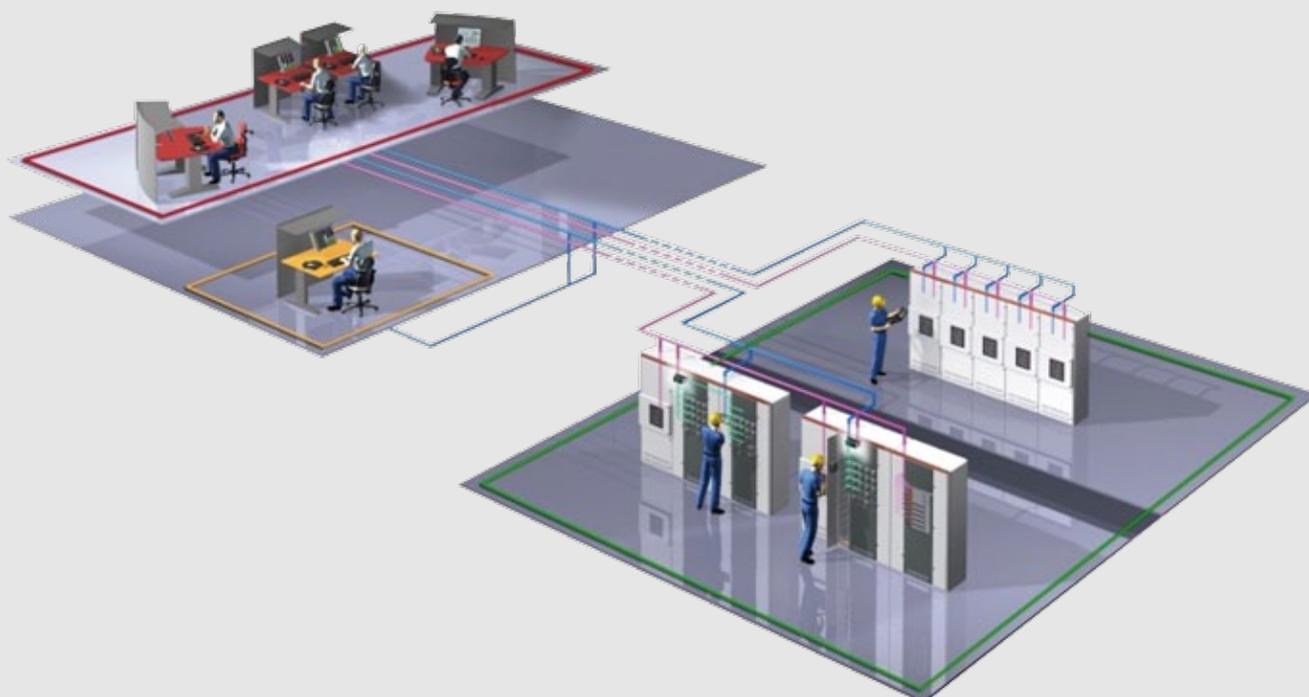


Product catalogue

MyRemoteCare

Cyber security deployment guideline



Disclaimer

The data, examples and diagrams in this manual are included solely for the concept or product description and are not to be deemed as a statement of guaranteed properties. All persons responsible for applying the equipment addressed in this manual must satisfy themselves that each intended application is suitable and acceptable, including that any applicable safety or other operational requirements are complied with. In particular, any risks in applications where a system failure and/or product failure would create a risk for harm to property or persons (including but not limited to personal injuries or death) shall be the sole responsibility of the person or entity applying the equipment, and those so responsible are hereby requested to ensure that all measures are taken to exclude or mitigate such risks.

This solution has been designed to be connected and communicate data and information in a secure way, by means of state-of-the-art technologies. It is the sole responsibility of the person or entity responsible for operation (accessing information) to take the necessary measures (such as, but not limited to, installation of firewalls, application of authentication measures, installation of anti-virus programs, etc.) to protect the data and the accesses, against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB is not liable for any such damages and/or losses.

This document has been carefully checked by ABB but deviations cannot be completely ruled out. In case any errors are detected, the reader is kindly requested to notify the manufacturer. Other than under explicit contractual commitments, in no event shall ABB be responsible or liable for any loss or damage resulting from the use of this manual or the application of the equipment.

Table of contents

005	1. Introduction
006 – 007	2. MyRemoteCare overview
008 – 010	3. Connectivity architecture
011	4. Plant connectivity description
012 – 014	5. MyRemoteCare gateway
015	6. MyRemoteCare website
016	7. MyRemoteCare mobile app
017	8. Protocol usage summary
018	9. System user summary

1 Introduction

01 The intended use of manuals in different lifecycles

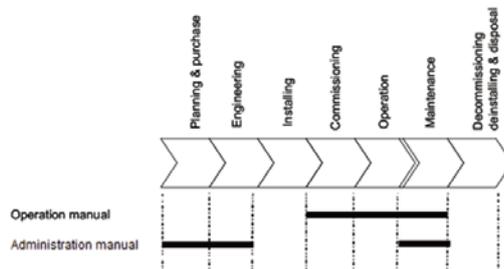
The cyber security document contains a brief overview of MyRemoteCare system security specification and implementation aspects.

Intended audience

This manual addresses the IT responsible person interested on ICT security aspects of ABB MyRemoteCare system.

The user must be trained in and have a good knowledge of client-server application, mobile networks and M2M applications. The manual contains terms and expressions commonly used to describe this kind of solutions.

Product documentation set



01

The Operation manual contains instructions on how to operate MyRemoteCare portal. The manual provides instructions for monitoring the plants, and setting on the software. The manual also describes how to identify errors or problems to determine the cause of a fault.

The Administration manual contains instructions on how to service and maintain the software platform. It contains all the application and functionality descriptions, like creating users, configuring notifications, etc.

 Some of the manuals are not available yet.

Revision history

Document revision/date	Product series version	History
2018-03-23	1.0	First release

 Download the latest documents from the ABB web site.
<http://new.abb.com/medium-voltage/service/maintenance/myremotecare>

Related documentation

Product series and product specific manuals can be downloaded from the ABB web site <http://new.abb.com/medium-voltage/service/maintenance/myremotecare>.

Symbols

-  The electrical warning icon indicates the presence of a hazard which could result in electrical shock.
-  The warning icon indicates the presence of a hazard which could result in personal injury.
-  The caution icon indicates important information or warning related to the concept discussed in the text. It might indicate the presence of a hazard which could result in corruption of software or damage to equipment or property.
-  The information icon alerts the reader of important facts and conditions.
-  The tip icon indicates advice on, for example, how to design your project or how to use a certain function.

Although warning hazards are related to personal injury, it is necessary to understand that under certain operational conditions, operation of damaged equipment may result in degraded process performance leading to personal injury or death. Therefore, comply fully with all warning and caution notices.

2 MyRemoteCare overview

02 Communication architecture

Overview

MyRemoteCare is ABB's online continuous condition monitoring system that supports the implementation of the condition-based maintenance services.

MyRemoteCare offers:

- Online asset health monitoring and analytics
- Managing and evaluating of asset condition and performance level
- Condition-based and proactive maintenance planning

With the above offerings, MyRemoteCare brings the following advantages:

- Reduce operational costs by optimizing maintenance scheduling
- Reduce downtime and increase production time
- Reduce risk of failure by detecting and generating warning at early stage
- Increase service availability, reliability, and safety

In today's environment, cybersecurity is very critical to ABB and its customers. ABB commits to fully focus on all cybersecurity challenges and to take all required actions to inform its customers about the cybersecurity risks.

System architecture

MyRemoteCare system is based on a modular, flexible, scalable, and highly available architecture.

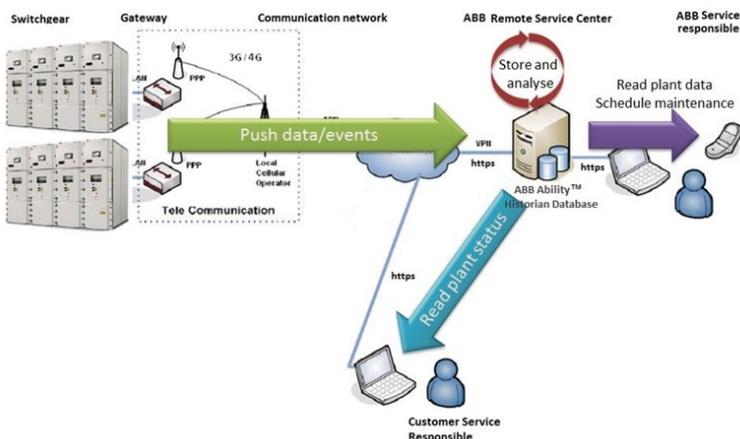
Data collection of MyRemoteCare composes of one or many remote data collectors (or gateways) which are capable of pushing data to MyRemoteCare server either by scheduling or on events.

Every single data collector node or gateway is independent of each other, so that a broken or communication loss does not distract the data transmission of the other. Once the broken node is restored and online, data is back-synchronized automatically.

Figure 2 depicts the system architecture of MyRemoteCare where MyRemoteCare gateways connect and push measurement and events data to server.

MyRemoteCare server consists of several service modules such as data collection service, notification and alarm service, report generation service, and scheduling service. Processed data are stored in database for further analysis and/or consumed by sophisticated performance analyzing algorithms.

MyRemoteCare servers are managed by ABB data center; therefore, standard data backup plan, disaster recovery plan, etc. are strictly followed.



Web-based access

MyRemoteCare is a web-based application. Users can access to MyRemoteCare web application from any computer or mobile device that connects to the Internet using a standard web browser. Advantages of MyRemoteCare being a web application are:

- Access from anywhere in the world with internet connection
- Centralized and secured data storage managed by ABB data centers

Single web application that is able to reach out to many devices with different Operating System (Windows, iOS, Android)

Data security and privacy

Technological advancements and breakthroughs have caused a significant evolution in the electric power grid. As a result, the emerging “smart grid” and “Internet of Things” are quickly becoming a reality. At the heart of these intelligent advancements are specialized IT systems – various monitoring and automation solutions such as monitoring and diagnostic systems. To provide end users with comprehensive real-time information, enabling higher reliability and greater control, automation systems have become ever more interconnected. To combat the increased risks associated with these interconnections, ABB offers a wide range of cyber security products and solutions for automation systems and critical infrastructure.

MyRemoteCare infrastructure has been designed to completely secure the data flow between plants and ABB service center, using the state-of-the-art of ICT (Information and Communication Technology) market.

To counter cyber security risks, open IT standards are equipped with cyber security mechanisms. These mechanisms, developed in a large number of enterprise environments, are proven technologies. They enable the design, development and continual improvement of cyber security solutions for automation systems, including monitoring and diagnostic applications.

ABB understands the importance of cyber security and its role in advancing the security of distribution networks. A customer investing in new ABB technologies can rely on system solutions where reliability and security have the highest priority.

Reporting of vulnerability or cyber security issues related to any ABB product can be done via cybersecurity@ch.abb.com.

The user's access to the data on the server is restricted by authorization levels, and the connection is secured and encrypted (SSL technology). Therefore, the data is strictly visible only to authorized personnel.

 ABB does not collect and store any information about energy production or consumption. MyRemoteCare system tracks only the life of monitored equipment applying predictive-maintenance algorithms.

3 Connectivity architecture

03 Gateway connectivity general principles

For the security analysis the connectivity architecture can be split in 3 components.

- The gateway which read diagnostic information from the electronic equipment and send information to the ABB Service center
- The ABB server which receive the diagnostic information and store it into a unified Database for analysis and driving maintenance activities
- The mobile App MyRemoteCare is a web-based application. Users can access to MyRemoteCare web application from any computer or mobile device that connects to the Internet using a standard web browser.

Advantages of MyRemoteCare being a web application are:

- Access from anywhere in the world with internet connection
- Centralized and secured data storage managed by ABB data centers
- Single web application that is able to reach out to many devices with different Operating System (Windows, iOS, Android)

The connectivity architecture consists of three components:

- Gateway: reads diagnostic information from electronic equipment and send information to server in ABB Service Center
- Server: receives diagnostic information sent by Gateway and store those information for further analytics and driving maintenance activities
- Client (web-based application or mobile app): requests diagnostic information from Server and present data to users on their computers, mobile phones, or tablets

With the three components described above, connectivity can be made in three separate areas:

- From Electronic equipment to gateway
- From gateway to server
- From client to server

In MyRemoteCare gateway, a communication port, namely EXT port, is a logical internal port that is mapped through the general packet radio system or universal mobile telecommunication system (GPRS/UMTS) of the gateway.

MyRemoteCare gateway is developed based on ABB Ability™ Platform which adapts advanced secure technologies to ensure data privacy, data security as well as service availability, and service security. The ABB Ability™ Platform follows the concepts of “Secure by Design” and “Defense in Depth” strategies, in which multiple layers of security controls are placed throughout system. These strategies intend to provide redundancy in the event a security control fails or a vulnerability is exploited that can cover aspects of personnel, procedural, technical and physical security for the duration of the system's life cycle.

Authentication

Certificate-based mutual authentication is used in all connections:

- From Electronic equipment to gateway
- From gateway to server
- From client to server

Data authorization and customer data protection

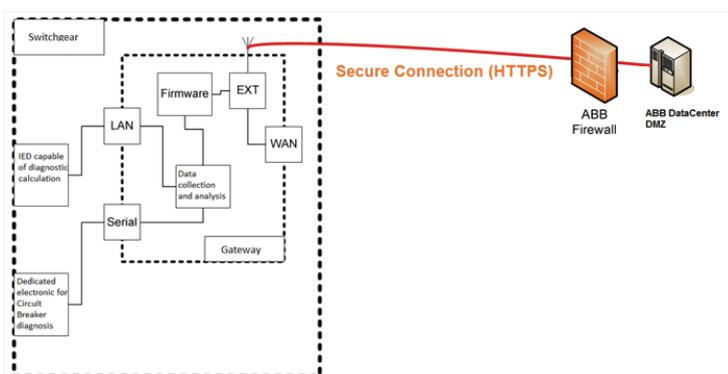
All data access, including APIs, UIs, device and system connections, follows the integrated role-based granular authorization model.

Hardening

Ability™ layers will be hardened by closing the possible attack surfaces to a minimum. All connections are taken from lower-level nodes (gateways), with only the open port TCP/443, to upper layers using secure web socket (HTTPS) communication.

Transport security

The data transfer between the gateway, Cloud, as well as the user access, are based on secure communication such as secure web socket (HTTPS).



04 Secure mobile network channel

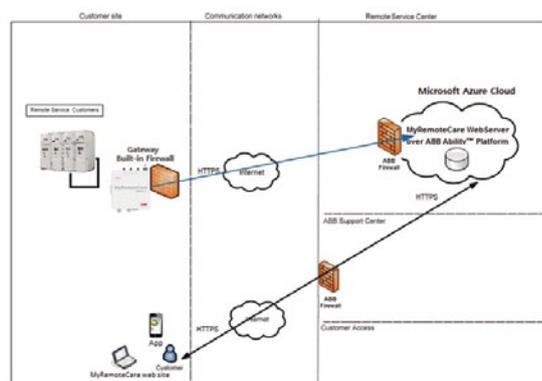
Mobile network secure channel

MyRemoteCare gateway initiates an outbound communication using SIM card with internal credentials on ABB Ability™ Embedded SDK to connect the ABB Ability™ server in the cloud.

MyRemoteCare gateway is a device that equipped with minimal Linux kernel. All backdoors, unused ports, and services are closed and disabled. MyRemoteCare gateway also has built-in software firewall turned on. The default gateway firewall setting, and the open port list will be documented in the later chapter.

MyRemoteCare solution is hosted on ABB Ability™ cloud, which is a managed environment on Microsoft Azure platform. All the data transfer between the gateway, Cloud, as well as the user access such as website and mobile app, are all based on secure communication (HTTPS).

The communication of MyRemoteCare gateway with MyRemoteCare server is only upwards. No downwards traffic is allowed. There is no possibility to reach the field electronic equipment from the internet via website or mobile app. The networks are logically de-coupled.



04

Security analysis

The system architecture is split in different components, where each access is controlled to ensure the maximum security to the involved networks and plants.

About the plant,

- The gateway is able to open communication sessions (e.g. using MODBUS protocol) to the devices on Serial channel
- The devices cannot open a data communication sessions to the gateway (e.g. they cannot query via Modbus the gateway)
- The devices cannot open any communication sessions above the gateway (e.g. to the MyRemoteCare server in ABB Ability™ cloud). Routing function disabled
- Anything above the gateway (e.g. the MyRemoteCare server in ABB Ability™ cloud) cannot open any communication sessions to the device

About the mobile network infrastructure,

- All communications between the gateway, Cloud, as well as the user access such as website or mobile app, are based on secure communication (HTTPS)
- The MyRemoteCare server entry and gateway point are both firewalled
- The gateway can only open the upwards communication sessions to MyRemoteCare server. No downwards traffic is allowed

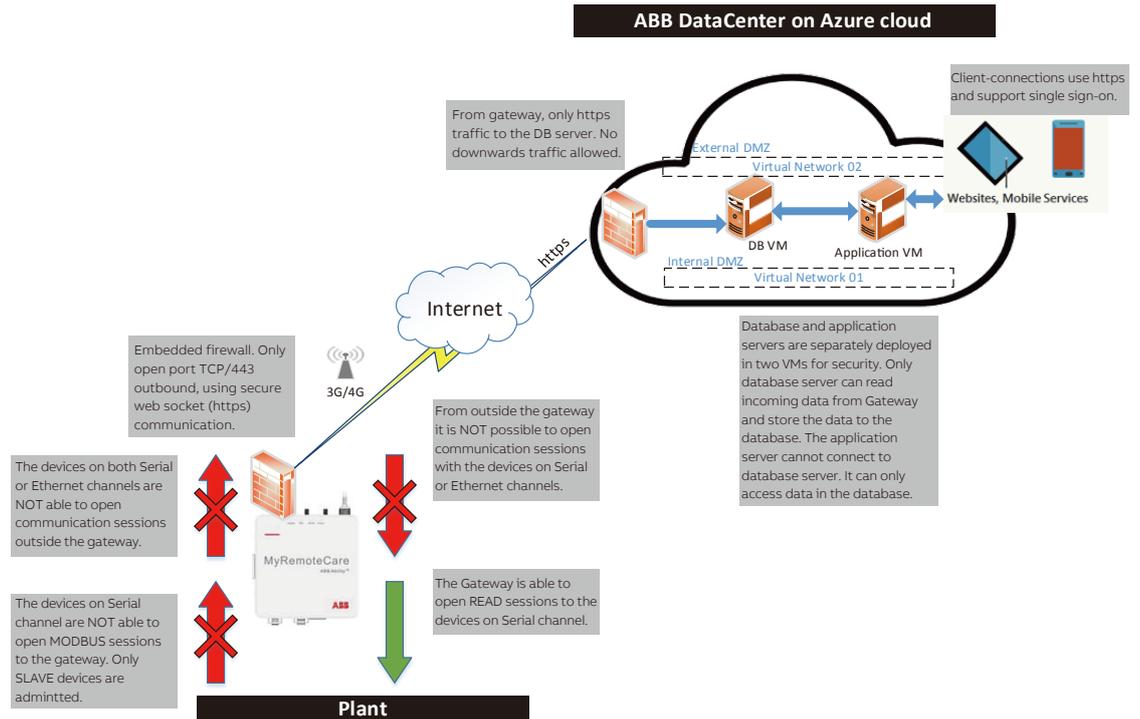
About the ABB datacenter,

- The MyRemoteCare solution is based on ABB Ability™ platform which is hosted on Microsoft Azure Cloud fully taking advantage of Microsoft security technologies and capabilities
- The application server (website and app) and database server (ABB Ability™ Historian) are logically separated. The application server cannot connect to database server. It can only access data in the database
- The traffic coming from gateway which ends onto the ABB firewall is redirected only to the database server. The other server of MyRemoteCare system cannot receive or send data towards to the gateway

3 Connectivity architecture

05 Security modular architecture

The mentioned topics are depicted in Figure 5.



05

Gateway authentication

Connectivity from electronic equipment to gateway: MDC4 is the diagnostic device that connect to MyRemoteCare gateway via serial communication; therefore, there is no authentication mechanism provided. Besides, MDC4 is simply a monitoring unit and not a controllable device.

Connectivity to gateway from configuration software: Gateway can be configured using its configuration software. Connectivity from configuration software to gateway is only available using HTTPS over LAN Ethernet. Generally, ABB service personnel is authorized to make configuration changes in the gateway. Once user is logged in, he or she can only make changes to the application configuration, but not the networking, routing parameters, and security settings.

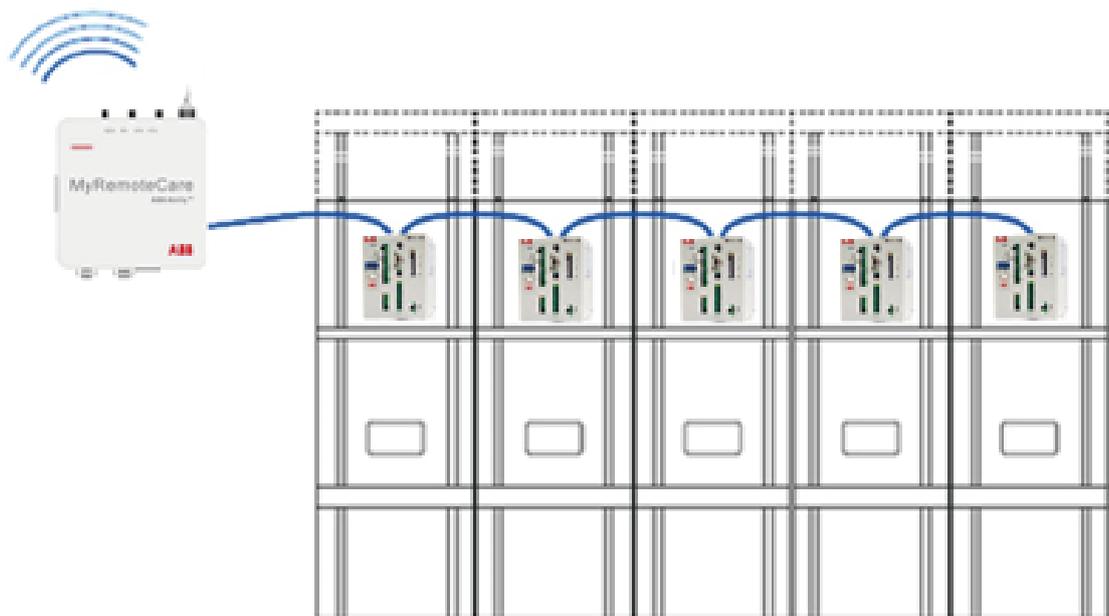
MyRemoteCare server authentication

User authentication is based either on username/password or ABB Single-Sign-on services. The communication protocol is HTTPS only. MyRemoteCare provides granular role-based access control that assure that only authorized users have access to restricted application functionality or features. Authorized users can mainly view analysis data, events, alarms, and reports. There is no direct access or control from web or mobile application to gateways.

4 Plant connectivity description

06 Scenario with MDC4 on RS485 bus

Monitoring devices such as MDC4 can only connect to gateway using RS485 serial communication and MODBUS RTU. The data transmission from these devices to gateway is strictly local; therefore, it is not possible for a gateway to remotely communicate to a monitoring device.



5 MyRemoteCare gateway

07 Gateway linear guide installation – bottom view

08 First login page, required to change the password

09 User password change

MyRemoteCare gateway aggregate data from connected diagnostic devices (e.g. MDC4) and send data to MyRemoteCare server.

MyRemoteCare gateway supports the following communication channels:

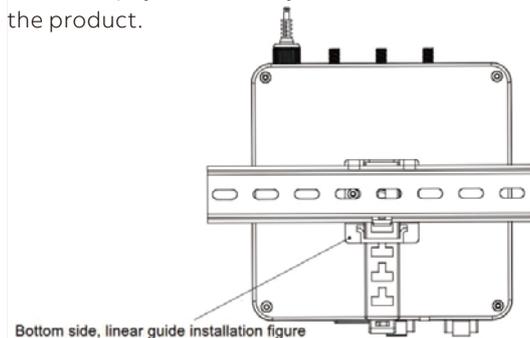
- Serial RS485 for MDC4 devices
- Ethernet LAN for gateway configuration
- Wi-Fi for local connectivity to mobile app

3G/4G modem for connection to MyRemoteCare server

Routing between the LAN port connected to the device and the WAN connection via modem to ABB remote server is not possible. Every communication between modem channel and LAN channel is prohibited to prevent direct local communication to ABB or, vice versa, from ABB to the device.

Gateway installation

The device is installed in the low voltage compartment of switchgear, which is locked by a door. The physical security must be assured for the product.



07

Gateway from/to ABB server connection

MyRemoteCare server is behind firewall and can accept only HTTPS communication through ABB Ability™ secure channel from gateway, which in turn is also behind built-in software firewall.

The gateway sends the following data.

- Plant communication diagnostic information (devices are alive or not)
- Devices alarms and quality changes

- Daily full report (full picture of the plant devices quality status)

No commands can be forced to the plant devices from ABB remote server.

Using the web configuration tool

MyRemoteCare gateway is accessible via the web configuration tool.

<https://192.168.1.1>

The access to the portal is only available via secure HTTPS protocol. It is responsibility of the user to use on his PC an updated browser and adopt secure behavior in terms of security and sensitive data handling.

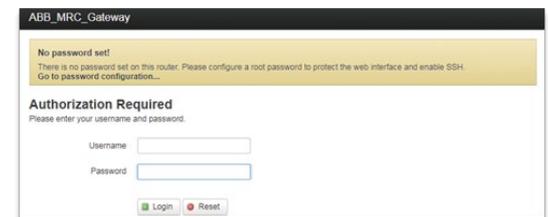
To use the web configuration tool, logging in and authorization are required.

User management

MyRemoteCare gateway provides a root user:

Username	Default password	Role
root	(empty)	administrator

You are required to change the password when first logging in.



08

You can also go to the System -> Administration, to change the user password.



09

- 10 How to enable/disenable each port
- 11 Firewall default setting
- 12 Change the Wi-Fi SSID and password

Hardening

Gateway is hardened by closing the possible attack surfaces to a minimum. Only the needed libraries and functions are included when building the Gateway image.

Besides, only the needed ports are open while others closed at start up. Below is the list of open port and service:

Port	Service	Purpose
443/HTTPS	web server	Encrypted web access, (https://192.168.1.1)
80/HTTP	web server	Re-directed to port 443

We recommend not to change the default setting.

How to enable/disenable each port

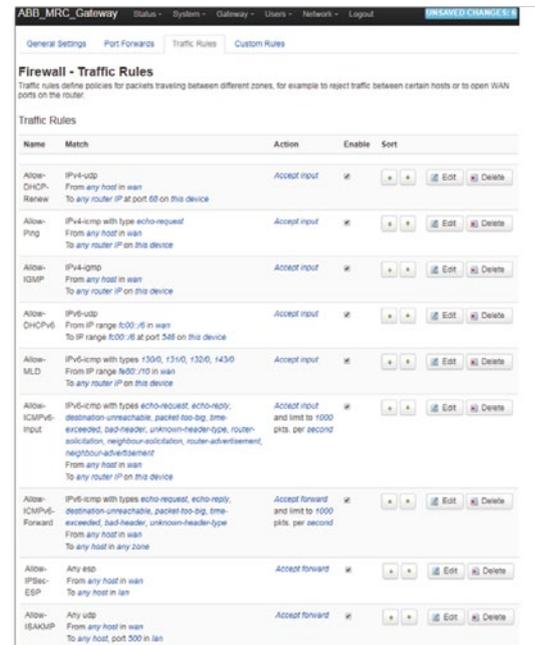
For debugging purpose, if you want to enable or disable a port, you can go to the page <https://192.168.1.1/cgi-bin/luci/admin/system/s tartup>, to enable or disable ports.



10

Firewall setting

The gateway is secured and behind firewall. The default firewall settings in gateway are below.



11

To summarize, below is the list of services that gateway allows by default settings.

- DHCP: used to dynamically assign an IP address to each device on a network
- PING: used to test the reachability of a host on an IP network
- IGMP, MLD: used to manage the multicast group
- IPSec-ESP: IPsec Encapsulating Security Payload
- ISAKMP: Internet security and key management protocol

We recommend not to change the default firewall settings.

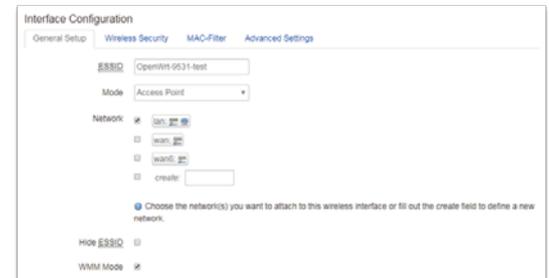
Wi-Fi setting

Gateway provides a Wi-Fi hotspot for MyRemoteCare mobile app local connection. To secure this channel, gateway doesn't broadcast its SSID.

To connect Wi-Fi, user should manually add this hidden SSID and password.

Default SSID	Password
MRCGateway	123456

We highly recommend user to change the default password. Please go to the gateway web configuration tool, Interface Configuration and Wireless Security setting, to change the password or SSID:



12

5 MyRemoteCare gateway

- 13 Backup/Restore
- 14 Flash operations
- 15 Flash firmware verify
- 16 Factory reset

Backup/Restore

When the gateway is configured properly, we recommend user to backup the configuration.

To backup/restore the gateway, please go to the gateway web configuration tool, Backup/Restore operations.



13

Flash firmware/application

To flash new firmware or application image, please go to the gateway web configuration tool, Flash operations:



14

The gateway firmware image or application image is only downloaded from MyRemoteCare website and executed via gateway web configuration tool. The gateway will verify the code before installation for security.



15

Audit trail

MyRemoteCare gateway offers an audit trail function, which is a chronological record of system, driver and user activities.

System log path: /root/log/abb_logSystem log format.

Time	User ID	Type of event	Success or failure	Component
------	---------	---------------	--------------------	-----------

Application log path: /home/GWLog_1.log
Application log format.

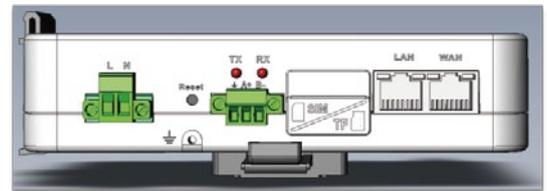
Time	User ID	Type of event	Success or failure	Component
------	---------	---------------	--------------------	-----------

Session ID	User IP
------------	---------

Factory reset

When a gateway is decommissioning or no longer in service, all sensitive data including user credentials and application data can be purged and reset. The information is divided into two hard drive partitions on flash: program and data. On factory reset, the data partition is overwritten with meaningless data. This functionality is provided by the OS.

Use a pin to long press the reset button of this device in front panel for 10 second to reset it to factory defaults.



16

6 MyRemoteCare website

17 Login page

18 MyRemoteCare website role groups

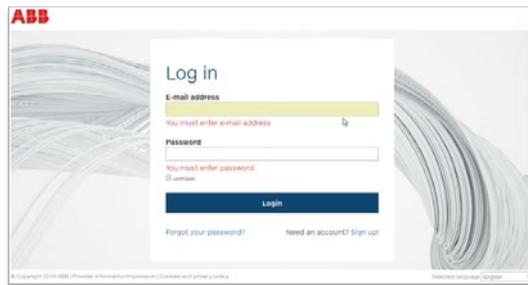
To access MyRemoteCare web application, go to:

<https://myremotecare.cn.abb.com>

The access to the web portal is only available via secure HTTPS protocol. It is responsibility of the users to use on his PC an updated browser and adopt secure behavior in terms of security and sensitive data handling.

Using the web portal

To use the web portal, logging in and authorization are required.



17

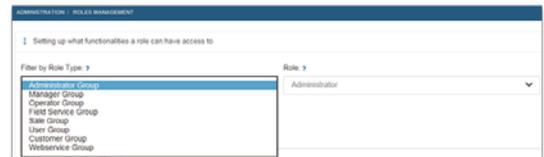
User management

Access to the web portal is allowed only after user authentication, based on user name and password. MyRemoteCare is using MyABB single-sign-on secure function. This service guarantees a unique account management for all possible ABB cloud services, like MyRemoteCare. The service username is the mail of the user, and allows only strong passwords following state-of-the-art guidelines (such as, but not limited to, minimum length of 8 characters, including at least 3 different character types among upper case letters, lower case letters, numbers and non-alphanumeric characters). ABB Single-Sign-On service offers also a procedure for password reset.

The session inactivity timeout is 30 minutes.

ABB privacy policy is available on web site: <http://new.abb.com/privacy-policy>.

MyRemoteCare web server provides the role-based user management. User will be assigned with the appropriate roles. There are eight role groups definition in MyRemoteCare web with accessibility to the different functionalities.



18

Open port and service

Port	Service	Purpose
443/HTTPS	web server	Encrypted web access
80/HTTP	web server	Re-directed to port 443

Audit trail

MyRemoteCare offers an audit trail function, which is a chronological record of system activities, such as Activity Log, Exception Tracking Log, and Configuration Change Log including IP addresses of the requests. The events are about authentication to the portal (login and logout), and application configuration (remote gateway configuration validation and update).

7 MyRemoteCare mobile app

19 Login page

The installation package of mobile app can be downloaded from MyRemoteCare website.

The mobile app access to MyRemoteCare backend server is only available via secure HTTPS protocol.

Using the mobile app

To use the mobile app, logging in and authorization are required.

User management

Same with the MyRemoteCare website, mobile app is using MyABB single-sign-on secure function.

Audit trail

Mobile app activities are also logged in web server.

ABB

Log in

E-mail address

Password

unmask

Login

[Forgot your password?](#)
[Need an account? Sign up!](#)

© Copyright 2016 ABB | [Provider Information/Impressum](#) |
[Cookies and privacy policy](#)
 Selected language: English

8 Protocol usage summary

The gateway uses the following protocol.

Purpose	Source/Master	Connection	Protocol	Security
Read MDC4 diagnostic and status data	Gateway queries MDC4 on serial port RS485 (each gateway has its own address)	Gateway to MDC4 on Serial RS485	Modbus RTU	No special security as serial communication. Write commands are secure with a key exchange between master and slave

Locally users can communicate with the gateway using the following protocols.

Purpose	Source/Master	Connection	Protocol	Security
Configure and check the plant devices communication and the communication with the ABB Server	User requests information and configures the gateway	User's PC to Gateway on Ethernet port (LAN) or User's mobile app to gateway on Wi-Fi	HTTPS	HTTPS and self-signed certificate

9 System user summary

Gateway

Username	Default password	Role
root	(empty)	administrator

Wi-Fi SSID	Default password
MRCGateway	123456

Copyright

This document and parts thereof must not be reproduced or copied without written permission from ABB, and the contents thereof must not be imparted to a third party, nor used for any unauthorized purpose.

The software or hardware described in this document is furnished under a license and may be used, copied, or disclosed only in accordance with the terms of such license.

Trademarks

ABB and ABB Ability™ are registered trademarks of ABB Group. All other brand or product names mentioned in this document may be trademarks or registered trademarks of their respective holders.

Guarantee

Please inquire about the terms of guarantee from your nearest ABB representative.

ABB Xiamen Switchgear Co., Ltd.

ABB Industrial Park, Torch High-Tech Zone, No. 319,

Xiamen, Fujian, P.R.China

Tel: +86 0592 602 6033

Fax: +86 0592 603 0505

Zip Code: 361006

Service HotLine: 800-820-9696 400-820-9696

<http://new.abb.com/cn>