RIELLO CONNECT SECURITY

Technologies used by the Riello Connect solution to keep your data safe.

RIELLO ELETTRONICA

riello ups

INDEX

Security together with ease-of-use are the cornerstones of the **Riello Connect** solution.

This document explains the security measures implemented within the **Riello Connect solution in order to keep your data safe.**

1

What is Riello Connect?

Riello Connect is a cloud-based remote management solution that provides service organizations and end-users with the ability to remotely monitor and control Riello UPS systems.

How Riello Connect works:

A Riello Connect communication gateway connects to the equipment in the field using a serial, Ethernet or I/O connection. The gateway sends information via the Internet or the cellular network (GSM/GPRS/3G/4G) to the cloud-based Riello Connect data centre.

By logging on to Riello Connect at www.riello-ups.com, users can see all parameters of their UPS system via a computer, tablet or smart phone.
With Riello Connect, it is also possible to set up a secure tunnel for remote programming or debugging with the user's regular configuration software. This functionality is called "Remote Access."

How your data is kept safe on the Riello Connect server

The data on Riello Connect is kept safe through a state-of-the art server infrastructure with backup power, fire protection and on-duty staff 24/7. Riello Connect is a redundant system on several distributed servers in several locations. This increases the availability for both the users and for the Riello Connect RCT gateways in the field, minimizing the risk of data loss.

Security for data transmission to/from Riello Connect

Security is so much more than just safeguarding the data on the Riello connect server. To keep the data safe when being sent to and from Riello Connect, the solution utilizes four different methods:

- **Encryption between the user's web browser and the Riello Connect cloud server**
- **Encryption between the Riello Connect RCT gateway and the Riello Connect cloud server**
- **User authentication when logging into Riello Connect (including two-step verification)**
- **Customised user permissions**

2

Encryption between the user's web browser and the cloud server (Website certificate)

A SSL/TLS 2048 bit RSA/256 bit AES encrypted connection is used to secure the communication between the user's web browser and Riello Connect. The identity of the Riello UPS website (https://www.riello-ups. com) is verified independently and has an Extended Validation SSL certificate.

When visiting websites that use SSL certificates with Extended Validation, the web browser address bar will display information about the legal identity of the owner in a distinctive green field.
Communications with the Riello Connect Cloud Server will always be protected by a session key with up to 256 bit encryption (minimum 128 bit).

3

Encryption between the remote gateway and the Riello Connect cloud server

The communication between the Riello Connect RCT remote gateway connected to the device, and the Riello Connect cloud server is encrypted by a Transport Layer Security (TLS) 128 bits key. This secures the communication to the device from where it is monitored.

Authentication between Riello Connect and the RCT gateway

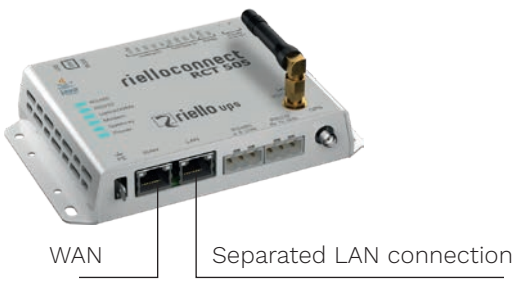
When the Riello Connect RCT gateway connects to Riello Connect, it is presented with a certificate that it needs to validate. This ensures that the gateway is really is connecting to Riello Connect (and no other server).
On the Riello Connect side, the RCT gateway is identified as a valid gateway via its unique credentials.

Security for mobile network communication

When communicating using the mobile network, the transmitted SSL/TLS encrypted data is also encapsulated by the standard GSM/3G/4G encryption.

When the Riello Connect Communication gateway connects to the mobile network, it receives an IP-address from the mobile operator which does not need to be public IP-address.
Therefore, it is impossible to browse or ping the gateway. Using a SIM card without a public IP-address for the Riello Connect gateway, will also prevent unwanted data traffic originating from search engines and bots scanning IP-addresses.

Inside the RCT



Security for Ethernet communication

The Riello Connect RCT 50x series gateways come with two Ethernet network ports — WAN and LAN. This separation makes it possible, for example, to use external firewalls on the LAN port to ensure that strict security policies can be applied.

"Firewall-friendly"

The Riello Connect RCT gateway needs to be able to communicate with the Riello Connect server in order to utilize the services. You can set up your firewall to block all inbound traffic to ensure that the site is secure, and the Riello Connect solution will still be able to operate. However, outgoing traffic is still required so the Riello Connect gateway can establish communication with Riello Connect (one outbound port needs to be open — if all outbound ports were blocked, it would mean that no communication would be allowed).

Ensuring secure communication

The Riello Connect RCT gateway should always be installed behind a firewall as the communication method used by the Riello Connect RCT gateway does not require the gateway to be exposed with public IP access.

When installed in such way, it is not possible to open a connection and establish communication from the internet to the Riello Connect RCT gateway — communication can only be made via Riello Connect.

This also applies when using a cellular connection, meaning that the Riello Connect RCT gateway should not be on a cellular subscription plan with a public IP address.

4

User authentication (including two-step verification)

Each user account on Riello Connect is protected by a password. It is the username and password that determines the access rights for the particular user. Riello Connect requires a password length of six characters but to ensure security, make sure that you:

- **use passwords that are not used on any other site**
- **follow normal best practice for password generation**

Two-step verification

The verification control is similar to what banks are using to increase their security level. It requires that the user's mobile number is registered on Riello Connect. When an authorized user wants to access the Riello Connect system, a two-step verification is used.
After the user has entered his/her user credentials on the Riello connect login page (username and password), the user will receive an SMS text message containing a one-time security code. This needs to be entered within 15 minutes to allow access to the Riello Connect system.

Enter your password to log on to Riello Connect.

You receive a text message to your mobile phone which you enter into Riello Connect.

That's it, you're signed in!

When a user logs into the Riello Connect system, the date and time is recorded in the system for a minimum of 4 weeks. This information is only stored in the system and is not available for the users.

The administrator of the account can see the last time each user accessed Riello Connect.

To ensure secure access to the Riello Connect account, all users as well as the administrator shall be configured for twostep verification, which requires each session to be verified with a security code received by SMS.

Each security code generated has 1.000.000 possible combinations. To prevent an account from being hacked, the Riello Connect system blocks a user for 10 minutes if 40 invalid codes have been entered. To prevent the intruder from blocking the user's phone, a maximum of 20 security codes can be requested before the request for new security codesfunctionality is blocked for 10 minutes.

Recovery codes (if you cannot receive the one-time security codes on your phone)

It is possible to print 10 recovery codes from the Riello Connect system. These can be used in situations in which a user's cell phone is lost, damaged and otherwise unavailable. The one-time recovery codes can be used for login instead.

5 Access rights for different users

The Riello Connect cloud server offers three user access levels, Administrator, Project Manager and User.

Administrator

On the Riello Connect account, there is only one Account Administrator. The Administrator assigns user settings and the different monitoring capabilities for each respective user.

All device monitoring configurations (templates, profiles, alarm and data logging) are created by the Administrator.

The Riello Connect Account Administrator is able to allow/ block Project Managers and Users from changing the user details such as contact details, phone numbers or alarm schedules.

The Account Administrator sets the user privileges for Project Managers and Users for example to:

- **Access a specific Riello Connect project (A Riello Connect project consists of one or several Riello Connect gateways and their connected devices).**
- **Limit read-only (view-only) privileges for access of remote data.**
- **Reception / acknowledgement of alarms.**
- **Remote Access functionality.**
- **Web services capabilities.**

Project Manager

The Project Manager has the same access rights as the Account Administrator for all systems in the specified project. The Project Manager is also able to add new Riello Connect remote gateways to the projects.

User

The user may be assigned with privileges such as access to a specific Riello Connect project or read-only (view-only) access of remote data.

6
Riello Connect Remote Access and Security

Remote Access is a Riello Connect service that opens up a secure tunnel to a UPS. This enables configuration, programming or debugging of the UPS from any location. Users utilize their regular configuration software just as if connected on site.

To establish the remote connection, the PC-based driver Riello Connect “Quick Connect” is installed on the PC. This creates a secure tunnel through Riello Connect to the Riello Connect gateway and establishes a virtual connection to the software application on the PC.

The tunnel established between the computer and the remote network can be used to create one or more channels for the actual connections to the remote devices.

From a security standpoint, the Remote Access functionality is no different from the rest of the Riello Connect solution.
The data is still SSL-protected going both to and from Riello Connect. The only difference is that the user logs on to Riello Connect with the Quick Connect software instead of going to www.riello-ups.com

Other ways of securing access to equipment

Whitelist for port forwarding

A Riello Connect administrator can select to “whitelist” certain IP-addresses. This gives users access to these addresses only, thus restricting them from accessing other IP addresses.

RPS S.p.A. - Member of the Riello Elettronica Group
Viale Europa, 7 - 37045 LEGNAGO (Verona) - Italy
T +39 0442 635811 - riello@riello-ups.com

DATRCSX0Y20LREN