

Product Cyber Security Guide

**InteliGen 1000, InteliGen 1000 Marine,
InteliMains 1010, InteliMains 1010
Marine, InteliNeo 6000, InteliSys 2000**

Table of contents	2
1 Document information	4
2 Overview of Cyber Security features	7
3 Overview of security related settings	16
4 Auditing the security	17
5 Getting started with the controller	18

Table of contents

1 Document information	4
1.1 Clarification of Notation	4
1.2 About this guide	4
1.3 Legal notice	4
1.4 Document history	6
2 Overview of Cyber Security features	7
2.1 Principle "defense in depth"	7
2.2 Security hardening	7
2.2.1 Physical separation	8
2.2.2 Logical segmentation	9
2.2.3 Intended network environment	9
2.3 Overview of related features	9
2.3.1 Trusted and untrusted interface	9
2.4 Authentication control	10
2.4.1 User accounts	10
2.4.2 Implicit user	11
2.4.3 Protection against brute force	12
2.5 Access Control	12
2.6 Remote Communication	13
2.6.1 AirGate 2nd Generation	13
2.6.2 Controller registration	13
2.6.3 AirGate Key	14
2.6.4 Connecting to controller	14
2.7 Firewall	14
2.7.1 Firewall Rules	14
2.7.2 Examples	14
2.7.3 Services influenced by firewall	15
3 Overview of security related settings	16
4 Auditing the security	17
4.1 Controller history	17
4.2 Active messaging	17
5 Getting started with the controller	18
5.1 After unboxing	18
5.2 Define roles and access rights	19
5.3 Create user accounts	19

5.3.1 Lost password	21
5.4 Adjusting firewall	23
5.5 Connecting to AirGate	24
5.5.1 Adjusting AirGate Key	24
5.5.2 Connecting to AirGate	24
5.6 Alerting	26
5.7 Backup and restore	26
5.8 Decommissioning and repairs	26
5.9 Information about vulnerabilities and incidents	27
5.9.1 Reporting an incident	27
5.10 Security patches	27

1 Document information

1.1 Clarification of Notation	4
1.2 About this guide	4
1.3 Legal notice	4
1.4 Document history	6

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.

WARNING: 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 IntelliGen1000, IntelliGen1000 Marine, IntelliMains1010, IntelliMains1010 Marine, IntelliNeo6000, IntelliSys2000 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.

IMPORTANT: Based on controller type some features procedures may be slightly different. To reflect this the document has some parts split into two parts, one for STANDARD controllers and one for ADVANCED.

- **STANDARD:** IntelliLite4, IntelliGen4 200, IntelliMains210 G2, IntelliGen500 G2, IntelliMains 510
- **ADVANCED:** IntelliGen 1000, IntelliMains 1010, IntelliGen 1000 Marine, IntelliMains 1010 Marine, IntelliNeo 6000, IntelliSys 2000

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. 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 its 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
3	InteliGen 1000 3.6.3 InteliGen 1000 Marine 1.6.0 InteliMains 1010 3.6.3 InteliMains 1010 Marine 1.6.0 InteliNeo 6000 2.1.0 InteliSys 2000 1.9.0	27.8.2025	Adéla Procházková
2	InteliGen 1000 3.3.1 InteliGen 1000 Marine 1.3.0 InteliMains 1010 3.3.1 InteliMains 1010 Marine 1.3.0 InteliNeo 6000 2.0.0 InteliSys 2000 1.6.0	14.11.2024	Adéla Procházková
1	InteliGen 1000 3.0.2 InteliGen 1000 Marine 1.2.2 InteliMains 1010 3.0.2 InteliMains 1010 Marine 1.2.0 InteliNeo 6000 1.4.0	20.2.2024	Adéla Procházková

[🔍 back to Document information](#)

2 Overview of Cyber Security features

2.1 Principle "defense in depth"	7
2.2 Security hardening	7
2.3 Overview of related features	9
2.4 Authentication control	10
2.5 Access Control	12
2.6 Remote Communication	13
2.7 Firewall	14

🔍 back to Table of contents

All devices mentioned in this document have been developed and are maintained with respect to international cybernetic security standard ISA(EN)62443-4-2, category "Embedded devices".

Minimal target security level (SL) in applicable component requirements (CR) is SL2.

IMPORTANT: Some functions and features are disabled by default. To conform with the above standard and security level these functions need to be enabled and adjusted/configured for the specific environment and application.

2.1 Principle "defense in depth"

"Defense in depth" principle is one of key principles in cybernetic security which prevents the attacker from taking over immediate and complete control of protected system when a single layer of protection is broken. It requires applying following rules:

- Creating multiple layers of protection
- Applying secure design principles
- Reducing possible attack surface

Devices mentioned in this document have been designed to allow the user or system integrator applying the principles above and thus getting the defense in depth principle into the application. However, this requires keeping several important rules when designing the application and it's structure and while operating it. This is called "security hardening".

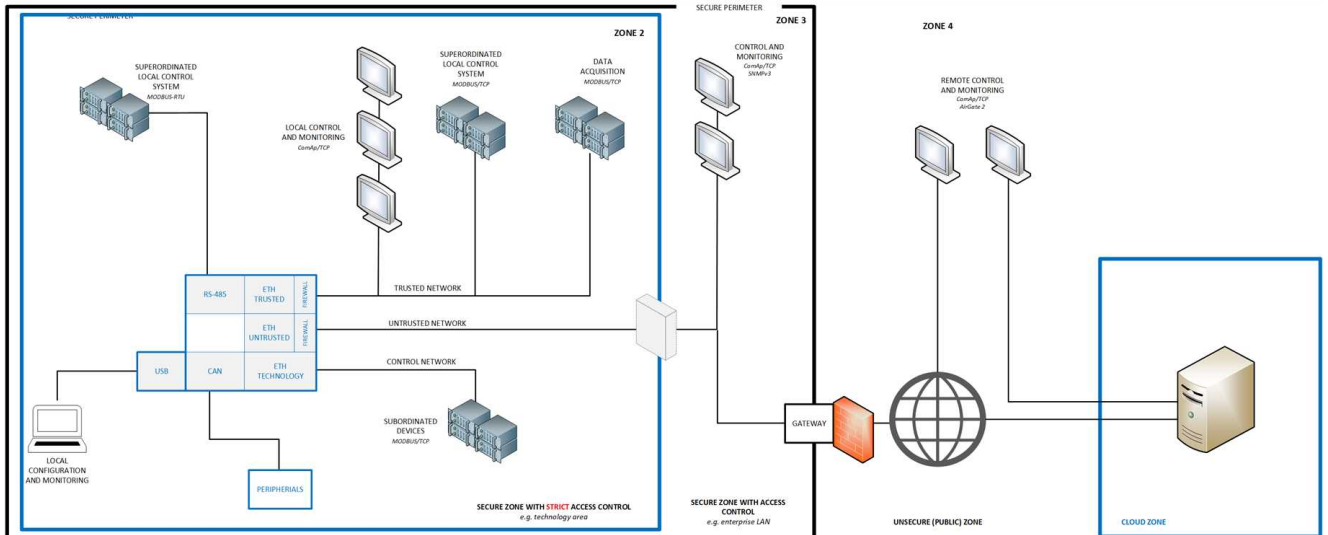
2.2 Security hardening

In principle, security hardening is a set of rules that should be used, above all, to reduce the attack surface .

1. All services using serial protocols (where authentication and encryption is not supported by nature) should be operated only inside a physically protected perimeter with strict physical access control in place.
2. Services that are based on IP protocol and where authentication and encryption is not used/supported should be operated inside protected perimeter as defined in previous point.
3. Built-in firewall function should be used to reduce attack surface by limiting the access to device services only for permitted stations.
4. Services operated via ethernet should be **preferably physically separated** according to criticality and level of protection. If physical separation is not possible then **logical segmentation** with firewall protection should be applied.

5. Services that are not used should be disabled.
6. Least privilege principle should be applied when access rights are defined for users as well as other components.
7. Passwords shall be defined with complexity adequate to the particular use case. "Simply-to-guess" passwords shall be avoided.

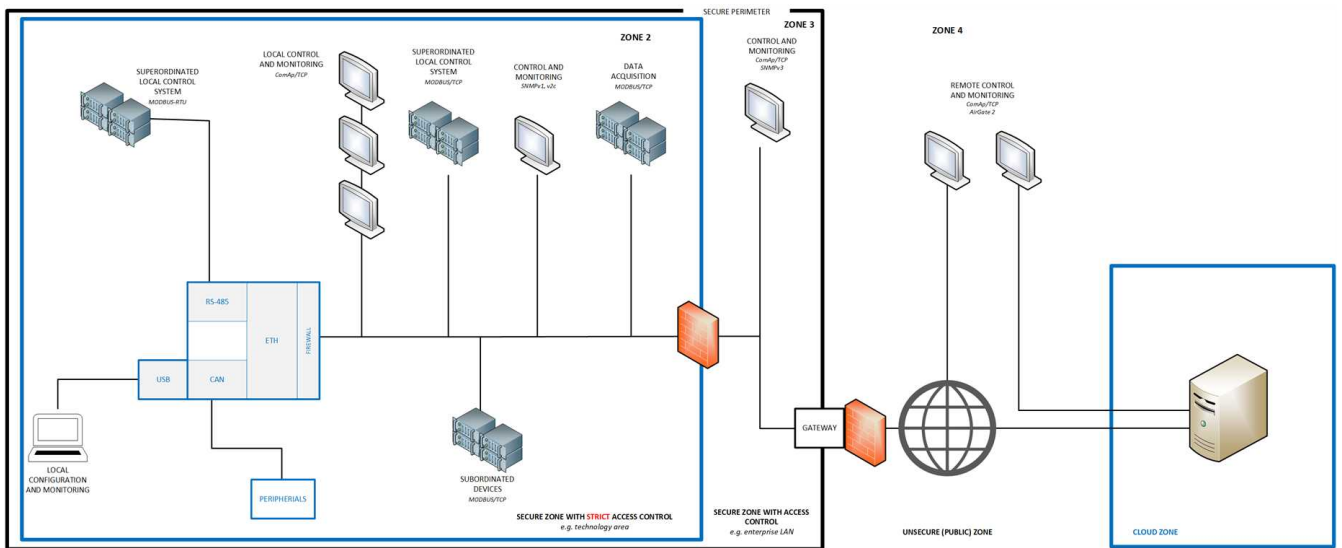
2.2.1 Physical separation



Requirements

- Keep technological network (CONTROL), local monitoring network (TRUSTED) and remote monitoring network (UNTRUSTED) fully separated, avoid any physical connection between them (neither wired nor wireless).
- **Strictly keep CONTROL and TRUSTED networks inside zone 2.**
- Apply controller built-in firewall at TRUSTED network to manage devices that can connect to the controller.
- Optional: for the UNTRUSTED network create a separate network segment at the border between zone 2 and 3 and use firewall at the bordering router to manage the access to the controller.
 - If no direct access to the controller via ComAp/TCP from zones 3 or 4 (i.e. only AirGate is used) then disable inbound traffic completely, otherwise create proper individual inbound rules as required.
 - Apply traffic monitoring and DoS protection.

2.2.2 Logical segmentation



Requirements

- Create a separate network segment at the border between zone 2 and 3 and use firewall at the bordering router.
- Keep all traffic related to technological communication and local monitoring inside zone 2, i.e. behind the firewall.
- If no direct access to the controller via ComAp/TCP from zones 3 or 4 (i.e. only AirGate is used) then disable inbound traffic completely, otherwise create proper individual inbound rules as required.
- Apply traffic monitoring and DoS protection at the bordering router.

2.2.3 Intended network environment

IMPORTANT: The device does not provide any kind of protection against network-level attacks. If there is a risk of network-level attacks the network shall be equipped with protection mechanisms to detect and/or prevent such attacks.

Example:

- The device will accept any request to open a TCP socket for an enabled TCP-based protocol. It will not detect potential malicious behavior, where an attacker would try to perform DoS attack by repeated opening dummy sockets of a particular TCP-based service. If there is a risk of such kind of attack an external dedicated protection must be installed in the network to detect and/or block it.
- The device does not perform any detection of possible ARP spoofing attack. If there is a risk of such kind of attack an external protection must be installed in the network to monitor the ARP traffic and detect discrepancies that may be signs of an attack.

2.3 Overview of related features

2.3.1 Trusted and untrusted interface

Devices which communicate with the controller via ComAp proprietary terminal protocol (i.e. HMI devices and configuration, diagnostic and monitoring tools) can connect via interfaces of two different categories:

- **Trusted interfaces** are the ones that must be connected to isolated networks, inside protected areas with managed physical access. That means it is possible to apply **less strict cybersecurity rules** for those interfaces. Trusted interfaces are:
 - Built-in display
 - USB
 - RS232/RS485
 - "Local" ethernet, *which is intended especially for local external display connection*
- **Untrusted interfaces** are the ones that may be connected to generic networks with internet access. This is why **strict cybersecurity rules** must apply for those interfaces. Untrusted interfaces are:
 - "General purpose" ethernet, *which is typically used for Internet connection*
 - Cellular modules

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

2.4 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.

2.4.1 User accounts

There must be at least one account with administrator level defined in the controller. Administrator can then define other user accounts. There is capacity for 30 user accounts in controllers described in this document.

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
role membership	mandatory	n/a	n/a	8bit long bitmask representing user membership in roles (see Access Control on page 12)

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 **Overview of related features (page 9)**)

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 IntelliConfig via some trusted interface (e.g. USB) and sent to technical support or put into ComAp password reset service at www.comap-control.com.
2. Action code is then returned to the adjusted backup e-mail address.
3. Action code must be then written into the controller using IntelliConfig via some trusted interface (e.g. USB). After that user accounts are reset to factory default state.

2.4.2 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 based on **ComAp protocol** 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
- Is fixedly member of role #1 (unless **Production mode (page 12)** is active)
- In Trusted interfaces (**see Overview of related features on page 9**) 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 is fixedly member of administrator role 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.

2.4.3 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.

2.5 Access Control

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

The user, who is logged-in, must be member of at least one role which matches at least one role required for the particular operation with the particular object.

- Each user must be member of at least one role
- Role #8 is administrator role
- Roles #1-7 are freely configurable roles (info) Role #1 is assigned to implicit user.

Table of required membership in roles

Operation	Required access level
read object	any role
write application object	role #1-#8, configurable
invoke application command	role #1-#8, configurable
read configuration	any role
write configuration	role #8 (administrators)
write firmware	role #8 (administrators)
manage user accounts	role #8 (administrators)

2.6 Remote Communication

2.6.1 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.
- 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").

2.6.2 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**.

IMPORTANT: If a controller has multiple interfaces connected to Internet (e.g. cellular and ethernet) and AirGate is active at both, the controller will register independently via each interface and thus will have two different AirGate ID, for each interface one.

2.6.3 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.

2.6.4 Connecting to controller

When connecting to the controller via AirGate from e.g. IntelliConfig 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 *Overview of related features (page 9)* it is also required that a user will login into the controller immediately after connection has been created.

2.7 Firewall

Built-in "firewall" function allows to restrict computers which can connect to the communication services in the controller based on computer IP address and port. 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!

2.7.1 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

2.7.2 Examples

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

Packet source IP address	Packet destination port	Evaluation	Rule fulfilled
192.168.1.100	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
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

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.

2.7.3 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

[🔍 back to Overview of Cyber Security features](#)

3 Overview of security related settings

Setpoint	Description	Recommended setting
AirGate Connection	Enables remote Internet connection via AirGate2 service using ComAp/TCP protocol	Disabled if not required
ComAp Client Inactivity Timeout	Timeout for closing an idle connection of ComAp/TCP protocol	To prevent blocking unused sockets adjust this setpoint to lowest possible value acceptable for the particular connected client (respect the period of communication used by that client).
Direct Connection	Enables the ComAp/TCP server at the respective interface	Disabled if not required
IP Firewall	Enables the firewall function (explained above in the chapter Firewall (page 14))	Firewall is strongly recommended as additional measure to limit access to the controller to only authorized devices if unsecured protocols like MODBUS/TCP or SNMP v1/v2 are used from outside the secured perimeter (trusted zone).
Messages	Enable sending alerts about various events (including security-related events) to specified targets via selected protocols. It can be SMS, e-mail or SNMP trap.	Enabled Channels and target addresses must be properly configured too. See controller global guide for details about Active Messages.
Modbus Client Inactivity Timeout	Timeout for closing an idle connection of ModBus/TCP protocol	To prevent blocking unused sockets adjust this setpoint to lowest possible value acceptable for the particular connected client (respect the period of communication used by that client).
Modbus Server	Enables the MODBUS/TCP server at the respective interface	Disabled if not required
NTP Clock Synchronization	Enables automatic adjustment of controller clock using NTP protocol	Disabled, unless local NTP server inside secure infrastructure is used.
SNMP Agent	Enables the SNMP Agent at the respective interface	Disabled if not required
User Logging Record	If enabled each user login is recorded in controller history, including user index and interface.	Enabled

4 Auditing the security

4.1 Controller history

Controller history is an event log with timestamps working on circular buffer principle, so newest record overwrite the oldest one. It contains operational events as well as security-related events such as:

- user login: user index and interface are recorded
- firmware update
- configuration update
- system restart
- change of any setpoint: object number, new value and user index are recorded
- brute-force protection activation

In history records the users are represented with their indexes. Users in administrator role can link the index to a username in IntelliConfig "User Administration" window.

IMPORTANT: To prevent loss of information, it is essential to read the history periodically with reasonable period.

4.2 Active messaging

Active messaging allows specified persons to be informed about events happened in the controller. It shall be enabled for the purpose of informing responsible people about the situation that the controller is under brute-force attack to break user credentials (brute-force protection activated).

5 Getting started with the controller

5.1 After unboxing

When the controller is unboxed user accounts are in **Factory default state** (page 11) and the respective warning is displayed.

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

It is necessary to login with default administrator account (see **Factory default state on page 11**) to perform some operations like changing the configuration, updating firmware etc.

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.

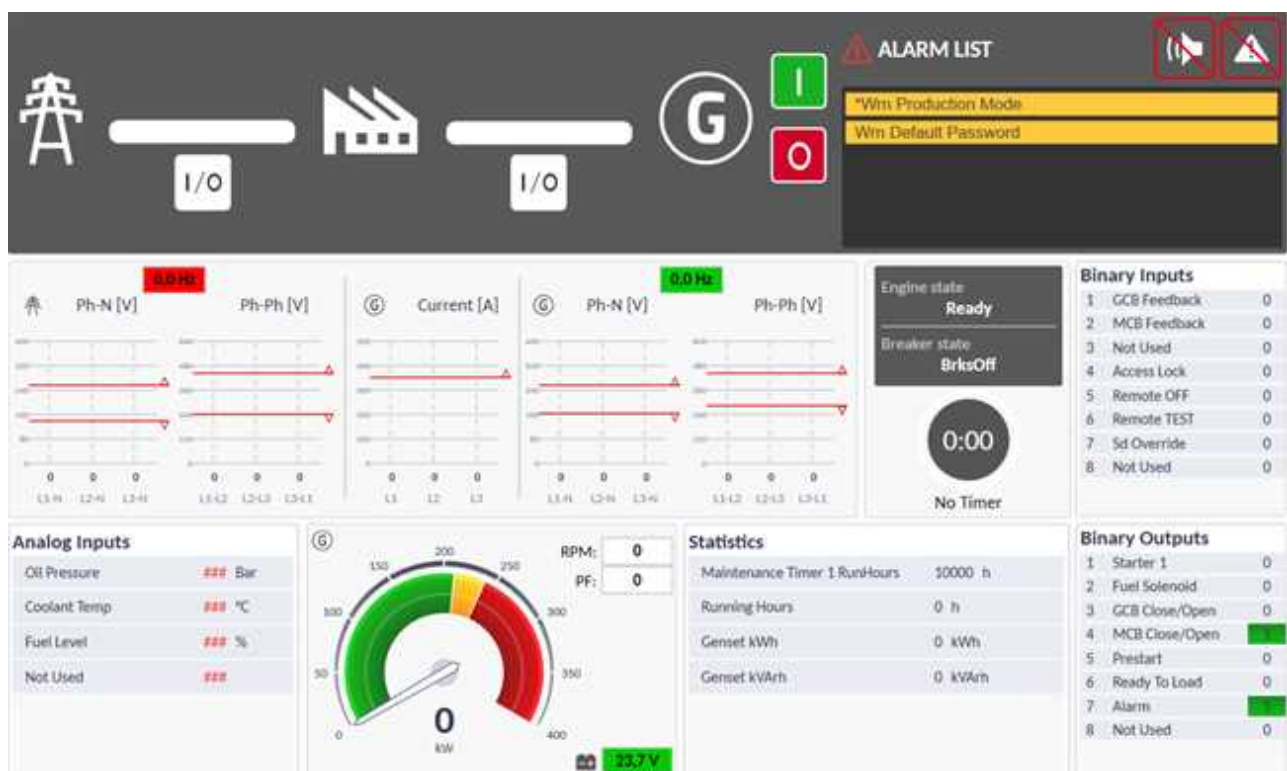
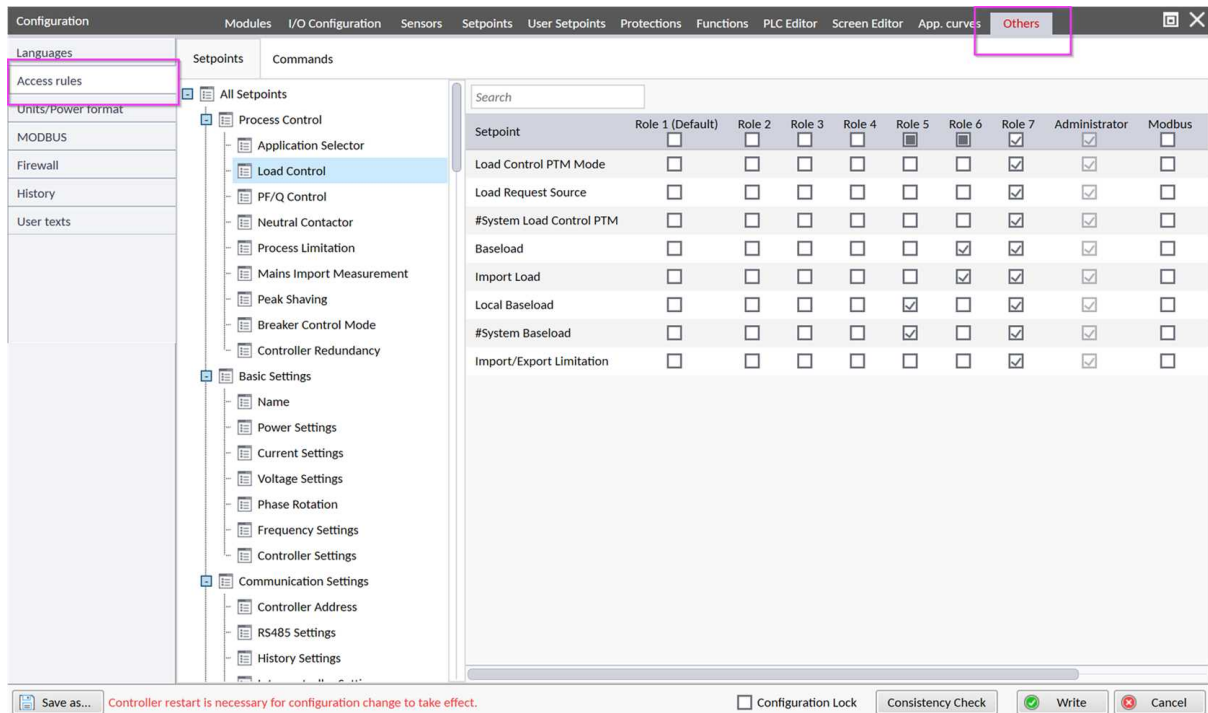


Image 5.1 Production Mode and Default Password alarms in IntelliConfig

5.2 Define roles and access rights

To define configurable access rights go to "Controller configuration" -> "Others" -> "Access rules".

Note: This is related only to write access. Read access is automatically granted to all roles.



1. Disable access for all roles to all setpoints and commands.
2. Define roles that will match the real situation how the controller is operated and maintained and assign them numbers 1 - 7.
3. For each role select setpoints and commands this particular role needs to adjust and/or invoke and give the access accordingly. (info) Access to a setpoint or command may be given to multiple roles.
4. **Do not give access to setpoints which a particular role does not need to adjust.**

5.3 Create user accounts

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

Procedure:

1. While Intelliconfig 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.

Note: If you login as administrator you must use username/password. Managing users is not allowed when administrator is logged in with UserID/PIN.

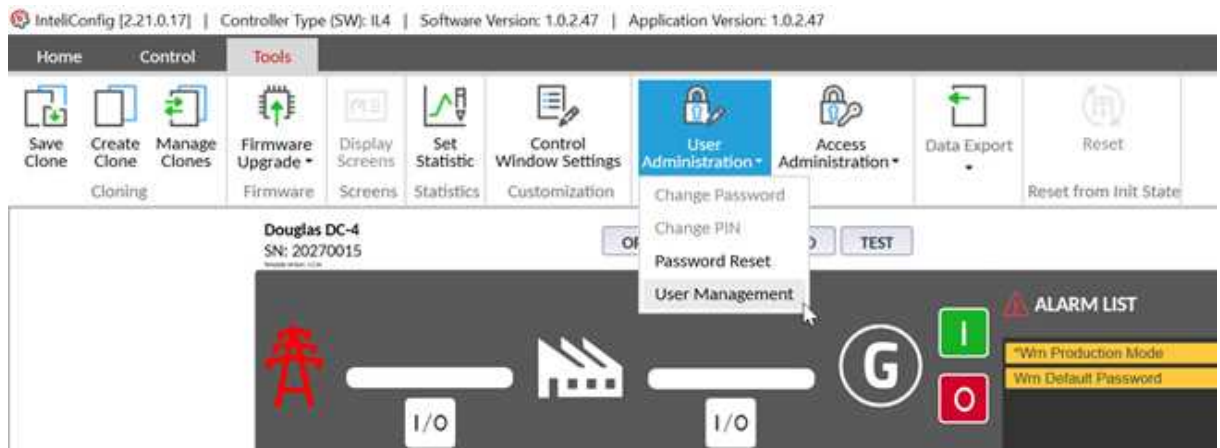


Image 5.2 User management menu in IntelConfig

2. Use buttons "Add (+)", "Remove (-)", "Edit" to create accounts and assign it into roles. See the chapter **Account attributes (page 10)** about details related to attributes of the accounts.

Note: One user account can be assigned to multiple roles.

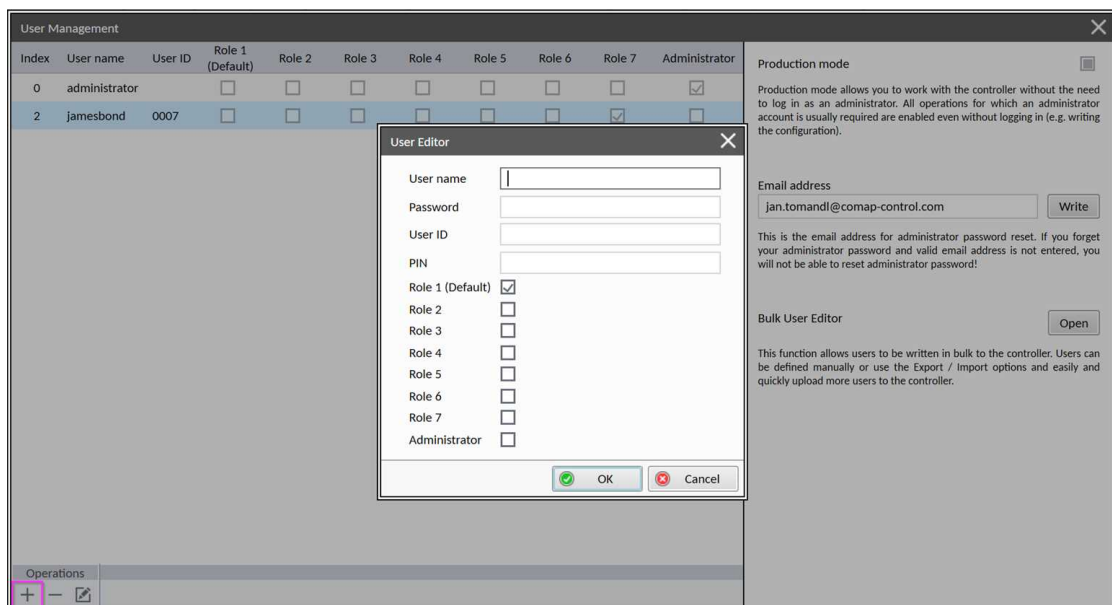


Image 5.3 Account attributes setup in IntelConfig

3. Keep "least privilege principle":
 - Create individual accounts as much as your application and controller account capacity allows it.
 - If using shared accounts use it for persons with similar or same roles (e.g. one account for engine maintenance technicians and other for electrical technicians).
 - Avoid sharing account among persons with different roles.
 - **Avoid providing administrator access for accounts which do not need it.**

Note: There must be at least one user in administrator role.

4. In the "User Management" window **adjust the backup e-mail address**.

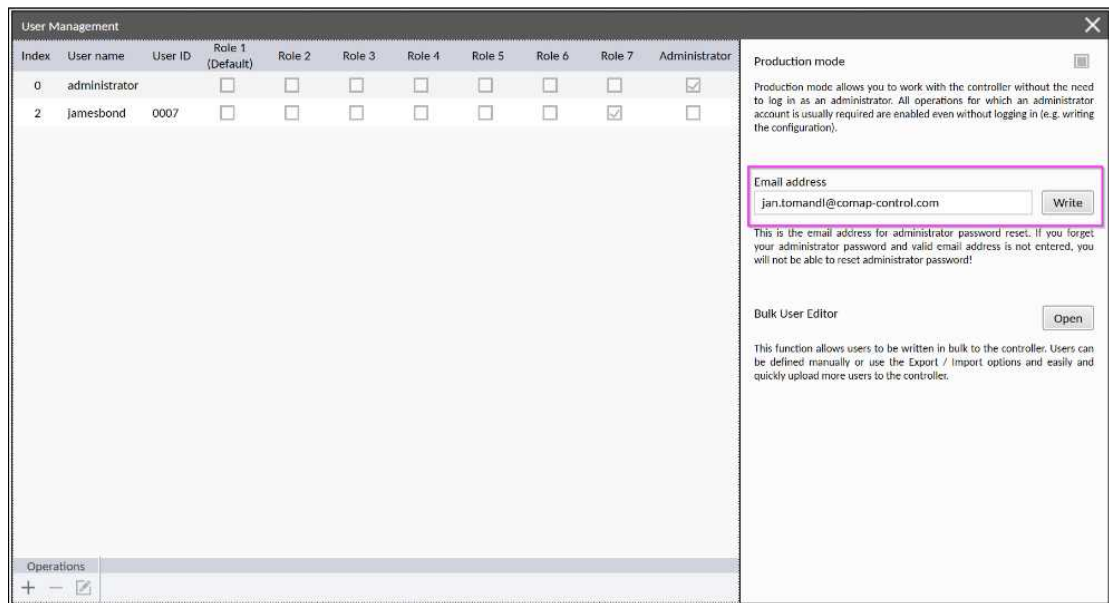


Image 5.4 Setup of email address for administrator password reset in IntelConfig

IMPORTANT: 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.

5. Login with some administrator account created in step 2.
6. Go again to the "User Management" window and remove the default administrator account or at least change his password. The alarm "*Wm Default Password*" will disappear.

5.3.1 Lost password

When the password for administrator account is lost it is possible to reset the controller into **Factory default state** (page 11), i.e. delete all user accounts and create the default administrator account.

Procedure:

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



Image 5.5 Password Reset option in IntelConfig

2. Press "Get reset code"

3. Copy the "PRRC code" into clipboard
4. Go to web browser and navigate to [ComAp – InteliBot \(comap-control.com\)](http://ComAp – InteliBot (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.

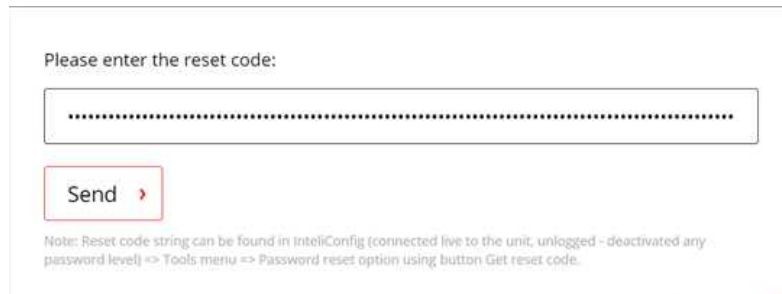


Image 5.6 Entering "PRRC code" in InteliBot

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

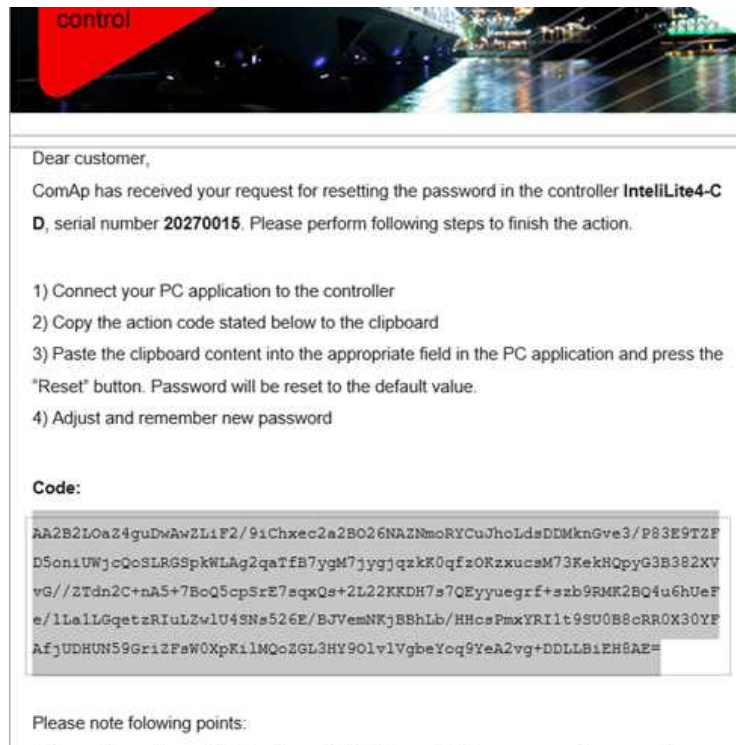


Image 5.7 Sample of email with "PRAC code"

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.

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

5.5 Connecting to AirGate

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

Note: If a controller has multiple interfaces connected to Internet (e.g. cellular and ethernet) and AirGate is active at both, the controller will register independently via each interface and thus will have two different AirGate ID, for each interface one.

5.5.1 Adjusting AirGate Key

1. Connect IntelliConfig (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"

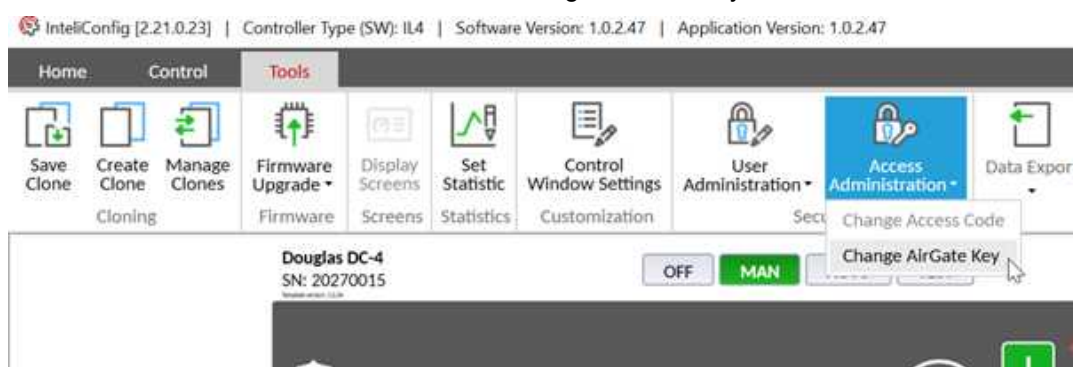


Image 5.10 Change AirGate Key menu in IntelliConfig

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.

5.5.2 Connecting to AirGate

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

1. **AirGate ID** – the 9-digit identifier of your controller. You can see it either at controller display or in IntelliConfig (when you connect e.g. via USB). The **AirGate ID is static**, once the controller has been registered it **will not change anymore**.
2. **AirGate server** – use "global.airgate.link:54441"

3. **Controller address** – according to controller setpoint "Communication Settings" → "(Terminal) Controller Address"
4. AirGate Key – as defined in controller, **see AirGate Key on page 14.**
5. **Username and password** of the account which will be logged in when connection is opened.

Image 5.11 AirGate connection setup in Intelliconfig

Firewall requirements

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.

Groups	Value Name	Value	Information
Engine	ETH Interface Status	Connected	AirGate Status
Generator	Current IP Address	10.102.0.11	
Load	Current Subnet Mask	255.255.252.0	Value Description:
Mains	Current Gateway	10.102.0.1	Controller help
User Buttons	Primary DNS	10.102.0.1	
Controller I/O	Secondary DNS	0.0.0.0	
Statistics	AirGate ID	203941612	
Info	AirGate Status	Conn operable	
Log Bout	AirGate Servicing Node	global.airgate.link	
Fixed Protections States	Last E-mail Result	30	
User Protections States	MAC Address	68-69-f2-01-ab-7f	
CM-Ethernet	Ethernet PHY mode	100-FD	
Date/Time			

Image 5.12 AirGate status in the controller values

Status	Meaning
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.
Connecting	Controller is attempting to establish TCP link to the node.
Creating secure channel	Controller is creating secure control (signaling) channel to the node.
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.
Registering	Controller is registering or checking registration with AirGate.
Resolving	Controller is resolving domain name of the node to which it is attempting to connect.
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 on page 24).
Wait to connect	Controller is waiting before next attempt to connect to a node is performed.

5.6 Alerting

It is recommended to use active alarm messaging, i.e. active e-mails and/or SMS and/or SNMP traps to inform responsible persons about incidents like activation of brute-force attack protection. See the respective controller User guide for details about using active e-mails, SMS and TRAPs.

5.7 Backup and restore

It is recommended to store the final installed controller firmware and configuration to secure storage so that it can be later on used for system restoration after disruption or failure.

Controller programming, configuration download and upload to the controller is done using IntelliConfig PC tool as described in the controller Global Guide.

5.8 Decommissioning and repairs

When the product shall be decommissioned or sent for a repair it is recommended to perform following steps:

- Replace the configuration with the default one
- Restore default administrator account
- Remove all other user accounts
- Erase backup e-mail address

5.9 Information about vulnerabilities and incidents

- Information about known vulnerabilities are available in a table at dedicated cybersecurity section of ComAp web pages (www.comap-control.com/services/cybersecurity). Each incident has assigned a unique identifier for simple referencing and also severity score based on Common Vulnerability Scoring System 3.1 (CVSS). Detailed information about the vulnerability, related product and recommended mitigation is available for download there.
- Information about patches are also included in New Features List documents released with each firmware update for each product.

5.9.1 Reporting an incident

If a (suspected) vulnerability is detected or an incident occurred ComAp strongly encourages customers and users to report such a security issue to ComAp (go to www.comap-control.com/support).

Please provide as much information as possible when reporting a security issue:

- Device information (order code or type, serial number)
- Firmware information (preferably "identification string")
- Archive containing collected logs if possible
- Description of operation environment (e.g. diagram of communication interfaces with configuration information)
- Description of the event
- Any other relevant information

5.10 Security patches

Security patches are distributed in a form of regular or extraordinary firmware updates.

- Details about update contents including information about contained security patches are published in "new features list" documents released for each update
- Firmware updates which contain important security patches related to known vulnerabilities listed in the cybersecurity section at the ComAp web pages are also directly linked from that list
- Procedure of installation of updates depend on controller (device) type and is described in the user documentation of that device

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