Getting Started with RUGGEDCOM CloudConnect

RUGGEDCOM RX1400

https://support.industry.siemens.com/cs/ww/en/view/109763521

Siemens Industry Online Support

Legal information

Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG ("Siemens"). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. You yourself are responsible for the proper and safe operation of the products in accordance with applicable regulations and must also check the function of the respective application example and customize it for your system.

Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. The application examples are not required to undergo the customary tests and quality inspections of a chargeable product; they may have functional and performance defects as well as errors. It is your responsibility to use them in such a manner that any malfunctions that may occur do not result in property damage or injury to persons.

Disclaimer of liability

Siemens shall not assume any liability, for any legal reason whatsoever, including, without limitation, liability for the usability, availability, completeness and freedom from defects of the application examples as well as for related information, configuration and performance data and any damage caused thereby. This shall not apply in cases of mandatory liability, for example under the German Product Liability Act, or in cases of intent, gross negligence, or culpable loss of life, bodily injury or damage to health, non-compliance with a guarantee, fraudulent non-disclosure of a defect, or culpable breach of material contractual obligations. Claims for damages arising from a breach of material contractual obligations shall however be limited to the foreseeable damage typical of the type of agreement, unless liability arises from intent or gross negligence or is based on loss of life, bodily injury or damage to health. The foregoing provisions do not imply any change in the burden of proof to your detriment. You shall indemnify Siemens against existing or future claims of third parties in this connection except where Siemens is mandatorily liable.

By using the application examples you acknowledge that Siemens cannot be held liable for any damage beyond the liability provisions described.

Other information

Siemens reserves the right to make changes to the application examples at any time without notice. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.

The Siemens terms of use (https://support.industry.siemens.com) shall also apply.

Security information

Siemens provides products and solutions with Industrial Security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the Internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at: https://www.siemens.com/industrialsecurity.

Security Disclaimer

This product makes available certain third party technology which is subject to separate license terms and conditions, including the following third party software license(s): Debian / Linux. By using such third party technology, you will have accepted the terms of such separate licenses and agreements, and you understand that Siemens is not responsible for the behavior or content of such third party technology or making security patches, updates or upgrades available.

Table of Contents

1 Introduction

1.1 Overview

This application description defines the steps to connect Industrial Internet of Things (IIoT) devices to various cloud services via the RUGGEDCOM CloudConnect VPE application.

The RUGGEDCOM RX1400 VPE is a virtual machine environment that supports Linux applications. The CloudConnect gateway application runs in this environment, and has its own Web-based user interface for configuration and maintenance.

This guide outlines the configuration steps (and examples) in the cloud service, the RUGGEDCOM RX1400, and the CloudConnect application to enable end-to-end communications from IIoT devices to the cloud service.

NOTE Registration with one of the supported cloud services is required.

1.2 CloudConnect for the RUGGEDCOM RX1400

The RUGGEDCOM RX1400 CloudConnect VPE application can be ordered from the factory pre-configured on a new RUGGEDCOM RX1400 device, or ordered as an electronic file that can be uploaded to an existing RUGGEDCOM RX1400.

The factory order option includes the RUGGEDCOM RX1400 device, an 8 GB industrial rated micro SD card, VPE license, and CloudConnect application pre-installed. The device comes pre-configured with VPE enabled and networking interfaces.

The upgrade option includes a VPE image and VPE license sent via electronic file transfer. The micro SD card is to be provided by the end user. A suggested RUGGEDCOM ROX II configuration is detailed in Section 2.2, “Configuring the RUGGEDCOM RX1400 VPE“.

Instructions for installing and updating virtual machine images are provided in the RUGGEDCOM ROX II User Guides.

1.3 Supported Cloud Services

At the time of publication, RUGGEDCOM CloudConnect supports the following cloud services:

- **Siemens MindSphere MS3.0 with Support for IOT Extension with MQTT**

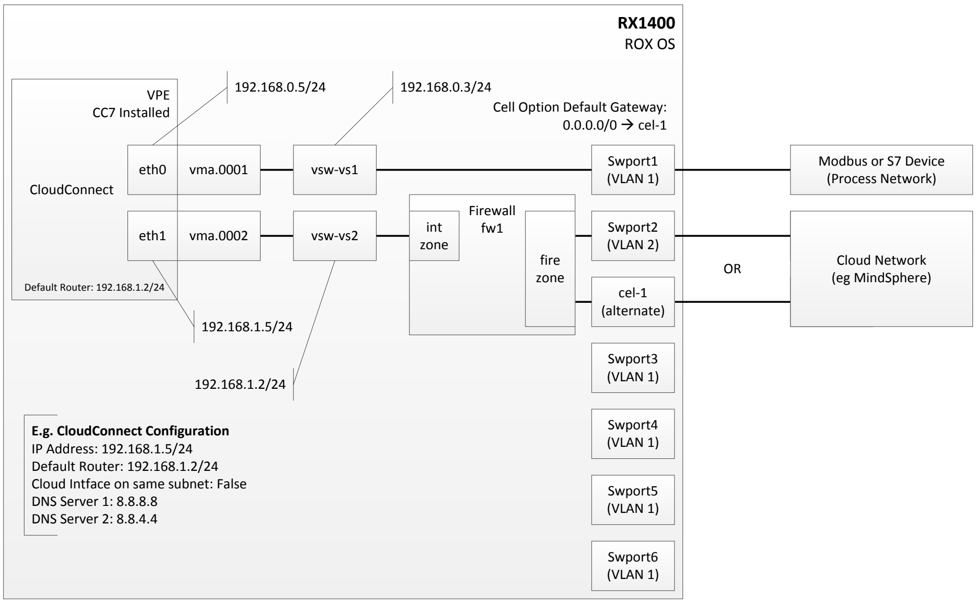
  https://documentation.mindsphere.io/resources/pdf/mindconnect-iot-extension-gs-en.pdf
- **Amazon Web Services (AWS) IoT Core**
  https://aws.amazon.com
- **Microsoft Azure IoT Hub**
  https://azure.microsoft.com/services/iot-hub/

For guidance on how to register with these services, refer to Section 2.3, “Configuring a Station“.

1.4 Default RUGGEDCOM RX1400 Factory Configuration

When RUGGEDCOM CloudConnect is ordered pre-installed at the factory, the RUGGEDCOM RX1400 is pre-configured to map virtual network interfaces to switch ports as shown:

Figure 1-1



E.g. CloudConnect Configuration
IP Address: 192.168.1.5/24
Default Router: 192.168.1.2/24
Cloud Intface on same subnet: False
DNS Server 1: 8.8.8.8
DNS Server 2: 8.8.4.4

1.5 Security Recommendations

- Configure a firewall on the RUGGEDCOM RX1400 device to control traffic from the VPE to the cloud.
- Consider securing the connection (e.g. with IPSec) between the VPE and IIoT devices, especially if the devices are not connected on the same local subnet.
- Check for updated firmware that may be available from Siemens. It is recommended the most up to date firmware/software is used as per the latest firmware release. By using outdated firmware versions, some available features may not be utilized and the absence of security updates or features may potentially expose your network to certain risks.
- Disable the DHCP client to avoid DHCP snooping. Do not expose DHCP enabled interfaces to the Internet or unknown networks. Use port security where available.
- Configure the Network Time Protocol (NTP) to help reject expired certificates.
- Make sure additional security recommendations defined in the RUGGEDCOM ROX II User Guides are followed.

1.6 Logging in to CloudConnect

To login to the CloudConnect user interface, do the following:

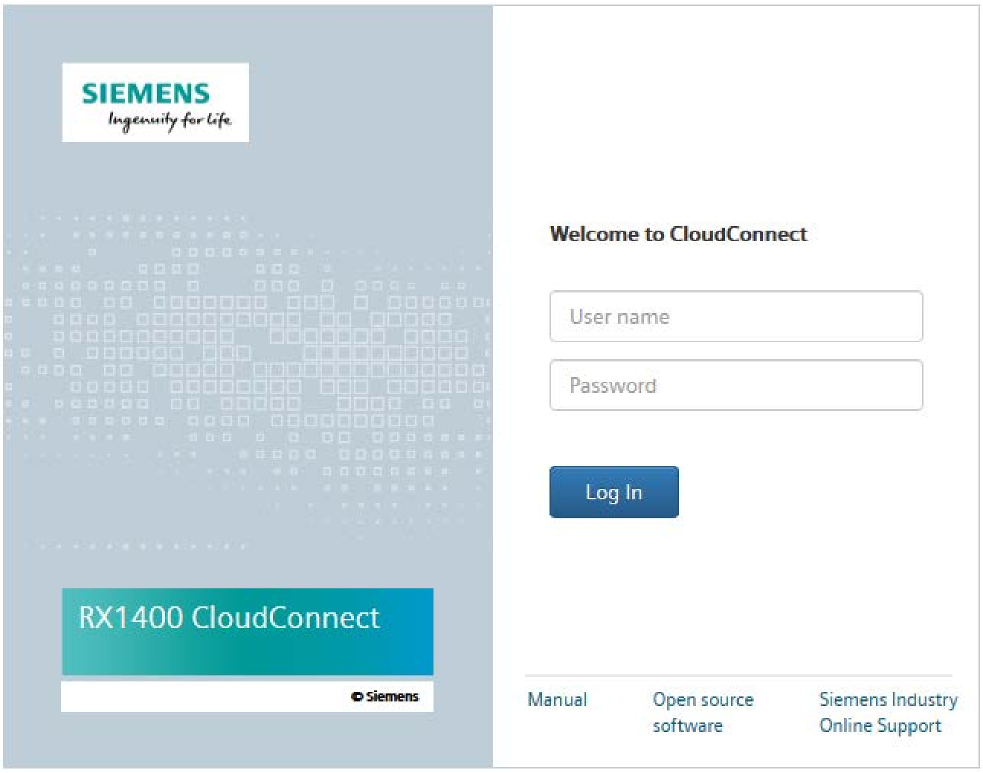
NOTE The CloudConnect user interface is available after step 2 in “General Procedure” is completed.

1. Open a browser via a computer on VLAN1 and enter the IP address for the CloudConnect service in the address bar. The default IP address for CloudConnect is 192.168.0.5.

2. At the login screen, enter your user name and password. The default credentials are:
   - User name: admin
   - Password: admin

   You will be prompted to change both the admin user name and password during the first login.

Figure 1-2



3. Click **Log In**.

2 Configuring CloudConnect

NOTE Tasks to be performed in the RUGGEDCOM ROX II user interface are described in as much detail as relates to this application. For further information about individual tasks, refer to the *RUGGEDCOM ROX II CLI* or *Web UI User Guide* for the RUGGEDCOM RX1400 available on the Siemens Industrial Online Support (SIOS) website [https://support.industry.siemens.com].

NOTE Tasks to be performed in CloudConnect are described in as much detail as relates to this application. For further information about individual tasks or specific parameters, refer to the *CloudConnect for RX1400 Configuration Manual* available through the user interface.

NOTE Refer to Figure 1-1 for an overview of the default RUGGEDCOM CloudConnect configuration for the RUGGEDCOM RX1400.

2.1 General Procedure

1. Register with one of the supported cloud service providers.
2. Configure the RUGGEDCOM RX1400 VPE.
   Refer to Section 2.2, "Configuring the RUGGEDCOM RX1400 VPE“.
3. Configure a Profile within CloudConnect for each registered cloud service.
   Refer to Section 2.3, "Configuring a Station".
4. Configure the chosen cloud service.
   Refer to Section 2.4, "Configuring Cloud Services".
5. Configure a profile in CloudConnect for each cloud service.
   Refer to Section 2.5, "Configuring Cloud Profiles Within CloudConnect".

2.2 Configuring the RUGGEDCOM RX1400 VPE

Complete the following tasks to configure the CloudConnect VPE application for the RUGGEDCOM RX1400:

1. Install the CloudConnect VPE application.
   Refer to Section 2.2.1, "Installing the CloudConnect VPE Application".
2. Define and enable virtual machine interfaces.
   Refer to Section 2.2.2, "Configuring Virtual Machine Interfaces".
3. Define virtual switches to bridge VMA and VLAN/routable interfaces.
   Refer to Section 2.2.3, "Configuring Virtual Switches".

If the device’s internal 4G LTE cellular modem is to be used to connect with CloudConnect services, perform the following additional steps:

1. Configure a cellular modem interface to allow the CloudConnect connection.
   Refer to Section 2.2.4, "Configuring a Cellular Modem Interface".
2. Configure a firewall to make sure traffic destined for the Internet is sent via the cellular modem interface.
   Refer to Section 2.2.5, "Configuring the Firewall".

NOTE Tasks performed in the RUGGEDCOM ROX II operating system are described in general. Further details are available in the RUGGEDCOM ROX II CLI or Web UI User Guides available on the Siemens Industrial Online Support (SIOS) website [http://support.industry.siemens.com].

2.2.1 Installing the CloudConnect VPE Application

Task

Install the CloudConnect VPE application on an existing RUGGEDCOM RX1400 device.

This step is not required if the application is installed at the factory.

Prerequisites

- RUGGEDCOM RX1400 running RUGGEDCOM ROX v2.11 (or higher)

Procedure

1. Order the CloudConnect application from Siemens Customer Support. Instructions on how to download the file will be provided.
2. Download the CloudConnect VPE image.
3. Save the image to a microSD/microSDHC card, formatted with the FAT32 or EXT4 file system.
4. Insert the microSD/microSDHC card into the RUGGEDCOM RX1400.
5. Follow the instructions in the *RUGGEDCOM ROX II User Guide* for adding a virtual machine image and extracting a virtual machine archive.

2.2.2 Configuring Virtual Machine Interfaces

Task

Define and enable the virtual machine interfaces **vma.0001** and **vma.0002** for the CloudConnect VPE application.

Procedure

For both vma.0001 and vma.0002, do the following:

1. Enable the virtual machine interface.
   Refer to instructions in the *RUGGEDCOM ROX II User Guide* for enabling/disabling a VPE network interface.
2. Add the virtual machine interface.
   Refer to instructions in the *RUGGEDCOM ROX II User Guide* for adding a virtual machine interface.

2.2.3 Configuring Virtual Switches

Task

Define virtual switches to bridge the two VMA interfaces and VLAN/routable interfaces.

Prerequisites

- RUGGEDCOM RX1400 running RUGGEDCOM ROX v2.11 (or higher)

Procedure

1. Login to the RUGGEDCOM RX1400 as an administrator.

2. Add the virtual network interfaces, vma.0001 and vma.0002, to the virtual machine configuration.
3. Create two virtual switches (e.g. **vs1** and **vs2**). The name of each is user-defined.
4. Assign a VLAN interface or routable interface, and the corresponding virtual network interface to each virtual switch interface (e.g. vma.0001 and switch.0001 to vsw-vs1, vma.0002 and switch.0002 to vsw-vs2).

NOTE Only IPv4 addresses are supported.

NOTE VPE interfaces (such as vma.0001) can only be assigned to a single virtual switch interface.

5. Assign IPv4 addresses to both virtual switch interfaces.

Example

```
ruggedcom(config)# show full-configuration interface virtualswitch
interface
 virtualswitch vs1
  no alias
  no proxyarp
  interface switch.0001
  !
  interface vma.0001
  !
 !
 virtualswitch vs2
  no alias
  no proxyarp
  interface switch.0002
  !
  interface vma.0002
  !
 !
!
```

```
ruggedcom(config)# show full-configuration ip vsw-vs1
ip vsw-vs1
 no bandwidth
 ipv4
  address 192.168.0.3/24
   no peer
  !
 !
 ipv6
  nd
   no enable-ra
   no adv-interval-option
   no home-agent-config-flag
   no managed-config-flag
   no other-config-flag
  !
 !
!

ruggedcom(config)# show full-configuration ip vsw-vs2
ip vsw-vs2
 no bandwidth
 ipv4
  address 192.168.1.2/24
   no peer
  !
 !
 ipv6
  nd
   no enable-ra
   no adv-interval-option
   no home-agent-config-flag
   no managed-config-flag
   no other-config-flag
  !
 !
!
```

2.2.4 Configuring a Cellular Modem Interface

Task

Define a cellular modem interface to a 4G LTE cellular network.

This step is only required if the device's internal 4G LTE cellular modem is to be used to connect with CloudConnect services.

Prerequisites

- RUGGEDCOM RX1400 running RUGGEDCOM ROX v2.10.0 (or higher)

Procedure

6. Login to the RUGGEDCOM RX1400 as an administrator.
7. Create a GSM profile for your telecom service provider with the following minimum settings:

Parameter	Description
apn	The name of the access point.
dial-string	The dial string provided by the wireless provider to connect to the access point. **Use the default setting.**
sim	The SIM index (1 or 2) to be used by the access point.

profile	The cellular connection profile.

8. Enable the cell modem interface.
9. Configure the PPP client and set it to connect to the GSM profile defined in step 2.
10. Configure a static route and assign it to the cellular modem interface (cel-1).
11. Verify the status of the cellular modem interface configuration.

Example

```
ruggedcom(config)# show full-configuration global cellular
global
 cellular profiles gsm telus
  apn SP.TELUS.COM
  ppp-config use-peer-dns
  no ppp-config dial-on-demand
  no ppp-config failover-on-demand
 !
!

ruggedcom(config)# show full-configuration interface cellmodem
interface
 cellmodem celport 1
  enabled
  no alias
  lte ppp-client connect-to telus
  lte firmware-update
   settings
    no repository-url
    mode manual-check-and-update
   !
  !
 !
!

ruggedcom(config)# show full-configuration routing ipv4
routing ipv4 route 0.0.0.0/0
 dev cel-1
  no distance
 !
!
```

2.2.5 Configuring the Firewall

Task

Define a firewall to provide a secure connection via the Internet between the cloud service and the CloudConnect application.

This step is only required if the device's internal 4G LTE cellular modem is to be used to connect with CloudConnect services.

Prerequisites

- RUGGEDCOM RX1400 running RUGGEDCOM ROX v2.11 (or higher)

Procedure

1. Login to the RUGGEDCOM RX1400 as an administrator.
2. Create a firewall configuration.
3. Create network zones named **fire** and **int**.

4. Add firewall interfaces for **cel-1** and **vsw-{interface}**, where {interface} is the virtual switch that is mapped to the CloudConnect cloud network interface, **vma.0002 (e.g. vsw-vs2)**.
5. Assign the interfaces to the **int** network zone.
6. Define the firewall policy. For example:
   - name: p1
   - source-zone: all
   - destination-zone: all
   - policy: accept
7. Define a MASQ rule with the following minimum settings:

Parameter	Description
out-interface	The outgoing interface. Set to **cel-1**.
source-hosts	A range and/or comma-separated list of subnet host IP addresses (i.e. CloudConnect's cloud network)

8. Validate the firewall configuration.
9. Enable the firewall configuration.

Example

```
ruggedcom(config)# show full-configuration security firewall
security
 firewall
  enable
  work-config   fw1
  active-config fw1
  fwconfig fw1
   fwzone fire
    type firewall
    no description
   !
   fwzone int
    no description
   !
   fwinterface cel-1
    zone int
    no description
   !
   fwinterface vsw-vs2
    zone int
    no description
   !
   fwpolicy p1
    source-zone all
    destination-zone all
    policy accept
    no description
   !
   fwmasq masq1
    out-interface cel-1
    no out-interface-specifics
    no ipalias
    source-hosts  192.168.1.0/24
    no address
    no description
   !
  !
 !
!
```

2.3 Configuring a Station

Task

Configure a station (end device) to communicate with CloudConnect via Modbus TCP or the S7 protocol.

Prerequisites

- A RUGGEDCOM RX1400 with the CloudConnect application installed
- A Modbus TCP or S7 remote device

Procedure

1. Login to the CloudConnect user interface as the *admin* user.
1. Navigate to **Process Access > Station Configuration**.
2. Under **Station name**, enter a station name.
3. On the **Settings** tab, select **Modbus/TCP** or **S7 protocol**.
4. On the **Modbus/TCP** or **S7** tab, configure the protocol. For more information, refer to the *RX1400 with CloudConnect Configuration Manual* available via the user interface.

2.4 Configuring Cloud Services

This section provides examples of how to configure each supported cloud service. For each service, a certificate must be defined to authenticate CloudConnect clients.

NOTE Each service offers multiple configuration options, such as generating a certificate or using a CA certificate provided by the user. The procedures described below only use a subset of the available options to demonstrate one way of configuring each cloud service. For more information, refer to the user documentation provided by each cloud service.

NOTE Procedures provided are considered accurate at the time of publication.

2.4.1 Configuring Siemens MindSphere with MindConnect IOT Extension

Overview

To enable an MQTT device connection with MindSphere, the MindConnect IoT Extension is required to be added to the MindSphere tenant. Information on how to activate the MindConnect IOT Extension is included in the “Welcome to MindSphere” email.

NOTE When properly configured, the RUGGEDCOM RX1400 with CloudConnect application will automatically create a device in the MindConnect IoT extension, with the device name entered in the CloudConnect user interface.

Task

Login to MindConnect IoT Extension and note the URL. Download the server certificate from the MindSphere tenant.

NOTE Only download the server certificate if TLS authentication is enabled.

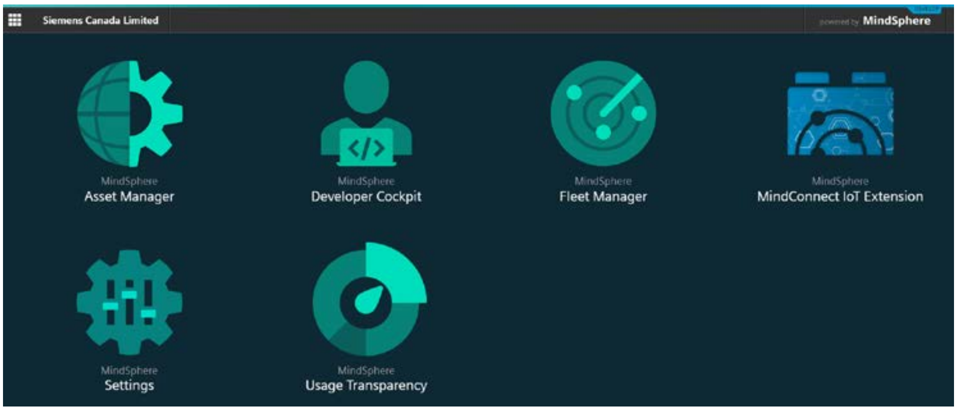
Prerequisites

- A MindSphere tenant with MindConnect IoT Extension enabled

Procedure

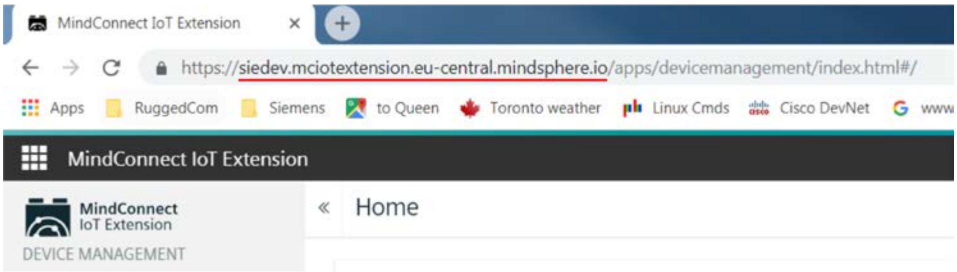
1. Login to the MindSphere tenant portal. Click **MindConnect IoT Extension**.

Figure 2-1



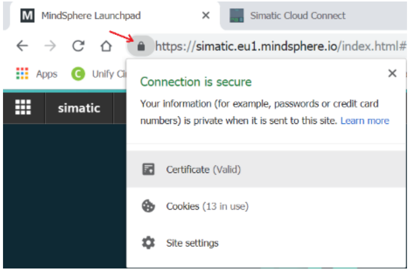
2. Login to MindConnect IoT Extension and note the URL. For example: *siedev.mciotextension.eu-central.minsphere.io*

Figure 2-2


MindConnect IoT Extension
https://siedev.mciotextension.eu-central.mindsphere.io/apps/devicemanagement/index.html#/
Apps
RuggedCom
Siemens
to Queen
Toronto weather
Linux Cmds
Cisco DevNet
www
MindConnect IoT Extension
MindConnect IoT Extension
DEVICE MANAGEMENT
Home

3. Temporarily record the URL in a text file.
4. **[OPTIONAL]** To use the encrypted MQTT communication over TLS, import the server certificate to the client.
   a. Click the secure icon on your browser.

Figure 2-3

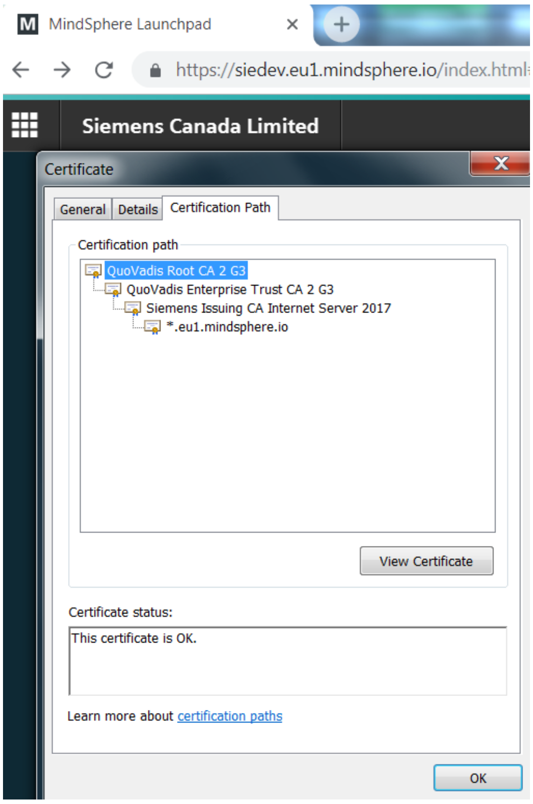


Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

   b. Click the **Certification Path** tab, select **QuoVadis Root CA 2 G3**, and then click **View Certificate**.

Figure 2-4



Certification path

- QuoVadis Root CA 2 G3
  - QuoVadis Enterprise Trust CA 2 G3
    - Siemens Issuing CA Internet Server 2017
      - *.eu1.mindsphere.io

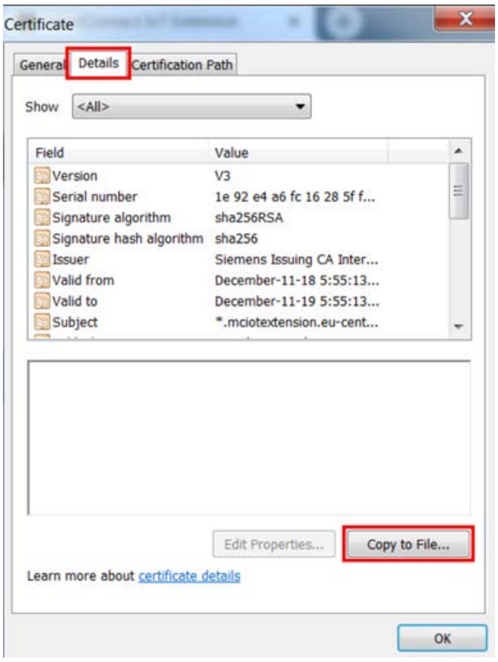
Certificate status:

This certificate is OK.

Learn more about certification paths

c. In the **Certificate** dialog, click the **Details** tab and then click **Copy to File**.

Figure 2-5



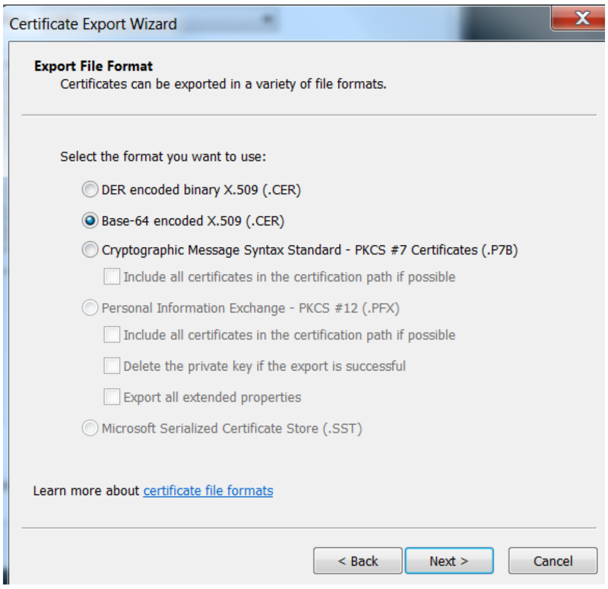
Show <All>

Field	Value
Version	V3
Serial number	1e 92 e4 a6 fc 16 28 5f f...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Siemens Issuing CA Inter...
Valid from	December-11-18 5:55:13...
Valid to	December-11-19 5:55:13...
Subject	*.mciotextension.eu-cent...

Learn more about certificate details

d. Select **Base-64-encoded X.509 (.CER)** and then click **Next**.

Figure 2-6



Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

● Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

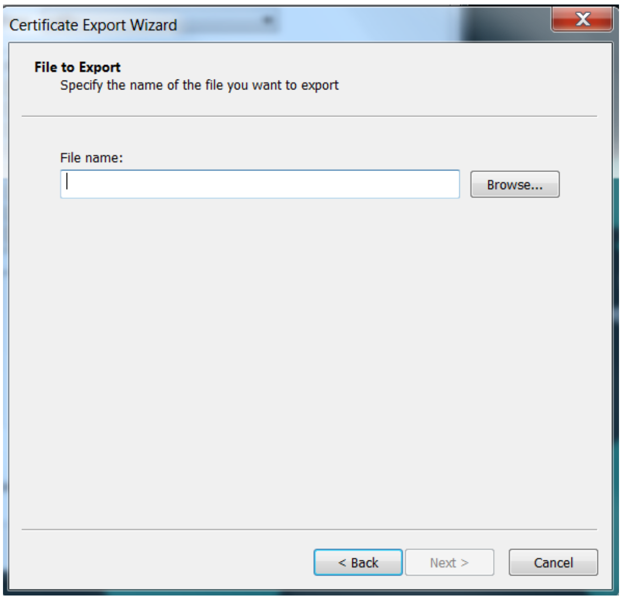
□ Export all extended properties

○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

e. Under **File Name**, enter the location where the server certificate will be saved, as well as the file name.

Figure 2-7



File to Export
Specify the name of the file you want to export

File name:

f. Click **Next** and then follow the remaining on-screen instructions to complete the process.

2.4.2 Configuring AWS IoT Core

Overview

Following the successful registration with the Amazon Web Service (AWS), a “thing” must be created within AWS. The thing defines the certificate and policies used to authenticate clients.

NOTE A dedicated “thing” is required for each device. AWS allows individual “things” to support multiple clients, but this is only recommended for testing purposes.

Task

Define a “thing“ that uses an X.509 certificate.

NOTE AWS also supports certificates signed by a Certificate Authority.

Prerequisites

- An AWS account

Procedure

1. Login to the AWS portal.
2. Under **AWS services**, search for “IoT Core” and then select the IOT core option. The AWS IoT Console page appears.
3. Register a new thing:
   a. Select **Manage** from the menu.
   b. On the **Manage** page, click **Register a thing**.
   c. Click **Create a single thing**.
   d. On the **Create a thing** page, define a name for the thing and then click **Next**.
   e. On the next page, click **Create Certificate**. A certificate, private key, and public key are generated.
   f. Download the three files. These are required to later connect to the cloud service.
   g. Click **Activate** to activate the certificate.
   h. Click **Done** to create the thing.
4. Define a policy for the thing:
   a. Navigate to **Secure > Policies**.
   b. On the **Policies** page, create a new policy and give it a name.
   c. Under **Action**, enter “iot:*”. This indicates that clients can subscribe and publish to the thing.
   d. Under Resources, enter “*”. This indicates the thing is accessible to all clients who have access to the certificate.
   e. Select **Allow**.
   f. Click **Create** to create the policy.
5. Attach the policy to the certificate:
   a. Navigate to **Secure > Certificates**.
   b. Select **Options** next to the policy marked Active.
   c. In the options, select **Attach Policy**, choose the policy, and then click **Attach**.
6. Obtain the broker address for the thing:
   a. Navigate to **Manage > Things** and select the new thing.
   b. Select **Interact**. The links required to access the thing are displayed.
   c. Copy the HTTPS link/Rest API Endpoint and save it temporarily (e.g in a text file). This link will be required to later configure CloudConnect.

2.4.3 Configuring Microsoft Azure IoT Hub

Overview

Microsoft Azure allows devices to communicate with IoT Hub device endpoints using either:

- MQTT v3.1.1 on port 8883
- CA-signed X.509 certificate and SAS tokens

This section describes how to configure an IoT Hub that will authenticate a device using a self-signed X.509 certificate.

NOTE A dedicated IoT Hub is required for each device.

Task

Define a Microsoft Azure-specific profile via the CloudConnect service for the RUGGEDCOM RX1400.

Prerequisites

- A Microsoft Azure account

Procedure

1. Login to the Microsoft Azure portal.
2. Choose **Create a resource**, and then select **Internet of Things**.
3. Create an IoT hub.
4. Define a unique name and resource group for the IoT Hub.
5. From the dashboard, select the IoT hub created in step 3.
6. Navigate to the IoT device explorer.
7. Click **Add** to add a new device.
8. Under **Device ID**, assign a name to the device.
9. Under **Authentication Type**, select **X.509 Self Signed**.
10. If a Certificate Authority (CA) is being used, follow the instructions available at https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-security-x509-get-started#createdevice to use an X.509 CA certificate.
11. Generate or use an existing self-signed certificate and set the primary and secondary thumbprint to the certificate’s thumbprint.
12. Click **Save**.

2.5 Configuring Cloud Profiles Within CloudConnect

Following the successful registration with and configuration of a cloud service, a profile must be configured within CloudConnect.

2.5.1 Configuring CloudConnect for Siemens MindSphere with MindConnect IoT Extensions

Task

Create a profile within CloudConnect for Siemens MindSphere.

Prerequisites

- A RUGGEDCOM RX1400 with the CloudConnect application installed and configured
- The server certificate obtained from MindSphere in Section 2.4.1, step 4
- A remote device with data points configured in CloudConnect

Procedure

1. Login to the CloudConnect user interface as the *admin* user.
2. Navigate to **Cloud Configuration - Profile**.
3. Create a new profile and configure as follows:
   - Under **Profile:**
     a. Enter and profile name and then click **Add**.
   - Under **Settings**:
     a. Set **Cloud Provider** to *MindConnect IOT Extension*.
     b. Set **Protocol** to *MQTT*.
     c. Select **Enable Profile**.
   - Under **MQTT Configuration**:
     a. Set MQTT version to v3.1.1.
     b. Set Broker address to the URL of your MindConnect IOT Extension.

        Example: `siedev.mciotextension.eu-central.mindsphere.io`
     c. If encrypted communication over TLS is not used, clear TLS and set Broker port to 1883.
     d. If encrypted communication over TLS is used, set Broker port to 8883, select TLS, and then set TLS version to TLS v1.2.
     e. Under **Client ID**, enter the name of the device that will be created in the MindConnect IOT Extension.
     f. Select **Authentication**.
     g. Enter your user name and password for the MindConnect IoT Extension.

        Note the user name must be in the form of *{tenant}/{email}*. For example: `siedev/john.doe@siemens.com`.
     h. Click **Save**.
   - Under **Security Settings:**
     a. Choose the server certificate exported previously in Section 2.4.1, step 4c.

        Import the server certificate.
     b. Click **Save**.
   - Under **Onboarding:**
     a. Under **Device name**, enter the same name entered under **Client ID** under the **MQTT Configuration** settings. This name will be used for creating a device in the MIndConnect IoT Extension after the onboarding was completed. The Client ID must match the Client ID entered in step e under **MQTT Configuration** above.
     b. Click **Save**.
4. Click **Save**.

5. Navigate to **Data and Topics > Data Points** and add one or more data points by entering a name, selecting its data type, the operand, the DB number (if the operant DB has been selected) and the offset.
6. Configure at least one trigger in CloudConnect to send the data to the cloud.
7. Add groups:
   a. Navigate to **Data and Topics > Topic Editor**.
   b. Add one or more groups.

NOTE By default, all groups have the topic “s/us”. MindSphere supports only one topic, unlike other cloud services.

NOTE Each data point can be assigned to a different group.

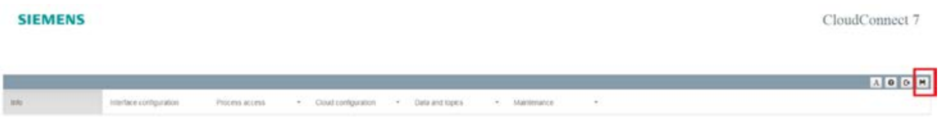
An attribute value is required for each data point.

   c. Assign each group to a data point and enter the correct attribute. For example, setting the attribute to “C” will cause the data point to display a temperature in degrees Celsius.

NOTE Only change the payload if the consequences are fully understood.

8. Select the correct payload. By default, the payload format for MindConnect IoT Extension will be used. Open the payload editor to select a different payload from a series of available templates or define a custom payload.
9. Click **Apply Settings** to apply the updated settings to CloudConnect. CloudConnect will connect to the configured cloud with its configurations.

Figure 2-8



For more information, refer to the *RX1400 with CloudConnect Configuration Manual*.

2.5.2 Configuring CloudConnect for AWS

Task

Create a profile within CloudConnect for AWS.

Prerequisites

- A RUGGEDCOM RX1400 with the CloudConnect application installed and configured.
- The certificate, private key, and root CA required by AWS thing to authenticate CloudConnect clients.
- A Modbus or S7 remote device with data points configured in Cloud Connect.

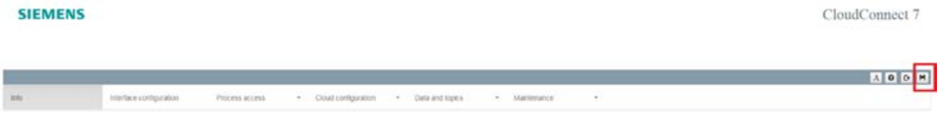
Procedure

1. Login to the CloudConnect WebUI as the *admin* user.
2. Navigate to the **Cloud Configuration – Profile**.
3. Create a new profile and configure it as follows:

- Under **Profile:**
    a. Enter and profile name and then click **Add**.
- Under **General Settings**:
    a. Set **Cloud Provider** to *AWS*.
    b. Set **Select Protocol** to *MQTT*.
    c. Select **Enable Profile**.
- Under **MQTT Configuration**:
    d. Set **MQTT Protocol version** to *v3.1*.
    e. Set **Broker Address** as the HTTPS link/Rest API Endpoint obtained when creating the AWS thing.
    f. Set **Broker Port** as *8883*.
    g. Select **Clean Session**.
    h. Select **Enable TLS**.
    i. Set **TLS Version** to *TLS v1.2*.

4. Click **Save**.
5. On the **Security Settings** tab, set the security settings:
    a. Import the AWS root CA certificate as the server certificate.
    b. Select **Use MQTT Client Certificate**.
    c. Import the AWS generated self-signed client certificate.
    d. Import the AWS generated self-signed private key.
6. Click **Save**.
7. Under **Data Topics – Topic Editor** in CloudConnect, add a new topic and then assign datapoints to the topic.
8. Click **Apply Settings** to apply the updated settings. CloudConnect will connect to the configured cloud with its configurations.

Figure 2-9



For more information, refer to the *RX1400 with CloudConnect Configuration Manual*.

2.5.3 Configuring CloudConnect for Microsoft Azure

Task

Create a profile within CloudConnect for Microsoft Azure.

Prerequisites

- A RUGGEDCOM RX1400 with the CloudConnect application installed and configured.
- The DigiCert Baltimore Root Certificate required by the IoT Hub to secure the connection. This certificate is available through the IoT Hub in the Microsoft Azure portal under the Azure-iot-sdk-c repository.
- A Modbus or S7 remote device with data points configured in Cloud Connect.

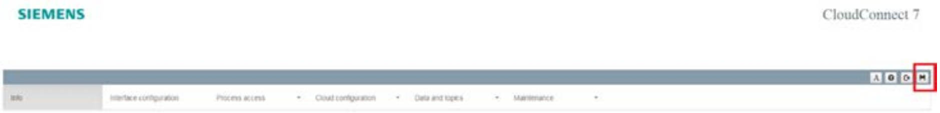
Procedure

1. Login to the CloudConnect WebUI as the *admin* user.
2. Navigate to **Cloud Configuration – Profile.**
3. Create a new profile and configure it as follows:
   - Under **Profile:**
     a. Enter and profile name and then click **Add**.
   - Under **General Settings**:
     a. Set **Cloud Provider** to *Azure*.
     b. Set **Select Protocol** to *MQTT*.
     c. Select **Enable Profile**.
   - Under **MQTT Configuration**:
     a. Set **MQTT Protocol version** to *v3.1.1*.
     b. Set **Broker Address** as the IoT Hub host name.
     c. Set **Broker Port** as *8883*.
     d. Set **Client ID** to the device ID create in the IoT Hub.
     e. Select **Enable Authentication**.
     f. Set **Username** to *{iothubhostname}/{device_id}/api-version=2016-11-14*, where *{iothubhostname}* is the full CName of the IoT hub.
     g. Leave **Password** blank to allow for authentication via the certificate.
     h. Select **Clean Session**.
     i. Select **Enable TLS**.
     j. Set **TLS Version** to *TLS v1.2*.
   - Under **Security Settings**:
     a. Under the **MQTT Server Certificate Manager**, import the DigiCert Baltimore Root Certificate.
     b. Under the **MQTT Client Certificate Manager**, import the self-signed certificate and private key.
4. Click **Save**.
5. Under the **Data Topics – Topic Editor** in CloudConnect, add a new topic with the following name:

```
devices/{device_id}/messages/events/
```

6. Assign datapoints to the topic.
7. Click **Apply Settings** to apply the updated settings to CloudConnect. CloudConnect will connect to the configured cloud with its configurations.

Figure 2-10



For more information, refer to the *RX1400 with CloudConnect Configuration Manual*.

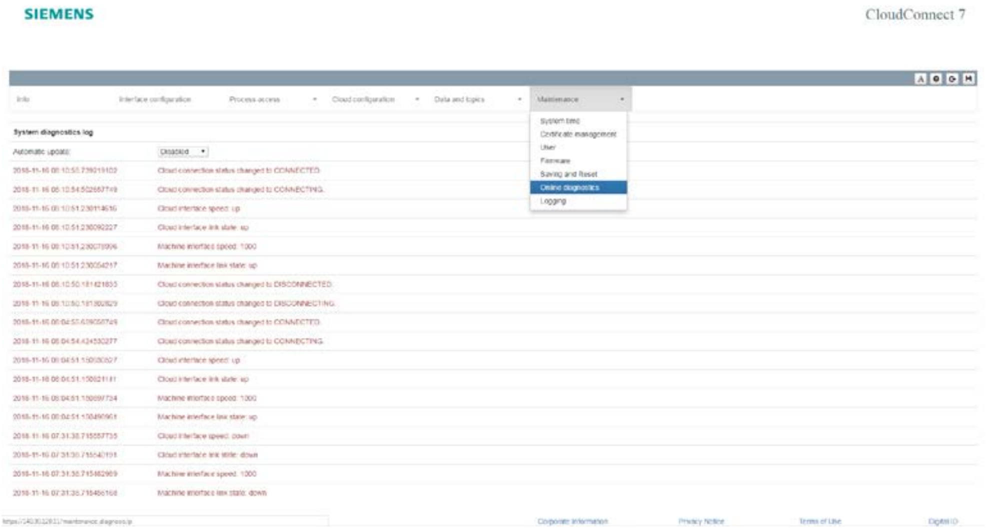
3 Online Diagnostics

CloudConnect offers a system diagnostic log under **Maintenance > Online Diagnostics**. The log provides important information for system administrators.

The log is refreshed automatically at a user-defined interval. It can also be disabled, if desired.

For more information, refer to the *RX1400 with CloudConnect Configuration Manual*.

Figure 3-1



System diagnostics log

Automatic update: Disabled

```
2018-11-16 08:10:55.739219102    Cloud connection status changed to CONNECTED.
2018-11-16 08:10:54.502667749    Cloud connection status changed to CONNECTING.
2018-11-16 08:10:51.230114616    Cloud interface speed: up
2018-11-16 08:10:51.230092227    Cloud interface link state: up
2018-11-16 08:10:51.230078996    Machine interface speed: 1000
2018-11-16 08:10:51.230054217    Machine interface link state: up
2018-11-16 08:10:50.181421835    Cloud connection status changed to DISCONNECTED.
2018-11-16 08:10:50.181392829    Cloud connection status changed to DISCONNECTING.
2018-11-16 08:04:55.609058749    Cloud connection status changed to CONNECTED.
2018-11-16 08:04:54.424530277    Cloud connection status changed to CONNECTING.
2018-11-16 08:04:51.150030827    Cloud interface speed: up
2018-11-16 08:04:51.150021181    Cloud interface link state: up
2018-11-16 08:04:51.150097734    Machine interface speed: 1000
2018-11-16 08:04:51.150490961    Machine interface link state: up
2018-11-16 07:31:38.715557735    Cloud interface speed: down
2018-11-16 07:31:38.715540191    Cloud interface link state: down
2018-11-16 07:31:38.715482969    Machine interface speed: 1000
2018-11-16 07:31:38.715456168    Machine interface link state: down
```

https://140.30.129.11/maintenance_diagnosis.jsp

4 Updating the CloudConnect Application

Updates to the CloudConnect application are available through Siemens Customer Support.

To update the CloudConnect application, do the following:

1. Order the updated CloudConnect application from Siemens Customer Support. Instructions on how to download the file will be provided.
2. Download the CloudConnect VPE image.
3. In the CloudConnect user interface, navigate to **Maintenance > Saving and Reset** and then click **Save to PC** to backup the configuration file.
4. In RUGGEDCOM ROX II:
    a. Backup the configuration.
    b. Stop the virtual machine.
5. Remove the microSD/microSDHC card from the RUGGEDCOM RX1400.
6. Access the microSD/microSDHC card and delete the *cc7* folder.
7. Add the image to the microSD/microSDHC card
8. Insert the microSD/microSDHC card into the RUGGEDCOM RX1400.
9. Follow the instructions in the *RUGGEDCOM ROX II User Guide* for adding a virtual machine image and extracting a virtual machine archive.
10. Startup the virtual machine and then login to the CloudConnect user interface.
11. Navigate to **Maintenance > Saving and Reset** and load the backup configuration file.

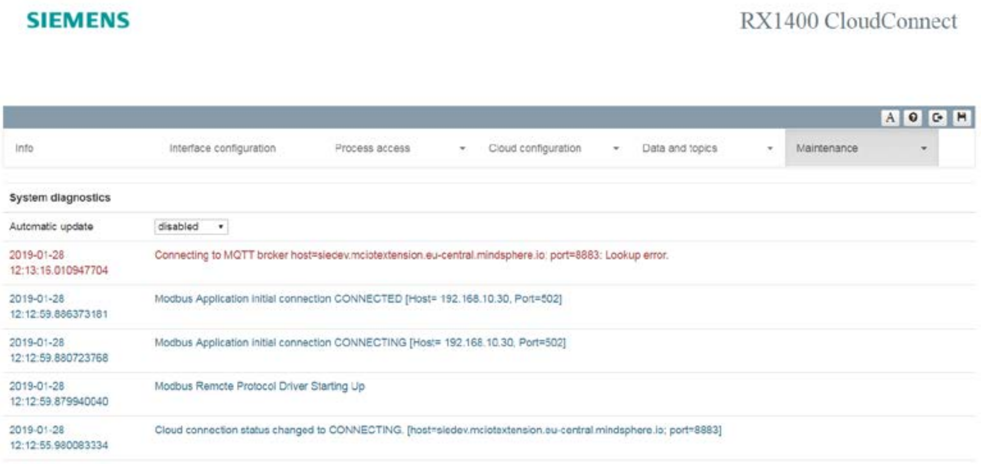
5 Appendix

5.1 Troubleshooting

5.1.1 Online Diagnostics

The CloudConnect application contains built in diagnostics to aid in troubleshooting of setup and configuration. The online diagnostics can be accessed via the **Maintenance** tab under **Online Diagnostics**,

Figure 5-1



System diagnostics

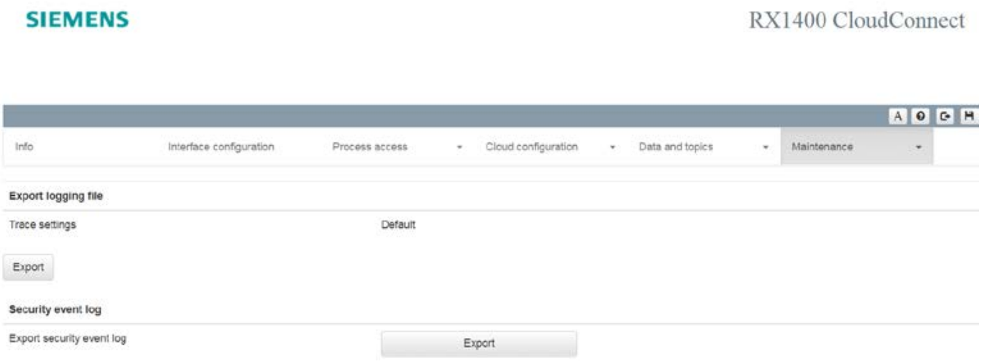
Automatic update	disabled
2019-01-28 12:13:16.010947704	Connecting to MQTT broker host=siedev.mciotextension.eu-central.mindsphere.io; port=8883: Lookup error.
2019-01-28 12:12:59.886373181	Modbus Application initial connection CONNECTED [Host= 192.168.10.30, Port=502]
2019-01-28 12:12:59.880723768	Modbus Application initial connection CONNECTING [Host= 192.168.10.30, Port=502]
2019-01-28 12:12:59.879940040	Modbus Remote Protocol Driver Starting Up
2019-01-28 12:12:55.980083334	Cloud connection status changed to CONNECTING. [host=siedev.mciotextension.eu-central.mindsphere.io; port=8883]

The online diagnostics can be configured to update via the **Automatic update** selection.

5.1.2 Log Files

To aid in troubleshooting, a trace log and security event log can be exported from CloudConnect to assist Siemens support with troubleshooting issues. These log files may be exported from the **Maintenance** tab under **Logging**,

Figure 5-2



Export logging file

Trace settings Default

Security event log

Export security event log

5.1.3 Connecting to the CloudConnect Linux Console

More advanced troubleshooting of networking issues may require access to the Linux console underlying the CloudConnect application in the Virtual Processing

Engine. This console can be accessed from the RUGGEDCOM ROX II command line interface using the `vm-console` command:

```
ruggedcom# vm-console
```

The default credentials are

- User: cloudconn
- Password: cc7+123

The following `sudo` commands are available for troubleshooting:

- **Using CloudConnect**

```
service cc_admin *
service civetweb *
service networking *
```

- **Emergency Network Configuration**

```
chown cloudconn /etc/network/interfaces
chown cloudconn /etc/network/interfaces.d
chown cloudconn /etc/network/interfaces.d/*
chown cloudconn /etc/resolv.conf
touch /etc/resolv.conf
touch /etc/network/interfaces
vi /etc/network/interfaces
vi /etc/hosts
vi /etc/resolv.conf

ip addr flush dev *
ifup *
ifdown *
```

- **Debian Updates**

```
apt-get update
apt-get upgrade
apt-get dist-upgrade
```

- **General**

```
reboot
ifconfig *
ping *

mv /etc/localtime /etc/localtime.old
rm /etc/localtime.old
mv /etc/localtime *
ln *
unlink *
date *
```

5.2 Service and Support

Industry Online Support

Do you have any questions or need assistance?

Siemens Industry Online Support offers round the clock access to our entire service and support know-how and portfolio.

The Industry Online Support is the central address for information about our products, solutions and services.

Product information, manuals, downloads, FAQs, application examples and videos – all information is accessible with just a few mouse clicks:
https://support.industry.siemens.com/

Technical Support

The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers – ranging from basic support to individual support contracts. Please send queries to Technical Support via Web form:
https://www.siemens.com/industry/supportrequest

SITRAIN – Training for Industry

We support you with our globally available training courses for industry with practical experience, innovative learning methods and a concept that's tailored to the customer's specific needs.

For more information on our offered trainings and courses, as well as their locations and dates, refer to our web page:
https://www.siemens.com/sitrain

Service offer

Our range of services includes the following:

- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts

You can find detailed information on our range of services in the service catalog web page:
https://support.industry.siemens.com/cs/sc

Industry Online Support app

You will receive optimum support wherever you are with the "Siemens Industry Online Support" app. The app is available for Apple iOS, Android and Windows Phone:
https://support.industry.siemens.com/cs/ww/en/sc/2067

5.3 Links and Literature

Table 5-1

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to this entry page of this application example https://support.industry.siemens.com/cs/ww/en/view/109763521

No.	Topic
\3\	RUGGEDCOM RX1400 Installation Guide https://support.industry.siemens.com/cs/ww/en/view/109480955
\4\	RX1400 with CloudConnect Configuration Manual (Available via the CloudConnect user interface)
\5\	RUGGEDCOM ROX II User Guides (Available via Siemens Industry Online Support website)

5.4 Change Documentation

Table 5-2

Version	Date	Modifications
V1.0	02/2019	First version