SÉCURITÉ RIELLO CONNECT

Les technologies de la solution
Riello Connect protègent vos données.

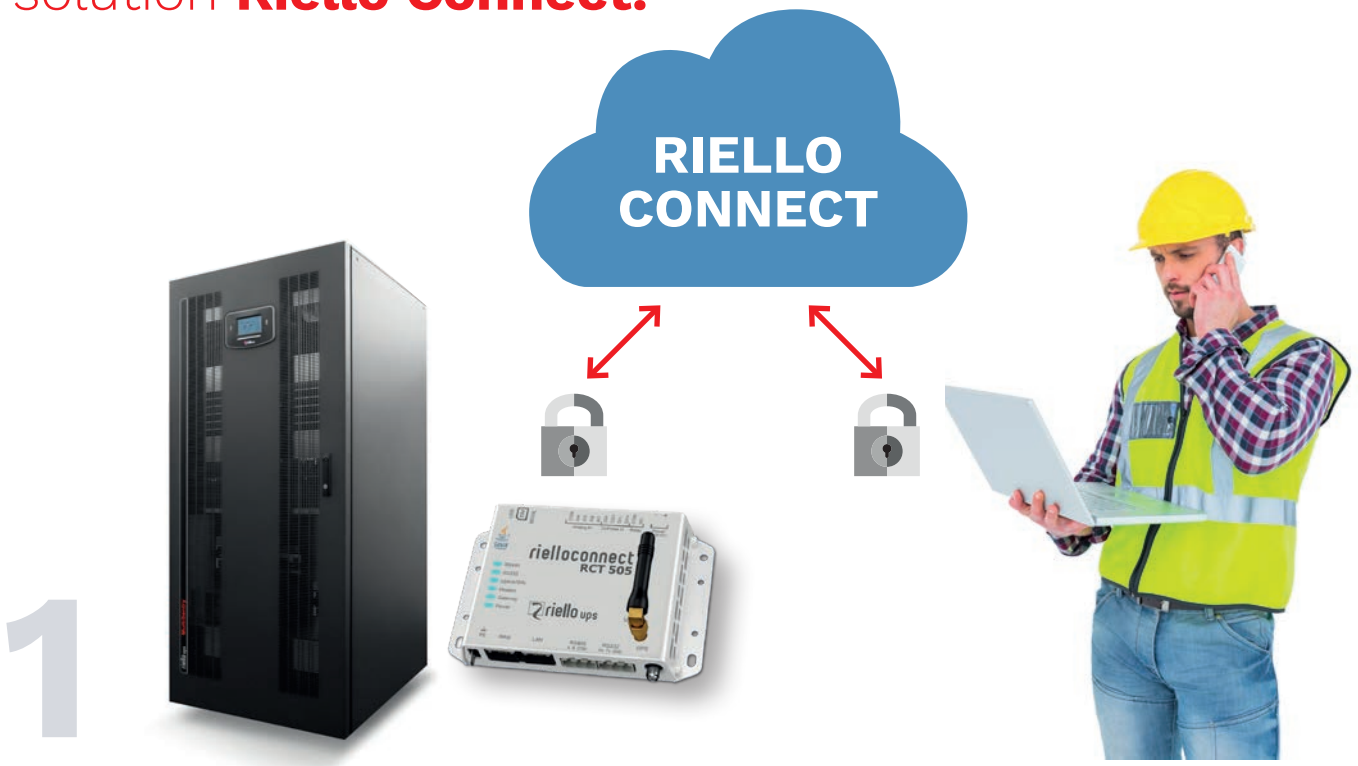
RIELLO ELETTRONICA

riello ups

SOMMAIRE

La sécurité et la convivialité sont les pierres angulaires de la solution **Riello Connect.**

Ce document décrit les mesures de sécurité mises en oeuvre dans la **solution Riello Connect afin de protéger vos données.**



1

Qu'est-ce que Riello Connect?

Riello Connect est une solution de gestion à distance, basée sur le nuage, permettant aux entreprises de services et aux utilisateurs finaux de gérer et de surveiller à distance les systèmes Riello UPS.

Comment fonctionne Riello Connect?

Une passerelle de communication Riello Connect se connecte à l'équipement sur le terrain via une connexion série, Ethernet ou entrée/sortie. La passerelle envoie les informations via Internet ou le réseau cellulaire (GSM/GPRS/3G/4G) au centre de données Riello Connect dans le nuage.

Une fois connectés à Riello Connect à partir du site www.rielloups.com, les utilisateurs peuvent afficher tous les paramètres de leur système ASI sur leur ordinateur, tablette ou téléphone intelligent.

Riello Connect permet également de configurer un tunnel sécurisé pour la programmation ou le dépannage à distance, en utilisant le logiciel de configuration standard de l'utilisateur. Cette fonctionnalité est appelée « Accès à distance ».

Comment vos données sont-elles protégées sur le serveur Riello Connect?

Les données de Riello Connect sont protégées grâce à une infrastructure de serveurs ultra moderne dotée d'une capacité de sauvegarde, un système de protection contre les incendies et un personnel de service opérationnel 24 heures sur 24 et 7 jours sur 7. Riello Connect est un système redondant sur plusieurs serveurs distribués sur plusieurs sites. Cela permet d'améliorer la disponibilité tant pour les utilisateurs que pour les passerelles RCT Riello Connect sur le terrain, minimisant ainsi le risque de perte de données.

Sécurité de la transmission de données vers et depuis Riello Connect

La sécurité ne se limite pas seulement à la protection des données sur le serveur Riello Connect. Pour protéger les données transmises vers et depuis Riello Connect, la solution utilise quatre méthodes différentes :

- **Le cryptage entre le navigateur web de l'utilisateur et le serveur Riello Connect dans le nuage**
- **Le cryptage entre la passerelle RCT Riello Connect et le serveur Riello Connect dans le nuage**
- **L'authentification utilisateur lors de la connexion à Riello Connect (notamment la vérification en deux étapes)**
- **Autorisations utilisateurs personnalisées**

2

Le cryptage entre le navigateur web de l'utilisateur et le serveur Riello Connect dans le nuage (certificat pour site web)

Une connexion chiffrée SSL/TLS RSA-2048/AES-256 bits est utilisée pour sécuriser la communication entre le navigateur web de l'utilisateur et Riello Connect. L'identité du site web Riello UPS (https://www.riello-ups.com) est vérifiée indépendamment et possède un certificat SSL à validation étendue.

Lorsque vous accédez à des sites web qui utilisent des certificats SSL à validation étendue, la barre d'adresse du navigateur web affiche des informations concernant l'identité juridique du propriétaire dans un champ distinctif de couleur verte.
Les communications avec le serveur Riello Connect seront toujours protégées par une clé de session dont le chiffrement peut aller jusqu'à 256 bits (128 bits au minimum).

3

Le cryptage entre la passerelle RCT Riello Connect et le serveur Riello Connect dans le nuage

La communication entre la passerelle distante RCT Riello Connect, connectée au terminal, et le serveur Riello Connect dans le nuage est chiffrée à l'aide d'une clé TLS (Transport Layer Security) de 128 bits. Cela permet de sécuriser la communication avec le terminal à partir duquel elle est surveillée.

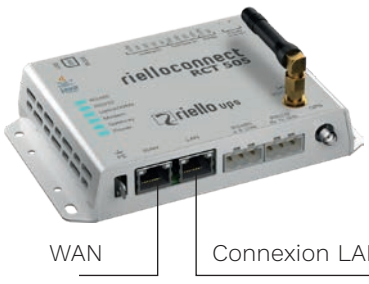
Authentification entre Riello Connect et la passerelle RCT

Lorsque la passerelle RCT Riello Connect se connecte à Riello Connect, elle doit valider le certificat qui lui est présenté. Cela permet d'assurer la connexion de la passerelle à Riello Connect (et non pas à un autre serveur). Du côté de Riello Connect, la passerelle RCT est identifiée comme passerelle valide avec les informations de connexion uniques.

Sécurité des communications sur réseau mobile

Lors des communications sur le réseau mobile, les données chiffrées SSL/TLS transmises, sont également protégées par le chiffrement GSM/3G/4G standard. Lorsque la passerelle de communication Riello Connect se connecte au réseau mobile, elle reçoit une adresse IP de l'opérateur mobile, qui ne doit pas nécessairement être une adresse IP publique. Ainsi, il est impossible de naviguer ou d'effectuer une commande ping sur la passerelle. L'utilisation d'une carte SIM sans adresse IP publique pour la passerelle Riello Connect, permet également de bloquer tout trafic de données indésirable en provenance des moteurs de recherche ainsi que le balayage des adresses IP.

Dans l'unité RCT



Sécurité des communications Ethernet

Les passerelles RCT Riello Connect série 50x sont dotées de deux ports Ethernet, un WAN et un LAN. Cette distinction permet, par exemple, d'utiliser des pare-feu externes sur le port LAN afin d'assurer l'application de stratégies de sécurité strictes.

Compatibilité avec les pare-feu

La passerelle RCT Riello Connect doit être capable de communiquer avec le serveur Riello Connect pour utiliser les services. Vous pouvez configurer votre pare-feu de façon à bloquer le trafic entrant afin d'assurer la sécurité du site, sans empêcher le fonctionnement de la solution Riello Connect.
Cependant, pour que la passerelle Riello Connect puisse communiquer avec Riello Connect, le trafic sortant demeure nécessaire (un port sortant doit donc être ouvert ; si tous les ports sortants sont bloqués, la communication ne peut avoir lieu).

Protection des communications

La passerelle RCT Riello Connect doit toujours être installée derrière le pare-feu puisque sa méthode de communication ne requiert pas d'être exposée avec un accès IP public.

Ce type d'installation empêche d'ouvrir une connexion et d'établir une communication internet avec la passerelle RCT Riello Connect. La communication peut uniquement être établie via Riello Connect.

Cela s'applique également dans le cas d'une connexion cellulaire, où la passerelle RCT Riello Connect ne doit pas faire l'objet d'un plan d'abonnement cellulaire avec une adresse IP publique.

4 Authentification utilisateur (notamment la vérification en deux étapes)

Chaque compte utilisateur Riello Connect est protégé par un mot de passe. Ce sont le nom d'utilisateur et le mot de passe qui déterminent les droits d'accès d'un utilisateur particulier.
Riello Connect requiert un mot de passe de six caractères, mais pour assurer la sécurité, vous devez :

- **choisir un mot de passe non utilisé pour un autre site**
- **appliquer les meilleures pratiques généralement utilisées pour générer les mots de passe**

Vérification en deux étapesi

Le contrôle de vérification est similaire aux mesures de sécurité utilisées par les banques pour améliorer leur niveau de protection. Il requiert l'enregistrement du numéro de mobile de l'utilisateur sur Riello Connect. Lorsqu'un utilisateur autorisé souhaite accéder au système Riello Connect, une vérification en deux étapes est utilisée.
Après avoir saisi ses informations de connexion sur la page de connexion de Riello Connect (nom d'utilisateur et mot depasse), l'utilisateur reçoit un message SMS contenant un code de sécurité à usage unique. Ce code doit être saisi dans un délai de 15 minutes pour autoriser l'accès au système Riello Connect.

Saisissez votre mot de passe pour vous connecter à Riello Connect

Vous recevez un message texte sur votre téléphone mobile que vous saisissez dans Riello Connect.

Et voilà, vous êtes connecté !

Lorsqu'un utilisateur se connecte au système Riello Connect, la date et l'heure sont enregistrées dans le système pendant quatre semaines minimum. Ces informations sont uniquement enregistrées dans le système et ne sont pas disponibles aux utilisateurs.

L'administrateur du compte peut savoir à quand remonte le dernier accès de chaque utilisateur à Riello Connect.

Pour protéger l'accès au compte Riello Connect, il est possible de configurer tous les utilisateurs, ainsi que l'administrateur, pour la vérification en deux étapes, qui consiste à vérifier chaque session à l'aide d'un code de sécurité envoyé par SMS.

Pour chaque code de sécurité généré, il existe un million de combinaisons possibles. Pour empêcher le piratage d'un compte, le système Riello Connect bloque un utilisateur pendant 10 minutes si 40 codes incorrects ont été saisis. Pour empêcher l'intrus de bloquer le téléphone d'un utilisateur, un maximum de 20 codes de sécurité peuvent être demandés avant que la fonctionnalité de demande d'un nouveau code de sécurité soit bloquée pendant 10 minutes.

Codes de récupération (dans le cas où vous ne pouvez pas recevoir un code de sécurité à usage unique sur votre téléphone)

Il est possible d'imprimer 10 codes de récupération à partir du système Riello Connect. Ces codes peuvent être utilisés en cas de perte, d'endommagement ou d'indisponibilité du téléphone d'un utilisateur.
Les codes de récupération à usage unique peuvent être utilisés pour se connecter.

5 Droits d'accès des différents utilisateurs

Le serveur Riello Connect dans le nuage offre trois niveaux d'accès utilisateur, à savoir Administrateur, Responsable de projet et Utilisateur.

Administrateur

Pour le compte Riello Connect, il n'existe qu'un seul Administrateur de compte. L'administrateur assigne les paramètres utilisateur et les différentes capacités de surveillance à chaque utilisateur respectif.

Toutes les configurations de surveillance de terminal (modèles, profils, alarmes et journaux de données) sont créées par l'administrateur.

L'administrateur de compte Riello Connect peut autoriser ou empêcher les Responsables de projet et les Utilisateurs de changer les détails des utilisateurs tels que les coordonnées de contact, les numéros de téléphone ou les programmations d'alarmes.

L'administrateur de compte définit les privilèges utilisateur des Responsables de projet et des utilisateurs, par exemple pour :

- **Accéder à un projet Riello Connect spécifique (un projet Riello Connect est constitué d'une ou de plusieurs passerelles Riello Connect et des terminaux associés).**
- **Limiter les privilèges d'accès aux données en lecture seule.**
- **Recevoir/acquitter des alarmes.**
- **Fonctionnalité d'accès à distance.**
- **Capacités relatives aux services web.**

Responsable de projet

Le responsable de projet possède les mêmes droits d'accès que l'administrateur de compte pour tous les systèmes du projet spécifié. Le responsable de projet peut également ajouter de nouvelles passerelles distantes Riello Connect aux projets.

Utilisateur

Des privilèges d'accès peuvent être assignés à l'utilisateur tels que l'accès à un projet Riello Connect spécifique ou encore l'accès en lecture seule à des données distantes.

6

Accès à distance au système Riello Connect et sécurité

L'accès à distance est un service Riello Connect qui ouvre un tunnel sécurisé pour un système ASI. Cela permet la configuration, la programmation ou le dépannage du système ASI depuis n'importe quel site. Les utilisateurs utilisent leur logiciel de configuration habituel comme s'ils étaient connectés au site.

Pour établir une connexion à distance, le pilote « Quick Connect » du système Riello Connect est installé sur le PC. Cela permet de créer un tunnel sécurisé, via Riello Connect, vers la passerelle Riello Connect et d'établir une connexion virtuelle à l'application logicielle sur le PC.

Le tunnel établi entre l'ordinateur et le réseau distant peut être utilisé pour créer un ou plusieurs canaux pour les connexions existantes aux terminaux distants.

Du point de vue de la sécurité, la fonctionnalité Accès à distance n'est pas différente du reste de la solution Riello Connect. Les données transmises vers et depuis Riello Connect sont toujours protégées par SSL. La seule différence est que l'utilisateur se connecte à Riello Connect avec le logiciel Quick Connect au lieu d'accéder par le site www.rielloups.com

Autres façons de sécuriser l'accès aux équipements

Liste blanche pour le transfert de ports

Un administrateur Riello Connect peut choisir de placer certaines adresses IP sur « liste blanche ». Cela permet aux utilisateurs d'accéder uniquement à ces adresses, et non pas à d'autres adresses IP.

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

DATRCSX0Y20LRFR