature at 1°C per 300 m above 900 m (1°F per 550 ft)</td>
</tr>
<tr>
<td></td>
<td>Storage 40...65°C (-40...149°F) with a maximum temperature gradation of 20°C per hour</td>
</tr>
<tr>
<td>Relative humidity</td>
<td>Operating 5...85% (noncondensing) at a maximum wet bulb temperature of 29°C (84.2°F)</td>
</tr>
<tr>
<td></td>
<td>Storage 5...95% at a maximum wet bulb temperature of 33°C (91°F)</td>
</tr>
<tr>
<td>Maximum vibration</td>
<td>Operating 0.26 Grms at 5...350 Hz in all orientations</td>
</tr>
<tr>
<td></td>
<td>Storage 1.87 Grms at 10...500 Hz for 15 min (all six sides tested)</td>
</tr>
<tr>
<td>Maximum shock</td>
<td>Operating Half sine shock in all operational orientations of 31 G ±5% with a pulse duration of 2.6</td>
</tr>
<tr>
<td></td>
<td>Storage Half sine shock on all six sides of 71 G ±5% with a pulse duration of 2 ms ±10%, square wave shock on all six sides of 27 G with velocity change at 235 in/s or greater</td>
</tr>
<tr>
<td>Maximum altitude</td>
<td>Operating -15.2...3048 m (-50...10,000 ft) For altitudes above 2950 ft, the maximum operating temperature is de-rated 1°F/547 ft.</td>
</tr>
<tr>
<td></td>
<td>Storage -15.2...10,668 m (-50...35,000 ft)</td>
</tr>
</tbody>
</table>
Table 20: Ordering data

<table>
<thead>
<tr>
<th>Description</th>
<th>Standard edition ARM600B2500NA</th>
<th>Enterprise edition ARM600B2505NA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet ports</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Power supply</td>
<td>single</td>
<td>dual</td>
</tr>
<tr>
<td>HDD</td>
<td>single</td>
<td>dual</td>
</tr>
<tr>
<td>RAID</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>CPU type</td>
<td>Intel Pentium G4500</td>
<td>Xeon</td>
</tr>
<tr>
<td>RAM</td>
<td>8 GB</td>
<td>32 GB</td>
</tr>
<tr>
<td>Max Arctic connections</td>
<td>300</td>
<td>3000</td>
</tr>
<tr>
<td>Size</td>
<td>1U 19&quot;</td>
<td>1U 19&quot;</td>
</tr>
</tbody>
</table>
### Section 11  Glossary

| AC       | Alternating current |
| API      | Application programming interface |
| APN      | Access Point Name |
| D-NAT    | Destination network address translation |
| DHCP     | Dynamic Host Configuration Protocol |
| DMZ      | De-militarized zone |
| DNS      | Domain Name System |
| EMC      | Electromagnetic compatibility |
| Ethernet | A standard for connecting a family of frame-based computer networking technologies into a LAN |
| GOOSE    | Generic Object-Oriented Substation Event |
| HMI      | Human-machine interface |
| HTTPS    | Hypertext Transfer Protocol Secure |
| ICMP     | Internet Control Message Protocol |
| iDRAC    | Integrated Dell remote access control |
| IEC      | International Electrotechnical Commission |
| IEC 61850| International standard for substation communication and modeling |
| IP       | Internet protocol |
| IP address | 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. |
| KPI      | Key performance indicator |
| L2TP     | Layer 2 tunneling protocol |
| LAN      | Local area network |
| LCD      | Liquid crystal display |
| M2M      | Machine to machine |
| MD5      | Message digest algorithm 5 |
| N/A      | Not applicable or available |
| NTP      | Network time protocol |
| PC       | 1. Personal computer |
2. Polycarbonate

**PCM600** Protection and Control IED Manager

**PSU** Power supply unit

**RAM** Random access memory

**RIO600** Remote I/O unit

**RTU** Remote terminal unit

**Rx** Receive/Received

**S-NAT** Source network address translation

**SCADA** Supervision, control and data acquisition

**SIM** Subscriber identity module

**SNMP** Simple Network Management Protocol

**SSH** Secure shell

**TCP** Transmission Control Protocol

**Tx** Transmit/Transmitted

**UDP** User datagram protocol

**USB** Universal serial bus

**VGA** Video graphics array

**VPN** Virtual Private Network

**WAN** Wide area network

**WHMI** Web human-machine interface

**XML** Extensible markup language