# MANUAL

# ICDM-RX

## Hardware Installation and Configuration

**EtherNet/IP (EN)**

**EtherNet/IP to Modbus (EN1)**

**Modbus (MOD)**

**PROFINET IO (PN)**

**PROFINET IO to Modbus (PN1)**

EtherNet/IP™

PROFI NET®

**PEPPERL+FUCHS**

*SENSING YOUR NEEDS*

**PEPPERL+FUCHS**

# Table of Contents

**PEPPERL+FUCHS**

**PEPPERL+FUCHS**

**PEPPERL+FUCHS**

# 1. Getting Started

This manual discusses initial ICDM-RX Industrial Gateway installation and hardware configuration for the following industrial protocol platforms.

- EtherNet/IP (type codes beginning with ICDM-RX/EN)
- EtherNet/IP to Modbus (type codes beginning with ICDM-RX/EN1)
- Modbus gateways (type codes beginning with ICDM-RX/MOD)
- PROFINET IO (type codes beginning with ICDM-RX/PN)
- PROFINET IO to Modbus (type codes beginning with ICDM-RX/PN1)

## 1.1. Manual Conventions

In this manual, the products are referred to as ICDM-RX/*xxx*, where *xxx* is defined in the following table.

| Physical Description | Model | Model Name In Manual |
|---|---|---|
| 1-port, DB9 serial port, DIN rail mount | ICDM-RX/EN-DB9/RJ45-DIN<br>ICDM-RX/EN1-DB9/RJ45-DIN<br>ICDM-RX/MOD-DB9/RJ45-DIN<br>ICDM-RX/PN-DB9/RJ45-DIN<br>ICDM-RX/PN1-DB9/RJ45-DIN | ICDM-RX/*xxx*-DB9/RJ45-DIN |
| 1-port, DB9 serial port, panel mount | ICDM-RX/EN-DB9/RJ45-PM<br>ICDM-RX/EN1-DB9/RJ45-PM<br>ICDM-RX/MOD-DB9/RJ45-PM<br>ICDM-RX/PN-DB9/RJ45-PM<br>ICDM-RX/PN1-DB9/RJ45-PM | ICDM-RX/*xxx*-DB9/RJ45-PM |
| 1-port, screw terminal serial port, DIN rail mount | ICDM-RX/EN-ST/RJ45-DIN<br>ICDM-RX/EN1-ST/RJ45-DIN<br>ICDM-RX/MOD-ST/RJ45-DIN<br>ICDM-RX/PN-ST/RJ45-DIN<br>ICDM-RX/PN1-ST/RJ45-DIN | ICDM-RX/*xxx*-ST/RJ45-DIN |
| 2-port, DB9 serial ports, DIN rail mount | ICDM-RX/EN-2DB9/RJ45-DIN<br>ICDM-RX/EN1-2DB9/RJ45-DIN<br>ICDM-RX/MOD-2DB9/RJ45-DIN<br>ICDM-RX/PN-2DB9/RJ45-DIN<br>ICDM-RX/PN1-2DB9/RJ45-DIN | ICDM-RX/*xxx*-2DB9RJ45-DIN |

3/7/20

**PEPPERL+FUCHS**

| Physical Description | Model | Model Name In Manual |
|---|---|---|
| 2-port, screw terminal serial ports, DIN rail mount | ICDM-RX/EN-2ST/RJ45-DIN<br>ICDM-RX/EN1-2ST/RJ45-DIN<br>ICDM-RX/MOD-2ST/RJ45-DIN<br>ICDM-RX/PN-2ST/RJ45-DIN<br>ICDM-RX/PN1-2ST/RJ45-DIN | ICDM-RX/*xxx*-2ST/RJ45-DIN |
| 4-port, DB9 serial ports, DIN rail mount | ICDM-RX/EN-4DB9/2RJ45-DIN<br>ICDM-RX/EN1-4DB9/2RJ45-DIN<br>ICDM-RX/MOD-4DB9/2RJ45-DIN<br>ICDM-RX/PN-4DB9/2RJ45-DIN<br>ICDM-RX/PN1-4DB9/2RJ45-DIN | ICDM-RX/*xxx*-4DB9/2RJ45-DIN |

## 1.2. Installation Overview

Installation and configuration follows these steps.

1. Connect the hardware (Page 8).
2. Install PortVision DX (Page 22).
3. Configure the ICDM-RX network settings (Page 25).
4. If necessary, update the firmware on the ICDM-RX (Page 29).
5. Go to https://www.pepperl-fuchs.com for your product to locate the protocol manual for your platform so that you can perform the following procedures:
   - Configure port characteristics using the appropriate web interface pages
   - Program the PLCs
6. Connect the serial device or devices (Page 53).

## 1.3. ICDM-RX/MOD Models Only

By default, ICDM-RX/MOD models are loaded with Modbus Router. If you want to implement the Modbus Server or Modbus TCP platform, you must go to https://www.pepperl-fuchs.com and download the appropriate firmware.

See *Uploading Firmware on the ICDM-RX* on Page 29 for information on loading the appropriate firmware.

## 1.4. Locating Software and Documentation

You can download the latest firmware assembly, PortVision DX, and the ICDM-RX documentation from the web site at: https://www.pepperl-fuchs.com.

***Note:*** *Review your firmware version using PortVision DX or the web interface Home page and then compare it to the firmware version on the web site. If a firmware version is not available that means that the latest version is loaded on the device.*

3/7/20

**PEPPERL+FUCHS**

7

# 2. Hardware Installation

This chapter discusses:

## 2.1. ICDM-RX/*xxx*-DB9/RJ45-PM Installation

Use the following procedure to install the ICDM-RX/*xxx*-DB9/RJ45-PM.

1. Place the ICDM-RX/*xxx*-DB9/RJ45-PM on a stable surface and skip to Step 2 or optionally mount the ICDM-RX/*xxx*-DB9/RJ45-PM using the mounting flanges or DIN rail adapters.

    a. Pick up the ICDM-RX/*xxx*-DB9/RJ45-PM so that the front of the device is facing you.

    b. Pick up a DIN rail clip. (The three tines should be on top and the **M4** label should face you.)

    c. Slide the DIN rail clip behind the ICDM-RX/*xxx*-DB9/RJ45-PM and line it up with one of the screw holes on the ICDM-RX/*xxx*-DB9/RJ45-PM.

    d. Insert the **M4** screw into the hole and tighten with a Phillips screwdriver.

    e. Repeat Steps b through d with the second DIN rail clip. Make sure the screws on both DIN rail clips line up.

    > **Note:** *If you need to remove the ICDM-RX/**xxx**-DB9/RJ45-PM from the DIN rail, exert pressure on the backside of the tabs at the bottom of both DIN rail clips.*

    f. Attach the ICDM-RX/*xxx*-DB9/RJ45-PM to the DIN rail.
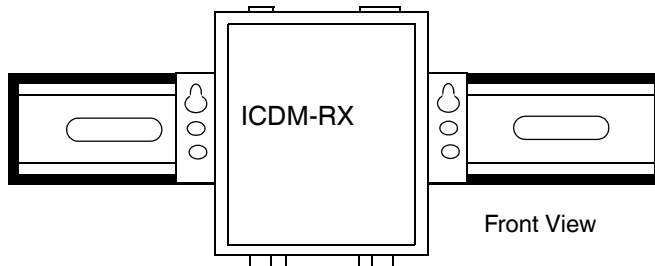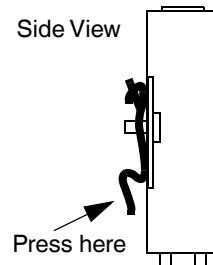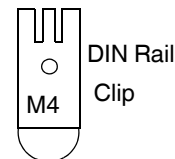
> **Note:** *Do not connect multiple units until you have changed the default IP address, see Preparing the ICDM-RX for Configuration on Page 21*

2. Connect the ICDM-RX/*xxx*-DB9/RJ45-PM port labeled **10/100 ETHERNET** to the same Ethernet network segment as the PLC using a standard network cable.

**PEPPERL+FUCHS**

3. Apply power to the ICDM-RX/**xxx**-DB9/RJ45-PM using the following procedure.

    *Note:* *See ICDM-RX/xxx-DB9/RJ45-PM Power Supply on Page 95, if you want to provide your own power supply.*

⚠
**Caution**

   ***Observe proper ESD techniques when connecting and disconnecting the ICDM-RX/xxx-DB9/RJ45-PM.***

   • Insert the earth ground wire into the earth ground screw terminal.

   • Insert the DC positive wire into the positive screw terminal and the DC return wire into the return screw terminal.

     Refer to *ICDM-RX/xxx-DB9/RJ45-PM Power Supply* on Page 95 for detailed power requirements.

   • Use a small flat head screw to lock the wires into place.

   • Verify that each wire has been tightened securely.

   • Plug the screw terminal power connector into the ICDM-RX/**xxx**-DB9/RJ45-PM.

     *Note:* *Align the plug properly. The scalloped side of the screw terminal power connector should be aligned with the scalloped side of the power jack on the unit.*

   • Connect the power supply to a power source.

4. Verify that the **Status** LED has completed the boot cycle and network connection for the ICDM-RX/**xxx**-DB9/RJ45-PM is functioning properly using the table below.
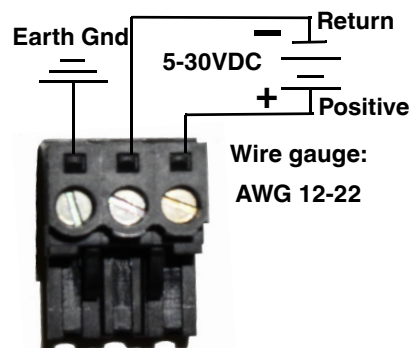
| ICDM-RX/*xxx*-DB9/RJ45-PM LED Descriptions | |
|---|---|
| Status | The amber **Status** LED on the device is lit, indicating you have power and it has completed the boot cycle. |
| | The **Status** LED flashes while booting and it takes approximately 15 seconds for the Bootloader to complete the cycle. When the Bootloader completes the cycle, the LED has a solid, steady light that blinks approximately every 10 seconds. |
| | ***If PN or PN1 model:*** |
| | When the Bootloader completes the cycle, the LED flashes rapidly for several times then stays off and blinks approximately every 10 seconds when there is no PLC connection. |
| Link/Act | If the red **Link/Act** LED is lit, it indicates a working Ethernet connection. |
| Duplex | If the red **Duplex** LED is lit, it indicates full-duplex activity. |
| 100 | If the red **100** LED is lit, it indicates a working 100 MB Ethernet connection (100 MB network, only). If the LED is not lit, it indicates a 10 MB Ethernet connection. |
| *Note:* For additional LED information, go to the Status LED table on Page 100. | |

⚠ ***Do not connect RS-422/485 devices until the IP address is configured and an appropriate port interface type has been configured. The default port setting is RS-232.***

3/7/20

**PEPPERL+FUCHS**

5.  Go to *Preparing the ICDM-RX for Configuration* on Page 21 to install PortVision DX, configure the network settings, and if necessary, upload the appropriate protocol firmware on the ICDM-RX/***xxx***-DB9/RJ45-PM.

## 2.2. ICDM-RX/*xxx*-ST/RJ45-DIN Installation

Use the following procedure to install the ICDM-RX/***xxx***-ST/RJ45-DIN. See *ICDM-RX/xxx-DB9/RJ45-DIN Installation* on Page 12 if the ICDM-RX has DB9 serial connectors.

1.  Attach the ICDM-RX/***xxx***-ST/RJ45-DIN 1-Port to the DIN rail adapter.

2.  Connect the power supply and apply power to the ICDM-RX/***xxx***-ST/RJ45-DIN using the power supply specifications on the product label and the following information.

    ⚠️ ***Observe proper ESD techniques when connecting and disconnecting the ICDM-RX/xxx-ST/RJ45-DIN.***

    a.  If the DIN rail is not connected to earth ground, insert the earth ground wire into the chassis ground screw terminal.

    *Note:*  *The chassis ground connection is made only if the DIN rail is NOT connected to earth ground.*

    b.  Insert the DC positive wire into the + screw terminal and the DC return wire into the - screw terminal.

        Refer to *ICDM-RX/xxx-DB9/RJ45-DIN or ICDM-RX/ xxx-ST/RJ45-DIN Power Supply* on Page 96 for detailed power requirements.

    c.  Use a small flat head screw driver to lock the wires into place.

    d.  Verify that each wire has been tightened securely.

    e.  Connect a UL Listed power supply and UL Listed power cord to a power source to apply power.

    *Note:*  *Do not connect multiple units until you have changed the default IP address, see Preparing the ICDM-RX for Configuration on Page 21*

    

3.  Connect the **10/100 port** to the same Ethernet network segment as the host PC using a standard network cable.

**PEPPERL+FUCHS**

4. Verify that the **STATUS** LED has completed the boot cycle and network connection for the ICDM-RX/*xxx*-ST/RJ45-DIN is functioning using the following table.

| ICDM-RX/*xxx*-ST/RJ45-DIN LED Descriptions | |
|---|---|
| **STATUS** | The **STATUS** LED on the device is lit, indicating you have power and it has completed the boot cycle. The **Status** LED flashes while booting and it takes approximately 15 seconds for the Bootloader to complete the cycle. When the Bootloader completes the cycle, the LED has a solid, steady light that blinks approximately every 10 seconds. *If PN or PN1 model:* When the Bootloader completes the cycle, the LED flashes rapidly for several times then stays off and blinks approximately every 10 seconds when there is no PLC connection. |
| **LINK** | If the **LINK** (green) LED is lit, it indicates a working Ethernet connection. |
| **ACT** | If the **ACT** (yellow) LED flashes, it indicates network activity. |
| *Note:* For additional LED information, go to the Status LED table on Page 100. | |

⚠️ ***Do not connect RS-422/485 devices until the IP address is configured and an appropriate port interface type has been configured. The default port setting is RS-232.***

5. Go to *Preparing the ICDM-RX for Configuration* on Page 21 for default network settings and how to configure the ICDM-RX for use.

**PEPPERL+FUCHS**

## 2.3. ICDM-RX/*xxx*-DB9/RJ45-DIN Installation

Use the following procedure to install the ICDM-RX/*xxx*-DB9/RJ45-DIN.

1. Attach the ICDM-RX/*xxx*-DB9/RJ45-DIN to the DIN rail adapter.

2. Connect the power supply and apply power to the ICDM-RX/*xxx*-DB9/RJ45-DIN using the power supply specifications on the product label and the following information.

⚠️ ***Observe proper ESD techniques when connecting and disconnecting the ICDM-RX/xxx-DB9/RJ45-DIN.***

a. If the DIN rail is not connected to earth ground, insert the earth ground wire into the chassis ground screw terminal.

*Note:* *The chassis ground connection is made only if the DIN rail is NOT connected to earth ground.*

b. Insert the DC positive wire into one of the + screw terminals and the DC return wire into the - screw terminal.

- A second redundant power supply can be connected to the unit by inserting the DC positive wire into the other + screw terminal and the DC return wire into the - screw terminal.

- The ICDM-RX/*xxx*-DB9/RJ45-DIN continues to operate if one of the two connected power supplies should fail.
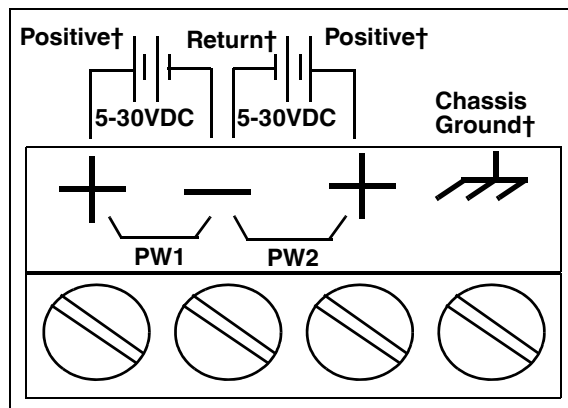


† Wire gauge: AWG 12-22

Refer to *ICDM-RX/xxx-DB9/RJ45-DIN or ICDM-RX/xxx-ST/RJ45-DIN Power Supply* on Page 96 for detailed power requirements.

c. Use a small flat head screw driver to lock the wires into place.

d. Verify that each wire has been tightened securely.

e. Connect a UL Listed power supply and UL Listed power cord to a power source to apply power.

*Note:* *Do not connect multiple units until you have changed the default IP address, see Preparing the ICDM-RX for Configuration on Page 21*

3. Connect the **10/100** port to the same Ethernet network segment as the host PC using a standard Ethernet cable.

**PEPPERL+FUCHS**

4. Verify that the **STATUS** LED has completed the boot cycle and network connection for the ICDM-RX/***xxx***-DB9/RJ45-DIN is functioning properly using the following table.

| ICDM-RX/*xxx*-DB9/RJ45-DIN LED Descriptions | |
|---|---|
| **STATUS** | The **STATUS** LED is lit, indicating you have power and it has completed the boot cycle. <br><br> The **STATUS** LED flashes while booting and it takes approximately 15 seconds for the Bootloader to complete the cycle. When the Bootloader completes the cycle, the LED has a solid, steady light that blinks approximately every 10 seconds. <br><br> ***If PN or PN1 model:*** <br><br> When the Bootloader completes the cycle, the LED flashes rapidly for several times then stays off and blinks approximately every 10 seconds when there is no PLC connection. |
| **LINK** | If the **LINK** (green) LED is lit, it indicates a working Ethernet connection. |
| **ACT** | If the **ACT** (yellow) LED flashes, it indicates network activity. |
| ***Note:*** *For additional LED information, go to the Status LED table on Page 100.* | |

⚠ ***Do not connect RS-422/485 devices until the IP address is configured and an appropriate port interface type has been configured. The default port setting is RS-232.***

5. Go to *Preparing the ICDM-RX for Configuration* on Page 21 for default network settings and how to configure the ICDM-RX for use.

3/7/20

**PEPPERL+FUCHS**

## 2.4. ICDM-RX/*xxx*-2ST/RJ45-DIN Installation

Use the following procedure to install the ICDM-RX/*xxx*-2ST/RJ45-DIN. See *ICDM-RX/xxx-2DB9RJ45-DIN Installation* on Page 16 if the ICDM-RX has DB9 serial connectors.

1. Attach the ICDM-RX/*xxx*-2ST/RJ45-DIN to the DIN rail adapter.

2. Connect the power supply and apply power to the ICDM-RX/*xxx*-2ST/RJ45-DIN using the power supply specifications on the product label and the following information.

> ⚠️ ***Observe proper ESD techniques when connecting and disconnecting the ICDM-RX/xxx*-2ST/ RJ45-DIN*.**

   a. If the DIN rail is not connected to earth ground, insert the earth ground wire into the chassis ground screw terminal.
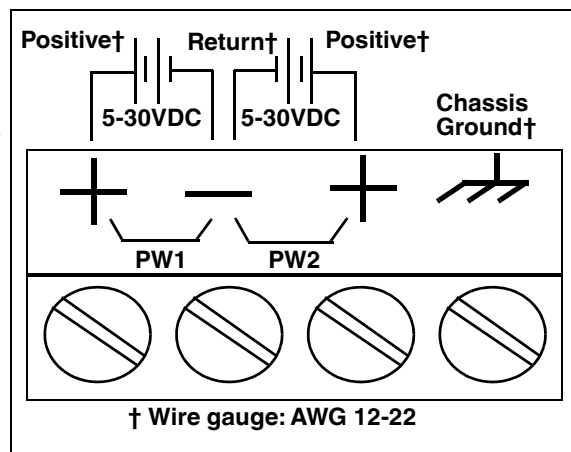
   *Note:* *The chassis ground connection is made only if the DIN rail is NOT connected to earth ground.*

   b. Insert the DC positive wire into the + screw terminal and the DC return wire into the - screw terminal.

      Refer to *ICDM-RX/xxx-2ST/RJ45-DIN Power Supply* on Page 97 for power requirements.

   c. Use a small flat head screw driver to lock the wires into place.

   d. Verify that each wire has been tightened securely.

   e. Connect a UL Listed power supply and UL Listed power cord to a power source to apply power.

*Note:* *Do not connect multiple units until you have changed the default IP address, see Preparing the ICDM-RX for Configuration on Page 21*



**Signal Ground†**    **Chassis Ground†**    **5-30VDC**

**Return†**    **Positive†**

**† Wire gauge: AWG 12-22**

**Signal Ground is used to connect RS-232 devices later in the installation.**

3. Connect the **10/100 port** to the same Ethernet network segment as the host PC using a standard network cable.

**PEPPERL+FUCHS**

4.  Verify that the **STATUS** LED has completed the boot cycle and network connection for the ICDM-RX/**xxx**-2ST/RJ45-DIN is functioning properly using the following table.

| ICDM-RX/**xxx**-2ST/RJ45-DIN LED Descriptions | |
|---|---|
| **STATUS** | The **STATUS** LED is lit, indicating you have power and it has completed the boot cycle.<br><br>The **STATUS** LED flashes while booting and it takes approximately 15 seconds for the Bootloader to complete the cycle. When the Bootloader completes the cycle, the LED has a solid, steady light that blinks approximately every 10 seconds.<br><br>*If PN or PN1 model:*<br><br>When the Bootloader completes the cycle, the LED flashes rapidly for several times then stays off and blinks approximately every 10 seconds when there is no PLC connection. |
| **LINK** | If the **LINK** (green) LED is lit, it indicates a working Ethernet connection. |
| **ACT** | If the **ACT** (yellow) LED flashes, it indicates network activity. |
| *Note:* For additional LED information, go to the Status LED table on Page 61. | |

> ⚠️ *Do not connect RS-422/485 devices until the IP address is configured and an appropriate port interface type has been configured. The default port setting is RS-232.*

5.  Go to *Preparing the ICDM-RX for Configuration* on Page 21 for default network settings and how to configure the ICDM-RX/**xxx**-2ST/RJ45-DIN for use.

**PEPPERL+FUCHS**

## 2.5. ICDM-RX/*xxx*-2DB9RJ45-DIN Installation

Use the following procedure to install the ICDM-RX/*xxx*-2DB9RJ45-DIN.

1.  Attach the ICDM-RX/*xxx*-2DB9RJ45-DIN to the DIN rail adapter.

2.  Connect the power supply and apply power to the ICDM-RX/*xxx*-2DB9RJ45-DIN using the power supply specifications on the product label and the following information.

⚠️ ***Observe proper ESD techniques when connecting and disconnecting the ICDM-RX/xxx-2DB9RJ45-DIN.***

a.  If the DIN rail is not connected to earth ground, insert the earth ground wire into the chassis ground screw terminal.

***Note:*** *The chassis ground connection is made only if the DIN rail is NOT connected to earth ground.*



**† Wire gauge: AWG 12-22**
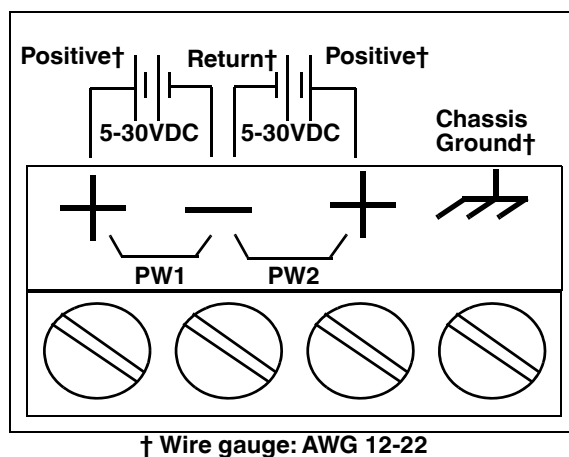
b.  Insert the DC positive wire into one of the + screw terminals and the DC return wire into the - screw terminal.

A second redundant power supply can be connected to the unit by inserting the DC positive wire into the other + screw terminal and the DC return wire into the - screw terminal. The ICDM-RX/*xxx*-2DB9RJ45-DIN continues to operate if one of the two connected power supplies should fail.

Refer to *ICDM-RX/xxx-2DB9RJ45-DIN Power Supply* on Page 98 for detailed power requirements.

c.  Use a small flat head screw driver to lock the wires into place.

d.  Verify that each wire has been tightened securely.

e.  Connect a UL Listed power supply and UL Listed power cord to a power source to apply power.

***Note:*** *Do not connect multiple units until you have changed the default IP address, see Preparing the ICDM-RX for Configuration on Page 21.*

**PEPPERL+FUCHS**

3.  Connect the **10/100 port** to the same Ethernet network segment as the host PC using a standard network cable.

4.  Verify that the **STATUS** LED has completed the boot cycle and network connection for the ICDM-RX/**xxx**-2DB9RJ45-DIN is functioning using the following table.

| ICDM-RX/*xxx*-2DB9RJ45-DIN LED Descriptions | |
| --- | --- |
| **STATUS** | The **STATUS** LED is lit, indicating you have power and it has completed the boot cycle.<br><br>The **STATUS** LED flashes while booting and it takes approximately 15 seconds for the Bootloader to complete the cycle. When the Bootloader completes the cycle, the LED has a solid, steady light that blinks approximately every 10 seconds.<br><br>*If PN or PN1 model:*<br><br>When the Bootloader completes the cycle, the LED flashes rapidly for several times then stays off and blinks approximately every 10 seconds when there is no PLC connection. |
| **LINK** | If the **LINK** (green) LED is lit, it indicates a working Ethernet connection. |
| **ACT** | If the **ACT** (yellow) LED flashes, it indicates network activity. |
| *Note:* For additional LED information, go to the <u>Status LED table</u> on Page 61. | |

⚠️ ***Do not connect RS-422/485 devices until the IP address is configured and an appropriate port interface type has been configured. The default port setting is RS-232.***

5.  Go to *Preparing the ICDM-RX for Configuration* on Page 21 for default network settings and how to configure the ICDM-RX for use.

3/7/20

**PEPPERL+FUCHS**

## 2.6. ICDM-RX/*xxx*-4DB9/2RJ45-DIN Installation

Use the following procedure to install ICDM-RX/*xxx*-4DB9/2RJ45-DIN.

1.  Attach the ICDM-RX/*xxx*-4DB9/2RJ45-DIN to the DIN rail adapter.

2.  Connect the power supply and apply power to the ICDM-RX/*xxx*-4DB9/2RJ45-DIN using the power supply specifications on the product label and the following information.

> ⚠️ *Observe proper ESD techniques when connecting and disconnecting the ICDM-RX/xxx-4DB9/2RJ45-DIN.*

a.  If the DIN rail is not connected to earth ground, insert the earth ground wire into the chassis ground screw terminal.

*Note:* *The chassis ground connection is made only if the DIN rail is NOT connected to earth ground.*

b.  Insert the DC positive wire into one of the + screw terminals and the DC return wire into the - screw terminal.

   • A second redundant power supply can be connected to the unit by inserting the DC positive wire into the other + screw terminal and the DC return wire into the - screw terminal.

   • The ICDM-RX/*xxx*-4DB9/2RJ45-DIN continues to operate if one of the two connected power supplies should fail.

   Refer to *ICDM-RX/xxx-4DB9/2RJ45-DIN Power Supply* on Page 99 for detailed power requirements.



**† Wire gauge: AWG 12-22**

c.  Use a small flat head screw driver to lock the wires into place.

d.  Verify that each wire has been tightened securely.

e.  Connect a UL Listed power supply and UL Listed power cord to a power source to apply power.

*Note:* *Do not connect multiple units until you have changed the default IP address, see Preparing the ICDM-RX for Configuration on Page 21*

3.  Connect one of the **10/100** ports to the same Ethernet network segment as the host PC using a standard Ethernet cable. You can daisy-chain another ICDM-RX or Ethernet device to the other port using a standard Ethernet cable.

*Note:* *PN and PN1 models: these models provide two Ethernet ports, E1 is the first port and E2 is the second port.*
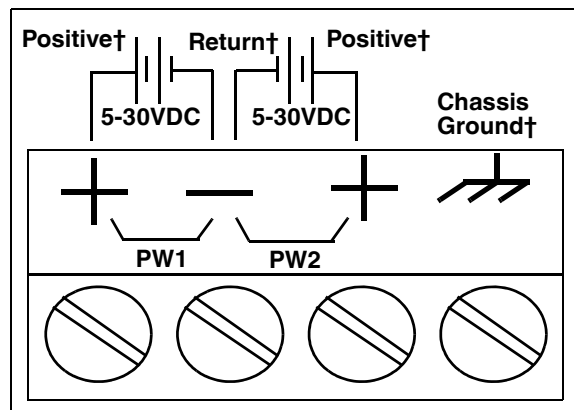
**PEPPERL+FUCHS**

4. Verify that the **STATUS** LED has completed the boot cycle and network connection for the ICDM-RX is functioning properly using the following table.

| ICDM-RX/*xxx*-4DB9/2RJ45-DIN LED Descriptions | |
|---|---|
| **STATUS** | The **STATUS** LED is lit, indicating you have power and it has completed the boot cycle. |
| | The **STATUS** LED flashes while booting and it takes approximately 15 seconds for the Bootloader to complete the cycle. When the Bootloader completes the cycle, the LED has a solid, steady light that blinks approximately every 10 seconds. |
| | ***If PN or PN1 model:*** |
| | When the Bootloader completes the cycle, the LED flashes rapidly for several times then stays off and blinks approximately every 10 seconds when there is no PLC connection. |
| **LINK** | If the **LINK** (green) LED is lit, it indicates a working Ethernet connection. |
| **ACT** | If the **ACT** (yellow) LED flashes, it indicates network activity. |
| *Note:* For additional LED information, go to the *S*tatus LED table *on Page 100.* | |

⚠️ **Do not connect RS-422/485 devices until the IP address is configured and an appropriate port interface type has been configured. The default port setting is RS-232.**

5. Go to *Preparing the ICDM-RX for Configuration* on Page 21 for default network settings and how to configure the ICDM-RX/*xxx*-4DB9/2RJ45-DIN for use.

## 2.7. Adding a Unit to an Existing Installation

Use this procedure to add another ICDM-RX to an existing configuration.

1. Install the ICDM-RX to an Ethernet hub or server NIC using the appropriate subsection found in this chapter.

   *Note:* Technical support recommends installing one unit at a time and testing that unit when installing multiple units. In the event troubleshooting must be done, a single unit is easier to resolve than several at once.

2. Power-up the new ICDM-RX and verify that the **PWR** or **STATUS** LED lights.

3. Program an IP address into the new ICDM-RX using PortVision DX.

4. If necessary, upload the latest firmware.

5. Configure serial ports to support the serial devices or upload configuration files from PortVision DX.

6. Connect the serial devices.

**PEPPERL+FUCHS**

## 2.8. Replacing Hardware

Use this procedure to replace hardware.

1. Remove the old unit and attach a new or spare ICDM-RX.
2. Connect the new ICDM-RX to the network hub or server NIC.
3. Apply power to the new ICDM-RX and verify that it passes the power on self-test.
4. Program the IP address of the new ICDM-RX.
5. If necessary, upload the latest protocol firmware.
6. Configure any ports as necessary to match the previous unit or upload configuration files from PortVision DX.
7. Transfer *all* cabling from the old ICDM-RX to the new ICDM-RX.
8. *It is not necessary* to shut down and restart the host PC.

**PEPPERL+FUCHS**

# 3. Preparing the ICDM-RX for Configuration

The ICDM-RX platform includes PortVision DX, which is the management and configuration application for Windows that you can use to manage the ICDM-RX.

This section contains these topics:

- *PortVision DX Overview*
- *PortVision DX Requirements* on Page 21
- *Installing PortVision DX* on Page 22
- *Configuring the Network Settings* on Page 25
- *Checking the Protocol Firmware Version* on Page 28
- *Uploading Firmware on the ICDM-RX* on Page 29

***Note:*** *If PortVision DX is already installed, go directly to Configuring the Network Settings on Page 25 to change the IP address on the ICDM-RX.*

## 3.1. PortVision DX Overview

PortVision DX automatically detects Pepperl+Fuchs Comtrol Ethernet-attached products physically attached to the local network segment so that you can configure the network address, upload firmware, and manage the following products:

- ICDM-RX family
- IO-Link Master (ICE2 and ICE3 models)
- RocketLinx managed switches

In addition to identifying Pepperl+Fuchs Comtrol Ethernet-attached products, you can use PortVision DX to display any third-party switch and hardware that may be connected directly to those devices. All non-Pepperl+Fuchs products and unmanaged RocketLinx switches are treated as non-intelligent devices and have limited feature support. For example, you cannot configure or update firmware on a third-party switch.

## 3.2. PortVision DX Requirements

Use PortVision DX to identify, configure, update, and manage the ICDM-RX on Windows operating systems.

PortVision DX requires that you connect the Pepperl+Fuchs Comtrol Ethernet-attached product to the same network segment as the Windows host system if you want to be able to scan and locate it automatically during the configuration process.

Before installing PortVision DX, consider the following:

- Use PortVision DX to upload firmware and apply changes to a ICDM-RX that is on the same local network segment as the system on which PortVision DX is installed. You cannot apply changes through PortVision DX to a ICDM-RX that is not on the same local network segment.
- Use PortVision DX to monitor any ICDM-RX on the network. The ICDM-RX does not have to be on the same local network segment as PortVision DX for monitoring purposes.

3/7/20

**PEPPERL+FUCHS**

## 3.3. Installing PortVision DX

During initial configuration, PortVision DX automatically detects and identifies ICDM-RX units, if they are in the same network segment.

You can download the latest version of PortVision DX.

1. Download PortVision DX from https://www.pepperl-fuchs.com.
2. Execute the **PortVision_DX[version].msi** file.
3. Click **Next** on the *Welcome* screen.
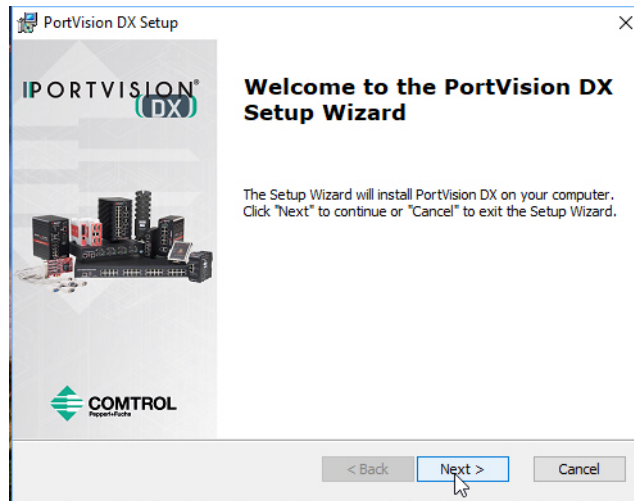


4. Click **I accept the terms in the License Agreement** and **Next**.

**PEPPERL+FUCHS**
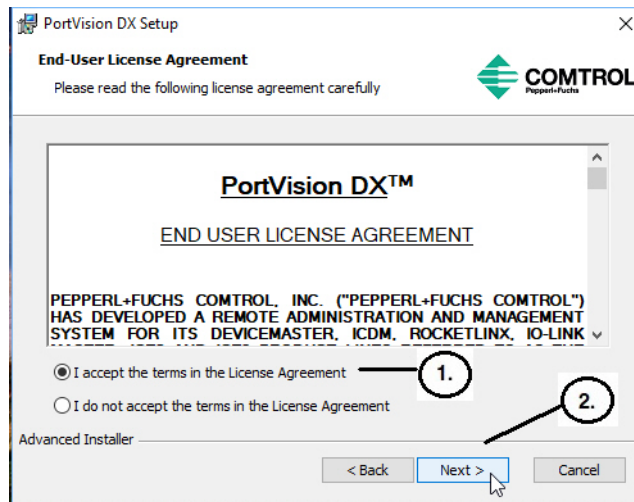
5. Click **Next** or optionally, browse to a different location and then click **Next**.
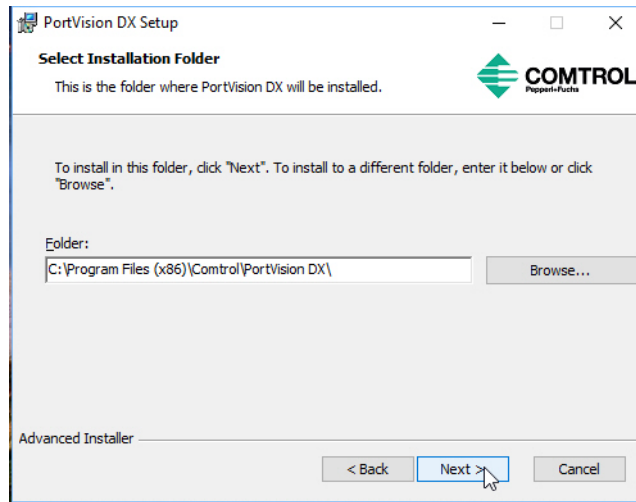
6. Click **Next** to configure the shortcuts.

**PEPPERL+FUCHS**
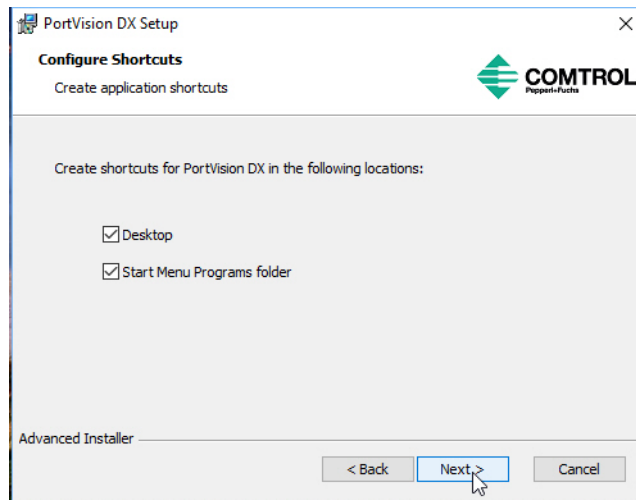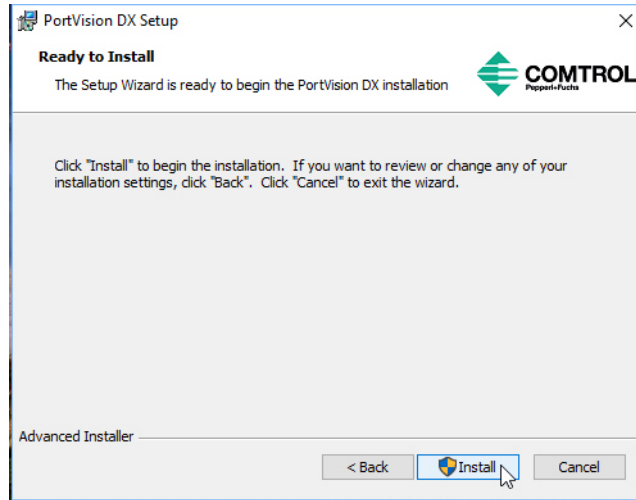
7.  Click **Install**.



8.  Depending on the operating system, you may need to click **Yes** to the *Do you want to allow the following program to install software on this computer?* query.

9.  Click **Launch PortVision DX** and **Finish** in the last installation screen.
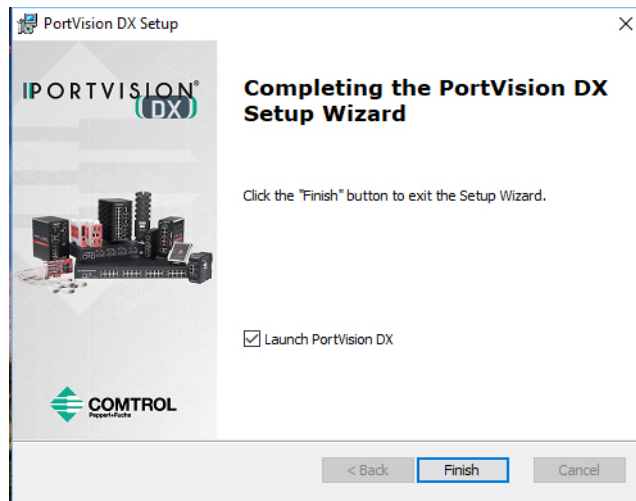


10. Depending on the operating system, you may need to click **Yes** to the *Do you want to allow the following program to make changes to this computer?* query.

PEPPERL+FUCHS

11. Select the Pepperl+Fuchs Comtrol Ethernet-attached products that you want to locate and then click **Scan**.

> **Note:** *If the Pepperl+Fuchs Comtrol Ethernet-attached product is not on the local segment and it has been programmed with an IP address, it will be necessary to manually add the Pepperl+Fuchs Comtrol Ethernet-attached product to PortVision DX.*

12. Go to Step 5 in the next section, *Configuring the Network Settings*, to program the ICDM-RX network settings.

If you need additional information about PortVision DX, refer to the **Help** system.

*You can save time if you only scan for ICDM-RXs.*
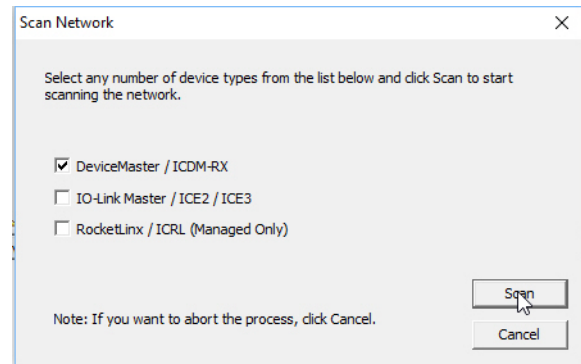
## 3.4. Configuring the Network Settings

Use the following procedure to change the default network settings on the ICDM-RX for your network. The default network settings are;

- IP address: 192.168.250.250
- Subnet mask: 255.255.0.0
- Gateway address: 192.168.250.1

> **Note:** *Technical Support advises configuring one new ICDM-RX at a time to avoid device driver configuration problems. If you want to configure multiple ICDM-RXs using the **Assign IP to Multiple Devices** option, see Configuring Multiple ICDM-RXs Network Addresses on Page 68.*

The following procedure shows how to configure a single ICDM-RX connected to the same network segment as the Windows system. If the ICDM-RX is not on the same physical segment, you can add it manually using *Adding a New Device in PortVision DX* on Page 68.

1. If you have not done so, install PortVision DX (*Installing PortVision DX* on Page 22).

2. Start PortVision DX using the **PortVision DX** desktop shortcut or from the **Start** button, click **Pepperl+Fuchs Comtrol > PortVision DX**.

3. Depending on your operating system, you may need to click **Yes** to the *Do you want to allow the following program to make changes to this computer?* query.

4. Click **Scan** to locate the Pepperl+Fuchs Comtrol Ethernet-attached products including the ICDM-RX on the network.
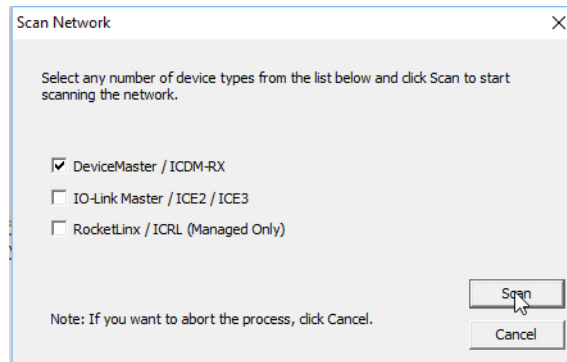
> **Note:** *If you do not have any RocketLinx managed switches or IO-Link Master (ICE2 and ICE3 models), it saves scanning time if you do not scan for them.*

**PEPPERL+FUCHS**

5. Highlight the ICDM-RX for which you want to program network information and open the **Properties** screen using one of these methods.

- Double-click the ICDM-RX in the *Device Tree* or *Device List* pane.
- Right-click the ICDM-RX in the *Device Tree* or *Device List* pane and click **Properties** in the popup menu
- Highlight the ICDM-RX in the *Device Tree* or *Device List* pane and click the **Properties** button.
- Highlight the ICDM-RX, click the **Manage** menu and then **Properties**.
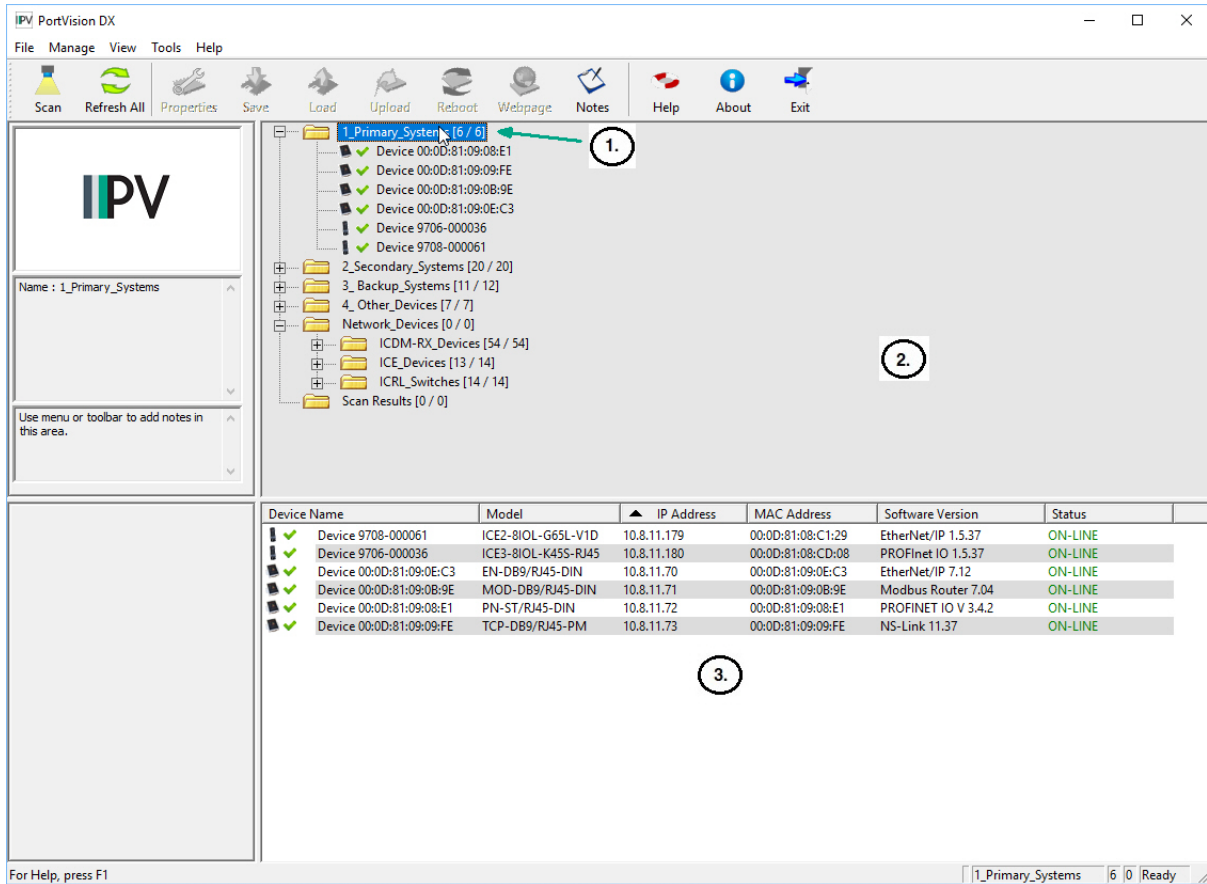


1. The contents of this folder is displayed in the **Device List** pane below. You can expand the tree and also view the devices in the **Device Tree** pane.
2. **Device Tree** pane
3. **Device List** pane

**PEPPERL+FUCHS**

4. *Optionally*, rename the ICDM-RX in the **Device Name** field.
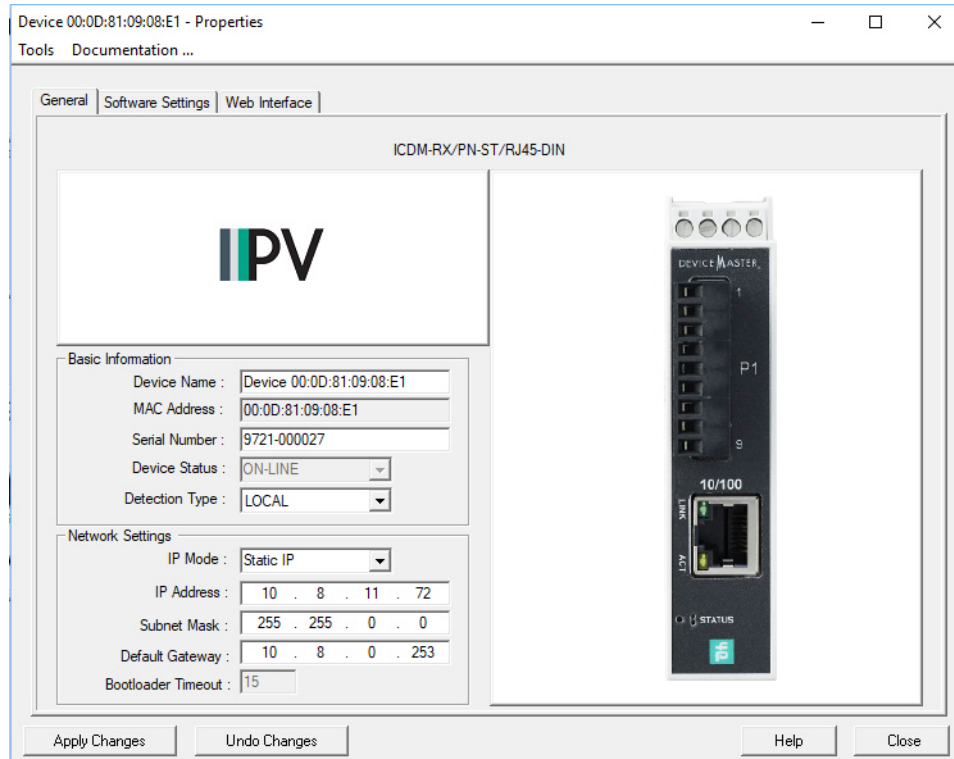


**Note:** *The MAC address Device Status fields are automatically populated and you cannot change those values.*

5. Optionally, enter the serial number, which is on a label on the ICDM-RX.

6. If necessary, you can change the **Detection Type**.
   - **REMOTE** means that the ICDM-RX is not connected to this segment of the network and it uses IP communications.
   - **LOCAL** means that the ICDM-RX is on this local network segment and uses UDP communications.

7. Change the ICDM-RX network properties as required for your site.

| DHCP IP† | Click this option if you want to use the ICDM-RX with DHCP. Make sure that you provide the MAC address of the ICDM-RX to the network administrator. |
|---|---|
| Static IP† | Click this option to program a static IP address and type the appropriate IP address, subnet mask, and default gateway values for your site in the provided boxes. |
| † **PROFINET IO:** *The network address entered here must be compatible with the IP address configuration entered in the TIA Portal project. See the ICDM-RX/PN Installation and Configuration manual for information about assigning addresses.* | |

**Note:** *For additional information, open the PortVision DX Help system.*

8. Click **Apply Changes** to update the network information on the ICDM-RX.

9. Click **Close** to exit the *Properties* window.

10. If if applicable, check your firmware version to make sure that it is the latest version using the next subsection, *Checking the Protocol Firmware Version*.

11. If necessary, use *Uploading Firmware on the ICDM-RX* on Page 29 to update or load the firmware for your ICDM-RX.

3/7/20

**PEPPERL+FUCHS**

## 3.5. Checking the Protocol Firmware Version

Use PortVision DX to check the firmware version before configuring the ports.

Depending on the model you purchased, the ICDM-RX may or may not have the protocol firmware loaded.

**Note:** *Models that have a protocol loaded on the ICDM-RX are identified in PortVision DX and the ICDM-RX is labeled accordingly.*

The following procedure shows how to use PortVision DX to check the firmware version on the ICDM-RX and check for the latest files.

**Note:** *If you have not done so, install PortVision DX (Installing PortVision DX on Page 22).*

1.  Start PortVision DX by double-clicking the PortVision DX desktop icon or click **Pepperl+Fuchs Comtrol > PortVision DX**.

2.  Examine the *List View* pane to see if or/and what version of the firmware is loaded on the ICDM-RX.
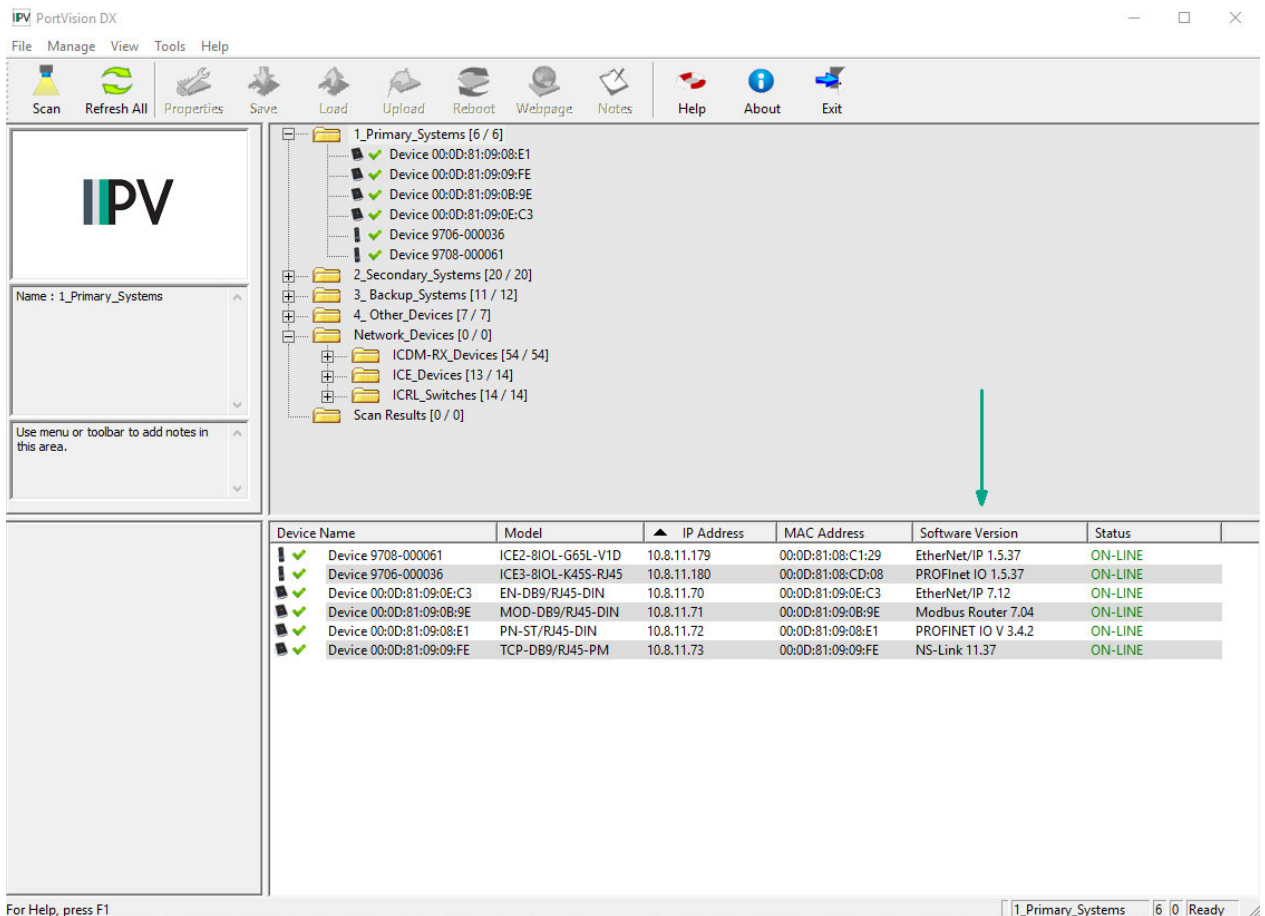


3.  Check https://www.pepperl-fuchs.com to see if there is a later version available.

    **ICDM-RX/MOD models only:** *By default, ICDM-RX/MOD models are loaded with Modbus Router. If you want to implement the Modbus Server or Modbus TCP platform, you must go to https://www.pepperl-fuchs.com, download the appropriate firmware, and upload it to your ICDM-RX/MOD.*

4.  If applicable, download the latest version and go to Step 3 in *Uploading Firmware on the ICDM-RX* on Page 29.

3/7/20

**PEPPERL+FUCHS**

## 3.6. Uploading Firmware on the ICDM-RX

You can verify that you have the latest firmware by checking https://www.pepperl-fuchs.com.

**Note:** ***ICDM-RX/MOD models only:***
*By default, ICDM-RX/MOD models are loaded with Modbus Router. If you want to implement the Modbus Server or Modbus TCP platform, you must go to https://www.pepperl-fuchs.com, download the appropriate firmware, and upload it to your ICDM-RX/MOD.*

If necessary, use the following procedure to update the firmware on your ICDM-RX for the appropriate protocol.

**Note:** *If you have not done so, install PortVision DX (Installing PortVision DX on Page 22) and install the firmware.msi file.*

1. Execute the **.msi** file that you downloaded for the firmware.

2. Start PortVision DX by double-clicking the PortVision DX desktop icon or click **Pepperl+Fuchs Comtrol > PortVision DX**.

3. Right-click the device or devices for which you want to upload firmware and click the **Advanced > Upload Firmware** menu option.
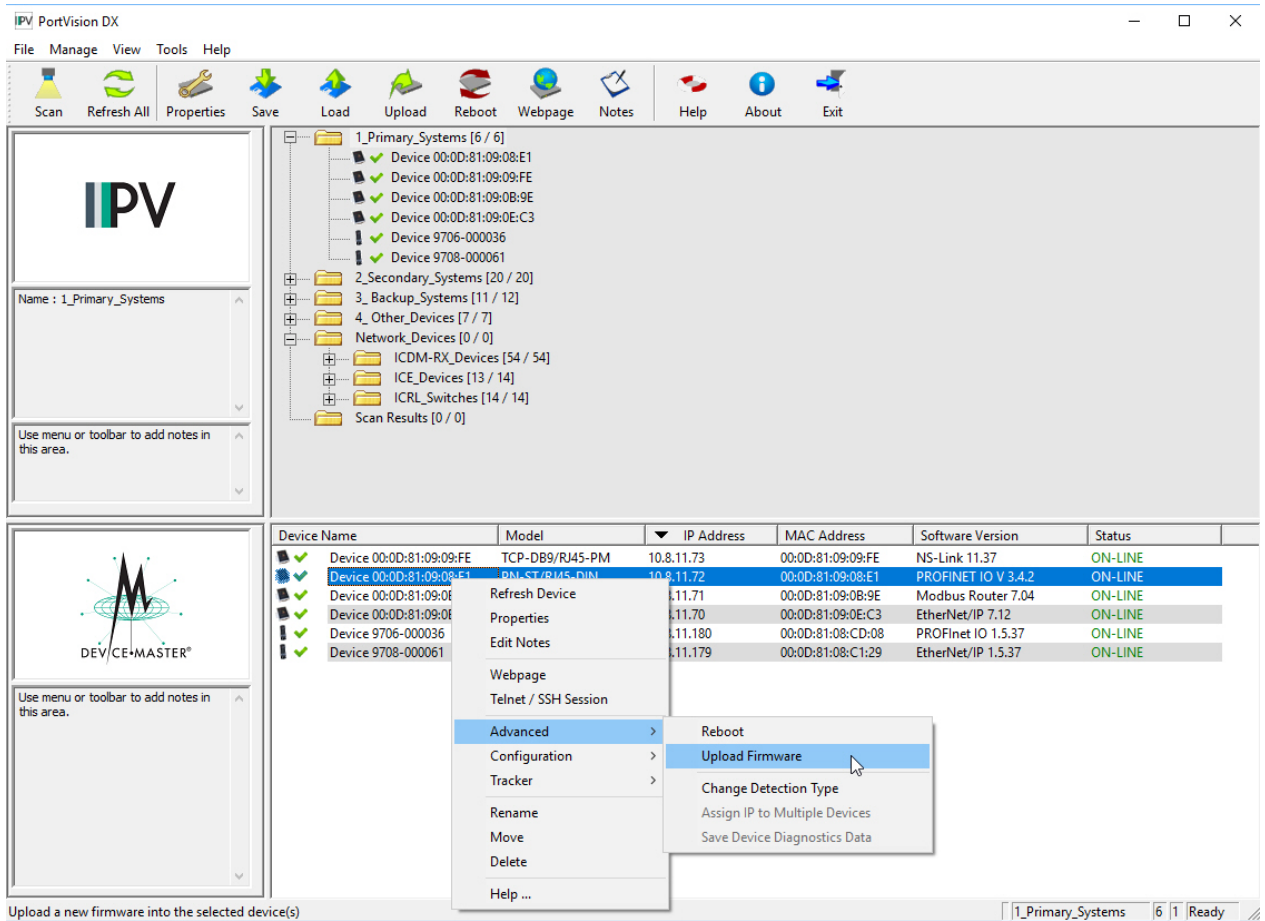


**Note:** *Optionally, you can highlight a device and use the **Load** button.*

4. Browse and select the protocol firmware (**.cmtl**) file and click **Open**.

**PEPPERL+FUCHS**

5. Click **Yes** to upload the firmware.
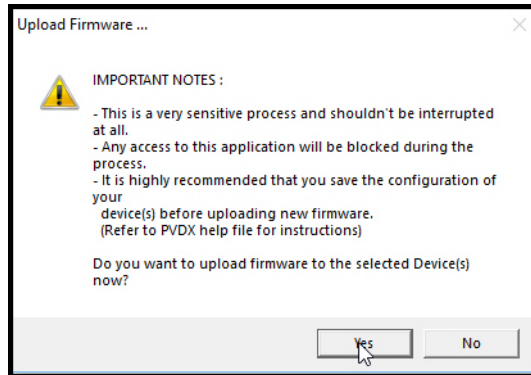


6. Click **OK** to the advisory message about waiting until the ICDM-RX is on-line and in the next minute the ICDM-RX unit or units should display **ON-LINE** in the **Status** field depending on the polling rate. If necessary, click **Refresh**.

7. Download the appropriate *User Manual* for your protocol for information about configuring the serial port or ports using the web page and programming your PLCs.

8. If you are planning on installing multiple ICDM-RXs, you may want to use the *Save/Load Configuration File* feature in PortVision DX.

   A configuration file can contain network settings and protocol settings. Refer to the PortVision DX help system or *Using Configuration Files* on Page 75 for detailed information.

9. After configuring the serial port characteristics and preparing your PLC programs, you can use the next section in this guide, to attach the serial device or devices.

**PEPPERL+FUCHS**

# 4. ICDM-RX Security

This subsection provides a basic understanding of the ICDM-RX security options, and the repercussions of setting these options. See *Restoring Defaults* on Page 81 if you want to return the ICDM-RX settings to their default values.

## 4.1. Understanding Security Methods and Terminology

The following table provides background information and definitions.

| Term or Issue Explanation | |
|---|---|
| CA (Client Authentication certificate) † | If configured with a CA certificate, the ICDM-RX requires all SSL/TLS clients to present an RSA identity certificate that has been signed by the configured CA certificate. As shipped, the ICDM-RX is not configured with a CA certificate and all SSL/TLS clients are allowed. |
| | This uploaded CA certificate that is used to validate a client's identity is sometimes referred to as a *trusted root certificate*, a *trusted authority certificate*, or a *trusted CA certificate*. This CA certificate might be that of a trusted commercial certificate authority or it may be a privately generated certificate that an organization creates internally to provide a mechanism to control access to resources that are protected by the SSL/TLS protocols. |
| | See *Key and Certificate Management* on Page 43 for more information. This section does not discuss the creation of CA Certificates. |
| Client Authentication | A process using paired keys and identity certificates to prevent unauthorized access to the ICDM-RX. Client authentication is discussed in *Client Authentication* on Page 38 and *Changing Keys and Certificates* on Page 46. |
| DH Key Pair Used by SSL Servers † | This is a private/public key pair that is used by some cipher suites to encrypt the SSL/TLS handshaking messages. Possession of the private portion of the key pair allows an eavesdropper to decrypt traffic on SSL/TLS connections that use DH encryption during handshaking. |
| | The DH (Diffie-Hellman) key exchange, also called exponential key exchange, is a method of digital encryption that uses numbers raised to specific powers to produce decryption keys on the basis of components that are never directly transmitted, making the task of a would-be code breaker mathematically overwhelming. |
| | The most serious limitation of Diffie-Hellman (DH key) in its basic or *pure* form is the lack of authentication. Communications using Diffie-Hellman all by itself are vulnerable to man in the middle attacks. Ideally, Diffie-Hellman should be used in conjunction with a recognized authentication method such as digital signatures to verify the identities of the users over the public communications medium. |
| | See *Certificates and Keys* on Page 38 and *Key and Certificate Management* on Page 43 for more information. |
| *† All ICDM-RX units are shipped from the factory with identical configurations. They all have the identical, self-signed, Pepperl+Fuchs Server RSA Certificates, Server RSA Keys, Server DH Keys, and no Client Authentication Certificates. For maximum data and access security, you should configure all ICDM-RX units with custom certificates and keys.* | |

**PEPPERL+FUCHS**

| Term or Issue Explanation (Continued) | |
|---|---|
| Digital Certificate | A digital certificate is an electronic *credit card* that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Some digital certificates conform to a standard, X.509. Digital certificates can be kept in registries so that authenticating users can look up other users' public keys.<br><br>See *Key and Certificate Management* on Page 43 for more information. |
| PKI (public key infrastructure) | A public key infrastructure (PKI) enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. Although the components of a PKI are generally understood, a number of different vendor approaches and services are emerging. Meanwhile, an Internet standard for PKI is being worked on.<br><br>The public key infrastructure assumes the use of public key cryptography, which is the most common method on the Internet for authenticating a message sender or encrypting a message. Traditional cryptography has usually involved the creation and sharing of a secret key for the encryption and decryption of messages. This secret or private key system has the significant flaw that if the key is discovered or intercepted by someone else, messages can easily be decrypted. For this reason, public key cryptography and the public key infrastructure is the preferred approach on the Internet. (The private key system is sometimes known as symmetric cryptography and the public key system as asymmetric cryptography.)<br><br>A public key infrastructure consists of:<br><br>• A certificate authority (CA) that issues and verifies digital certificate. A certificate includes the public key or information about the public key<br><br>• A registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requestor<br><br>• One or more directories where the certificates (with their public keys) are held<br><br>• A certificate management system<br><br>For more information, see *SSL Authentication* on Page 37, *SSL Performance* on Page 39, *SSL Cipher Suites* on Page 40, and *ICDM-RX Supported Cipher Suites* on Page 40. |

| Term or Issue Explanation (Continued) | |
|---|---|
| RSA Key Pair† | This is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption. RSA is widely used in electronic commerce protocols, and is believed to be sufficiently secure given sufficiently long keys and the use of up-to-date implementations. The system includes a communications channel coupled to at least one terminal having an encoding device, and to at least one terminal having a decoding device.<br><br>• Public key is a value provided by some designated authority as an encryption key that, combined with a private key derived from the public key, can be used to effectively encrypt messages and digital signatures.<br><br>• Private Key<br>  - One half of the *key pair* used in conjunction with a public key<br>  - Both the public and the private keys are needed for encryption /decryption but only the owner of a private key ever needs to know it. Using the RSA system, the private key never needs to be sent across the Internet.<br>  - The private key is used to decrypt text that has been encrypted with the public key.<br>    Thus, if *User A* sends *User B* a message, *User A* can find out *User B's* public key (but not *User B's* private key) from a central administrator and encrypt a message to *User B* using *User B's* public key. When *User B* receives it, *User B* decrypts it with *User B's* private key. In addition to encrypting messages (which ensures privacy), *User B* can authenticate *User B* to *User A* (so that *User A* knows that it is really *User B* who sent the message) by using *User B's* private key to encrypt a digital certificate.<br><br>See *Key and Certificate Management* on Page 43 for more information. |
| SSH (Secure Shell) | Secure Shell (SSH) allows data to be exchanged using a secure channel between two networked devices. Replaces telnet which has no security. SSH requires password authentication – even if the password is empty.<br><br>See *SSH Server* on Page 37 for more information. |
| SSL (Secure Sockets Layer) | The Secure Sockets Layer (SSL) is the predecessor of (TLS) Transport Layer Security.<br><br>SSL is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers.<br><br>SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. Developed by Netscape, SSL also gained the support of Microsoft and other Internet client/server developers as well and became the de facto standard until evolving into Transport Layer Security.<br><br>SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.<br><br>See Pages 37 through 40 for detailed information about SSL.<br><br>***Note:*** *Two slightly different SSL protocols are supported by the ICDM-RX: SSLv3 and TLSv1.* |
| TLS (Transport Layer Security) | Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).<br><br>TLS and SSL are not interoperable. The TLS protocol does contain a mechanism that allows TLS implementation to back down to SSL 3.0. |
| **Secure Config Mode** | Unencrypted access to administrative and diagnostic functions are disabled. See *Secure Config Mode* on Page 36 and *Configure/Enable Security Features Overview* on Page 42 for more information. |

**PEPPERL+FUCHS**

| Term or Issue Explanation (Continued) | |
|---|---|
| *Man in the Middle attack* | A man in the middle attack is one in which the attacker intercepts messages in a public key exchange and then retransmits them, substituting his own public key for the requested one, so that the two original parties still appear to be communicating with each other. |
| | The attack gets its name from the ball game where two people try to throw a ball directly to each other while one person in between them attempts to catch it. In a man in the middle attack, the intruder uses a program that appears to be the server to the client and appears to be the client to the server. The attack may be used simply to gain access to the message, or enable the attacker to modify the message before retransmitting it. |
| *How Public and Private Key Cryptography Works* | In public key cryptography, a public and private key are created simultaneously using the same algorithm (a popular one is known as RSA) by a certificate authority (CA). |
| | The private key is given only to the requesting party and the public key is made publicly available (as part of a digital certificate) in a directory that all parties can access. |
| | The private key is never shared with anyone or sent across the Internet. You use the private key to decrypt text that has been encrypted with your public key by someone else (who can find out what your public key is from a public directory). |
| | Thus, if *User A* sends *User B* a message, *User A* can find out *User B's* public key (but not *User B's* private key) from a central administrator and encrypt a message to *User B* using *User B's* public key. When *User B* receives it, *User B* decrypts it with *User B's* private key. In addition to encrypting messages (which ensures privacy), *User B* can authenticate *User B* to *User A* (so *User A* knows that it is really *User B* who sent the message) by using *User B's* private key to encrypt a digital certificate. When *User A* receives it, *User A* can use *User B's* public key to decrypt it. |
| *Who Provides the Infrastructure?* | A number of products are offered that enable a company or group of companies to implement a PKI. The acceleration of e-commerce and business-to-business commerce over the Internet has increased the demand for PKI solutions. Related ideas are the virtual private network (VPN) and the IP Security (IPsec) standard. Among PKI leaders are: |
| | • RSA, which has developed the main algorithms used by PKI vendors. |
| | • Verisign, which acts as a certificate authority and sells software that allows a company to create its own certificate authorities. |
| | • GTE CyberTrust, which provides a PKI implementation methodology and consultation service that it plans to vend to other companies for a fixed price. |
| | • Xcert, whose Web Sentry product that checks the revocation status of certificates on a server, using the Online Certificate Status Protocol (OCSP). |
| | • Netscape, whose Directory Server product is said to support 50 million objects and process 5,000 queries a second; Secure E-Commerce, which allows a company or extranet manager to manage digital certificates; and Meta-Directory, which can connect all corporate directories into a single directory for security management. |

The following topic references are from: http://searchsecurity.techtarget.com/

• PKI (public key infrastructure)

• How Public/Private Key Cryptography Works

• Who Provides the Infrastructure

• Digital Certificate

• DH Key

• Man in the Middle attack

The RSA Key pair topic reference is from: http://en.wikipedia.org/wiki/RSA

**PEPPERL+FUCHS**

## 4.2. TCP and UDP Socket Ports Used by the ICDM-RX

Following list is all of the logical TCP and UDP socket ports implemented in ICDM-RXs.

| Socket Port Number Descriptions | |
|---|---|
| 22 SSH<br>23 Telnet | TCP Ports 22 (ssh) and 23 (telnet) are used for administrative and diagnostic purposes and aren't required for normal use and are enabled by default and Port 23 may be disabled. |
| 80 HTTP<br>443 SSL or HTTPS | TCP Ports 80 (http) and 443 (https) are used by the web server for administration and configuration and are enabled by default and cannot be disabled. |
| 161 SNMP | UDP Port 161 is used by the SNMP agent if SNMP is enabled which is the default. |
| 4606 | TCP Port 4606 is required if you want to use the web interface or PortVision DX if you want to update firmware without setting up a TFTP server and this port cannot be disabled. |
| 4607 | TCP Port 4607 is only used for diagnostic purposes and is not required for normal operation and this port cannot be disabled. |
| TCP 8000 - 8xxx | Incremented per serial port on the ICDM-RX.<br>For example: An ICDM-RX 4-port would have Ports 8000 through 8003. |
| UDP 7000 - 7xxx | Incremented per serial port on the ICDM-RX.<br>For example: An ICDM-RX 4-port would have Ports 7000 through 7003. |

**PEPPERL+FUCHS**

## 4.3. ICDM-RX Security Features

The following subsections provide information about ICDM-RX security features.

### 4.3.1. Secure Config Mode

The ICDM-RX supports Secure Config mode.

| Security Mode Information | |
|---|---|
| **Secure Config** | Encrypts/authenticates configuration and administration operations (web server, IP settings, load SW, and so forth.). **Secure Config mode**: <br>• Disables MAC mode admin commands except for ID request†. <br>• Disables TCP/IP admin commands except for ID request†. <br>• Disables telnet console access (Port 23)†. <br>• Disables unencrypted http:// access via Port 80. <br>• Disables e-mail notification and SNMP features. <br>• Two values for http READ and WRITE commands: A3: Enable. |
| † *Affects both RedBoot and the default application for your protocol.* | |

### 4.3.2. Security Comparison

This table displays addition information about security feature comparisons.

| | **Weakest** | | | | **Strongest** |
|---|---|---|---|---|---|
| | 0 | 1 | 2 | 3 | 4 |
| **Supported by** | None | Password | Authentication | Secure Config | Key & Certificate |
| RedBoot | yes | yes | yes | no | no |
| TCP to Serial Ports | yes | yes | yes | no | no |
| SSH to Serial Ports | no | no | no | yes | yes |
| UDP to Serial Ports | yes | yes | yes | disabled | disabled |
| Telnet/Port23 | yes | yes | yes | disabled | disabled |
| SSH Telnet/Port 22 | yes | yes | yes | yes | yes |
| Telnet Port 4607 | yes | yes | yes | disabled | yes |
| SSH (PuTTY) 4607 | no | no | no | yes | disabled |
| HTTP (Port 80) | yes | yes | yes | disabled | disabled |
| HTTPS (Port 443) | no | no | no | yes | yes |
| Email | yes | yes | yes | disabled | disabled |
| SNMP | yes | yes | yes | disabled | disabled |

3/7/20

**PEPPERL+FUCHS**

### 4.3.3. SSH Server

The ICDM-RX SSH server has the following characteristics:

- Requires password authentication – even if the password is empty.
- Enabled/disabled along with telnet access independently of **Secure Config** mode.
- The ICDM-RX uses third-party MatrixSSH library from PeerSec Networks: http://www.peersec.com/.

### 4.3.4. SSL Overview

ICDM-RX SSL provides the following features:

- Provides both encryption and authentication.
  - Encryption prevents a third-party eavesdropper from viewing data that is being transferred.
  - Authentication allows both the client (that is, web browser) and server (that is. ICDM-RX) to ensure that only desired parties are allowed to establish connections. This prevents both unauthorized access and man-in-the-middle attacks on the communications channel.
- Several slightly different SSL protocols are supported by the ICDM-RX, SSLv3, TLSv1.0, TLS1.1, and TLS1.2.
- The ICDM-RX uses third-party MatrixSSL library from PeerSec Networks: http://www.peersec.com/matrixssl.html.

### 4.3.5. SSL Authentication

ICDM-RX SSL authentication has the following features:

- Authentication means being able to verify the identity of the party at the other end of a communications channel. A username/password is a common example of authentication.
- SSL/TLS protocols allow authentication using either RSA certificates or DSS certificates. ICDM-RX supports only RSA certificates.
- Each party (client and server) can present an ID certificate to the other.
- Each ID certificate is signed by another *authority* certificate or key.
- Each party can then verify the validity of the other's ID certificate by verifying that it was signed by a trusted authority. This verification requires that each party have access to the certificate/key that was used to sign the other party's ID certificate.

#### 4.3.5.1. Server Authentication

*Server Authentication* is the mechanism by which the ICDM-RX proves its identity.

- The ICDM-RX (generally an SSL server) can be configured by uploading an ID certificate that is to be presented to clients when they connect to the ICDM-RX.
- The private key used to sign the certificate must also be uploaded to the ICDM-RX.

  *Note:* *Possession of that private key will allow eavesdroppers to decrypt all traffic to and from the ICDM-RX.*

- The corresponding public key can be used to verify the ID certificate but not to decrypt traffic.
- All ICDM-RX are shipped from the factory with identical self-signed ID certificates and private keys. This means that somebody could (with a little effort) extract the factory default private key from the ICDM-RX firmware and use that private key to eavesdrop on traffic to/from any other ICDM-RX that is being used with the default private key.
- The public/private key pairs and the ID certificates can be generated using **openssl** command-line tools.

3/7/20

**PEPPERL+FUCHS**

- If the server authentication certificate in the ICDM-RX is not signed by an authority known to the client (as shipped, they are not), then interactive SSL clients such as web browsers will generally warn the user.

- If the name in server authentication certificate does not match the *hostname* that was used to access the server, then interactive SSL clients such as web browsers will generally warn the user.

### 4.3.5.2. Client Authentication

*Client Authentication* is the mechanism by which the ICDM-RX verifies the identity of clients (that is, web browsers and so forth).

- Clients can generally be configured to accept a particular unknown server certificate so that the user is not subsequently warned.

- The ICDM-RX (generally an SSL server) can be configured by uploading a trusted *authority* certificate that will be used to verify the ID certificates presented to the ICDM-RX by SSL clients. This allows you to restrict access to the ICDM-RX to a limited set of clients which have been configured with corresponding ID certificates.

- ICDM-RX units will be shipped without an authority certificate and will not require clients to present ID certificates. This allows any and all SSL clients to connect to the ICDM-RX.

### 4.3.5.3. Certificates and Keys

To control access to the ICDM-RX's SSL/TLS protected resources you should create your own custom CA certificate and then configure authorized client applications with identity certificates signed by the custom CA certificate.

This uploaded CA certificate that is used to validate a client's identity is sometimes referred to as a *trusted root certificate*, a *trusted authority certificate*, or a *trusted CA certificate*. This CA certificate might be that of a trusted commercial certificate authority or it may be a privately generated certificate that an organization creates internally to provide a mechanism to control access to resources that are protected by the SSL/TLS protocols.

The following is a list that contains additional information about certificates and keys:

- By default, the ICDM-RX is shipped without a CA (Certificate Authority) and therefore allowing connections from any SSL/TLS client. If desired, controlled access to SSL/TLS protected features can be configured by uploading a client authentication certificate to the ICDM-RX.

- Certificates can be obtained from commercial certificate authorities (VeriSign, Thawte, Entrust, and so forth.).

- Certificates can be created by users for their own use by using **openssl** command line tools or other applications.

- Certificates and keys to be uploaded to the ICDM-RX must be in the **.DER** binary file format, not in the **.PEM** ASCII file format. (The **openssl** tools can create files in either format and can convert files back and forth between the two formats.)

- Configuring Certificates and keys are configured by four uploaded files on the bottom *Key and Certificate Management* portion of the *Edit Security Configuration* web page:

  - **RSA Key Pair used by SSL and SSH servers**

    This is a private/public key pair that is used for two purposes:

    - It is used by some cipher suites to encrypt the SSL/TLS handshaking messages. Possession of the private portion of this key pair allows an eavesdropper to both decrypt traffic on SSL/TLS connections that use RSA encryption during handshaking.

    - It is used to sign the Server RSA Certificate in order to verify that the ICDM-RX is authorized to use the server RSA identity certificate. Possession of the private portion of this key pair allows somebody to pose as the ICDM-RX.

    If the Server RSA Key is replaced, a corresponding RSA server certificate must also be generated and uploaded as a matched set or clients are not able to verify the identity certificate.

**PEPPERL+FUCHS**

- **RSA Server Certificate used by SSL servers**
  - This is the RSA identity certificate that the ICDM-RX uses during SSL/TLS handshaking to identify itself. It is used most frequently by SSL server code in the ICDM-RX when clients open connections to the ICDM-RX's secure web server or other secure TCP ports. If an ICDM-RX serial port configuration is set up to open (as a client), a TCP connection to another server device, the ICDM-RX also uses this certificate to identify itself as an SSL client if requested by the server.
  - In order to function properly, this certificate must be signed using the Server RSA Key. This means that the server RSA certificate and server RSA key must be replaced as a pair.

- **DH Key pair used by SSL servers**

  This is a private/public key pair that is used by some cipher suites to encrypt the SSL/TLS handshaking messages.

  Possession of the private portion of the key pair allows an eavesdropper to decrypt traffic on SSL/TLS connections that use DH encryption during handshaking.

- **Client Authentication Certificate used by SSL servers**

  If configured with a CA certificate, the ICDM-RX requires all SSL/TLS clients to present an RSA identity certificate that has been signed by the configured CA certificate. As shipped, the ICDM-RX is not configured with a CA certificate and all SSL/TLS clients are allowed.

## 4.3.6. SSL Performance

The ICDM-RX has these SSL performance characteristics:

- Encryption/decryption is a CPU-intensive process, and using encrypted data streams will limit the number of ports that can be maintained at a given serial throughput. For example, the table below shows the number of ports that can be maintained by SocketServer at 100% throughput for various cipher suites and baud rates.

|  | 9600 | 38400 | 57600 | 115200 |
|---|---|---|---|---|
| RC4-MD5 | 32 | 16 | 10 | 5 |
| RC4-SHA | 32 | 13 | 9 | 4 |
| AES128-SHA | 28 | 7 | 5 | 2 |
| AES256-SHA | 26 | 7 | 4 | 2 |
| DES3-SHA | 15 | 3 | 2 | 1 |

*Note:* *These throughputs required 100% CPU usage, so other features such as the web server are very unresponsive at the throughputs shown above. To maintain a usable web interface, one would want to stay well below the maximum throughput/port numbers above.*

- The overhead required to set up an SSL connection is significant. The time required to open a connection to SocketServer varies depending on the public-key encryption scheme used for the initial handshaking. These are typical setup times for the three public-key encryption schemes for the ICDM-RX:
  - RSA 0.66 seconds
  - DHE 3.84 seconds
  - DHA 3.28 seconds

- Since there is a certain amount of overhead for each block of data sent/received on an SSL connection, the SocketServer polling rate and size of bocks that are written to the SocketServer also has a noticeable effect on CPU usage. Writing larger blocks of data and a slower SocketServer polling rate will decrease CPU usage and allow somewhat higher throughputs.

**PEPPERL+FUCHS**

## 4.3.7. SSL Cipher Suites

This subsection provides information about SSL cipher suites.

- An SSL connection uses four different facilities, each of which can use one of several different ciphers or algorithms. A particular combination of four ciphers/algorithms is called a "cipher suite".

- A Cipher Suite consists of
  - Public Key Encryption Algorithm
    - Used to protect the initial handshaking and connection setup.
    - Typical options are RSA, DH, DHA, DHE, EDH, SRP, PSK. The ICDM-RX supports RSA, DHA, DHE.
  - Authentication Algorithm
    - Used to verify the identities of the two parties to each other.
    - Typical options are RSA, DSA, ECDSA. The ICDM-RX supports only RSA.
  - Stream Cipher
    - Used to encrypt the user-data exchanged between the two parties.
    - Typical options: RC4, DES, 3DES, AES, IDEA, Camellia, NULL. The ICDM-RX supports RC4, 3DES, AES.
  - Message Authentication Code
    - Hash function (checksum) used to verify that each message frame has not be corrupted or changed while in transit.
    - Typical options include MD5, SHA, MD2, MD4. The ICDM-RX supports MD5, SHA

- In the design of the SSL/TLS protocols the choices of four of the above are not independent of each other: only certain combinations are defined by the standards. The standard combinations of protocol (SSL or TLS) and cipher suites support by ICDM-RX are shown in the following table.

## 4.3.8. ICDM-RX Supported Cipher Suites

The ICDM-RX supports the cipher suites:

| Protocol | Public Key | Authentication | Cipher | MAC |
|---|---|---|---|---|
| SSL | RSA | RSA | 3DES | SHA |
| SSL | RSA | RSA | RC4 | SHA |
| SSL | RSA | RSA | RC4 | MD5 |
| SSL | DHE | RSA | 3DES | SHA |
| SSL | DHA | RSA | RC4 | MD5 |
| SSL | RSA | RSA | NULL | MD5 |
| SSL | RSA | RSA | NULL | SHA |
| TLS | RSA | RSA | AES128 | SHA |
| TLS | RSA | RSA | AES256 | SHA |
| TLS | DHE | RSA | AES128 | SHA |
| TLS | DHE | RSA | AES256 | SHA |
| TLS | DHA | RSA | AES128 | SHA |
| TLS | DHA | RSA | AES256 | SHA |

3/7/20

**PEPPERL+FUCHS**

#### 4.3.8.1. SSL Resources

You can refer to the following SSL resources for more information:

- Standard reference book is SSL and TLS by Eric Rescorla

- Wikipedia page on SSL/TLS provides a good overview:  http://en.wikipedia.org/wiki/TLS

- **openssl** contains command-line tools to do the following. More information is available at: http://www.openssl.org/

    - Create/examine keys/certificates

    - Act as client or server

- **ssldump** is a -command line tool that displays a human-readable dump of an SSL connection's handshaking and traffic:. More information can be found at: http://www.rtfm.com/ssldump/.

    - If provided with server's private key, can decrypt data stream

    - Can display decoded data stream in ASCII/hex

    - Can display contents of handshaking packets (including ID certificates)

**PEPPERL+FUCHS**

## 4.4. Configure/Enable Security Features Overview

You can enable ICDM-RX security features the web page. *Key and Certificate Management* must be done using the *Security* tab in the ICDM-RX web pages.

If you want secure COM ports, you must also **Enable SSL Mode** and enter any applicable server or client certificates in the NS-Link device driver for Windows. See *Device Driver (NS-Link) Installation* on Page 36.

The following illustration shows the **Security Settings** page under the **Network** menu and is discussed in the following table.
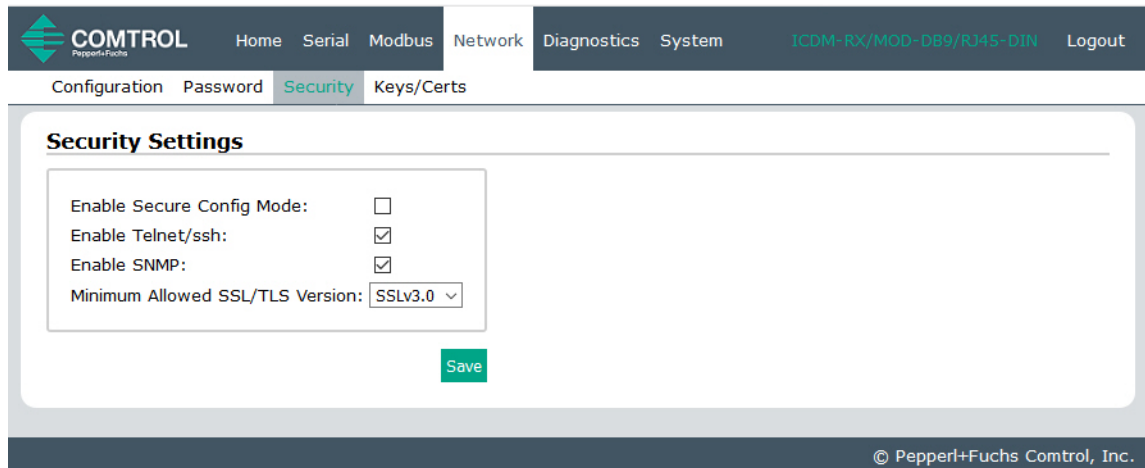


*Note:* The Security Settings page is the same across all protocols, this example is a Modbus product.

| Security Option Descriptions | |
|---|---|
| **Enable Secure Config Mode** | If **Secure Config Mode** is enabled, unencrypted access to administrative and diagnostic functions is disabled. **Secure Config Mode** changes ICDM-RX behavior as follows: <br><br> • Telnet access to administrative and diagnostic functions is disabled. SSH access is still allowed. <br><br> • Unencrypted access to the web server via Port 80 (http://URLs) is disabled. <br><br> • Encrypted access to the web server via Port 443 (https://URLs) is still allowed. <br><br> • Administrative commands that change configuration or operating state which are received using the Pepperl+Fuchs proprietary TCP driver protocol on TCP Port 4606 are ignored. <br><br> • Administrative commands that change configuration or operating state that are received using the Pepperl+Fuchs MAC mode proprietary Ethernet protocol number 0x11FE are ignored. |
| **Enable Telnet/ssh** | This option enables or disables the telnet security feature after you click **Save** and the ICDM-RX has been rebooted. *This option is enabled by default.* |
| **Enable SNMP** | This option enables or disables the SNMP security feature after you click **Save** and the ICDM-RX has been rebooted. *This option is enabled by default*. |

**PEPPERL+FUCHS**

| Security Option Descriptions (Continued) | |
|---|---|
| **Minimum Allowed SSL/TLS Version** | You can select the appropriate version for your environment.<br>• SSLv3.0<br>• TLSv1.0 (default)<br>• TLSv1.1<br>• TLSv1.2 |

## 4.4.1. Key and Certificate Management

Key and Certificate management is only available in the **Network | Keys/Cert** web page.



| Key and Certificate Management Option Descriptions | |
|---|---|
| RSA Key pair used by SSL and SSH servers | This is a private/public key pair that is used for two purposes:<br><br>It is used by some cipher suites to encrypt the SSL/TLS handshaking messages. Possession of the private portion of this key pair allows an eavesdropper to both decrypt traffic on SSL/TLS connections that use RSA encryption during handshaking.<br><br>It is used to sign the Server RSA Certificate in order to verify that the ICDM-RX is authorized to use the server RSA identity certificate. Possession of the private portion of this key pair allows somebody to pose as the ICDM-RX.<br><br>If the Server RSA Key is to be replaced, a corresponding RSA identity certificate must also be generated and uploaded or clients are not able to verify the identity certificate. |

| Key and Certificate Management Option Descriptions (Continued) | |
|---|---|
| RSA Server Certificate used by SSL servers | This is the RSA identity certificate that the ICDM-RX uses during SSL/TLS handshaking to identify itself. It is used most frequently by SSL server code in the ICDM-RX when clients open connections to the ICDM-RX's secure web server or other secure TCP ports. If an ICDM-RX serial port configuration is set up to open (as a client) a TCP connection to another server device, the ICDM-RX also uses this certificate to identify itself as an SSL client if requested by the server.<br><br>In order to function properly, this certificate must be signed using the Server RSA Key. This means that the server RSA certificate and server RSA key must be replaced as a pair. |
| DH Key pair used by SSL servers | This is a private/public key pair that is used by some cipher suites to encrypt the SSL/TLS handshaking messages.<br><br>*Note:* *Possession of the private portion of the key pair allows an eavesdropper to decrypt traffic on SSL/TLS connections that use DH encryption during handshaking.* |
| Client Authentication Certificate used by SSL servers | If configured with a CA certificate, the ICDM-RX requires all SSL/TLS clients to present an RSA identity certificate that has been signed by the configured CA certificate. As shipped, the ICDM-RX is not configured with a CA certificate and all SSL/TLS clients are allowed.<br><br>See *Client Authentication* on Page 38 for more detailed information |
| • *All ICDM-RX units are shipped from the factory with identical configurations. They all have the identical, self-signed, Pepperl+Fuchs Server RSA Certificates, Server RSA Keys, Server DH Keys, and no Client Authentication Certificates*.<br><br>• *For maximum data and access security, you should configure all ICDM-RX units with custom certificates and keys*. | |

3/7/20

**PEPPERL+FUCHS**

## 4.5. Using a Web Browser to Set Security Features

The follow procedures are discussed below:

- *Changing Security Configuration*
- *Changing Keys and Certificates* on Page 46

### 4.5.1. Changing Security Configuration

Use the following steps to change security settings in the ICDM-RX.

1. Enter the IP address of the ICDM-RX in the *Address* field of your web browser and press the **Enter** key.
2. Click **Network** | **Security**.
3. Click the appropriate check boxes to enable or disable security for your environment.



Refer to the help system or *Configure/Enable Security Features Overview* on Page 42 for detailed information.

4. After making changes, click **Save.**

**PEPPERL+FUCHS**

## 4.5.2. Changing Keys and Certificates

Use the following steps to update security keys and certificates in the ICDM-RX. Refer to the help system or *Key and Certificate Management* subsection on Page 46 for detailed information.

1. If necessary, enter the IP address of the ICDM-RX in the *Address* field of your web browser and press the **Enter** key.

2. Click **Network | Keys/Certs**.

3. Click **Browse** to locate the key or certificate file, highlight the file, and click **Open**.

4. Click **Upload**.

5. Click **Save**, but changes will not take effect until the ICDM-RX is rebooted.

   *Note:* *The key or certificate notation changes from factory or none to* ***User*** *when the ICDM-RX is secure.*

   You can reboot the ICDM-RX by clicking **System | Reboot** or use the PortVision DX reboot option.

PEPPERL+FUCHS

## 4.6. Password Authentication

This section discusses three methods of configuring password authentication.

• Using the web page

• Using telnet or SSH

### 4.6.1. Using the Web Page

You can easily set up a password to secure the ICDM-RX. Use the following procedure to configure a password using the web page.

*Note:* *There is no password set from the factory.*

Use the following information to configure a password for this ICDM-RX.

1. Log into the ICDM-RX using your web browser and the IP address of the ICDM-RX.

2. Click **Network | Password**.

3. If changing an existing password, enter that password in the **Old Password** field.

4. Enter a new password and enter the confirmation password.

5. Click the **Save** button.

When anyone attempts to log into the ICDM-RX, you must enter the following:

• admin for the username

• The configured password for the password

### 4.6.2. Using Telnet or SSH

If you have not done so, install PortVision DX, which is a Windows application. If necessary, you can download from https://www.pepperl-fuchs.com the latest version of PortVision DX and install that version.

This subsection discusses the following topics:

• *Login Authentication* on Page 47

• *Configuring Passwords* on Page 50

• *Telnet Commands* on Page 51

#### 4.6.2.1. Login Authentication

Use the following steps to access a telnet session in PortVision DX so that you can set the log-in authentication.
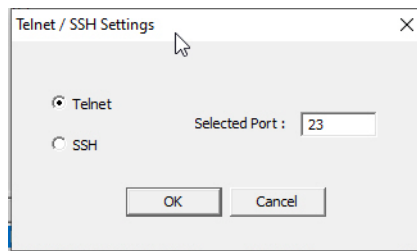
1. Start PortVision DX.

2. If this is the first time you have started PortVision DX:

   a. Click the **Scan** button on the Toolbar to locate the ICDM-RX for which you want to configure password authentication.

   b. Click the ICDM-RX option or other appropriate models.

   c. Click the **Scan** button.
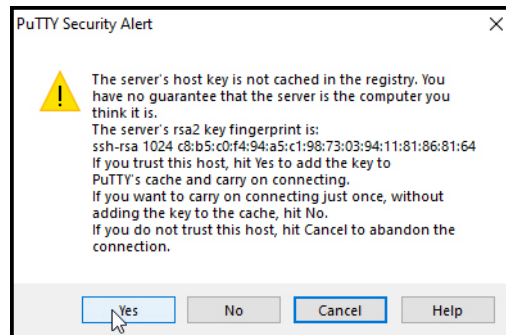
3/7/20

**PEPPERL+FUCHS**
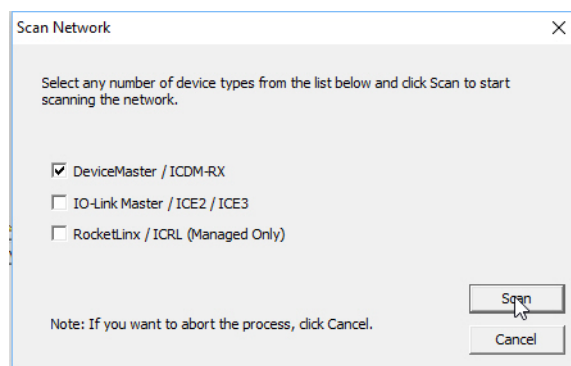
3. Highlight the ICDM-RX in the Device List pane (lower) that you want to configure for password authentication and click **Telnet / SSH Session**.
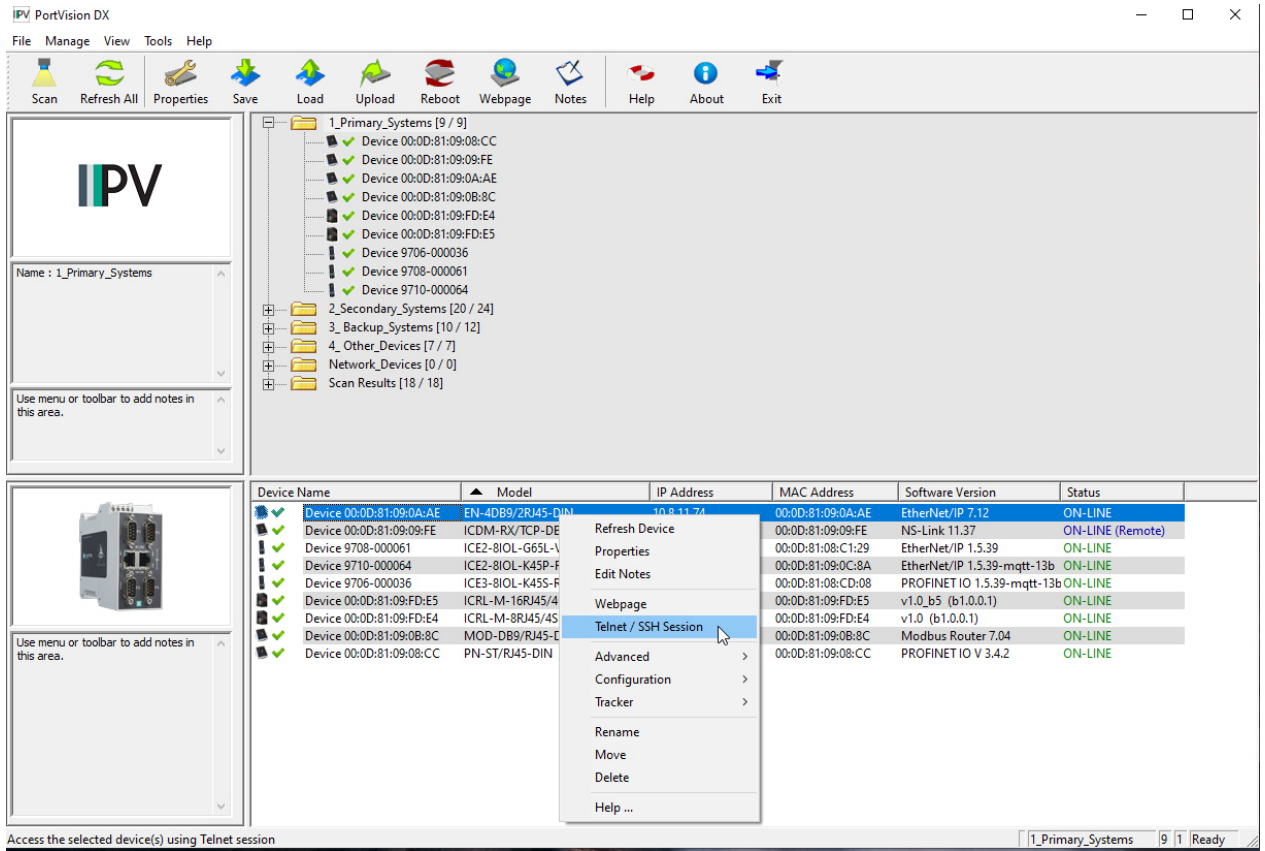


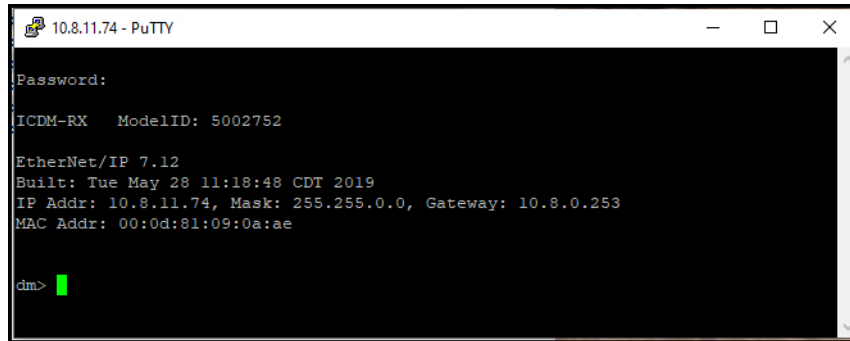4. Click the **Telnet** or **SSH** option, leave the **Selected Port** number as 23 or 22, and click **Ok**.



5. If you select **SSH**, click **Yes** to the *PuTTY Security Alert.*

**PEPPERL+FUCHS**

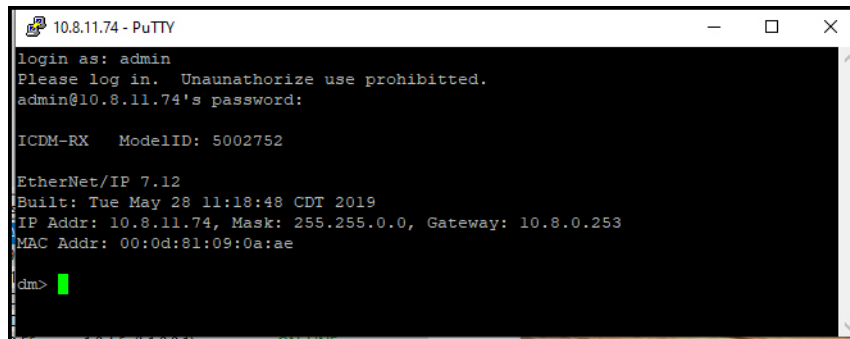6. If this is a Telnet session and the ICDM-RX has a password configured, type the password and press Enter.



**Note:** *If a password has not been configured, press Enter.*

If this is an SSH session, type admin for the login and the ICDM-RX has a password configured, type the password and press Enter
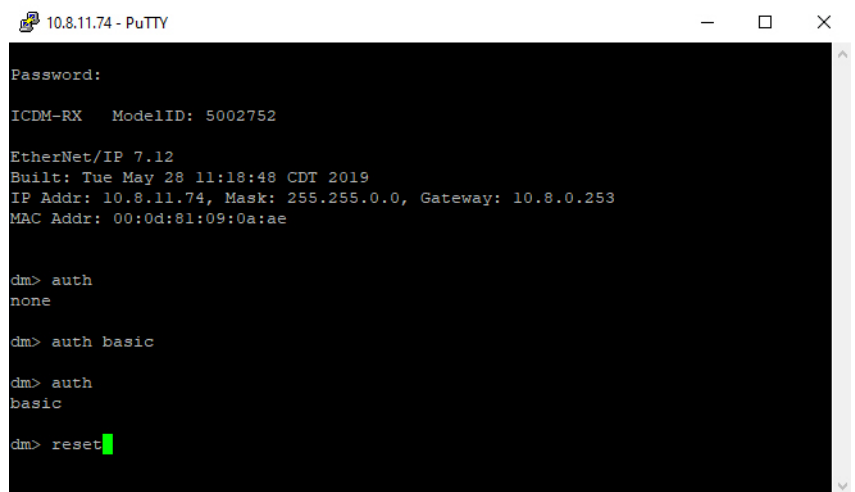


7. Type **auth** and press Enter to see the authentication status, none indicates that there is no authentication set.

8. Type **auth** basic and press Enter to enable enforcing log-in functionality.

9. Type **reset** and press Enter.

10. Close the PuTTY window.

    PortVision DX temporarily displays that ICDM-RX as OFF-LINE until the next polling cycle because the ICDM-RX is rebooting.

To disable enforcing log-in functionality, type **auth none**.



3/7/20

**PEPPERL+FUCHS**

### 4.6.2.2. Configuring Passwords

Use the following procedure to configure a ICDM-RX password.

1. Highlight the ICDM-RX in the Device List pane (lower) that you want to configure for a password and click **Telnet / SSH Session**.

2. Click the Telnet or SSH option, leave the Selected Port number as 23, and click Ok.

3. If you select **SSH**, click **Yes** to the *PuTTY Security Alert.*
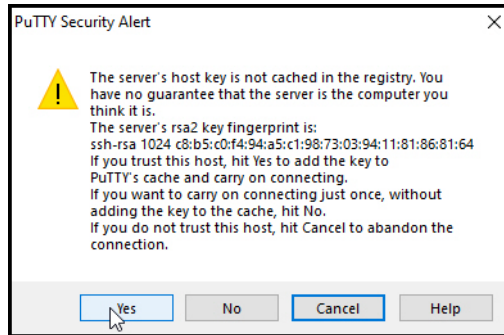


4. If this is a Telnet session and the ICDM-RX has a password configured, type the password and press Enter.



*Note:* *If a password has not been configured, press Enter.*

If this is an SSH session, type admin for the login and the ICDM-RX has a password configured, type the password and press Enter

**PEPPERL+FUCHS**
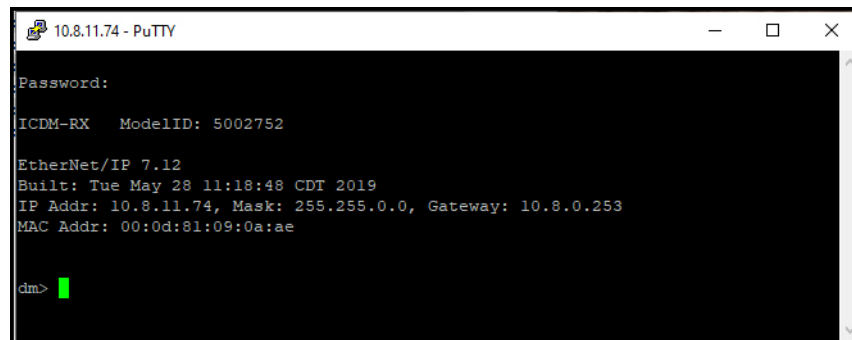
5. Type password and the password that you want to set. The example below shows setting the password to do-not-use-admin.

```
10.8.11.74 - PuTTY                                    —   □   ×
login as: admin
Please log in.  Unaunathorize use prohibitted.
admin@10.8.11.74's password:

ICDM-RX    ModelID: 5002752

EtherNet/IP 7.12
Built: Tue May 28 11:18:48 CDT 2019
IP Addr: 10.8.11.74, Mask: 255.255.0.0, Gateway: 10.8.0.253
MAC Addr: 00:0d:81:09:0a:ae

dm> password do-not-use-admin
Password set
dm> quit
```
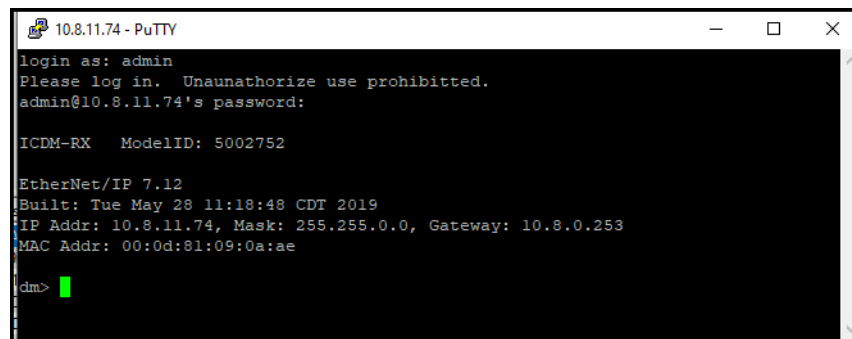
**Note:** *Make sure that you do not forget the password because after you configure the ICDM-RX with Secure Config Mode, you will not be able to recover the password and will need to return it to the factory to have the default setting loaded.*

6. Type **quit** and press Enter.

#### 4.6.2.3. Telnet Commands

To access telnet help, type help.

```
10.8.11.74 - PuTTY                                    —   □   ×
dm> help
auth          - Set the authentication method used by web server
boot          - Show bootloader version
help          - help [cmd] - Display help information
ip            - Set IP configuration
logdump       - Dump diagnostic log
mac           - Show MAC address
model         - View the Model ID
password      - Set the password
reset         - Resets the device
secureconf    - Enable/disable encryption for config
sernum        - View the Serial Number
snmp          - Enable/disable SNMP
telnet        - Enable/disable telnet
teltimeout    - Set the telnet timeout period (seconds)
timeout       - Set time (seconds) until default application loads automatically
ver           - Display firmware revision
quit          - Exit session

dm>
```

**PEPPERL+FUCHS**
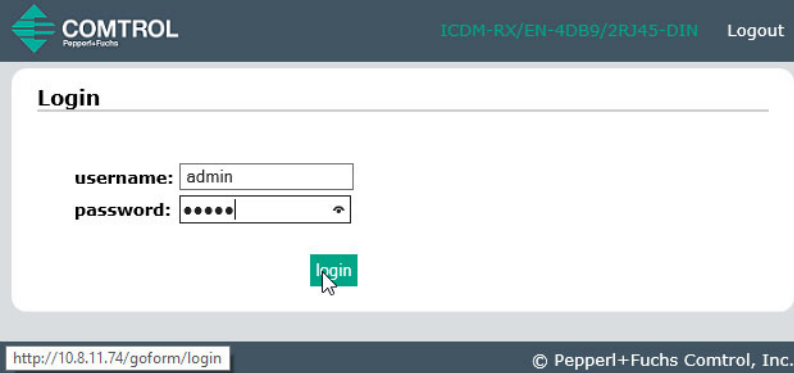
### 4.6.3. Web Page Password Access

When the authentication is set to require a password, such as basic, you will need to log into each web server session whether you use PortVision DX or a web browser.

Use these steps to log in:

1.  Leave the User name blank.
2.  Type in your password. If there is no password configured, leave the Password blank.
3.  Click OK.



Once logged in, you will have full read/write access to the web pages.

**PEPPERL+FUCHS**

# 5. Connecting Serial Devices

This section discusses connecting your serial devices to the ICDM-RX. It also provides you with information to build serial or test cables and loopback connectors to test the serial ports.

- *DB9 Connectors* on Page 54
- *RJ45 Connectors* on Page 57
- *Four Screw Terminals (ICDM-RX/xxx-2ST/RJ45-DIN)* on Page 60
- *Nine Screw Terminals (ICDM-RX/xxx-ST/RJ45-DIN)* on Page 63

⚠️ **Caution** ***Make sure that you have configured the ports for the correct communications mode before connecting any devices. The default mode is RS-232. There is a remote possibility that connecting a serial device for the wrong mode could damage the serial device.***



3/7/20

**PEPPERL+FUCHS**
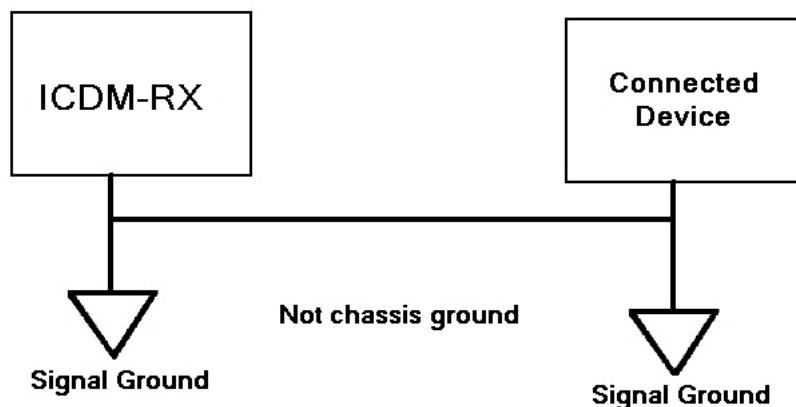
## 5.1. DB9 Connectors

This subsection provides the following information:

- Connector pin assignments (below)
- *DB9 Null-Modem Cables (RS-232)* on Page 55
- *DB9 Null-Modem Cables (RS-422)* on Page 55
- *DB9 Straight-Through Cables (RS-232/485)* on Page 55
- *DB9 Loopback Plugs* on Page 56
- *Connecting DB9 Serial Devices* on Page 56

| | | *DB9 Connector Pin Outs* | |
|---|---|---|---|
| **Pin** | **RS-232** | **RS-422 and *RS-485 Full-Duplex (Master/Slave)†*** | **RS-485 Half-Duplex** |
| 1 | DCD | Not used | Not used |
| 2 | RxD | RxD- | Not used |
| 3 | TxD | TxD- | TRxD- |
| 4 | DTR | Not used | Not used |
| 5 | Signal GND | Signal GND | Signal GND |
| 6 | DSR | Not used | Not used |
| 7 | RTS | TxD+ | TRxD+ |
| 8 | CTS | RxD+ | Not used |
| 9 | RI | Not used | Not Used |
| † | DIN rail models support RS-485 full-duplex. | | |

Refer to the hardware manufacturer's installation documentation if you need help with connector pin outs or cabling for the serial device. This illustrates the DB9 connector signals.
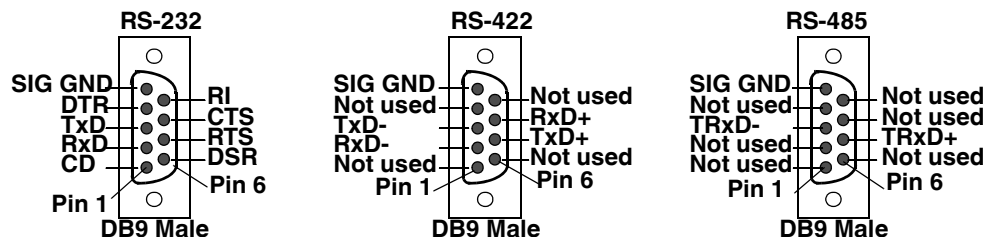
**PEPPERL+FUCHS**

### 5.1.1. DB9 Null-Modem Cables (RS-232)

Use the following figure if you need to build an RS-232 null-modem cable. A null-modem cable is required for connecting DTE devices.

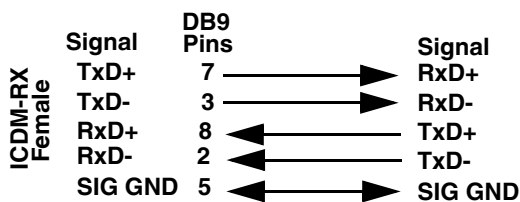| ICDM-RX Female Signal | DB9 Pins | | DB9 Pins | DB25 Pins | RJ45 Pins | Signal |
|---|---|---|---|---|---|---|
| TxD | 3 | → | 2 | 3 | 5 | RxD |
| RxD | 2 | ← | 3 | 2 | 4 | TxD |
| RTS | 7 | → | 8 | 5 | 8 | CTS |
| CTS | 8 | ← | 7 | 4 | 1 | RTS |
| DSR | 6 | ← | 4 | 20 | 2 | DTR |
| DCD | 1 | ← | 1 | 8 | 6 | DCD |
| DTR | 4 | → | 6 | 6 | 7 | DSR |
| SIG GND | 5 | ← → | 5 | 7 | 3 | SIG GND |
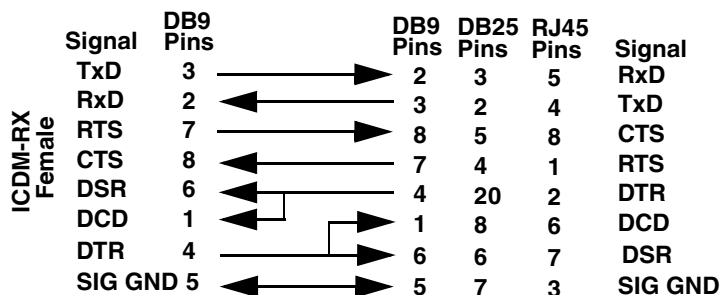
*Note:* *You may want to purchase or build a straight-through cable and purchase a null-modem adapter.*
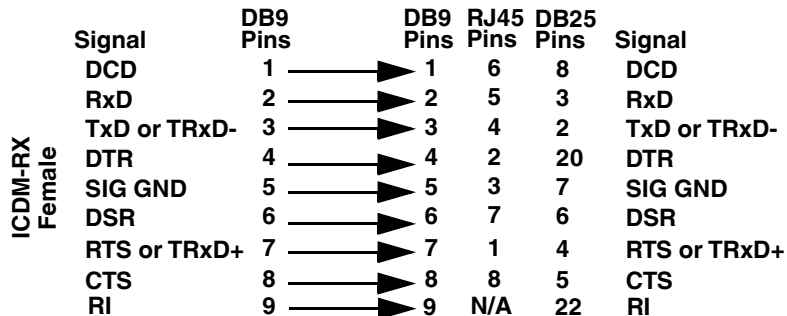
### 5.1.2. DB9 Null-Modem Cables (RS-422)

Use the following figure if you need to build an RS-422 null-modem cable.

| ICDM-RX Female Signal | DB9 Pins | | Signal |
|---|---|---|---|
| TxD+ | 7 | → | RxD+ |
| TxD- | 3 | → | RxD- |
| RxD+ | 8 | ← | TxD+ |
| RxD- | 2 | ← | TxD- |
| SIG GND | 5 | ← → | SIG GND |

*Note:* *RS-422 pin outs are not standardized. Each peripheral manufacturer uses different pin outs. Refer to the peripheral documentation to determine the pin outs for the signals above.*

### 5.1.3. DB9 Straight-Through Cables (RS-232/485)

Use the following figure if you need to build an RS-232 or RS-485 straight-through cable. Straight-through cables are used to connect modems and other DCE devices.

| ICDM-RX Female Signal | DB9 Pins | | DB9 Pins | RJ45 Pins | DB25 Pins | Signal |
|---|---|---|---|---|---|---|
| DCD | 1 | → | 1 | 6 | 8 | DCD |
| RxD | 2 | → | 2 | 5 | 3 | RxD |
| TxD or TRxD- | 3 | → | 3 | 4 | 2 | TxD or TRxD- |
| DTR | 4 | → | 4 | 2 | 20 | DTR |
| SIG GND | 5 | → | 5 | 3 | 7 | SIG GND |
| DSR | 6 | → | 6 | 7 | 6 | DSR |
| RTS or TRxD+ | 7 | → | 7 | 1 | 4 | RTS or TRxD+ |
| CTS | 8 | → | 8 | 8 | 5 | CTS |
| RI | 9 | → | 9 | N/A | 22 | RI |

**PEPPERL+FUCHS**

### 5.1.4. DB9 Loopback Plugs

*Loopback connectors* are DB9 female serial port plugs with pins wired together that are used in conjunction with application software to test serial ports. The ICDM-RX is shipped with a a single loopback plug (RS-232/422).
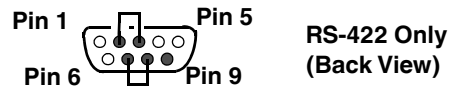
Wire the following pins together to build additional plugs or replace a missing RS-232 loopback plug:

- Pins 1 to 4 to 6
- Pins 2 to 3
- Pins 7 to 8 to 9

**Pin 1** ... **Pin 5**  **RS-232 Only**  **The RS-232 loopback plug**
**Pin 6** ... **Pin 9**  **(Back View)**  **also works for RS-422.**

Wire the following pins together for an RS-422 loopback plug:

- Pins 2 to 3
- Pins 7 to 8

**Pin 1** ... **Pin 5**  **RS-422 Only**
**Pin 6** ... **Pin 9**  **(Back View)**

### 5.1.5. Connecting DB9 Serial Devices

You can use this information to connect serial devices to DB9 connectors.

1. Connect your serial devices to the appropriate serial port on the ICDM-RX using the appropriate cable.

   *Note:* *Refer to the hardware manufacturer's installation documentation if you need help with connector pin outs or cabling for the peripheral device.*

2. Verify that the devices are communicating properly.

   *Note:* *ICDM-RX DIN models do not have TX/RX LEDs.*

   The RX (yellow) and TX (green) LEDs function accordingly when the cable is attached properly to a serial device.

   **DB9 LEDs** [RX1* / TX1*]
   \* Represents port number.

   - After power cycling the ICDM-RX (appropriate models), the RX/TX LEDs are off.
   - The LEDs do not function as described until the port has been opened by an application.

   | Mode | LEDs |
   |---|---|
   | RS-232 | RX LEDs (yellow) are lit while receiving data |
   | RS-422 | TX LEDs (green) are lit during active data transmission |
   | RS-485 | |

3. You can refer to *ICDM-RX LEDs* on Page 103 for information about the remaining LEDs.

3/7/20

## 5.2. RJ45 Connectors

This subsection provides the following information:

- Connector pin assignments (below)
- *RJ45 Null-Modem Cables (RS-232)*
- *RJ45 Null-Modem Cables (RS-422)* on Page 58
- *RJ45 Straight-Through Cables (RS-232/485)* on Page 58
- *RJ45 Loopback Plugs* on Page 58
- *RJ45 RS-485 Test Cable* on Page 58
- *Connecting RJ45 Devices* on Page 59

You can build your own null-modem or straight-through RJ45 serial cables if you are using the DB9 to RJ45 adapters using the following subsections.
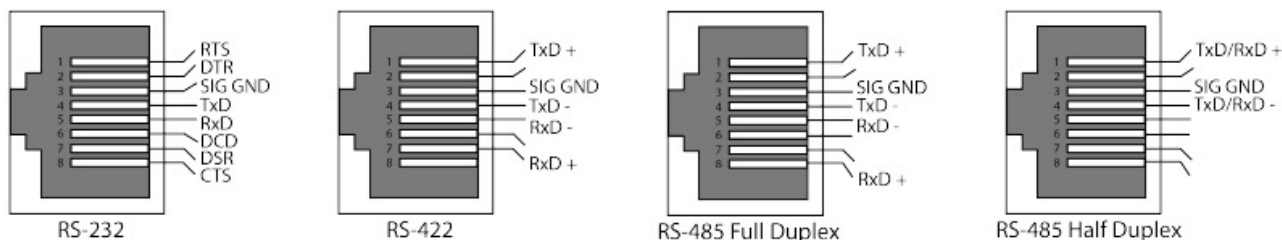


| Pin | RS-232 | RS-422 | RS-485 |
|-----|--------|--------|--------|
| 1 | RTS | TxD+ | TRxD+ |
| 2 | DTR | Not used | Not used |
| 3 | Signal GND | Signal GND | Signal GND |
| 4 | TxD | TxD- | TRxD- |
| 5 | RxD | RxD- | Not used |
| 6 | DCD | Not used | Not used |
| 7 | DSR | Not used | Not used |
| 8 | CTS | RxD+ | Not used |

### 5.2.1. RJ45 Null-Modem Cables (RS-232)

Use the following figure if you need to build an RS-232 null-modem cable. A null-modem cable is required for connecting DTE devices.
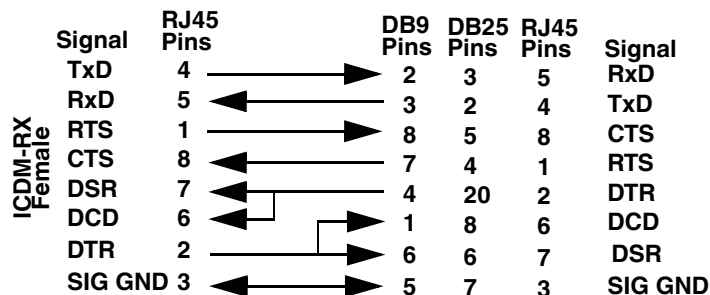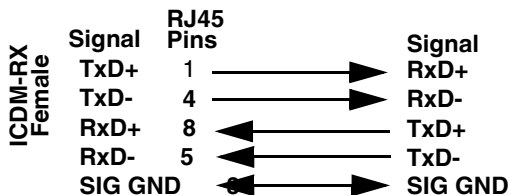


*Note:* You may want to purchase or build a straight-through cable and purchase a null-modem adapter. For example, a null-modem cable can be used to connect COM2 of one PC to COM2 of another PC.

3/7/20

**PEPPERL+FUCHS**

### 5.2.2. RJ45 Null-Modem Cables (RS-422)
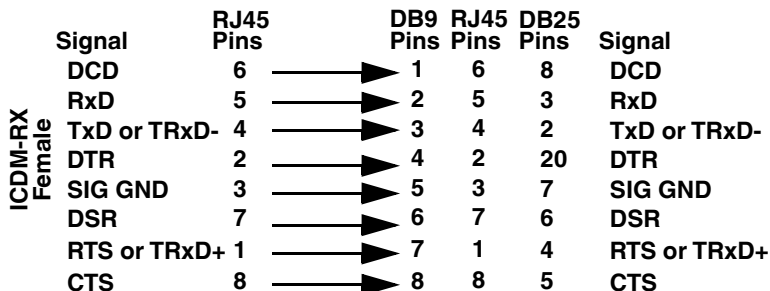
Use the following figure if you need to build an RS-422 null-modem RJ45 cable. A null-modem cable is required for connecting DTE devices.

| ICDM-RX Female Signal | RJ45 Pins | | Signal |
|---|---|---|---|
| TxD+ | 1 | → | RxD+ |
| TxD- | 4 | → | RxD- |
| RxD+ | 8 | ← | TxD+ |
| RxD- | 5 | ← | TxD- |
| SIG GND | 6 | ←→ | SIG GND |

**Note:** *RS-422 pin outs are not standardized. Each peripheral manufacturer uses different pin outs. Please refer to the documentation for the peripheral to determine the pin outs for the signals above.*

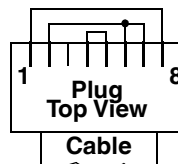### 5.2.3. RJ45 Straight-Through Cables (RS-232/485)

Use the following figure if you need to build an RS-232 or RS-485 straight-through cable. Straight-through cables are used to connect modems and other DCE devices.

| ICDM-RX Female Signal | RJ45 Pins | | DB9 Pins | RJ45 Pins | DB25 Pins | Signal |
|---|---|---|---|---|---|---|
| DCD | 6 | → | 1 | 6 | 8 | DCD |
| RxD | 5 | → | 2 | 5 | 3 | RxD |
| TxD or TRxD- | 4 | → | 3 | 4 | 2 | TxD or TRxD- |
| DTR | 2 | → | 4 | 2 | 20 | DTR |
| SIG GND | 3 | → | 5 | 3 | 7 | SIG GND |
| DSR | 7 | → | 6 | 7 | 6 | DSR |
| RTS or TRxD+ | 1 | → | 7 | 1 | 4 | RTS or TRxD+ |
| CTS | 8 | → | 8 | 8 | 5 | CTS |

### 5.2.4. RJ45 Loopback Plugs

*Loopback connectors* are RJ45 serial port plugs with pins wired together that are used in conjunction with application software to test serial ports. The ICDM-RX is shipped with a a single loopback plug (RS-232/422).
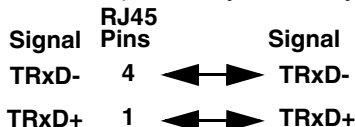
- Pins 4 to 5
- Pins 1 to 8
- Pins 2 to 6 to 7

**The RS-232 loopback plug also works for RS-422.**

Plug Top View

Cable

### 5.2.5. RJ45 RS-485 Test Cable

You can use a straight-through cable as illustrated previously, or build your own cable.

| Signal | RJ45 Pins | | Signal |
|---|---|---|---|
| TRxD- | 4 | ←→ | TRxD- |
| TRxD+ | 1 | ←→ | TRxD+ |

**Note:** *RS-422 pin outs are not standardized. Each peripheral manufacturer uses different pin outs. Please refer to the documentation for the peripheral to determine the pin outs for the signals above.*

**PEPPERL+FUCHS**

## 5.2.6. Connecting RJ45 Devices

You can use this information to connect serial devices to RJ45 connectors.

1. Connect your serial devices to the appropriate serial port on the ICDM-RX using the appropriate cable.

   **Note:**  *Refer to the hardware manufacturer's installation documentation if you need help with connector pin outs or cabling for the peripheral device.*

2. If the ICDM-RX has RX/TX LEDs, verify that the devices are communicating properly.

   The RX (yellow) and TX (green) LEDs function accordingly when the cable is attached properly to a serial device.

   • After power cycling the ICDM-RX, the RX/TX LEDs are off.

   • The LEDs do not function as described until the port has been opened by an application.
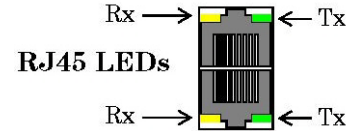
| Mode | LED Functions |
|------|---------------|
| RS-232 | RX LEDs (yellow) are lit while receiving data |
| RS-422 | TX LEDs (green) are lit during active data transmission |
| RS-485 | |

3. You can refer to *ICDM-RX LEDs* on Page 103 for information about the remaining LEDs.

## 5.3. Four Screw Terminals (ICDM-RX/*xxx*-2ST/RJ45-DIN)

This subsection discusses the following topics for the ICDM-RX/*xxx*-2ST/RJ45-DIN with 4 serial screw terminals.

- *Serial Terminal (4) Connectors* on Page 60
- *Serial Terminal (4) Null-Modem Cables (RS-232)* on Page 61
- *Serial Terminal (4) Null-Modem Cables (RS-422)* on Page 61
- *Serial Terminal (4) Straight-Through Cables (RS-232/485)* on Page 62
- *Serial Terminal (4) Loopback Signals* on Page 62
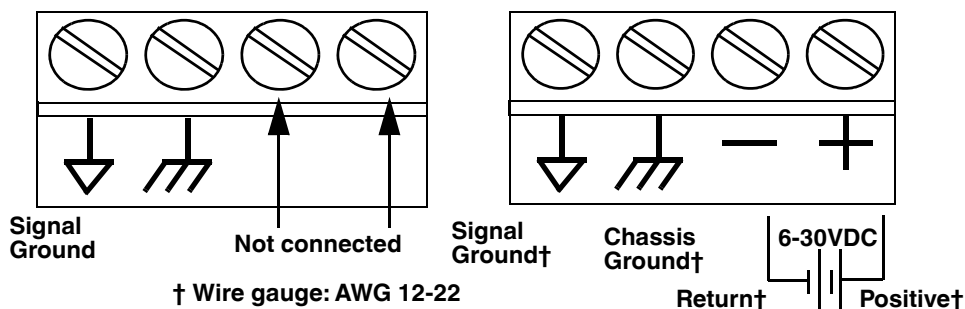- *Connecting Serial Devices* on Page 62

### 5.3.1. Serial Terminal (4) Connectors

Use the following table or drawings for signal information. The signals for **SERIAL2** are the same as **SERIAL1**.
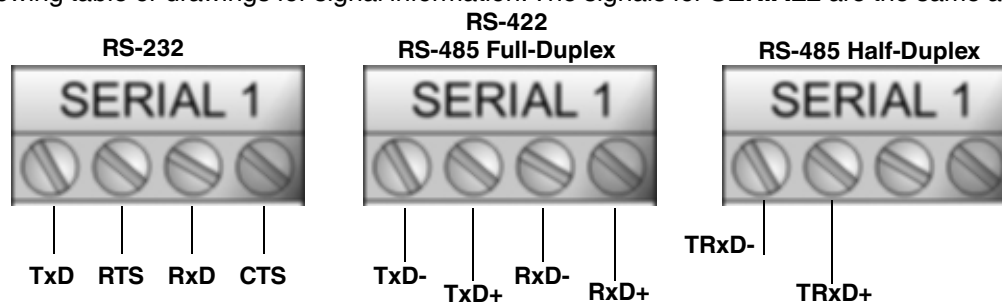


† Ground must be connected to the appropriate signal ground terminal.

**RS-232: Connecting the Ground**



† Wire gauge: AWG 12-22

| RS-232† | TxD | RTS | RxD | CTS |
|---|---|---|---|---|
| RS-422/RS-485 Full-Duplex | TxD- | TxD+ | RxD- | RxD+ |
| RS-485 Half-Duplex | TRxD- | TRxD+ | | |
| † RS-232 ground must be connected to the signal ground terminal. | | | | |

3/7/20

**PEPPERL+FUCHS**

## 5.3.2. Serial Terminal (4) Null-Modem Cables (RS-232)

An RS-232 null-modem cable is required for connecting DTE devices.

**RS-232 Null-Modem Cable**
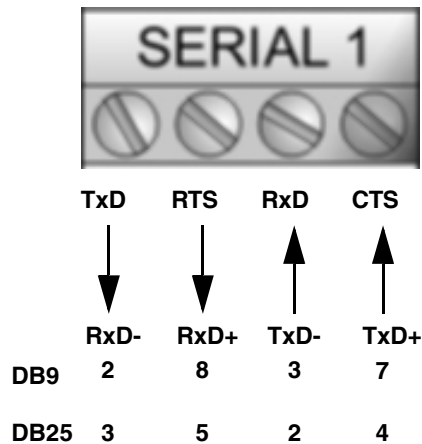


| | TxD | RTS | RxD | CTS |
|---|---|---|---|---|
| | ↓ | ↓ | ↑ | ↑ |
| | RxD | CTS | TxD | RTS |
| DB9 | 2 | 8 | 3 | 7 |
| DB25 | 3 | 5 | 2 | 4 |
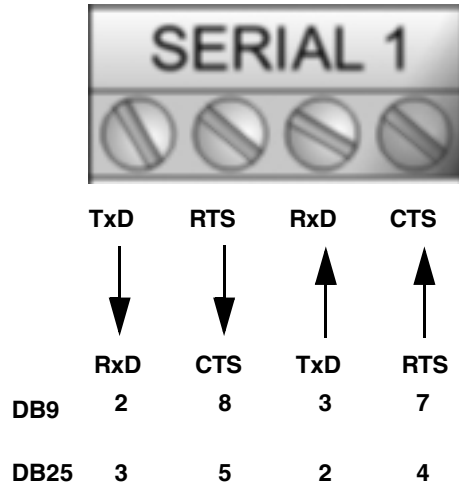
## 5.3.3. Serial Terminal (4) Null-Modem Cables (RS-422)

An RS-422 null-modem cable is required for connecting DTE devices.

**RS-422 Null-Modem Cable**



| | TxD | RTS | RxD | CTS |
|---|---|---|---|---|
| | ↓ | ↓ | ↑ | ↑ |
| | RxD- | RxD+ | TxD- | TxD+ |
| DB9 | 2 | 8 | 3 | 7 |
| DB25 | 3 | 5 | 2 | 4 |

*Note:* *RS-422 pin outs are not standardized. Each peripheral manufacturer uses different pin outs. Please refer to the documentation for the peripheral to determine the pin outs for the signals above.*

**PEPPERL+FUCHS**

### 5.3.4. Serial Terminal (4) Straight-Through Cables (RS-232/485)

RS-232 or RS-485 straight-through cables are used to connect modems and other DCE devices.

**RS-232/422 Straight-Through Cable**



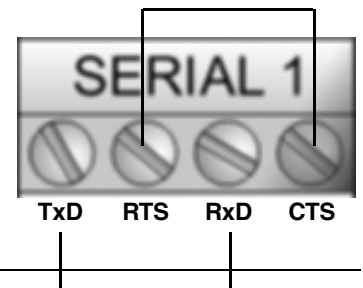|  | TxD or TRxD- | RTS or TRxD+ | RxD | CTS |
|---|---|---|---|---|
| DB9 | 3 | 7 | 2 | 8 |
| DB25 | 2 | 4 | 3 | 5 |
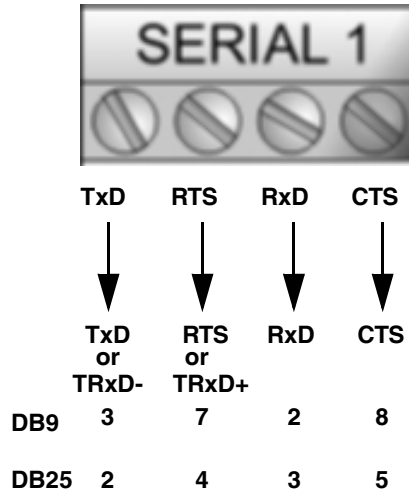
### 5.3.5. Serial Terminal (4) Loopback Signals

Use this drawing to wire a loopback, which is used in conjunction with application software to test serial ports.

Wire the terminals together to create a loopback.

- TxD to RxD
- RTS to CTS



### 5.3.6. Connecting Serial Devices

Use the following information to connect the ICDM-RX/*xxx*-2ST/RJ45-DIN with serial terminals.

1. Connect your serial devices to the appropriate serial port on the ICDM-RX/*xxx*-2ST/RJ45-DIN using the appropriate cable. You can build your own cables or loopbacks using the appropriate discussions.

*Note:* *Refer to the hardware manufacturer's installation documentation if you need help with connector pin outs or cabling for the serial device.*

2. You can refer to *ICDM-RX LEDs* on Page 103 for information about the LEDs.

3/7/20

**PEPPERL+FUCHS**

## 5.4. Nine Screw Terminals (ICDM-RX/*xxx*-ST/RJ45-DIN)

This subsection discusses the following topics for the ICDM-RX/*xxx*-ST/RJ45-DIN with 9 serial screw terminals.

• *Screw Terminal Connectors (9)* on Page 63
• *Screw Terminal (9) Null-Modem RS-232 Cables* on Page 64
• *Screw Terminal (9) Null-Modem RS-422 Cables* on Page 64
• *Screw Terminal (9) RS-232/485 Straight-Through Cables* on Page 65
• *Screw Terminal (9) Loopback Signals* on Page 65
• *Connecting Serial Devices* on Page 65

### 5.4.1. Screw Terminal Connectors (9)

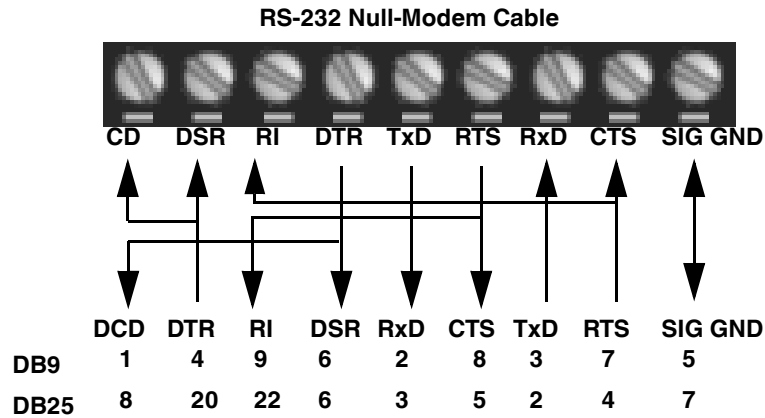Use the following table or drawings for signal information.
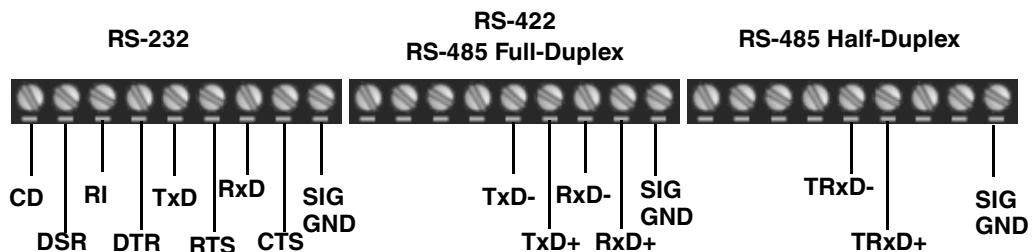


† *Ground must be connected to the signal ground terminal.*

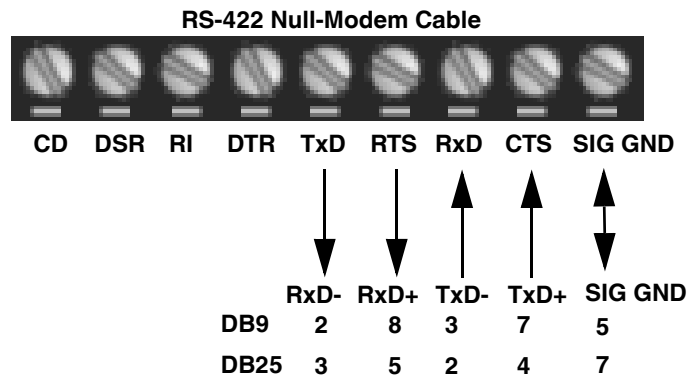|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| **RS-232** | CD | DSR | RI | DTR | TxD | RTS | RxD | CTS | Signal GND |
| **RS-422/RS-485 Full-Duplex** | N/A | N/A | N/A | N/A | TxD- | TxD+ | RxD- | RxD+ | Signal GND |
| **RS-485 Half-Duplex** | N/A | N/A | N/A | N/A | TRxD- | TRxD+ | N/A | N/A | Signal GND |
| *† Ground must be connected to the signal ground terminal.* | | | | | | | | | |

**PEPPERL+FUCHS**

## 5.4.2. Screw Terminal (9) Null-Modem RS-232 Cables

An RS-232 null-modem cable is required for connecting DTE devices.

**RS-232 Null-Modem Cable**

| | CD | DSR | RI | DTR | TxD | RTS | RxD | CTS | SIG GND |
|---|---|---|---|---|---|---|---|---|---|
| | DCD | DTR | RI | DSR | RxD | CTS | TxD | RTS | SIG GND |
| DB9 | 1 | 4 | 9 | 6 | 2 | 8 | 3 | 7 | 5 |
| DB25 | 8 | 20 | 22 | 6 | 3 | 5 | 2 | 4 | 7 |

## 5.4.3. Screw Terminal (9) Null-Modem RS-422 Cables

An RS-422 null-modem cable is required for connecting DTE devices.

**RS-422 Null-Modem Cable**

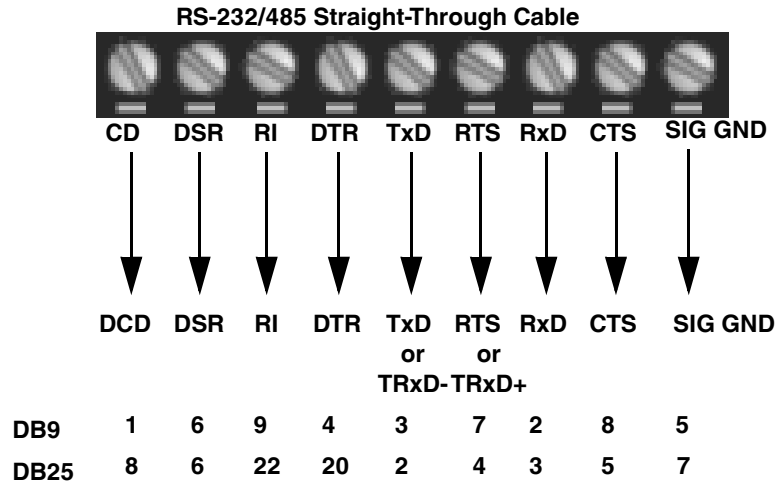| | CD | DSR | RI | DTR | TxD | RTS | RxD | CTS | SIG GND |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | RxD- | RxD+ | TxD- | TxD+ | SIG GND |
| DB9 | | | | | 2 | 8 | 3 | 7 | 5 |
| DB25 | | | | | 3 | 5 | 2 | 4 | 7 |

*Note:* RS-422 pin outs are not standardized. Each peripheral manufacturer uses different pin outs. Please refer to the documentation for the peripheral to determine the pin outs for the signals above.

3/7/20

**PEPPERL+FUCHS**

### 5.4.4. Screw Terminal (9) RS-232/485 Straight-Through Cables

RS-232 or RS-485 straight-through cables are used to connect modems and other DCE devices.

**RS-232/485 Straight-Through Cable**

| | CD | DSR | RI | DTR | TxD | RTS | RxD | CTS | SIG GND |
|---|---|---|---|---|---|---|---|---|---|
| | DCD | DSR | RI | DTR | TxD or TRxD- | RTS or TRxD+ | RxD | CTS | SIG GND |
| DB9 | 1 | 6 | 9 | 4 | 3 | 7 | 2 | 8 | 5 |
| DB25 | 8 | 6 | 22 | 20 | 2 | 4 | 3 | 5 | 7 |

### 5.4.5. Screw Terminal (9) Loopback Signals

Use this drawing to wire a loopback, which is used in conjunction with application software  to test serial ports.

CD    DSR    RI    DTR        TxD    RTS    RxD    CTS
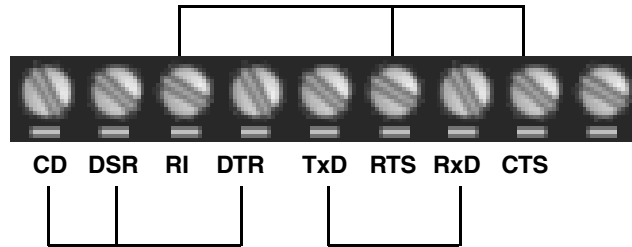
Wire the terminals together to create a loopback.

- TxD to RxD
- RTS to CTS to RI
- DTR to CD to DSR

### 5.4.6. Connecting Serial Devices

Use the following information to connect the ICDM-RX with serial terminals.

1.  Connect your serial devices to the appropriate serial port on the ICDM-RX using the appropriate cable. You can build your own cables or loopbacks using the appropriate discussions.

*Note:*  *Refer to the hardware manufacturer's installation documentation if you need help with connector pin outs or cabling for the serial device.*

2.  You can refer to *ICDM-RX LEDs* on Page 103 for information about the LEDs.

3/7/20

**PEPPERL+FUCHS**

# 6. Managing the ICDM-RX

This section discusses the following ICDM-RX maintenance procedures:

- *Rebooting the ICDM-RX*
- *Uploading Firmware to Multiple ICDM-RXs* on Page 67
- *Configuring Multiple ICDM-RXs Network Addresses* on Page 68

  *Note:*  *You can configure the network addresses for multiple ICDM-RXs, configure common settings for the ICDM-RXs, and save the settings to a configuration file that you can use to load settings up to all or selected ICDM-RXs.*

- *Adding a New Device in PortVision DX* on Page 68
- *Changing the Bootloader Timeout* on Page 71, which discusses changing the Bootloader timeout
- *Managing Bootloader* on Page 76, which also discusses checking the Bootloader version and downloading the latest Bootloader
- *Restoring Factory Defaults (Specific Models - Reset Button)* on Page 79
- *Restoring Defaults* on Page 81
- *Accessing RedBoot Commands in Telnet/SSH Sessions (PortVision DX)* on Page 82

*Note:*  *You can optionally refer to RedBoot Procedures on Page 86 if you want to perform procedures at the RedBoot level.*

## 6.1. Rebooting the ICDM-RX

There are many ways to reboot the ICDM-RX.

| Method | Procedure |
|---|---|
| PortVision DX | Right-click the ICDM-RX or ICDM-RXs in the *Device List* pane, click **Advanced >Reboot** and then **Yes**.<br><br>*Note:*  *If security has been enabled in the web page, you will need to reboot the ICDM-RX in the web page.* |
| Web page | **System** \| **Reboot:** You have 10 seconds to Cancel before the ICDM-RX automatically reboots. Optionally, you can click **Reboot Now**. |
| Telnet | Type **reset**. |
| ICDM-RX<br>DIN Rail Models | ICDM-RX DIN rail models have a **Reset/Restore** switch.<br><br>• If the **Reset/Restore** switch is depressed for less than 2 seconds, the ICDM-RX reboots.<br>• If the **Reset/Restore** switch is depressed for greater than approximately 5 seconds it restores the ICDM-RX to the factory default values. |

**PEPPERL+FUCHS**

## 6.2. Uploading Firmware to Multiple ICDM-RXs

You can use this procedure if your ICDM-RX is connected to the host PC, laptop, or if the ICDM-RX resides on the local network segment.

1. If you have not done so, install PortVision DX (*Installing PortVision DX* on Page 22) and **Scan** the network.

2. Shift-click the multiple ICDM-RXs on the **Main** screen that you want to update and use one of the following methods:

    - Click the **Upload** button.
    - Right-click and then click **Advanced > Upload Firmware**.
    - Click **Advanced >Upload Firmware** in the **Manage** menu.
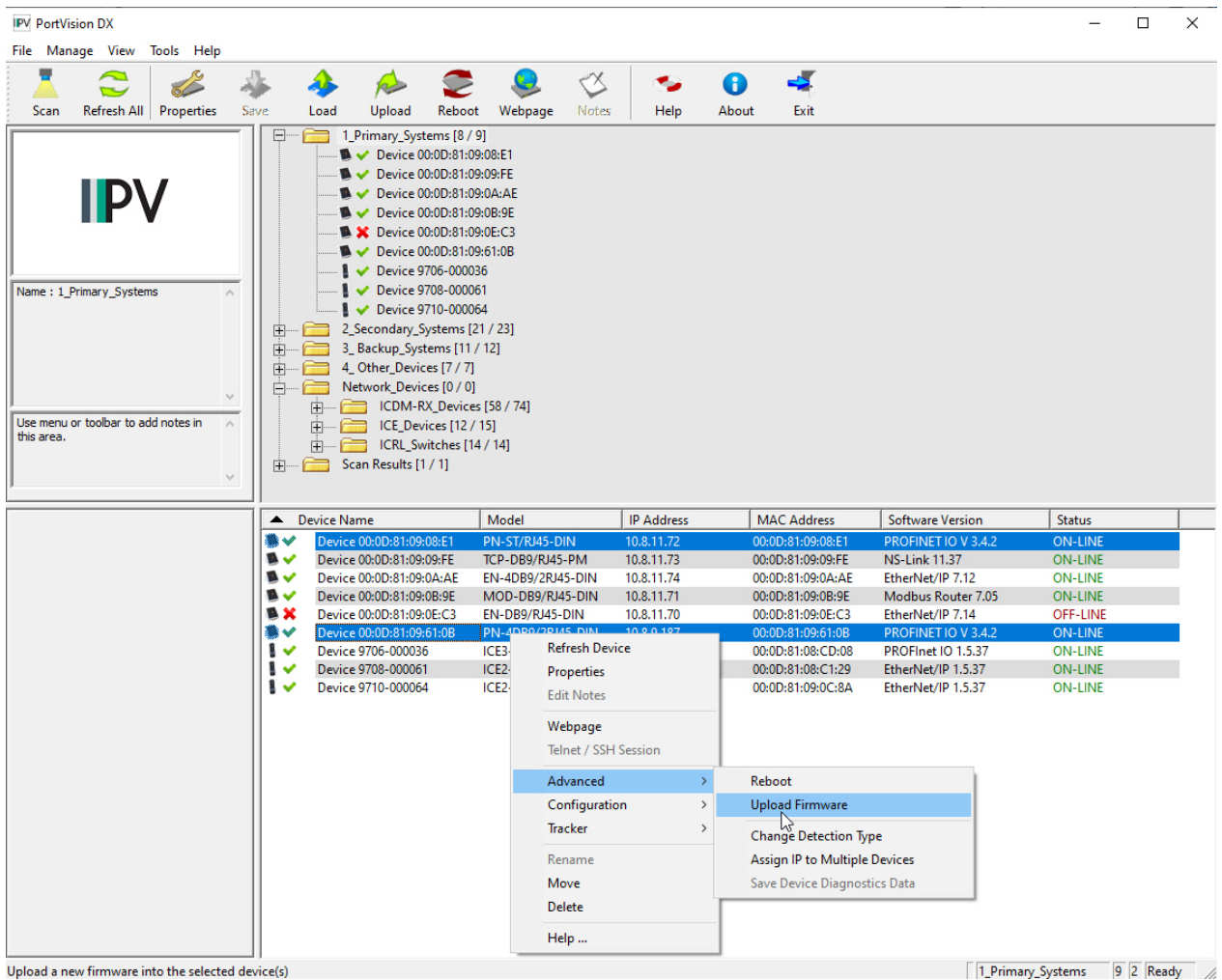


3. Browse, click the firmware (**.cmtl**) file, **Open** (*Please locate the new firmware*), and then click **Yes** (*Upload Firmware*).

    It may take a few moments for the firmware to upload onto the ICDM-RX. The ICDM-RX reboots itself during the upload process.

4. Click **Ok** to the advisory message about waiting to use the device until the status reads **ON-LINE**.

In the next polling cycle, PortVision DX updates the *Device List* pane and displays the new firmware version.

3/7/20

**PEPPERL+FUCHS**

## 6.3. Configuring Multiple ICDM-RXs Network Addresses

You can configure the network addresses for multiple ICDM-RXs using the **Assign IP to Multiple Devices** option.

In addition, you can also configure common settings for the ICDM-RX web page and save the settings to a configuration file that you can load to all or selected ICDM-RXs. See *Configuration File* on Page 74 for more information.

The ICDM-RXs must be on the same network segment for this procedure to work. Use the following steps to configure multiple ICDM-RXs.

1. If you have not done so, install PortVision DX (*Installing PortVision DX* on Page 22) and **Scan** the network.

2. Shift-click the ICDM-RXs for which you want to program network information, right-click, and click **Advanced > Assign IP to Multiple Devices**.

3. Enter the starting IP address, subnet mask, IP Gateway and click **Proceed**.

   PortVision DX displays the programmed IP addresses in the *Device List* pane after the next refresh cycle.
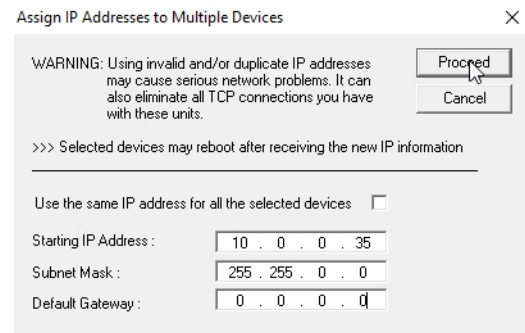
## 6.4. Adding a New Device in PortVision DX

You can add a new ICDM-RX manually, if you do not want to scan the network to locate and add new ICDM-RXs, but there may be cases where you want to use the *Add New Device* window to:

• Configure ICDM-RX units that are not on the local network (remote) using *Remote Using the IP Address* on Page 68.

• Pre-configure an ICDM-RX in PortVision DX (local) using *Local Using the IP Address or MAC Address* on Page 69.

### 6.4.1. Remote Using the IP Address

Use the following procedure to add a remote ICDM-RX to PortVision DX.

1. Access the *New Device* window using one of these methods:

   • Click **Add New > Device** in the *Manage* menu.

   • Right-click a folder or a RocketLinx switch in the *Device Tree* pane (anywhere in the pane, as long as an ICDM-RX is not highlighted and you are in a valid folder) and click **Add New > Device**.

2. Select the appropriate ICDM-RX in the **Device Type** drop list.

3. Select the appropriate model in the **Device Model** drop list.

4. Enter a friendly device name in the **Device Name** list box.

5. Select **REMOTE** for the *Detection Type*.

6. Optionally, enter the serial number in the **Serial Number** list box.

7.  Enter the IP Address for the ICDM-RX. It is not necessary to enter the Subnet Mask and Default Gateway.



8.  Click **OK** to close the *Add New Device* window. It may take a few moments to save the ICDM-RX.

9.  If necessary, click **Refresh** for the new ICDM-RX to display in the *Device Tree* or *Device List* panes. The ICDM-RX shows OFF-LINE if it is not attached to the network or if an incorrect IP address was entered.

### 6.4.2. Local Using the IP Address or MAC Address

Use the following procedure to add a local ICDM-RX to PortVision DX if you do not want to scan the network.

1.  Locate the network information or MAC address of the ICDM-RX you want to add.

2.  Access the *New Device* window using one of these methods:

    • Click **Add New > Device** in the *Manage* menu.

    • Right-click a folder or a RocketLinx switch in the *Device Tree* pane (anywhere in the pane, as long as an ICDM-RX is not highlighted and you are in a valid folder) and click **Add New > Device**.

3.  Select the appropriate ICDM-RX in the **Device Type** drop list.



4.  Select the appropriate model in the **Device Model** drop list.

5.  Enter a friendly device name in the **Device Name** list box.

6.  Select **LOCAL** for the *Detection Type*.

3/7/20

**PEPPERL+FUCHS**

69

7.   Enter the MAC address or network information.

*Note:*   *A MAC address label is attached to all ICDM-RX units.*

8.   Optionally, enter the serial number in the **Serial Number** list box.

9.   Click **Ok**.

10. If necessary, click **Refresh** for the new ICDM-RX to display in the *Device Tree* or *Device List* panes. The ICDM-RX shows OFF-LINE if it is not attached to the network or if an incorrect IP address was entered.

   •

**PEPPERL+FUCHS**

## 6.5. Changing the Bootloader Timeout
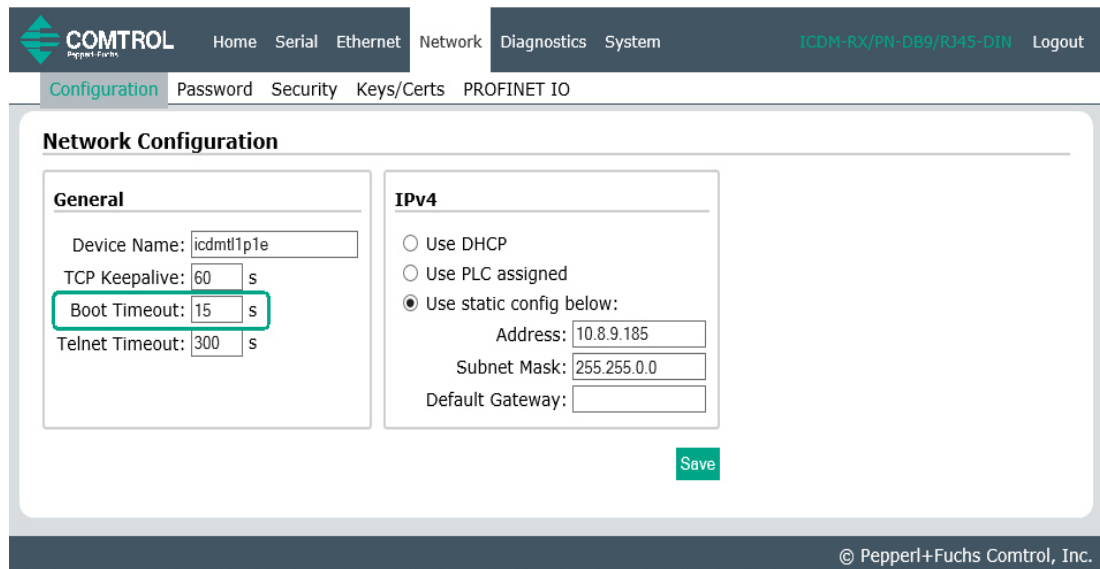
PEPPERL+FUCHS

**PEPPERL+FUCHS**

Use the following procedure to change the Bootloader timeout to 45 seconds. You can use this procedure to return the Bootloader timeout to 15 seconds after you have successfully uploaded SocketServer.

1. If necessary, use your browser to access the ICDM-RX using the IP address.

2. Click **Network**.

**PEPPERL+FUCHS**

3. Enter 45 in the **Boot Timeout** field and click **Save**.



*Note:* *You should return the Bootloader Timeout value back to 15 seconds after you upload the firmware.*
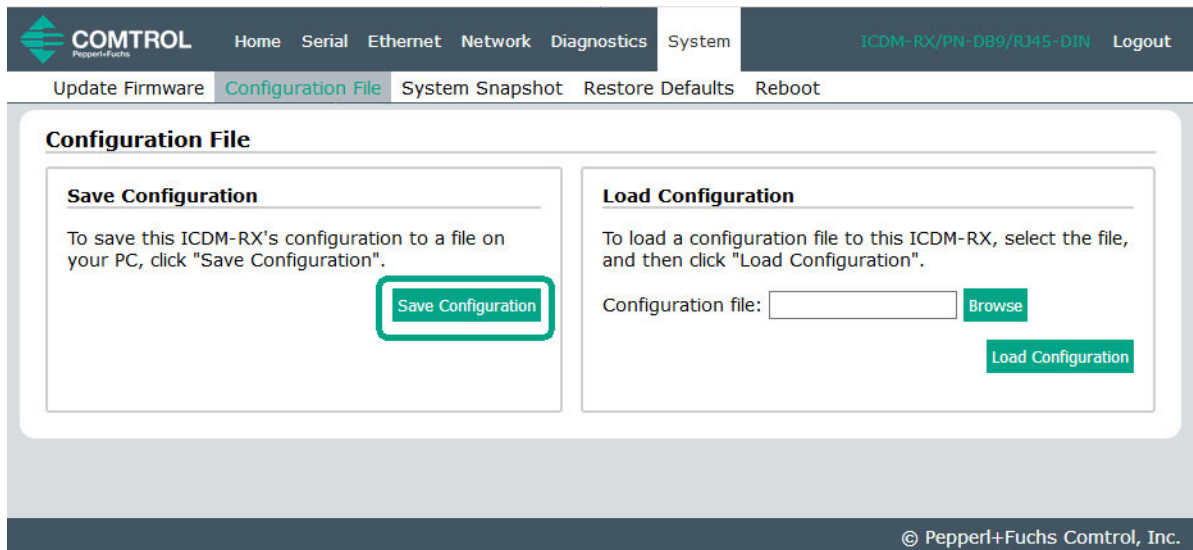
## 6.6. Using Configuration Files

This subsection discusses how to create (save) and load ICDM-RX configuration files. You may want to create ICDM-RX configuration files for these reasons:

- Save the ICDM-RX configuration settings so that you can load them on similar ICDM-RXs to save configuration ICDM-RX

- Save the ICDM-RX configuration settings because you need to remove a firmware version to install a new firmware version and you want to reload the configuration settings into the new firmware.

### 6.6.1. Saving Configuration Files

Use this procedure to save configuration files.

1. Enter the IP address into your browser to access the web interface.
2. Click **System | Configuration File**.
3. Click the **Save Configuration** button.



4. Depending on your browser, may need to click save or direct it to a specific file location.

**PEPPERL+FUCHS**

### 6.6.2. Loading Configuration Files

Use the following procedure to load configuration files.

1.  If necessary, enter the IP address in your browser.
2.  Click **System** | **Configuration File**.
3.  Click the **Browse** button and select the configuration file. The default configuration file name is:

    **dm_xxx.xxx.xxx.xxx.ds**

    Where *xxx.xxx.xxx.xxx* is the IP address and *.ds* is the file extension.
4.  Click the **Load Configuration** button.
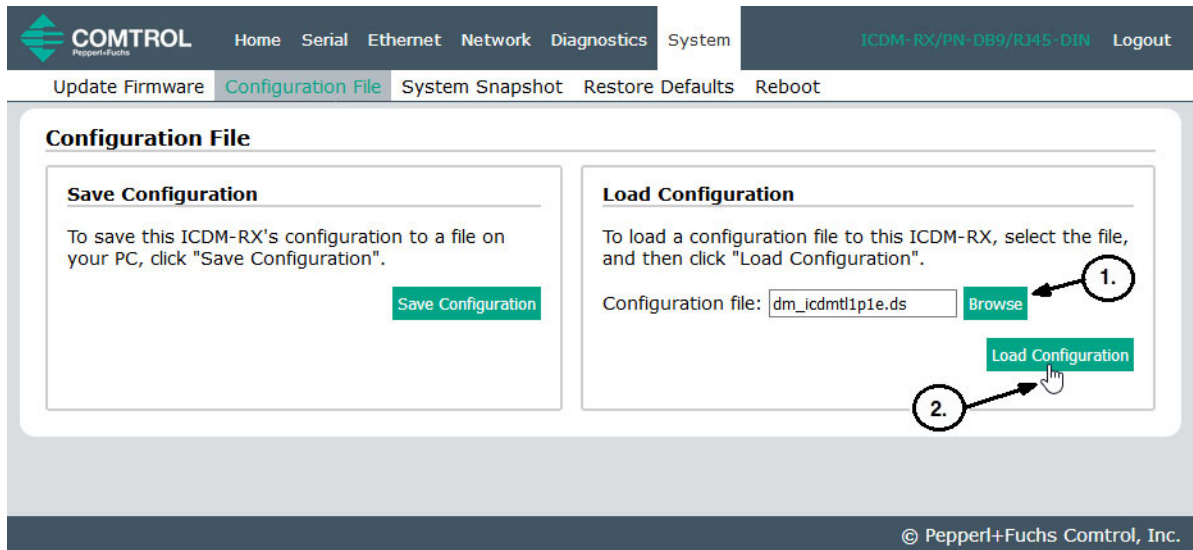


## 6.7. Managing Bootloader

*Bootloader* refers to the operating system that runs on the ICDM-RX hardware during the power on phase, which then loads the default application (for example, EtherNet/IP, EtherNet/IP to Modbus, Modbus Router, PROFINET IO, or PROFINET IO to Modbus firmware).

**Note:** *Typically, you should not update the Bootloader unless advised to do so by Pepperl+Fuchs Technical Support.*

There are several methods and tools that you can use to check the Bootloader version or update the Bootloader.

*   **PortVision DX** is the easiest way to check the Bootloader version and upload the latest version.
*   Optionally, RedBoot can be used to check the Bootloader version and update the Bootloader. See *RedBoot Procedures* on Page 86 for procedures.

3/7/20

**PEPPERL+FUCHS**

## 6.7.1. Checking the Bootloader Version

The following procedure uses PortVision DX to check the Bootloader version. Optionally, you can use RedBoot, see *Determining the Bootloader Version* on Page 90.

1. If you have not done so, install PortVision DX (*Installing PortVision DX* on Page 22) and **Scan** the network.

2. Right-click the ICDM-RX in the *Device List* pane and click **Advanced > Reboot**.

3. Click **Yes** to the *Confirm Reboot* query.

4. Right-click the ICDM-RX in the *Device List* pane, click **Refresh.** You may need to do this several times until you catch the reboot cycle in the *Device List* pane. The Bootloader version is briefly displayed during the reboot cycle before  application (for example, EtherNet/IP,  EtherNet/IP to Modbus, Modbus Router, PROFINET IO, or PROFINET IO to Modbus firmware) loads.

5. Check the **https://www.pepperl-fuchs.com** web site to see if a later version of Bootloader is available.
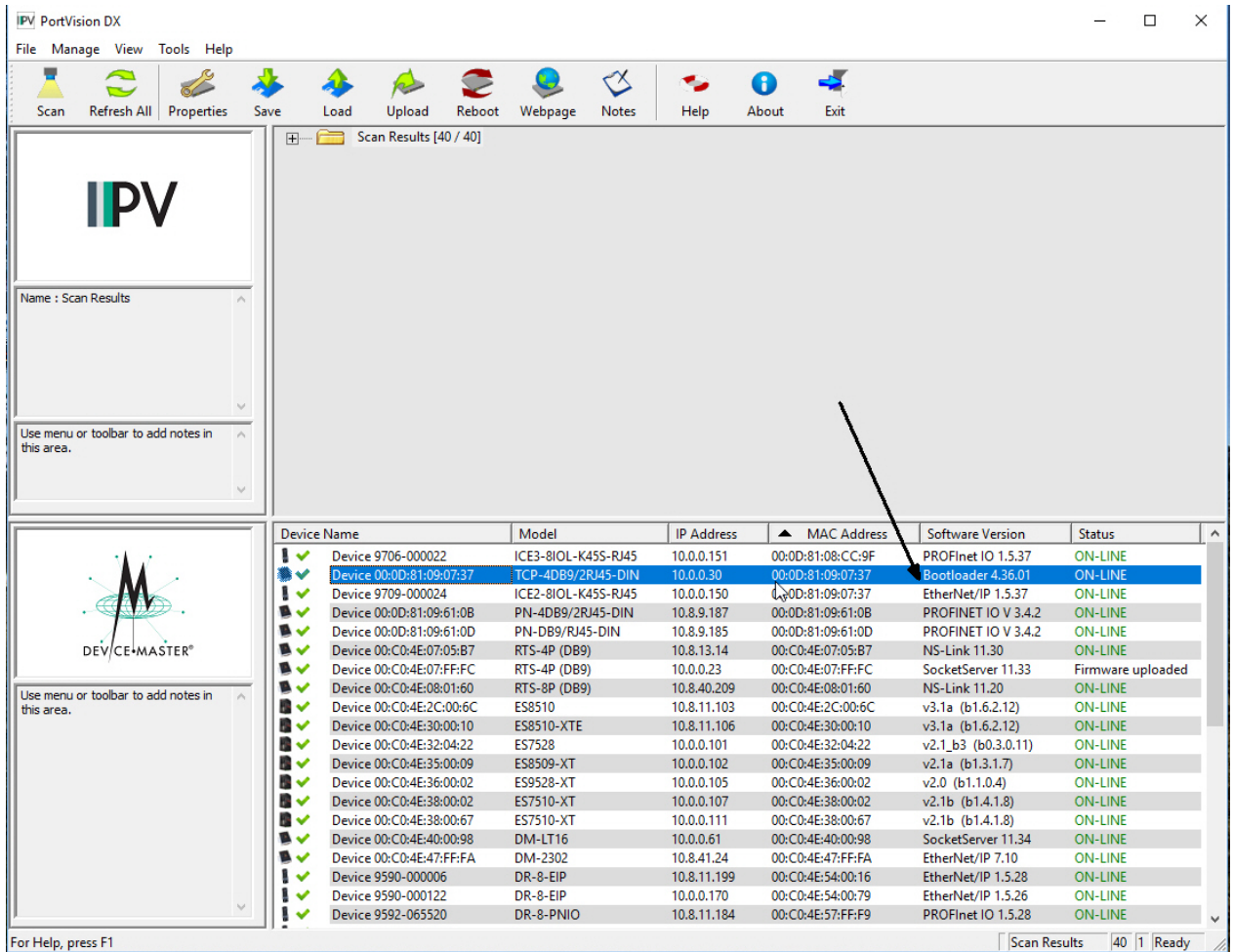


6. Go to the next subsection if you need upload a new version of Bootloader.

PEPPERL+FUCHS

## 6.7.2. Uploading Bootloader

Use the following procedure to upload Bootloader to the ICDM-RX. Typically, you should not update the Bootloader unless advised to do so by Pepperl+Fuchs Technical Support or a notice has been posted with the firmware at https://www.pepperl-fuchs.com.

*Note:* *Technical Support does not recommend updating Bootloader across a WAN. For best results, connect the ICDM-RX directly to a PC or laptop to upload Bootloader.*

> ⚠️ ***Make sure that power is not interrupted while uploading Bootloader. Power interruption while uploading Bootloader will require that the ICDM-RX must be sent into Pepperl+Fuchs so that it can be reflashed.***

***If you are not successful uploading firmware into the ICDM-RX, do not upload Bootloader.***

1. If you have not done so, install PortVision DX (*Installing PortVision DX* on Page 22) and **Scan** the network.

2. If necessary, check the Bootloader version (*Checking the Bootloader Version* on Page 77) and download the latest version.

3. Right-click the ICDM-RX for which you want to update, click **Advanced > Upload Firmware**, browse to the Bootloader **.cmtl** file, and then click **Open**.

**PEPPERL+FUCHS**

4.  Click **Yes** to the *Upload Firmware* message that warns you that this is a sensitive process.
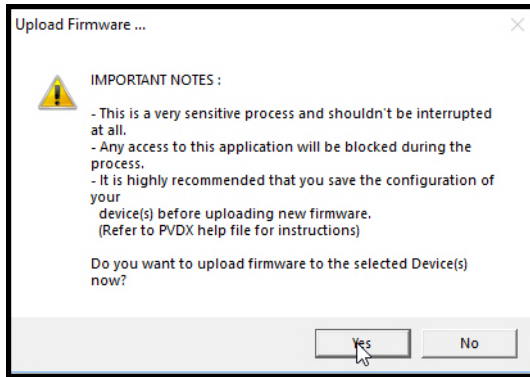


5.  Click **OK** to the second *Upload Firmware* message.
6.  Right-click the ICDM-RX and click **Refresh** until the Bootloader version displays in the *Device List* pane and verify that the new version loaded.

## 6.8. Restoring Factory Defaults (Specific Models - Reset Button)

Use the following procedures to restore the ICDM-RX DIN rail models to the factory defaults.

To return to default port settings, see *Restoring Defaults* on Page 81.

If Technical Support advises you to restore the ICDM-RX factory defaults, depress the **Reset/Restore** switch for greater than 5 seconds.

| Model | Reset Location |
|---|---|
| ICDM-RX/*xxx*-DB9/RJ45-DIN<br>ICDM-RX/*xxx*-ST/RJ45-DIN | Reset button hole to the left of the STATUS LED.<br> |

**PEPPERL+FUCHS**

| Model | Reset Location |
|-------|----------------|
| ICDM-RX/*xxx*-2DB9RJ45-DIN | Reset button hole below the logo on the top, left side. |
| ICDM-RX/*xxx*-2ST/RJ45-DIN | Reset button hole below Ethernet port and above the logo. |
| ICDM-RX/*xxx*-4DB9/2RJ45-DIN | Reset button hole below the logo on the top, left side. |

3/7/20

**PEPPERL+FUCHS**

Restoring the ICDM-RX DIN rail models resets the following to their factory defaults:

- Port settings
- Network settings
- Password
- Telnet enable
- Start up time-out
- SSL enable
- Telnet time-out

## 6.9. Restoring Defaults

Use the following procedure to return some or all of the ICDM-RX settings to factory default values.

1. Open the web interface bye entering the IP address in your browser.
2. Click **System** | **Restore Defaults**.
3. Select the items that you want to restore to factory defaults.
4. Click the **Restore** button.
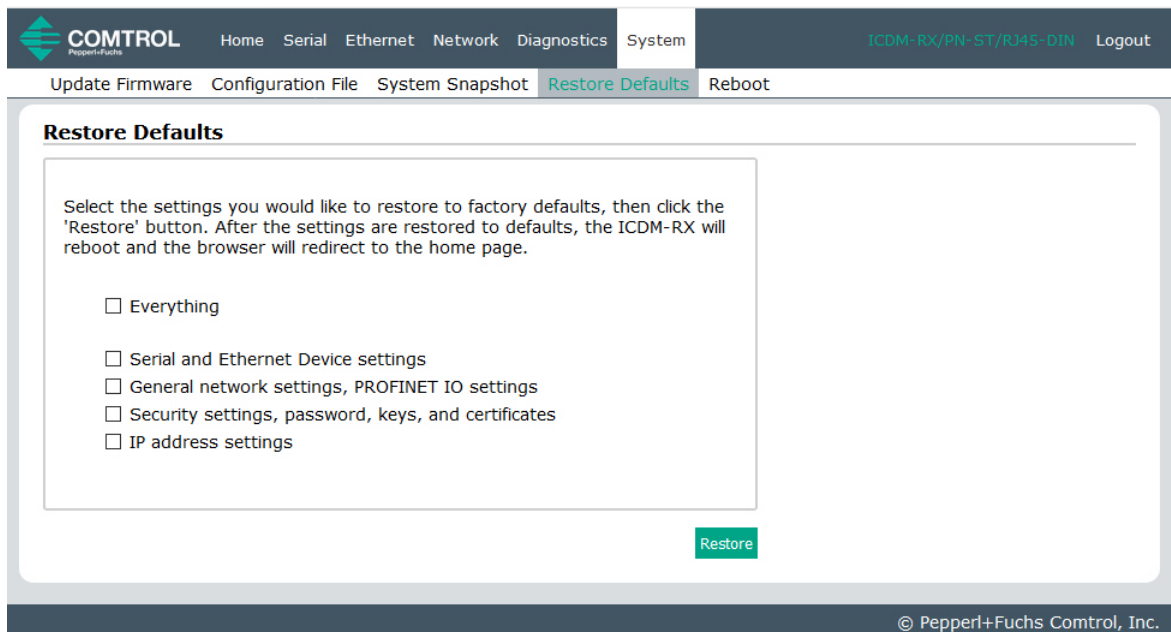


**Note:** This screen shot illustrates the Restore Defaults for PROFINET IO, each ICDM-RX Industrial Gateway contains protocol-specific settings.

**PEPPERL+FUCHS**

## 6.10. Accessing RedBoot Commands in Telnet/SSH Sessions (PortVision DX)

You can open a Telnet or SSH session using PortVision DX to access RedBoot commands.

Use the following procedure to access a telnet or SSH session with PortVision DX.
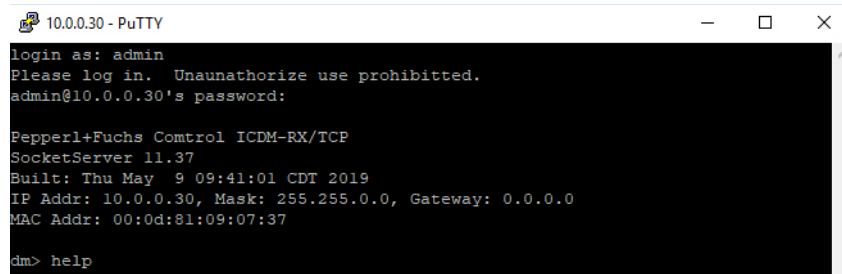
1. In PortVision DX, PortVision DX, right-click the ICDM-RX in the *Device List* pane for which you want to open a telnet session, and click **Telnet/SSH Session**.
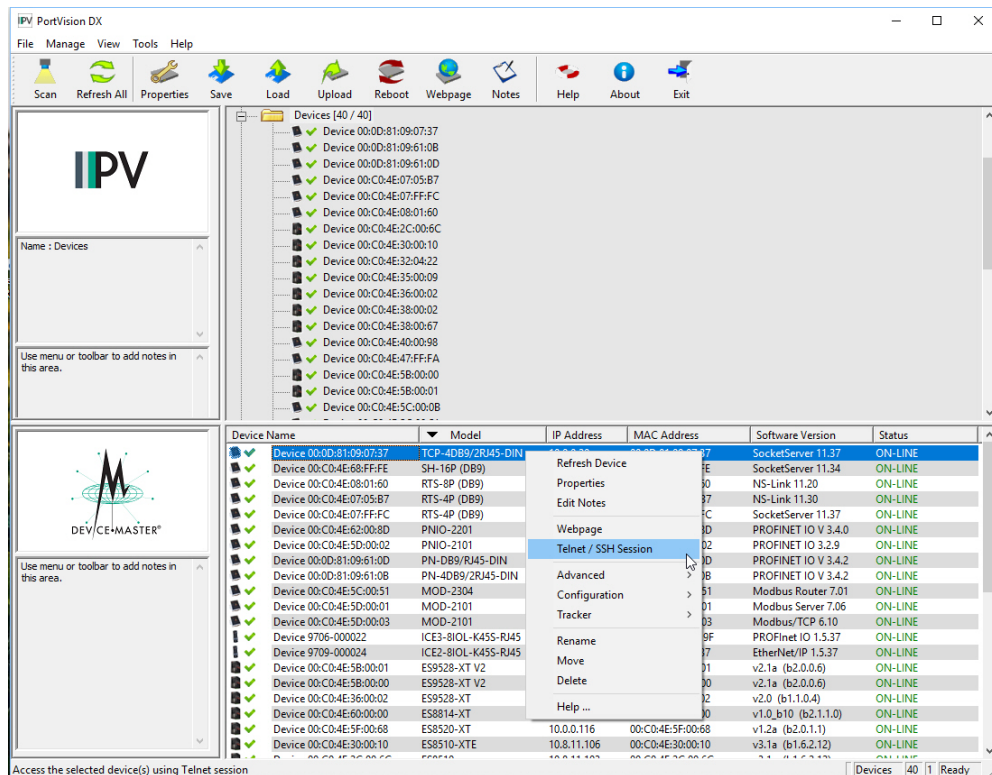


2. Select **Telnet** or **SSH**, leave the **Selected Port** number, and click **OK**

**PEPPERL+FUCHS**
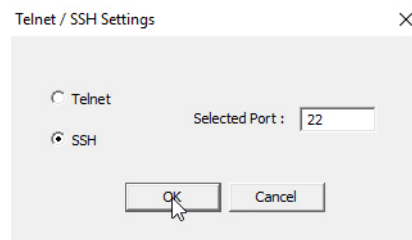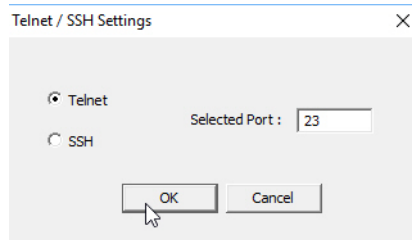
3.  If necessary, enter the password and press **Enter**. If a password has not been set, press **Enter**. If using an SSH session, enter **admin** as the login and press **Enter.**
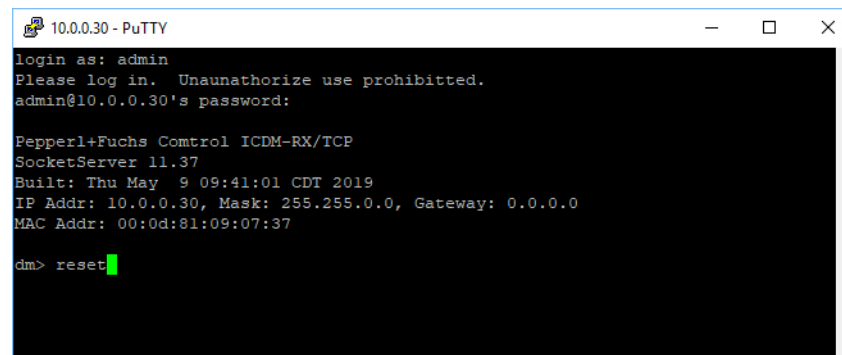
```
10.0.0.30 - PuTTY                                    —  □  ×
login as: admin
Please log in.  Unaunathorize use prohibitted.
admin@10.0.0.30's password:

Pepperl+Fuchs Comtrol ICDM-RX/TCP
SocketServer 11.37
Built: Thu May  9 09:41:01 CDT 2019
IP Addr: 10.0.0.30, Mask: 255.255.0.0, Gateway: 0.0.0.0
MAC Addr: 00:0d:81:09:07:37

dm> help
```

If the PuTTY screen flashes in the background and does not appear as shown above, make sure that **Enable Telnet/ssh** has not been disabled in the web page. To check this, return to PortVision DX, right-click the ICDM-RX in the *Device List* pane, and click **Webpage**. Click the **Network | Security** and verify that the **Enable Telnet/ssh** option is enabled, If it is not, click the option and then click **Save**, and close the web interface.

4.  Type **Reset**, press **Enter**, and close the telnet session.

```
10.0.0.30 - PuTTY                                    —  □  ×
login as: admin
Please log in.  Unaunathorize use prohibitted.
admin@10.0.0.30's password:

Pepperl+Fuchs Comtrol ICDM-RX/TCP
SocketServer 11.37
Built: Thu May  9 09:41:01 CDT 2019
IP Addr: 10.0.0.30, Mask: 255.255.0.0, Gateway: 0.0.0.0
MAC Addr: 00:0d:81:09:07:37

dm> reset
```

**PEPPERL+FUCHS**

5. Quickly re-open the telnet or SSH session using the previous steps.
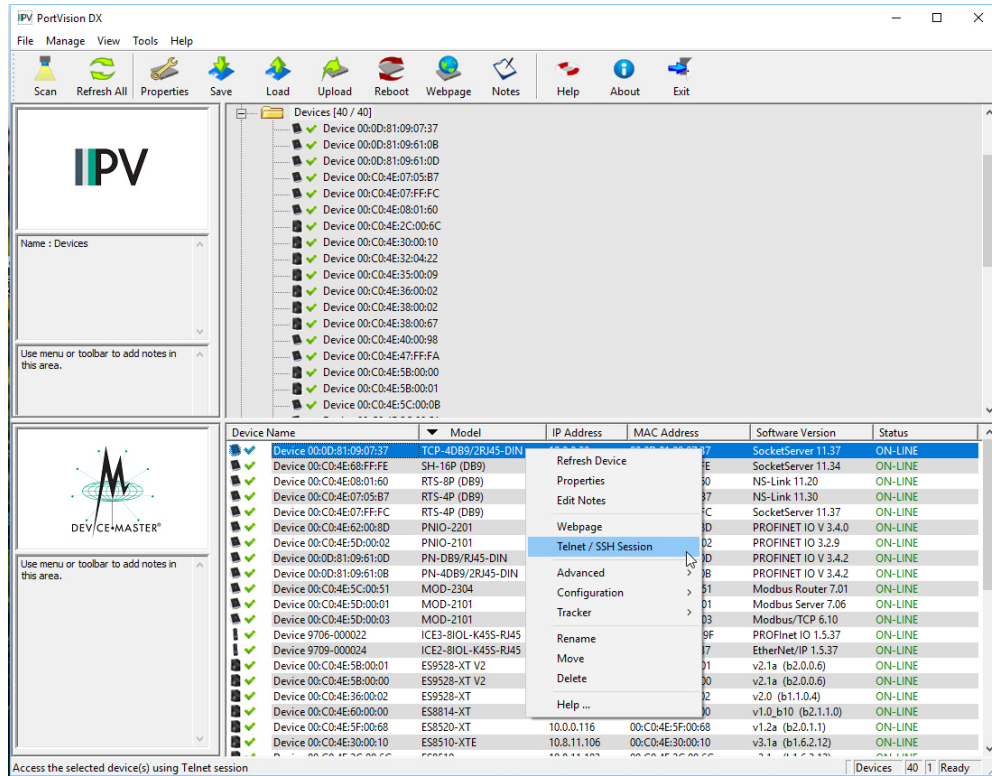


6. Select **Telnet** or **SSH**, leave the **Selected Port** number, and click **OK**

**PEPPERL+FUCHS**
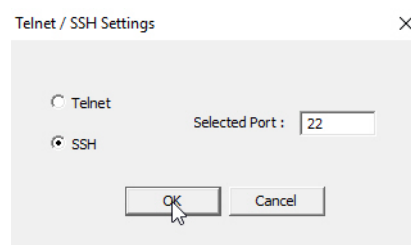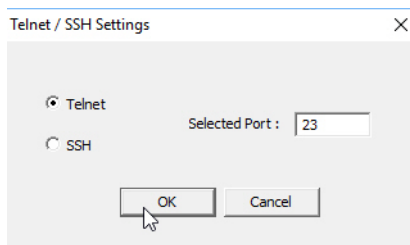
7. Press **Enter**. You can type **help** to review the RedBoot commands. You can also refer to *RedBoot Command Overview* on Page 92.

```
10.0.0.30 - PuTTY                                          −   □   ×
ver

**************************************************
**
**   Comtrol DeviceMaster and ICDM-RX Bootloader 4.36.01
**   Platform: Comtrol DeviceMaster (Cortex-M3)
**   RedBoot(tm) environment - built 15:00:45, Jun  6 2019
**   Portions Copyright (C) 2000, Red Hat, Inc.
**   Portions Copyright (C) Pepperl+Fuchs Comtrol, Inc.
**
**************************************************

RAM: 0x10000000-0x10018000 [0x100018d4-0x1000bc6a available]
     0x10080000-0x1008a000 [0x10080000-0x1008a000 available]
     0x20000000-0x20010000 [0x20000000-0x20010000 available]
     0x28000000-0x29000000 [0x28000000-0x29000000 available]
FLASH: 0x14000000-0x147fffff, 2048 x 0x1000 blocks
RedBoot> help
Set/show web authentication
    auth [noaccess,none,basic,md5,invalid]
Set/Query the system console baud rate
    baudrate [-b <rate>]
Show/set Board revision
    boardrev [rev-number]
Manage machine caches
    cache [ON | OFF]
Show/set catalog number
    catalognum [catalog number]
Display/switch console channel
    channel [-1|<channel number>]
Show chassis features
    chassis
Compute a 32bit checksum [POSIX algorithm] for a range of memory
    cksum -b <location> -l <length>
Clear application configuration
    clearconfig
Show/Set CPU clock frequency
    cpufreq
Calibrate SDRAM clock delay
    delaycal <passes>
Show/set Device Id
    deviceid [device id]
Disable program loading
    disable
Display (hex dump) a range of memory
    dump -b <location> [-l <length>] [-s] [-1|-2|-4]
Show/set eeprom version
    eepromvers [ver]
Manage FLASH images
    fis {cmds}
Show flash info
    flash
Execute code at a location
    go [-w <timeout>] [-c] [-n] [entry]
Help about help?
    help [<topic>]
Display command history
    history
Show/set HW feature flags
    hwflags [flags]
Show/set IP address config
```

*Note:* *The dm prompt should be replaced by a Redboot prompt. If not, you can reset the Bootloader timeout for a longer time period and retry this procedure.*

3/7/20

**PEPPERL+FUCHS**

# 7. RedBoot Procedures

You can use this section as a reference if you want to perform tasks in RedBoot.

- *Accessing RedBoot Overview* on Page 86
- *Establishing a Serial Connection* on Page 87
- *Establishing a Telnet Connection* on Page 88
- *Determining the Network Settings* on Page 89
- *Configuring the Network Settings* on Page 89
- *Changing the Bootloader Timeout* on Page 90
- *Determining the Bootloader Version* on Page 90
- *Resetting the ICDM-RX* on Page 91
- *Configuring Passwords* on Page 91
- *RedBoot Command Overview* on Page 92

Optionally, you can install PortVision DX on a Windows system on the network and perform all of these tasks. PortVision DX provides a Telnet/SSH session, which is discussed in *Accessing RedBoot Commands in Telnet/ SSH Sessions (PortVision DX)* on Page 82.

## 7.1. Accessing RedBoot Overview

To access RedBoot, you can use one of the following methods:

- A *serial* connection between Port 1 on the ICDM-RX and a COM port on a PC (Page 87). If you plan on using the serial method, you will need a null modem cable, a terminal program installed and configured on the PC, and a **Bootloader Timeout** value in excess of 15 seconds. If the **Bootloader Timeout** value has been reduced to 1 second, this procedure will NOT be possible.

  ***Note:*** *Use the serial connection method, if the ICDM-RX is not on the same Ethernet network segment as the PC.*

  If you do not know the IP address of the ICDM-RX you must use a serial connection to communicate with the ICDM-RX.

- A *telnet* connection (Page 88), if the ICDM-RX is locally accessible by Ethernet. A *telnet connection* requires that you know the IP address. In addition, the IP address must also be valid for the network to which it is attached.

  For example: The network segment must be 192.168.250.x to telnet to the ICDM-RX default IP address if you have not changed the IP address to operate on your network.

**PEPPERL+FUCHS**

## 7.2. Establishing a Serial Connection

Use the following procedure to set up a serial connection with a terminal server program. You can use PuTTY (Windows) or optionally, PuTTY can be accessed from PortVision DX using **Tools > Applications > PuTTY**.

1.  Connect a null-modem cable from an available COM port on your PC to **Port 1** on the ICDM-RX.

    ***Note:*** *See Connecting Serial Devices on Page 53, if you need to build a null-modem cable.*

2.  Configure the terminal server program to the following values:
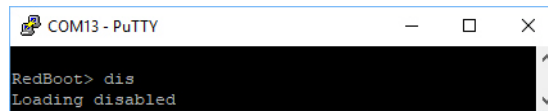
    *   Bits per second = 57600
    *   Data bits = 8
    *   Parity = None
    *   Stop bits = 1
    *   Flow control = None

    ***Note:*** *If you do not disable Bootloader from loading (Steps 3 through 5) within the time-out period (default is fifteen seconds), an application will be loaded from flash and started. If this happens, repeat Steps 3 through 5. The **#!DM** command is the only case-sensitive command and must be in uppercase.*

3.  Reset the ICDM-RX.

    ***Note:*** *Depending on the model, disconnect and reconnect the power cable (external power supply and no power switch) or turn the power switch on and then off (internal power supply).*

4.  Immediately type **#!DM** and press **Enter** in the terminal program.



5.  At the **RedBoot>** prompt, type **dis**, and press **Enter**.
6.  Verify that loading has been disabled.
7.  You can use the appropriate procedure listed on Page 86 or use the *RedBoot Command Overview* on Page 92 to perform the desired task.

**PEPPERL+FUCHS**

## 7.3. Establishing a Telnet Connection

Use the following procedure to telnet to the ICDM-RX.

1. Open a telnet session, enter the ICDM-RX IP address.

    If using Windows, you can use PortVision DX, see *Accessing RedBoot Commands in Telnet/SSH Sessions (PortVision DX)* on Page 82.

2. Press the **Enter** key if you did not program a password or type the password and press **Enter**.
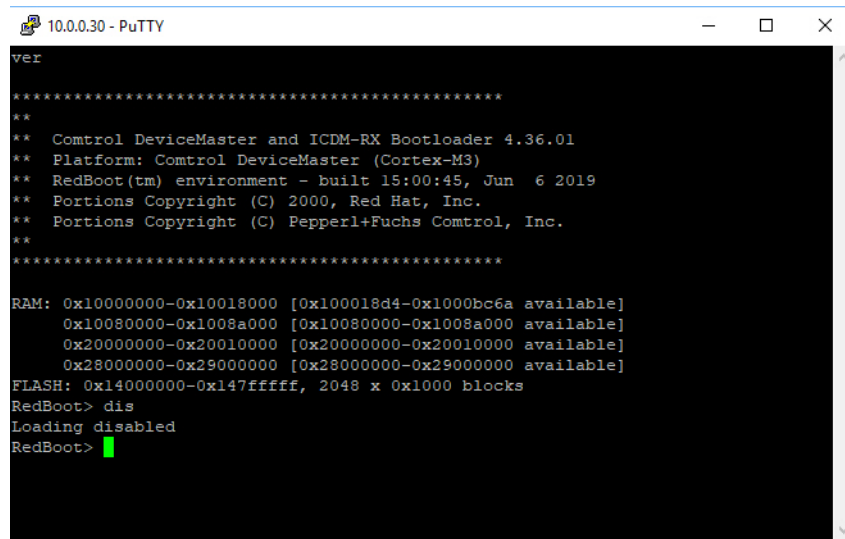
```
10.0.0.30 - PuTTY                                    —   □   ×

Password:

Pepperl+Fuchs Comtrol ICDM-RX/TCP
SocketServer 11.37
Built: Thu May  9 09:41:01 CDT 2019
IP Addr: 10.0.0.30, Mask: 255.255.0.0, Gateway: 0.0.0.0
MAC Addr: 00:0d:81:09:07:37


dm> reset
```

   *Note:* *The ICDM-RX does not come pre-programmed with a password.*

3. Type **reset**, and close the session.
4. Open a new telnet session, enter the ICDM-RX IP address, and the password.
5. Type **dis** to disable the Bootloader.
6. Verify that the system responds with a **Loading disabled** message.

```
10.0.0.30 - PuTTY                                    —   □   ×
ver

**********************************************
**
**   Comtrol DeviceMaster and ICDM-RX Bootloader 4.36.01
**   Platform: Comtrol DeviceMaster (Cortex-M3)
**   RedBoot(tm) environment - built 15:00:45, Jun  6 2019
**   Portions Copyright (C) 2000, Red Hat, Inc.
**   Portions Copyright (C) Pepperl+Fuchs Comtrol, Inc.
**
**********************************************

RAM: 0x10000000-0x10018000 [0x100018d4-0x1000bc6a available]
     0x10080000-0x1008a000 [0x10080000-0x1008a000 available]
     0x20000000-0x20010000 [0x20000000-0x20010000 available]
     0x28000000-0x29000000 [0x28000000-0x29000000 available]
FLASH: 0x14000000-0x147fffff, 2048 x 0x1000 blocks
RedBoot> dis
Loading disabled
RedBoot>
```

**PEPPERL+FUCHS**

## 7.4. Determining the Network Settings

If you are not sure what the network information is on an ICDM-RX, you can perform the following procedure.

The default network settings are:

- IP address: 192.168.250.250
- Subnet mask: 255.255.0.0
- Gateway address: 192.168.250.1

1. Establish communications with the ICDM-RX using the serial (Page 87) or telnet (Page 88) method.
2. At the **RedBoot** prompt, type **ip**.

The IP address, subnet mask, and IP gateway values will display.



```
10.0.0.30 - PuTTY                                    —  □  ×
Loading disabled
RedBoot> ip

IP:     10.0.0.30
Mask:   255.255.0.0
Gateway: 0.0.0.0

RedBoot>
```
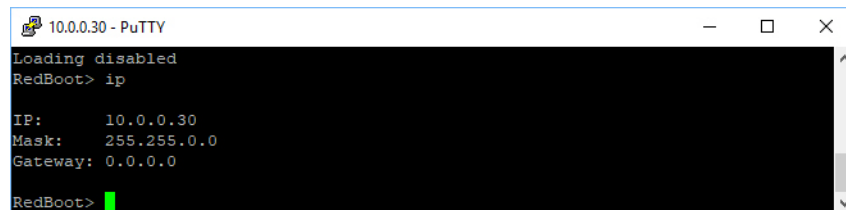
*Note:* *Optionally, you can install PortVision DX on a Windows system on the network and see the IP information in the Device List pane.*

## 7.5. Configuring the Network Settings

Use the following procedure to program the IP address using RedBoot.

1. Establish communications with the ICDM-RX using the serial (Page 87) or telnet (Page 88) method.
2. Enter **ip [*addr mask gateway*]** and press the **Enter** key to configure the IP address. *Where*:

    ***addr*** = IP address you want to use

    ***mask*** = matches you network subnet mask

    ***gateway*** = assigned by your network administrator

    *Make sure that each value is separated by a space*.

```
RedBoot>dis
Loading disabled
RedBoot> ip 192.168.11.152 255.255.0.0 192.168.0.254
RedBoot>
IP:     192.168.11.152
Mask:   255.255.00
Gateway: 192.168.0.254
RedBoot> reset
.. Resetting
```

3. Verify that RedBoot responds with your configured network information or reissue the command.
4. Type **reset** to reset the ICDM-RX, if you do not have any other related RedBoot tasks.

3/7/20

**PEPPERL+FUCHS**

89

## 7.6. Changing the Bootloader Timeout

Use the following procedure to change the Bootloader timeout value.

1. Establish communications with the ICDM-RX using the serial (Page 87) or telnet (Page 88) method.

2. At the **RedBoot** prompt, type **timeout.**

```
RedBoot> dis
Loading disabled
RedBoot> timeout
Timeout 15 seconds
RedBoot> timeout 45
timeout 45 seconds
RedBoot>_
```

RedBoot responds with the current Bootloader timeout value.
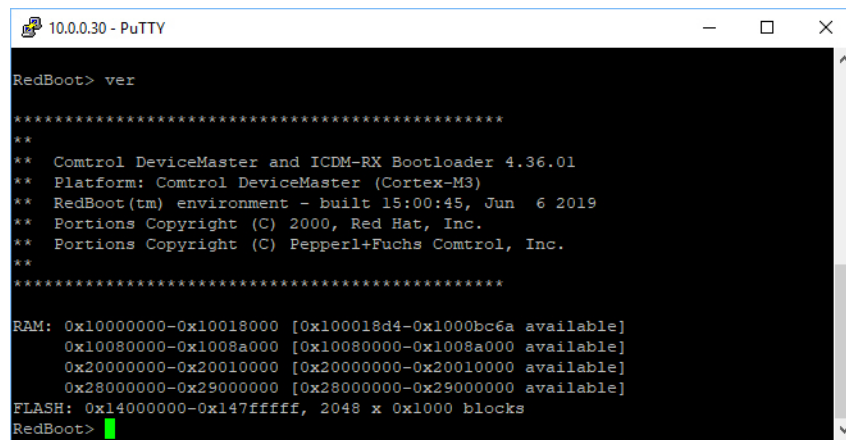
3. Type **timeout** and a value to change the timeout value. For example, **timeout 45** to change the Bootloader timeout to 45 seconds.

## 7.7. Determining the Bootloader Version

Use the following procedure to determine what Bootloader version is loaded in the ICDM-RX.

1. Establish communications with the ICDM-RX using the serial (Page 87) or telnet (Page 88) method.

2. At the **RedBoot** prompt, type **version**.

The Bootloader information displays.



3. Type **reset** to reset the ICDM-RX, if you do not have any other related RedBoot tasks.

*Note:* *Optionally, you can install PortVision DX on a Windows system on the network and see the Bootloader version in the Device List pane. Reboot the ICDM-RX, right-click the ICDM-RX and click Refresh Device until the Bootloader version displays. The Bootloader version is only displayed for a few moments.*

**PEPPERL+FUCHS**

## 7.8. Resetting the ICDM-RX

When you have completed your tasks in RedBoot, you must enter a **reset** command at the **RedBoot**> prompt for the ICDM-RX to begin operation.

*Note:* *The LEDs on the ICDM-RX will go through the power up sequence. The ICDM-RX has completed its reset cycle when the **PWR** or **Status** LED is lit and it stops flashing.*

```
RedBoot> dis
Loading disabled
RedBoot> reset
```
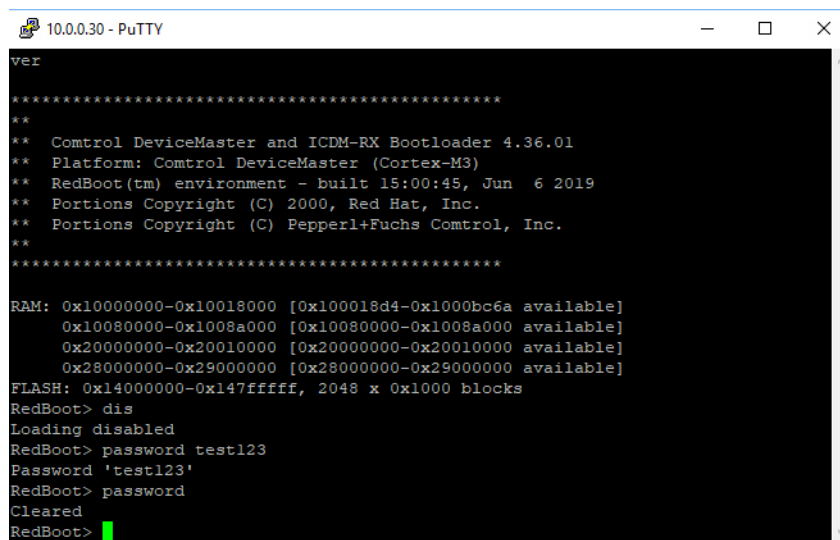
## 7.9. Configuring Passwords

This section discusses how to configure a password for the web and telnet server.

Use the following procedure to establish the ICDM-RX password for the Web and telnet server. Establishing a password prevents unauthorized changes to the ICDM-RX configuration.

1. Establish communications with the ICDM-RX using the serial (Page 87) or telnet method (Page 88).

2. Type **password** [**your_password**] and press **Enter**.

   *Note:* *If you forget your password, you can reprogram the password using the serial method which bypasses the password.*



```
ver

************************************************
**
**   Comtrol DeviceMaster and ICDM-RX Bootloader 4.36.01
**   Platform: Comtrol DeviceMaster (Cortex-M3)
**   RedBoot(tm) environment - built 15:00:45, Jun  6 2019
**   Portions Copyright (C) 2000, Red Hat, Inc.
**   Portions Copyright (C) Pepperl+Fuchs Comtrol, Inc.
**
************************************************

RAM: 0x10000000-0x10018000 [0x100018d4-0x1000bc6a available]
     0x10080000-0x1008a000 [0x10080000-0x1008a000 available]
     0x20000000-0x20010000 [0x20000000-0x20010000 available]
     0x28000000-0x29000000 [0x28000000-0x29000000 available]
FLASH: 0x14000000-0x147fffff, 2048 x 0x1000 blocks
RedBoot> dis
Loading disabled
RedBoot> password test123
Password 'test123'
RedBoot> password
Cleared
RedBoot>
```

*Note:* *The Bootloader version on your ICDM-RX may be different than the version displayed in this above.*

See the **auth** command in the *RedBoot Command Overview* on Page 92, if you want to set up Web browser authentication.

**PEPPERL+FUCHS**

## 7.10. RedBoot Command Overview

The following table is an overview of RedBoot commands available. After accessing RedBoot, you can review the list of commands on-line by entering **help** and pressing the **Enter** key..

| RedBoot Commands | |
|---|---|
| **auth**<br>**{noaccessˌnoneþasicˌmd5ˌinvalid}** | Sets or displays web authentication. The default is set to **none**, which means that there is no authentication required to access the web server.<br><br>To deny access to the web server, click **noaccess** or **invalid**. If access is attempted, a message appears to notify the user that access is denied.<br><br>To configure the web server to request an un-encrypted password, click **basic**. To configure the web server to request an encrypted password, click **md5**. (Some browsers do not support the **md5** command.) |
| **baudrate [-b <rate>]** | Set/Query the system console baud rate. |
| **boardrev†** | Displays the board revision. |
| **cache [ON | OFF]** | Manages machine caches. |
| **catalognum [catalog number]†** | Shows catalog number. |
| **channel [-1|<channel number>]** | Displays or switches the console channel. |
| **chassis†** | Displays chassis information. |
| **cksum -b <location> -l <length>** | Computes a 32-bit checksum [POSIX algorithm] for a range of memory. |
| **clearconfig** | Clears the application configuration. |
| **cpufreq†** | Shows CPU clock frequency. |
| **delaycal <passes>†** | Calibrates SDRAM clock delay. |
| **deviceid [device id]†** | Shows the Device ID. |
| **disable** | Disables automatic load of the default application. |
| **dump-b<location>[-l<length>][-s] [-1|-2|-4]** | Display (hex dump) a range of memory. |
| **eepromvers [ver]†** | Shows the eeprom version. |
| **fis {cmds}** | Manages flash images. |
| **flash** | Shows flash information. |
| **go [-w <timeout>] [-c] [-n] [entry]** | Executes code at a location. |
| **help <topic>** | Displays available RedBoot commands. |
| **history** | Displays command history. |
| **hwflags†** | Shows the HW feature flags. |
| **ip [addr mask gateway]** | Displays or sets the IP address configuration. |
| **load [-r] [-v] [-h <host>]**<br>**[-p <TCP port>]**<br>**[-m <varies>]**<br>**[-c <channel_number>]**<br>**[-b <base_address>]**<br>**<file_name>** | Loads a file. |
| **loop 232|422|int port-number** | Runs a loopback test on the port. |
| **mac†** | Displays the Ethernet MAC address. |

3/7/20

| RedBoot Commands (Continued) | |
|---|---|
| **mcmp-s<location>-d<location>-l<length> [-1l-2l-4]** | Compares two blocks of memory. |
| **mcopy-s<location>-d<location>-l<length> [-1l-2l-4]** | Copies memory from one address to another. |
| **mem_read <start_addr> (<end_addr>)** | Reads from memory. |
| **mem_write <value> <start_addr> (<end_addr>)** | Writes to memory. |
| **mfill -b <location> -l <length> -p <pattern> [-1l-2l-4]** | Fills a block of memory with a pattern. |
| **model [model-number]†** | Shows the model number. |
| **modelname [model name]†** | Shows the model name. |
| **numether [num]†** | Shows the number of Ethernet ports. |
| **numserial [num]†** | Shows the number of serial ports. |
| **oemid [id]†** | Shows the OEM ID. |
| **password {password}** | Sets or deletes the password. |
| **ping [-v] [-n <count>] [-l <length>] [-t <timeout>] [-r <rate>] [-i <IP_addr>] -h <IP_addr>** | Network connectivity test. |
| **ramtest <passes>** | Tests the RAM. |
| **ramtime [reg [<value>]]** | Shows RAM timing register values. |
| **reset** | Resets the ICDM-RX. |
| **secureconf [disablelenable]** | Sets or displays secure config enable. |
| **securedata [disablelenable]** | Sets or displays secure data enable. |
| **sernum [prefix] [serial_number]** **sernum [serial_number]†** | Displays device serial number (if available). |
| **?** | Displays short help. |
| **snmp [disablelenable]** | Sets or displays SNMP enable. |
| **summary** | Displays a summary that includes the bootloader version, network address information, MAC address, and security settings. |
| **telnet [disable \| enable}** | Sets or displays telnet server enable. Disables telnet. |
| **teltimeout [seconds]** | Shows or sets telnet time-out. |
| **terse** | Terse command response mode. |
| **t485 port #1 port #2** | Runs port-to-port RS-485 test. Port numbering is Port 0 through 15 and you must connect a straight-through cable such as Ethernet patch cord. |
| **timeout {seconds}** | Displays or sets Bootloader time-out value. |
| **vendorid [vendor id]†** | Shows the vendor ID. |
| **version** | Displays RedBoot version information. |
| **x-b<location>[-l<length>][-s][-1l-2l-4]** | Display (hex dump) a range of memory. |
| **kszdump** | Dump pre-determined set of KSZ8863 registers. |

3/7/20

PEPPERL+FUCHS

| RedBoot Commands (Continued) | |
|---|---|
| **kszrd <r1> [r2]** | Read specified KSZ8863 registers. |
| **kszrestart** | Restart KSZ8863. |
| **kszwr <r1> <val>** | Read specified KSZ8863 registers. |
| *† Read-only items that you cannot change in Redboot.* | |

**PEPPERL+FUCHS**

# 8. External Power Supply Specifications

This section discusses information that you may need if you wish to use your own external power supplies.

- *ICDM-RX/xxx-DB9/RJ45-PM Power Supply* on Page 95
- *ICDM-RX/xxx-DB9/RJ45-DIN or ICDM-RX/xxx-ST/RJ45-DIN Power Supply* on Page 96
- *ICDM-RX/xxx-2ST/RJ45-DIN Power Supply* on Page 97
- *ICDM-RX/xxx-2DB9RJ45-DIN Power Supply* on Page 98
- *ICDM-RX/xxx-4DB9/2RJ45-DIN Power Supply* on Page 99

## 8.1. ICDM-RX/*xxx*-DB9/RJ45-PM Power Supply

This table provides specifications for the power supply shipped with the ICDM-RX 1-port panel mount. This table provides specifications for the optional power supply from Pepperl+Fuchs.

**Screw Terminal Connector**



**Wire gauge:
AWG 12-22**

| Pepperl+Fuchs Power Supply: ICDM-RX/*xxx*-DB9/RJ45-PM | |
|---|---|
| Input line frequency | 43-63 Hz |
| Input line voltage | 90-260 VAC |
| Output voltage | 24VDC |
| Output current | 500 mA @ 24VDC |

This table provides the specifications, if you intend on using your own power supply.

| ICDM-RX/*xxx*-DB9/RJ45-PM External Power Supply | |
|---|---|
| Output voltage† | 5-30VDC |
| Current† | 100 mA (Min) @ 24VDC |
| Power | 2.5 W |
| † Any power supply that meets current consumption, voltage, power, and connector pin outs requirements can be used. | |

## 8.2. ICDM-RX/*xxx*-DB9/RJ45-DIN or ICDM-RX/*xxx*-ST/RJ45-DIN Power Supply

This table provides the specifications to purchase a power supply for an ICDM-RX/*xxx*-DB9/RJ45-DIN or ICDM-RX/*xxx*-ST/RJ45-DIN.
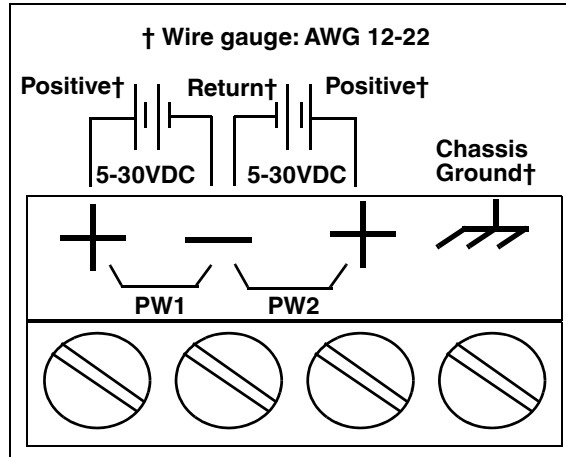


This table provides the specifications, if you intend on using your own power supply.

| ICDM-RX/*xxx*-DB9/RJ45-DIN or ICDM-RX/*xxx*-ST/RJ45-DIN External Power Supply | |
| --- | --- |
| Output voltage† Current† Power | 5-30VDC 100 mA (Min) @ 24VDC 2.5 W |
| † Any power supply that meets current consumption, voltage, power, and connector pin outs requirements can be used. | |

PEPPERL+FUCHS

## 8.3. ICDM-RX/*xxx*-2ST/RJ45-DIN Power Supply

This table provides the specifications to purchase a power supply for an ICDM-RX/*xxx*-2ST/RJ45-DIN.
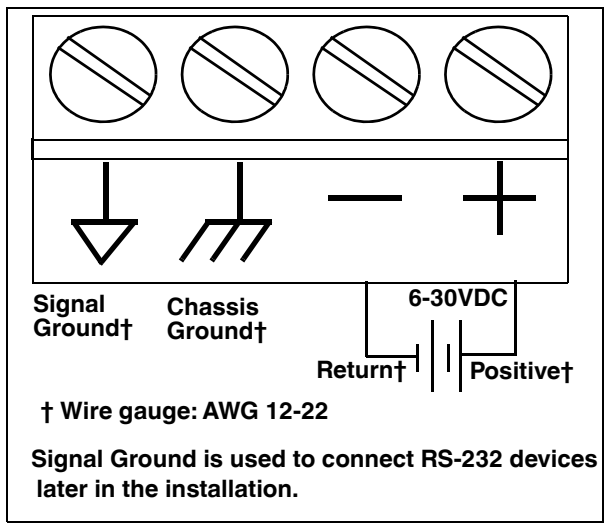


**Signal Ground†**  **Chassis Ground†**  **6-30VDC**

**Return†**  **Positive†**

**† Wire gauge: AWG 12-22**

**Signal Ground is used to connect RS-232 devices later in the installation.**

This table provides specifications if you intend on using your own power supply.

| ICDM-RX/*xxx*-2ST/RJ45-DIN External Power Supply | |
|---|---|
| Output voltage† Current† Power | 6-30VDC 100 mA (Min) @ 24VDC 2.5 W |
| *†  Any power supply that meets current consumption, voltage, power, and connector pin outs requirements can be used.* | |

**PEPPERL+FUCHS**

## 8.4. ICDM-RX/*xxx*-2DB9RJ45-DIN Power Supply

This table provides the specifications to purchase a power supply for an ICDM-RX/*xxx*-2DB9RJ45-DIN.

```
        † Wire gauge: AWG 12-22

Positive†      Return†      Positive†
   ┌─┤├─┬────┬─┤├─┐                    Chassis
   │       │      │           Ground†

  5-30VDC      5-30VDC
 ┌──────────────────────────────────────┐
 │    +       —       +          ⏚      │
 │     \___/   \___/                     │
 │      PW1     PW2                      │
 ├────────┬────────┬────────┬───────────┤
 │   ⊘    │   ⊘    │   ⊘    │    ⊘      │
 └────────┴────────┴────────┴───────────┘
```

This table provides specifications if you intend on using your own power supply.

| ICDM-RX/*xxx*-2DB9RJ45-DIN External Power Supply | |
|---|---|
| Output voltage† Current† Power | 5-30VDC 100 mA (Min) @ 24VDC 2.5 W |
| *† Any power supply that meets current consumption, voltage, power, and connector pin outs requirements can be used.* | |

3/7/20

## 8.5. ICDM-RX/*xxx*-4DB9/2RJ45-DIN Power Supply

This table provides the specifications to purchase a power supply for an ICDM-RX/*xxx*-4DB9/2RJ45-DIN.



**† Wire gauge: AWG 12-22**

This table provides specifications if you intend on using your own power supply.
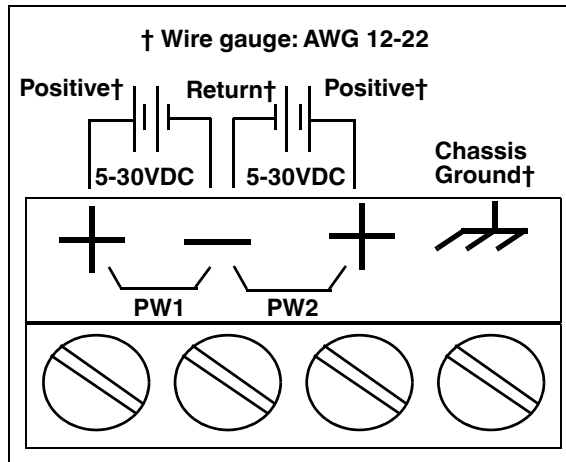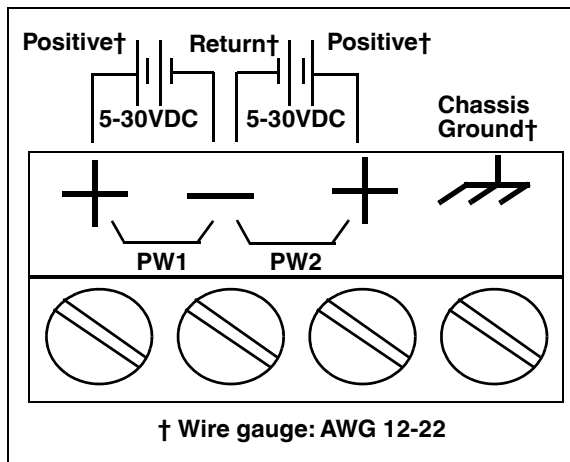
| ICDM-RX/*xxx*-4DB9/2RJ45-DIN External Power Supply | |
|---|---|
| Output voltage† | 5-30VDC |
| Current† | 100 mA (Min) @ 24VDC |
| Power | 2.5 W |
| *† Any power supply that meets current consumption, voltage, power, and connector pin outs requirements can be used.* | |

3/7/20

**PEPPERL+FUCHS**

# 9. Troubleshooting and Technical Support

This section contains troubleshooting information for your ICDM-RX. You may want to review the following subsections before calling Technical Support because they will request that you perform many of the procedures or verifications before they will be able to help you diagnose a problem.

- *Troubleshooting Checklist* on Page 100
- *General Troubleshooting* on Page 101
- *Daisy-Chaining ICDM-RX With Dual Ethernet Ports* on Page 102
- *ICDM-RX LEDs* on Page 103

If you cannot diagnose the problem, you can contact Technical Support.

## 9.1. Troubleshooting Checklist

The following checklist may help you diagnose your problem:

- Verify that you are using the correct types of cables on the correct connectors and that all cables are connected securely.

  *Note:* *Most customer problems reported to Pepperl+Fuchs Technical Support are eventually traced to cabling or network problems.*

| Model | Connected to | Ethernet Cable | Connector Name |
|---|---|---|---|
| ICDM-RX/*xxx*-DB9/RJ45-PM | Ethernet hub or NIC | Standard | 10/100 ETHERNET |
| ICDM-RX/*xxx*-DB9/RJ45-DIN<br>ICDM-RX/*xxx*-ST/RJ45-DIN<br>ICDM-RX/*xxx*-2DB9RJ45-DIN<br>ICDM-RX/*xxx*-2ST/RJ45-DIN | Ethernet hub or NIC | Standard | 10/100 |
| ICDM-RX/*xxx*-4DB9/2RJ45-DIN | Ethernet hub or NIC | Standard | 10/100 - E1/E2 |

- Verify that the network IP address, subnet mask, and gateway is correct and appropriate for the network. Make sure that the IP address programmed into the ICDM-RX matches the unique reserved IP configured address assigned by the system administrator.

  - If IP addressing is being used, the system should be able to ping the ICDM-RX.

  - If using DHCP, the host system needs to provide the subnet mask and gateway.

- Verify that the Ethernet hub and any other network devices between the system and the ICDM-RX are powered up and operating.

- Reboot the system, then reset the power on the ICDM-RX and watch the **PWR** or **Status** (Page 103) light activity.

| PWR or Status LED | Description |
|---|---|
| 5 sec. off, 3 flashes, 5 sec. off, 3 flashes... | RedBoot$^{TM}$ checksum failure. |
| 5 sec. off, 4 flashes, 5 sec. off, 4 flashes... | SREC load failure. |

3/7/20

**PEPPERL+FUCHS**

*PROFINET IO only:*

| Status  or PWR LED | Description |
|---|---|
| Blinks every 10 seconds | No PLC connection. |
| On (solid) | One or more PLC connections have been established. |
| Flashing | • LED flashing mode is enabled.<br>• Error detected or diagnostics information available. |

• If you have a spare ICDM-RX, try replacing the device.

## 9.2. General Troubleshooting

This table illustrates some general troubleshooting tips.

*Note:  Make sure that you have reviewed the Troubleshooting Checklist on Page 100.*

| General Condition | Explanation/Action |
|---|---|
| **PWR** or **Status** LED flashing | Indicates that boot program has not downloaded to the unit.<br>1. Reboot the system.<br>2. Make sure that you have downloaded the most current firmware for your protocol.<br>    *Note:  If the PWR or Status LED is still flashing, contact Technical Support.* |
| **PWR** or **Status** LED not lit and not blinking every 10 seconds<br>*PROFINET IO Only* | Indicates that power has not been applied or there is a hardware failure. Contact Technical Support. |
| Cannot ping the device through Ethernet hub | Isolate the ICDM-RX from the network. Connect the device directly to the NIC in the host system. |
| Cannot ping or connect to the ICDM-RX | The default ICDM-RX IP address is often not accessible due to the subnet masking from another network unless **192.168** is used in the network.<br><br>In most cases, it will be necessary to program in an address that conforms to your network. |
| ICDM-RX continuously reboots when connected to some Ethernet switches or routers | Invalid IP information may also cause the switch or router to check for a gateway address. Lack of a gateway address is a common cause. |

PEPPERL+FUCHS

## 9.3. Daisy-Chaining ICDM-RX With Dual Ethernet Ports

The ICDM-RX models with dual Ethernet ports follow the IEEE specifications for standard Ethernet 10/100BASE-TX topologies.

When using the **E1** and **E2** ports, the ICDM-RX is classified as a switch. When using the **UP** port only, it is a simple end node device.

The maximum number of daisy-chained ICDM-RX units, and the maximum distance between units is based on the Ethernet standards and will be determined by your own environment and the conformity of your network to these standards.

Pepperl+Fuchs has tested with seven ICDM-RX units daisy-chained together using 10 foot CAT5 cables, but this is not the theoretical limit. You may experience a performance hit on the devices at the end of the chain, so it is recommended that you overload and test for performance in your environment. The OS and the application may also limit the total number of ports that may be installed.

Following are some quick guidelines and URLs of additional information. Note that standards and URLs do occasionally change.

- Ethernet 10BASE-T Rules

    - The maximum number of repeater hops is four.

    - You can use Category 3 or 5 twisted-pair 10BASE-T cables.

    - The maximum length of each cable is 100m (328ft).

        ***Note:*** *Category 3 or 5 twisted pair cables look the same as telephone cables but they are not the same. The network will not work if telephone cables are used to connect the equipment.*

- Fast Ethernet 100BASE-TX rules

    - The maximum number of repeater hops is two (for a Class II hub). A Class II hub can be connected directly to one other Class II Fast Ethernet hub. A Class I hub cannot be connected directly to another Fast Ethernet hub.

    - You must use Category 5 twisted-pair 100BASE-TX cables.

    - The maximum length of each twisted-pair cable is 100m (328ft).

    - The total length of twisted-pair cabling (across directly connected hubs) must not exceed 205m (672ft).

        ***Note:*** *Category 5 twisted pair cables look the same as telephone cables but they are not the same. The network will not work if telephone cables are used to connect the equipment.*

- IEEE 802.3 specification: A network using repeaters between communicating stations (PCs) is subject to the 5-4-3 rule of repeater placement on the network:

    - Five segments connected on the network.

    - Four repeaters.

    - Three segments of the 5 segments can have stations connected. The other two segments must be inter-repeater link segments with no stations connected.

        Additional information may be found by searching the web.

**PEPPERL+FUCHS**

## 9.4. ICDM-RX LEDs

The LEDs indicate that the default ICDM-RX application is running. If you have loaded PortVision DX, you can check the ICDM-RX status on-line.

| Model | Network LEDs |
|---|---|
| ICDM-RX/*xxx*-DB9/RJ45-PM | • The **Status** LED on the front of the unit is lit, which indicates that it has power and has completed the boot cycle.<br><br>The **Status** LED flashes while booting and it takes approximately 15 seconds for the Bootloader to complete the cycle. When the Bootloader completes the cycle, the LED has a solid, steady light that blinks approximately every 10 seconds.<br><br>*PROFINET IO only*: When the Bootloader completes the cycle, the LED flashes rapidly for several times then stays off and blinks approximately every 10 seconds when there is no PLC connection.<br><br>• The red **Link Act** LED is lit, which indicates a working Ethernet connection.<br><br>• If the red **Duplex** LED is lit, it indicates full-duplex activity.<br><br>• If the red **100** LED is lit, it indicates a working 100 MB Ethernet connection (100 MB network, only). |
| ICDM-RX/*xxx*-DB9/RJ45-DIN<br>ICDM-RX/*xxx*-ST/RJ45-DIN<br>ICDM-RX/*xxx*-2DB9RJ45-DIN<br>ICDM-RX/*xxx*-2ST/RJ45-DIN<br>ICDM-RX/*xxx*-4DB9/2RJ45-DIN | • The **STATUS** LED on the front of the unit is lit, which indicates that it has power and has completed the boot cycle.<br><br>The **STATUS** LED flashes while booting and it takes approximately 15 seconds for the Bootloader to complete the cycle. When the Bootloader completes the cycle, the LED has a solid, steady light that blinks approximately every 10 seconds<br><br>*PROFINET IO only:* When the Bootloader completes the cycle, the LED flashes rapidly for several times then stays off and blinks approximately every 10 seconds when there is no PLC connection.<br><br>• If the **LINK** (green) LED is lit, it indicates a working Ethernet connection.<br><br>• If the **ACT** (yellow) LED flashes, it indicates network activity. |

**PEPPERL+FUCHS**

# FACTORY AUTOMATION –
# SENSING YOUR NEEDS

# www.pepperl-fuchs.com

**PEPPERL+FUCHS**

*SENSING YOUR NEEDS*

TDOCT-6548_ENG

3/7/20