

**SIEMENS**

Getting Started

# SIMATIC NET

Industrial Ethernet - Cloud

CloudConnect for RUGGEDCOM RX1400

Edition

06/2021

<https://www.siemens.com>

# SIEMENS

## SIMATIC NET

### Industrial Ethernet - Cloud CloudConnect for RUGGEDCOM RX1400

Getting Started

Preface	
Introduction	1
Configuring CloudConnect	2
Updating CloudConnect	3
Troubleshooting	4

## Legal Information

### Warning Notice System

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

 <b>DANGER</b>
---

indicates that death or severe personal injury will result if proper precautions are not taken.
---

 <b>WARNING</b>
--

indicates that death or severe personal injury may result if proper precautions are not taken.
--

 <b>CAUTION</b>
--

indicates that minor personal injury can result if proper precautions are not taken.
--

 <b>NOTICE</b>
---

indicates that property damage can result if proper precautions are not taken.
--

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

### Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

### Proper Use of Siemens Products

Note the following:

 <b>WARNING</b>
--

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.
--

### Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

### Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

# Table of Contents

<b>Preface</b> .....	<b>v</b>
Related Documents .....	v
Training .....	v
Customer Support .....	vi
Contacting Siemens .....	vi
<b>1 Introduction</b> .....	<b>1</b>
1.1 CloudConnect on the RUGGEDCOM RX1400 .....	1
1.2 Supported Cloud Services .....	1
1.3 Default Factory Configuration .....	2
1.4 Security Recommendations .....	2
1.5 Logging In to CloudConnect .....	3
<b>2 Configuring CloudConnect</b> .....	<b>5</b>
2.1 Configuring the RUGGEDCOM RX1400 .....	6
2.1.1 Installing the CloudConnect Application .....	6
2.1.2 Configuring Virtual Machine Interfaces .....	7
2.1.3 Configuring Virtual Switches .....	7
2.1.4 Configuring the Cellular Modem Interface .....	9
2.1.5 Configuring a Firewall .....	11
2.2 Configuring a Station .....	12
2.3 Configuring Cloud Services .....	13
2.3.1 Configuring MindConnect .....	13
2.3.1.1 Obtaining the MindConnect IoT Extension URL .....	14
2.3.1.2 Obtaining the MindConnect IoT Extension Server Certificate .....	15
2.3.2 Configuring AWS IoT Core .....	19
2.3.3 Configuring Microsoft Azure IoT Hub .....	20
2.4 Configuring Cloud Profiles Within CloudConnect .....	21
2.4.1 Configuring CloudConnect for Siemens MindSphere with the MindConnect IoT Extension .....	21
2.4.2 Configuring CloudConnect for AWS .....	25
2.4.3 Configuring CloudConnect for Microsoft Azure .....	26
2.5 Resetting the Password .....	28
<b>3 Updating CloudConnect</b> .....	<b>29</b>
<b>4 Troubleshooting</b> .....	<b>31</b>
4.1 Online Diagnostics .....	31
4.2 Log Files .....	31
4.3 Connecting to the CloudConnect Linux Console .....	32



# Preface

This document describes the installation and configuration of CloudConnect on the RUGGEDCOM RX1400. It is intended for use by network technical support personnel who are familiar with the operation of networks. It is also recommended for use by network and system planners, system programmers, and line technicians.

## Related Documents

The following are other documents related to this product that may be of interest. Unless indicated otherwise, each document is available on the [Siemens Industry Online Support \(SIOS\)](https://support.industry.siemens.com) [<https://support.industry.siemens.com>] website.

---

**Note**

Documents listed are those available at the time of publication. Newer versions of these documents or their associated products may be available. For more information, visit SIOS or consult a Siemens Customer Support representative.

---

## Product Notes

Product notes are available online via [SIOS](https://support.industry.siemens.com/cs/ca/en/ps/16008/pm) [<https://support.industry.siemens.com/cs/ca/en/ps/16008/pm>].

## Configuration/Reference Manuals

Document Title	Link
RX1400/APE1808 with CloudConnect Configuration Manual	Available via the CloudConnect application
RUGGEDCOM ROX II Configuration Manuals	<a href="https://support.industry.siemens.com/cs/ca/en/ps/15989/man">https://support.industry.siemens.com/cs/ca/en/ps/15989/man</a>

## Installation Manuals

Document Title	Link
RUGGEDCOM RX1400 Installation Manual	<a href="https://support.industry.siemens.com/cs/us/en/view/109480955">https://support.industry.siemens.com/cs/us/en/view/109480955</a>

## Training

Siemens offers a wide range of educational services ranging from in-house training of standard courses on networking, Ethernet switches and routers, to on-site customized courses tailored to the customer's needs, experience and application.

Siemens' Educational Services team thrives on providing our customers with the essential practical skills to make sure users have the right knowledge and expertise to understand the various technologies associated with critical communications network infrastructure technologies.

Siemens' unique mix of IT/Telecommunications expertise combined with domain knowledge in the utility, transportation and industrial markets, allows Siemens to provide training specific to the customer's application.

For more information about training services and course availability, visit <https://www.siemens.com> or contact a Siemens Sales representative.

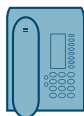
## Customer Support

Customer support is available 24 hours, 7 days a week for all Siemens customers. For technical support or general information, contact Siemens Customer Support through any of the following methods:



### Online

Visit <http://www.siemens.com/automation/support-request> to submit a Support Request (SR) or check on the status of an existing SR.



### Telephone

Call a local hotline center to submit a Support Request (SR). To locate a local hotline center, visit [https://w3.siemens.com/aspa\\_app/?lang=en](https://w3.siemens.com/aspa_app/?lang=en).



### Mobile App

Install the Industry Online Support app by Siemens AG on any Android, Apple iOS or Windows mobile device and be able to:

- Access Siemens' extensive library of support documentation, including FAQs and manuals
- Submit SRs or check on the status of an existing SR
- Contact a local Siemens representative from Sales, Technical Support, Training, etc.
- Ask questions or share knowledge with fellow Siemens customers and the support community

## Contacting Siemens

<b>Address</b>	Siemens AG Industry Sector 300 Applewood Crescent Concord, Ontario Canada, L4K 5C7
<b>Telephone</b>	Toll-free: 1 888 264 0006 Tel: +1 905 856 5288

	Fax: +1 905 856 1995
<b>E-Mail</b>	<a href="mailto:info.ruggedcom@siemens.com">info.ruggedcom@siemens.com</a>
<b>Web</b>	<a href="https://www.siemens.com">https://www.siemens.com</a>





# Introduction

CloudConnect on the RUGGEDCOM RX1400 connects Industrial Internet of Things (IIoT) devices to various cloud services.

The RUGGEDCOM RX1400 features a Virtual Processing Engine (VPE) 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 Getting Started guide outlines the configuration steps required to enable end-to-end communications between IIoT devices and the cloud service.

---

**Note**

Registration with one of the supported cloud services is required.

---

## 1.1 CloudConnect on the RUGGEDCOM RX1400

The RUGGEDCOM RX1400 can be ordered with CloudConnect pre-installed and configured. CloudConnect can also be ordered as a virtual machine image to install on an existing device.

- When ordering the RUGGEDCOM RX1400 with CloudConnect, you receive the device, an 8 GB industrial rated microSD card, the VPE license, and the CloudConnect application pre-installed. The VPE is enabled by default and all networking interfaces are configured.

The only configuration required is to create a station, configure the chosen cloud service, and create a cloud profile.

- When ordering CloudConnect as a separate virtual machine image, you receive the VPE image and license sent via electronic file transfer. The image and license must be uploaded to a RUGGEDCOM RX1400 and configured.

For information about how to configure the CloudConnect application, refer to "[Configuring the RUGGEDCOM RX1400 \(Page 6\)](#)".

## 1.2 Supported Cloud Services

CloudConnect supports the following cloud services:

- **Siemens MindSphere MS3.0 with the MindConnect IoT Extension**

<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 information on how to register with these services, refer to "Configuring a Station (Page 12)".

### 1.3 Default Factory Configuration

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

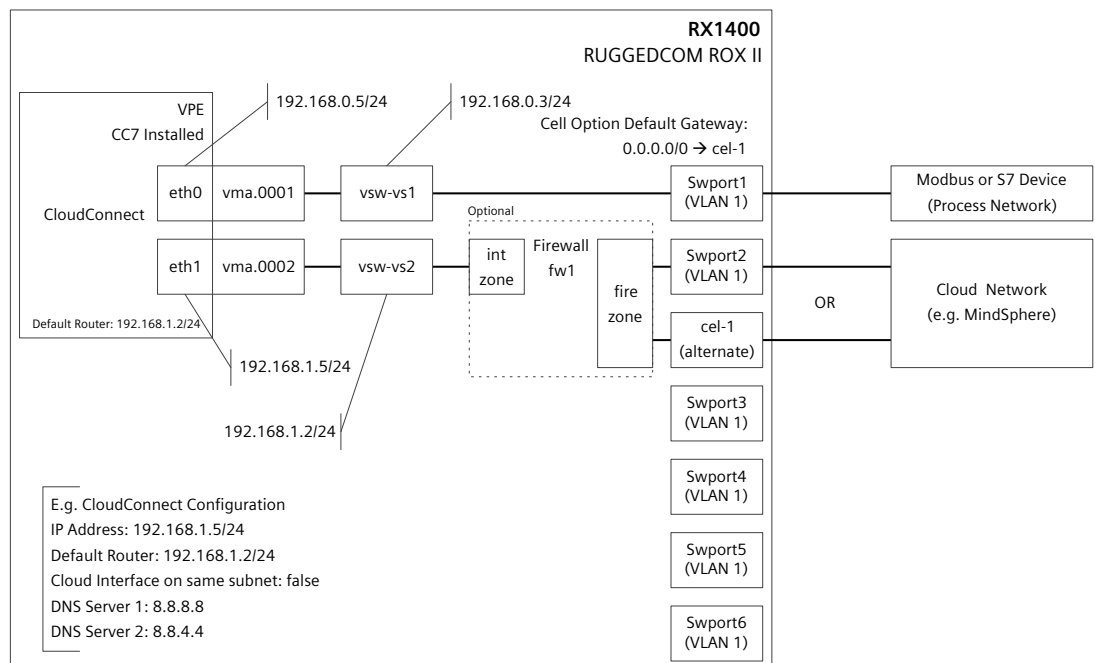


Figure 1.1 Factory Configuration

### 1.4 Security Recommendations

- If using a cellular interface, configure a firewall on the RUGGEDCOM RX1400 to control traffic from the VPE to the cloud.
- Consider securing the connection (e.g. with IPsec) between the device and other 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 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.
- Make sure to set the password for the Linux console when commissioning CloudConnect. A strong password will prevent unauthorized access to sensitive data and actions.

#### NOTICE

The Linux console password is not recoverable if forgotten. Make sure to record the password in a secure manner for future reference later, if needed.

- Configure the Network Time Protocol (NTP) on the device to help reject expired certificates.
- Control physical access to the device to prevent unauthorized access to sensitive data and actions.
- Make sure additional security recommendations outlined in the *RUGGEDCOM ROX II Configuration Manuals* are followed.

For more information, refer to the *RUGGEDCOM ROX II Configuration Manuals* on SIOS [<https://support.industry.siemens.com>].

## 1.5 Logging In to CloudConnect

To log in to the CloudConnect user interface, do the following:

### Note

The CloudConnect user interface is available once the RUGGEDCOM RX1400 is configured. For devices that were ordered with CloudConnect pre-installed, the interface is available immediately.

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 username and password. The default credentials are:

<b>Username</b>	admin
-----------------	-------

Password	admin
----------	-------

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

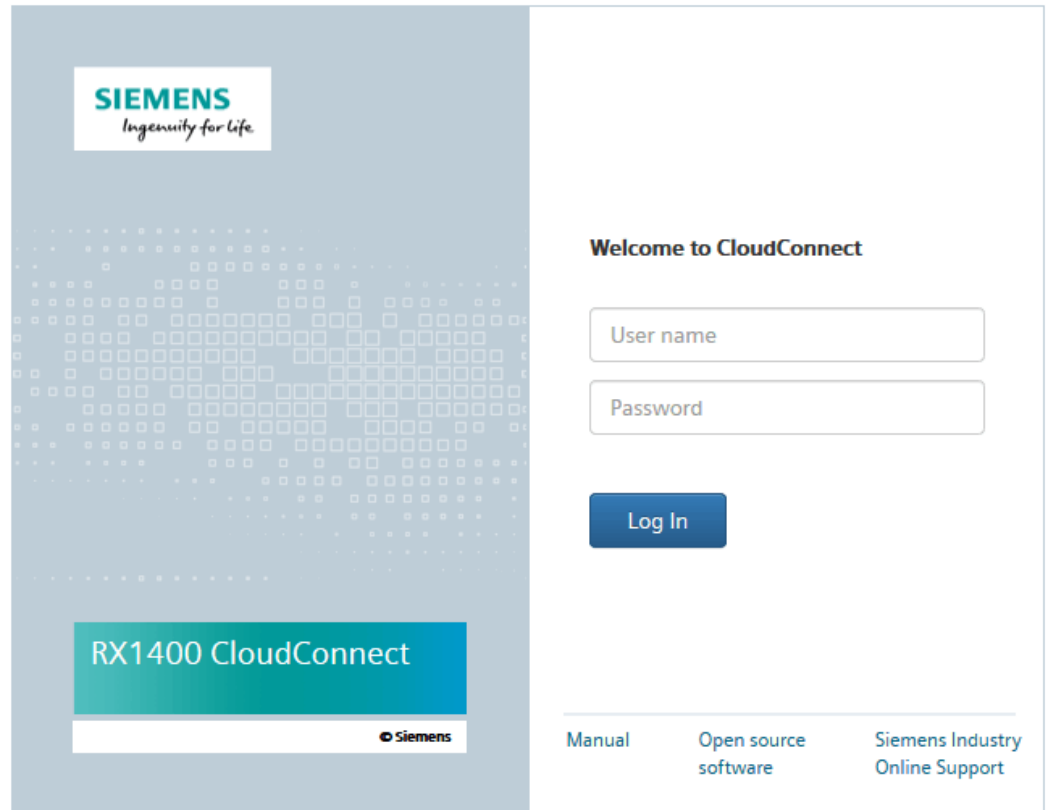


Figure 1.2 CloudConnect Log In Page

3. Click **Log In**.

## Configuring CloudConnect

To configure CloudConnect on the RUGGEDCOM RX1400, do the following:

---

**Note**

For an overview of the default factory configuration of CloudConnect on the RUGGEDCOM RX1400, refer to ["Default Factory Configuration \(Page 2\)"](#).

---

1. Register with one of the supported cloud service providers.  
For a list of supported cloud services, refer to ["Supported Cloud Services \(Page 1\)"](#).
2. Configure the RUGGEDCOM RX1400 and CloudConnect network interfaces.  
For more information, refer to the following:
  - ["Configuring the RUGGEDCOM RX1400 \(Page 6\)"](#)
  - *RX1400/APE1808 with CloudConnect Configuration Manual*

---

**Note****Configuration hazard – risk of communication loss**

The IP address assigned to the Cloud interface (p1) for CloudConnect must be unique on the network. If another device on the network shares the same IP address, it may bring down both the Cloud (P1) and Process (P2) interfaces. In this scenario, the VPE will need to be reset via the Linux console.

---

3. Make sure the IP address assigned to Cloud interface (p1) in CloudConnect is not used by any other device on the network.  
For more information about IP addresses for Ethernet interfaces, refer the *RX1400/APE1808 with CloudConnect Configuration Manual*.
4. Configure a station (end device) within CloudConnect for each registered cloud service.  
For more information, refer to ["Configuring a Station \(Page 12\)"](#).
5. Configure the chosen cloud service.  
For more information, refer to ["Configuring Cloud Services \(Page 13\)"](#).
6. Configure a profile in CloudConnect for each cloud service.  
For more information, refer to ["Configuring Cloud Profiles Within CloudConnect \(Page 21\)"](#).

## 2.1 Configuring the RUGGEDCOM RX1400

Complete the following tasks to configure CloudConnect on the RUGGEDCOM RX1400:

---

### Note

Configuration of the device must be done via the RUGGEDCOM ROX II user interface. Refer to these manuals for specific instructions on how to perform certain tasks.

The *RUGGEDCOM ROX II Configuration Manuals* are available on SIOS [<https://support.industry.siemens.com>].

---

### Note

#### Requirement

The RUGGEDCOM RX1400 must have RUGGEDCOM ROX v2.11 or higher installed.

---

1. Install the CloudConnect application.  
For more information, refer to "[Installing the CloudConnect Application \(Page 6\)](#)".
2. Configure and enable virtual machine interfaces.  
For more information, refer to "[Configuring Virtual Machine Interfaces \(Page 7\)](#)".
3. Configure virtual switches to bridge VMA and VLAN/routable interfaces.  
For more information, refer to "[Configuring Virtual Switches \(Page 7\)](#)".
4. If the device's internal 4G LTE cellular modem is to be used to connect with CloudConnect services:
  - a. Configure a cellular modem interface to allow the CloudConnect connection.  
For more information, refer to "[Configuring the Cellular Modem Interface \(Page 9\)](#)".
  - b. Configure a firewall to make sure traffic destined for the Internet is sent via the cellular modem interface.  
For more information, refer to "[Configuring a Firewall \(Page 11\)](#)".

### 2.1.1 Installing the CloudConnect Application

The CloudConnect application is installed on the RUGGEDCOM RX1400 under the VPE as a virtual machine image.

To install the CloudConnect application, do the following:

1. Order the CloudConnect application from Siemens Customer Support. Instructions on how to download the file will be provided.
2. Download the CloudConnect virtual machine 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.  
For more information, refer to the *RUGGEDCOM RX1400 Installation Manual* [<https://support.industry.siemens.com/cs/us/en/view/109480955>].
5. Add a virtual machine interface and extract a virtual machine archive.  
For more information, refer to the *RUGGEDCOM ROX II Configuration Manuals* available on SIOS [<https://support.industry.siemens.com>].

## 2.1.2 Configuring Virtual Machine Interfaces

The virtual machine interfaces, **vma.0001** and **vma.0002**, must be enabled for CloudConnect.

To configure and enable these interfaces, do the following for both:

1. Enable the virtual machine interface.  
For more information, refer to "Enabling/Disabling the VPE Network Interface" in the *RUGGEDCOM ROX II Configuration Manuals* available on SIOS [<https://support.industry.siemens.com>].
2. Add the virtual machine interface.  
For more information, refer to "Adding a Virtual Interface" in the *RUGGEDCOM ROX II Configuration Manuals* available on SIOS [<https://support.industry.siemens.com>].

## 2.1.3 Configuring Virtual Switches

Two virtual switches are required to bridge the two VMA interfaces and the VLAN/routable interfaces.

To configure the virtual switches, do the following:

1. Log in to the device 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# conf
Entering configuration mode private
ruggedcom(config)# switch vlans static-vlan 2
ruggedcom(config-static-vlan-2)# commit
Commit complete.
ruggedcom(config-static-vlan-2)# end
ruggedcom# conf
Entering configuration mode private
ruggedcom(config)# interface virtualswitch vs1
ruggedcom(config-virtualswitch-vs1)# interface switch.0001
ruggedcom(config-interface-switch.0001)# exit
ruggedcom(config-virtualswitch-vs1)# interface vma.0001
ruggedcom(config-interface-vma.0001)# exit
ruggedcom(config-virtualswitch-vs1)# exit
ruggedcom(config-interface)# virtualswitch vs2
ruggedcom(config-virtualswitch-vs2)# interface switch.0002
ruggedcom(config-interface-switch.0002)# exit
ruggedcom(config-virtualswitch-vs2)# interface vma.0002
ruggedcom(config-interface-vma.0002)# commit
The following warnings were generated:
  'interface virtualswitch vs1 interface switch.0001': IP Address of Interface
switch.0001 will become inactive and hidden if changes are committed as
Interface switch.0001 was added to virtual switch vs1.
  'interface virtualswitch vs1 interface vma.0001': IP Address of Interface
vma.0001 will become inactive and hidden if changes are committed as
Interface vma.0001 was added to virtual switch vs1.
  'interface virtualswitch vs2 interface switch.0002': IP Address of Interface
switch.0002 will become inactive and hidden if changes are committed as
Interface switch.0002 was added to virtual switch vs2.
  'interface virtualswitch vs2 interface vma.0002': IP Address of Interface
vma.0002 will become inactive and hidden if changes are committed as
Interface vma.0002 was added to virtual switch vs2.
Proceed? [yes,no] yes
Commit complete.
ruggedcom(config-interface-vma.0002)# end
ruggedcom# show running-config 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# conf
Entering configuration mode private
ruggedcom(config)# ip vsw-vs1
ruggedcom(config-ip-vsw-vs1)# ipv4 address 192.168.0.3/24
ruggedcom(config-address-192.168.0.3/24)# commit
Commit complete.
ruggedcom(config-address-192.168.0.3/24)# end
ruggedcom# show running-config 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# conf
Entering configuration mode private
ruggedcom(config)# ip vsw-vs2
ruggedcom(config-ip-vsw-vs2)# ipv4 address 192.168.1.2/24
ruggedcom(config-address-192.168.1.2/24)# commit
Commit complete.
ruggedcom(config-address-192.168.1.2/24)# end
ruggedcom# show running-config 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

```

## 2.1.4 Configuring the Cellular Modem Interface

If the device's internal 4G LTE cellular modem is to be used to communicate with the CloudConnect service, a cellular modem interface to the modem is required.

To configure the cellular mode interface, do the following:

1. Log in to the device as an administrator.

2. 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. <b>Use the default setting.</b>
sim	The SIM index (1 or 2) to be used by the access point.
profile	The cellular connection profile.

3. Enable the cell modem interface.
4. Configure the PPP client and set it to connect to the GSM profile defined in [Step 2](#).
5. Configure a static route and assign it to the cellular modem interface (cel-1).
6. Verify the status of the cellular modem interface configuration.

**Example**

```

ruggedcom# config
Entering configuration mode private
ruggedcom(config)# global
ruggedcom(config-global)# cellular profiles gsm telus
ruggedcom(config-gsm-telus)# apn SP.TELUS.COM
ruggedcom(config-gsm-telus)# ppp-config use-peer-dns
ruggedcom(config-gsm-telus)# no ppp-config dial-on-demand
ruggedcom(config-gsm-telus)# no ppp-config failover-on-demand
ruggedcom(config-gsm-telus)# commit
ruggedcom(config-settings)# commit
Commit complete.
ruggedcom(config-settings)# end
ruggedcom# show running-config 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
Entering configuration mode private
ruggedcom(config)# interface
ruggedcom(config-interface)# cellmodem celport 1
ruggedcom(config-cellmodem-celport/1)# enabled
ruggedcom(config-cellmodem-celport/1)# no alias
ruggedcom(config-cellmodem-celport/1)# lte ppp-client connect-to telus
ruggedcom(config-cellmodem-celport/1)# lte firmware-update
ruggedcom(config-firmware-update)# settings
ruggedcom(config-settings)# no repository-url
ruggedcom(config-settings)# mode manual-check-and-update
ruggedcom(config-settings)# commit
Commit complete.
ruggedcom(config-settings)# end
ruggedcom# show running-config 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
Entering configuration mode private
ruggedcom(config)# routing ipv4 route 0.0.0.0/0
ruggedcom(config-route-0.0.0.0/0)# dev cel-1
ruggedcom(config-dev-cel-1)# no distance
ruggedcom(config-dev-cel-1)# commit
ruggedcom(config-settings)# commit
Commit complete.
ruggedcom(config-settings)# end
ruggedcom# show running-config routing ipv4 route
routing ipv4 route 0.0.0.0/0
dev cel-1
no distance
```

## 2.1.5 Configuring a Firewall

If the device's internal 4G LTE cellular modem is to be used to communicate with the CloudConnect service, a firewall is required. The firewall provides a secure connection via the Internet between the cloud service and the CloudConnect application.

To configure the firewall, do the following:

1. Log in to the device 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:

Parameter	Value
fwpolicy	p1
policy	accept
source-zone	all
destination-zone	all

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
Entering configuration mode private
ruggedcom(config)# security firewall fwconfig fw1
ruggedcom(config-fwconfig-fw1)# fwzone fire
ruggedcom(config-fwzone-fire)# type firewall
ruggedcom(config-fwzone-fire)# fwzone int
ruggedcom(config-fwzone-int)# fwinterface cel-1
ruggedcom(config-fwinterface-cel-1)# fwinterface vsw-vs2
ruggedcom(config-fwinterface-vsw-vs2)# zone int
ruggedcom(config-fwinterface-vsw-vs2)# fwpolicy p1
ruggedcom(config-fwpolicy-p1)# source-zone all
ruggedcom(config-fwpolicy-p1)# destination-zone all
ruggedcom(config-fwpolicy-p1)# policy accept
ruggedcom(config-fwpolicy-p1)# fwmasq masq1
ruggedcom(config-fwmasq-masq1)# out-interface cel-1
ruggedcom(config-fwmasq-masq1)# source-hosts 192.168.1.0/24
ruggedcom(config-fwmasq-masq1)# commit
Commit complete.
ruggedcom(config-fwmasq-masq1)# end
ruggedcom# show running-config security firewall
security
firewall
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
!
!
!
```

## 2.2 Configuring a Station

A station, or end device, is required to communicate with CloudConnect via Modbus TCP or the S7 protocol.

To configure a station, do the following:

1. Log in to the CloudConnect user interface as the **admin** user.
2. Navigate to **Process Access » Station Configuration**.
3. Under **Station name**, enter a station name.
4. On the **Settings** tab, select **Modbus/TCP** or **S7** protocol.
5. On the **Modbus/TCP** or **S7** tab, configure the protocol.

For more information, refer to the *RX1400/APE1808 with CloudConnect Configuration Manual*.

## 2.3 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 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.

---

### 2.3.1 Configuring MindConnect

To enable an MQTT device connection with MindSphere, the MindConnect IoT Extension needs 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 will automatically create a device in the MindConnect IoT extension, with the device name entered in the CloudConnect user interface.

---

### Note

#### Requirement

- A MindSphere tenant with **MindConnect IoT Extension** enabled
-

To configure MindConnect, do the following:

1. Add the MindConnect IoT Extension to the MindSphere tenant. This is required to enable an MQTT device connection with MindSphere.

For more information, refer to the *Welcome to MindSphere* e-mail.

2. Obtain the URL for the MindConnect IoT Extension.

For more information, refer to "[Obtaining the MindConnect IoT Extension URL \(Page 14\)](#)".

3. If encrypted communication over TLS is required, obtain the server certificate for the MindConnect IoT extension.

For more information, refer to "[Obtaining the MindConnect IoT Extension Server Certificate \(Page 15\)](#)".

### 2.3.1.1 Obtaining the MindConnect IoT Extension URL

To obtain the URL for the MindConnect IoT Extension, do the following:

1. Log in to the MindSphere tenant portal.

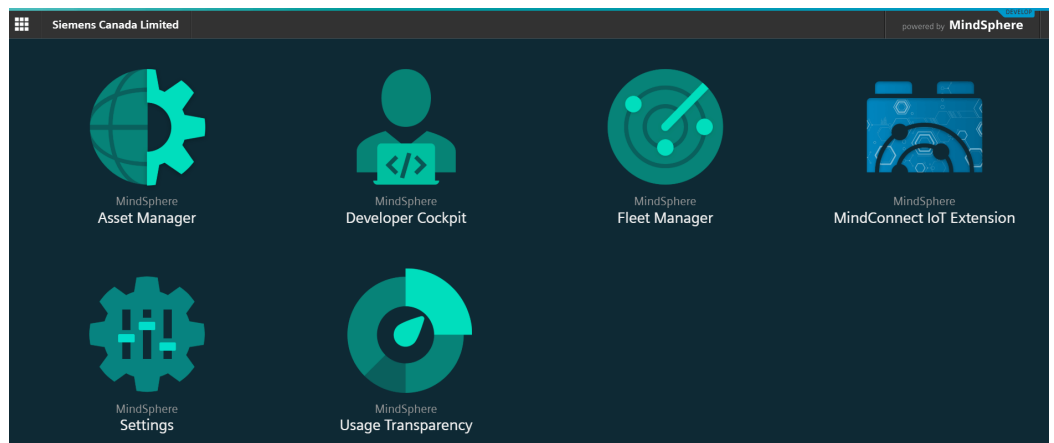


Figure 2.1 MindSphere Tenant Portal – Main Menu

2. Click **MindConnect IoT Extension**. A browser window appears.

3. Log in to **MindConnect IoT Extension** and note the URL. For example:

siedev.mciotextension.eu-central.minsphere.io

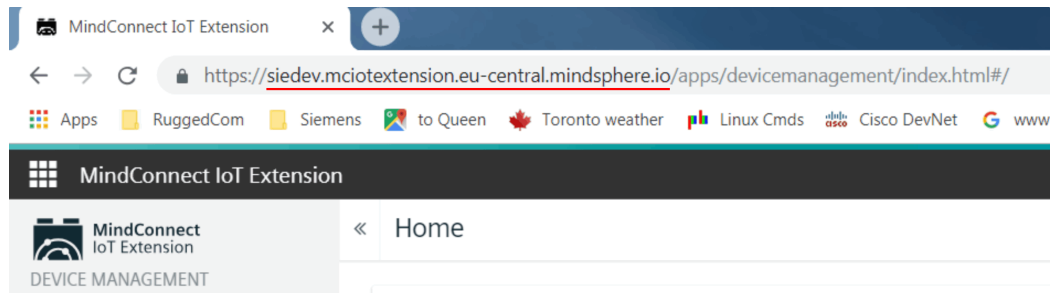


Figure 2.2 MindConnect IoT Extension URL

4. Temporarily record the URL.

### 2.3.1.2 Obtaining the MindConnect IoT Extension Server Certificate

1. Log in to the MindSphere tenant portal.

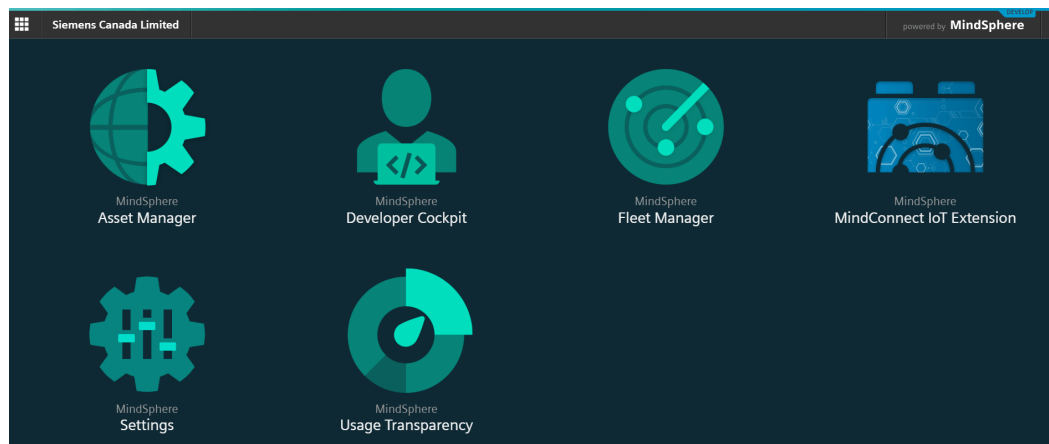


Figure 2.3 MindSphere Tenant Portal – Main Menu

2. Click **MindConnect IoT Extension**. A browser window appears.
3. Log in to **MindConnect IoT Extension**.



4. Click the secure icon on your browser.

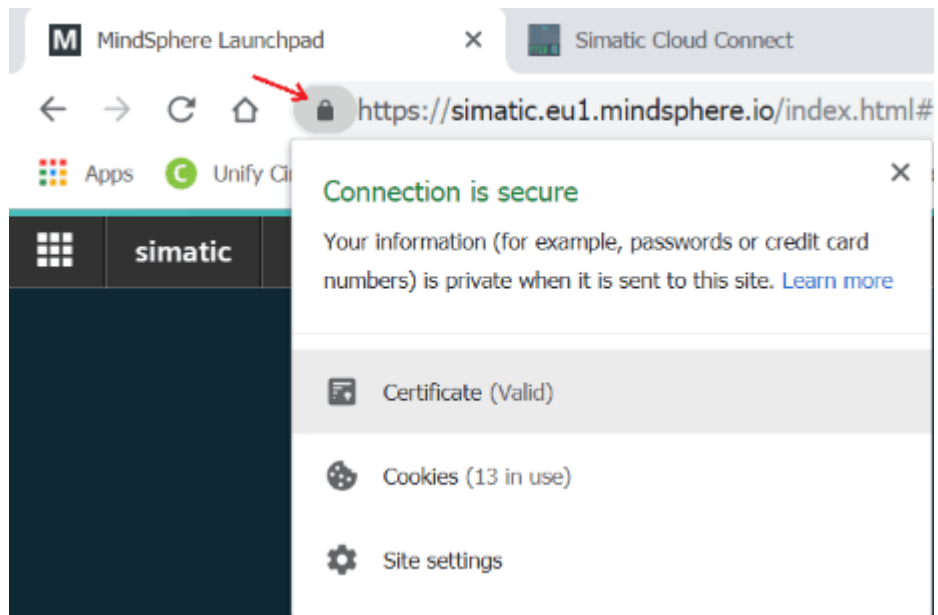


Figure 2.4 Secure Icon

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

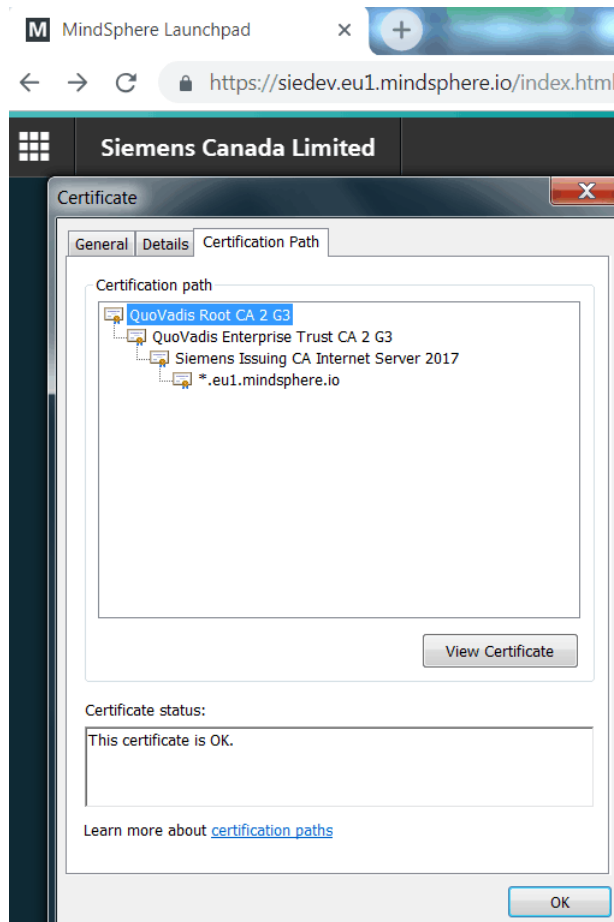


Figure 2.5 Certification Path Tab

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

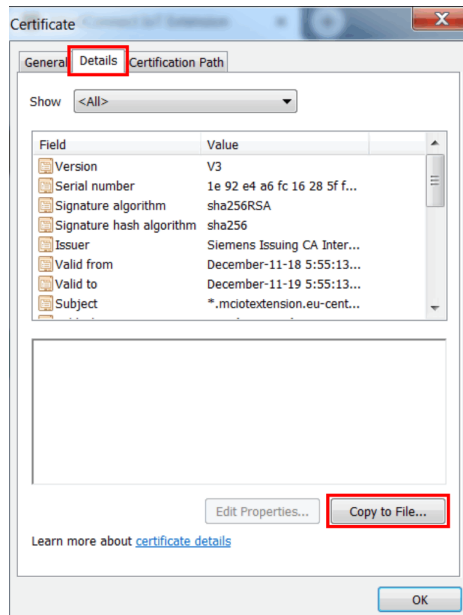


Figure 2.6 Certificate Details Tab

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

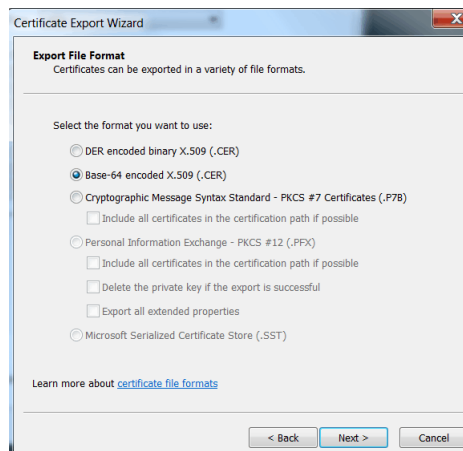


Figure 2.7 Certificate Export Wizard – Export File Format

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

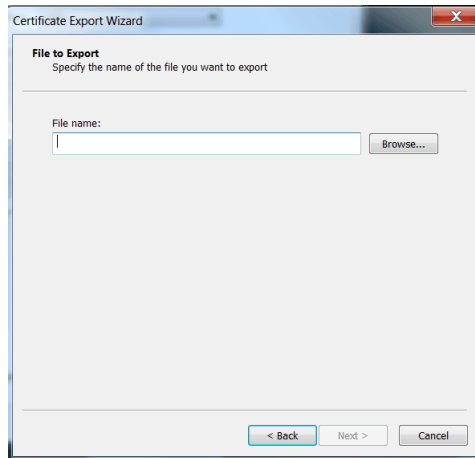


Figure 2.8 Certificate Export Wizard – File to Export

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

## 2.3.2 Configuring AWS IoT Core

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.

---

To configure a *thing* that uses an X.509 certificate, do the following:

---

### Note

#### Requirement

- An AWS account
- 

- Log in to the AWS portal.
- 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.

### 2.3.3 Configuring Microsoft Azure IoT Hub

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.

---

To configure a Microsoft Azure profile via the CloudConnect service, do the following:

---

**Note****Requirements**

- A Microsoft Azure account
- 

1. Log in 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**.

## 2.4 Configuring Cloud Profiles Within CloudConnect

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

### 2.4.1 Configuring CloudConnect for Siemens MindSphere with the MindConnect IoT Extension

To create a profile within CloudConnect for Siemens MindSphere, do the following:

---

**Note****Requirements**

- A RUGGEDCOM RX1400 with the CloudConnect application installed and configured
  - The server certificate obtained from MindSphere in "[Obtaining the MindConnect IoT Extension URL \(Page 14\)](#)"
  - A remote device with data points configured in CloudConnect
- 

1. Log in 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:**
  - Enter a 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 the MindConnect IoT Extension.

For example:

```
siedev.mciotextension.eu-central.mindsphere.io
```

For information about how to obtain the URL, refer to ["Obtaining the MindConnect IoT Extension URL \(Page 14\)"](#).

- 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/winston.smith@company.com
```

- h. Click **Save**.
- Under **Security Settings:**
    - a. Choose the server certificate exported previously in ["Configuring MindConnect \(Page 13\)"](#).
    - b. Import the server certificate.
    - c. 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 has been completed.

The Client ID must match the Client ID entered previously under the **MQTT Configuration** configuration.

- 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 operand 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 2.9

For more information, refer to the *RX1400/APE1808 with CloudConnect Configuration Manual*.

## 2.4.2 Configuring CloudConnect for AWS

To create a profile within CloudConnect for AWS, do the following:

---

### Note

#### Requirements

- 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 CloudConnect
- 

1. Log in 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**:
    - Enter a profile name and then click **Add**.
  - Under **Settings**:
    - a. Set **Cloud Provider** to *AWS*.
    - b. Set **Protocol** to *MQTT*.
    - c. Select **Enable Profile**.
  - Under **MQTT Configuration**:
    - a. Set **MQTT version** to *v3.1.1*.
    - b. Set **Broker address** as the HTTPS link/Rest API Endpoint obtained when creating the AWS thing.
    - c. Set **Broker port** to *8883*.
    - d. Select **Clean Session**.
    - e. Select **Enable TLS**.
    - f. 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 to CloudConnect . CloudConnect will connect to the configured cloud with its configurations.



Figure 2.10

For more information, refer to the *RX1400/APE1808 with CloudConnect Configuration Manual*.

### 2.4.3 Configuring CloudConnect for Microsoft Azure

To create a profile within CloudConnect for Microsoft Azure, do the following:

---

#### Note

#### Requirements

- 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 CloudConnect.

- 
1. Log in 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:**
    - Enter a profile name and then click **Add**.
  - Under **Settings:**
    - a. Set **Cloud Provider** to `Azure`.
    - b. Set **Protocol** to `MQTT`.
    - c. Select **Enable Profile**.
  - Under **MQTT Configuration:**
    - a. Set **MQTT version** to `v3.1.1`.
    - b. Set **Broker address** as the IoT Hub host name.
    - c. Set **Broker port** to `8883`.
    - d. Set **Client ID** to the device ID create in the IoT Hub.
    - e. Select **Enable Authentication**.
    - f. Set **Username** to `{ IoT Hub Hostname }/{ Device ID }/api-version=2016-11-14`, where `{ IoT Hub Hostname }` 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 **Data Topics – Topic Editor** in CloudConnect, add a new topic with the name `devices/{ Device ID }/messages/events/`.
6. Click **Apply Settings** to apply the updated settings to CloudConnect . CloudConnect will connect to the configured cloud with its configurations.



Figure 2.11

For more information, refer to the *RX1400/APE1808 with CloudConnect Configuration Manual*.

## 2.5 Resetting the Password

To reset the password for CloudConnect, do the following:

1. Access the Linux console.

For more information, refer to "[Connecting to the CloudConnect Linux Console \(Page 32\)](#)".

2. At the prompt, enter the following command:

```
echo "1" > /var/tmp/reset && sudo reboot
```

After entering this command, the password for CloudConnect will reset and the Linux system will reboot.

## Updating CloudConnect

Updates for CloudConnect are available through Siemens Customer Support.  
To update CloudConnect on the RUGGEDCOM RX1400, do the following:

---

**Note**

The following procedure is outlined in more detail in the *RX1400/APE1808 with CloudConnect Configuration Manual*.

---

**Note**

The firmware update updates CloudConnect and may include updated Debian OS packages.

---

1. Order the firmware update from Siemens Customer Support. Instructions on how to download the file will be provided.
2. Download the CloudConnect virtual machine image. The image will be a file with a \*.upd extension.
3. Log in to the CloudConnect user interface.
4. Navigate to **Maintenance » Firmware update**.
5. Load the firmware and then click **Update firmware**.
6. Follow the prompts and wait for the update to complete.



## Troubleshooting

CloudConnect provides tools for troubleshooting network issues, including an online diagnostics tool, system logging and a Linux console.

### 4.1 Online Diagnostics

CloudConnect offers a system diagnostic log under **Maintenance » Online Diagnostics**. The log provides important information for system administrators to aid in troubleshooting of the setup and configuration.

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

For more information, refer to the *RX1400/APE1808 with CloudConnect Configuration Manual*.

The screenshot shows the Siemens CloudConnect web interface. At the top left is the Siemens logo, and at the top right is the text "RX1400 CloudConnect". Below the header is a navigation menu with tabs: Info, Interface configuration, Process access, Cloud configuration, Data and topics, and Maintenance. The Maintenance tab is selected. Under the Maintenance tab, there is a section for "System diagnostics". Below this section, there is a dropdown menu for "Automatic update" set to "disabled". The log entries are as follows:

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]

Figure 4.1 Online Diagnostics

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

### 4.2 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**,



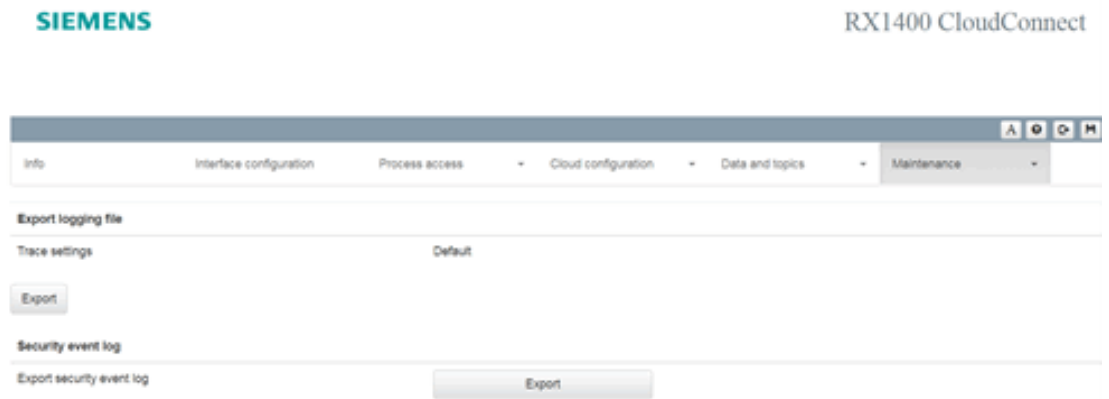




Figure 4.2 Online Diagnostics

### 4.3 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.

 <b>NOTICE</b>
<p>The Linux console password is not recoverable if forgotten. Make sure to record the password in a secure manner for future reference later, if needed.</p>

 <b>NOTICE</b>
<p><b>Configuration hazard – risk of data corruption</b></p> <p>Access to the Linux Console is provided for troubleshooting purposes and should only be used by Siemens technicians. Misuse of the Linux Console commands can corrupt the operational state of the device and render it inaccessible.</p>

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:

<b>User</b>	cloudconn
<b>Password</b>	cc7+123

#### Accessing the Console For the First Time

When accessing the Linux console for the first time, you will be asked to provide a password. Make sure the password meets the minimum requirements set by your organization.

```
You are required to change your password immediately (root enforced)
```

```
Changing password for cloudconn.  
(current) UNIX password:  
New password:  
Retype new password:
```

## Available Commands

The following sudo commands are available for troubleshooting:

- **Using CloudConnect**

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

- **Emergency Network Configuration**

```
touch /etc/resolv.conf  
touch /etc/network/interfaces  
ip addr flush dev *  
ifup *  
ifdown *
```

- **Debian Updates**

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

- **General**

```
General  
reboot  
ifconfig *  
ping *  
mv /etc/localtime *  
rm /etc/localtime.old  
mv /etc/localtime *  
ln *  
unlink *  
date *
```



## Further Information

Siemens RUGGEDCOM  
<https://www.siemens.com/ruggedcom>

Industry Online Support (service and support)  
<https://support.industry.siemens.com>

Industry Mall  
<https://mall.industry.siemens.com>

Siemens AG  
Digital Industry  
Process Automation  
Postfach 48 48  
90026 NÜRNBERG  
GERMANY