
DISTRIBUTION SOLUTIONS

ABB Ability™ Condition Monitoring for electrical systems – CMES

User Management Quick Guide



NOTICE

This document contains information about one or more ABB products and may include a description of or a reference to one or more standards that may be generally relevant to the ABB products. The presence of any such description of a standard or reference to a standard is not a representation that all of the ABB products referenced in this document support all of the features of the described or referenced standard. In order to determine the specific features supported by a particular ABB product, the reader should consult the product specifications for the particular ABB product.

ABB may have one or more patents or pending patent applications protecting the intellectual property in the ABB products described in this document.

The information in this document is subject to change without notice and should not be construed as a commitment by ABB. ABB assumes no responsibility for any errors that may appear in this document.

Products described or referenced in this document are designed to be connected and to communicate information and data through network interfaces, which should be connected to a secure network. It is the sole responsibility of the system/product owner to provide and continuously ensure a secure connection between the product and the system network and/or any other networks that may be connected.

The system/product owners must establish and maintain appropriate measures, including, but not limited to, the installation of firewalls, application of authentication measures, encryption of data, installation of antivirus programs, and so on, to protect these products, the network, its system, and interfaces against security breaches, unauthorized access, interference, intrusion, leakage, and/or theft of data or information.

ABB performs functionality testing on the products and updates that we release. However, system/product owners are ultimately responsible for ensuring that any product updates or other major system updates (to include but not limited to code changes, configuration file changes, third-party software updates or patches, hardware change out, and so on) are compatible with the security measures implemented. The system/product owners must verify that the system and associated products function as expected in the environment in which they are deployed.

In no event shall ABB be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, nor shall ABB be liable for incidental or consequential damages arising from use of any software or hardware described in this document.

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. This product meets the requirements specified in EMC Directive 2014/30/EU and in Low Voltage Directive 2014/35/EU.

The ABB Ability™ Condition Monitoring for electrical systems – CMES uses these open source components:

jquery version	3.2.1	Copyright JS Foundation and other contributors, https://js.foundation/
jqueryui.com	1.12.1	Copyright JS Foundation and other contributors, exact contribution history, see https://github.com/jquery/jquery
perfect scrollbar	1.1.0	The MIT License (MIT) Copyright (c) 2012-2017 Hyunje Jun and other contributors
selectric	1.13.0	Copyright (c) 2016 Leonardo Santos

MIT license

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

TRADEMARKS

MNS is a registered or pending trademark of ABB.

Ability is a trademark of ABB.

All rights to copyrights, registered trademarks, and trademarks reside with their respective owners.

Copyright © 2018/2019 ABB.

All rights reserved.

Release: April 2019

Document Number: 1TGC908006

Revision: M0202

Table of Contents

- 1. General.....1**
 - 1.1. Target Group1
 - 1.2. Terminology1
 - 1.3. Related Documentation1
 - 1.4. Related System Version.....1
- 2. Introduction.....2**
 - 2.1. Default settings2
- 3. Configuring the User Management for the CMES.....3**
 - 3.1. Creating a New User for CMES3
 - 3.2. Changing an existing User Password 8
 - 3.3. Changing the Password of Admin User10
- 4. Network connectivity17**
- 5. Troubleshooting18**

List of Figures

Figure 1– Select Computer Management	3
Figure 2– Computer Management Window	4
Figure 3– Select “New User”	4
Figure 4– Add New User	5
Figure 5– Add user to “RTDB-operator” group	6
Figure 6– Add user to "RTDB-readonly" group	6
Figure 7– User added to “RTDB-operator” group	7
Figure 8– User Changes Own Password	8
Figure 9– Double Click - Change Password	10
Figure 10 – Follow steps 1... 3 according following description	11
Figure 11 – Enter new password	11
Figure 12 – Disconnect Remote Desktop	12
Figure 13 – Press OK	12
Figure 14 – Follow the steps, see detailed description below	13
Figure 15– Generic Credential – Add a generic credential.....	14
Figure 16– Add “CPIMS/ADMIN” with new admin password.....	14
Figure 17– Add “CPIMS/DBADMIN” with new admin password	15
Figure 18– Press OK to continue after entering new user credentials	15
Figure 19– Changing of admin password finished – Press OK	16

1. General

1.1. Target Group

The MNS Digital Edge device is the hardware platform for **ABB Ability™ Condition Monitoring for electrical systems** (in the following 'CMES').

Audiences of this manual are service technicians and switchgear operators on site. This document describes the communication and user interfaces of the MNS Digital Edge device and CMES.

The reader shall be familiar with the terms and concept of ABB MNS Low Voltage Switchgear.

The reader shall be familiar with the terms and concept of Microsoft Windows®.

1.2. Terminology

List of the terms, acronyms, abbreviations and definitions that the document uses.

Abbreviation	Term	Description
CMES		Abbreviation for on-premise ABB Ability™ Condition Monitoring for electrical systems
	MNS Digital Edge	Hardware platform for on-premise Edge computing, including CMES and cloud connectivity
MNS		Modular Low Voltage Switchgear family from ABB
	Windows OS	Windows Operating System. Windows® is a registered trademark of Microsoft Corporation. All other trademarks are the property of their respective owners.

1.3. Related Documentation

[1] 1TGC908002M0203 ABB Ability Condition Monitoring for electrical systems – CMES - User Manual

1.4. Related System Version

The content of this document is related to MNS Digital Release 2.0

2. Introduction

This document provides an introduction on how to setup or change login credentials for the user management of the CMES.

2.1. Default settings

The MNS Digital Edge is provided from ABB with the custom specific project installed. Within project specification the customer defines the number of users which have access to CMES and the respective user roles. In this case ABB will set-up the CMES with the agreed user accounts. After delivery it's mandatory to change at least the user passwords.

In case the users and roles are not defined from project, 2 default users are installed: Administrator and Operator.

This is also valid when the MNS Digital Edge is ordered as spare part.

Default login credentials are:

Administrator

User name: EdgeGwAdmin

Password: PleaseChangeMe

Operator

User name: EdgeGwUser

Password: PleaseChangeMe

For cyber security reason, it's mandatory to change the password after installation of the MNS Digital Edge.

ABB will take no liability caused by using the default passwords.

Please contact your IT department about details of password management and cyber security measures in your company. A process for regular update of anti-virus software needs to be implemented.

By default, the Windows Defender is installed and activated. Please ensure to update the Windows OS and the anti-virus software on regular basis.

3. Configuring the User Management for the CMES

This chapter explains possible adaptations of the user management for users of the pre-installed MNS Digital Edge:

- Create a new user
- Adding a new user
- Changing users
- Changing passwords by Windows remote desktop application.

3.1. Creating a New User for CMES

To create a new user, you have to login as administrator. The following steps are describing the workflow how to create a new user with the role “operator”. An operator has the permissions to acknowledge alarms. It is also described how to give a user the role “Read Only” at the crucial steps. This user has no permission to acknowledge alarms.

Step	Actions	Remark
1	<ul style="list-style-type: none"> • Login by remote desktop¹ as administrator 	The password is provided from your ABB contact together with the MNS Digital Edge.
2	<ul style="list-style-type: none"> • Right click windows symbol “Computer Management”-Local Users and Groups” 	

¹To access the windows operating system alternatively a monitor, keypad and mouse can be connected to the MNS Digital Edge.

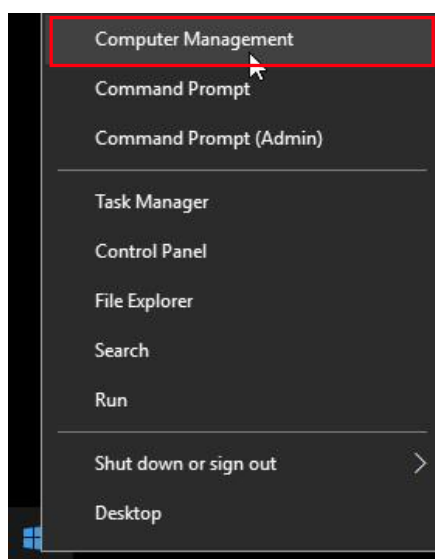


Figure 1– Select Computer Management

The computer management window will open

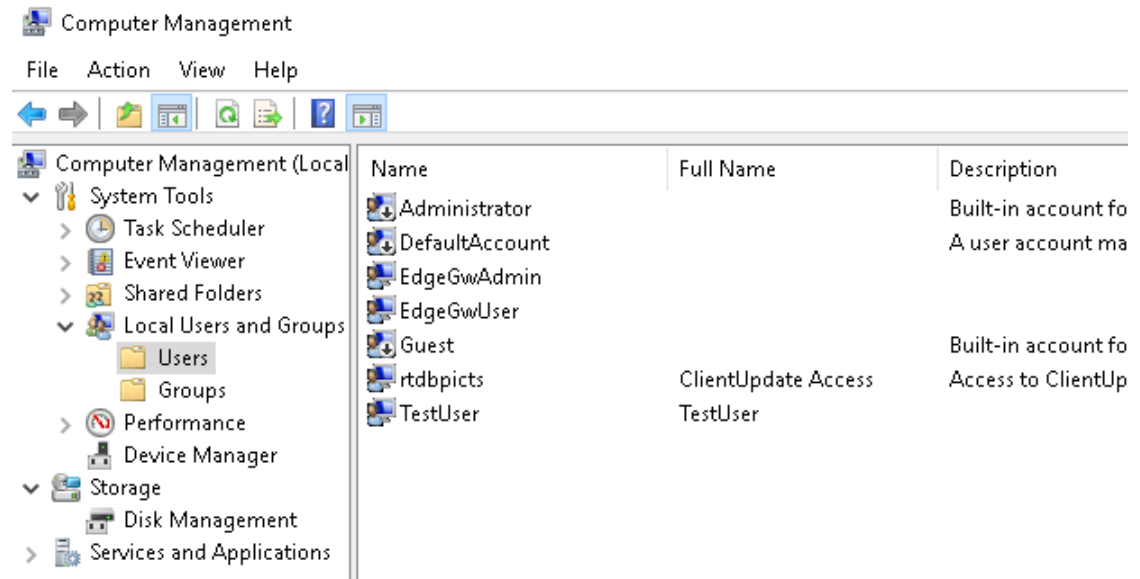


Figure 2– Computer Management Window

Step	Actions	Remark
3	<ul style="list-style-type: none"> • Right Click at “Users” – “New User...” • Enter new user name, password, Pass-word never expires and press Create and Close 	



Figure 3– Select “New User”

New User

User name:

Full name:

Description:

Password:

Confirm password:

☐ User must change password at next logon

☐ User cannot change password

☒ Password never expires

☐ Account is disabled

Help Create Close

Figure 4– Add New User

Step	Actions	Remark
4	<ul style="list-style-type: none"> Right click at “NewUser” and the properties page opens Select tab “Member Of” Press Add Enter “RTDB-operator” or “RTDB-readonly” Press “check names” and Ok 	<p>Add user to rtdb-operator group</p> <p>Creates a new user with role “Operator”</p> <p>Creates a new user with role “read only”</p>

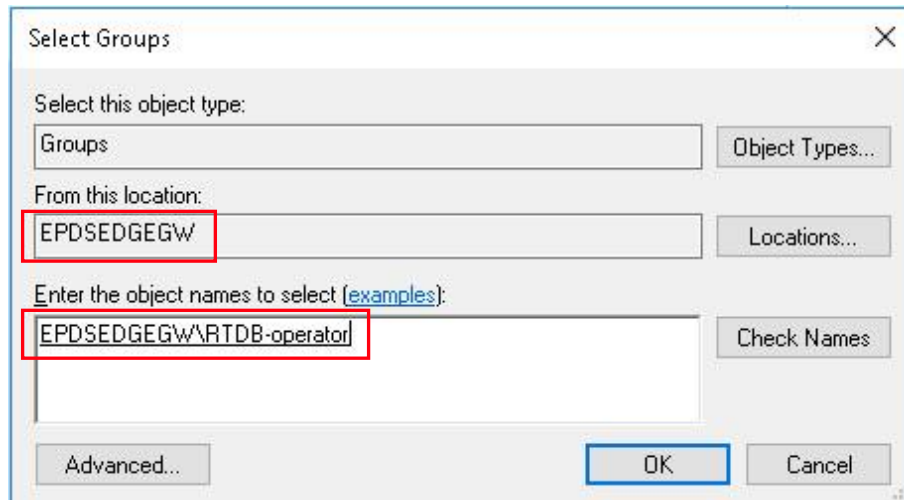


Figure 5– Add user to “RTDB-operator” group

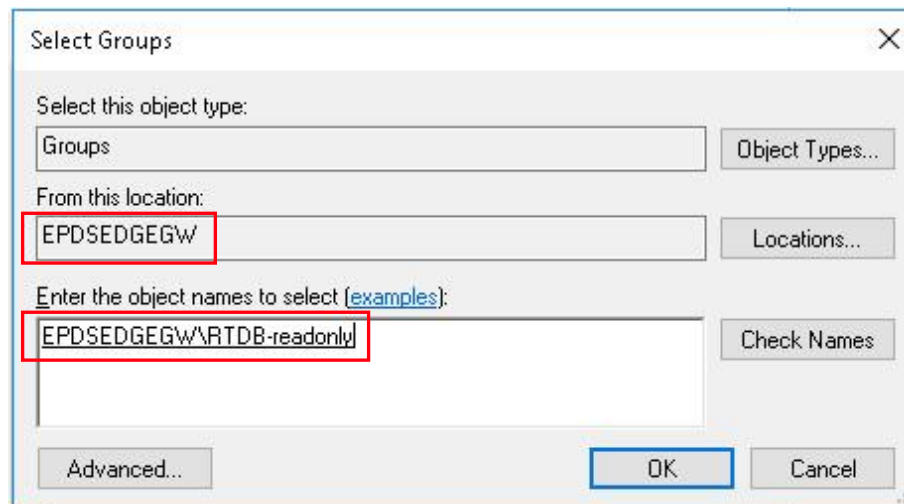


Figure 6– Add user to "RTDB-readonly" group

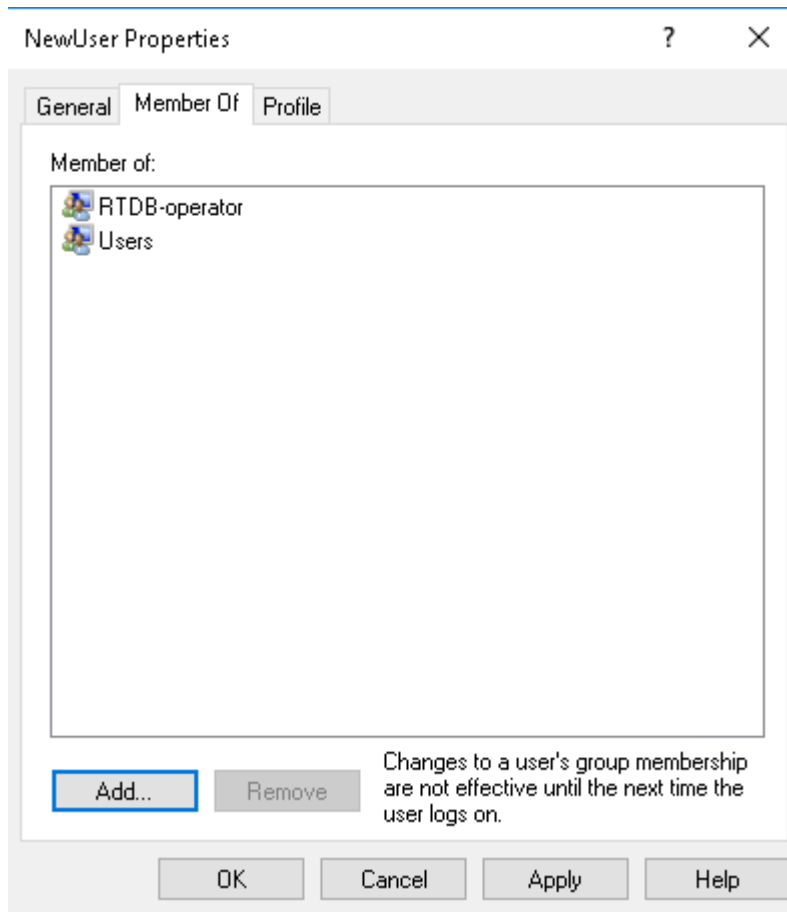


Figure 7– User added to “RTDB-operator” group

3.2. Changing an existing User Password

Due to cyber security reasons a user should change its own password from time to time. This could be done in following way:

Step	Actions	Remark
1	<ul style="list-style-type: none"> • Login by remote desktop with user name and password 	User login– Before user can login the administrator has to add user to Remote Desktop Users (Right click windows symbol – Computer Management – Local Users and Groups – Groups - Remote Desktop Users).
2	<ul style="list-style-type: none"> • Left click windows symbol – “Settings” – “Accounts” – Sign-in options” • Section Password – Press “Change” button • Enter current password, new password twice and hint • Press Next • Press Finish 	Change current password, see following explanation about password complexity requirements

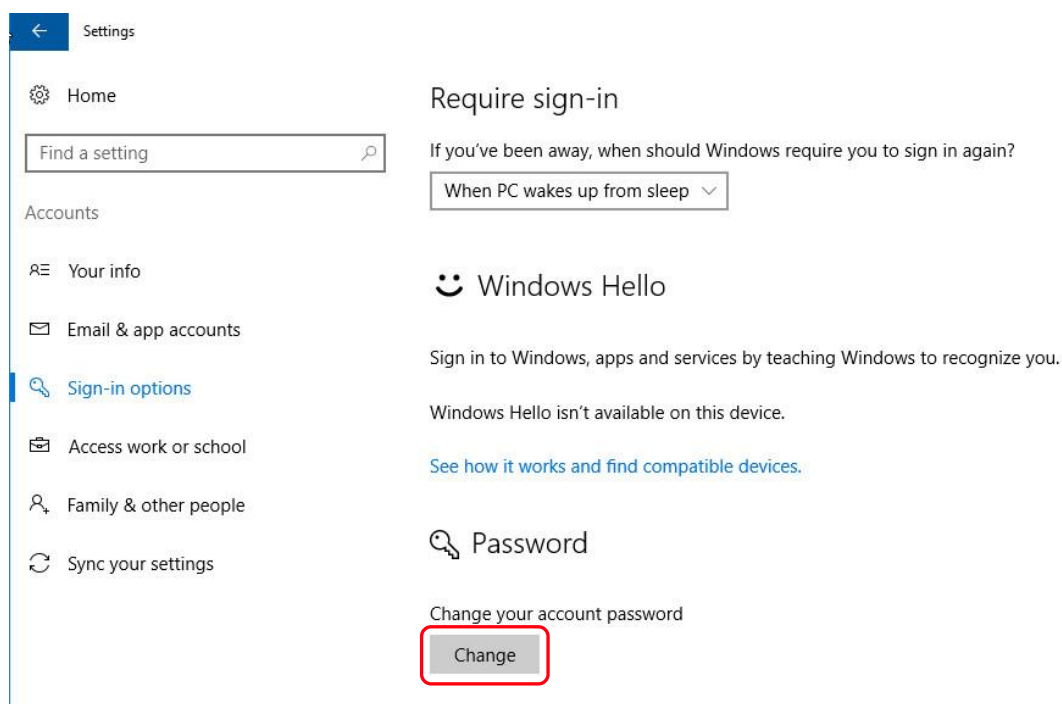


Figure 8– User Changes Own Password

Password Complexity Rules and Password History

The password has to contain characters from three of the following categories:

- Uppercase letters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
- Lowercase letters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
- Base 10 digits (0 through 9)
- Non-alphanumeric characters (special characters): (~!@#\$%^&* _+= ` \(){}[];:"'<>.,?/) Currency symbols such as the Euro or British Pound are not counted as special characters for this policy setting.
- Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages

A new password is only accepted by Windows when it is differs from four previous passwords.

3.3. Changing the Password of Admin User

This chapter explains how to change password of the administrator user.

Step	Actions	Remark
1	<ul style="list-style-type: none"> Login by remote desktop with admin user name and password <p>Default is: EdgeGwAdmin– “PleaseChangeMe”</p>	<p>The name of the user account has been provided as a setup parameter during the installation.</p> <p>The admin user must have administrator privileges (or other privileges for running as a service and accessing the database tables locally).</p>
2	<ul style="list-style-type: none"> Open Windows Explorer Goto folder “D:\Software\SystemConfigurationScripts\Change-AdminPassword” 	
3	<ul style="list-style-type: none"> Double click “Change Admin Password” and continue with Yes 	

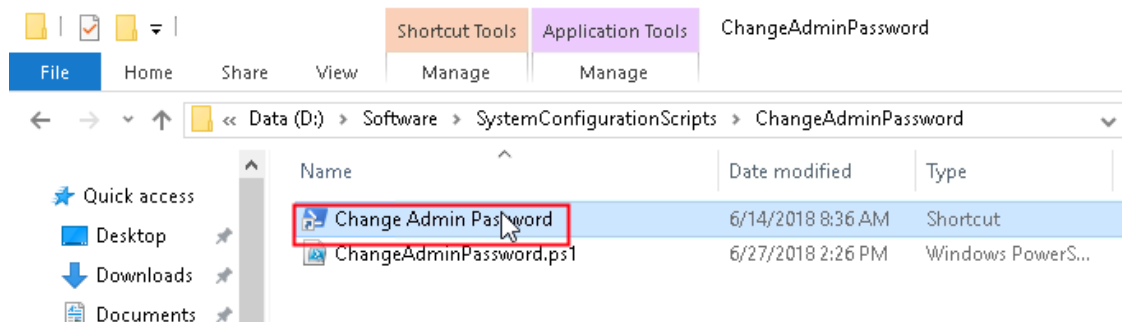


Figure 9– Double Click - Change Password

4	<ul style="list-style-type: none"> Wait until following dialog pops up
---	---

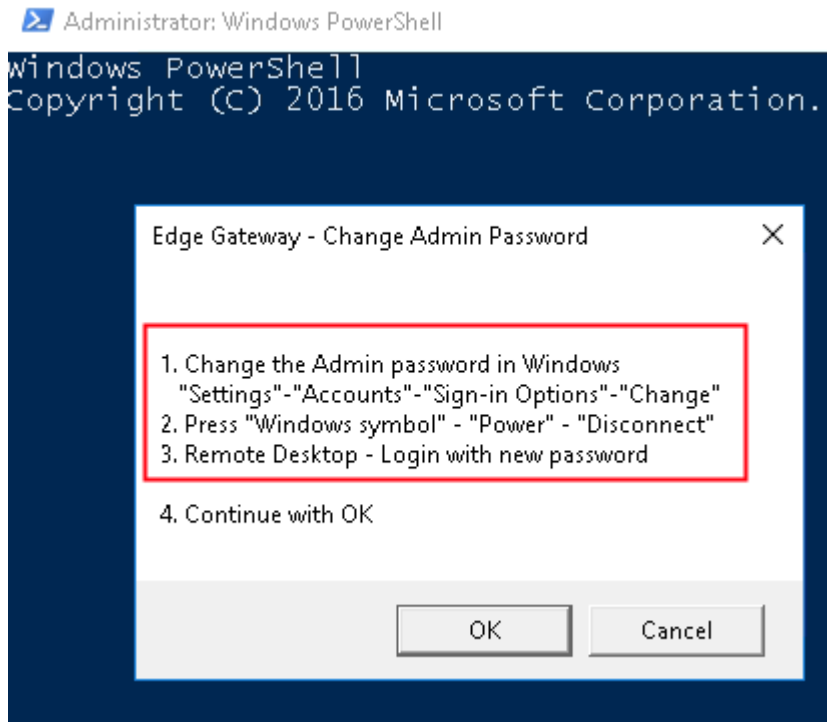


Figure 10 – Follow steps 1... 3 according following description

5	<ul style="list-style-type: none"> Change the Admin password, Left mouse click at "Windows symbol" - "Settings" - "Accounts" - "Sign-in Options" - "Change" 	
6	<ul style="list-style-type: none"> Enter new password 	Change current password, see in chapter 3.2 explanation about password complexity

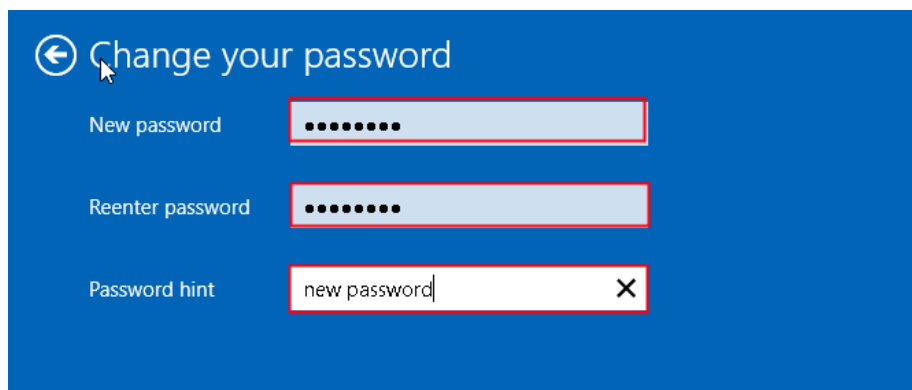


Figure 11 – Enter new password

- 7 • End your connection to the computer – Press “Windows Symbol” - “Power” - “Disconnect” **Do not reboot or logout!**

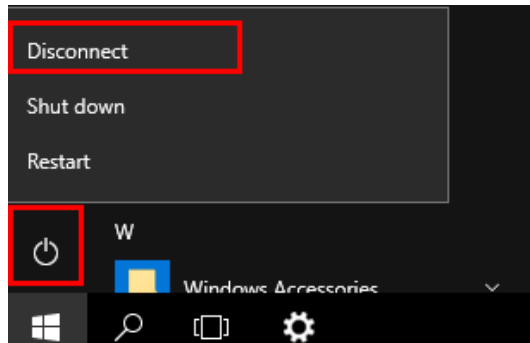


Figure 12 –Disconnect Remote Desktop

- Login by remote desktop with admin user name "EdgeGwAdmin" and new password

- 9 • Press Ok See next picture

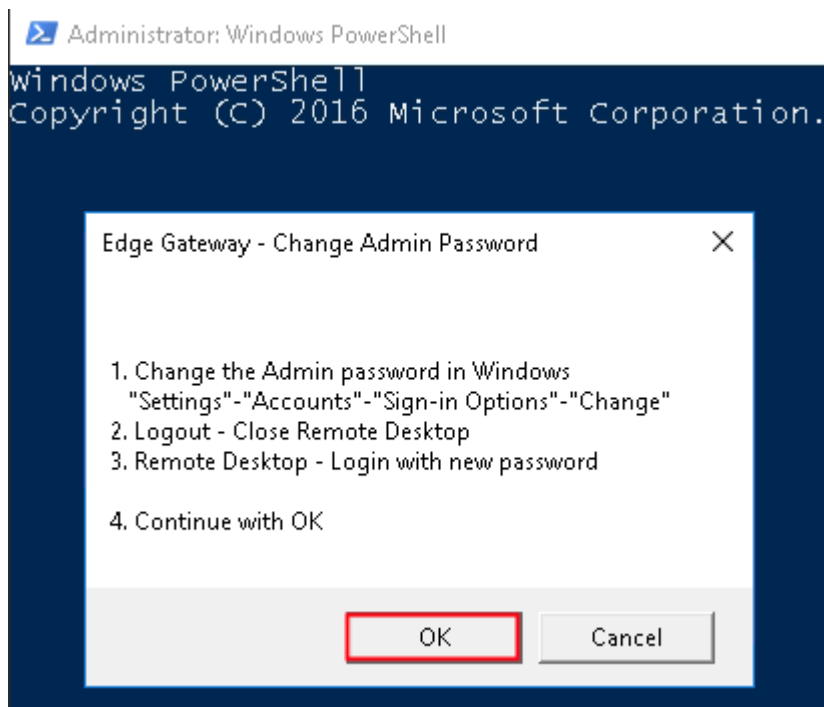


Figure 13 – Press OK

-
- 10 • Wait until following dialog pops up

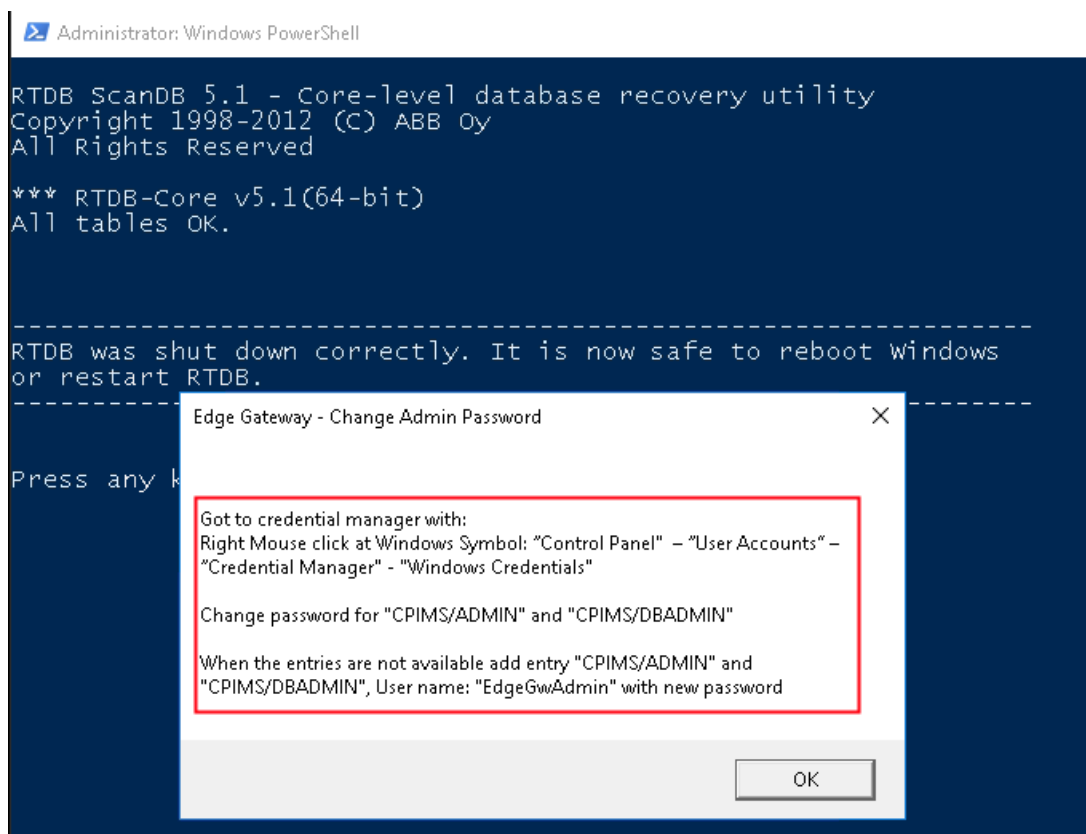


Figure 14 – Follow the steps, see detailed description below

-
- 11
- Right Mouse click at Windows Symbol –
 “Control Panel” – “User Accounts” –
 “Credential Manager” – “Windows
 credentials tab – Generic Creden-
 tials”
 - Change password of admin user in the
 Windows vault entry “CPIMS/ADMIN”
 and CPIMS/DBADMIN”
 - When entries are not available add ge-
 neric credential “CPIMS/ADMIN”
 and “CPIMS/DBADMIN” with new ad-
 min password
-

Manage your credentials

View and delete your saved login information for websites, connected applications and networks.



Web Credentials



Windows Credentials

Restore Credentials

Windows Credentials

[Add a Windows credential](#)

No Windows credentials.

Certificate-Based Credentials

[Add a certificate-based credential](#)

No certificates.

Generic Credentials

[Add a generic credential](#)

No generic credentials.

Figure 15– Generic Credential – Add a generic credential

Add a Generic Credential

← → ▾ ▴ > Control Panel > User Accounts > Credential Manager > Add a Generic Credential ▾ ↻ Search

Type the website address and your credential information

Make sure that the user name and password that you type can be used to access the location.

Internet or network address:

User name:

Password:

Figure 16– Add “CPIMS/ADMIN” with new admin password

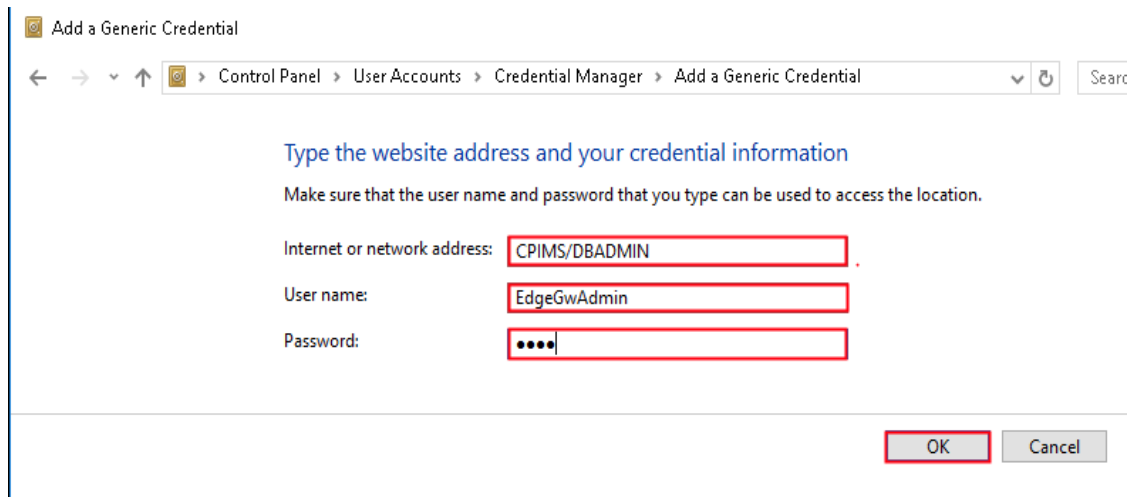


Figure 17– Add “CPIMS/DBADMIN” with new admin password

12 • Press OK

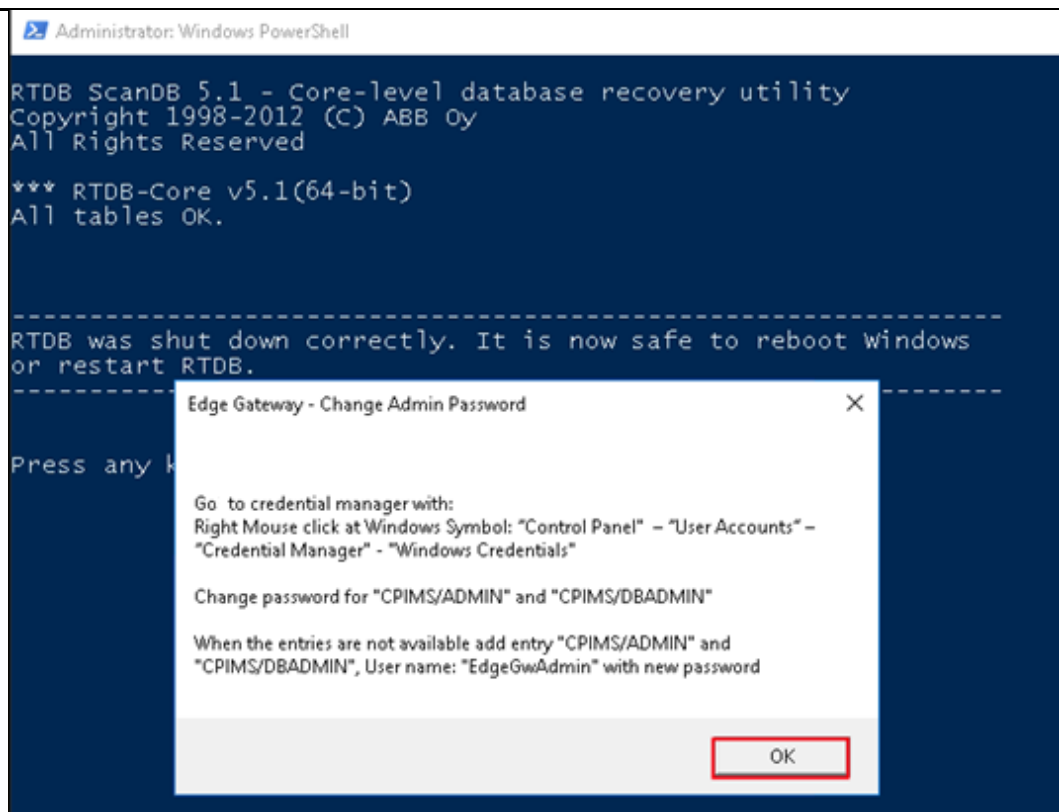


Figure 18– Press OK to continue after entering new user credentials

13 • Wait until following windows comes up Finish password change. and press OK

```

Administrator: Windows PowerShell
13:43:16.354 OK - "RTDB_OpcDaServer"
13:43:18.261 OK - "RTDB_OpcHdaServer"
13:43:19.402 OK - "RTDB_OpcUaServer"
13:43:21.730 OK - "CpmPlusKM_VtrinServers"
13:43:22.839 OK - "CpmPlusKM_OpcServers"
13:43:23.761 OK - "CpmPlusKM_Tcc"
13:43:24.683 OK - "CpmPlusKM_VtrinLink"
13:43:25.714 OK - "CpmPlusKM_EventForwarder"
13:43:26.121 OK - Keeping Uninstalled : "EMO_CommonServices"
13:43:26.386 OK - Keeping Uninstalled : "EMO_ContractCalculation"
13:43:27.504 OK - "vtrin-NetSync"
13:43:27.597 OK: [16] application features "all" installed
=====
STARTING the RTDB service

SERVICE = RTDB D:\RTDBData
DSN = EDGE GATEWAY-97-RTDB
COMPUTER = EDGE GATEWAY-97

(Note: you should use "Stop RTDB" command first to verify
that no local applications are accessing the database before
the RTDB services are started. They could prevent ScanDB from
repairing possible inconsistencies).
=====
Continue to START ? (Y/N) : The RTDB D:\RTDBData service is starting.
The RTDB D:\RTDBData service was started successfully.

-----
You can now manage the RTDB services by using Control Panel/Services
and Task Manager.

While the program is running, RTDB is
checking the database consistency. The RTDB services are not yet available.
-----

Press any key to continue.

Edge Gateway - Change Admin Password X
Changing of Admin password finished
OK

```

Figure 19– Changing of admin password finished – Press OK

If the MNS Digital Edge is connected to the ABB Ability Cloud you must supply the password also for the NetSync Server synchronizing the data with the cloud:

Step	Actions	Remark
14	<ul style="list-style-type: none"> • Press (right mouse click) “Windows Symbol” - “Computer Management” “Disconnect” • Select “Services and Applications” – “Services” • Search for an entry starting with “Vtrin-NetSync” • Open “Properties” – “Log On” • Enter new Password to field “Password” and “Confirm Password” • Close Dialogue with “Ok” and close program 	The NetSync Server needs the credential of the CMES admin to read the local database and credentials.

4. Network connectivity

Since the MNS Digital Edge is connected to an Ethernet network it is customer's sole responsibility to provide and continuously ensure a secure connection between the MNS Digital Edge and customer network or any other network (as the case may be).

The MNS Digital Edge has following service ports open on the integrated Ethernet interfaces:

Port	Service	Purpose
443	https / wss	WEB user-interface of ABB Ability™ Condition Monitoring for electrical systems - CMES
3389	RDP	Windows remote login, e.g. used for the above described user password management

Customer shall establish and maintain appropriate measures (such as but not limited to the installation of firewalls, application of authentication measures, encryption of data, installation of antivirus programs, etc.) to protect the MNS Digital Edge including CMES, the network, its system and interfaces against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information.

ABB Ltd. and its affiliates are not liable for damages and/or losses related to such security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information.

5. Troubleshooting

Abbreviation	Solution
No access to CMES web page	Check if the correct IP address has been entered in the address bar of the web browser.
	Check if the MNS Digital Edge is powered on and no fault is indicated by the front LEDs.
	Ping the IP address of the MNS Digital Edge from the Web client PC
No login possible	Check if correct user name and password has been entered

Revision History

Rev.	Page	Change Description	Date / Initial
M0201	all	Initial release	2018-04-11 EPDS/KGM
M0202	8-15	Complexity Rules for passwords, Changing of administrator password using power shell script	2018-11-19 EPDS/JK



ABB

Publication Editor:
ABB Automation Products GmbH
Ladenburg, Germany

Local Contacts on
<http://www.abb.com/mns>