ComAp
The heart of smart control

InteliLite 4

Cyber Security Guide

Written by Jan Tomandl
Prague, Czech Republic
ComAp a.s., U Uranie 1612/14a,
170 00 Prague 7, Czech Republic
Tel: +420 246 012 111
E-mail: info@comap-control.com, www.comap-control.com

Cyber Security Guide

Table of contents

1 Document information

1.1 Clarification of Notation

***Note:** This type of paragraph calls the reader's attention to a notice or related theme.*

> **IMPORTANT: This type of paragraph highlights a procedure, adjustment etc., which can cause a damage or improper function of the equipment if not performed correctly and may not be clear at first sight.**

> **Example:** This type of paragraph contains information that is used to illustrate how a specific function works.

1.2 About this guide

This document should give a guidance for users how to use new features related to cybernetic security in InteliLite 4 controllers.

The document also points on the differences between the previous controllers and the new ones to help with migration to the new devices.

The structure of the document is created with focus to provide guidance from unboxing the controller till putting into operation and maintenance.

Certain level of user experience with ComAp controllers is expected.

1.3 Legal notice

This End User's Guide/Manual as part of the Documentation is an inseparable part of ComAp's Product and may be used exclusively according to the conditions defined in the "END USER or Distributor LICENSE AGREEMENT CONDITIONS – COMAP CONTROL SYSTEMS SOFTWARE" (License Agreement) and/or in the "ComAp a.s. Global terms and conditions for sale of Products and provision of Services" (Terms) and/or in the "Standardní podmínky projektů komplexního řešení ke smlouvě o dílo, Standard Conditions for Supply of Complete Solutions" (Conditions) as applicable.

ComAp's License Agreement is governed by the Czech Civil Code 89/2012 Col., by the Authorship Act 121/2000 Col., by international treaties and by other relevant legal documents regulating protection of the intellectual properties (TRIPS).

The End User and/or ComAp's Distributor shall only be permitted to use this End User's Guide/Manual with ComAp Control System Registered Products. The Documentation is not intended and applicable for any other purpose.

Official version of the ComAp's End User's Guide/Manual is the version published in English. ComAp reserves the right to update this End User's Guide/Manual at any time. ComAp does not assume any responsibility for its use outside of the scope of the Terms or the Conditions and the License Agreement.

Licensed End User is entitled to make only necessary number of copies of the End User's Guide/Manual. Any translation of this End User's Guide/Manual without the prior written consent of ComAp is expressly prohibited!

Even if the prior written consent from ComAp is acquired, ComAp does not take any responsibility for the content, trustworthiness and quality of any such translation. ComAp will deem a translation equal to this End User's Guide/Manual only if it agrees to verify such translation. The terms and conditions of such verification must be agreed in the written form and in advance.

For more details relating to the Ownership, Extent of Permitted Reproductions Term of Use of the Documentation and to the Confidentiality rules please review and comply with the ComAp's License Agreement, Terms and Conditions available on www.comap-control.com.

Security Risk Disclaimer

Pay attention to the following recommendations and measures to increase the level of security of ComAp products and services.

Please note that possible cyber-attacks cannot be fully avoided by the below mentioned recommendations and set of measures already performed by ComAp, but by following them the cyber-attacks can be considerably reduced and thereby to reduce the risk of damage. ComAp does not take any responsibility for the actions of persons responsible for cyber-attacks, nor for any damage caused by the cyber-attack. However, ComAp is prepared to provide technical support to resolve problems arising from such actions, including but not limited to restoring settings prior to the cyber-attacks, backing up data, recommending other preventive measures against any further attacks.

Warning: Some forms of technical support may be provided against payment. There is no legal or factual entitlement for technical services provided in connection to resolving problems arising from cyber-attack or other unauthorized accesses to ComAp's Products or Services.

General security recommendations and set of measures

1. AccessCode

- Change the AccessCode BEFORE the device is connected to a network.

- Use a secure AccessCode – ideally a random string of 8 characters containing lowercase, uppercase letters and digits.

- For each device use a different AccessCode.

2. Password

- Change the password BEFORE the device enters a regular operation.

- Do not leave displays or PC tools unattended if an user, especially administrator, is logged in.

3. Controller Web interface

- The controller web interface at port TCP/80 is based on http, not https, and thus it is intended to be used only in closed private network infrastructures.

- Avoid exposing the port TCP/80 to the public Internet.

4. MODBUS/TCP

- The MODBUS/TCP protocol (port TCP/502) is an instrumentation protocol designed to exchange data between locally connected devices like sensors, I/O modules, controllers etc. From it's nature it does not contain any kind of security – neither encryption nor authentication. Thus it is intended to be used only in closed private network infrastructures.

- Avoid exposing the port TCP/502 to the public Internet.

5. SNMP

- The SNMP protocol (port UDP/161) version 1,2 is not encrypted. Thus it is intended to be used only in closed private network infrastructures.

- Avoid exposing the port UDP/161 to the public Internet.

General security recommendations and set of measures

1. Production mode
   - Disable production mode BEFORE the controller is put into regular operation.
2. User accounts
   - Change password for the existing default administrator account or replace that account with a completely new one BEFORE the controller is put into regular operation mode.
   - Do not leave PC tools (e.g. InteliConfig) unattended while a user, especially administrator, is logged in.
3. AirGate Key
   - Change the AirGate Key BEFORE the device is connected to the network.
   - Use a secure AirGate Key – preferably a random string of 8 characters containing lowercase, uppercase letters and digits.
   - Use a different AirGate Key for each device.
4. MODBUS/TCP
   - The MODBUS/TCP protocol (port TCP/502) is an instrumentation protocol designed to exchange data between locally connected devices like sensors, I/O modules, controllers etc. By it's nature it does not contain any kind of security – neither encryption nor authentication. Thus it is intended to be used only in closed private network infrastructures.
   - Avoid using MODBUS/TCP in unprotected networks (e.g. Internet).
5. SNMP
   - The SNMP protocol (port UDP/161) version 1 and version 2 are not encrypted. They are intended to be used only in closed private network infrastructures.
   - Avoid using SNMP v1 and v2 in unprotected networks (e.g. Internet).

1.4 Document history

Revision number	Related sw. version	Date	Author
1	N/A	4.1.2022	Jan Tomandl

back to Document information

2 Overview of Cyber Security features in InteliLite 4

back to Table of contents

2.1 Zone model

Zone model is a principle used to split the controller "terminal" communication interfaces into two categories:

2.1.1 Trusted interfaces

Trusted interfaces are the ones that are used locally, inside buildings, mostly protected by some physical access restrictions etc. That means it is possible to apply **less strict Cyber Security rules** for those interfaces. Trusted interfaces are:

- Built-in display
- USB
- RS232/RS485
- "Local" Ethernet, which is intended especially for local external display connection

2.1.2 Untrusted interfaces

Untrusted interfaces are the ones that are not under full control of the asset owner or operator, that are running outside a protected infrastructure and may be exposed to anyone. This is why **more strict Cyber Security rules** must apply for those interfaces. Untrusted interfaces are:

- "General purpose" Ethernet, which is typically used over Internet (e.g. CM3-ETH module in InteliLite 4)
- Cellular modules

Note: *The differences in Cyber Security rules that apply for trusted and untrusted interfaces will be mentioned in further parts of the document.*

2.2 Authentication control

Authentication of users to the controller is based on user accounts, similarly to personal computers, web services etc. When a connection with the controller is established a **user must authenticate (log-in)** into the controller.

Note: *There is not any "Access Code" anymore.*

2.2.1 User accounts

- There must be at least one account with administrator level defined in the controller
- Administrator can then define other user accounts

- InteliLite 4 has 5 user accounts

Account attributes

Each user account has following attributes:

Attribute	Status	Length	Character allowed	Note
username	mandatory	6-15	lowercase letters, uppercase letters, digits	Must be unique in the controller Must contain at least 1 letter
user ID	optional	4	digits	Must be unique in the controller Must be exactly 4 digits long
PIN	optional	4	digits	Must be exactly 4 digits long
password	mandatory	6-15	lowercase letters, uppercase letters, digits	Must contain at least 1 letter and 1 digit
access level	mandatory	N/A	number	0,1,2 ... administrator

User login

When a connection with the controller is established an **user must authenticate (log-in)** into the controller. The user may log in into the controller using one of following methods:

- Entering valid combination of username and password
- Entering valid combination of user ID and PIN (only **Trusted interfaces (page 6)**)

> **IMPORTANT: It is not possible to manage users while administrator is logged in with UID/PIN only. Managing users requires the administrator to log-in with username/password.**

Factory default state

In factory default state there is one single account defined in the controller:

username	**password**
"administrator"	<controller s.n.>

The alarm “Wrn Default Password” is displayed while the factory default account is present in the controller.

Lost password

If administrator password is lost and it is no more possible to manage the controller the user accounts can be reset back to factory default state.

> **IMPORTANT: In controller the backup e-mail address must be correctly filled-in to perform the reset operation!**

1. Request code must be read from controller using InteliConfig via some trusted interface (e.g. USB) and sent to technical support or put into ComAp "InteliBot" service.
2. Action code is then returned to the adjusted backup e-mail address.
3. Action code must be then written into the controller using InteliConfig via some trusted interface (e.g. USB). After that user accounts are reset to factory default state.

2.2.2 Implicit user

Implicit user is a special feature which is targeted to:

- Keep the rule that while a connection is established and running a user must always be logged-in into the controller and
- Allow displays, SCADAs and other local monitoring devices to have certain limited access (mostly read and display operational values) without a physical user needed to log-in.

Implicit user has following features:

- Is fixedly present in the controller, not visible in the user account table
- Has fixed access level 0 (unless **Production mode (page 8)** is active)
- In **Trusted interfaces (page 6)** the implicit user is automatically logged-in all the time while not any physical user is logged in into the controller

> **IMPORTANT: Implicit user function is available only at trusted interfaces.**

Production mode

The Production mode is intended to simplify manufacturing process for OEMs.

- While production mode is active the implicit user has **administrator level** and alarm "Wrn Production Mode" is displayed
- Practically it means that while production mode is active it is possible to perform **any operation with the controller without any user needed to login**.

> **IMPORTANT: Production mode must be disabled before the controller is put into regular operation.**

2.2.3 Protection against brute force

The controller is actively protected against brute-force attacks aiming to retrieve credentials and gain unauthorized access to the controller.

If the protection is active for any account or interface or was previously active the alarm "Wrn Brute Force Protection Active" is displayed.

Account protection – username

The protection takes place if a person attempting to login into the controller repeatedly provides a correct username (i.e. username that does exist in some account in the controller) but incorrect password.

- If login fails (=incorrect password provided) 5 times after each other the appropriate username is blocked for 1 minute.
- Every next failed login causes the username is blocked for twice longer period than the previous period was, but maximum blocking time is 20 minutes
- While the username is blocked it is not possible to login using the respective username via any interface even with correct password. Other accounts (usernames) are untouched.
- The time between attempts is not taken into account. The counter of failed attempts is cleared first when the respective user performs successful login.

Account protection – user ID

The protection takes place if a person attempting to login into the controller repeatedly provides a correct user ID but incorrect PIN.

- If login fails (=incorrect PIN provided) 10 times after each other the user ID is blocked permanently.
- The user must login into his account with username and password and then change his PIN.
- The time between attempts is not taken into account.

Interface protection

The protection takes place if a person attempting to login into the controller repeatedly provides incorrect user identification, i.e. the identifier is neither a valid username nor user ID.

- After 20 consequent attempts as described above the respective interface is blocked for 2 minutes.
- While the interface is blocked it is not possible to log-in, even with correct credentials.

2.3 Access Control

Access to the controller from the communication interfaces (i.e. reading objects, writing objects, command invoking, firmware updating) is based on **access levels**.

The user, who is logged-in, must have access level higher or equal to the access lever required for the particular operation.

- Lowest access level is 0
- Highest access level is "administrator"
- Total number of levels available depends on controller type (InteliLite 4 has levels 0,1,2,3, administrator level is 3)

Table of required access levels

Operation	Required access level
read object	0
write application object	configurable
invoke application command	configurable
read configuration	0
write configuration	administrator
write firmware	administrator
manage user accounts	administrator

Note: *The principle of levels is known from previous controllers and basically remains without changes.*

2.4 Remote Communication

2.4.1 AirGate 2nd Generation

AirGate second generation, aka AirGate 2.0, is new generation of AirGate technology which is developed with focus on increasing **reliability, Cyber Security and level of user experience**.

It is a distributed system consisting of multiple nodes. It provides higher capacity, redundancy and more optimal routing of the traffic.

It is based purely on TCP protocol. All the traffic is fully encrypted. It provides first level of defense for connected controllers.

Although there are some setpoints related to AirGate 2.0, practically the function is **plug-and-play** and does not require any adjustments except adjusting "**AirGate Key**", which is the "password" used by the system to provide the first level of defense – prevent connected controllers from even getting into touch with unauthorized subjects. In other words: AirGate 2.0 will not pass any connection request onto the controller if correct AirGate Key is not provided with the connection request.

AirGate function is **enabled/disabled by setpoint *AirGate Connection***. Location of the setpoint depends on controller and interface type (e.g. in setpoint group “CM-4G-GPS” or “CM-Ethernet”).

2.4.2 Controller registration

Controller is registered automatically when it is first time connected to Internet and AirGate function is enabled. After successful registration the controller obtains "**AirGate ID**" which consists of 9 digits (no characters) and is **displayed in controller values**.

2.4.3 AirGate Key

AirGate Key is a kind of "password" which must be defined in controller (e.g. via USB) prior to AirGate connection can be established with that controller.

2.4.4 Connecting to controller

When connecting to the controller via AirGate from e.g. InteliConfig following parameters must be provided:

- **AirGate node – "global.airgate.link"** or any other node
- **Connection port – 54441**
- **Device AirGate ID** – the 9-digit identification number obtained during registration
- AirGate key – the string defined in controller (as described above)

***Note:** As the AirGate is **Untrusted interfaces (page 6)** it is also required that a user will login into the controller immediately after connection has been created.*

2.5 Firewall

Firewall function allows to **restrict computers which can connect to the communication services** in the controller based on computer IP address. E.g. it is possible to restrict that in the local network only one specific computer (let's say SCADA computer in the control room..) can access controller's MODBUS/TCP server.

- Firewall function is enabled/disabled by setpoint *IP Firewall*. Location of the setpoint depends on controller and interface type (e.g. in setpoint group "CM-4G-GPS" or "CM-Ethernet").
- Firewall function affects only incoming traffic for application services (i.e. application services that "listen" for connection), thus **AirGate is not influenced** as it is not a "listening" service but it actively creates outgoing traffic.

> **IMPORTANT: Improper adjustment of the firewall can cause the current connection would be interrupted and the controller would remain inaccessible remotely!**

2.5.1 Firewall Rules

The firewall rules are defined in controller configuration. The rules are based on white-list principle, i.e. if rule is fulfilled the traffic is allowed to pass through, if not the traffic is dropped. Please note, that this principle implies no rule = no traffic = remote access completely denied.

- A rule is defined as IP ADDRESS, MASK, PORT.
- A rule is fulfilled if:
  - (packet_source_ip & rule_mask == rule_ip_address) and (packet_destination_port == rule_port)
    & ... bitwise multiplication
    and ... logical multiplication

2.5.2 Examples

Rule: IP=**192.168.1.0**, MASK=**255.255.255.0**, PORT=**23**

Packet source IP address	Packet destination port	Evaluation	Rule fulfilled
192.168.2.100	23	PACKET: 192.168.002.100 MASK: 255.255.255.000 RESULT: 192.168.002.000 ✗ Result <> Rule IP ✓ Port = Rule port	NO
192.168.1.100	23	PACKET: 192.168.001.100 MASK: 255.255.255.000 RESULT: 192.168.001.000 ✓ Result = Rule IP ✓ Port = Rule port	YES
192.168.1.100	25	PACKET: 192.168.001.100 MASK: 255.255.255.000 RESULT: 192.168.001.000 ✓ Result = Rule IP ✗ Port = Rule port	NO

***Note:** Some communication services (protocols) have their IP ports adjustable by setpoints. E.g. ComAp/TCP protocol is listening by default at port 23, but can be changed to any other port number by setpoint. The firewall rules must be adjusted to match the port to which the service is adjusted.*
E.g. if ComAp/TCP protocol port was changed from default 23 to, let's say, 9923 the firewall rules for this protocol must be created for port 9923 as well.

2.5.3 Services influenced by firewall

Service (protocol)	Protocol	Default port	Port is adjustable
ComAp direct TCP connection server	ComAp/TCP	23	YES
Device discovery	ComAp/UDP	2413	NO
MODBUS server	MODBUS/TCP	502	NO
SNMP agent	SNMP/UDP	161	NO

Note: *Valid for InteliLite 4 controller equipped with plug-in Ethernet module.*

▲ back to Overview of Cyber Security features in InteliLite 4

3 Getting started with the controller

3.1 After unboxing

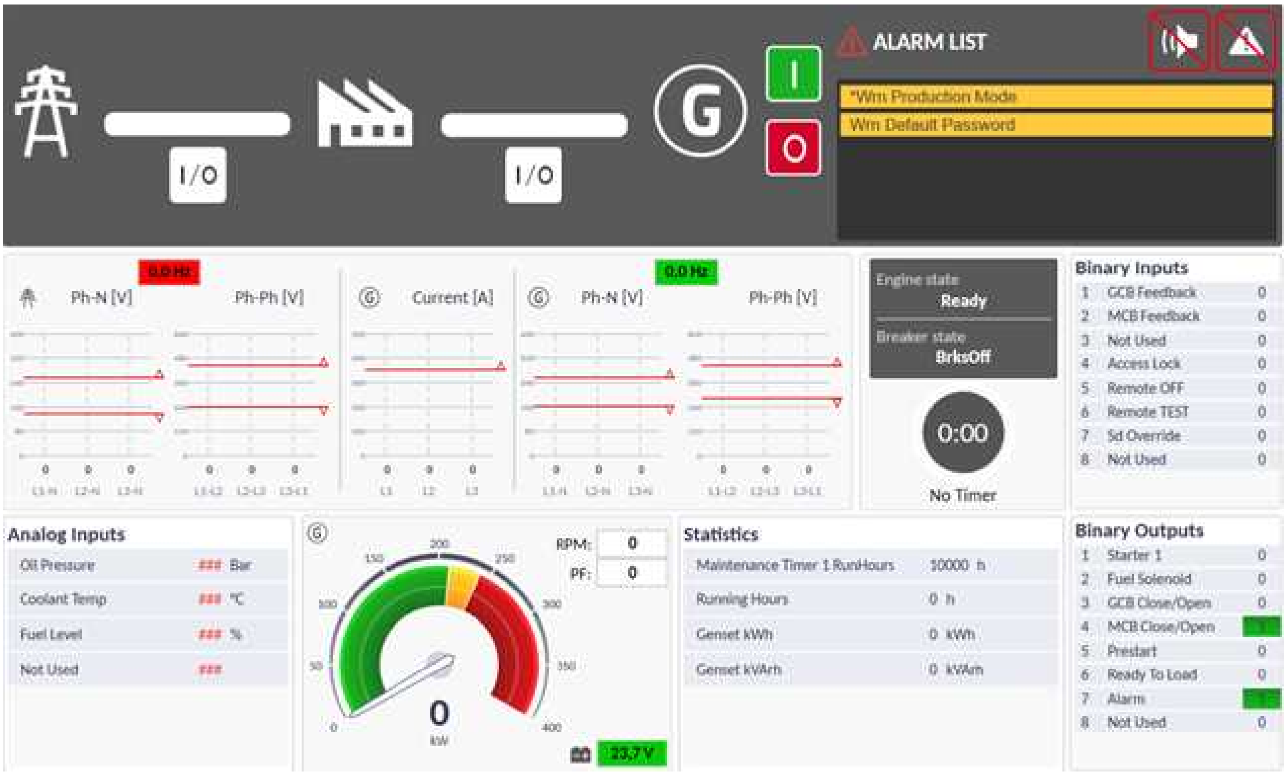
When the controller is unboxed:

1. User accounts are in **Factory default state (page 7)** and the respective warning is displayed.
2. The controller is in **Production mode (page 8)** and the respective warning is displayed.

Now it is the suitable moment to **connect InteliConfig via USB and prepare the controller for operation**, i.e. create/modify the controller configuration, adjust setpoints etc.

It is not needed to login to the controller with the default administrator account. The production mode enables **performing any operation without user login**.

> **IMPORTANT: It is not recommended to connect the controller now to any untrusted network as the user accounts are in factory default state and the controller would be exposed to risk of unauthorized access.**



*Wrn Production Mode
Wrn Default Password

Engine state: Ready
Breaker state: BrksOff

0:00
No Timer

Binary Inputs

1	GCB Feedback	0
2	MCB Feedback	0
3	Not Used	0
4	Access Lock	0
5	Remote OFF	0
6	Remote TEST	0
7	Sd Override	0
8	Not Used	0

Analog Inputs

Oil Pressure	###	Bar
Coolant Temp	###	°C
Fuel Level	###	%
Not Used	###	

Statistics

Maintenance Timer 1 RunHours	10000	h
Running Hours	0	h
Genset kWh	0	kWh
Genset kVArh	0	kVArh

Binary Outputs

1	Starter 1	0
2	Fuel Solenoid	0
3	GCB Close/Open	0
4	MCB Close/Open	1
5	Prestart	0
6	Ready To Load	0
7	Alarm	1
8	Not Used	0

Image 3.1 Production Mode and Default Password alarms in InteliConfig

3.2 Create user accounts

Creating user user accounts is the next step prior to putting into operation is finalized.

Procedure:

1. While InteliConfig is still connected via USB to the controller and either administrator is logged in or production mode is active go to menu "Tools" → "User Administration" → "User management". The user management window will open.

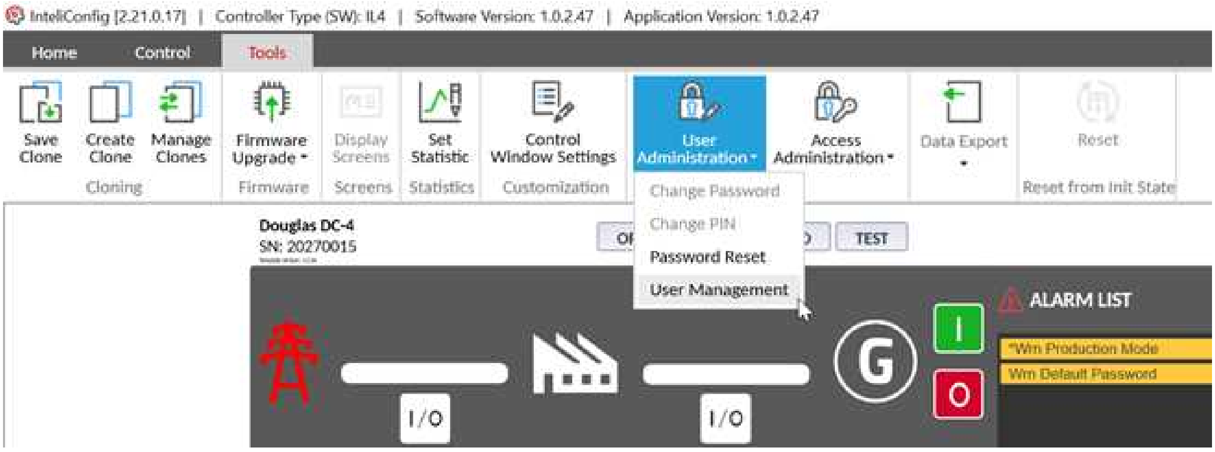
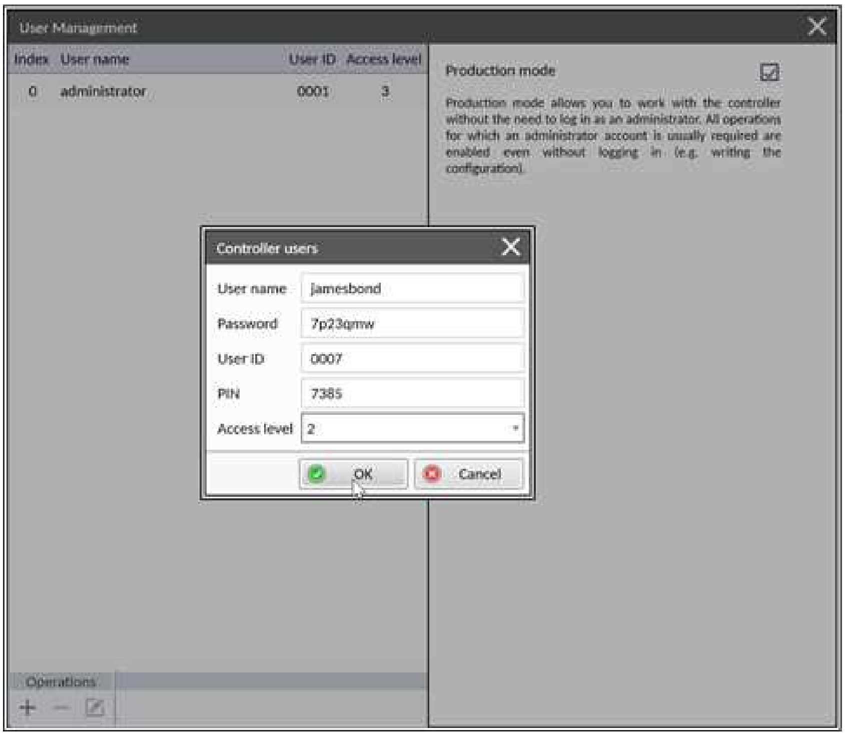


Image 3.2 User management menu in InteliConfig

2. Use buttons "Add","Remove","Edit" to create accounts according to your needs. See the chapter **Account attributes (page 7)** about details related to attributes of the accounts.



Index	User name	User ID	Access level
0	administrator	0001	3

Production mode ☑

Production mode allows you to work with the controller without the need to log in as an administrator. All operations for which an administrator account is usually required are enabled even without logging in (e.g. writing the configuration).

User name: jamesbond

Password: 7p23qmw

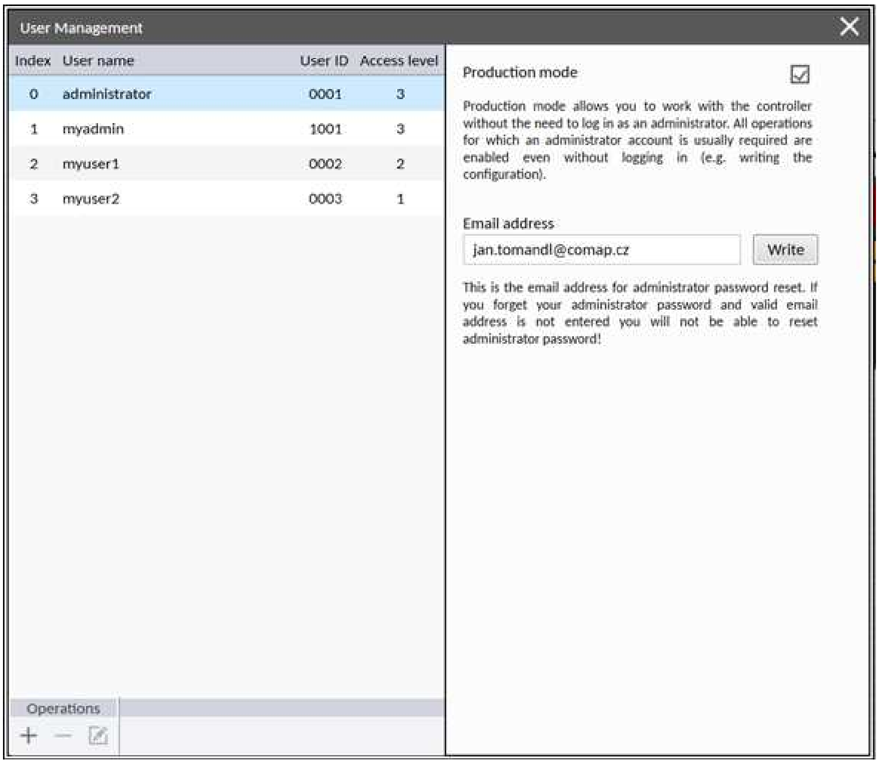
User ID: 0007

PIN: 7385

Access level: 2

Image 3.3 Account attributes setup in InteliConfig

3. Keep principles as follows:
   a. There must be at least one account with administrator level
   b. Create individual accounts as much as your application and controller account capacity allows it
   c. If using shared accounts is needed use it for persons with similar or same roles (e.g. one account for engine maintenance technicians and other for electrical technicians)
   d. Avoid sharing account among persons with different roles
   e. **Avoid providing administrator level for accounts which do not need it**
4. In the "User Management" window **adjust the backup e-mail address**.


User Management

Index	User name	User ID	Access level
0	administrator	0001	3
1	myadmin	1001	3
2	myuser1	0002	2
3	myuser2	0003	1

Production mode ☑

Production mode allows you to work with the controller without the need to log in as an administrator. All operations for which an administrator account is usually required are enabled even without logging in (e.g. writing the configuration).

Email address

jan.tomandl@comap.cz

This is the email address for administrator password reset. If you forget your administrator password and valid email address is not entered you will not be able to reset administrator password!

Image 3.4 Setup of email address for administrator password reset in InteliConfig

5. Adjusting correct backup e-mail address is an essential step for resetting user accounts to default state (if administrator password is lost). The action code for resetting is automatically sent to this e-mail address and thus if incorrect address is provided it will not be possible to receive the code.
6. Go again to the "User Management" window and remove the default administrator account or at least change his password. The alarm "*Wrn Default Password*" will disappear.
7. In the "User Management" window disable the "Production mode". The alarm "*Wrn Production Mode*" will disappear.

3.2.1 Lost password

When the password for administrator account is lost it is possible to reset the controller into **Factory default state (page 7)**, i.e. delete all user accounts and create the default administrator account.

Procedure:

1. Connect InteliConfig via USB to the controller, go to "Tools" → "User Administration" → "Password reset".

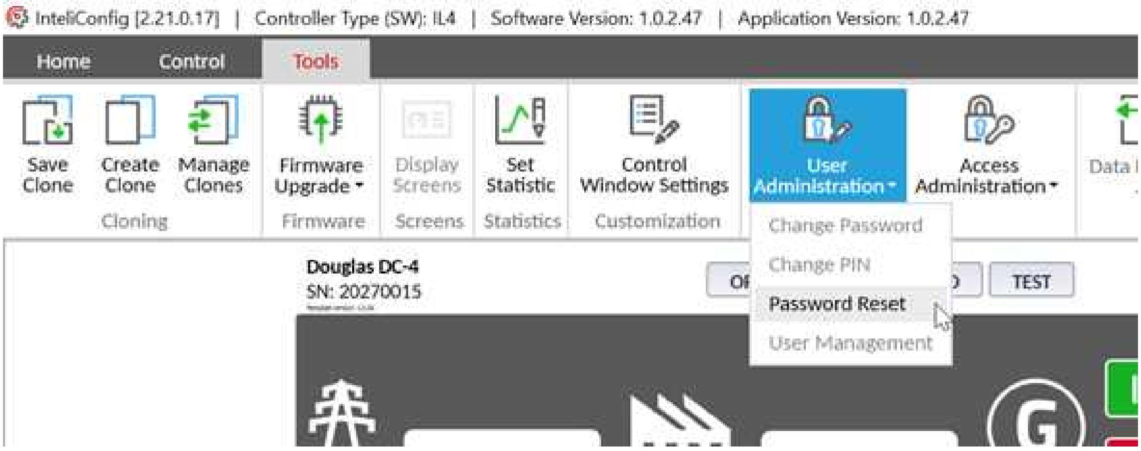
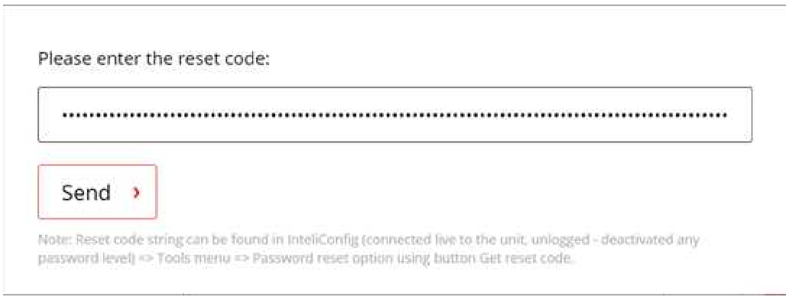

InteliConfig [2.21.0.17] | Controller Type (SW): IL4 | Software Version: 1.0.2.47 | Application Version: 1.0.2.47

Image 3.5 Password Reset option in InteliConfig

2. Press "Get reset code"
3. Copy the "PRRC code" into clipboard
4. Go to web browser and navigate to [ComAp – InteliBot (comap-control.com)](comap-control.com)
5. Select "Password issues" → "Controller password" and proceed according to InteliBot instructions. When prompted to enter PRRC code paste the code obtained by InteliConfig into the InteliBot dialog.



Please enter the reset code:

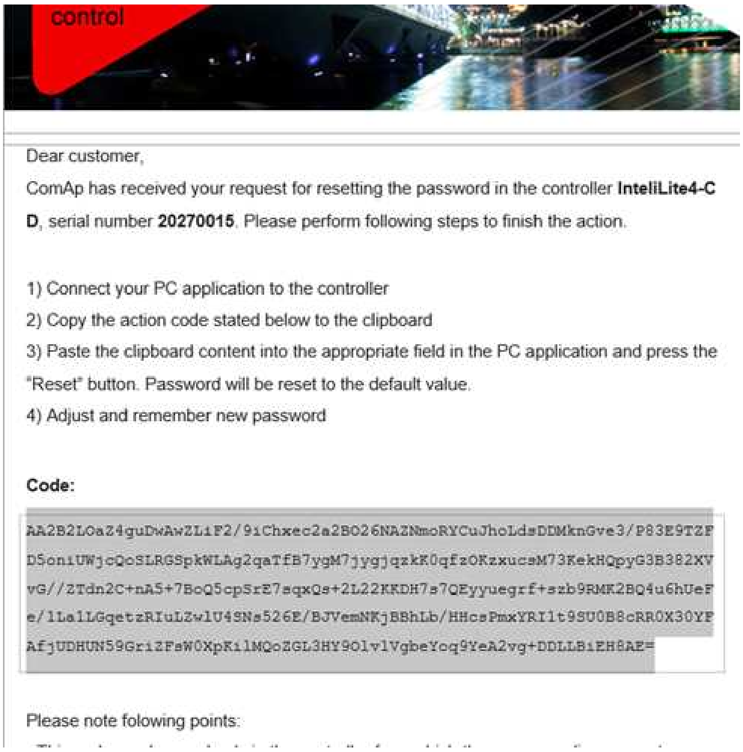
•••

Send ›

Note: Reset code string can be found in InteliConfig (connected live to the unit, unlogged - deactivated any password level) => Tools menu => Password reset option using button Get reset code.

Image 3.6 Entering "PRRC code" in InteliBot

6. After a while you will receive e-mail with "PRAC code". Select carefully the code a copy it to clipboard.



Dear customer,

ComAp has received your request for resetting the password in the controller **InteliLite4-CD**, serial number **20270015**. Please perform following steps to finish the action.

1) Connect your PC application to the controller
2) Copy the action code stated below to the clipboard
3) Paste the clipboard content into the appropriate field in the PC application and press the "Reset" button. Password will be reset to the default value.
4) Adjust and remember new password

Code:

```
AA2B2LOaZ4guDwAwZLiF2/9iChxec2a2BO26NAZNmoRYCuJhoLdsDDMknGve3/P83E9TZF
D5oniUWjcQoSLRGSpkWLAg2qaTfB7ygM7jygjqzkK0qfzOKzxucsM73KekHQpyG3B382XV
vG//ZTdn2C+nA5+7BoQ5cpSrE7sqxQs+2L22KKDH7s7QEyyuegrf+szb9RMK2BQ4u6hUeF
e/1La1LGqetzRIuLZw1U4SNs526E/BJVemNKjBBhLb/HHcsPmxYRI1t9SU0B8cRR0X30YF
AfjUDHUN59GriZFsW0XpKi1MQoZGL3HY9Olv1VgbeYoq9YeA2vg+DDLLBiEH8AE=
```

Please note folowing points:

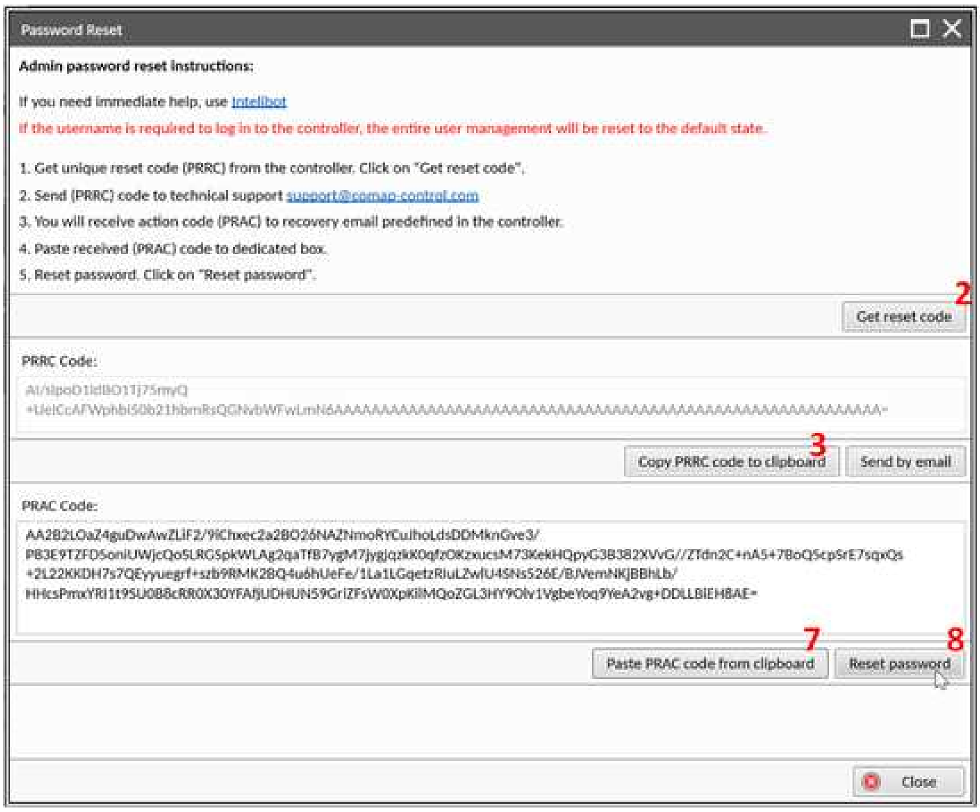
Image 3.7 Sample of email with "PRAC code"

7. Paste the PRAC code into the InteliConfig "Password Reset" window into the "PRAC code" field.

   > ***Note:*** *You may close the "Password Reset" window or even temporarily disconnect InteliConfig between steps 3 and 7.*

8. Click on "Reset Password" button.

> **IMPORTANT: You should disconnect the untrusted controller interfaces from the networks while the default administrator account is present in the controller.**


Password Reset

Admin password reset instructions:

If you need immediate help, use Intelibot

If the username is required to log in to the controller, the entire user management will be reset to the default state.

1. Get unique reset code (PRRC) from the controller. Click on "Get reset code".
2. Send (PRRC) code to technical support support@comap-control.com
3. You will receive action code (PRAC) to recovery email predefined in the controller.
4. Paste received (PRAC) code to dedicated box.
5. Reset password. Click on "Reset password".

PRRC Code:

```
AI/slpoD1ldBO1Tj75myQ
+UeICcAFWphbi50b21hbmRsQGNvbWFwLmN6AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=
```

PRAC Code:

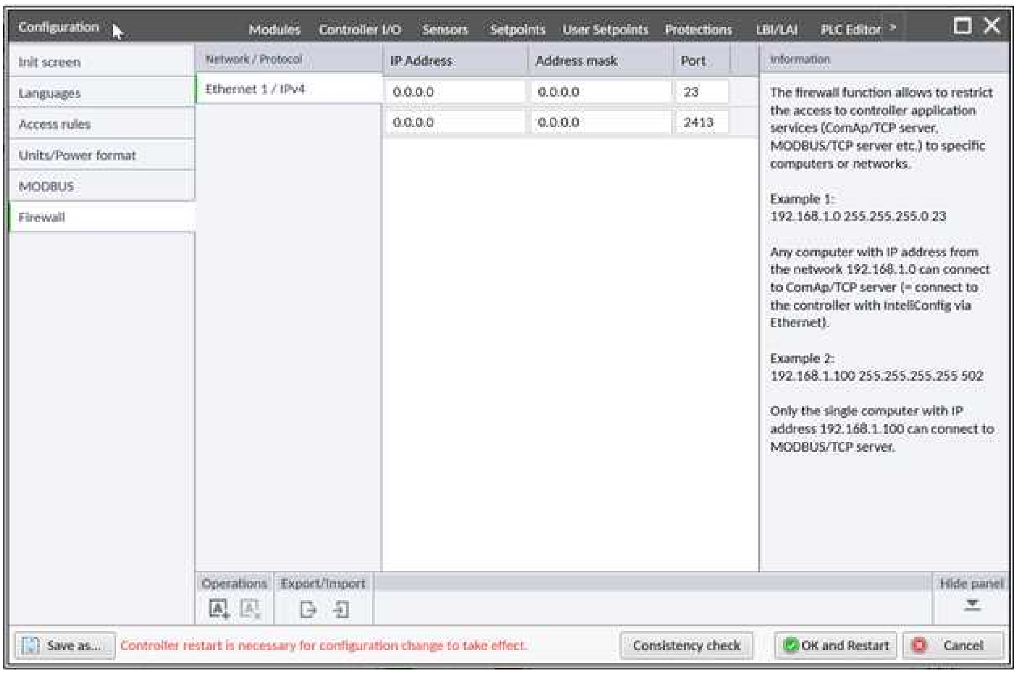
```
AA2B2LOaZ4guDwAwZLiF2/9iChxec2a2BO26NAZNmoRYCuJhoLdsDDMknGve3/
PB3E9TZFD5oniUWjcQo5LRG5pkWLAg2qaTfB7ygM7jygjqzkK0qfzOKzxucsM73KekHQpyG3B382XVvG//ZTdn2C+nA5+7BoQ5cpSrE7sqxQs
+2L22KKDH7s7QEyyuegrf+szb9RMK2BQ4u6hUeFe/1La1LGqetzRIuLZwlU4SNs526E/BJVemNKJBBhLb/
HHcsPmxYRI1t95U0B8cRR0X30YFAfjUDHUN59GrIZFsW0XpKilMQoZGL3HY9Olv1VgbeYoq9YeA2vg+DDLLBIEHBAE=
```

Image 3.8 Password Reset window in InteliConfig

3.3 Adjusting firewall

The function (aim) of the Firewall is explained above in the chapter **Firewall (page 10)**.

- Firewall rules are defined in configuration, tab "Others" → "Firewall".
- Firewall is enabled or disabled by setpoint "IP firewall".
- Firewall is individual for each IP protocol-based interface.



Network / Protocol	IP Address	Address mask	Port
Ethernet 1 / IPv4	0.0.0.0	0.0.0.0	23
	0.0.0.0	0.0.0.0	2413

Information

The firewall function allows to restrict the access to controller application services (ComAp/TCP server, MODBUS/TCP server etc.) to specific computers or networks.

Example 1:
192.168.1.0 255.255.255.0 23

Any computer with IP address from the network 192.168.1.0 can connect to ComAp/TCP server (= connect to the controller with InteliConfig via Ethernet).

Example 2:
192.168.1.100 255.255.255.255 502

Only the single computer with IP address 192.168.1.100 can connect to MODBUS/TCP server.

Controller restart is necessary for configuration change to take effect.

Image 3.9 Firewall setup in InteliConfig

If Firewall is enabled **there must be at least one rule for each service** you want to use.

- If you do not want to restrict access to a particular service define rule 0.0.0.0/0.0.0.0 for the respective port.
- If you want to restrict access to a particular service for just specific IP address(es) or ranges define one or more rules for the respective port, which will match your needs.
- If you do not want to use a service at all do not create any rule for the respective port.

Examples of rules

Rule	Allowed IP address
0.0.0.0/0.0.0.0	any
10.10.1.0/255.255.255.0	range 10.10.1.1 to 10.10.1.255
10.10.1.100/255.255.255.255	single address 10.10.1.100

3.4 Connecting to AirGate

AirGate is mostly plug-ang-play function and does not require additional adjustments except adjusting " AirGate Key".

Procedure:

1. Connect InteliConfig (e.g. via USB) to the controller and login as an user with administrator access level.
2. Go to menu "Tools" → "Access Administration" → "Change AirGate Key"

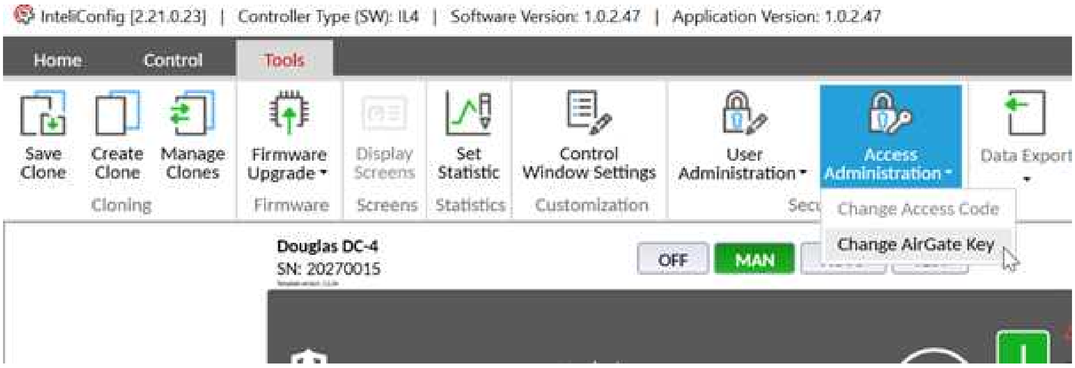


Image 3.10 Change AirGate Key menu in InteliConfig

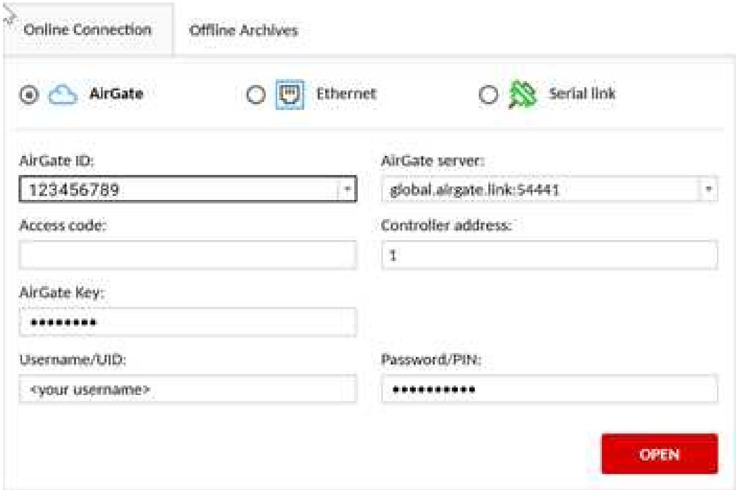
3. Think out some string consisting of digits and letters with length 6-15 chars and put it into the dialog.

Note: *AirGate Key can not be displayed. If the key is forgotten new one must be defined.*

3.4.1 Connecting to AirGate procedure

In InteliConfig select "AirGate connection" and fill-in the connection dialog as follows:

- **AirGate ID** – the 9-digit identifier of your controller. You can see it either at controller display or in InteliConfig (when you connect e.g. via USB). The **AirGate ID is static**, once the controller has been registered it **will not change anymore**.
- **AirGate server** – use "**global.airgate.link:54441**"
- **Controller address** – according to controller setpoint "Communication Settings" → "(Terminal) Controller Address"
- AirGate Key – as defined in controller, **see AirGate Key on page 10**.
- **Username and password** of the account which will be logged in when connection is opened.



Online Connection | Offline Archives

● AirGate ○ Ethernet ○ Serial link

AirGate ID: 123456789

AirGate server: global.airgate.link:54441

Access code:

Controller address: 1

AirGate Key: ••••••••

Username/UID: <your username>

Password/PIN: ••••••••••

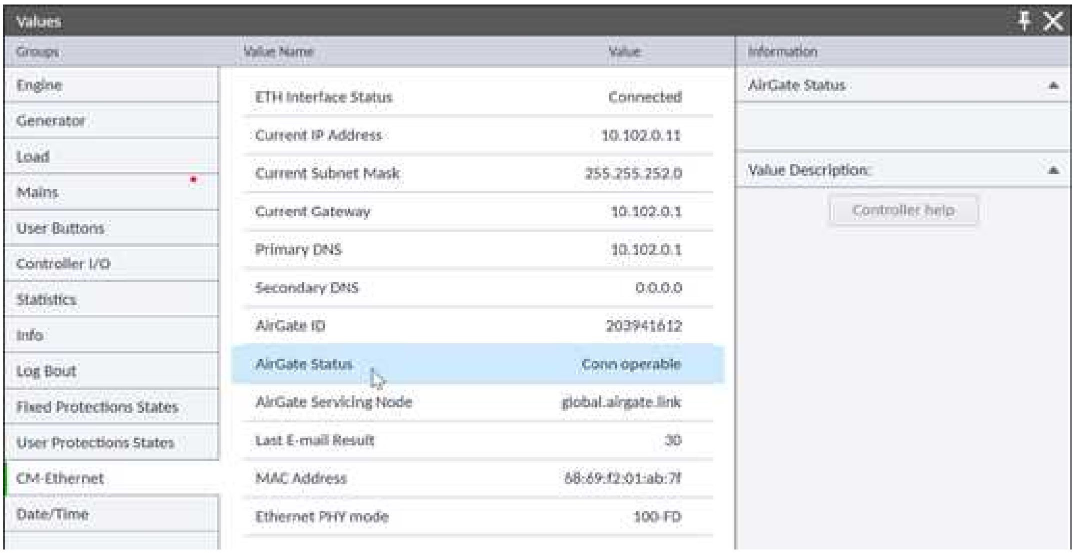
Image 3.11 AirGate connection setup in InteliConfig

Firewall requirements

> **IMPORTANT: This is related to firewall located in the network infrastructure (LAN), not to the controller firewall function.**
> **There is not any requirement for inbound traffic. All traffic related to AirGate is outbound (i.e. from controller to Internet)**
> **Outbound TCP traffic from Controller IP address to any IP address in Internet to port 54440 must be allowed.**

AirGate diagnostic information

There is a value "*AirGate status*" which is telling the user what is the correct status of the service.



Value Name	Value
ETH Interface Status	Connected
Current IP Address	10.102.0.11
Current Subnet Mask	255.255.252.0
Current Gateway	10.102.0.1
Primary DNS	10.102.0.1
Secondary DNS	0.0.0.0
AirGate ID	203941612
AirGate Status	Conn operable
AirGate Servicing Node	global.airgate.link
Last E-mail Result	30
MAC Address	68:69:f2:01:ab:7f
Ethernet PHY mode	100-FD

Image 3.12 AirGate status in the controller values

Status	Meaning
Not defined	Indicated while the controller is actually not trying to connect to AirGate. This is initial value of the status. This is also indicated while AirGate is disabled.
Wait to connect	Controller is waiting before next attempt to connect to a node is performed.
Resolving	Controller is resolving domain name of the node to which it is attempting to connect.
Connecting	Controller is attempting to establish TCP link to the node.
Creating secure channel	Controller is creating secure control (signaling) channel to the node.
Registering	Controller is registering or checking registration with AirGate.
Connected, inoperable	Controller is connected to AirGate, but AirGate will not forward connection requests to it. This is e.g. the controller if the controller is blacklisted.
Connected, operable	Controller is connected to AirGate and ready for connection with clients.
Suspended AGkeyEmpty	Controller is not connected to AirGate due to AirGate Key has not been adjusted. Adjust it according to the procedure above (**see Connecting to AirGate procedure on page 18**).

▲ **back to Getting started with the controller**