

groov RIO
UNIVERSAL I/O
USER'S GUIDE

groov RIO UNIVERSAL I/O USER'S GUIDE

for
GRV-R7-MM1001-10
GRV-R7-MM2001-10

Form 2324-260505—May 2026

OPTO 22
Your Edge in Automation.™

43044 Business Park Drive • Temecula • CA 92590-3614
Phone: 800-321-OPTO (6786) or 951-695-3000
Fax: 800-832-OPTO (6786) or 951-695-2712
www.opto22.com

Product Support Services
800-TEK-OPTO (835-6786) or 951-695-3080
Fax: 951-695-3017
Email: support@opto22.com
Web: support.opto22.com

groov RIO UIO User's Guide
Form 2324-260505—May 2026
Copyright © 2020-2026 Opto 22.
All rights reserved.
Printed in the United States of America.

The information in this manual has been checked carefully and is believed to be accurate; however, Opto 22 assumes no responsibility for possible inaccuracies or omissions. Specifications are subject to change without notice.

Opto 22 warrants all of its products to be free from defects in material or workmanship for 30 months from the manufacturing date code. This warranty is limited to the original cost of the unit only and does not cover installation, labor, or any other contingent costs. Opto 22 I/O modules and solid-state relays with date codes of 1/96 or newer are guaranteed for life. This lifetime warranty excludes reed relay modules, *groov* and SNAP serial communication modules, SNAP PID modules, and modules that contain mechanical contacts or switches. Opto 22 does not warrant any product, components, or parts not manufactured by Opto 22; for these items, the warranty from the original manufacturer applies. Refer to Opto 22 form 1042 for complete warranty information.

Wired+Wireless controllers and brains are licensed under one or more of the following patents: U.S. Patent No(s). 5282222, RE37802, 6963617; Canadian Patent No. 2064975; European Patent No. 1142245; French Patent No. 1142245; British Patent No. 1142245; Japanese Patent No. 2002535925A; German Patent No. 60011224.

Opto 22 FactoryFloor, *groov*, *groov* EPIC, *groov* RIO, mobile made simple, The Edge of Automation, Optomux, and Pamux are registered trademarks of Opto 22. Generation 4, *groov* Server, ioControl, ioDisplay, ioManager, ioProject, ioUtilities, *mistic*, Nvio, Nvio.net Web Portal, OptoConnect, OptoControl, OptoDataLink, OptoDisplay, OptoEMU, OptoEMU Sensor, OptoEMU Server, OptoOPCServer, OptoScript, OptoServer, OptoTerminal, OptoUtilities, PAC Control, PAC Display, PAC Manager, PAC Project, PAC Project Basic, PAC Project Professional, SNAP Ethernet I/O, SNAP I/O, SNAP OEM I/O, SNAP PAC System, SNAP Simple I/O, SNAP Ultimate I/O, and Wired+Wireless are trademarks of Opto 22.

ActiveX, JScript, Microsoft, MS-DOS, VBScript, Visual Basic, Visual C++, Windows, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries. Linux is a registered trademark of Linus Torvalds. ARCNET is a registered trademark of Datapoint Corporation. Modbus is a registered trademark of Schneider Electric, licensed to the Modbus Organization, Inc. Wiegand is a registered trademark of Sensor Engineering Corporation. Allen-Bradley, CompactLogix, ControlLogix, MicroLogix, SLC, and RSLogix are either registered trademarks or trademarks of Rockwell Automation. CIP and EtherNet/IP are trademarks of ODVA. Raspberry Pi is a trademark of the Raspberry Pi Foundation. The registered trademark Ignition by Inductive Automation® is owned by Inductive Automation and is registered in the United States and may be pending or registered in other countries. CODESYS® is a registered trademark of 3S-Smart Software Solutions GmbH.

groov includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org>)

All other brand or product names are trademarks or registered trademarks of their respective companies or organizations.

Opto 22
Your Edge in Automation.

Table of Contents

Chapter 1: Welcome	1
Welcome to <i>groov</i> RIO!	1
<i>groov</i> RIO as Edge I/O	2
<i>groov</i> RIO as Remote I/O in an Opto 22 Control System	3
<i>groov</i> RIO with Modbus/TCP or Custom PC-based Control Programs	4
Requirements	5
Power Requirements	5
Field Device Wiring	5
Software Requirements	5
About This Guide	5
What's In This Guide?	5
Service and Maintenance	6
Service (Product Support)	6
 Chapter 2: Mounting and Wiring a <i>groov</i> RIO Module	 7
Gathering your Equipment and Information	7
Familiarizing Yourself with a <i>groov</i> RIO	7
Mounting	9
Choosing a Location	9
Mounting on DIN Rail	9
Mounting on a Panel	11
Wiring Field Devices	11
Understanding Spring Wire Clamps and Preparing Wires	11
Wiring Instructions	12
Removing Wires	14
Bundling Wires with a Cable Tie Mount	14
Connecting Power Supply	16
External Power Source or Supply	16
Power Over Ethernet (PoE)	16
Selecting an Ethernet Network Interface to Connect to a Network	16
 Chapter 3: Initializing a <i>groov</i> RIO UIO	 17
 Chapter 4: Navigating <i>groov</i> Manage	 21
Understanding the Page Navigation Aids	21

Learning How Information is Organized in <i>groov</i> Manage	22
Navigating Through <i>groov</i> Manage on a Computer or Mobile Device	22
Finding Information About I/O Channels	22

Chapter 5: Managing User Accounts, Certificates, and Firewall 25

Managing User Accounts	25
Understanding Permissions	26
Managing Accounts Through LDAP	27
Creating Local User Accounts and Configuring Their Access	40
Managing Certificates on your <i>groov</i> RIO	41
Which <i>groov</i> RIO Applications are Clients, Which are Servers	41
<i>groov</i> RIO as a Server: Creating Server Certificates	41
<i>groov</i> RIO as a Client: Adding a Server's Certificate	43
Configuring the Firewall	45
Creating a Firewall Rule	46
Changing a Firewall Rule	47

Chapter 6: Connecting to a Network or Multiple Networks 51

Before You Begin: What to have and What to Know	51
Start with an Ethernet Connection	51
Finding Your <i>groov</i> RIO on the Network	52
Carefully Schedule Network Changes	52
Identifying Your Network Topology	52
A Single, Flat Network	52
A Network With Multiple LANs	53
Understanding the Network Interfaces	54
Keeping LANs Separate	54
Connecting Multiple <i>groov</i> RIOs Into Daisy-Chains or Rings	55
Wireless Networks	57
Wireless Network Security	57
Virtual Private Networks (VPN) with OpenVPN	58
Choosing Between Automatic and Manual connections	59
Understanding the Difference Between Automatic and Manual Connections	59
For Network Administrators: Tools for Managing Network Traffic to/From <i>groov</i> Devices	60
Examples of Advanced Network Configurations	60
Static IP Address	61
Port Redirection	61
Domain Name and DNS Server IP Address Management	61
Gateway IP Address Management	62
Static Routes	62
Changing the Ethernet Network Interface to Switched Mode	63
Changing the Ethernet Network Interface to Independent Mode	65
Connecting to a Wireless LAN (WLAN0)	67
Configuring for a Wireless Network with WEP, WPA, WPA2, or No Encryption	67
Configuring for a Wireless Network with WPA2-Enterprise Encryption	70
Connecting to a Virtual Private Network (VPN) (TUN0)	73
Configuration Tasks for Network Administrators	75

Adding a Static IP Address	75
Enabling Port Redirection	77
Changing the DNS Server and Domain Name Assignments	79
Changing Gateway IP Address Assignments	80
Adding a Static Route	81
Disabling a Network Interface.....	83
Testing the Network Connections and Fine-Tuning Security.....	84
Chapter 7: Configuring <i>groov</i> RIO System Features	85
Setting and Adjusting Date, Time, and Time Zones	85
Setting the Date and Time Manually	86
Setting the Date, Time, and Time Zone by Synchronizing with Time Servers	86
Setting the Time and Time Zone by Selecting a Location	87
Managing The USB Port	87
Connecting Serial Devices	87
Device Name and Port Number	88
Finding Device Names and Port Numbers	89
Attaching and Detaching a USB Storage Device	89
Requirements for USB Storage Devices	89
Understanding How <i>groov</i> RIO Handles USB Storage Devices	89
Reviewing Security Issues with USB Storage Devices	89
Disabling Access to USB Storage Devices	89
Attaching a USB Storage Device	90
Detaching a USB Storage Device	91
Copying, Moving, or Downloading a File on a USB Storage Device	92
Installing an Approved USB WiFi Adapter.....	93
Enabling Node-RED	94
Uploading Files to <i>groov</i> RIO's Internal File System or USB Storage Device	95
Configuring <i>groov</i> RIO for Shell Access	96
Chapter 8: Configuring I/O	99
Selecting Functions, Signals, and Features.....	99
Selecting a Method for Configuring I/O	100
Configuring I/O Through <i>groov</i> Manage.....	101
Configuring I/O Through CODESYS Development System	103
Checking Compatibility Between Library Package, Development System, and Firmware	104
Adding a <i>groov</i> RIO to a CODESYS Project	106
Adding Channels and Selecting Signal Types (Plugging in Devices)	107
Changing Signal Types (Updating Devices)	107
Setting Features (Configuring Object Parameters)	108
Understanding How Quality Errors are Reported	111
Viewing Information About a Quality Error	111
Chapter 9: Creating and Updating PID Loops	113
Understanding How a PID Works	113
PIDs and Control Programs	113
PID Loops on <i>groov</i> RIO	114

Understanding PID Algorithms	114
Configuring a PID Loop	115
Changing a PID Loop	119
Disabling a PID Loop	120
Inspecting a PID	120
Changing PID Parameters	121
View Specific Values on the Chart	122
Adjusting the Scale of the Charts	122
Chapter 10: Enabling Data Services—MQTT and OPC UA	123
Overview of Configuring and Enabling Data Service	123
Exposing Data (Public Access)	124
Enabling Public Access of the PID Loops through <i>groov</i> Manage	124
Enabling Public Access of the Scratch Pad Area through <i>groov</i> Manage	125
Creating a Scanned Device	126
Configuring and Enabling MQTT	128
Choosing the Right MQTT Client and Payload Type	129
Configuring and Enabling the Data Services MQTT Client	130
The MQTT String Configuration Page	131
The MQTT Broker Configuration Page	132
Configuring and Enabling the Data Services OPC UA Server	132
OPC UA Servers on <i>groov</i> RIO	132
Configuring and Enabling the Data Services OPC UA Server	133
Enabling Data Services and Testing Connections	135
Chapter 11: Developing Node-RED Flows	137
For Experienced Node-RED Developers	137
Learning about Node-RED on RIO	137
Learning to Develop a Node-RED Flow	138
Opening the Node-RED Editor	138
Creating a Flow	139
Deploying the Flow and Testing It	140
Adding a Function Node	140
Installing <i>groov</i> I/O Nodes	141
Installing <i>groov</i> View Nodes to Access Data Stores	143
Installing Opto 22 PAC Control Nodes	144
Chapter 12: Maintaining a <i>groov</i> RIO	149
Backing up Your <i>groov</i> RIO Settings	149
Restoring a Backup or Specific Settings from a Backup File	151
Updating Firmware on a <i>groov</i> RIO	154
Downloading and Installing the Firmware File	155
Troubleshooting	158
Browser Reports that URL to <i>groov</i> RIO UIO is Unreachable	158
CODESYS: “Invalid Channel Type. Module or channel may not be compatible.”	160
CODESYS: Can’t Connect to <i>groov</i> RIO Module	161
Resetting to Factory Defaults	162
Collecting Information for Product Support	162

Conducting an OptoSupport Remote Support Service (RSS) Session	164
Initiating an RSS Session	164
Pausing and Resuming an RSS Session	165
Ending the RSS Session	166
Appendix A: Specifications	167
GRV-R7-MM1001-10, GRV-R7-MM2001-10	167
Features	168
Specifications	169
Wiring Assignments	176
Appendix B: Wiring Diagrams	177
Wiring Field Devices	177
<i>groov</i> RIO Explorer	177
GRV-R7-MM1001-10, GRV-r7-MM20001-10	178
Appendix C: <i>groov</i> RIO Explorer	179
The <i>groov</i> RIO Explorer	180
Assigning Functions and Signals to a Channel	181
Moving and Deleting Signals	182
Viewing Possible Signals and Channels	182
Replacing a Signal	183
Exporting and Importing Combinations of Functions and Signals	184
Exporting	184
Importing	184
Working with Samples	185

1: Welcome

WELCOME TO *groov* RIO!

Opto 22's *groov* RIO® is an independent, intelligent Ethernet-based input/output (I/O) module designed as edge I/O for industrial internet of things (IIoT) applications. *groov* RIO solves two main problems with most remote I/O today:

- First, instead of requiring you to specify several components (rack, power supply, bus coupler, module types, and more), which is time-consuming, difficult, and requires significant domain expertise, **one part number is all you need**. One part number includes built-in multifunction, multi-signal I/O; an I/O processor; power over Ethernet (PoE); and mounting without the need for a rack or chassis—all in a compact industrial package.
- Second, communicating data among field devices, control systems, company software, and cloud services is no longer complex and costly, requiring PLCs, programming, and middleware. Instead, ***groov* RIO simplifies IIoT and automation applications** by including built-in processing and communications: web-based configuration, flow logic software, efficient data communication methods, and multiple automation and information technology protocols.

With *groov* RIO, you don't need a PLC, PAC, or industrial PC. You can place the module almost anywhere, configure it using just a web browser, and communicate data between field devices and on-premises or cloud-based systems and software.



***groov* RIO offers features for a variety of applications. You can:**

- Place the module almost anywhere. *groov* RIO operates through a wide range of operating temperatures (-20 to 70 °C), and is UL Hazardous Locations approved and ATEX compliant. Mount it on a DIN rail or panel.
- Supply power by either Power over Ethernet (PoE) **or** 10–32 VDC power supply.
- Simplify field connections using the 26-pin removable field connector with spring clamp wire retention. Supports wire sizes 22 to 14 AWG.
- Use web-based software to configure I/O channels: inputs or outputs; signals including voltage, current, thermocouple, ICTD; mechanical relays. Thousands of field I/O combinations are possible in one module.
- Use intelligent features like counting, latching, clamping, and more.
- Connect additional devices like a Wi-Fi adapter, a USB memory stick (up to 32 GB), or a USB-to-serial adapter via the *groov* RIO's USB port (you supply the additional devices).
- Easily see the status of power, network, and I/O activity on the module's LEDs.
- Use embedded software to quickly set up data communications.

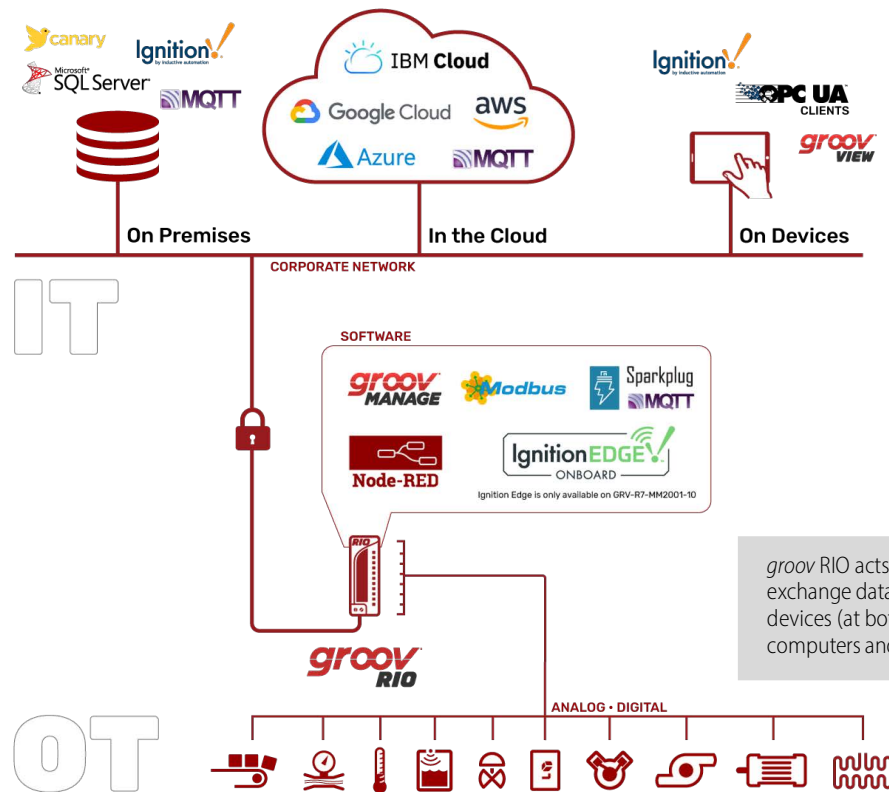
groov RIO as Edge I/O

groov RIO is primarily used as edge I/O in IIoT applications. As you can see in the diagram below, edge I/O bridges the operations technology (OT) world of sensors and actuators, shown at the bottom of the diagram, and the information technology (IT) world of computers and corporate software, at the top.

groov RIO's embedded software and protocol support make it possible to exchange data between these two realms more easily and securely. Embedded software and protocol support include:

- **groov Manage**—Web-based software for configuring groov RIO I/O channels, security, and communications
- **Node-RED**—Software for creating simple data flows to send data to cloud services, databases, other I/O channels, and APIs. Pre-built nodes make flow creation easy.
- **MQTT**—Built-in support for MQTT, an efficient publish/subscribe protocol for exchanging data. Only a simple configuration is needed to publish I/O data and subscribe to commands as Sparkplug-B or string payloads.
- **Modbus®/TCP**—Support for the well-known industrial protocol. groov RIO acts as a Modbus/TCP slave right out of the box.
- **Ignition Edge**—(GRV-R7-MM2001-10 only) Connect to Allen-Bradley®, Siemens®, and Modbus®/TCP devices via OPC UA and create efficient IIoT communications using MQTT with Sparkplug B payload (requires purchase of license [GROOV-LIC-EDGE8](#)).

groov RIO as Edge I/O

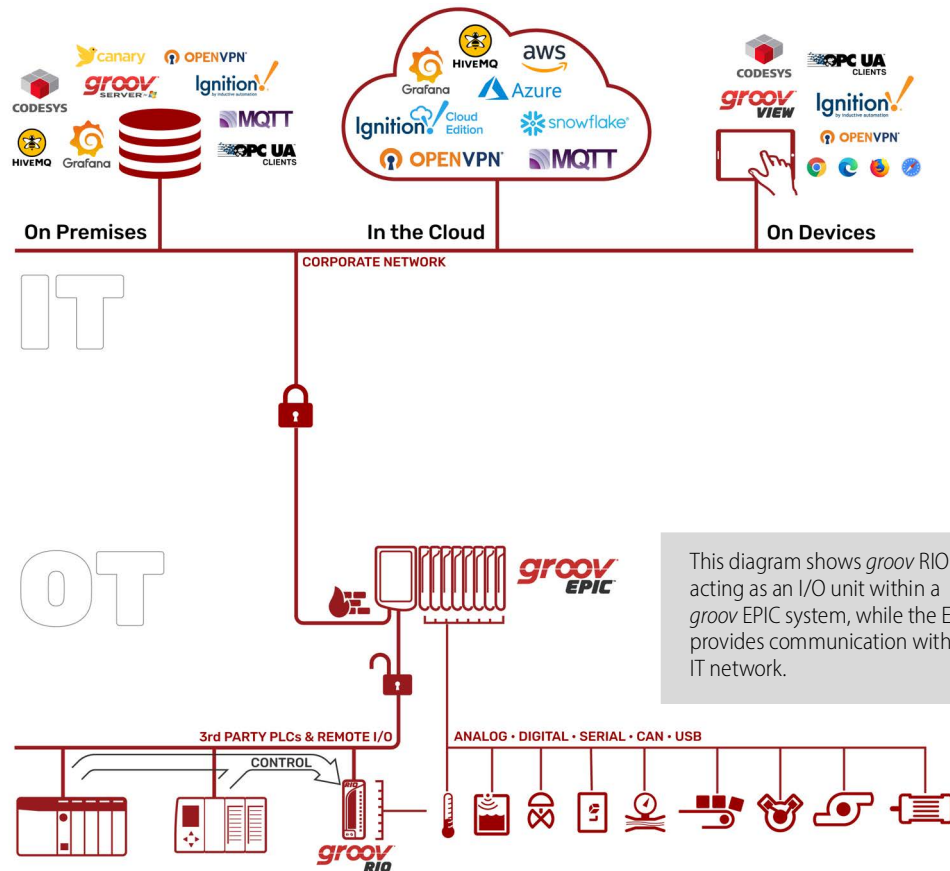


groov RIO as Remote I/O in an Opto 22 Control System

In addition to its use as independent edge I/O for IIoT applications, *groov* RIO can also be used as remote I/O with an Opto 22 *groov* EPIC® processor or SNAP PAC controller. The diagram below shows RIO used with *groov* EPIC.

groov RIO is wired to field devices and acts as an I/O unit within the EPIC's control and I/O network. As an I/O unit, *groov* RIO is compatible with any of the EPIC's programming methods—PAC Control, CODESYS and IEC 61131-3 languages like Ladder Diagram and Function Block Diagram, or languages like C/C++ or Python to build custom control programs. If you have a custom control program, you can access *groov* RIO using its OptoMMP memory map addresses or via REST APIs.

groov RIO as Remote I/O in an Opto 22 Control System



groov RIO with Modbus/TCP or Custom PC-based Control Programs

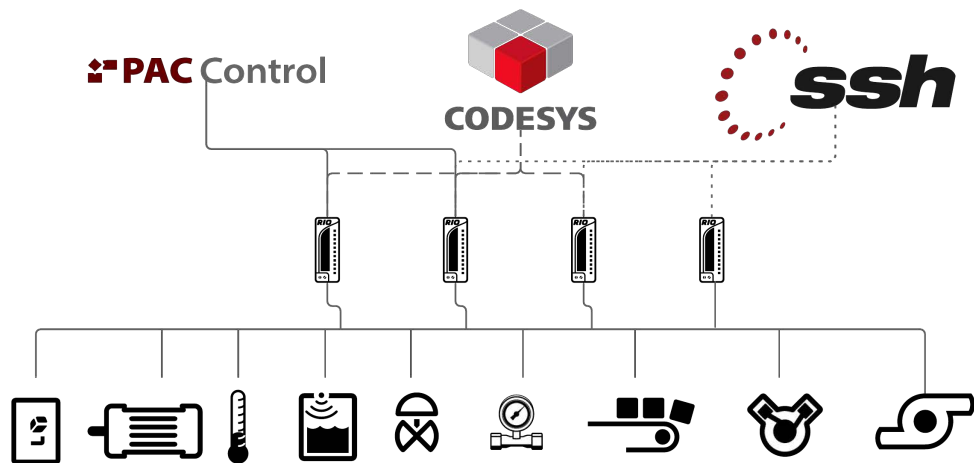
groov RIO can also be accessed by Modbus/TCP masters and by PCs running custom-built control programs:

Modbus/TCP—Because *groov* RIO is a Modbus/TCP slave out of the box, you can use your favorite Modbus/TCP master device or software to poll *groov* RIO's I/O channels.

C++ or .NET and free SDKs—With your favorite development tool and our free SDKs, you can programmatically access I/O values on a *groov* RIO module by accessing the OptoMMP memory map locations of each channel.

HTTP/S, JSON, and REST APIs—Opto 22 provides REST APIs for *groov* Manage, which you use to access the I/O values on a RIO module. A Swagger API document is built into *groov* RIO to quickly access REST API calls and evaluate responses.

groov RIO with Modbus/TCP or Custom PC-based Control Programs



In this diagram, a group of *groov* RIOs are I/O units within a PAC Control strategy. At the same time, they can respond to a CODESYS application and to a PC running a custom control program.

REQUIREMENTS

Power Requirements

You can supply power to a *groov* RIO UIO with either of the following methods (but not both at the same time):

- An external 10 to 32 V DC power source or supply, capable of providing at least 10 Watts
- Power over Ethernet (PoE) through the ETH1 network interface

Field Device Wiring

Connect field devices to *groov* RIO with wire of size 22-14 AWG. Keep the wires as short as possible.

Software Requirements

If you are using *groov* RIO as an independent edge I/O unit, all you need is a web browser to configure I/O, security, and networking, and to create Node-RED flows.

If you are using *groov* RIO as remote I/O with an Opto 22 system running:

- a PAC Control strategy, you need to run PAC Project 10.3000 or higher. If you are running a PAC Control strategy on a:
 - *groov* EPIC processor, you need GRV-EPIC-PR1 firmware version 2.0.0 or higher.
 - SNAP PAC controller, you need firmware 10.3a or higher.
- a CODESYS application, you need CODESYS Development System, V3.5 SP15 Patch 1 or newer (32-bit version) with Opto 22 Library Package for CODESYS Development System version 2.0.0.0 installed.

ABOUT THIS GUIDE

This user's guide shows you how to mount your *groov* RIO, how to connect field devices, how to configure the I/O channels, and much more.

What's In This Guide?

Chapter 1: Welcome describes *groov* RIO and how this document is organized.

Chapter 2: Mounting and Wiring a *groov* RIO Module describes all the requirements for supplying power, plus instructions on mounting and wiring a *groov* RIO.

Chapter 3: Initializing a *groov* RIO UIO describes what to do after you power up your *groov* RIO, which includes creating the first user ID, which has administrator privileges.

Chapter 4: Navigating *groov* Manage describes how to navigate through *groov* Manage and find some important information.

Chapter 5: Managing User Accounts, Certificates, and Firewall describes how you configure RIO to limit what services can connect to it.

Chapter 6: Connecting to a Network or Multiple Networks describes all the factors to consider when you connect a RIO to a network, from a single, simple network to a complex set of networks.

Chapter 7: Configuring *groov* RIO System Features describes what to do after you finish initializing *groov* RIO, which includes setting date, time, and time zones; attaching USB devices, and enabling Node-RED.

SERVICE AND MAINTENANCE

Chapter 8: Configuring I/O describes how to select the functions (input or output), signal types (discrete, analog), and any corresponding features for each channel through *groov* Manage. It also describes where to find information if you want to write a PAC Control strategy or custom application can access your RIO.

Chapter 9: Creating and Updating PID Loops explains how PID loops work and how to create them through *groov* Manage.

Chapter 10: Enabling Data Services—MQTT and OPC UA introduces you to MQTT, how it works in RIO, and how to configure it.

Chapter 11: Developing Node-RED Flows describes what an experienced Node-RED developer needs to know to start writing flows that access RIO's data, as well as provide step-by-step instructions for those new to Node-RED.

Chapter 12: Maintaining a groov RIO describes all the tasks you can do to keep your RIO performing smoothly, how to install firmware updates, perform periodic backups, review guidance to do basic troubleshooting, information to collect should you need to contact Product Support, and an overview of how to conduct an OptoRSS (Remote Support Service) session.

Appendix A: Specifications lists the specifications for each channel of a RIO, as well as the specifications common to all channels on a RIO.

Appendix B: Wiring Diagrams lists all the wiring diagrams for GRV-R7-MM1001-10 and GRV-R7-MM2001-10.

Appendix C: groov RIO Explorer describes our online app that helps you see different combinations and arrangements of channel configurations, help you choose combinations and arrangements that are valid, and create wiring diagrams for your chosen combination.

SERVICE AND MAINTENANCE

To keep your *groov* RIO up-to-date with the latest firmware fixes and features, you'll want to regularly check for and apply maintenance, as described in ["Updating Firmware on a groov RIO" on page 154](#).

If you encounter any problems with your *groov* RIO, follow the instructions in ["Collecting Information for Product Support" on page 162](#) before contacting Opto 22 Product Support.

Service (Product Support)

If you are having problems installing or using *groov* RIO products and cannot find the help you need in this guide or on our website, contact Opto 22 Product Support.

Phone: 800-TEK-OPTO
(800-835-6786 toll-free in the U.S. and Canada)
951-695-3080
Monday through Friday,
7 a.m. to 5 p.m. Pacific Time

Email: support@opto22.com

Opto 22 website: www.opto22.com

NOTE: Email messages and phone calls to Opto 22 Product Support are grouped together and answered in the order received.

2: Mounting and Wiring a *groov* RIO Module

GATHERING YOUR EQUIPMENT AND INFORMATION

Gathering up all the supplies, information, and equipment you need before you mount and wire your *groov* RIO can help get your module up and running more quickly:

- An accessible power source that complies with the requirements described in [“Power Requirements” on page 5](#).
- The proper gauge wires to connect the *groov* RIO to your field devices as described in [“Wiring Field Devices” on page 11](#).
- Pen and paper to note important information that you might need during this process or to keep for future reference.
- The spring clamp tool that ships with your *groov* RIO, which helps you connect wires to the correct pins on the terminal connector.

In addition, make sure you have a list of all the I/O channels (sometimes referred to as points) that you need set up. This might be in a form of a document that maps which channels will connect to a specific field device/point. If you are working with a terminal strip, review the terminal number assignments, making sure you understand which terminal numbers are assigned to specific channels.

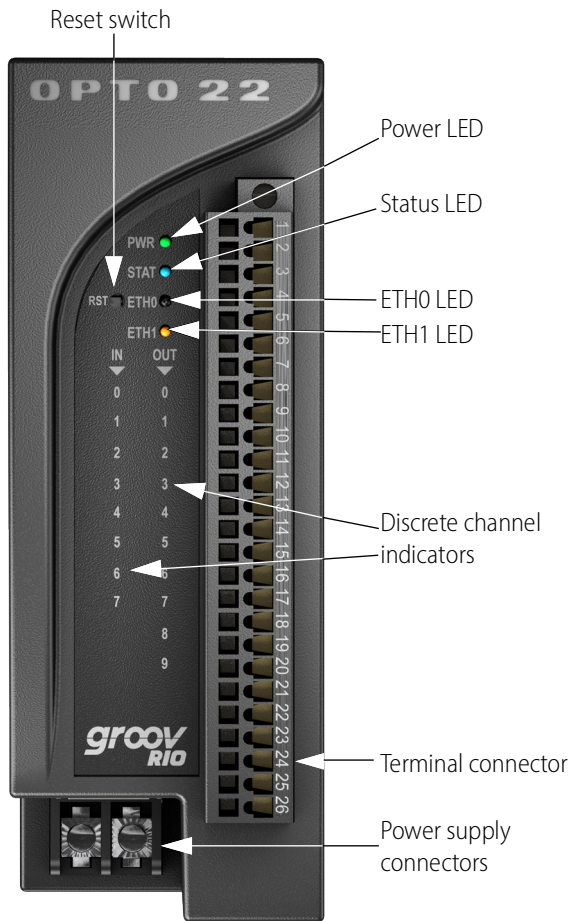
If you are connecting multiple *groov* RIOs, you’ll need to determine if you are connecting them to the network in a daisy-chain formation or star formation.

FAMILIARIZING YOURSELF WITH A *groov* RIO

Take a look at the *groov* RIO and familiarize yourself with its features shown in the diagrams on the following page. You can always come back and review these diagrams when you need to.

FAMILIARIZING YOURSELF WITH A groov RIO

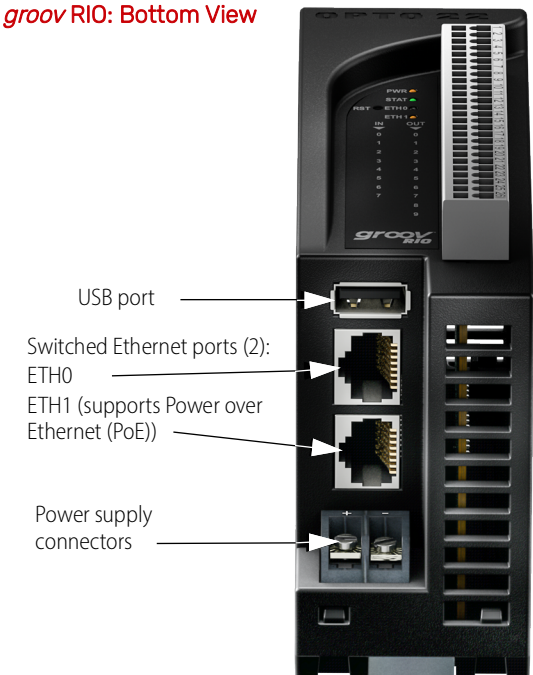
groov RIO: Front View



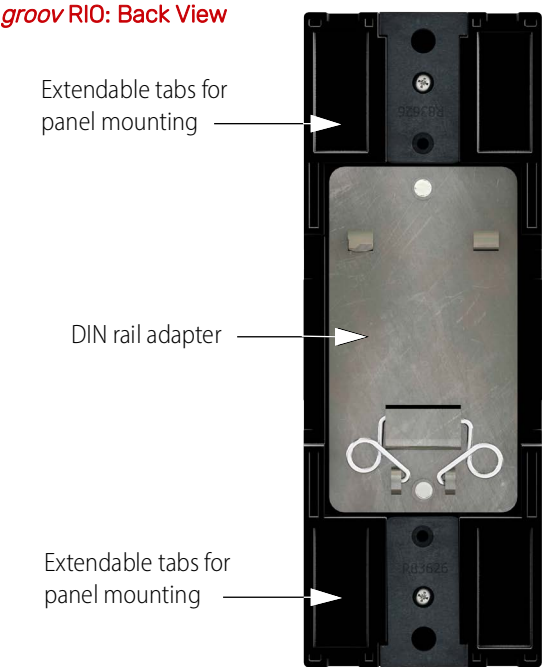
LEDs

LED	Indicates															
PWR	The status of power. • Solid green—<i>groov</i> RIO is powered on. • Solid red—<i>groov</i> RIO is restarting.															
STAT	Indicates whether <i>groov</i> RIO is running or resetting. • Solid green—<i>groov</i> RIO is running normally. • Blinking green—<i>groov</i> RIO is starting (power on) or restarting (initiated by Reset button). • Blinking between green and red—<i>groov</i> RIO is resetting to factory defaults.															
ETH0, ETH1	Network connection speed and whether there is any transmission activity: <table><tr><th>Color</th><th>Connection Speed</th><th>Transmission Activity</th></tr><tr><td>Solid green</td><td>1 Gbps</td><td>No</td></tr><tr><td>Blinking green</td><td>1 Gbps</td><td>Yes</td></tr><tr><td>Solid orange</td><td>10 or 100 Mbps</td><td>No</td></tr><tr><td>Blinking orange</td><td>10 or 100 Mbps</td><td>Yes</td></tr></table>	Color	Connection Speed	Transmission Activity	Solid green	1 Gbps	No	Blinking green	1 Gbps	Yes	Solid orange	10 or 100 Mbps	No	Blinking orange	10 or 100 Mbps	Yes
Color	Connection Speed	Transmission Activity														
Solid green	1 Gbps	No														
Blinking green	1 Gbps	Yes														
Solid orange	10 or 100 Mbps	No														
Blinking orange	10 or 100 Mbps	Yes														

groov RIO: Bottom View



groov RIO: Back View



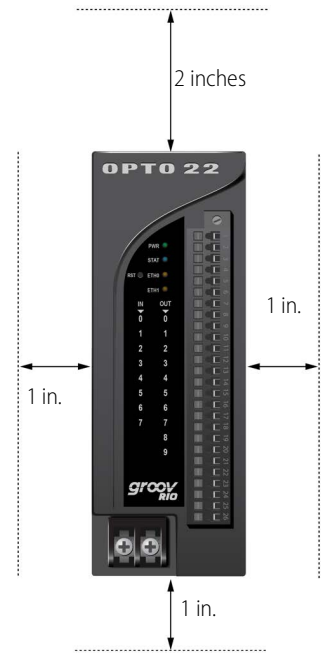
MOUNTING

You can mount *groov* RIO modules onto DIN rail or onto a panel.

Choosing a Location

Initial set up (as described in “3: Initializing a *groov* RIO UIO”) of a *groov* RIO requires a wired Ethernet connection. After the initial setup, the module can remain connected by Ethernet cable or you can switch to a wireless connection through a USB WiFi adapter (review “[Installing an Approved USB WiFi Adapter](#)” on page 93). Final placement of the *groov* RIO should be in a location that complies with the following guidelines:

- Locate a suitable wall or panel near the electrical panel or equipment you are monitoring and near a source of DC power capable of supplying power as indicated in the Power Supply specification (see “[A: Specifications](#)” on page 167).
- Make sure that there is a minimum of 2 inches clearance on the top, and 1 inch clearance on the bottom, on each side, and in front of the module after it is mounted. Also allow enough room around the module for power and field wiring through the bottom and in front of the module.
- Mount the module as shown in the diagram: with the Opto 22 logo at the top.
- Make sure you can see the MAC and hostname label on the side of the module.



Complying with these guidelines ensures that the *groov* RIO performs as described in the specifications.

Mounting on DIN Rail

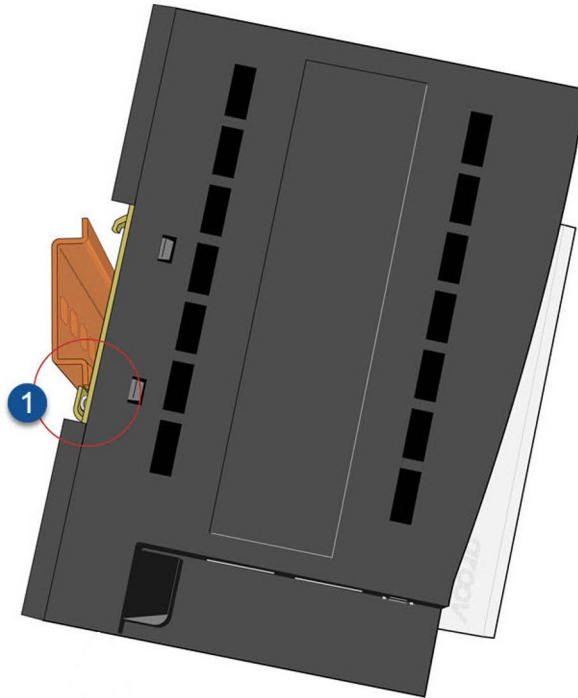
Before mounting your *groov* RIO:

- Ensure that the vents around the module are not obstructed.
- Ensure that the mounting location meets the clearances described above.

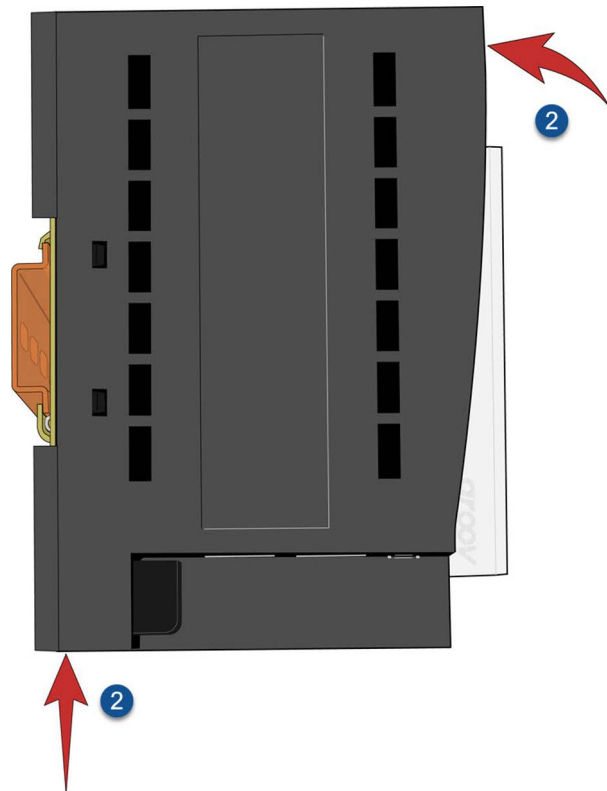
The module is built with a DIN rail adapter for use on 35 mm DIN rail. No additional assembly is required.

MOUNTING

1. Hold your module so that the Opto 22 logo is at the top and at an angle such that the top of the DIN rail adapter is away from the DIN rail and the bottom of the DIN rail adapter can slide behind the bottom lip of the DIN rail. See the circled area in the image below.



2. Push the bottom part of the module upward, making sure that you feel the clip catch on to the rail, and simultaneously push the top half of the module toward the DIN rail until the top of the DIN rail adapter engages the top lip of the DIN rail.



Before you release the module, verify that the top and bottom of the DIN rail adapters have engaged the DIN rail.

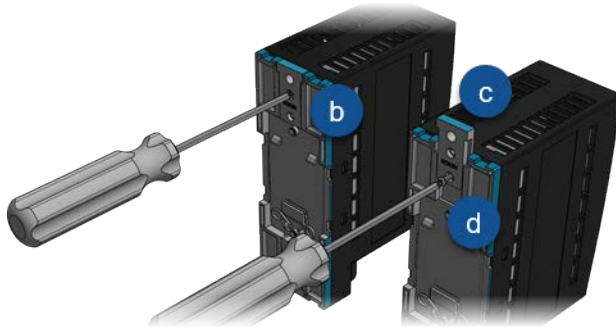
Mounting on a Panel

Before mounting your *groov* RIO on a panel:

- Ensure that the vents around the module are not obstructed.
- Review the clearances requirements described in [“Choosing a Location” on page 9](#).

After checking these items, you can attach the module to a panel:

1. Extend and secure the tabs to expose the mounting holes on each tab:
 - a. Turn the module so you can see the backside.



- b. With a small Phillips screwdriver, remove the tab-locking screw on one tab.
 - c. Slide the tab out so the middle hole on the tab aligns with the screw hole on the module.
 - d. Reinsert the tab-locking screw to the torque indicated for the panel mount tab screw in the specifications table on .
 - e. Repeat steps b through d with the other tab.
2. Use the module as a template to mark where the holes should be drilled and tapped on the panel and verify placement before attaching the module.
 3. Attach the module to the panel with screws (not provided):
 - a. Tighten a screw into one tab *close* to the torque indicated for the panel mount tab screw in the specifications table on .
 - b. Tighten another screw into the second tab *up* to the torque indicated for the panel mount tab screw.
 - c. Return to the first screw and re-tighten the screw up to the torque indicated.

WIRING FIELD DEVICES

Because you can configure each channel to be an input or an output, as well as different signal types, it is very important that you determine how each channel will be configured before you start wiring field devices to the terminal connector. For important information and guidance on selecting channel configurations, see [“Selecting Functions, Signals, and Features” on page 99](#).

Understanding Spring Wire Clamps and Preparing Wires

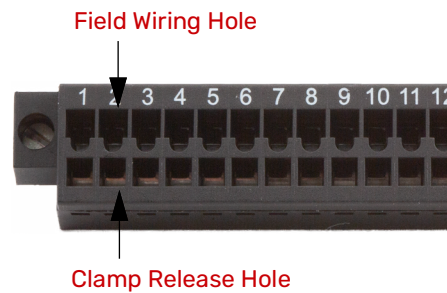
Before you begin wiring your field devices to your *groov* RIO module, make sure you select and prepare the appropriate wires and review how to use the spring clamps on terminal connectors:

Select and prepare the appropriate wire. The terminal connectors are rated for 28–14 AWG wire. Strip the wire according to the Wire Strip Length listed in the Specifications table on . If you're using stranded wire, twist or tin the strands or add ferrules to make it easier to insert the wire and create a stronger connection.

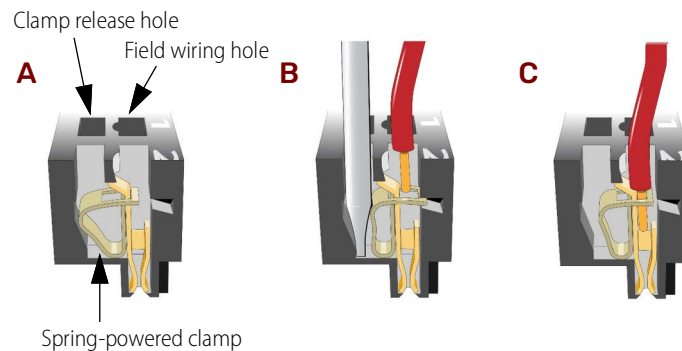
Use the right tool. To open the spring clamps, make sure to use either:

- a flathead screwdriver with a tip dimension of 2.5 mm x 0.4 mm, **or**
- the *groov* spring-clamp terminal tool, typically supplied with a . You can order a replacement spring-clamp terminal tool on our website www.opto22.com. Search for [GRV-TEX-SCTOOL](#).

Familiarize yourself with the spring clamps. On the terminal connector, each terminal number has a corresponding **clamp release hole** and **field wiring hole**.



A spring-powered clamp sits between the clamp release hole and the field wiring hole (**A**). When you push the correct screwdriver (see above for dimensions) or the *groov* spring-clamp tool straight down into the clamp release hole, the diameter of the screwdriver or tool displaces the spring laterally, which exposes the hole through which you can insert the wire (**B**). When you pull the screwdriver or spring-clamp tool straight up, the spring returns to its original position, which causes the clamp to hold the wire (**C**). You can view a [video](#) that explains how to wire your field devices and demonstrates how the spring clamp works on our website, www.opto22.com.

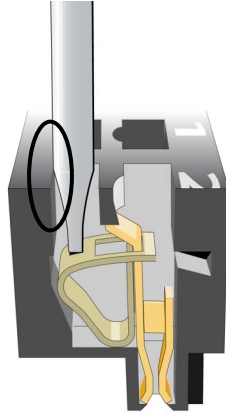


Wiring Instructions

CAUTION: For electrical safety, turn off power to *groov* RIO and de-energize field devices wired to the terminal connector before starting.

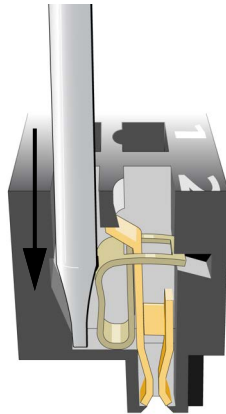
1. To make it easier to handle the screwdriver or the spring-clamp terminal tool and the field wires, secure the module or terminal connector:
 - If you are working with the terminal connector while it is attached to the module, make sure the module is screwed securely to the DIN rail or panel.

- If you are working only with the terminal connector, secure the terminal connector with a clamp.
- 2. Open the spring clamp:
 - a. Insert the screwdriver or spring-clamp terminal tool into the clamp release hole, pressing the tool against the side of the hole furthest from the terminal numbers.



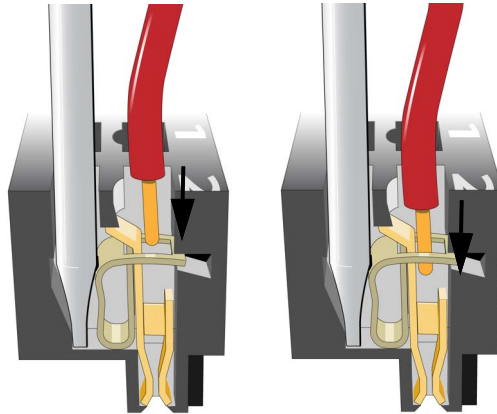
- b. Press straight down firmly until you feel the screwdriver or tool reach the bottom.

Important: Let the shape of the tool, as it is pressed straight down, open the clamp. Do not rock or wiggle the tool because it may damage the clamp.

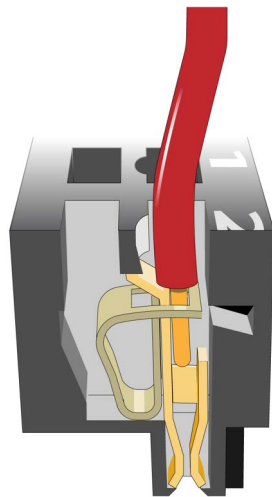


- c. You can confirm that the clamp is open by looking into the field wiring hole.
 - If the hole is dark, the clamp is open. You can go to the next step.
 - If you see a shiny surface, repeat steps a through c. **Important:** Do not rock or wiggle the tool to try to open the clamp because it may damage the clamp.

3. Insert the wire into the field wiring hole.



4. Pull out the screwdriver or spring-clamp terminal tool. The spring returns to its original position and clamps down on the wire.



5. Test that the wire is secure by gently pulling on it. If the wire pulls out, repeat steps 2 and 3.

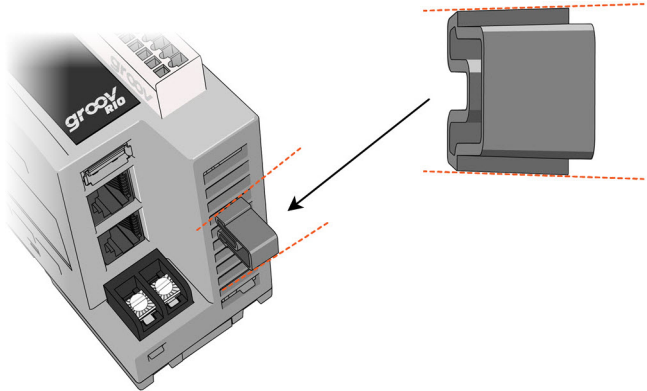
Removing Wires

1. Insert the screwdriver or spring-clamp terminal tool into the clamp release hole, pressing the tool against the side of the hole furthest from the terminal numbers.
2. Press straight down firmly until you feel the screwdriver or tool reach the bottom.
3. Pull the wire out.
4. Pull out the screwdriver or spring-clamp terminal tool. The spring returns to its original position.

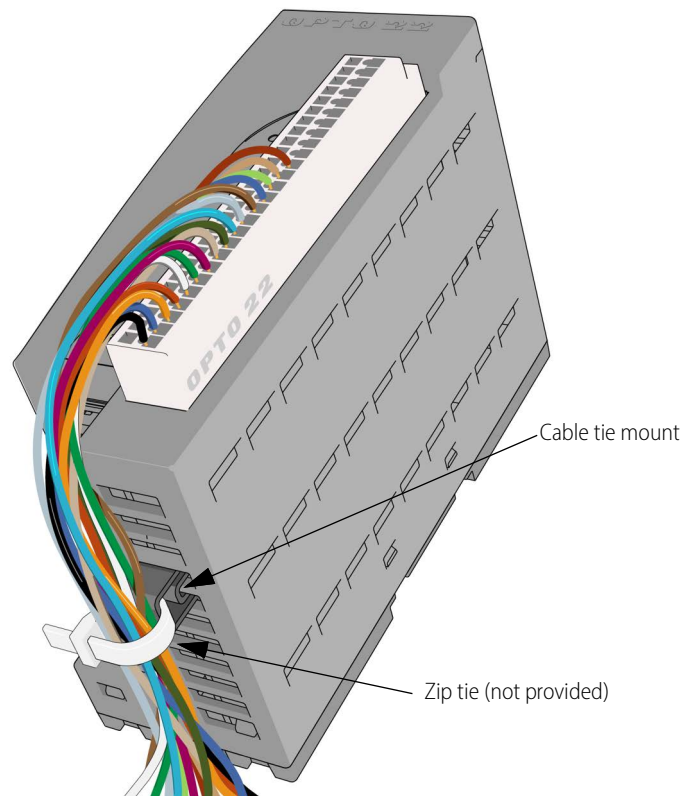
Bundling Wires with a Cable Tie Mount

Each *groov* RIO comes with two user-installable cable tie mounts. You only need to attach one mount.

1. Identify the thin side of the mount, then position it over a vent so that the thin side faces the ports and is to the right of the PCB, which is visible through the vents (see image on [page 8](#)).
2. With one hand, hold the *groov* RIO down on a sturdy surface. With the other hand, push the mount in, beginning with the thin side. Push until you hear a loud click.
3. Verify that the mount is securely inserted by gently pulling on it; it should not come out.



Thread a zip tie (not included) through the mount. Collect the wires into a bundle, wrap the zip tie around the bundle, then clip the excess zip tie.



Removing the Cable Tie Mount

If you need to remove the mount, you'll need to use needle-nose pliers. First remove the zip tie and move the wires out of the way. Then, grab the mount with the pliers and pull; you may need to twist the pliers to pull the mount out of the vent. The mount will most likely deform or break as you pull it out; the mounts are designed to be used only once.

CONNECTING POWER SUPPLY

Power over Ethernet (PoE) using an Ethernet cable connected to the ETH1 network interface.

External Power Source or Supply

Connect *groov* RIO to an external power source with a 22 to 14 AWG wire. Keep the wires as short as possible. Connect the wires as shown:



Note: If you supply power through an external power source, do not supply power through PoE.

Power Over Ethernet (PoE)

If you want to supply power through an Ethernet cable, keep the following in mind:

- Do not supply power through an external power source.
- Select an Ethernet cable that meets your application's speed and power requirements.
- Connect the Ethernet cable to the ETH1 network interface of the *groov* RIO. The ETH0 network interface does not support PoE.
- Select Power Sourcing Equipment (PSE; for example, a PoE compatible Ethernet Switch or active injector) that supports IEEE 802.3af. If you are connecting the PSE to *groov* RIO and other powered devices (PDs), make sure it has sufficient power available for *groov* RIO and all the other PDs.

Note: Some power injectors may advertise compatibility with IEEE 802.3af and operate as a passive PoE injector. These type of injectors may not work with *groov* RIO.

SELECTING AN ETHERNET NETWORK INTERFACE TO CONNECT TO A NETWORK

Even if you plan to connect your *groov* RIO to a wireless network, you must start with a wired connection to either ETH0 or ETH1. Which one you choose depends on your power supply selection:

- **DC power supply**—You can choose either ETH0 or ETH1.
- **PoE**—You must use ETH1.

3: Initializing a *groov* RIO UIO

After you connect your *groov* RIO UIO to a power supply and a network, it runs through its start-up sequence, which includes obtaining an IP address from the DNS server on the network.

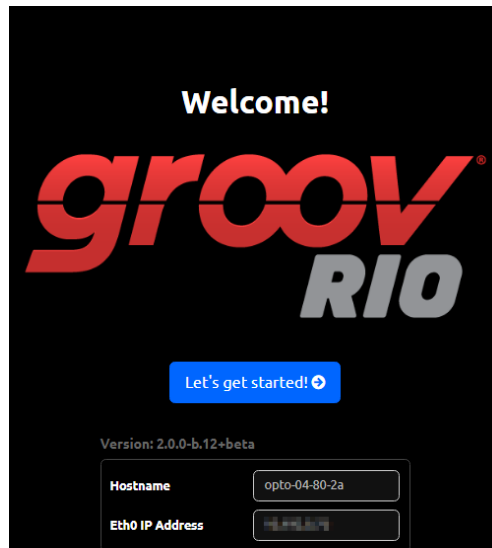
- If your network uses DNS and DHCP to assign and manage IP addresses, go to [step 1](#) (below).
- If your network does not use DNS and DHCP to assign and manage IP addresses, you will need to install and run (on a Windows machine) *groov* Find. *groov* Find is an optional utility program you can use on a Microsoft Windows computer to locate *groov* RIO modules, *groov* EPIC processors, and *groov* Boxes on your network. (If you are not familiar with *groov* Find, see [“Downloading and Running groov Find” on page 159](#).) Make note of the IP address that *groov* Find identifies for your *groov* RIO UIO and keep it for future reference. Then go to [step 3](#) (below) and use that IP address instead of the host name.

Your first tasks will be to log into *groov* Manage, create the first administrator account, determine if you need to run Quick Start, and check whether you have the latest firmware installed.

1. Wait for the STAT LED to stop blinking and show a solid green color.
2. From a computer or mobile device connected to the same network, open up a web browser.
3. In the URL bar, enter `https://<RIO default hostname>`, where `<RIO default hostname>` is the host name listed on the label on the side of unit.



The Welcome! screen appears on the browser window.

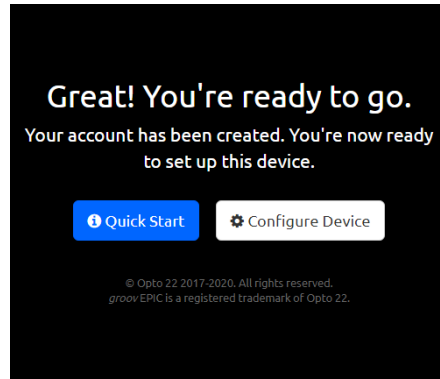


If, after a few minutes, you do not see the Welcome! screen or you get an error from the browser, check ["Browser Reports that URL to groov RIO UIO is Unreachable" on page 158.](#)

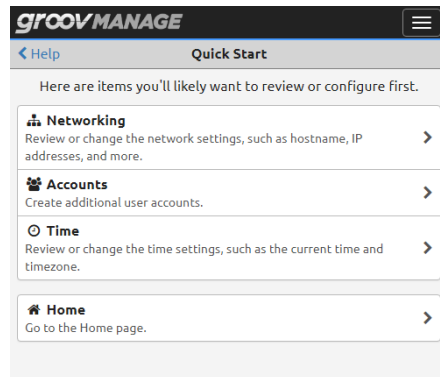
4. Click Let's get started! (). You'll see the Create an Account screen.
Read the information in the warning box. This administrator account is very important because it provides system administrator permission over the *groov* RIO, which gives you access to all the functions you need to configure it, maintain it, and create other accounts.
It's important to remember the username and password to this account. *groov* RIO does not provide a way to recover this password nor an alternate way to access this account if you forget the password. Also, Opto 22 cannot recover this password or provide access to the account.

The image shows a black screen with the title "Create an Account" in white. Below the title is the text "First, let's create your *administrator* account. Please set your credentials below." A yellow warning box contains the following text: "Warning: The account you create here is the first and only Administrator account until you add more accounts. Your account password is not recoverable. If you can no longer access this device as an Administrator you will be unable to configure the device or adjust user accounts. See documentation for more information." Below the warning box are three input fields: "Username", "Password", and "Confirm Password". At the bottom is a blue button with the text "Create Account" and a right-pointing arrow. At the very bottom, small white text reads: "© Opto 22 2017-2020. All rights reserved. groov EPIC is a registered trademark of Opto 22."

5. Type in a username and password for this administrator account, then click Create Account.
It is a good idea to follow best practices regarding passwords (for example, mixing cases and including numbers) when you create your password. Your password must be a minimum of 1 character and can be a maximum of 128 characters.
6. *groov* Manage displays a screen with these options:



- **Quick Start**—The quick start provides a list of suggested configuration steps that you should complete first to get your *groov* RIO up and running. You may want to choose this option if this is the first time you configure a *groov* RIO. If you select this option, go to the next step.
 - **Configure Device**—If you select this option, *groov* Manage displays the *groov* Manage Home page, where you can make any configuration changes. You may want to choose this option if you have configured a *groov* RIO before or you feel confident you have all the information and understand the technology and software installed on the *groov* RIO to complete any configuration steps. If you select this option, skip to [step 8](#).
7. Click Quick Start. *groov* Manage displays the Quick Start page.



The boxes are organized to suggest an order in which to complete the configuration. However, you do not have to follow this order nor do a configuration task for every box. Here's why you might want to complete each step:

- **Networking**—You might want to configure or change networking settings because you want to change the IP address or hostname that was assigned to the unit. You might want to set the IP address manually (which would make it a static IP address) or disable a network interface.
- **Accounts**—You might want to create additional accounts as required by the design of your application.

- **Time**—You can choose between manually setting the date and time, selecting a time zone from a list, or selecting a time server that will synchronize your *groov* RIO UIO's date and time with that time server's date and time.

After you finish each configuration task, click back to return to the Quick Start page.

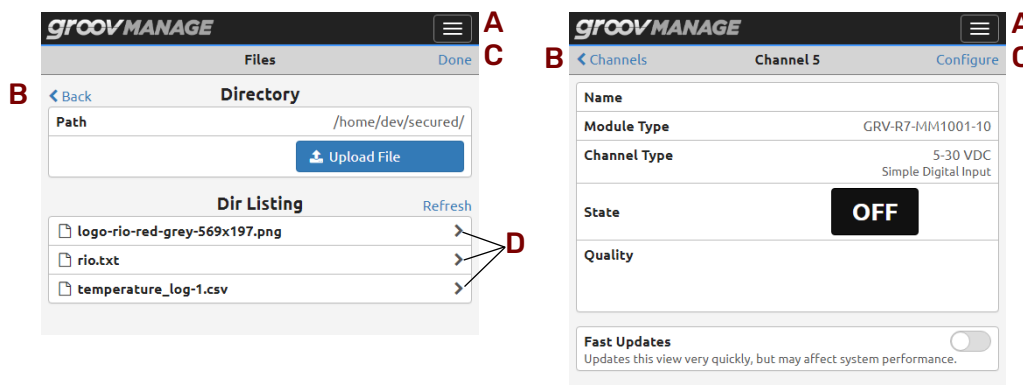
8. In *groov* Manage, click the menu button () , then select Info and Help.
9. In the Info and Help page, click About.
10. In the *groov* RIO section, note the version in the System Version field.
11. Log on to opto22.com and enter the part number for your *groov* RIO in the Search box. Select the search result that includes "Firmware" as part of the title; for example GRV-R7-MM1001-10 Firmware.
12. Note the firmware version number listed on the page.
 - If the version number on the web page is the same as the version number you noted in [step 10](#), you have the latest version of firmware installed on your *groov* RIO. You can continue on to selecting the functions, signal types, and features for each channel and configuring *groov* RIO.
 - If the version number on the web page is higher than the version number you noted in [step 10](#), you should update the firmware on your *groov* RIO UIO. Follow the instructions in "[Updating Firmware on a groov RIO](#)" on [page 154](#). After you update the firmware, you can continue on to selecting the functions, signal types, and features for each channel and configuring *groov* RIO.

4: Navigating *groov* Manage

When you connect to your *groov* RIO through a web browser, you see *groov* Manage—the “central command” interface to your *groov* RIO module—which helps you configure, troubleshoot, and commission your module, network interfaces, and data communications. You can navigate through *groov* Manage in much the same way you navigate through any other web application. You can click on navigation aides like the navigation bar or links, and scroll up and down through long pages.

UNDERSTANDING THE PAGE NAVIGATION AIDS

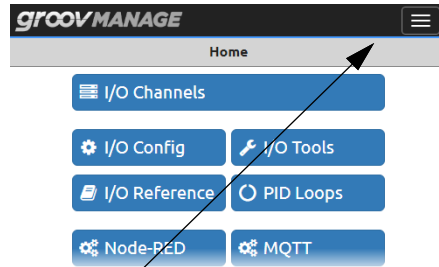
The diagram below identifies some of the important page navigation aids:



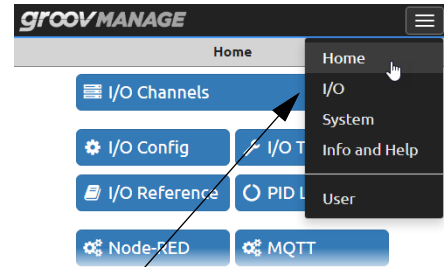
- A Menu button (☰).** Click or tap on this button to access a list of important pages. This button can help you quickly jump to these pages.
- B Back, Cancel, or previous page.** The upper-left area of the page provides a way to cancel any changes you might have made to fields on the current page, return to the previous page, or both.
- C Save, Configure, or Done.** If there are settings on the page that you can change, the upper-right area of the page displays the word Configure. Click on Configure to open up the page where you actually make the changes.
If this area shows the word Save, you must click on it to save any changes you made to settings on the page. If, after saving, the module must restart an application or service, it displays a message to let you know.
If this area is blank, that means you can't make any changes to this page.
- D Links.** When you see these arrows, it indicates that clicking or tapping on the arrow will open another page that displays more information and provides functions related to the item. For example, when you click Project Management in the Node-RED page, *groov* Manage displays another page with information and functions to help you manage a Node-RED project.

LEARNING HOW INFORMATION IS ORGANIZED IN *groov* MANAGE

At the top of the *groov* Manage page is a navigation bar that always remains visible as you navigate through the pages:



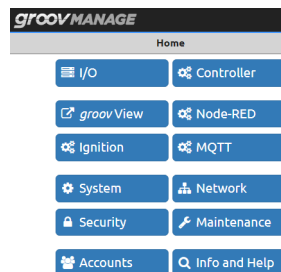
Navigation bar with the menu closed.



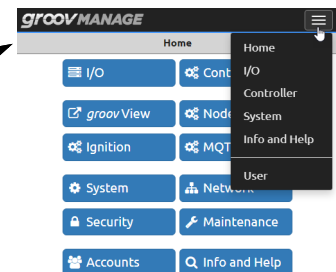
Navigation bar with the menu open.

This navigation bar contains a menu button (☰) that gives you quick access to the most frequently visited pages of *groov* Manage:

- **Home**—The main page of *groov* Manage.



Navigation bar, with the menu button closed.



Navigation bar, with the menu button open.

- **I/O**—The page that displays a visual representation of the channels on *groov* RIO.
- **System**—The page that displays functions to help you configure system-level settings, like network settings, time zone settings, file management, and the ability to restart *groov* RIO.
- **Info and Help**—The page that gives you access to more information about *groov* RIO, like log files, I/O reference information, on-board documentation, firmware versions, and access to the Quick Start page.
- **User**—The page that displays the user name of the current user and the fields to change the current user's password.

NAVIGATING THROUGH *groov* MANAGE ON A COMPUTER OR MOBILE DEVICE

You can navigate through *groov* Manage on a computer or mobile device in much the same way you navigate through any other web application. You can **Drag-and-drop**—a feature commonly used on a computer to visually and easily move files from one location to another. You can drag-and-drop files into *groov* RIO UIO on any *groov* Manage page with an upload button.

FINDING INFORMATION ABOUT I/O CHANNELS

To view information about and make changes to channels, you access the I/O Channels page of *groov* Manage. To reach that page, log into your *groov* RIO with a user ID that has administrator privileges and then do any of the following:

- Click or tap on the menu button (☰), then select I/O.
- On the Home page, click or tap I/O Channels.

Either action displays the I/O Channels page. The page displays a table where each row is a channel.

Channel	Function	Signal Type	Value
0	DI	Input_Zero	OFF
1	DO	Input_One	ON
2	AI	Temp_One	66.870 Degrees F
3	AI	Temp_Two	67.495 Degrees F
4	DI	< no name >	OFF
5	DI	< no name >	OFF

- A** The gray box shows the channel number at the top, the function and signal type on the bottom.
- B** For each channel, this area shows the channel name (if one has been assigned) at the top and a summary of the signal information on the bottom. The summary varies; it could be the state of a discrete input or output, the temperature reading from an ICTD probe, or quality indication.

5: Managing User Accounts, Certificates, and Firewall

Cybersecurity can seem like a complex topic; Opto 22 provides many resources to help you understand it better:

- For a primer on cybersecurity in an industrial automation setting and information about the features that Opto 22 provides in *groov* devices to help you with cybersecurity, review the [groov Products Cybersecurity Design and Best Practices Technical Note](#) (form 2310). This form describes some of the security features designed into *groov* products. You may want to review this technical note carefully with your IT department to determine which security features provided by *groov* RIO UIO will work best with your application and network.
- For a video series about how to implement specific aspects of cybersecurity, go to www.opto22.com and, in the **Search** box, type `video cybersecurity`.
- For blog posts that cover general aspects of cybersecurity in an industrial automation setting, go to www.opto22.com and click **Community > Opto Blog**. In the **Search** box, type `cybersecurity`.

The topics covered in these resources address many aspects of security. While planning and designing for security, remember to consider other best practices: for example, requiring that authorized users change their passwords every three months or securing the control equipment in a locked cabinet with keys accessible to a limited number of personnel.

This chapter describes how to implement security measures in the following three areas:

- Accounts
- Security certificates
- Firewalls

MANAGING USER ACCOUNTS

User accounts can be managed locally or through an LDAP (Lightweight Directory Access Protocol) server:

- **Locally**—You create, manage, and store them on the *groov* RIO UIO.
- **LDAP server**—You configure your *groov* RIO UIO to connect to an LDAP server and authenticate a user, which then determines the user's permission with permission information stored on the *groov* RIO UIO.

Both of these methods have the following in common:

- They require a local system administrator account. Typically, you would use the account you created when you initialized your *groov* RIO UIO (see).
- You need to understand *permissions* (the ability to access some services and features in *groov* RIO UIO) and determine which permissions you will grant each user, users, or (in the case of an LDAP server) groups of users. To learn more about permissions, see [“Understanding Permissions”](#).

Understanding Permissions

When you create user accounts, you have specific ideas in mind about which people or software needs access to the services and information on your *groov* RIO UIO. Managing these people and software is key to maintaining security. Here are some examples:

- **People**—You may want a line operator to monitor and control equipment on the line while a supervisor can see widget production but has no control over the equipment. Or, you may want a central station to monitor equipment at remote sites and field technicians to control it from a tablet.
- **Software**—It's not just people who may need access to information on your *groov* RIO UIO. You may also want software applications to access data. For example:
 - A company database could subscribe to data from remote equipment to write daily reports for managers to see on their phones.
 - A custom application you've written in C++, .NET, JavaScript®, or another programming language could share operational data from remote automation equipment, which then appears to technicians on their tablets.
 - A cloud data service like Amazon Web Services® (AWS) could provide data on trucks and freight containers to logistics personnel.
 - A Node-RED flow could tweet status to operators when pressure is unusually low.

These examples illustrate the importance of carefully matching up the services and information available on your *groov* RIO UIO to the correct user account.

Review the following information to determine which permission to give a user and at what level (for those permissions that offer various levels):

- **System-wide Administrator**—can do the following:
 - Create and manage other local user accounts. This includes:
 - Changing the passwords of other users, including other system-wide administrators.
 - Logging out a specific user or all users currently logged into *groov* RIO UIO.
 - Modifying the permissions of other users including other system-wide administrators, and for systems set up to manage user access through LDAP servers, changing the mapping of permissions.
 - Note: A system-wide administrator cannot change their own permissions.*
 - Manage the session expiration for each user, as well as the global session expiration.
 - Access all applications and services running on *groov* RIO UIO.
 - Change settings that affect the overall operation of *groov* RIO UIO, for example:
 - Network settings
 - I/O configuration
 - Time and date services (like time zones)
 - Security settings
 - Has **Editor** permission to *groov* View (see below).
 - Has **Editor** permission to Node-RED (see below).
 - Has **Read-Write** permission to the PAC Control REST APIs (see below).
- **groov Manage**—*groov* Manage is a system-wide administrator permission.
- **Node-RED**—There are several levels of access to Node-RED:
 - **Editor**—User can open the Node-RED editor to build and manage Node-RED flows.
 - **Dashboard UI**—User can interact with a Node-RED flow built with Node-RED dashboard UI nodes. This permission would be suitable for Operators or Kiosk users.
 - **None**—Cannot access Node-RED. This is the default.
- **Data Service OPC UA Server**—The Data Services OPC UA server provides OPC UA clients access to the local I/O. Select one of the following permissions:

- **Read-Write**
- **Read-Only**
- **None** (default)

Managing Accounts Through LDAP

If your site manages user accounts through a Lightweight Directory Access Protocol (LDAP) service, you can configure your *groov* RIO UIO to connect to the LDAP server, authenticate a user, and then determine the user's permissions.

Before you begin: Verify that you have access to a user account with system administrator permissions on your *groov* RIO UIO. Typically, the account you created when you initialized your *groov* RIO UIO has these permissions (review [Chapter 3: Initializing a groov RIO UIO](#)).

Note: *This account gives you direct, local access to your groov RIO UIO and is **not** managed by your LDAP service.*

Work with your LDAP administrator as you do the following:

1. Identify which users (or groups of users) require access and for what reasons; for example, you may not want to give an operator controlling a line with a *groov* View app the same permissions as a system administrator that maintains your *groov* RIO UIO. To learn more about permissions and how *groov* Manage assigns them to a user, review ["Understanding How LDAP and groov Manage Authenticate Users and Assign Permissions" on page 28](#).
2. In your LDAP database, create any users and groups you identified in [step 1](#).
When you create a group, make a note of the fully-qualified distinguished name of the group because you need this information in a later step.
3. Collect the following information about your LDAP server and LDAP database:
 - The ID and password of the manager account, which is the account that typically routes authentication requests from LDAP clients to the LDAP server.
 - Connection information like server hostname and password as well as security and encryption requirements.

You can find the list of specific information to collect in ["Information Required to Configure Communication to an LDAP Server" on page 29](#).

- The absolute and relative distinguished names (DNs) of objects that, when concatenated, identify where LDAP stores user and group information in the database.
- Group names, which can be stored in an LDAP database as either the name of an attribute on a user object or group objects.
- Objects that should be ignored (filtered out of searches).

You can find the list of specific information to collect in ["Information Required to Authenticate Users Through LDAP" on page 30](#).

4. Determine the *default* local permissions to grant to **any** authenticated user. If you are creating groups, determine the permissions to grant to each group.
5. Configure the default permissions in *groov* Manage as described in ["Configuring Default Permissions" on page 31](#).

6. If you created groups, create permission maps in *groov* Manage as described in [“Creating Permission Maps” on page 32](#).
7. Configure your *groov* RIO UIO to connect to your LDAP server and correctly request the authentication of a user as described in [“Configuring LDAP Server Communication and User Authentication” on page 33](#).
8. If your LDAP server requires TLS or LDAPS encryption, update the security certificates as described in [“Updating SSL/TLS Certificates” on page 36](#).
9. Restart the LDAP client and test the connection as described in [“Restart LDAP Client and Test Connection” on page 39](#).

Understanding How LDAP and *groov* Manage Authenticate Users and Assign Permissions

When a user logs into *groov* Manage, *groov* Manage sends a request to the LDAP server to authenticate the user. After the LDAP server authenticates the user, *groov* Manage determines which services the user can access by reviewing the default permissions and permission maps:

- **Default permissions**—Permissions granted to **any** authenticated LDAP user. You only need to specify default permissions if:
 - you have a small set of users and no user groups.
 - you want to grant all users the same permissions, and you only have to change permissions for a couple of users or occasionally change permissions.

When you manage permissions this way, you are managing permissions *locally* on the *groov* RIO UIO.

Important: *Carefully consider what access you grant for default permissions. Remember that **any** authenticated LDAP user is granted default permissions. If security and safety are a concern, it is good practice to specify either:*

- *no permissions, or*
- *a minimal set of permissions to some services, and no System Administrator permission.*

For a list of services and their permissions, see [“Understanding Permissions” on page 26](#).

- **Permission maps**—A way to indicate which set of permissions to grant to a user belonging to a specific group. In *groov* Manage, you can map an LDAP group to a set of permissions. After authenticating a user and assigning the user the default permissions, *groov* Manage checks through its list of groups to determine if the user is a member of any of those groups. If so, it grants the user the same permissions that are granted to that group. If your application requires more complex user management (for example, you want to manage groups of users and each group requires a different set of permissions), then you want to work with permission maps.

Resolving multiple permission levels. What if a user is a member of a group that is granted a permission level that is either lower or higher than the default permissions? Or, what if the user is a member of multiple groups? *groov* Manage always assigns the user the highest permission level that it finds. Therefore, if *groov* Manage finds that a user is in a group with a higher permission level to a service than the default permission, it assigns that higher level to the user. If *groov* Manage finds the user in multiple groups, it assigns the highest level of permission to a service that it finds in any of the groups.

For example, if you set the permission level for Node-RED to Editor in the default permissions, but a user is a member of an LDAP group granted Dashboard UI permission to Node-RED, *groov* Manage grants the user Editor permission. (Because Editor is a higher permission level than Dashboard UI.)

Changing permissions and when changes take effect. How to change a user’s permissions and when the changes take effect depends on whether you manage permissions locally or through maps.

- **Local permissions**—A *groov* RIO UIO system administrator can change the user’s permissions at any time on the *groov* RIO UIO. *groov* Manage saves these changes and they take effect the next time the user logs in.

- **Permissions mapping**—A *groov* RIO UIO system administrator or the LDAP administrator can make changes through any of the following methods:
 - In *groov* Manage, the *groov* RIO UIO system administrator updates the permissions in the group map.
 - On the LDAP server, the LDAP administrator adds or removes a user from the group in the LDAP database.
 - On the LDAP server, the LDAP administrator creates a new group in the LDAP database and adds the user to the group. Then, the *groov* RIO UIO system administrator adds a map in the LDAP Permissions page to indicate the permissions *groov* Manage should grant to members of that group.

For any of these methods, *groov* Manage enforces the changes in group membership after the time set in the **Group Update** field (see “[Configuring LDAP Server Communication and User Authentication](#)” on [page 33](#)). At that moment, any logged in LDAP user whose group membership changed would be immediately affected.

There is another option, though it is the least preferred method because **any** LDAP user currently logged in would be immediately logged out: in *groov* Manage, the *groov* RIO UIO system administrator changes the default permissions.

Information Required to Configure Communication to an LDAP Server

Server hostname and port number. The hostname and port number of the LDAP server through which it communicates with LDAP clients. The hostname must be in the format *hostname.second-level-domain.top-level-domain* (for example, myldap.example.com). The port numbers are generally:

- 389 for LDAP and LDAP over StartTLS
- 636 for LDAPS (in rare cases, this may change)

In environments with distributed, redundant, or backup LDAP servers, *groov* RIO UIO only supports querying against the primary server and it does not support referrals.

Group Update. How frequently, in minutes, *groov* Manage requests updates to its local cache of information from the LDAP server. Specify 0 to disable these updates.

TLS Mode. Determines the type of encryption:

- **Clear Text**—The LDAP communication is not encrypted. To protect sensitive information, avoid selecting this option.
- **StartTLS**—The connection is started without encryption, and then TLS encryption is added. No sensitive information is sent until TLS is added to the connection. This is the preferred setting.
- **LDAPS**—The connection is started with TLS encryption. All information is sent after TLS is added to the connection. Select this only if your site uses this (deprecated) standard.

Validate Certificates. This applies only when you select **StartTLS** or **LDAPS** as the **TLS Mode**. If you enable this option, the LDAP server checks the public key certificate in *groov* Manage to verify the identity of its LDAP client.

The following table summarizes the information to collect and options to select:

Setting	Value
Server Hostname and port number:	_____:
Group Update:	_____ minutes (0 to disable)
TLS Mode:	Select one: • Clear Text • Start TLS • LDAPS
Validate Certificate:	Yes or No; If yes, file name of certificate: _____

Information Required to Authenticate Users Through LDAP

Work with your LDAP administrator to obtain the following information:

- Typically, authentication requests are routed through a specific account on the LDAP server:
 - Manager Distinguished Name.** (Abbreviated to **Manager DN**.) The fully-qualified distinguished name of the manager account, which queries the LDAP server for user and groups information.
 - Manager Password.** The password for the manager account (**Manager DN**).
- groov* Manage sends the following information to the LDAP server, which the server then uses to compose a query to find a user:
 - Root Distinguished Name.** (Commonly abbreviated to **root DN**.) The unique key for an object in the LDAP database that serves as the root when LDAP server appends the following objects to it:
 - User Search Base** (see below)
 - Group Search Base (when **Group Mode** is set to **Group Query**; see below)

The format of root DN is a series of relative distinguished names. For example:
dc=example, dc=com
 - User Search Base.** The parent DN of all users in the LDAP database. Do not include the root DN because *groov* Manage appends the User Search Base DN to the root DN.
 - User Filter.** A list of objects that an LDAP query should include while searching through the User Search Base. Any object not matching the filter is ignored (filtered out). It must be in the form `attribute={ 0 }`. One example: for an Active Directory database, you may want to specify `sAMAccountName={ 0 }`. (`sAMAccountName` is a specialized attribute).
 - Email attribute.** The name of the attribute on a user object that contains the user's email address.
- In an LDAP database, you can indicate that a user belongs to a specific group or groups by either listing the name of the group in an attribute of the user object, or by listing the user in an attribute of a group object.
 - If your LDAP database is set up to list the name of the group in an attribute of the user object, you provide the name of that attribute in the **User Attribute** field.
 - If your LDAP database is set up to list the user in an attribute of a group object, then you need to collect the following information:
 - Group Search Base.** The relative DN that holds group objects. The LDAP server concatenates this DN to the root DN.
 - Group Filter.** A list of objects that an LDAP query should include while searching through the Group Search Base. Must be in the form `attribute=value`. Any object not matching the filter is ignored (filtered out).
 - Group Member Attribute.** The name of the attribute on a group object that lists all the users that belong to the group.

Configuring Default Permissions

1. Log into your *groov* RIO UIO with a user ID that has system administrator permission.
2. Click Accounts, then LDAP Settings. *groov* Manage displays the main LDAP page.

groovMANAGE

< Accounts **LDAP**

LDAP (Lightweight Directory Access Protocol) provides directory and authentication services over a network.

You can configure the *groov* Manage LDAP client to allow users to sign into this device with LDAP credentials.

You can manage LDAP user permissions and session expiration locally, per user, with default values applied until the user is provisioned, or you can manage LDAP user permissions and session expiration by mapping LDAP groups.

Settings >
Server information, options, user and group query settings.

Permissions and Sessions >
Default permissions, permission and session expiration assignment.

Restart Client

Test Connection

Username Required

Password Required

Test Connection

3. Click Permissions and Sessions. *groov* Manage displays the LDAP Permissions page.

groovMANAGE

< LDAP **LDAP Permissions** Save

Default Permissions

System-wide Administrator	No
Device Administrators have full access to all applications and services.	
groov Manage	None
Node-RED	None

Group Permissions

Add Permissions

4. In the Default Permissions section, select the permission level for each listed service.

Important: Carefully consider what access you grant as default permissions. Remember that **any** authenticated LDAP user is granted default permissions. If security and safety are a concern, it is good practice to specify either:

- no permissions, or

- a minimal set of permissions to some services and no System Administrator permission.

For a list of services and their permissions, see [“Understanding Permissions” on page 26](#).

5. Click Save. *groov* Manage validates the information and then saves it.
If *groov* Manage finds any invalid information, it highlights (in red) the fields with invalid information and shows a message with guidance on how to fix it. After you fix the information, click on Save.

Creating Permission Maps

1. Log into your *groov* RIO UIO with a user ID that has system administrator permission.
2. Click Accounts, then LDAP Settings. *groov* Manage displays the main LDAP page.

GROOVMANAGE

Accounts LDAP

LDAP (Lightweight Directory Access Protocol) provides directory and authentication services over a network.

You can configure the *groov* Manage LDAP client to allow users to sign into this device with LDAP credentials.

You can manage LDAP user permissions and session expiration locally, per user, with default values applied until the user is provisioned, or you can manage LDAP user permissions and session expiration by mapping LDAP groups.

Settings >
Server information, options, user and group query settings.

Permissions and Sessions >
Default permissions, permission and session expiration assignment.

Restart Client

Test Connection

Username Required

Password Required

Test Connection

3. Click Permissions and Sessions. *groov* Manage displays the LDAP Permissions page.

GROOVMANAGE

LDAP LDAP Permissions Save

Default Permissions

System-wide Administrator	No
Device Administrators have full access to all applications and services.	
groov Manage	None
Node-RED	None

Group Permissions

Add Permissions

4. Click Add Permissions in the Group Permissions section.

Group DN *Required*
The fully-qualified distinguished name of the group.

System-wide Administrator Device Administrators have full access to all applications and services.	No
groov Manage	None
Node-RED	None

Cancel Delete OK

Add Permissions

5. In the Group DN field, enter the fully-qualified distinguished name of the group, making sure it matches what LDAP would return (see [step 2 on page 27](#)).
6. For each service listed, select the permissions you want to grant to the users in this group.
7. Click OK.
8. If you want to create more groups, return to [step 4](#).
9. Click Save. *groov* Manage validates the information and then saves it.
If *groov* Manage finds any invalid information, it highlights (in red) the fields with invalid information and shows a message with guidance on how to fix it. After you fix the information, click on Save.

Configuring LDAP Server Communication and User Authentication

Before you begin, make sure you have the information described in:

- ["Information Required to Configure Communication to an LDAP Server" on page 29](#)
- ["Information Required to Authenticate Users Through LDAP" on page 30](#)

Let's get started:

1. Log into your *groov* RIO UIO with a user ID that has system-wide administrator permission.

2. Click **Accounts > LDAP Settings**. *groov* Manage displays the main LDAP page.

groovMANAGE

Accounts

LDAP

LDAP (Lightweight Directory Access Protocol) provides directory and authentication services over a network.

You can configure the *groov* Manage LDAP client to allow users to sign into this device with LDAP credentials.

You can manage LDAP user permissions and session expiration locally, per user, with default values applied until the user is provisioned, or you can manage LDAP user permissions and session expiration by mapping LDAP groups.

Settings

Server information, options, user and group query settings.

Permissions and Sessions

Default permissions, permission and session expiration assignment.

Restart Client

Test Connection

Username

Required

Password

Required

Test Connection

- Click **Settings**. *groov* Manage displays the LDAP Settings page.
- Configure the following LDAP settings:

groovMANAGE LDAP Settings Save

Server *example.com:389*
hostname:port

Root DN *dc=example,dc=com*

Options

Permissions Mode Permissions Mappings
Use LDAP for authentication only or for both authentication and authorization.

Group Update (min) 3
This is how often in minutes the local cache of LDAP groups is updated (0 disables updates).

TLS Mode Clear Text

Search Subtree ☒
Queries for users and groups will recurse more than one level.

Manager

Manager DN *cn=manager,cn=users,dc=example,dc=com*
The bind DN of the manager.

Manager Password *Required*

User Search

User Search Base *Required*

User Filter *sAMAccountName={0}*
User filters have the form attribute={0}.

Email Attribute *Optional*

Group Search

Group Mode User Attribute

User Member Of Attribute *memberOf*
The attribute on a user object which maps groups to the user.

Delete Settings

- a. Enter the **Server** and **Root DN** information you collected in “[Information Required to Configure Communication to an LDAP Server](#)” on page 29.
- b. In the **Options** section:
 - Set **Permissions Mode** to either **Local Permissions** or **Permissions Mapping**. To understand the difference, see .
 - In the **Group Update (min)** field, enter how often (in minutes) *groov* Manage should request an update of its local cache of information.
 - Click **TLS Mode** to select the type of security encryption for the connection to the LDAP server (see).

For **LDAPS** or **StartTLS**, if you enable the **Validate Certificates** switch, you can upload the TLS certificate now or later on (for instructions, see). If you want to upload it now, click on the **Upload the certificate** link. *groov* Manage opens a new tab in your browser to display the Client Certificate page. Upload the certificate, then close that browser tab to return to the LDAP Settings page, and continue with the rest of these instructions.

- In the **Search Subtree** field, enable this switch if you want the LDAP server to search through the subtrees that branch off the User Search Base or the Group Search Base.
- c. For the **Manager** and **User Search** sections, enter the information you collected in .
- d. In the **Group Search** section: if **Permissions Mode** is set to **Local Permissions**, do not specify anything for **Group Search**. If **Permissions Mode** is set to **Permissions Mapping**, click **Group Mode** to specify how group information is stored in the LDAP database.
 - Select **User Attribute** if group membership is stored as an attribute to the user object. Enter the name of the attribute in the **User Member Of Attribute** field.
 - Select **Group Query** if the group membership is stored in group objects. Enter the information you collected in in the fields.
- 5. Click **Save**. *groov* Manage validates some of the information and then saves it. If *groov* Manage finds any invalid information, it highlights the fields with invalid information in red, and shows a message with guidance on how to fix them. After you fix the information, click **Save**.

Updating SSL/TLS Certificates

If you selected TLS or LDAPS for the TLS mode, you need to make sure that the public certificate for your LDAP server is stored in the trusted store of the *groov* RIO UIO. Your LDAP administrator can provide you with a copy of this certificate. Make sure that the certificate is accessible to the computer or mobile device that you are using to connect to the *groov* RIO UIO.

1. Log into your *groov* RIO UIO with a user ID that has system administrator permission.
2. Click Accounts, then LDAP Settings. *groov* Manage displays the main LDAP page.

groovMANAGE

Accounts LDAP

LDAP (Lightweight Directory Access Protocol) provides directory and authentication services over a network.

You can configure the *groov* Manage LDAP client to allow users to sign into this device with LDAP credentials.

You can manage LDAP user permissions and session expiration locally, per user, with default values applied until the user is provisioned, or you can manage LDAP user permissions and session expiration by mapping LDAP groups.

Settings >
Server information, options, user and group query settings.

Permissions and Sessions >
Default permissions, permission and session expiration assignment.

Restart Client

Test Connection

Username Required

Password Required

Test Connection

3. Click Settings. *groov* Manage displays the LDAP Settings page.

groovMANAGE

LDAP LDAP Settings Save

Server *example.com:389*
hostname:port

Root DN *dc=example,dc=com*

Options

Permissions Mode **Permissions Mappings**
Use LDAP for authentication only or for both authentication and authorization.

Group Update (min) **3**
This is how often in minutes the local cache of LDAP groups is updated (0 disables updates).

TLS Mode **Clear Text**

Search Subtree ☒
Queries for users and groups will recurse more than one level.

Manager

Manager DN *cn=manager,cn=users,dc=example,dc=com*
The bind DN of the manager.

Manager Password *Required*

User Search

User Search Base *Required*

User Filter *sAMAccountName={0}*
User filters have the form attribute={0}.

Email Attribute *Optional*

Group Search

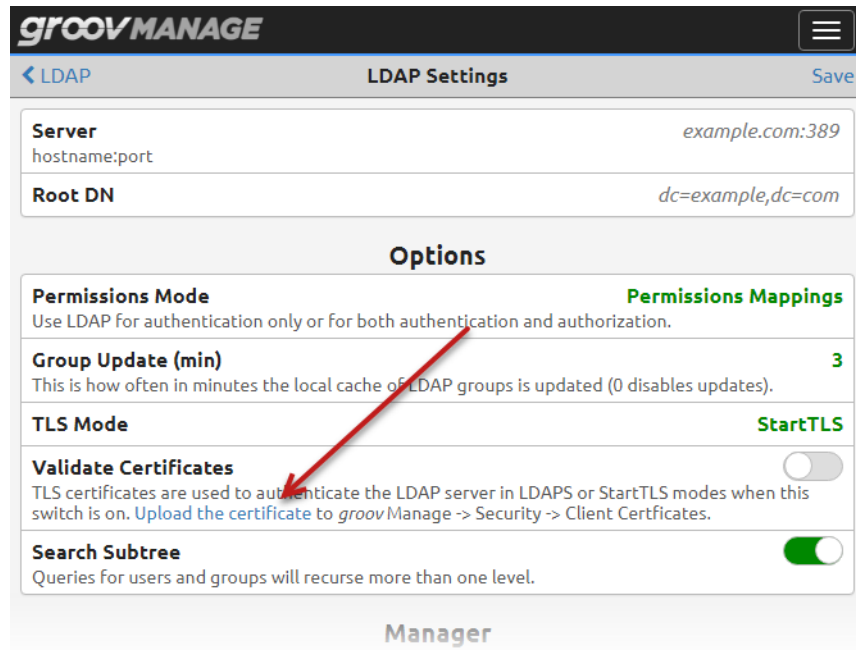
Group Mode **User Attribute**

User Member Of Attribute *memberOf*
The attribute on a user object which maps groups to the user.

Delete Settings

4. In the Options section, if TLS Mode is not set to TLS or LDAPS, click on the field and select the appropriate option. *groov* Manage displays the Validate Certificates field. Click the switch to enable this field.
5. Click Save. *groov* Manage validates the information and then saves it.
If *groov* Manage finds any invalid information, it highlights (in red) the fields with invalid information and shows a message with guidance on how to fix it. After you fix the information, click on Save.

- Click Upload the Certificate.



groovMANAGE

LDAP Settings [Save](#)

Server *example.com:389*
hostname:port

Root DN *dc=example,dc=com*

Options

Permissions Mode **Permissions Mappings**
Use LDAP for authentication only or for both authentication and authorization.

Group Update (min) **3**
This is how often in minutes the local cache of LDAP groups is updated (0 disables updates).

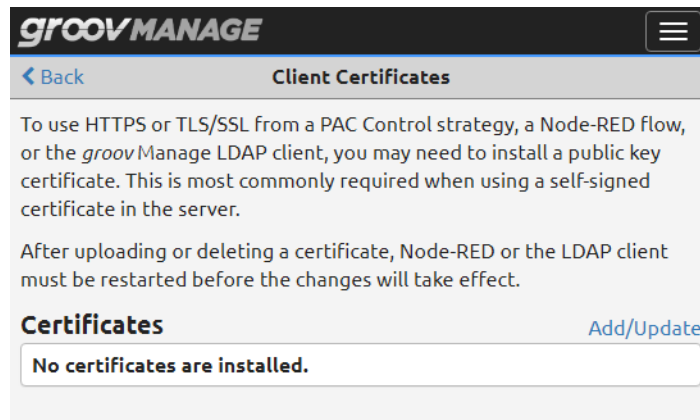
TLS Mode **StartTLS**

Validate Certificates ☐
TLS certificates are used to authenticate the LDAP server in LDAPS or StartTLS modes when this switch is on. [Upload the certificate](#) to groov Manage -> Security -> Client Certificates.

Search Subtree ☒
Queries for users and groups will recurse more than one level.

Manager

groov Manage displays the Client Certificates page.



groovMANAGE

[Back](#) **Client Certificates**

To use HTTPS or TLS/SSL from a PAC Control strategy, a Node-RED flow, or the groov Manage LDAP client, you may need to install a public key certificate. This is most commonly required when using a self-signed certificate in the server.

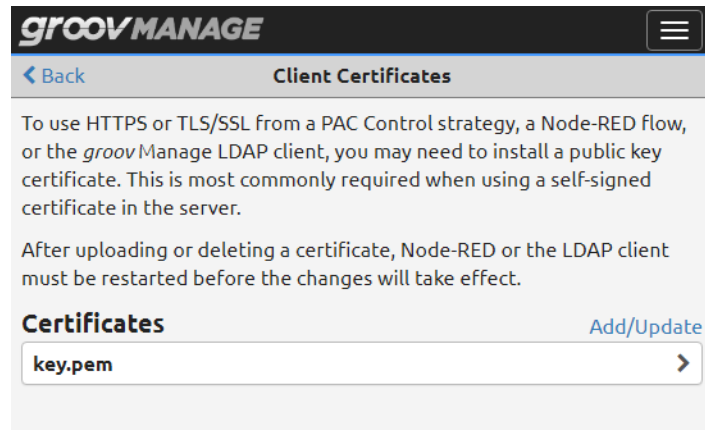
After uploading or deleting a certificate, Node-RED or the LDAP client must be restarted before the changes will take effect.

Certificates [Add/Update](#)

No certificates are installed.

- Click Add/Update.
- Navigate to the folder where you stored the LDAP server's public certificate and select the certificate file.

9. Click Open. *groov* Manage uploads the file and you'll see it listed in the Certificates section.



groovMANAGE

[< Back](#) **Client Certificates**

To use HTTPS or TLS/SSL from a PAC Control strategy, a Node-RED flow, or the *groov* Manage LDAP client, you may need to install a public key certificate. This is most commonly required when using a self-signed certificate in the server.

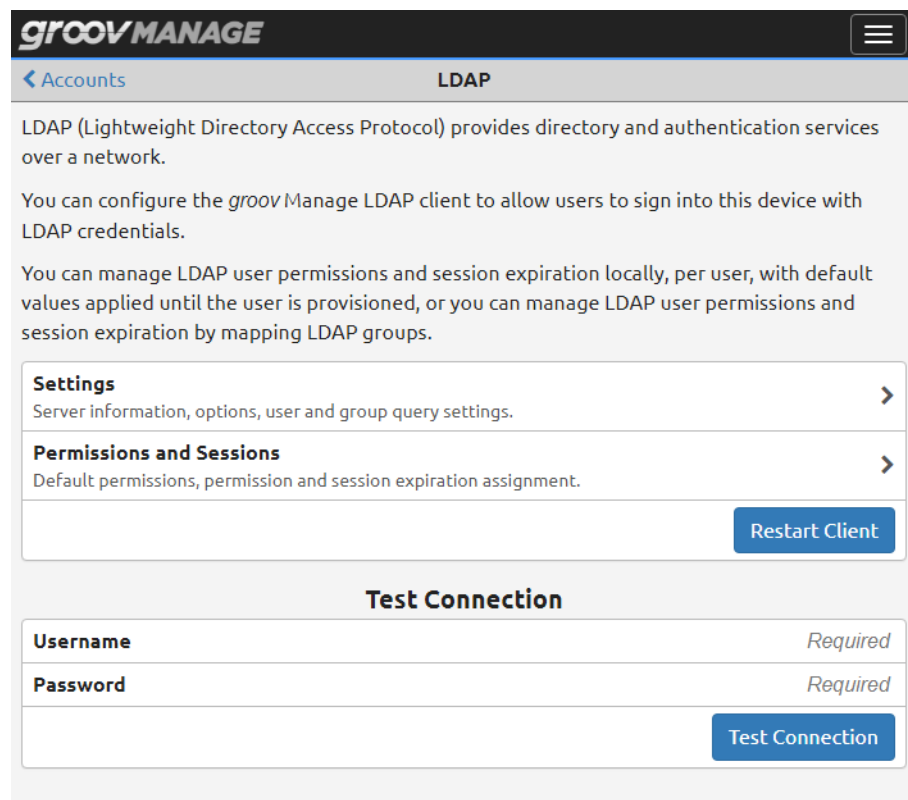
After uploading or deleting a certificate, Node-RED or the LDAP client must be restarted before the changes will take effect.

Certificates [Add/Update](#)

key.pem	>
---------	---

Restart LDAP Client and Test Connection

1. Log into your *groov* RIO UIO with a user ID that has system administrator permission.
2. Click Accounts, then LDAP Settings. *groov* Manage displays the main LDAP page.



groovMANAGE

[< Accounts](#) **LDAP**

LDAP (Lightweight Directory Access Protocol) provides directory and authentication services over a network.

You can configure the *groov* Manage LDAP client to allow users to sign into this device with LDAP credentials.

You can manage LDAP user permissions and session expiration locally, per user, with default values applied until the user is provisioned, or you can manage LDAP user permissions and session expiration by mapping LDAP groups.

Settings >
Server information, options, user and group query settings.

Permissions and Sessions >
Default permissions, permission and session expiration assignment.

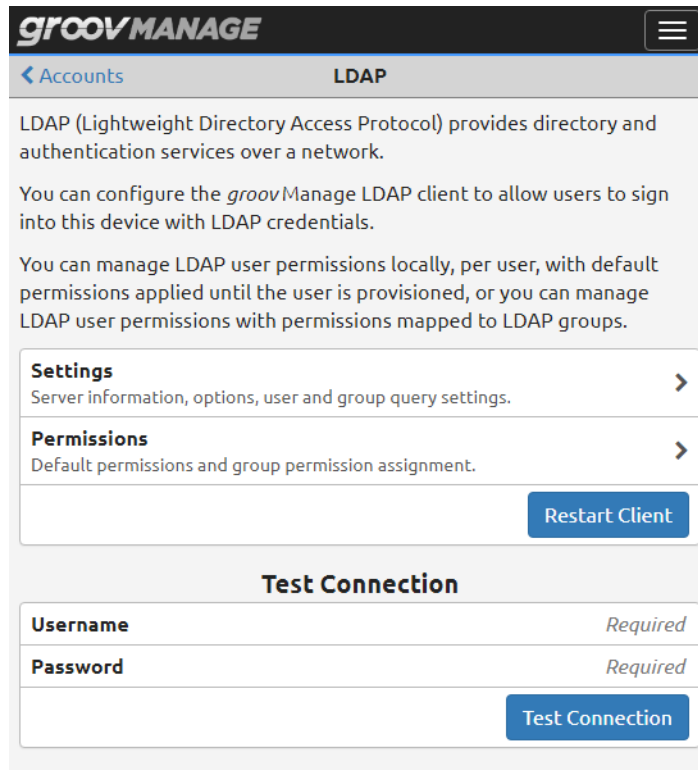
[Restart Client](#)

Test Connection

Username	Required
Password	Required

[Test Connection](#)

3. In the LDAP page, click Restart Client.



groovMANAGE

[← Accounts](#) **LDAP**

LDAP (Lightweight Directory Access Protocol) provides directory and authentication services over a network.

You can configure the *groov*Manage LDAP client to allow users to sign into this device with LDAP credentials.

You can manage LDAP user permissions locally, per user, with default permissions applied until the user is provisioned, or you can manage LDAP user permissions with permissions mapped to LDAP groups.

Settings
Server information, options, user and group query settings.

Permissions
Default permissions and group permission assignment.

Restart Client

Test Connection

Username *Required*

Password *Required*

Test Connection

4. You can test your configuration by entering the user name and password of a user in your LDAP database (in the Test Connection section), then clicking Test Connection.

Creating Local User Accounts and Configuring Their Access

With *groov* Manage, you can create user accounts and limit access to functionality, features, or even HMI. You manage these accounts (their creation, deletion, and their access to services/resources) on your *groov* RIO UIO. Before you create a user account, consider the following questions:

- How many users do you want to create?
- What functions do you want the users to access?
- How will you secure (encrypt or password-protect) the information about the users?

Creating Local User Accounts

After you consider what types of users you want to create and what they will have access to, do the following:

1. Log into your *groov* RIO with a user ID that has system administrator permission.
2. Click Accounts.
3. Click Add (in the upper right corner).
4. Type in the required information and select the permissions you want that user to have.
5. Click Save (in the upper right corner).

Repeat these steps for every user account you want to create.

MANAGING CERTIFICATES ON YOUR *groov* RIO

Like other web servers that contain sensitive data—for example, your bank—*groov* RIO uses an SSL/TLS certificate to:

- encrypt communications and,
- prove the *groov* RIO's identity to client browsers.

Just as certificates can create trustworthy connections between your bank and your browser, you can help create trustworthy connections between your *groov* RIO and client/server applications. To understand how this works, see .

For a quicker experience configuring and enabling other services, like the Data Services MQTT client or OPC UA server, first prepare and upload the security certificates.

Which *groov* RIO Applications are Clients, Which are Servers

To know whether you need to create a server certificate (then add it to clients) or add client certificates (so that your *groov* RIO can trust a server), you need to know which applications on your *groov* RIO operate as clients and which operate as servers. The following applications on your *groov* RIO can act as **servers**:

- *groov* Manage
- *groov* Manage OPC UA
- *groov* View
- Node-RED

If you want clients to create secure, encrypted connections to these server applications, you must create certificates for these servers, then install them into the client's trust store.

The following applications on your *groov* RIO can act as **clients**:

- a PAC Control strategy (only *groov* EPICs can run PAC Control strategies)
- a Node-RED flow
- the MQTT publisher (in Data Service)
- the *groov* Manage LDAP client

If you want servers to create secure, encrypted connections to these client applications, you must install the verified certificates of those servers into the *groov* RIO's trust store.

groov RIO as a Server: Creating Server Certificates

If your clients (typically browsers on computers and mobile devices that have access to your OT or IT network) need to have secure and easy access to your *groov* RIO, then install the *groov* RIO's public certificate into the trust store of those clients. A network administrator can help you because they have access to system administrator-level utilities to add certificates to the trust stores of clients. You will need to provide a custom self-signed (see [page 41](#)) or CA-verified (see [page 42](#)) server certificate created by or for your *groov* RIO to your network administrator.

How you add the certificate to the trust store of each client varies. Refer to your operating system's help for guidance on managing the trust store or root program or work with your network administrator.

Creating a Custom Self-Signed Certificate

1. Log into your *groov* RIO with a user ID that has system administrator permission.
2. Click Security > Server SSL > Create Certificate.
3. In the Create Certificate page, enter the information requested.

Server Name—Enter the fully qualified domain name or IP address of this *groov* RIO that others will use to access it. The server name may contain letters a–z (case insensitive), digits 0–9, or a hyphen (-). No other characters are allowed. The server name must not start with a hyphen.

Example:

If the URL that others will use to access the *groov* RIO is `https://process1.acme.com`, then type in `process1.acme.com`

Example:

If the URL that others will use to access the *groov* RIO is `https://mobilehmi.mydomain.com`, then type in `mobilehmi.mydomain.com`

Email—The email address of the individual in your organization requesting the certificate and who would be responsible for responding to any inquiries about this certificate.

Department—Information to differentiate between divisions within an organization. For example, “Engineering” or “IT”. If applicable, you can enter the DBA (doing business as) name in this field.

Organization—The legally registered name of your business. The listed organization must be the legal registrant of the domain name in the certificate request. If you are enrolling as a small business or sole proprietor, please enter the certificate requester’s name in this field, and the DBA (doing business as) name in the Organizational Unit field.

City or Locality—Name of the city or locality where your organization is located. Please spell out the name of the city or locality. Do not abbreviate.

State—Name of state, province, region, territory where your organization is located. Please enter the full name. Do not abbreviate.

Country Code—The two-letter International Organization for Standardization (ISO-) format country code for the country in which your organization is legally registered. See <http://www.digicert.com/ssl-certificate-country-codes.htm> for a list of codes. For example, the code for the United States is US.

Days until expiration—Enter the number of days before the certificate is expired and has to be replaced. Opto 22 recommends 3560 (10 years).

RSA key size—Enter the size of the RSA key. The default size of 2048 is a generally recommended value. Higher values will take longer to create.

4. Click Create. *groov* Manage immediately installs the new private key and certificate, and then restarts *groov* Manage.

Your *groov* RIO now has new copies of the Public Certificate, Private key, and CSR, which you can download when you need to request a CA-signed certificate.

Creating or Switching to a CA-verified Certificate

When you create or switch to a Certificate Authority (CA)-signed certificate, consider the following:

- The cost of a certificate from a certificate authority ranges from free to \$300 or more, depending on the features and company you buy them from. Please work with your IT department before you begin this task.
- You will send the CSR to the certificate authority of your choice. The certificate authority verifies the identification information and signs the CSR, which then becomes a CA-signed certificate. That’s why it is important that you enter accurate information in [step 3 of “Creating a Custom Self-Signed Certificate” on page 41](#).

If you have not created a custom self-signed certificate, do that first. See [“Creating a Custom Self-Signed Certificate” on page 41](#).

1. Log into your *groov* RIO with a user ID that has system administrator permission.
2. Click Security > Server SSL > Download CSR.
3. Navigate to a folder where you want to store the CSR file. Make a note of the file name and path to the folder. Click Save.

4. Go to the certificate authority (most likely a web site) and provide them with the information they request in whatever format they request.
When filling out a form for a CA-signed certificate, keep in mind that an SSL certificate works with any operating system. If you are asked to select an operating system, select “other” if it is an option. It’s OK to select a specific operating system, if necessary.
5. Finish the transaction with the certificate authority and receive your new SSL certificate.
6. Upload the new SSL certificate to your *groov* RIO:
 - a. Return to the View Certificate page. (See steps 1 and 2.)
 - b. Click Upload Certificate.
 - c. Click Public Certificate.
 - d. Navigate to the folder where you stored the new SSL certificate. Click Open. *groov* Manage uploads the file and then displays the Upload Certificate page.
 - e. Click Private Key.
 - f. Navigate to the folder where you stored the private key file. Click Open. *groov* Manage uploads the file and then displays the Upload Certificate page.
 - g. Click Upload (in the top right). *groov* Manage displays a message that it must restart. Click on Reload.

After *groov* Manage restarts, you can begin working with services that requires a CA-signed certificate.

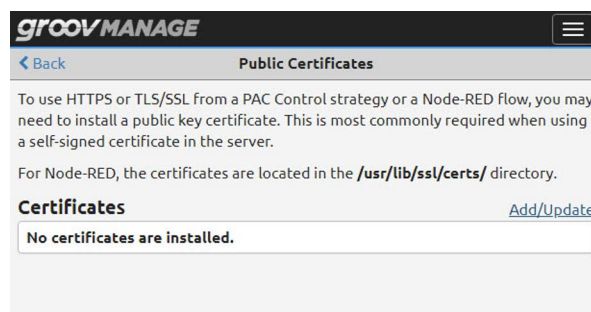
groov RIO as a Client: Adding a Server’s Certificate

There are several reasons you might need to upload a public key certificate from a server:

- To enable secure client/server communication (with HTTPS or TLS/SSL) between your *groov* RIO (acting as client) and a PAC Control strategy or a Node-RED flow (acting as a server).
- To enable secure communications to MQTT brokers.

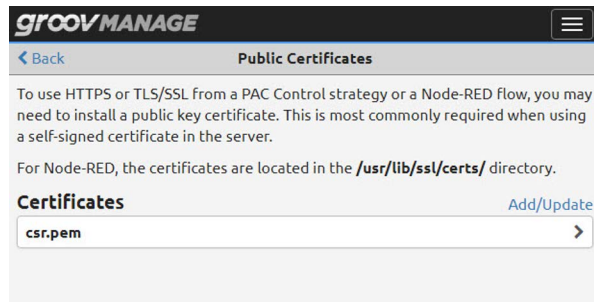
To upload a public key certificate, you must make sure that it is stored on a computer or mobile device that can connect to your *groov* RIO.

1. Log into your *groov* RIO with a user account that has system administrator permission.
2. Click Security > Client SSL.
3. In the Public Certificates window, click Add/Update.



4. Navigate to the folder where you stored the certificate and select the certificate (.pem) file.

- Click Open. *groov* Manage uploads the file and you'll see it listed in the Certificates section.



If you need to upload another certificate, repeat steps 3 through 5.

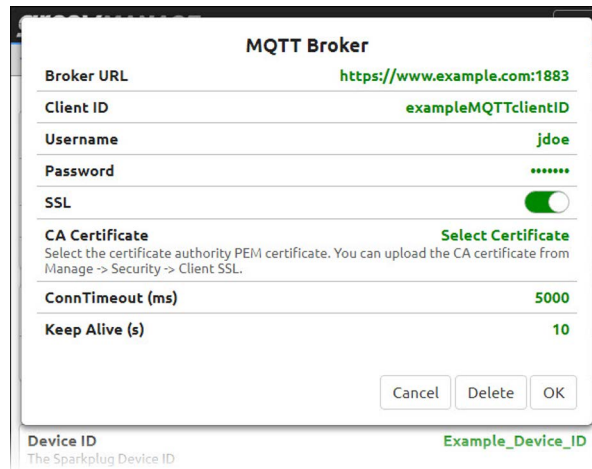
Changing SSL Security Features for Sparkplug

If you are using Sparkplug with MQTT to publish data from *groov* RIO, you must first create and install a CA-signed Certificate on the *groov* RIO.

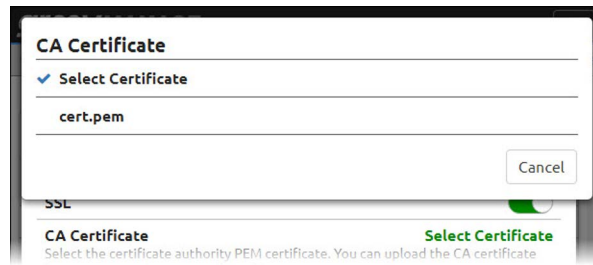
- For instructions on creating the certificate, see [“Creating or Switching to a CA-verified Certificate” on page 42](#).
- For instructions on installing the certificate on the module, see [“groov RIO as a Client: Adding a Server’s Certificate” on page 43](#).

After you installed the certificate(s):

- Log into your *groov* RIO with a user ID that has administrator privileges.
- Click MQTT > Configuration.
- For each MQTT Broker that you have listed on the MQTT page and for which you want to enable SSL:
 - Click the broker name to open its MQTT Broker settings window.
 - Click the slider so that it shows green (). *groov* Manage displays a new row below the SSL row.



- c. Click Select Certificate. *groov* Manage displays the CA Certificate window with a list of public key certificates installed on the module. Select the certificate you want.



groov Manage refreshes the MQTT Broker settings window to show the name of the certificate you chose.

- d. Click OK.
4. When you are done modifying all the MQTT Brokers that you wanted to change, click Save.

If there are any errors in any of changes you made, *groov* Manage highlights the broker with the error in red. Select that broker to view more information about the errors. Make any necessary changes and try saving again.

CONFIGURING THE FIREWALL

You might be accustomed to hearing or reading about firewalls to protect corporate networks, home networks, and even individual computers. *groov* RIO contains firewall technology to protect it from unauthorized connections and communication. The *host* firewall on your *groov* RIO can help you open and close ports on each network interface (ETH0, ETH1, WLAN0, TUN0).

Before you configure the host firewall on *groov* RIO, make sure you understand the following:

- Firewall rules and how they work. For a primer on firewalls, you may want to read [groov EPIC Security Series, Part 2: What's a Firewall?](#) on our OptoBlog.
- If you need to create a new rule, you need to know the protocol (TCP, UDP, or both) and the port number, or range of port numbers, to which this rule will apply.
- The default firewall port numbers and rules. These rules are in the firewall as part of the default factory settings. These rules are set for the most common industrial automation applications and you don't want to accidentally assign a rule to these ports because it might disrupt communications to these applications. If you don't use these applications, you should close these ports:

	ETH0 (trusted networks)	ETH1 (untrusted networks)
PAC Control	22001	443 (and 80, which redirects for 443)
CODESYS	1217, 4840, 11740	
Modbus TCP/IP	8502	
OptoMMP	2001	
Ignition Edge and Ignition Designer	8043, 8088	
<i>groov</i> View	443	

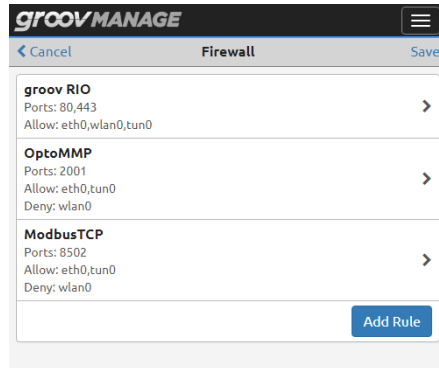
Remember that you want to connect trusted networks to the ETH0 network interface and any untrusted networks to the ETH1 network interface.

Creating a Firewall Rule

When you make changes to the *groov* RIO's firewall, the changes take effect immediately. So, make sure you schedule this change during a time that minimizes the impact to your application and users. If necessary, notify your users of this change so they can plan accordingly.

To create a new rule for the firewall:

1. Log into your *groov* RIO with a user ID that has system administrator permission.
2. Click Security.
3. Click Firewall. The Firewall page displays the rules currently in effect and may look similar to this:

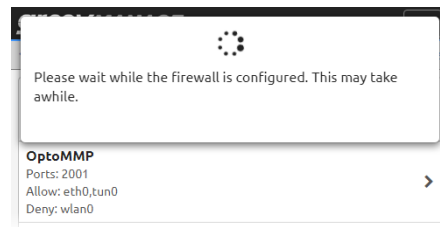


4. Click Add Rule. Type in information for the new rule:
 - **Title**—This will display as a new section title, which has limited space. A title of less than 30 character fits well in the space.
 - **Protocol**—Select which protocol this rules applies to.
 - **Port**—Type in the port number or port number range. Specify a port range by typing in the first port number in the range, followed by a colon, then the last number in the port range, with no spaces between the numbers and the colon.
 - **eth0, wlan0, or tun0**—Select which port this rule applies to by moving the slider to the right so that it shows green ().

- Click OK. If there are any errors in your selections, *groov* Manage highlights the error and displays an error message.

Fix the error or errors and then click OK.

- Repeat the previous two steps for any additional rules you want to create.
- Click Save. *groov* Manage displays a message that it is configuring the firewall.



After *groov* Manage finishes saving and implementing the changes, it displays the Security page.

Please note that adding or changing firewall rules (which effectively opens ports in the firewall) does not start the listening services that may or may not be behind those ports. If you encounter problems accessing those services, check that the services are on and listening.

Changing a Firewall Rule

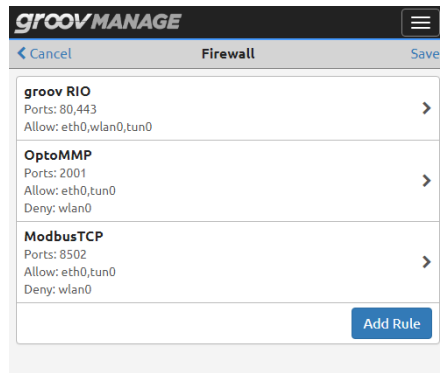
When you make changes to *groov* RIO's firewall, the changes take effect immediately. So, make sure you schedule this change during a time that minimizes the impact to your system and users. If necessary, notify your users of this change so they can plan accordingly.

To change a firewall rule:

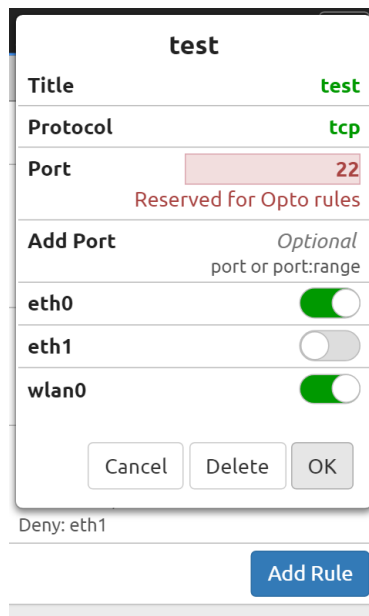
- Log into your *groov* RIO with a user ID that has system administrator permission.

CONFIGURING THE FIREWALL

2. Click Security > Firewall. The Firewall page displays the rules currently in effect and may look similar to this:



3. Click or tap on the rule you want to change.
4. Make changes.
5. Click OK. If there are any errors in your changes, *groov* Manage highlights the error and displays an error message.



Fix the error or errors and then click OK.

6. Click Save. *groov* Manage displays a message that it is configuring the firewall.



If there are any conflicts with existing rules, *groov* Manage will highlight the row with the conflict and then you can change the rule to eliminate the conflict.

After *groov* Manage finishes saving and implementing the changes, it displays the Security page.

Please note that adding or changing firewall rules (which effectively opens ports in the firewall) does not start the listening services that may or may not be behind those ports. If you encounter problems accessing those services, check that the services are on and listening.

6: Connecting to a Network or Multiple Networks

BEFORE YOU BEGIN: WHAT TO HAVE AND WHAT TO KNOW

groov RIO provides a rich set of features and functionality to connect to networks both simple and complex. For simple networks, *groov* RIO is ready to connect right out of the box. Just plug an Ethernet cable into ETH0 and let the network's DHCP server do the rest.

However, networks in industrial environments can be more complex—often involving multiple network subnets (or LANs), each with its own requirements—so organizations usually have network administrators in an IT department managing these networks. The administrators may implement network *policies*: a set of rules and guidelines for managing network traffic and workload that are applied to all equipment and users on a network. Any devices connected to the network (including your *groov* RIO) need to comply with these policies.

Opto 22 developed the [Guide to Networking *groov* Products](#) (form 2161), which provides an introduction to networking principles for users that are not familiar with networking technology and defines some basic terminology. The guide describes:

- The basics of networking that apply to many industrial environments and how to connect *groov* products to these networks.
- Network topologies to help you identify the topology of the network running at your site and how you might want to connect your *groov* products to that network.
- The different ways you can communicate to the internet from a *groov* product.

This chapter uses many of the concepts and terms introduced in that guide to explain *groov* RIO networking capabilities and how to connect it to a network. By reviewing the [Guide to Networking *groov* Products](#) and this chapter with your network administrator, you can develop a common understanding with your network administrator of the *groov* RIO capabilities and your site's network requirements to:

- make sure you connect your *groov* RIO correctly, and
- configure it properly to comply with your network policies.

If you do not have an IT department that manages your site's network, the [Guide to Networking *groov* Products](#) can help you learn how networks can operate in an industrial environment and identify areas of additional learning to determine how best to connect your *groov* RIO to your network.

Start with an Ethernet Connection

When you initialized your *groov* RIO (review [“Selecting an Ethernet Network Interface to Connect to a Network” on page 16](#)), you were required to connect to an Ethernet network through either ETH0 or ETH1. The descriptions in this chapter assume you are starting with this connection. After you complete your network configurations, if you no longer need an active network connection to either ETH0 or ETH1, you can do any of the following:

IDENTIFYING YOUR NETWORK TOPOLOGY

- Remove the Ethernet cable from ETH0 or ETH1.
- Disable ETH0 or ETH1 through *groov* Manage; review [“Disabling a Network Interface” on page 83](#).
- Leave ETH0 or ETH1 connected to a network, though you may want to enable features to protect the module; review [“5: Managing User Accounts, Certificates, and Firewall” on page 25](#).

Finding Your *groov* RIO on the Network

If tools like PAC Control or your browser can't find your *groov* RIO, Opto 22 offers a Windows-based tool called *groov* Find—available from our website—that can help you locate your *groov* RIO on the network. Download and install *groov* Find before you begin changing network settings; for instructions, review [“Downloading and Running *groov* Find” on page 159](#).

Carefully Schedule Network Changes

Changes to network settings (for example, adding a virtual private network or assigning a static IP address) require a restart of the network connections on your *groov* RIO. Changes to the Ethernet network interface mode (from switched to independent or back) requires a *reboot* of your *groov* RIO. Schedule these tasks at a time that minimizes the impact on your application and equipment.

IDENTIFYING YOUR NETWORK TOPOLOGY

Identifying your network's topology can help you identify where in your network to connect your *groov* RIO. When you've determined that, then you can identify the policies in effect on that network so you can configure your *groov* RIO to comply with those policies.

The [Guide to Networking *groov* Products](#) (form 2161) categorizes networks into two topologies:

- a single, flat network, or
- a network with multiple LANs, where each LAN may have different network settings (policies) set by a network administrator.

A Single, Flat Network

By default, a *groov* RIO is set up to work in a single, flat, wired network: you plug an Ethernet cable into ETH0 or ETH1, turn on the *groov* RIO, and a DHCP server assigns it an IP address and subnet mask, which connects it to the network. This set up is typically found in small organizations or a site with a small network and few devices. You can skip most of the instructions in this chapter and you may want to review [“Testing the Network Connections and Fine-Tuning Security” on page 84](#).

Even in a single, flat network, there are options available that can help you control and monitor more field devices without adding another LAN to your network:

- If you have several RIOs that you want to connect to your network, you can save some resources (including the expense of buying additional networking equipment) by *daisy-chaining* your RIOs. There are some important considerations to review, as described in [“Daisy-Chains” on page 55](#)
- Another option for connecting multiple RIOs is to create *rings*. Like daisy-chains, there are important considerations to review as described in [“Rings and Ethernet Redundancy” on page 56](#).

While single, flat networks usually do not require changes to default network settings, review the list of advanced network configurations in [“For Network Administrators: Tools for Managing Network Traffic to/From *groov* Devices”](#) to learn if your network requires advanced configurations that need to be made to your *groov* RIO.

Converting Your Single, Flat Ethernet Network into a Network With Two Ethernet LANs

If you determine that your single, flat Ethernet network needs to evolve into a network with multiple LANs, the networking features available on your *groov* RIO can help you support that change.

- Review [“A Network With Multiple LANs” on page 53](#) for guidance and best practices.
- The network interface on your *groov* RIO can change to *independent mode* so that you can connect a second Ethernet LAN. For more information about independent mode, review [“Changing the Ethernet Network Interface to Independent Mode” on page 65](#).

A Network With Multiple LANs

As described in [Guide to Networking *groov* Products](#) (form 2161), complex networks can contain several separate network subnets (or LANs); some can be categorized as *trusted* and others as *untrusted*. A network with multiple LANs requires careful management by a network administrator who may develop and implement policies to control various aspects (like security, workload, or performance) on each LAN; devices that connect to any of the LANs need to comply with these policies.

Trusted vs Untrusted LANs

What are the characteristics of a trusted and untrusted LAN?

- **Trusted**—Generally considered the OT (*operational technology*) LAN, it has limited to no access to the internet, very few employees in an organization can access this LAN, and the applications that have access to this LAN are restricted to those needed to operate and monitor equipment.
- **Untrusted**—Generally considered the IT (*information technology*) LAN, it provides varying degrees of access to the internet, usually all employees in an organization can access this LAN, and many of the applications and equipment that have access to this LAN are involved in running an organization’s business (like PCs, office applications, printers, etc.).

A network administrator may implement a different set of policies for each LAN to manage security (for example, setting firewall rules and user access/privileges) and performance.

Examples: Networks with Multiple LANs

Generally, there are three types of LANs: Ethernet, wireless, and virtual private networks (VPNs). Network administrators can arrange these LANs in many combinations; the following examples describe some common arrangements:

- An Ethernet network with a VPN—Small organizations in a single building typically have an Ethernet network and may install a VPN to allow authorized employees remote access to the network. This may also be the case for a large organization with several physically disparate sites where each site might have an Ethernet network for access within the site and a VPN to manage access into the site from outside.
- An Ethernet network with a wireless LAN—Both large and small organizations typically have an Ethernet network as their primary LAN and then add a wireless LAN to connect equipment that may be difficult to reach. Enabling security protocols on wireless LANs help protect assets and information.
- A network with two (or more) Ethernet LANs—Typically, the OT LAN (where all of the equipment and control applications operate) is the trusted LAN because you want restricted access to sensitive equipment. In very large sites, you may have multiple OT LANs, each encompassing a separate production line.

The IT LAN—often requiring access to the internet and managing access for all of the company employees so they can access office equipment—is the untrusted network. You may have multiple IT LANs; for example, as a courtesy, you may provide a guest LAN for visitors with restricted access to your company assets.

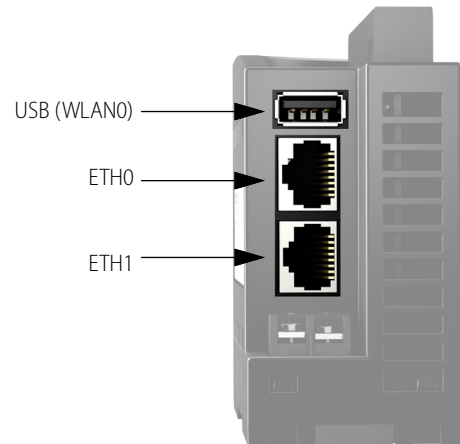
Opto 22 provides an online tool on our website that can help you understand the many ways you can connect your *groov* RIO different network topologies. To use the tool, go to our website (www.opto22.com) and click

Products > IIoT System Architecture. Click through each main story page to learn how each layer of the architecture illustrates another way to connect your *groov* RIO.

UNDERSTANDING THE NETWORK INTERFACES

A *groov* RIO provides several different network interfaces so that you can connect it to up to three or four separate LANs, and you can modify the settings of each interface to comply with each LAN's policies:

- Wired communications through either ETH0 or ETH1. These interfaces can be configured to operate in switched mode or independent mode:
 - **Switched mode**—Both interfaces share the same IP address, therefore they are on the same network. You can't connect two different LANs to these interfaces while in switched mode.
 - **Independent mode**—You can connect a different network to each interface.
- Wireless communication through an approved USB WiFi adapter connected to the USB port. For a list of approved adapters, see [“Installing an Approved USB WiFi Adapter” on page 93](#).
- A virtual private network (VPN) connected through either ETH0, ETH1 (if in independent mode), or WLAN0.



WLAN0 is physically separated from ETH0/ETH1, which means—by default—there is no communication or routing between the wired and wireless networks.

NOTE: *In very unique circumstances, you may route network traffic between two of these interfaces through a mechanism called port redirection. However, because there are risks to port redirection, make sure you review [“Port Redirection” on page 61](#) before selecting this option.*

When configured in independent mode, the network interfaces are configured to connect trusted networks to ETH0 and untrusted networks to ETH1. The remaining interfaces (WLAN0 and VPN0) are disabled. These configurations can be changed; however, if you want to take advantage of these default firewall rules, assign a trusted network to ETH0 and an untrusted network to ETH1.

Examples: Networks with Multiple LANs

Let's return to the examples we introduced on [page 53](#). Each network interface on the *groov* RIO can be connected and configured to each LAN as follows:

- A single, flat network with a wireless LAN—Configure ETH0 to connect to your local control network (trusted) and configure WLAN0 to connect to the internet (untrusted).
- A single, flat network with a VPN—Configure ETH0 to connect to a local network (trusted), configure OpenVPN® Tunnel 0 to connect to a virtual private network (trusted). The remaining interface, WLAN0, is disabled by default.
- A network with two Ethernet LANs—Configure the network interfaces to independent mode. Then, configure ETH0 to connect to a local control network (trusted) and configure ETH1 to connect to a local office network (untrusted).

Keeping LANs Separate

Network administrators create separate LANs on a network to improve security and performance, and to ease the management of the many devices connected to a LAN. They usually create these LANs by physically

separating them with networking equipment like routers. In large, complex networks with many routers, hubs, and switches, it's possible that some of the networking equipment might be connected to the same LAN. If you connect a device with two network interfaces (like a *groov* RIO in independent mode) to the same LAN, the network equipment can get confused about which network interface to use for communication, which can lead to lost data.

Before you connect a *groov* RIO to a LAN, check the following items:

- While in independent mode, do not connect the Ethernet cables that are connected to ETH0 and ETH1 to the same router, hub, or switch.
- If you connect Ethernet cables to different switches, hubs, or routers, make sure that those router, hubs, or switches are not connected to the same LAN. Check with your IT department to ensure these devices are not on the same LAN.
- Make sure that the wireless LAN is not on the same LAN as the Ethernet LAN.

While in independent mode, check that each network interface (ETH0, ETH1, and WLAN0) on the *groov* RIO is connected to a different LAN¹.

Connecting Multiple *groov* RIOs Into Daisy-Chains or Rings

The two Ethernet network interfaces on a *groov* RIO, by default, operate as a switch. This makes it possible to connect multiple *groov* RIOs through their Ethernet network interfaces to form an Ethernet communication chain. A communication chain can be in the form of a daisy-chain, or, beginning with firmware version 4.1.0, rings. Both can save on network hardware costs like additional Ethernet hubs or cabling.

Daisy-Chains

A daisy-chain can be faster to deploy and save you costs on cabling over a ring. It also does not require that the devices on the chain or even on the LAN connected to the chain deploy protocols like Rapid Spanning Tree (RSTP). However, the primary disadvantage is similar to that of a serial network: an issue with one *groov* RIO may cause a communication loss to the downstream *groov* RIOs. If you choose to daisy-chain *groov* RIOs, keep in mind the following:

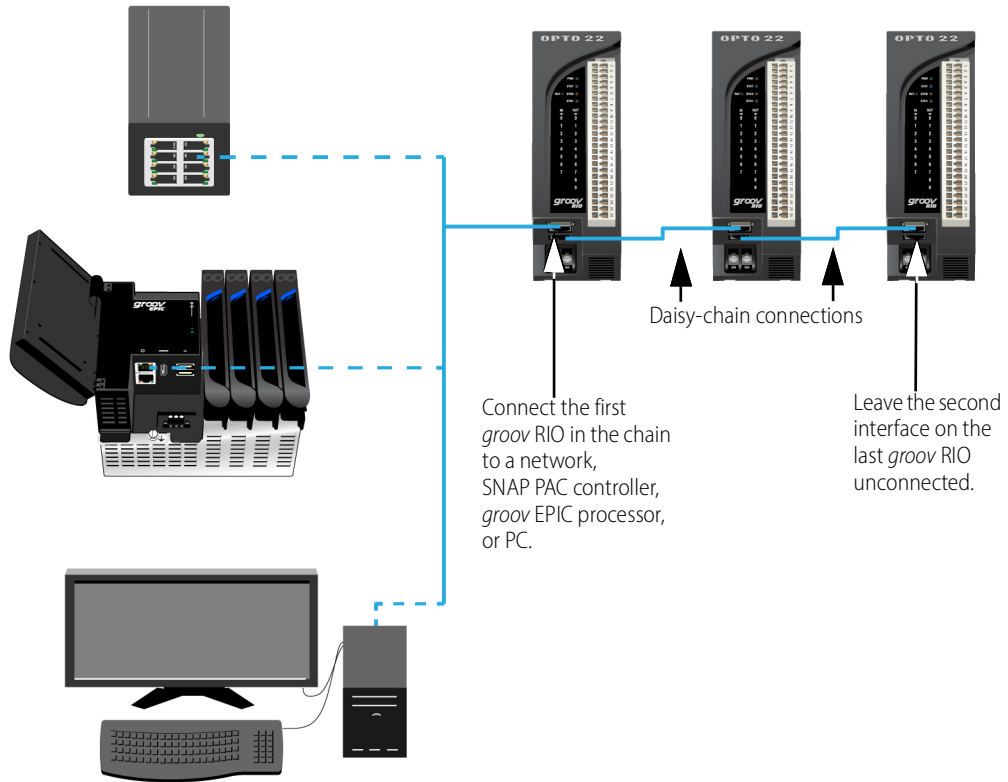
- When you update firmware on *groov* RIOs in the chain, you must update them one at a time.
- You cannot daisy-chain *groov* RIOs through WLAN0, the wireless network interface.
- As a general rule, do not connect the second interface on the last *groov* RIO in the chain to any other device. If you want to convert the daisy-chain into a ring, review [“Rings and Ethernet Redundancy” on page 56](#).
- You cannot include *groov* RIOs powered through PoE into a daisy-chain. Each RIO must be powered by an external power source or supply (review [“Connecting Power Supply” on page 16](#)).

¹ If you configure port redirection, you'll have two network interfaces connected to the same network. Make sure you understand the risks and how port redirection works before implementing it.

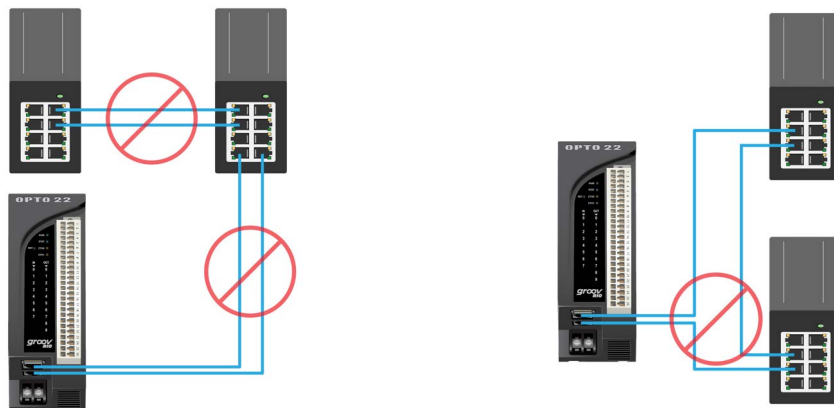
UNDERSTANDING THE NETWORK INTERFACES

The following illustrations show the correct and incorrect way to daisy-chain multiple *groov* RIOs:

DAISY-CHAIN: CORRECT ETHERNET CONNECTIONS



DAISY-CHAIN: INCORRECT ETHERNET CONNECTIONS

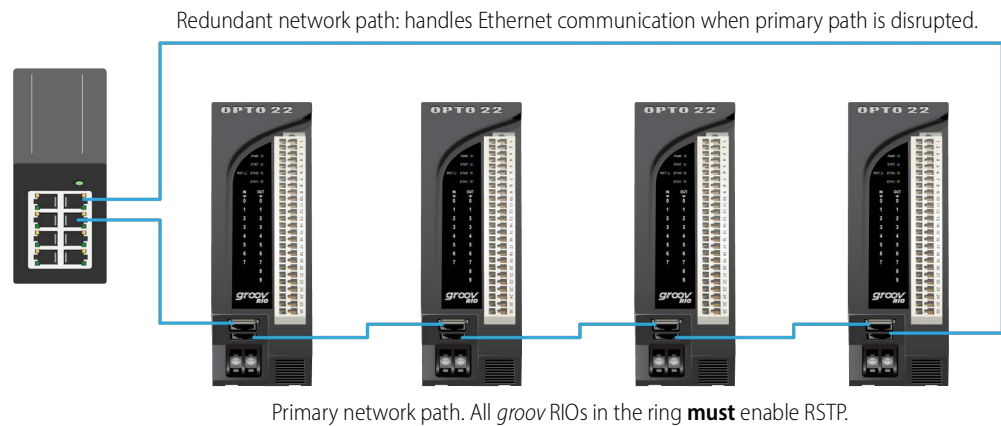


9

Rings and Ethernet Redundancy

Creating a *ring* can help overcome some of the deficiencies of daisy chains and provide *Ethernet redundancy*: if the primary Ethernet communication path fails, your application can switch to another path of Ethernet communication. To create a ring of *groov* RIOs, you need:

- More cabling than a daisy-chain to connect the available Ethernet port on the last *groov* RIO in the chain to the same hub or a hub on the same LAN.
- Deployment of a spanning tree protocol (STP) or rapid spanning tree protocol (RSTP), compliant with the IEEE 802.1w standard, on **all** the devices on the ring to prevent *broadcast storms*. (Broadcast storms are a sudden and significant increase in the network traffic when a ring is formed. The storm can—at a minimum—interrupt the operations of other devices on the LAN and at worst, bring down the entire LAN.)



The Rapid Spanning Tree Protocol (RSTP) was added in firmware version 4.1.0. (In version 4.1.0, it is enabled by default. In version 4.1.1, it is disabled by default.) If you plan on creating a ring of *groov* RIOs, RSTP **must** be enabled on every *groov* RIO in the ring, as well as any other devices on that ring.

- If the network equipment (for example, a router) has BPDU guard enabled, you must disable it on the two ports connected to the beginning and end of the ring.
- When you update firmware on *groov* RIOs in the chain, you must update them one at a time.
- You cannot ring *groov* RIOs through WLAN0, the wireless network interface.
- You cannot include *groov* RIOs powered through PoE into a ring. Each RIO must be powered by an external power source or supply (review [“Connecting Power Supply” on page 16](#)).

The benefit of a ring is that it creates another (redundant) network path to the *groov* RIOs, which helps your control application remain in constant communication with your *groov* RIOs.

WIRELESS NETWORKS

Wireless networks are useful when existing infrastructure makes it impractical or too costly to connect your *groov* RIO to an Ethernet LAN. However, keep in mind that wireless connections may not have the same performance characteristics as an Ethernet connection, so evaluate the effectiveness of a wireless connection against the needs of your control application.

*Make sure you purchased and installed a supported USB WiFi adapter (review [“Installing an Approved USB WiFi Adapter” on page 140](#)) to your *groov* RIO.*

Wireless Network Security

Your network administrators should carefully evaluate the security needs of your wireless network. *groov* RIO supports the following methods of encryption and authentication:

VIRTUAL PRIVATE NETWORKS (VPN) WITH OpenVPN

- **None**—No encryption and no authentication.
- **WEP, WPA, or WPA2**—Use either a passphrase in ASCII or a pre-shared key (PSK) in hexadecimal.
- **WPA2-Enterprise**—Uses a combination of identity, password, EAP client certificate, and WAP server certificate for the following Extensible Authentication Protocols (EAP): TLS, TTLS, and PEAP.

Each EAP method has a different set of requirements:

Method	Identity	Password	EAP Client Certificate	WAP Server Certificate
TLS	Check with network administrator ^a	Does not apply	Required	Required
TTLS				
• PAP	Required	Required	Check with network administrator ^a	Required
• CHAP	Required	Required	Check with network administrator ^a	Required
• MSCHAPv2	Required	Required	Check with network administrator ^a	Required
PEAP				
• MSCHAPv2	Required	Required	Check with network administrator ^a	Required

^aNetwork administrators may or may not implement some security features. Check with your network administrator to determine if this security feature is required to connect your *groov* RIO to the wireless network.

VIRTUAL PRIVATE NETWORKS (VPN) WITH OpenVPN

There are many resources available online to help you learn about and set up a virtual private network (VPN) with OpenVPN® technology. This section assumes you have a functioning OpenVPN server. The *groov* RIO works as an OpenVPN client that connects to the OpenVPN server. (A *groov* RIO cannot be set up as an OpenVPN server.) You need the OpenVPN server administrator to provide you with the following:

- A username and password to login to the OpenVPN server.
- If necessary, a username and password for proxy connections.
- Depending on the security and authentication configuration of the OpenVPN server, you may need some or all of these files and information:
 - A public key, also known as a certificate, which is typically available as a file that ends in `.cert`.
 - A private key that is created specifically for the *groov* RIO UIO. It is typically available as a file that ends in `.key`.
 - A Certificate Authority (CA) certificate and key, which helps verify the public and private keys. These are also typically provided in files, with the certificate file that ends in `.cert` and the key file that ends in `.key`.
 - An OpenVPN static key, if required. Not all sites implement OpenVPN static keys. This key is typically stored in a file called `static.key`.
- The following information about the OpenVPN server:
 - **Protocol**—The communications protocol used by the OpenVPN server.
 - **OpenVPN server hostname** and **port number**—The hostname is usually a fully qualified domain name (for example, *vpnserver.example.com*) or it could be an IP address.
 - **Encryption Cipher**—The encryption cipher used by the OpenVPN server.

- **LZO Compression**—If the OpenVPN server uses LZO compression, then you need to enable it on the *groov* RIO UIO.

Some of this information can be provided in a configuration file, which you can then upload into the *groov* RIO UIO. Uploading a configuration file could make configuring the *groov* RIO UIO easier and you are less likely to introduce typing errors. When you receive the configuration file, review it to make sure it has the following information (and in the format indicated), as appropriate for your OpenVPN server's security and authentication requirements:

- **Certificate Authority (CA)**—The CA section should be surrounded by `<ca>` and `</ca>` tags. Inside those tags, the certificate text should be surrounded by `<cert>` and `</cert>` tags.
- **Private and Public Key**—The key text should be surrounded by `<key>` and `</key>` tags.
- **Open VPN static key**—The key text should be surrounded by `<tls-auth>` and `</tls-auth>` tags.

If the configuration file does not contain this information, you can edit the file and add it, making sure it is surrounded by the tags described previously.

If the administrator can't provide a configuration file, collect the information and save it in a secure place. You can use the tables in [Appendix I: Network Information Tables](#) as guides for organizing this information.

CHOOSING BETWEEN AUTOMATIC AND MANUAL CONNECTIONS

As described on [page 51](#), network policies are rules applied to devices on a LAN. Some of these rules are implemented at the device level; for example, firewall rules and user privileges. *groov* Manage on your *groov* RIO helps manage firewall settings and user privileges. Other policies are enforced by networking equipment like DHCP servers, DNS servers, and routers.

Your *groov* RIO has network settings that your network administrator can change so that it complies with network policies. Knowing what network settings need to be changed determines if your *groov* RIO connects to your network automatically or manually.

Understanding the Difference Between Automatic and Manual Connections

When a device (like a *groov* RIO) joins a network, typically a DHCP server assigns the following information to the device's network settings:

- An IP address and subnet mask, which uniquely identifies the device within the network.
- The IP address and domain name of a DNS server. When the device needs to communicate to other devices in the network, the device "asks" the DNS server to help it "find" the other devices.
- The IP address of a gateway server. When the device needs to communicate to devices in other networks (including the internet), the device "asks" the gateway server to help it "find" the devices in the other networks.

Each network interface on the *groov* RIO can connect to a LAN automatically or manually. By default, all the interfaces are configured to connect automatically. However, you may need to change this setting:

When to choose automatic connections. Select this method if:

- The *groov* RIO is connecting to a single, flat network and you don't need to change any of the default network settings.
- The DHCP server can assign the IP address and subnet mask, but you or your network administrator want to override the gateway address or DNS IP address and name server that may have been assigned by the DHCP server. For more information, review "[Domain Name and DNS Server IP Address Management](#)" on [page 61](#) and "[Gateway IP Address Management](#)" on [page 62](#).

When to choose manual connections. Choose the manual method of connecting to a LAN if you need to implement any of the advanced network configurations described in [“For Network Administrators: Tools for Managing Network Traffic to/From groov Devices” on page 60](#). Work with your IT department (if available) to review the information described in each section, and collect the information required to implement any of these configurations.

The following table summarizes the similarities and differences between automatic and manual connections:

Functionality	Automatic	Manual
DHCP server can assign the IP address and subnet mask.	●	●
You want to override the gateway address.	●	●
You want to override the DNS IP address and name server that may have been assigned by the DHCP server.	●	●
You want to assign a static IP address.		●
You want to implement any of the advanced network configurations described in “For Network Administrators: Tools for Managing Network Traffic to/From groov Devices” on page 60 .		●

FOR NETWORK ADMINISTRATORS: TOOLS FOR MANAGING NETWORK TRAFFIC TO/FROM groov DEVICES

If you maintain a complex network, *groov* RIO provides network settings to support some performance, security, and efficiency policies. These settings require knowledge of advanced networking concepts and practices:

- [Static IP Address](#)
- [Port Redirection](#)
- [Domain Name and DNS Server IP Address Management](#)
- [Gateway IP Address Management](#)
- [Static Routes](#)

Most of the settings are available on all the network interfaces (ETH0/ETH1, WLAN0, and TUN0).

Examples of Advanced Network Configurations

Network administrators implement advanced network configurations to improve stability and performance of the network, or to ease management of the many devices on a network:

- **Example 1**—In network environment where network administrators organizes devices on a network for ease of management, the administrator may want to assign the *groov* RIO a specific IP address and subnet mask.
- **Example 2**—In a network environment that has multiple DNS servers, a network administrator may want to assign a specific DNS server IP address and domain name to the *groov* RIO. Or, the administrator may want to assign multiple DNS servers to the *groov* RIO and assign the order in which to query each server.
- **Example 3**—In a network environment that has multiple gateways, a network administrator may want to assign a specific gateway to the *groov* RIO and assign the order in which that gateway should query your *groov* RIO's network interface.
- **Example 4**—Route traffic leaving the *groov* RIO through a specific path by controlling which DNS server the module queries.

- **Example 5**—Route traffic from one network interface (ETH0/ETH1, WLAN, or OpenVPN Tunnel 0) to another network interface. (This is referred to as *port redirection*.)

Static IP Address

An **IP Address** and **Subnet Mask** create a unique network address. The network address is usually assigned by the DHCP server and may change due to a variety of circumstances (for example, a power outage). A network administrator may want to assign your *groov* RIO a static IP address so that the network address does not change. In a *groov* RIO, the Ethernet network interfaces must have different IP addresses and subnet masks according to their operating mode:

- In switched mode, both interfaces (ETH0 and ETH1) share the IP address and subnet mask.
- In independent mode, each interface (ETH0 and ETH1) must have a different IP address and subnet mask.

While the IP address must be *different* than any other device *on the same LAN*, the subnet mask must be the *same* as all other devices *on the same LAN*. For example:

- All the devices on LAN A are assigned a subnet mask of 255.255.0.0.
- All the devices on LAN B are assigned a subnet mask of 255.0.0.0.

If you connect your *groov* RIO to LAN A, make sure to specify 255.255.0.0 as the subnet mask.

Port Redirection

You should only implement port redirection on your *groov* RIO if you are redirecting packets between two trusted networks connected to the *groov* RIO network interfaces (ETH0/ETH1, WLAN0, or TUN0). Make sure you read the following two documents and discuss your plans with your network administrator:

- [Guide to Networking groov Products](#) (form 2161)
- [groov EPIC Cybersecurity Design and Best Practices Technical Note](#) (form 2310)

It is important to understand the risks and create mitigation plans for those risks.

You need to collect the following information to create rules in *groov* Manage to indicate that network traffic that arrives through a port on one network interface (the *external* port) is redirected to a port on another interface (the *redirect* port).

- **Title**—(Optional) A descriptive name for the rule. The name can be only letters (in either uppercase, lowercase, or mixed case) and numbers; no spaces or special characters.
- **Protocol**—The protocol (TCP, UDP, or both) used by the packets.
- **External Port**—The port number through which packets arrive.
- **External Interface**—The network interface (ETH0/ETH1, WLAN0, or TUN0) through which packets arrive.
- **Redirect Address**—*groov* RIO sends (redirects) the packets to this IP address.
- **Redirect Port**—*groov* RIO sends (redirects) the packets to this port number.
- **Redirect Interface**—*groov* RIO sends (redirects) to this network interface (ETH0/ETH1, WLAN0, or TUN0).
- **Source**—(Optional) Indicates that this rule applies only to packets received from this IP address or subnet. This is a way to limit which device (if you specify an IP address) or devices (if you specify a subnet) on a network can use port redirection.

Domain Name and DNS Server IP Address Management

In a basic network, when a new device connects to the network, the DHCP server assigns the device a domain name and domain name server (DNS) IP address. When the device is looking for resources on the network, like printers and other computers, it delivers a search request to the DNS server. In more complex networks, where

there may be multiple DNS servers, network administrators use several different techniques to manage the workload on these servers. One technique is to assign the device a specific domain name and DNS server IP address; the network administrator may also assign more than one DNS server IP address and indicate in which order the device should query each server.

You can assign up to three domain name servers to each network interface on the *groov* RIO UIO and indicate the order in which to communicate with the servers. You can set the DNS order of a network provisioning domain to specify the priority that name servers and search domains are added to the DNS resolver's configuration, which has a maximum limit of three name servers and six search domains. When a DNS request is made, the resolver queries name servers in series in the order defined in the configuration. If a response is received with either a successful resolution or with a reply code (such as "Name not found"), no other name servers are queried. If the DNS request times out, the next name server is tried until all name servers are exhausted. Be aware that name resolution of secondary and tertiary name servers may be slow due to the sequential nature of queries by the DNS resolver.

For each network interface that requires this configuration, you need:

- **DNS Server Override** and **DNS Domain Override**—The DNS server IP addresses and domain name. You can specify up to three DNS servers.
- **DNS Order**—A number, beginning with 1, that identifies the order in which network interfaces are queried. Number 1 indicates the first network interface to be queried.

Gateway IP Address Management

If your network policy requires the assignment of a specific gateway IP address, review the information in ["Redirecting Traffic Initiated by an Incoming Connection Request" on page 187](#) to understand how a gateway queries the network interface of a *groov* RIO and—if there are multiple active network interfaces—prioritizes their use.

For each network interface that requires this configuration, you need:

- **Gateway IP Address**—In *groov* Manage, you enter this in the **Gateway Override** field.
- **Gateway Order**—The order in which the network interface's gateway is queried for off-subnet destination-based routing, with 1 being the highest priority (the network interface queried first). You can alter this order by changing the number. The gateway associated with the active interface with the lowest gateway order is used as the default gateway. For more information about this topic, see ["H: Advanced Networking Configurations" on page 187](#).

Static Routes

Network administrators create static routes to help balance network traffic in small networks. As a packet travels through a network, it travels through different networking equipment and devices (like a *groov* RIO) on its way to its destination. Each piece of equipment or device that it travels through is called a *hop*. If a network administrator identifies that certain packets destined for a specific IP address create a heavy traffic pattern, the administrator can help alleviate the heavy traffic by modifying the hops along the route.

If a network administrator identifies a *groov* RIO as one hop in a heavily traveled route, the administrator can modify the *groov* RIO's network interface to redirect the packets through a different gateway. To indicate which gateway the packet should travel and which packets should travel through that gateway, you need:

- **Nexthop Address** or **Subnet**—The IP address of the next hop along the route that the packet would normally travel through.
- **Gateway Address**—The IP address of the gateway through which the packet should travel.
- **Interface**—The network interface on the *groov* RIO through which the packets travel.

You can have multiple static routes so that you can direct packets with different next hop addresses to different gateways.

CHANGING THE ETHERNET NETWORK INTERFACE TO SWITCHED MODE

Change from independent mode to switched mode, when you want to move your *groov* RIO from a two LAN environment to a single LAN environment. Before you make the change, make sure you are prepared:

- Have physical access to your *groov* RIO to connect and disconnect Ethernet cables.
- Schedule this task during a time that it doesn't disrupt your application or equipment operation because the change will reboot your *groov* RIO..
- Make sure to have one active connection to your *groov* RIO.
 - If you have Ethernet cables connected to both Ethernet network interfaces, disconnect one. This is important because after your RIO reboots, if there are two active Ethernet connections to different LANs while your RIO is in switched mode, communication can be disrupted on both LANs.
 - If you have an active WiFi connection, you can disconnect both Ethernet network interfaces.
- If you are connecting to a new LAN, understand the network policies in place for that LAN and what network settings you need to change on your *groov* RIO to comply with those policies. For introductory information about policies, review [“Identifying Your Network Topology” on page 52](#). For a general review of all the network settings available on your RIO, review:
 - [“Choosing Between Automatic and Manual connections” on page 59](#)
 - [“For Network Administrators: Tools for Managing Network Traffic to/From groov Devices” on page 60](#)
- If you are creating rings or daisy chains, make sure you understand the correct way to connect your *groov* RIOs to create these topologies; review [“Connecting Multiple groov RIOs Into Daisy-Chains or Rings” on page 55](#). You may also want to have the Ethernet cables and additional RIOs ready so you can begin connecting them after you finish changing to switched mode.

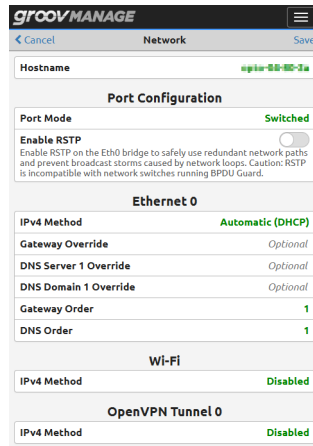
When you are ready, follow these steps:

1. Log into the *groov* RIO module with a user ID that has administrator privileges.
2. Click **Network > Configure**. The Network configuration page displays the Network configuration page with two Ethernet sections: **Ethernet 0** and **Ethernet 1**.

The screenshot shows the 'groovMANAGE' interface for Network configuration. At the top, there are 'Cancel' and 'Save' buttons. Below is a 'Hostname' field with the value 'groov-84-B5-3a'. The 'Port Configuration' section shows 'Port Mode' set to 'Independent'. Below this are two Ethernet sections: 'Ethernet 0' and 'Ethernet 1'. Each section has fields for 'IPv4 Method' (set to 'Automatic (DHCP)'), 'Gateway Override' (Optional), 'DNS Server 1 Override' (Optional), 'DNS Domain 1 Override' (Optional), 'Gateway Order' (set to 1 for Ethernet 0 and 2 for Ethernet 1), and 'DNS Order' (set to 1 for Ethernet 0 and 2 for Ethernet 1). Below the Ethernet sections are 'Wi-Fi' and 'OpenVPN Tunnel 0' sections, both with 'IPv4 Method' set to 'Disabled'.

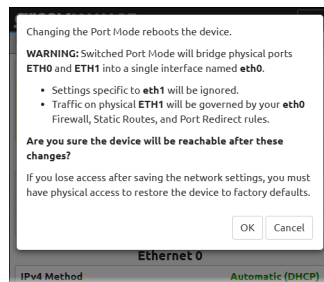
3. In the **Port Configuration** section, click **Independent** in the **Port Mode** field.
4. Click **Switched**. *groov* Manage changes the Network configuration page to display one Ethernet section: **Ethernet 0**.

CHANGING THE ETHERNET NETWORK INTERFACE TO SWITCHED MODE

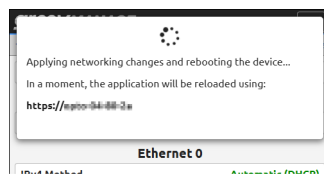


5. Configure Ethernet 0.
 - a. Enable RSTP. There are very few situations in which you want to disable RSTP and a best practice is to leave it enabled to avoid the issues described in [“Rings and Ethernet Redundancy” on page 56](#). A network administrator can determine if it needs to be disabled.
 - b. If you are connecting your *groov* RIO into a ring, discuss with your network administrator whether to adjust **RSTP Priority**. The network administrator typically manages the priority level of all devices in a ring and can best determine if the priority needs to be changed. On a RIO, the available priority levels are **Primary**, **Normal**, and **Lowest**.

If you are not connecting your *groov* RIO into a ring, do not change **RSTP Priority**.
 - c. The remainder of the fields in the **Ethernet 0** section are typically advanced networking options. If you need to change any of these settings, review [“Configuration Tasks for Network Administrators” on page 75](#).
6. Click **Save**. *groov* Manage displays the following warning message:



7. Click **OK**. *groov* Manage displays the following progress message:



8. After your *groov* RIO finishes rebooting, connect the Ethernet cable from the new LAN to either network interface (ETH0 or EHT1).

9. Verify that the network connection works by using a computer on the same network to connect to your *groov* RIO. If you have any issues, refer to [“Browser Reports that URL to groov RIO UIO is Unreachable” on page 158](#).

Your *groov* RIO is now connected to your LAN. If you plan on creating a daisy chain or a ring, review the information in [“Connecting Multiple *groov* RIOs Into Daisy-Chains or Rings” on page 55](#) to minimize issues.

CHANGING THE ETHERNET NETWORK INTERFACE TO INDEPENDENT MODE

By default, the Ethernet network interfaces on a *groov* RIO module operate in switched mode: the interfaces (ETH0 and ETH1) share an IP address and can only connect to one LAN (through either interface). For a RIO to connect to two LANs, you need to change the mode to *independent*.

Work with your network administrator as you prepare for this change:

- Have physical access to your *groov* RIO to connect and disconnect Ethernet cables.
- Schedule this task during a time that it doesn’t disrupt your application or equipment operation because the change will reboot your *groov* RIO.
- Make sure to have one active connection to your *groov* RIO.
 - If you have an active Ethernet connection, make sure the Ethernet cable is connected to ETH0. This allows you to modify network settings (like firewall rules, port redirect rules, and static routes) on ETH1 so that when your RIO reboots, ETH1 is ready to connect to the new LAN.
 - If you have an active WiFi connection, you can disconnect both Ethernet network interfaces.
- For each LAN, understand the network policies in place for that LAN and what network settings you need to change on your *groov* RIO to comply with those policies. For introductory information about policies, review [“Identifying Your Network Topology” on page 52](#). For a general review of all the network settings available on your RIO, review:
 - [“Choosing Between Automatic and Manual connections” on page 59](#)
 - [“For Network Administrators: Tools for Managing Network Traffic to/From *groov* Devices” on page 60](#)

Remember to also have an Ethernet cable available to eventually connect to the new LAN.

- Know which LAN you are connecting to which network interface. While both network interfaces have the same settings, the defaults differ. The default configuration for ETH0 is to connect it to a trusted LAN, typically the OT network. The default configuration for ETH1 is to connect it to an untrusted LAN, usually the IT network. Take advantage of these defaults by assigning each network interface the matching LAN. For more information about trusted and untrusted networks, review [“A Network With Multiple LANs” on page 53](#).

When you are ready, follow these steps:

1. Log into the *groov* RIO module with a user ID that has administrator privileges.
2. Modify the following network settings on ETH1 to comply with the network policies on the new LAN:
 - Modify any firewall rules (for more information and instructions, review [“Configuring the Firewall” on page 45](#)).
 - A network administrator may implement port redirection rules to facilitate communication between two trusted networks. To learn more about port redirection, review [“Port Redirection” on page 61](#). For instructions, review [“Enabling Port Redirection” on page 77](#).
 - A network administrator may implement static routes to help manage traffic. To learn more about static routes, review [“Static Routes” on page 62](#). For instructions, review [“Adding a Static Route” on page 81](#).
3. Click **Network > Configure**. The Network configuration page displays only one Ethernet section: **Ethernet 0**.

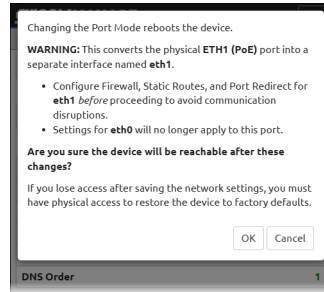
CHANGING THE ETHERNET NETWORK INTERFACE TO INDEPENDENT MODE

The screenshot shows the 'groovMANAGE' interface with the 'Network' tab selected. The 'Port Configuration' section has 'Port Mode' set to 'Switched'. Below this, the 'Ethernet 0' section is visible, showing 'IPv4 Method' as 'Automatic (DHCP)' and various override options. The 'Wi-Fi' and 'OpenVPN Tunnel 0' sections are also visible, both with 'IPv4 Method' set to 'Disabled'.

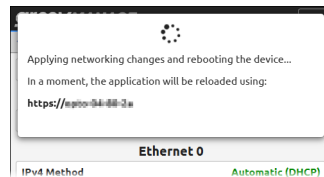
4. In the **Port Configuration** section, click on **Switched** in the **Port Mode** field.
5. Click **Independent**. *groov* Manage changes the Network configuration page to display two Ethernet sections: Ethernet 0 and Ethernet 1.

The screenshot shows the 'groovMANAGE' interface with the 'Network' tab selected. The 'Port Configuration' section has 'Port Mode' set to 'Independent'. Below this, there are two Ethernet sections: 'Ethernet 0' and 'Ethernet 1'. Both sections show 'IPv4 Method' as 'Automatic (DHCP)' and various override options. The 'Wi-Fi' and 'OpenVPN Tunnel 0' sections are also visible, both with 'IPv4 Method' set to 'Disabled'.

6. Configure **Ethernet 0** and **Ethernet 1**.
 - a. Change the **IPv4 Method** only if you need to assign a static IP address or implement any of the advanced network configurations described in [“For Network Administrators: Tools for Managing Network Traffic to/From groov Devices”](#) on page 60. For more information about the two different IPv4 methods, review [“Understanding the Difference Between Automatic and Manual Connections”](#) on page 59.
 - b. The remainder of the fields are typically advanced networking options. If you need to change any of these settings, review [“Configuration Tasks for Network Administrators”](#) on page 75.
7. Click **Save**. *groov* Manage displays the following warning message:



8. Click **OK**. *groov* Manage displays the following progress message:



9. After your *groov* RIO finishes rebooting, connect the Ethernet cable from the new LANs to the network interface (ETH0 or ETH1) you assigned to it. Verify that the network connection works by using a computer on the same network to connect to your *groov* RIO. If you have any issues, refer to [“Browser Reports that URL to groov RIO UIO is Unreachable” on page 158](#). Repeat this step for both network interfaces.

CONNECTING TO A WIRELESS LAN (WLAN0)

Before you begin, make sure you attached a supported WiFi adapter to the USB interface (review "Installing an Approved USB WiFi Adapter" on page 140).

groov RIO supports several different encryption and authentication protocols (review [“Wireless Network Security” on page 57](#)). Follow the instructions appropriate for the type of security implemented by your wireless network:

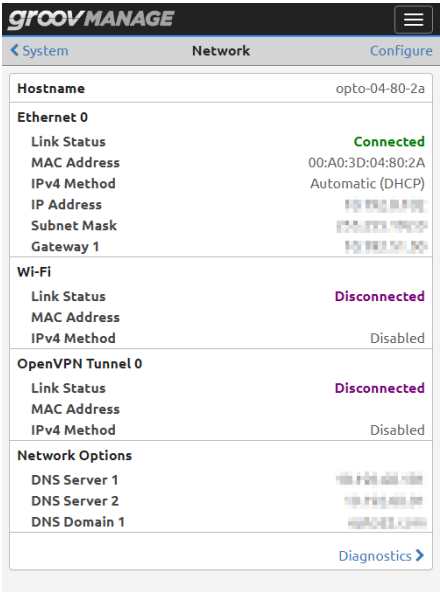
- “Configuring for a Wireless Network with WEP, WPA, WPA2, or No Encryption” on page 67
- “Configuring for a Wireless Network with WPA2-Enterprise Encryption” on page 70

Configuring for a Wireless Network with WEP, WPA, WPA2, or No Encryption

Changes to network interfaces require a restart of the network connections. Schedule changes to network connections at a time that minimizes their impact on your application and equipment.

1. Log into the *groov* RIO with a user ID that has administrator privileges.
2. Click or tap **Network**. *groov* Manage displays the Network status page.

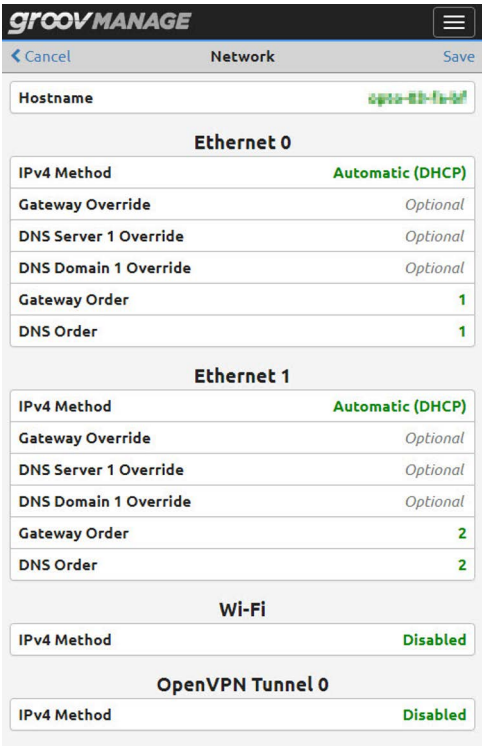
CONNECTING TO A WIRELESS LAN (WLAN0)



The Network status page shows you the current network configuration, and provides access to the Network configuration page, as well as diagnostic tools.

In the example above, *groov* RIO is connected to a network through a cable plugged into ETH0. There is no WiFi connection through WLAN0, and no connection to a virtual private network. The values listed in the Network Options section were assigned by the local DHCP server.

- 3. Click or tap **Configure**. *groov* Manage displays the Network configuration page. The example below shows the default settings.



Ethernet 0 shows the current settings for ETH0. Wi-Fi shows the current settings for WLAN0. OpenVPN Tunnel 0 shows the current settings for a virtual private network.

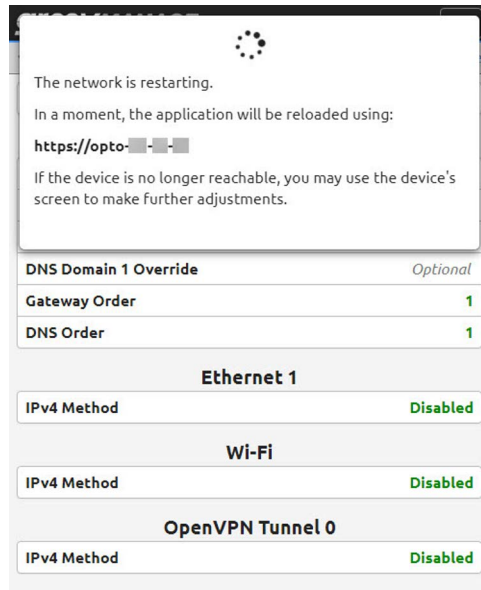
4. In the Network configuration page, scroll down to the **Wi-Fi** section.
5. Click **IPv4 Method** and select **Automatic (DHCP)** or **Manual (Static IP)**. *groov* Manage updates the Wi-Fi section of the Network configuration page with additional fields:

The image shows two versions of the 'Wi-Fi' configuration section in a network management interface. The left version shows the 'Automatic (DHCP)' setting for the 'IPv4 Method'. The right version shows the 'Manual (Static)' setting, which has expanded the configuration fields to include 'IP Address' (10.20.30.40), 'Subnet Mask' (255.255.255.0), 'Gateway Address' (Optional), 'DNS Server 1' (Optional), and 'DNS Domain 1' (Optional). A text box with an arrow points to these additional fields, stating: 'These fields are typically for advanced networking configurations described on .' Below both sections is the 'OpenVPN Tunnel 0' section.

Some of the new fields are for advanced networking situations; provides instructions for using these fields.

6. In the **SSID** field, type in the name of the wireless access point (WAP). This is typically a text string from 1 to 32 characters. In the consumer area, this is commonly referred to as the "WiFi name".
7. Set the **Encryption** field with the appropriate option:
 - If your wireless network does *not* implement any encryption, leave this field set to **None** and click **Save**. *groov* Manage asks you to verify that you want to save your changes and notifies you that the network will be restarted. Click **Yes**. After the restart, you are done; you can skip the rest of these steps.
 - If your wireless network implements encryption, click **Encryption** and select **WEP**, **WPA**, or **WPA2**.
8. Click **Key Type** and select whether the wireless network requires a passphrase or PSK.
9. Click **Key** and type in the passphrase or key value.
10. Click **Save**. *groov* Manage asks you to verify that you want to save your changes and notifies you that the network will be restarted. Click **Yes**.

CONNECTING TO A WIRELESS LAN (WLANO)

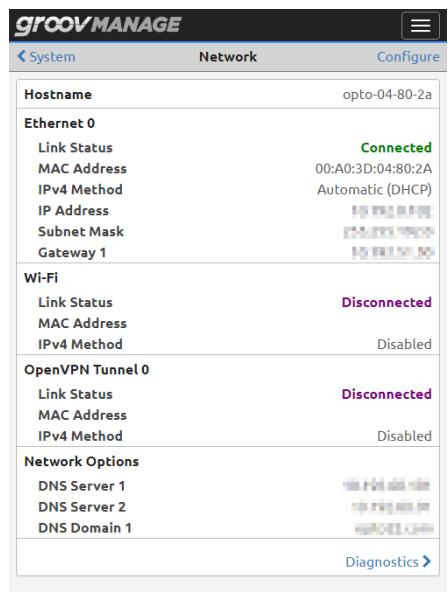


11. After the network connections are restarted, if *groov* Manage doesn't reappear and you can't access your RIO through any of the network connections you configured, start up *groov* Find to help you locate your RIO (see ["Downloading and Running groov Find" on page 159](#)).
12. After you reconnect to your RIO, you can test the network connections and fine-tune your security settings. If you need to set up a virtual private network (VPN), see ["Testing the Network Connections and Fine-Tuning Security" on page 84](#).

Configuring for a Wireless Network with WPA2-Enterprise Encryption

Changes to network interfaces require a restart of the network connections. Schedule changes to network connections at a time that minimizes their impact on your application and equipment.

1. Log into the *groov* RIO with a user ID that has administrator privileges.
2. Click or tap **Network**. *groov* Manage displays the Network status page.



The Network status page shows you the current network configuration, and provides access to the Network configuration page, as well as diagnostic tools.

In the example above, *groov* RIO is connected to a network through a cable plugged into ETH0. There is no WiFi connection through WLAN0, and no connection to a virtual private network. The values listed in the Network Options section were assigned by the local DHCP server.

3. Click or tap **Configure**. *groov* Manage displays the Network configuration page. The example below shows the default settings.

groovMANAGE

Network

Hostname: *groov-11-11-11*

Ethernet 0

IPv4 Method: **Automatic (DHCP)**

Gateway Override: *Optional*

DNS Server 1 Override: *Optional*

DNS Domain 1 Override: *Optional*

Gateway Order: **1**

DNS Order: **1**

Ethernet 1

IPv4 Method: **Automatic (DHCP)**

Gateway Override: *Optional*

DNS Server 1 Override: *Optional*

DNS Domain 1 Override: *Optional*

Gateway Order: **2**

DNS Order: **2**

Wi-Fi

IPv4 Method: **Disabled**

OpenVPN Tunnel 0

IPv4 Method: **Disabled**

Ethernet 0 shows the current settings for ETH0. Wi-Fi shows the current settings for WLAN0. OpenVPN Tunnel 0 shows the current settings for a virtual private network.

4. In the Network configuration page, scroll down to the **Wi-Fi** section.
5. Click **IPv4 Method** and select **Automatic (DHCP)** or **Manual (Static IP)**. *groov* Manage updates the Wi-Fi section of the Network configuration page with additional fields:

DNS Order: **2**

Wi-Fi

IPv4 Method: **Automatic (DHCP)**

SSID: *Required*

Encryption: **None**

Gateway Override: *Optional*

DNS Server 1 Override: *Optional*

DNS Domain 1 Override: *Optional*

Gateway Order: **3**

DNS Order: **3**

OpenVPN Tunnel 0

DNS Order: **2**

Wi-Fi

IPv4 Method: **Manual (Static)**

SSID: *Required*

Encryption: **None**

IP Address: **10.20.30.40**

Subnet Mask: **255.255.255.0**

Gateway Address: *Optional*

DNS Server 1: *Optional*

DNS Domain 1: *Optional*

Gateway Order: **3**

DNS Order: **3**

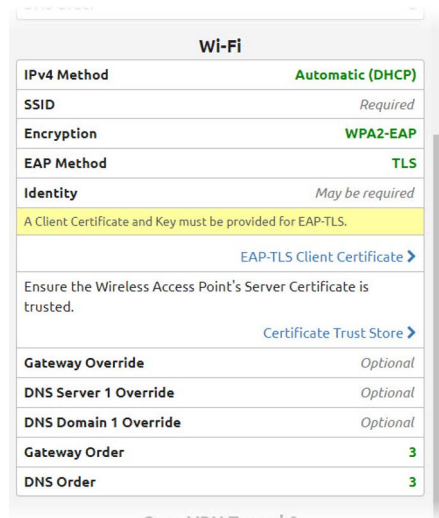
OpenVPN Tunnel 0

These fields are typically for advanced networking configurations described on .

CONNECTING TO A WIRELESS LAN (WLAN0)

Some of the new fields are for advanced networking situations; provides instructions for using these fields.

6. In the **SSID** field, type in the name of the wireless access point (WAP). This is typically a text string from 1 to 32 characters. In the consumer area, this is commonly referred to as the “WiFi name”.
7. Click **Encryption** and select **WPA2-Enterprise**. *groov* Manage updates the Wi-Fi section:



Wi-Fi	
IPv4 Method	Automatic (DHCP)
SSID	Required
Encryption	WPA2-EAP
EAP Method	TLS
Identity	May be required
A Client Certificate and Key must be provided for EAP-TLS.	
EAP-TLS Client Certificate >	
Ensure the Wireless Access Point's Server Certificate is trusted.	
Certificate Trust Store >	
Gateway Override	Optional
DNS Server 1 Override	Optional
DNS Domain 1 Override	Optional
Gateway Order	3
DNS Order	3

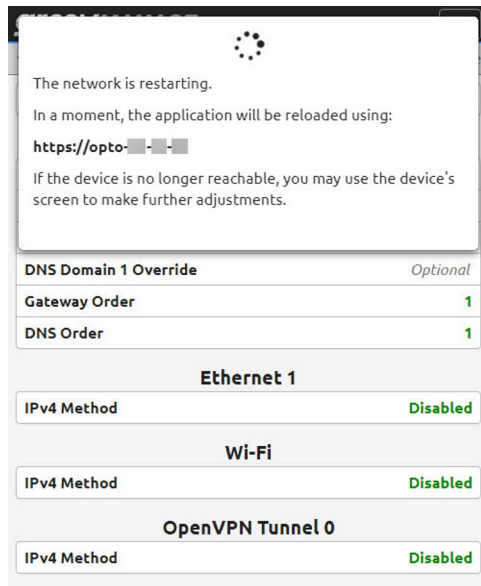
8. Click **EAP Method**, select the EAP (TLS, TTLS, or PEAP) implemented by your wireless network, enter the credentials (if required), and upload all required certificates:
 - For TLS, consult with your network administrator to determine if you must enter a value for the **Identity** field. Not all wireless networks implement this field.
 - For TTLS or PEAP, specify the following information:
 - **Inner EAP Method**—The type of handshake. For TTLS, you can select either **PAP**, **CHAP**, or **MSCHAPv2**. For PEAP, the only option is **MSCHAPv2**.
 - **Identity and Password**—Obtain this information from your network administrator. If the type of handshake is PAP or MSCHAPv2, a password is required.
9. (Optional) Before you click on either the **EAP-TLS Client Certificate** link or the **Certificate Trust Store** link, click **Save** on the Network configuration page to save any changes you have made. *This will restart your network connections.*
10. For all EAPs, an EAP client certificate is required; some sites may also require a wireless network's server certificate. Obtain these certificates (in either **DER** or **PEM** format) from your network administrator. Verify that the private key file is not password protected.

To upload the EAP-TLS client certificate:

- a. Click **EAP-TLS Client Certificate**.
- b. Click **Yes** on the confirmation window.
- c. Click **Upload Certificate**.
- d. Click **Public Certificate**.
- e. Navigate to the folder where you stored the EAP-TLS, EAP-TTLS, or EAP-PEAP client certificate file.
- f. Select the file and click **OK**.
- g. Click **Private Key**.
- h. Navigate to the folder where you stored the EAP-TLS, EAP-TTLS, or EAP-PEAP key file.
- i. Select the file and click **OK**.
- j. Click **Upload**. *groov* Manage checks the files to verify that they are in the correct format.

To upload the wireless network's server certificate:

- k. Click **Certificate Trust Store**.
 - l. Click **Yes** on the confirmation window.
 - m. Click **Add/Update**.
 - n. Navigate to the folder where you stored the wireless network's server certificate file.
 - o. Select the file and click **OK**. *groov* Manage checks the files to verify that they are in the correct format.
11. Click **Save**. *groov* Manage asks you to verify that you want to save your changes and notifies you that the network will be restarted. Click **Yes**.



12. After the network connections are restarted, if *groov* Manage doesn't reappear and you can't access your RIO through any of the network connections you configured, start up *groov* Find to help you locate your RIO (see ["Downloading and Running groov Find" on page 159](#)).
13. After you reconnect to your RIO, you can test the network connections and fine-tune your security settings. If you need to set up a virtual private network (VPN), see ["Testing the Network Connections and Fine-Tuning Security" on page 84](#).

CONNECTING TO A VIRTUAL PRIVATE NETWORK (VPN) (TUN0)

Before you begin:

- Make sure you have configured at least one physical network connections. You may want to review the following for instructions on creating a physical network connection:
 - ["Changing the Ethernet Network Interface to Switched Mode" on page 63](#)
 - ["Changing the Ethernet Network Interface to Independent Mode" on page 65](#)
 - ["Connecting to a Wireless LAN \(WLAN0\)" on page 67](#)
- Check that you have all the information you collected when you reviewed ["Virtual Private Networks \(VPN\) with OpenVPN" on page 58](#).
- Verify that the OpenVPN server is reachable.

After verifying all of these items, you can configure the OpenVPN client on the *groov* RIO UIO:

CONNECTING TO A VIRTUAL PRIVATE NETWORK (VPN) (TUNO)

1. From a browser, connect to the *groov* RIO UIO and log into *groov* Manage with a user ID and password that has system administrator permission.
2. If you are entering the configuration manually (without a configuration file as described in [“Virtual Private Networks \(VPN\) with OpenVPN” on page 58](#)), upload the public key:
 - a. From the *groov* Manage Home page, click **Security > Client SSL**.
 - b. Click **Add/Update**.
 - c. Navigate to the folder where you stored the public key (.cert) file.
 - d. Select the key and click **Open**.
3. Click **Back > Home** to return to the *groov* Manage Home page.
4. Click **Network > Configure**.
5. In the **OpenVPN Tunnel 0** section, click **IPv4 Method** and select **Automatic (DHCP)**.

IPv4 Method Disabled

OpenVPN Tunnel 0

IPv4 Method Automatic (DHCP)

Use Configuration Wizard ☐
Guided input for basic client configuration.

[Upload Client Configuration File](#)

[Set User Credentials](#)

[Set Proxy Credentials](#)

Current Configuration >

Gateway Order	255
DNS Order	255

6. Enter the configuration information you collected when you reviewed [“Virtual Private Networks \(VPN\) with OpenVPN” on page 58](#).
 - If your VPN information is in a client configuration file, click **Upload Configuration File**. Navigate to the folder where you stored the configuration file, select it, and click **Open**. Click **Set User Credentials** to enter the OpenVPN server username and password. If necessary, click **Set Proxy Credentials** to enter the proxy credentials. Go to [step 7](#).
 - If you need to enter the configuration information manually, click the **User Configuration Wizard** switch so that it turns green. Perform the following steps:
 - a. Click **Protocol** to select the protocol used by your OpenVPN server.
 - b. Enter the IP address or full domain name of the OpenVPN server in the **Remote Host** field.
 - c. To enter the port number, click in the space between the - and + sign. Type in the port number.
 - d. Click **Select Certificate** and select the certificate you uploaded in [step 2](#) on [page 74](#).
 - e. In the **Username** and **Password** fields, type in the OpenVPN server username and password. (Not the proxy username and password.)
 - f. Click **Encryption Cipher** and select the cipher used by your OpenVPN server from the list.

IPv4 Method Disabled

OpenVPN Tunnel 0

IPv4 Method Automatic (DHCP)

Use Configuration Wizard ☒
Guided input for basic client configuration.

Protocol udp

Remote Host Required

Remote Port ⊖ ⊕

Remote Public Cert Select Certificate
Select the certificate authority PEM certificate. You can upload the CA certificate from Manage -> Security -> Client SSL.

Username Required

Password Required

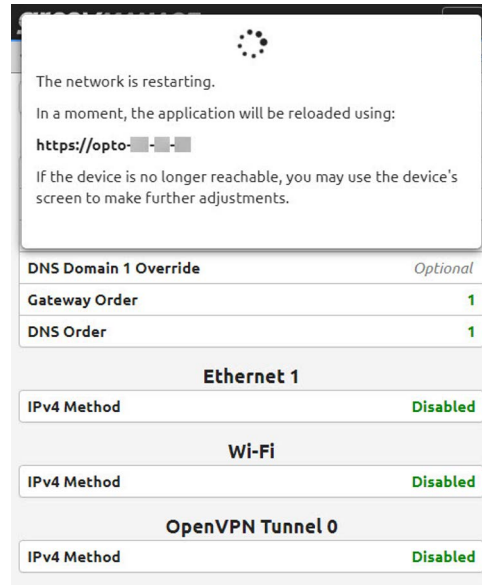
Encryption Cipher None

LZ0 Compress ☐

Gateway Order 255

DNS Order 255

- g. If the OpenVPN server uses LZO compression, slide the **LZO Compress** switch to the right so it turns green.
 - h. If you need to modify the **Gateway Order** and **DNS Order**, click on those numbers and change them.
7. Click **Save**. If *groov* Manage reports any errors, fix those errors and click **Save**. Otherwise, *groov* Manage displays a message that it will restart the network connections.



CONFIGURATION TASKS FOR NETWORK ADMINISTRATORS

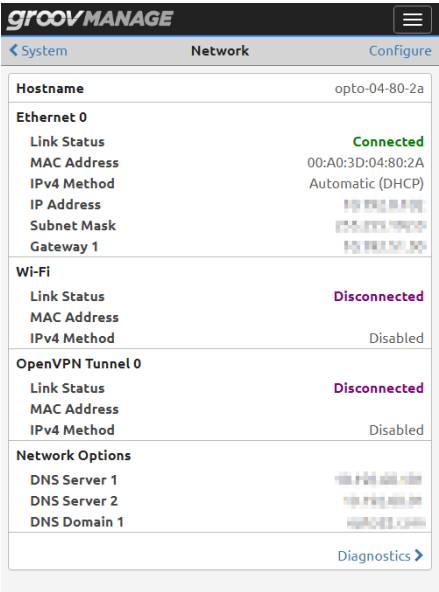
This section describes how to implement the following advanced networking situations:

- [“Adding a Static IP Address” on page 75](#)
- [“Enabling Port Redirection” on page 77](#)
- [“Changing the DNS Server and Domain Name Assignments” on page 79](#)
- [“Changing Gateway IP Address Assignments” on page 80](#)
- [“Adding a Static Route” on page 81](#)

Adding a Static IP Address

Before you begin, make sure you have the IP address and subnet mask values as described in [“Understanding the Difference Between Automatic and Manual Connections” on page 59](#). Changes to network interfaces require a restart of the network connections. Schedule changes to network connections at a time that minimizes their impact on your application and equipment.

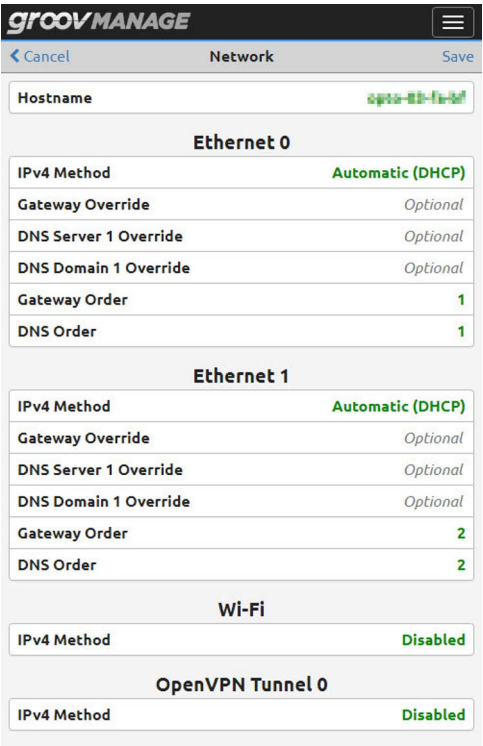
1. Log into the *groov* RIO with a user ID that has administrator privileges.
2. Click or tap **Network**. *groov* Manage displays the Network status page.



The Network status page shows you the current network configuration, and provides access to the Network configuration page, as well as diagnostic tools.

In the example above, *groov* RIO is connected to a network through a cable plugged into ETH0. There is no WiFi connection through WLAN0, and no connection to a virtual private network. The values listed in the Network Options section were assigned by the local DHCP server.

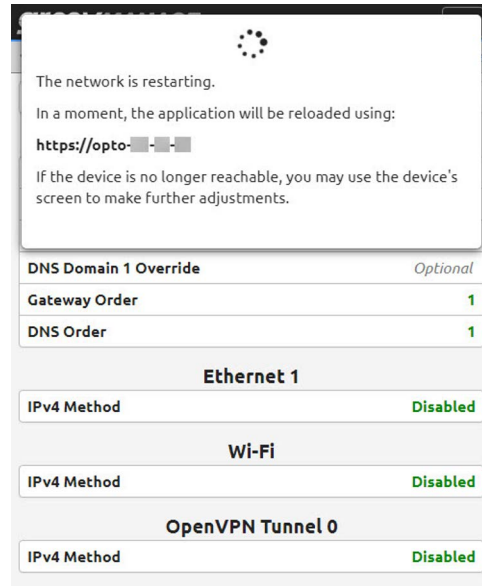
3. Click or tap **Configure**. *groov* Manage displays the Network configuration page. The example below shows the default settings.



Ethernet 0 shows the current settings for ETH0. Wi-Fi shows the current settings for WLAN0. OpenVPN Tunnel 0 shows the current settings for a virtual private network.

Change the IPv4 method for the network interface (**Ethernet 0**, **Ethernet 1**, or **Wi-Fi**) that needs the static IP address to manual: click the **IPv4 Method** field and select **Manual (Static)**. *groov* Manage displays another set of fields.

4. In the **IP Address** field, type in the IP address. If required, type in the new subnet mask IP address in the **Subnet Mask** field.
5. Click **Save**. *groov* Manage asks you to verify that you want to save your changes and notifies you that the network will be restarted. Click **Yes**.



6. After the network connections are restarted, if *groov* Manage doesn't reappear and you can't access your RIO through any of the network connections you configured, start up *groov* Find to help you locate your RIO (see ["Downloading and Running groov Find" on page 159](#)).
7. After you reconnect to your RIO, you can test the network connections and fine-tune your security settings. If you need to set up a virtual private network (VPN), see ["Testing the Network Connections and Fine-Tuning Security" on page 84](#).

Enabling Port Redirection

Make sure you reviewed ["Port Redirection" on page 61](#) and that you collected all the information described in that section.

1. Log into the *groov* RIO with a user ID that has administrator privileges.

- Click **Network > Port Redirect**. *groov* Manage displays the Port Redirect page:

groovMANAGE

Cancel Port Redirect Save

Port redirect allows hosts on one network to communicate with a host on another network subject to the restrictions of the port redirect configuration.

Port redirect is enabled when there is at least one rule.

Status

Status Disabled

Rules

Add Rule

- Click **Add Rule**. *groov* Manage displays the New Rule page:

New Rule

Title Optional

Protocol tcp/udp

External Port Required

External Interface eth0

Redirect Address Required

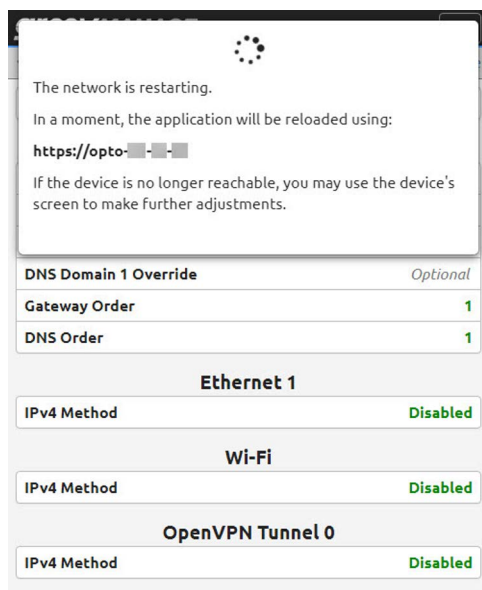
Redirect Port Required

Redirect Interface eth1

Source Optional

Cancel Delete OK

- Fill out the fields with the information described in [“Port Redirection” on page 61](#).
- Click **OK**. If *groov* Manage reports any errors, fix those errors, and click **Save**. Otherwise, *groov* Manage displays a message that it will restart the network connections.
- If you need to create another rule, repeat steps 3 through 5.
- Click **Save**. *groov* Manage asks you to verify that you want to save your changes and notifies you that the network will be restarted. Click **Yes**.



8. After the network connections are restarted, if *groov* Manage doesn't reappear and you can't access your RIO through any of the network connections you configured, start up *groov* Find to help you locate your RIO (see ["Downloading and Running groov Find" on page 159](#)).
9. After you reconnect to your RIO, you can test the network connections and fine-tune your security settings. If you need to set up a virtual private network (VPN), see ["Testing the Network Connections and Fine-Tuning Security" on page 84](#).

Changing the DNS Server and Domain Name Assignments

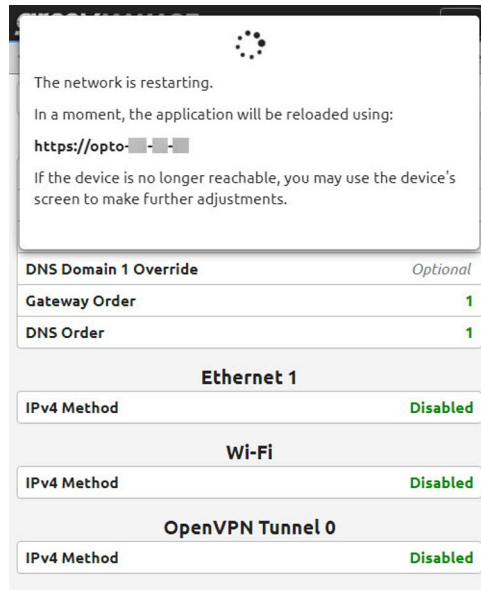
These steps are to override the following assignments done by the DHCP server:

- DNS server IP address
- Domain name

You can also add more DNS server and specify the order in which the servers are queried.

Before you begin, make sure you have the IP address and subnet mask values as described in ["Domain Name and DNS Server IP Address Management" on page 61](#).

1. From a browser, connect to the *groov* RIO and log into *groov* Manage with a user ID and password that has system administrator permission.
2. Click **Network > Configure**.
3. If the **IPv4 Method** is set to **Automatic**, change it to **Manual**. After you make the change, *groov* Manage displays a different set of fields.
4. Enter the DNS server IP address and domain name as a pair. If you need to enter more than one set, *groov* Manage displays another set of fields after you enter the first set:
 - **DNS Server 1 Override** with its corresponding **DNS Domain 1 Override**
 - **DNS Server 2 Override** with its corresponding **DNS Domain 2 Override**
 - **DNS Server 3 Override** with its corresponding **DNS Domain 3 Override**
5. In the **DNS Order** field, specify which of the three DNS servers should be queried first: 1, 2, or 3.
6. Click **Save**. *groov* Manage asks you to verify that you want to save your changes and notifies you that the network will be restarted. Click **Yes**.

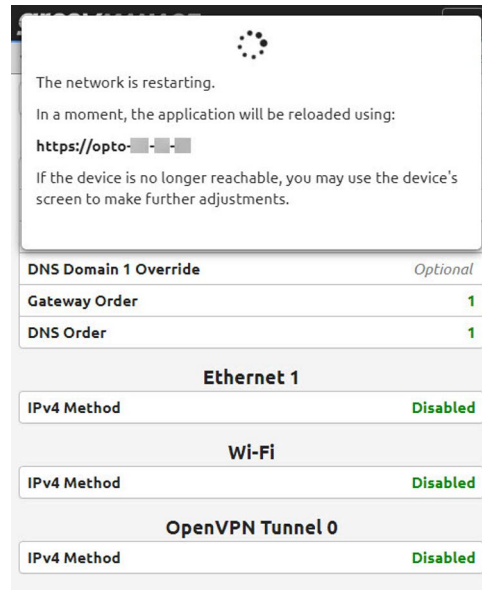


7. After the network connections are restarted, if *groov* Manage doesn't reappear and you can't access your RIO through any of the network connections you configured, start up *groov* Find to help you locate your RIO (see ["Downloading and Running groov Find" on page 159](#)).
8. After you reconnect to your RIO, you can test the network connections and fine-tune your security settings. If you need to set up a virtual private network (VPN), see ["Testing the Network Connections and Fine-Tuning Security" on page 84](#).

Changing Gateway IP Address Assignments

Typically, DHCP servers assign a gateway to each device, including your *groov* RIO, on the network. These assignments may need to be changed as described in ["Gateway IP Address Management" on page 62](#). Before you begin, make sure you have the IP addresses for the gateways and which network interface to assign them.

1. From a browser, connect to the *groov* RIO and log into *groov* Manage with a user ID and password that has system administrator permission.
2. Click **Network > Configure**.
3. If the **IPv4 Method** is set to **Automatic**, change it to **Manual**. After you make the change, *groov* Manage displays a different set of fields.
4. In the **Gateway Address** field, type in the IP address of the gateway that a network administrator assigned to the network interface.
5. In the **Gateway Order** field, type in a number indicating the priority—assigned by the network administrator—of the network interface relative to the other network interfaces assigned to that gateway. The smaller the number, the higher the priority.
6. Click **Save**. *groov* Manage asks you to verify that you want to save your changes and notifies you that the network will be restarted. Click **Yes**.

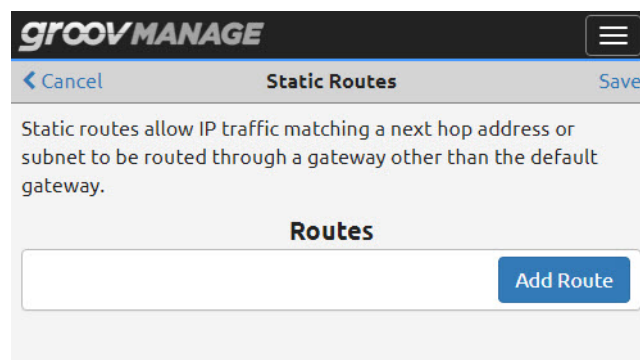


7. After the network connections are restarted, if *groov* Manage doesn't reappear and you can't access your RIO through any of the network connections you configured, start up *groov* Find to help you locate your RIO (see ["Downloading and Running groov Find" on page 159](#)).
8. After you reconnect to your RIO, you can test the network connections and fine-tune your security settings. If you need to set up a virtual private network (VPN), see ["Testing the Network Connections and Fine-Tuning Security" on page 84](#).

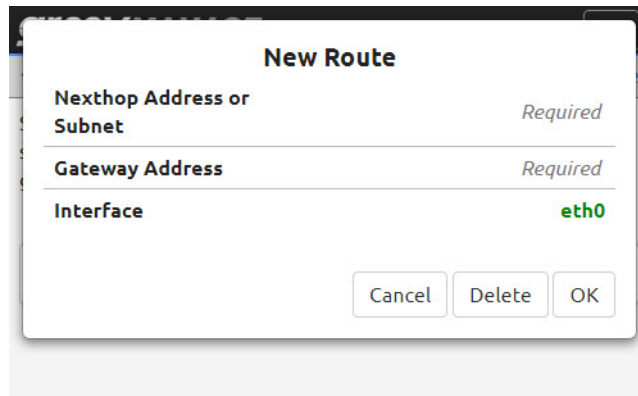
Adding a Static Route

Make sure you reviewed ["Static Routes" on page 62](#) and that you collected all the information described in that section.

1. Log into *groov* Manage with a user ID and password that has system administrator permission.
2. Click **Network > Static Routes**. *groov* Manage displays the Static Routes page:

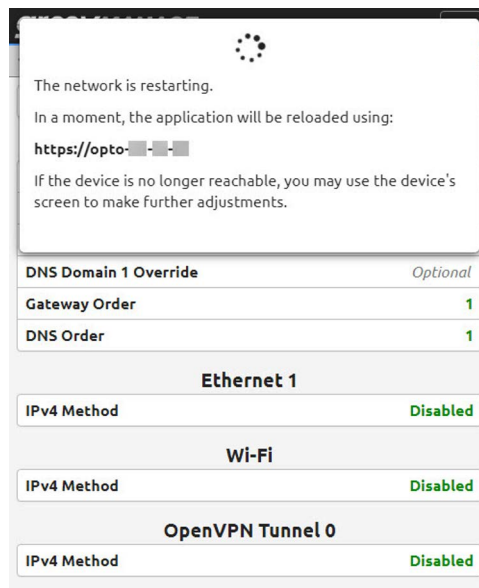


- Click **Add Route**. *groov* Manage displays the New Route page:



The image shows a 'New Route' dialog box with three input fields: 'Nextthop Address or Subnet' (marked 'Required'), 'Gateway Address' (marked 'Required'), and 'Interface' (with 'eth0' selected). At the bottom are 'Cancel', 'Delete', and 'OK' buttons.

- Fill out the fields with the information you collected in [“Static Routes” on page 62](#).
- Click **OK**. If *groov* Manage reports any errors, fix those errors, and click **Save**. Otherwise, *groov* Manage displays a message that it will restart the network connections.
- If you need to create another route, repeat steps 3 through 5.
- Click **Save**. *groov* Manage asks you to verify that you want to save your changes and notifies you that the network will be restarted. Click **Yes**.



The image shows a notification dialog stating 'The network is restarting.' and 'In a moment, the application will be reloaded using: https://opto-...'. Below the notification is a configuration screen with the following sections:

- DNS Domain 1 Override** (Optional)
- Gateway Order** (1)
- DNS Order** (1)
- Ethernet 1**
 - IPv4 Method: Disabled
- Wi-Fi**
 - IPv4 Method: Disabled
- OpenVPN Tunnel 0**
 - IPv4 Method: Disabled

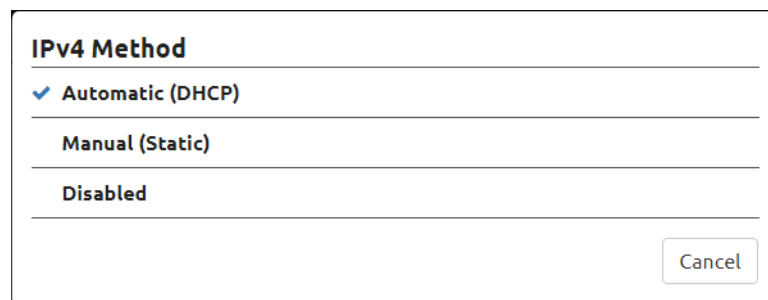
- After the network connections are restarted, if *groov* Manage doesn't reappear and you can't access your RIO through any of the network connections you configured, start up *groov* Find to help you locate your RIO (see [“Downloading and Running groov Find” on page 159](#)).
- After you reconnect to your RIO, you can test the network connections and fine-tune your security settings. If you need to set up a virtual private network (VPN), see [“Testing the Network Connections and Fine-Tuning Security” on page 84](#).

DISABLING A NETWORK INTERFACE

When you disable a network interface, the network interface is closed and network access is denied. If, with your new network configuration, you won't be using some of your network interfaces, you may want to disable them to prevent unauthorized access to your *groov* RIO. However **do not** disable those network interfaces until you have **verified** that your new network configurations works; if you don't test it, you may end up with a *groov* RIO that is inaccessible (including through *groov* Find) and you will have to reset it to factory defaults.

Important: Do not disable all network interfaces unless you have physical access to the module. If you disable all the interfaces, the only way to reopen needed interfaces and gain network access is for an authorized *groov* Manage user with administrator privileges to log in through the built-in display and enable the needed interfaces. If you do not have such a user, you will need to reset your module to factory defaults (see [“How to Reset to Factory Defaults” on page 276](#)).

1. From the Network configuration page, click or tap the **IPv4 Method** currently assigned (the text in green) to the network interface you want to disable. *groov* Manage displays the IPv4 Method window.



IPv4 Method

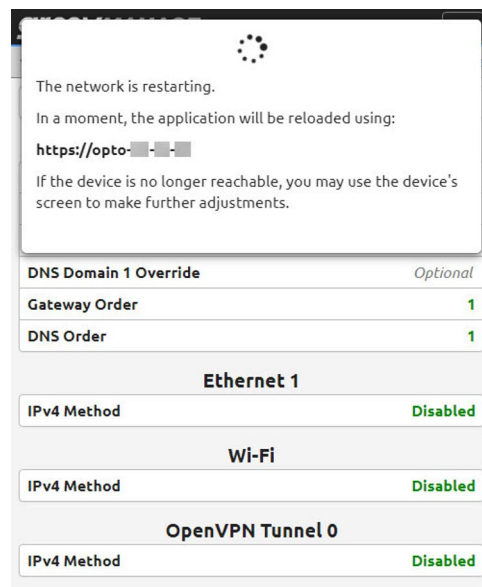
✓ Automatic (DHCP)

Manual (Static)

Disabled

Cancel

2. Click or tap **Disabled**.
3. Click **Save**. *groov* Manage asks you to verify that you want to save your changes and notifies you that the network will be restarted. Click **Yes**.



The network is restarting.
In a moment, the application will be reloaded using:
https://opto-...
If the device is no longer reachable, you may use the device's screen to make further adjustments.

DNS Domain 1 Override *Optional*

Gateway Order **1**

DNS Order **1**

Ethernet 1

IPv4 Method **Disabled**

Wi-Fi

IPv4 Method **Disabled**

OpenVPN Tunnel 0

IPv4 Method **Disabled**

TESTING THE NETWORK CONNECTIONS AND FINE-TUNING SECURITY

4. After the network connections are restarted, if *groov* Manage doesn't reappear and you can't access your RIO through any of the network connections you configured, start up *groov* Find to help you locate your RIO (see ["Downloading and Running groov Find" on page 159](#)).
5. After you reconnect to your RIO, you can test the network connections and fine-tune your security settings. If you need to set up a virtual private network (VPN), see ["Testing the Network Connections and Fine-Tuning Security" on page 84](#).

TESTING THE NETWORK CONNECTIONS AND FINE-TUNING SECURITY

To test the network connections, do one of the following:

- If you switched to **Automatic**, wait a few seconds for the module to receive an IP address from the DHCP server. The logon page refreshes and displays the IP address after it receives it.
- If you switched to **Manual**, verify that the IP address works by trying to connect to the module from a web browser. You can also try the `ping` command in a command prompt window using a Windows computer that is connected to the same network.

If you encounter any issues with ETH0, ETH1, and WLAN0, see ["Troubleshooting" on page 158](#) for topics regarding network connections. If you are troubleshooting issues with an OpenVPN connection, you can review the VPN client logs for messages. To access the logs, from the *groov* Manage home page, click **Info and Help > Logs > OpenVPN Client**.

For enhanced security, disable any network interfaces you are not using. For example, if you are not using ETH0, remember to do one of the options listed in ["Start with an Ethernet Connection" on page 51](#).

You may also want to update your security options and firewall settings:

- ["Managing Certificates on your groov RIO" on page 41](#)
- ["Configuring the Firewall" on page 45](#)

7: Configuring *groov* RIO System Features

A user with administrator privileges is the only user that can change system features. System features provide services like access control, device management, and time management.

SETTING AND ADJUSTING DATE, TIME, AND TIME ZONES

Setting and adjusting the date, time, and time zones can help you with more than just setting *groov* RIO to the local time:

- You can change the date and time of your *groov* RIO to test time-sensitive features of your control program.
- You can synchronize the clock on your *groov* RIO to any number of time servers from around the world.
- You can specify multiple time servers to function as backups of each other, or specify a device as a time server.

When you turn on your *groov* RIO for the first time and after it establishes network connectivity, it sets the time from a default time server. To see the default time server, from the *groov* Manage Home page, click System > Time. The bottom half of the screen lists the time servers.

groovMANAGE

< System Time Settings

Time [Set Time](#)

Year	⊖	2020	⊕
Month	⊖	2	⊕
Day	⊖	20	⊕
Hour	⊖	0	⊕
Minute	⊖	20	⊕
Second	⊖	36	⊕

All currently signed-in users may be signed out after setting the time.

Time Zone [Set Zone](#)

Region	Universal
Locality	

Time Servers [Set NTP](#)

Enable NTP ☒

Time Server 1	0.pool.ntp.org
Time Server 2	1.pool.ntp.org
Time Server 3	2.pool.ntp.org

Sync your clock with servers on the Internet such as 0.pool.ntp.org.

Setting the Date and Time Manually

There might be a few reasons why you want to set the date and time manually instead of synchronizing to time servers:

- You want to test time-sensitive features in your control program, so you want to be able to adjust the date and time to test those features.
- You are working in an environment (for example, a disconnected test environment) where changes in time will not affect production or other critical applications.

Note: *Changing the time manually will log out any users that are currently logged onto your groov RIO. Carefully choose when you will change the time to minimize any adverse effect on other users.*

To set the date and time manually:

1. Log into groov RIO with a user ID that has administrator authority.
2. Click System ( System), then Time ( Time).
3. In the Time Servers section, turn off the Enable NTP setting by moving the slider to the left so that it shows grey ().
4. Click Set NTP.
5. In the Time section, select values for Year, Month, Day, Hour, Minute, and Second.
6. Click Set Time. groov Manage displays a message while it's setting the date and time. When it finishes, the message disappears.

Now your date and time are set.

IMPORTANT: *If you set the date and time manually, the time will not update for Daylight Savings Time (for those areas that observe Daylight Savings Time). So, you must remember to manually update the date and time during those events.*

Setting the Date, Time, and Time Zone by Synchronizing with Time Servers

If you are not familiar with time servers, you can learn more about them through the NTP Pool Project at www.pool.ntp.org. When you are selecting a time server, remember the following:

- It is a good idea to select a couple of time servers to serve as backups in case groov RIO cannot establish a connection to the primary time server or if that time server becomes unavailable. The steps below instruct you to set two additional time servers.
- If you had set your date and time manually, setting the date and time as described in this section will overwrite your manual settings.

Note: Changing the time manually will log out any users that are currently signed into your groov RIO. Carefully choose when you will change the time to minimize any adverse affect on other users.

To select the primary time server and a few backups:

1. Log into groov RIO with a user ID that has administrator privileges.
2. Click System ( System), then Time ( Time).
3. In the Time Servers section, click Time Server 1. Enter the host name of the time server.
4. Click Time Server 2. Enter the host name of a second time server.
5. Click Time Server 3. Enter the host name of a third time server.
6. Click Set NTP. groov Manage displays a message while it's synchronizing with the time servers. When it finishes, the message disappears.

Now your date and time are set, as well as the time zone. The date and time will be updated automatically during the switches between Standard Time and Daylight Savings Time, according to the schedule set by the time servers.

Setting the Time and Time Zone by Selecting a Location

If you want to set the time by selecting your location, do the following steps:

1. Log into *groov* RIO with a user ID that has administrator privileges.
2. Click System ( System), then Time ( Time).
3. In the Time Zone section, click Region to select a general geographical area of the world.
To set the time for cities or regions in the United States of America, select America as the region. America encompasses North, Central, and South America.
4. Click Locality to select a specific city that most closely approximates the city within the time zone you want to set.
5. Click Set Zone. *groov* Manage displays a message while it's setting the time. When it finishes, the message disappears.

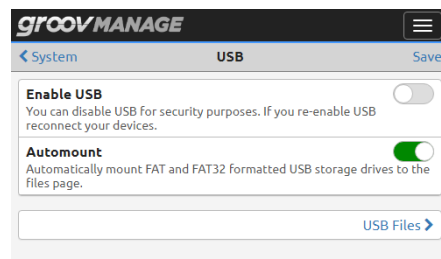
MANAGING THE USB PORT

groov RIO can work with any of the following devices inserted into the USB port:

- USB storage devices. Certain requirements must be met, as described in [“Requirements for USB Storage Devices” on page 89](#).
- USB-to-serial adapters. Only certain adapters are supported. You can find a list at [“Connecting Serial Devices” on page 87](#).
- WiFi adapters. Only certain adapters are supported. For a list, see [“Installing an Approved USB WiFi Adapter” on page 93](#).

If you do not plan on attaching any USB devices, it would be a good security practice to leave the USB port disabled. Disabling the USB port prevents any unauthorized access to RIO through the port. By default, the port is disabled, so if you plan on attaching any of the devices listed above, you need to enable the USB port. :

1. Log into *groov* RIO with a user ID that has administrator privileges.
2. Click System > USB.



3. Click the Enable USB slider so that it turns green.
4. Click Save. *groov* Manage returns you to the System page. Now you can:
 - Attach a USB storage device (see [“Attaching and Detaching a USB Storage Device” on page 89](#)).
 - Connect a serial device(s) (see [“Connecting Serial Devices” on page 87](#)).
 - Attach a WiFi adapter (see [“Installing an Approved USB WiFi Adapter” on page 93](#)).

CONNECTING SERIAL DEVICES

You can connect serial devices to *groov* RIO by inserting a USB-to-serial adapter into the USB port. Before you attach the adapter, make sure you enabled USB as described in [“Managing The USB Port” on page 87](#).

Note: Only Node-RED flows can access serial devices connected through a USB-to-serial adapter.

The following table lists USB-to-serial adapters supported by *groov* RIO.

Device Manufacturer	Model
B&B Electronics™	USOPTL4 (isolated RS-485)
	USPTL4 (non-isolated RS-485)
	USO9ML2 (isolated RS-232)
Gearmo®	GM-482422 (non-isolated RS-485/RS-422)
	GM-FTD1-A12 (non-isolated RS-232)
	SERIAL-B (non-isolated RS-232)

You can expand the number of serial devices you can connect to *groov* RIO by installing a USB hub to the USB port. When you do this, it's important to keep track of the device names and port numbers that *groov* RIO assigns to the USB-to-serial adapter that you plug into each USB port on the hub (see [“Understanding How *groov* RIO Assigns Port Numbers and Device Names When Using a Hub” on page 88](#)). One way to do this is:

1. Go to the Serial Devices page in *groov* Manage (Home > System > Serial Devices).
2. Insert an adapter into a port. *groov* Manage will detect the adapter, assign it a device name and port number, then refresh the page to show the information.
3. Make note of the device name and port number so that you have it handy as you develop Node-RED flows.

If you move a serial device from one USB port of the USB hub to another port on the hub, *groov* RIO assigns it a new port number, and possibly a new device name. These changes might require changes to your Node-RED flows.

Before you start connecting an adapter of USB hub to your RIO, see [“Managing The USB Port” on page 87](#).

Device Name and Port Number

groov RIO assigns `/dev/ttySer0` as the device name and 0 as the port number to the USB-to-serial adapter you plug into the USB port. You use the device name and port number in your Node-RED flow to access the serial device.

Understanding How *groov* RIO Assigns Port Numbers and Device Names When Using a Hub

If you connect a USB **hub** to the USB port, *groov* RIO includes a suffix to the device name and port number to identify the port number on the USB **hub**. For example, if you connect a 4-port USB hub to the USB port, then *groov* RIO assigns device names and port numbers as follows:

If a USB-to-serial adapter is plugged into port <i>x</i> of the USB hub...	<i>groov</i> RIO assigns it a device name of...	and a port number of...
1	<code>/dev/ttySer0.1</code>	0.1
2	<code>/dev/ttySer0.2</code>	0.2
3	<code>/dev/ttySer0.3</code>	0.3
4	<code>/dev/ttySer0.4</code>	0.4

IMPORTANT: If you move the adapter from one USB port on the USB hub to another USB port, *groov* RIO will assign a new port number and device name to the adapter. Any Node-RED flow that references the old port number and device name will need to be modified to refer to the new port number and device name.

Finding Device Names and Port Numbers

You can find device names and port numbers through *groov* Manage.

1. Log into your *groov* RIO with a user ID that has administrator privileges.
2. Click the menu button () , then click System.
3. Click Serial Devices. The Serial Devices page shows the device names and port numbers for any USB-to-serial adapter plugged into the USB port.

ATTACHING AND DETACHING A USB STORAGE DEVICE

You can attach a USB storage device to the USB port on *groov* RIO, then use *groov* Manage to copy files to and from its internal storage. Adding a USB storage device can also increase the amount of storage available for file activities like data logging.

Important: *You should store any critical files in the unit's internal storage. Internal storage utilizes a power-fail safe file system that prevents data, file and file system corruption in the event that power is removed. USB storage devices do not utilize a power-fail safe file system.*

Requirements for USB Storage Devices

groov RIO supports reading and writing to USB storage devices formatted in either FAT or FAT32 file systems. This means that *groov* RIO can not access partitions larger than 32 GB. If you want to read and write to a USB storage device that is larger than 32 GB, you must format (with a computer) that USB storage device with multiple FAT32 partitions. *groov* RIO will be able to read and write to all of the partitions on a properly formatted USB storage device.

Understanding How *groov* RIO Handles USB Storage Devices

In addition to the disabling the USB port (see [“Managing The USB Port” on page 87](#)), *groov* RIO provides another setting that helps manage security issues when dealing with USB storage devices: **Automount**. When this setting and **Enable USB** are enabled, when you attach a USB storage device, *groov* Manage has immediate access to its content. If you disable Automount (but leave Enable USB enabled), you will have to go through some extra steps to give *groov* Manage access to the content of a storage device.

Reviewing Security Issues with USB Storage Devices

If you do attach a USB storage device, keep the following points in mind:

- Because there is no mechanism to physically secure (or lock) the USB storage device to *groov* RIO, it can be removed by anyone that has access to the unit. It's important to apply important security practices, like keeping the unit secured under lock and key and providing the key to only trusted individuals.
- To prevent someone from inserting an unauthorized USB storage device that could contain malicious software, the Enable USB setting is disabled by default. Carefully consider the security risks before enabling this setting for an extended period of time.

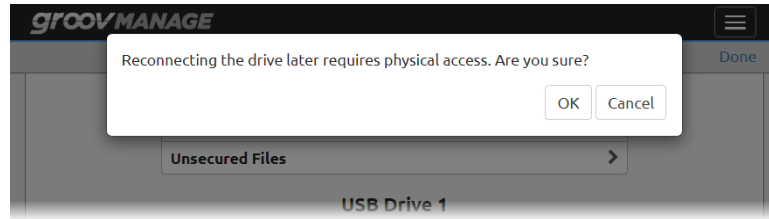
Disabling Access to USB Storage Devices

If you do not plan on using USB storage devices, it would be a good security practice to disable the ability to access USB storage devices. You can still use the USB port for other devices, like supported USB-to-serial adapters or WiFi adapters.

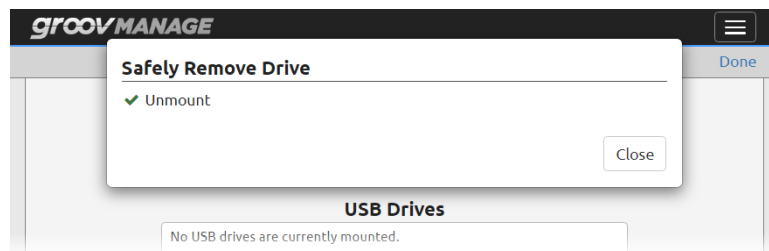
1. Log into your *groov* RIO with a user ID that has administrator privileges.
2. From the *groov* Manage Home page, click System > USB.

ATTACHING AND DETACHING A USB STORAGE DEVICE

3. If you have a USB storage device plugged into *groov* RIO, unmount it.
 - a. Click USB Files.
 - b. Click Safely Remove. *groov* Manage displays the following message; click OK to continue:



- c. When *groov* Manage successfully unmounts the storage device, it displays the following message. Click Close to continue.



4. Click the Automount slider so that it turns gray ().
5. Click Save. *groov* Manage displays the System page.

groov Manage no longer has automatic access to the contents of a USB storage device inserted into the USB port. However, as long as Enable USB is enabled, it can work with USB-to-serial adapters and WiFi adapters.

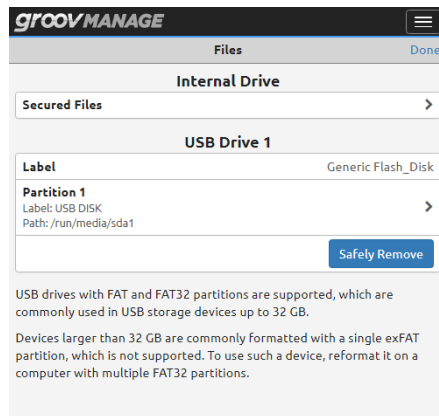
Attaching a USB Storage Device

Before you attach a USB storage device, make you understand:

- ["Requirements for USB Storage Devices" on page 89](#)
- ["Reviewing Security Issues with USB Storage Devices" on page 89](#)

Also, make sure you have Enable USB (see ["Managing The USB Port" on page 87](#)) and Automount (see ["Understanding How groov RIO Handles USB Storage Devices" on page 89](#)) enabled.

Insert the USB storage device into the USB port. To verify that *groov* Manage has access to the USB storage device, from the *groov* Manage Home page, click System > Files. *groov* Manage displays the Files page. *groov* Manage lists the USB storage device in a section called USB Drive, typically followed by a number:



You can now copy, move, and download files (see [“Copying, Moving, or Downloading a File on a USB Storage Device” on page 92](#)).

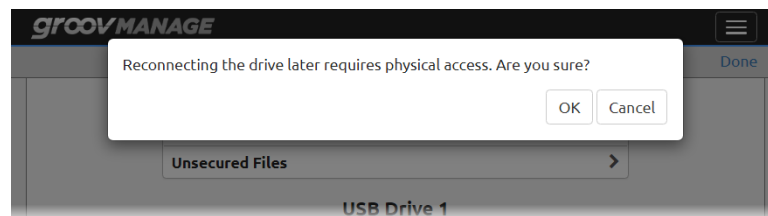
Detaching a USB Storage Device

Before you detach a USB storage device, evaluate the consequences; for example, would it cause an interruption to your data logging process? After evaluating the consequences and taking measures to mitigate those consequences, unmount the device and then remove it.

1. Log into your *groov* RIO with a user ID that has administrator privileges.
2. From the *groov* Manage Home page, click System > USB, then USB Files.
3. Click Safely Remove.

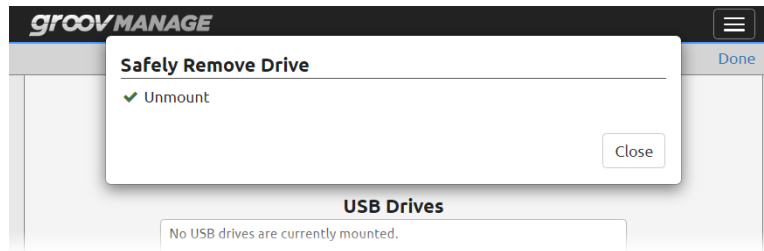
If *groov* Manage detects that a file on the USB storage device is still being used by a service, it will not proceed. One likely service that might be using the storage device is a Node-RED flow that is logging data to the storage device. Check any services that might be using the storage device.

Otherwise, *groov* Manage displays the following message, which reminds you that if you want to reconnect the storage device in the future, you will have to physically reinsert it. Click OK to continue:



ATTACHING AND DETACHING A USB STORAGE DEVICE

When *groov* Manage successfully unmounts the storage device, it displays the following message. Click Close to continue.



4. Click Done in the Files page.
5. Physically remove the USB storage device from the USB port.
6. Verify that the device no longer shows up in *groov* Manage.

If you do not plan on attaching USB storage devices for an extended amount of time, disable Automount to prevent *groov* Manage from automatically accessing content on any storage device inserted into the USB port (see [“Reviewing Security Issues with USB Storage Devices” on page 89](#)).

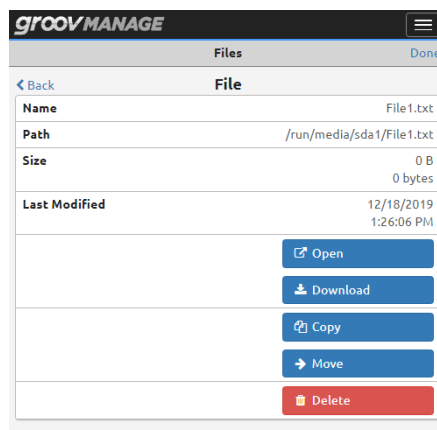
Copying, Moving, or Downloading a File on a USB Storage Device

Before you begin, make sure you have properly mounted the USB storage device as described in [“Attaching a USB Storage Device” on page 90](#).

- Copy and move means to transfer a file from the USB storage device to *groov* RIO’s internal storage.
- Download means to transfer a file from the USB storage device to your computer or mobile device.

These instructions describe how to copy, move, or download one file at a time.

1. Log into your *groov* RIO with a user ID that has administrator privileges.
2. From the *groov* Manage Home page, click System > USB, then USB Files.
3. Click on Partition 1, or, if you have multiple partitions on the USB storage device, scroll to the correct partition and click the partition name.
4. In the Dir Listing section, navigate to the folder that has the file you want to copy, move, or download.
5. Click on the file name. *groov* Manage displays a list of all the actions you can take on the file:



- To copy a file to RIO’s internal storage, click Copy.
- To move a file to RIO’s internal storage, click Move.

- To download a file to the computer or mobile device, click Download.
- 6. Click Back (top left).
 - If you need to copy, move, or download another file, repeat [step 4](#) and [5](#).
 - If you are done copying, moving, or downloading files, click Done (top right corner). *groov* Manage returns you to the USB page.

INSTALLING AN APPROVED USB WIFI ADAPTER

If you want to connect your *groov* RIO to a wireless network, Opto 22 recommends that you purchase and install one of the following USB WiFi adapters, which Opto 22 has tested and verified works with *groov* RIO. Unverified WiFi adapters should not be used.

Device Manufacturer	Model
ALFA	AWUS036ACS
Netgear	AC1200 (A6150)
Netis	WF2180 WF2190
Panda Wireless	PAU0A AC600 PAU0D AC1200
Linksys	AE6000
TP-Link	Archer T1U
Sabrent	AC600

Collect the following information before starting:

- SSID of the wireless network.
- Encryption method required to access the wireless network.

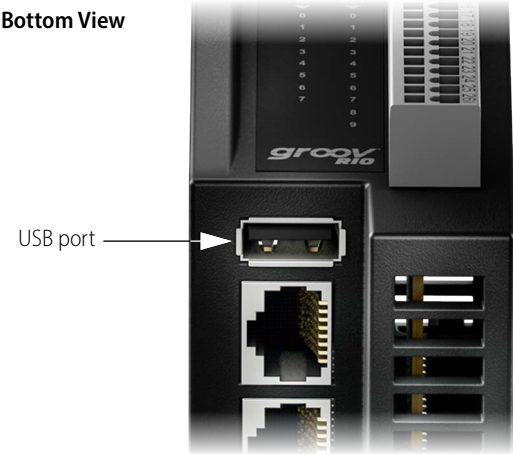
If you are manually assigning an IP address, make sure you also have the IP address and subnet mask you want to assign to the unit.

Also, make sure you have enabled the USB port (see [“Managing The USB Port” on page 87](#)).

1. Log into your *groov* RIO with a user ID that has administrator privileges.
2. Insert the WiFi adapter into the USB connector on the bottom of the unit.

Note: If you have a USB storage device inserted into the port, make sure you remove it according to the instructions in [“Detaching a USB Storage Device” on page 91](#).

ENABLING Node-RED



3. In *groov* Manage, go to the Network page (Home > System > Network). If the Wi-Fi section of the Network page now has a MAC Address, then *groov* RIO is communicating with the WiFi adapter.

No WiFi adapter inserted; no MAC address

Subnet Mask		192.168.1.0/24
Gateway 1		192.168.1.1
Wi-Fi		
Link Status	Disconnected	
MAC Address		
IPv4 Method	Disabled	
OpenVPN Tunnel 0		
Link Status	Disconnected	

WiFi adapter installed; MAC address available

Subnet Mask		192.168.1.0/24
Gateway 1		192.168.1.1
Wi-Fi		
Link Status	Connected	
MAC Address	30:23:03:D9:22:FD	
IPv4 Method	Disabled	
OpenVPN Tunnel 0		
Link Status	Disconnected	

Note, however, WiFi is disabled. The next step is to enable WiFi.

4. Click Configure (top right corner of the Network page).
5. In the Wi-Fi section, click Disabled.
6. In the IPv4 Method window, click the connection method you want: Automatic (DHCP) or Manual.
7. Enter the information you collected.
8. Click Save. Read the message that *groov* Manage displays and click OK. After *groov* Manage verifies the information and saves the configuration, it displays the network page.

Subnet Mask	192.168.1.0/24
Gateway 1	192.168.1.1
Wi-Fi	
Link Status	Connected
SSID	doc
MAC Address	30:23:03:D9:22:FD
IPv4 Method	Automatic (DHCP)
IP Address	192.168.1.10
Subnet Mask	255.255.255.0
Gateway 2	192.168.1.1
OpenVPN Tunnel 0	
Link Status	Disconnected

groov RIO is now connected to your wireless network.

ENABLING Node-RED

Node-RED is an open-source, multi-platform software program, where you connect (*wire*) together devices, databases, cloud applications, and APIs (application programming interfaces) to create simple logic flows to accomplish specific goals. It is pre-installed on your *groov* RIO; you do not have to download and install it on a

computer or embedded device. You just have to enable it, then start creating Node-RED flows. This tight integration also means that some RIO functions, like backup, apply to your Node-RED projects.

By default, Node-RED is disabled. To enable it:

1. Log into your *groov* RIO with a user ID that has system administrator privileges.
2. In the *groov* Manage Home page, click Node-RED.
3. Click Enable. After the Status field says Running, wait a few seconds before opening the Node-RED Editor.

UPLOADING FILES TO *groov* RIO'S INTERNAL FILE SYSTEM OR USB STORAGE DEVICE

groov RIO identifies files that you upload as “user files”. You can store files in:

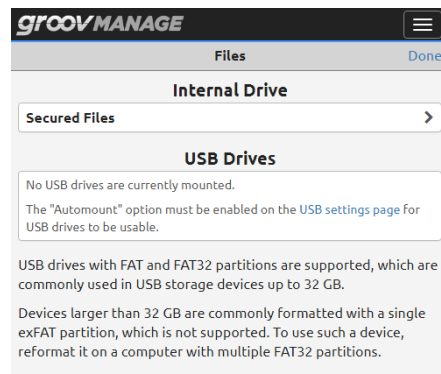
- The “secured area” of the internal file system, where only services with authentication (for example, a user name and password, or an API key) over a secure protocol (HTTPS) can access the files.
- A USB storage device attached to the USB port of your RIO. Before you attach a USB storage device to the USB port, review “[Managing The USB Port](#)” on [page 87](#) to make sure *groov* Manage can access the storage device.

Note that when you backup your system:

- Only the first 10 MB of files that you uploaded are included in the backup file.
- The files stored on the USB storage device are not included in the backup file.

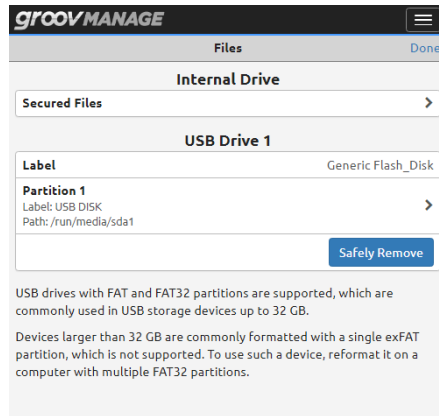
When *groov* Manage performs a backup, it lists all the files it included into the backup file in the *groov* Manage log file. You can check the log file to determine which other files you need backup by other means. (See “[Backing up Your groov RIO Settings](#)” on [page 149](#).)

1. Log into your *groov* RIO with a user ID that has administrator privileges.
2. Click System > Files. *groov* Manage displays the Files page.



If you had correctly mounted a USB storage device, it would appear in the USB Drives section, like this:

CONFIGURING groov RIO FOR SHELL ACCESS



3. Upload a file.

To the internal file system, click Secured Files > Upload File.

To the USB storage device, click the name of the partition where you want to store the file, then click Upload File.

- a. Navigate to the folder that contains the file you want to upload and select that file.
- b. Click Open. *groov* Manage uploads the file and then refreshes the Dir Listing section to list the file you just uploaded.
- c. If you need to upload another file, click Upload File and repeats steps a and b. For USB storage devices, if you need to upload another file to another partition, click Back, select the other partition, click Upload File and then repeats steps a and b.

When you are done uploading files, click **Done**.

CONFIGURING *groov* RIO FOR SHELL ACCESS

Accessing *groov* RIO through the secure shell is for advanced programming. Opto 22 provides a wealth of information on our developer website (developer.opto22.com).

IMPORTANT: Be aware that Opto 22 provides very limited support if you choose to connect to and run through SSH.

The only configuration needed is to obtain and upload the *groov* RIO SSH Access license file:

1. If you haven't already done so, purchase the free [GROOV-LIC-SHELL](#) license from our website. After you complete your purchase, you will receive an Activation key by email.
2. Make a note of the serial number of your *groov* RIO, which is on a label attached to the side of the module. The Serial Number is a string of numbers preceded by "SN:". (For an example, see [page 18](#).)
3. On a computer or mobile device connected to the Internet, go to manage.groov.com.
 - If you do not have a MyOpto account, fill out the fields under "Register" and click Register. Follow the rest of the instructions online to complete your registration. Click Manage groov (on the lower left side) and update your *groov* User Registration information, if requested, then click Submit.
 - If you do have a MyOpto account, log in. Update your *groov* User Registration information, if requested, and click Submit.
4. Click Activate.
5. Type in the Activation key and click Activate.

HP PRODUCTS SUPPORT ABOUT US COMMUNITY SEARCH

SUBSCRIBE

← **Activate groov**

Your Activation Key is in the certificate packed in the box with your *groov*, or sent to you by mail or email when you bought your *groov* product.

Enter your activation key:

ACTIVATE

This key unlocks additional functionality for one of your *groov* products. **Choose a groov type below.**

☐ groov EPIC ☐ groov RIO

- Click groov RIO.

HP PRODUCTS SUPPORT ABOUT US COMMUNITY SEARCH

SUBSCRIBE

← **Activate groov**

Your Activation Key is in the certificate packed in the box with your *groov*, or sent to you by mail or email when you bought your *groov* product.

Enter your activation key:

ACTIVATE

This key unlocks additional functionality for one of your *groov* products. **Choose a groov type below.**

☐ groov EPIC ☒ groov RIO

- Type in the serial number you noted in [step 2](#) and click Submit.

HP PRODUCTS SUPPORT ABOUT US COMMUNITY SEARCH

SUBSCRIBE

← **Activate groov**

Your Activation Key is in the certificate packed in the box with your *groov*, or sent to you by mail or email when you bought your *groov* product.

Enter your activation key:

ACTIVATE

This key unlocks additional functionality for one of your *groov* products. **Choose a groov type below.**

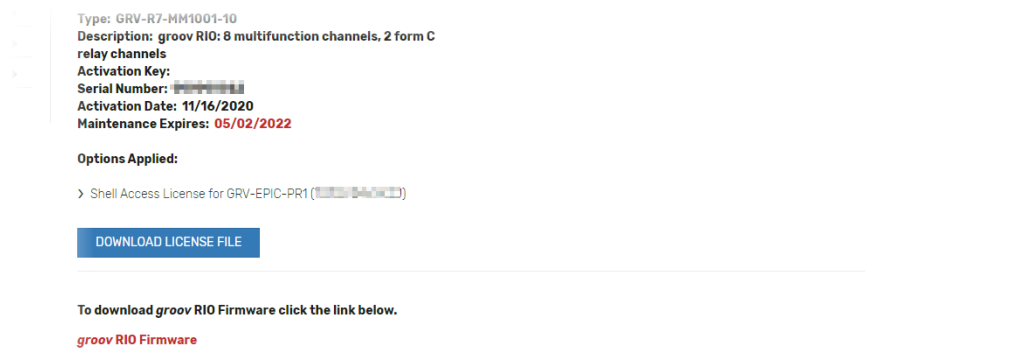
☐ groov EPIC ☒ groov RIO

Enter the serial number of your groov RIO.

SUBMIT

- Review the terms of unlocking Shell Access on *groov* RIO and click Apply to accept the terms.
- Click Download License File to save the license file onto your computer or mobile device and remember where you saved it.

CONFIGURING groov RIO FOR SHELL ACCESS



10. In another browser window or tab on your currently open browser window, log into your *groov* RIO with a user ID that has administrator privileges.
11. From the *groov* Manage Home page, click System > License.
12. Click Upload license, then navigate to the folder where you stored the *groov* RIO SSH Access license file. Make note of the IP address and port number listed underneath. Connect to the shell through whatever SSH client you prefer.

8: Configuring I/O

SELECTING FUNCTIONS, SIGNALS, AND FEATURES

Before you can configure your I/O, you need to know which channel is going to serve which function and signal, plus select which features (if available) you need:

- Function: Input or output.
- Signal: Analog or discrete.
- Feature: On State, Off State, Linearization, etc. for those signals that offer features. (For a complete list of features, see [Appendix A: Specifications](#).)

Note that for CODESYS applications, only a limited set of features are available. The instructions will indicate which features are available for CODESYS applications.

If you have not determined this yet, here are a couple of options to help you select the right combination:

- **groov RIO Explorer**— An Opto 22 web app that can help you select a combination of functions, signal types, and features, and make sure you select channels that can support your choices. When you finish with the *groov* RIO Explorer, you can save a wiring diagram, which will come in handy when it's time to wire up your devices. Another way to you can use the wiring diagram is to annotate it with specification information like ranges and scaling for analog inputs, or feature selections for discrete inputs. To learn how to use the *groov* RIO Explorer, see [Appendix C: groov RIO Explorer](#).
- **Reviewing spec tables, feature tables, and wiring diagrams**—Review the information in [Appendix A: Specifications](#) and [Appendix B: Wiring Diagrams](#) as you follow these steps:
 - a. Review the features table to select which function, signal type, and, if applicable, which feature you want for each channel. If you are working with CODESYS Development System, check the table on [page 108](#) for the list of features supported in that environment. You might find it helpful to note your selections in a table like the one on the following page:

SELECTING A METHOD FOR CONFIGURING I/O

	Function (Input or Output)	Signal Type (Analog or Discrete)	Feature (if applicable)	Default Values or Specific Settings (if applicable)
Channel 0				
Channel 1				
Channel 2				
Channel 3				
Channel 4				
Channel 5				
Channel 6				
Channel 7				
Channel 8				
Channel 9				

- b. For each channel, check the corresponding section of the specification table and verify that you've correctly selected everything. For example, if you selected a discrete input with a counter feature for channel 0, go to the "Discrete Counter Input" section of the chart and verify that channel 0 is within the range listed for "Available Channels". Also check that the signal that is coming in (for inputs) or leaving (for outputs) meets the specifications listed.
- c. Review the wiring diagrams and check for any additional requirements; for example, any fusing requirements. It may be helpful to print relevant wiring diagrams and annotate them with information you collected in the previous two steps or additional information you may need when it's time to wire your field devices.

Taking the time to check your selections will make it less likely that you'll run into trouble later on, and save you time.

SELECTING A METHOD FOR CONFIGURING I/O

There are several ways to configure I/O. For whichever way you select, you'll want to have the information you collected in ["Selecting Functions, Signals, and Features" on page 99](#) handy. This information can speed up the configuration process.

- *groov* Manage: If you are using your RIO unit as an edge node, where you'll just be transmitting tags to a cloud service through MQTT or through Node-RED flows, you'll want to configure your I/O through *groov* Manage (see ["Configuring I/O Through *groov* Manage"](#) below).
- PAC Control: If you are adding your RIO as an I/O unit to a PAC Control strategy, you'll want to follow the instructions in the [PAC Control User's Guide](#) (form 1700) instead of the instructions in this chapter.
- CODESYS Development System: If you are adding your RIO as a remote I/O unit to a CODESYS application, you'll want to follow the directions in ["Configuring I/O Through CODESYS Development System" on page 103](#).
- OptoMMP: You'll want to review the [OptoMMP Protocol Guide](#) (form 1465) to learn the memory map locations used for I/O configuration.

Note: You cannot use these methods in combination. Any configuration you make through one method can overwrite configurations made through another method.

CONFIGURING I/O THROUGH *groov* MANAGE

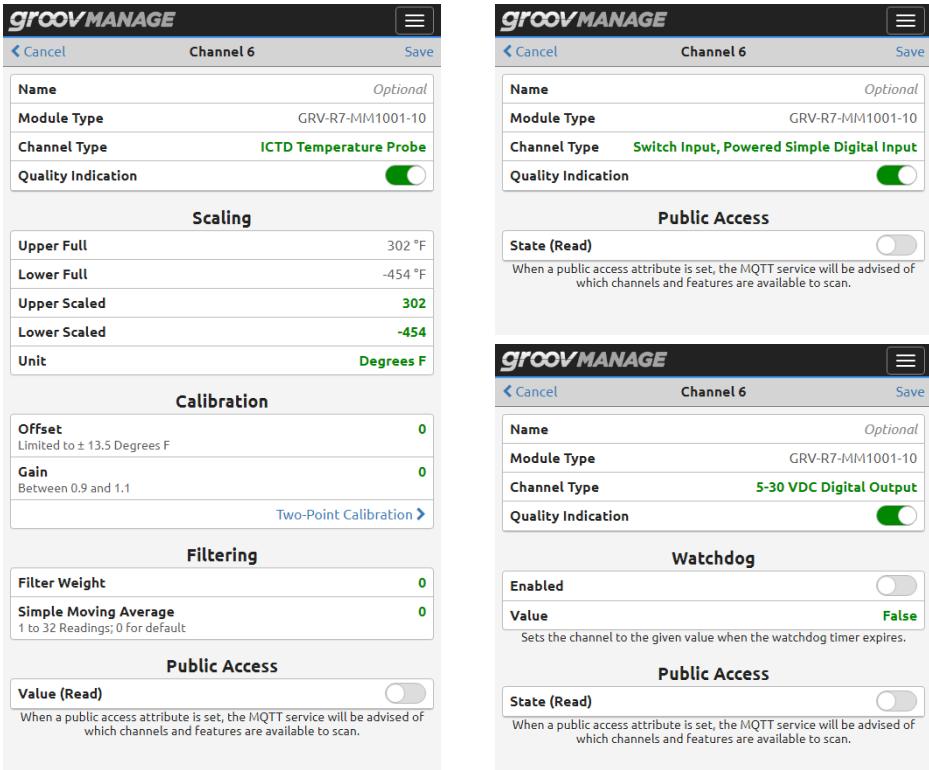
1. Log into your *groov* RIO with a user ID that has administrator privileges.
2. From the *groov* Manage Home page, click I/O Channels. The I/O Channels page displays a quick summary of channel configurations. If you are configuring channels for the first time, the page looks like this:

groovMANAGE		
I/O Channels		
0	< no name >	>
DI	OFF	
1	< no name >	>
DI	OFF	
2	< no name >	>
DI	OFF	
3	< no name >	>
DI	OFF	
4	< no name >	>
DI	OFF	
5	< no name >	>
DI	OFF	
6	< no name >	>
DI	OFF	
7	< no name >	>
DI	OFF	
8	< no name >	>
DO	OFF	
9	< no name >	>
DO	OFF	

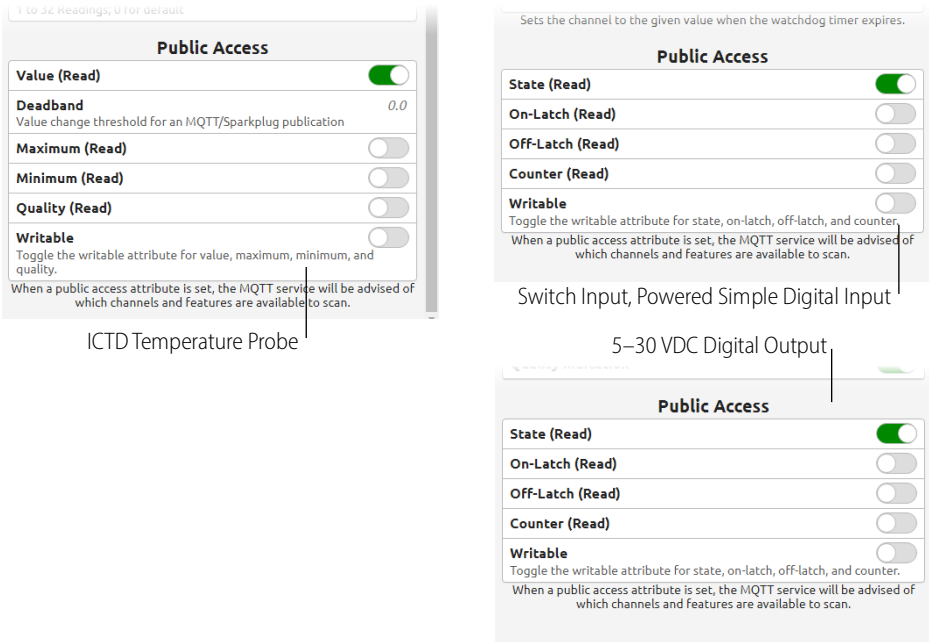
3. With each channel, do the following:
 - a. Click a channel.
 - b. Click Configure.
 - c. Assign a Name to help you quickly and uniquely identify this channel and to help you differentiate it from other channels that might be configured similarly. This is optional.
 - d. Click Channel Type and select a value. Review the information you collected for that channel to select the correct one.

CONFIGURING I/O THROUGH groov MANAGE

Depending on the channel type you select, *groov* Manage may change the content of channel page. The following images show a few examples of how the page changes depending on the channel type you select:



- e. If you are transmitting values through MQTT, you want to enable the Value (Read) switch in the Public Access section. When you do, *groov* Manage displays another set of switches to help you identify the specific values you want available to send, as well as whether to make them writable.



- f. Review the rest of the fields on the channel page and make changes based on the needs of your application. For example, you may want to set a Watchdog timer on a channel or set the scaling values for a temperature probe.
- g. Click Save. *groov* Manage displays the channel page with information based on your selected channel type. For the same examples shows in [step d](#), this is what the channel page may look like:

Note that the above image shows channel 6 configured to sense from an ICTD temperature probe. However, an actual probe has not been wired to channel 6 on this RIO, which means that RIO is sensing values that are out of range from this configuration. RIO reports this as a quality error.

When you are done configuring all your channels, *groov* Manage displays your selections on the I/O Channels page.

If you haven't already done so, wire your field devices to your RIO as described in ["Wiring Field Devices" on page 11](#).

CONFIGURING I/O THROUGH CODESYS DEVELOPMENT SYSTEM

After you add the Opto 22 Library Package for CODESYS Development System, you can add *groov* RIO (and *groov* EPIC) devices to your CODESYS projects. In CODESYS, a *groov* RIO is an Ethernet device, and each channel is a device you "plug" into that Ethernet device. To select the signal types and features for each channel, you configure the parameters of the device you "plugged in". To differentiate between the *groov* RIO "device" and the channel "device", we will include "(*groov* RIO)" or "(channel)" after each reference to "device", as necessary. You may also want to read the note below for more clarification on terminology differences.

Here's what you need to do to configure I/O through CODESYS Development System:

1. Verify that you have the correct version of the Opto 22 Library Package, CODESYS Development System, and *groov* RIO firmware. For guidance on what to check, see ["Checking Compatibility Between Library Package, Development System, and Firmware" on page 86](#).
2. Add the RIO to your CODESYS project.
3. Add channels by "plugging in" devices.

4. Select the signal types and configure the features for each channel by editing the “plugged in” device’s parameters.

Note on terminology: Throughout this chapter, instructions may use CODESYS terminology that differs from standard Opto 22 terminology. For example:

- In the CODESYS Development System interface, the term “device” refers to many different objects: a controller, an Ethernet adapter, a field device, or an I/O module. In this guide, “device” typically refers to a field device (a valve, a pump, a quadrature encoder, etc.). The following chapters use the CODESYS definition of “device”:

- [Chapter 12: Configuring CODESYS and groov RIO for IEC61131-3](#)
- [Chapter 13: Working with groov RIO Devices in CODESYS Projects](#)

All other chapters of this guide use the Opto 22 definition of “device”.

- In CODESYS terminology, a *groov* EPIC processor, a *groov* RIO, and channels on a *groov* RIO are referred to as “devices”; the following chapters use this definition:

- [Chapter 12: Configuring CODESYS and groov RIO for IEC61131-3](#)
- [Chapter 13: Working with groov RIO Devices in CODESYS Projects](#)

All other chapters of this guide refer to a *groov* EPIC processor as a processor, a *groov* RIO as a *groov* RIO module, and a channel as a channel.

- An “application,” in CODESYS terminology, is roughly equivalent to a PAC control strategy in Opto 22 terminology.

Checking Compatibility Between Library Package, Development System, and Firmware

The CODESYS Development System offers a rich and broad range of support for devices. As with any robust development system, it’s important to keep up-to-date with releases and review the features, enhancements, and fixes included in each release, as well as diligently check for compatibility with related software and firmware. In the CODESYS development environment, it’s important to check compatibility between three main pieces:

- **Opto 22 Library Package for CODESYS Development System.** The package contains information for CODESYS Development System so that it can configure *groov* EPIC processors, *groov* I/O modules, and *groov* RIO modules. Opto 22 updates the package each time a new module is introduced, as well as to deliver , and bug fixes. You want to review the readme to learn:
 - Which version of the package delivered support for the *groov* I/O or RIO module you want to use in your application.
 - The features, enhancements, or bug fixes delivered in each version of the package.
 - The pre- or co-requisites (for example, a new version of firmware for a *groov* I/O or RIO module) that might be required by one of these features, enhancements, or bug fixes.
 - Whether the package requires an updated version of the CODESYS Development System.

You should periodically check the Opto 22 website for updates to the package. For instructions on installing the latest version of the package into CODESYS Development System, see [“Updating Device Information with the Latest Version of Opto 22 Library Package” on page 105](#).

- **CODESYS Development System.** The Development System periodically releases features, enhancements, and bug fixes that may affect how it works with library packages and with device firmware. It’s important to check that you are running with a version of CODESYS Development System that is compatible with the Opto 22 Library Package. To check the version number, see the CODESYS online help.
- **groov RIO Firmware.** Opto 22 updates the firmware to add enhancements and features or to fix bugs. Make sure to check the Readme file to learn whether it’s compatible with the version of the Opto 22

Library Package installed in your CODESYS Development System. If you need to update RIO firmware, see [“Updating Firmware on a groov RIO” on page 154](#).

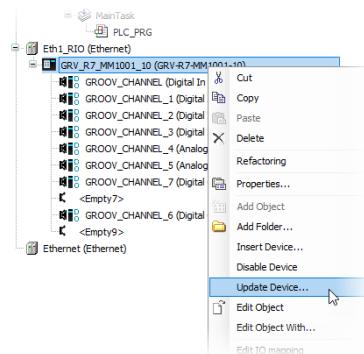
Updating Device Information with the Latest Version of Opto 22 Library Package

If this is the first time you are adding a *groov* RIO device to your project, you only have to do steps 1, 2, 10, and 11. If you are updating existing RIO devices in your projects, do all of the steps.

1. Download and install the latest version of the library package from our website.
 - a. Go to the Opto 22 website, www.opto22.com.
 - b. Enter “Opto 22 Library Package” in the search box to find the page “Opto 22 Library Package for CODESYS Development System” and click the link.
 - c. Click Download and save the package to the same computer where you installed CODESYS Development System.
 - d. Open CODESYS Development System and install the package. For instructions on how to do this, see [Installing/Uninstalling a Package](#) in the CODESYS Online Help.
2. Review the readme for the Opto 22 Library Package for CODESYS Development System. Pay particular attention to the following:
 - If the package requires a newer version of CODESYS Development System than your current version, install the new version before proceeding further.
 - Make note of any additional tasks you may have to do after updating device information; for example, installing a new version of RIO module firmware.

Remember: If you are adding a groov RIO device for the first time, you can skip down to step 10.

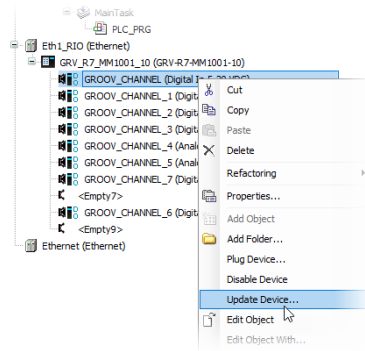
3. Open your CODESYS project and, in the Device tree, expand the RIO device to see all the channels.
4. Right-click the RIO device and select Update Device.



5. If the Update Device window does not automatically select the correct RIO device, navigate through the window to find it and select it.
6. Click Update Device.

CODESYS Development installs the new information about the RIO device. Now you need to update device information for each channel:

7. Right-click on a configured channel on the RIO device and click Update Device.

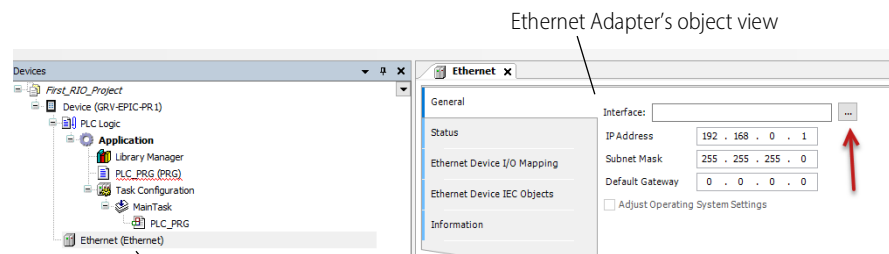


8. In the Update Device window, select the same device type (if it's not already selected). If applicable, choose the highest version number. Click Update Device.
9. Repeat [step 7](#) and [step 8](#) for each channel on the RIO.
10. Save your project.
11. If you noted any additional tasks in [step 2](#), make those changes now. Then, rebuild your project, test the changes, and verify that your application works as expected.

Adding a groov RIO to a CODESYS Project

Before you begin, verify that the PLC and the RIO are on the same network.

1. Open CODESYS Development System.
2. Open your project. (Click File > Open Project. Navigate to the folder where you stored the project file, select the project file, and then click Open.)
3. Add an Ethernet adapter to your PLC. With this adapter, you will identify which port on the RIO communicates to the PLC.
 - a. Right-click on your PLC.
 - b. Click Add Device.
 - c. Under Fieldbusses, expand Ethernet Adapter, then click Ethernet.
 - d. Click Add Device.
 - e. Click Close.
 - f. Double-click the Ethernet adapter to open the Ethernet Adapter's object view.
 - g. Click the More button () next to the Interface field.



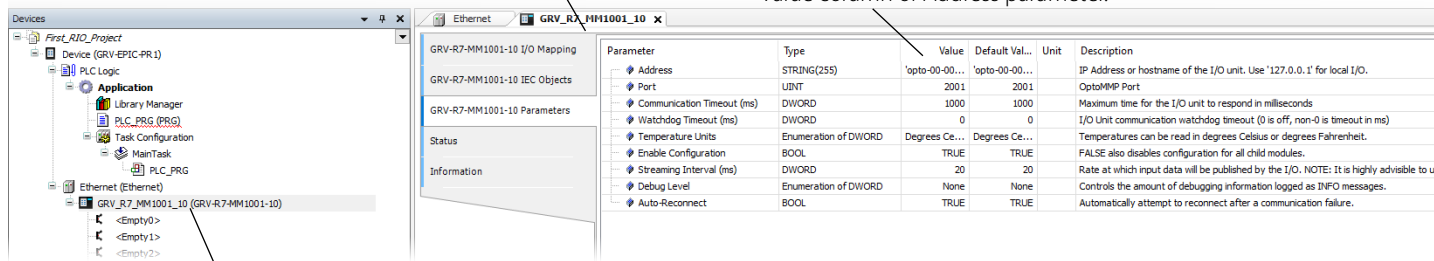
The Ethernet Adapter added in steps [a](#) through [e](#).

- h. Select eth0 or eth1, whichever port is connected to the network.
- i. Click OK.

4. Add the RIO to the Ethernet adapter:
 - a. Right-click on the Ethernet adapter you just added.
 - b. Click Add Device.
 - c. Expand Miscellaneous and select a RIO by its part number. For example, GRV-R7-MM1001-10.
 - d. Click Add Device.
 - e. Click Close.
5. Assign the RIO's IP address to the address parameter of the device.
 - a. Double-click the RIO device you just added. CODESYS Development System opens the object view. If the Parameters tab is not selected, then select it.
 - b. Click on the Value column for the Address parameter. Enter either the hostname or the IP address of the RIO, surrounded by single quotes.

Object view of the RIO device added in step 4.

Value column of Address parameter.



The RIO device added in step 4.

- 6.** Save your project.

Adding Channels and Selecting Signal Types (Plugging in Devices)

To configure a channel, you “plug in” a device to your RIO. Now is when you need the information you collected when you reviewed [“Selecting Functions, Signals, and Features” on page 99](#).

1. Right-click on a channel (empty slot) and select Plug Device.

Remember to pay careful attention to the channel you select; remember that not all channels support all functions, signal types, or features.

2. In the Plug Device window, expand Miscellaneous, then select which signal you want to assign to that channel (device).

- 3.** Click Plug Device.

You can continue adding/configuring channels by clicking on another channel, selecting a signal type in the Plug Device window, then clicking Plug Device.

4. Click Close when you are done.

Changing Signal Types (Updating Devices)

If you want to change signal type you assigned to a particular channel (device):

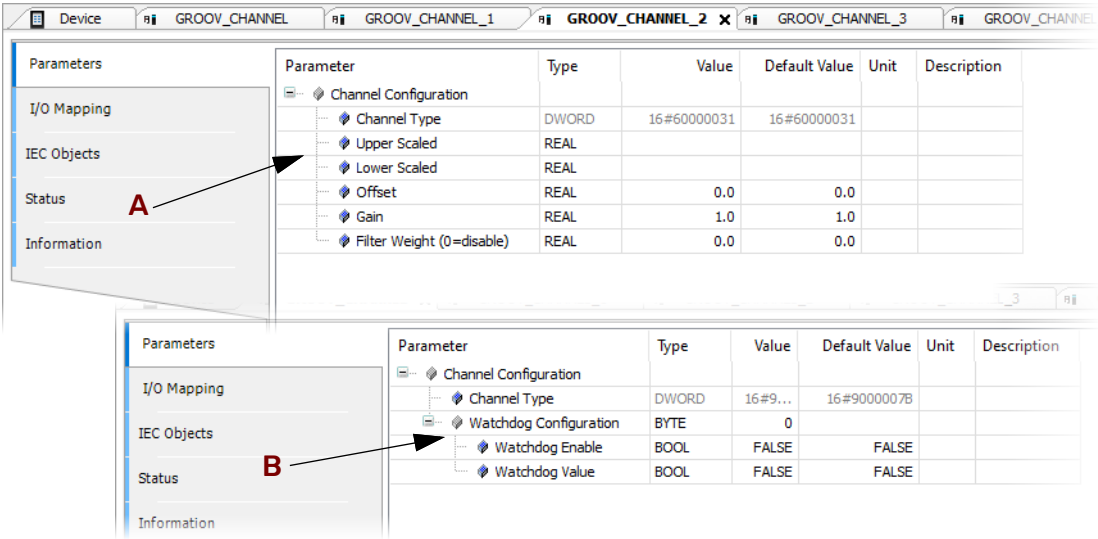
1. Right-click on the channel and select Update Device.
2. In the Update Device window, expand Miscellaneous, then select the new signal you want to assign to that channel (device).
3. Click Update Device.

You can continue changing signal types by clicking on another channel (device), selecting a new signal type in the Update Device window, then clicking Update Device.

4. Click Close.

Setting Features (Configuring Object Parameters)

In CODESYS Development System, a *groov* RIO feature is identified as an object’s parameter. For example, an analog ICTD Temperature signal has several features, which are listed in the table on [page 108](#). In CODESYS Development System, you would see these features listed as parameters in the Parameters tab of the object view.



- A** Features for an ICTD signal on a channel of a GRV-R7-MM1001-10. Compare the parameters list with the list of features on the table for an analog input ICTD signal. All but two features are available on CODESYS.
- B** Features for a digital output signal on channel 0 of a GRV-R7-MM1001-10. Compare the parameters list with the list of features on the table for a digital output DC sinking signal. Only one feature is available on CODESYS: Watchdog Timeout Value.

The following table lists the features for the functions and signal types that you can select and configure on a GRV-R7-MM1001-10.

Function	Signal Types	Features
Input Channels	Digital	- Digital - Switch Input, powered Channels 0-7: - On/Off State Channels 0 & 1: - Counting
	Analog	- Voltage - Current - ICTD - Thermocouple - Millivolt - Scaling - Offset and Gain - Average Filter Weight

Function	Signal Types	Features
Output Channels	Digital	• DC Sinking • On/Off State • Watchdog Timeout Value
	Analog	• Current • Voltage • Scaling • Clamping • Watchdog Timeout Value
	Mechanical Relay	• Form C-NO • Form C-NC • On/Off State • Watchdog Timeout Value

For a list of the signal types and features for all RIO models, see [Appendix A: Specifications](#). If a feature listed in that appendix is not listed in the Parameters tab of the object view, the feature is not configurable through CODESYS Development System.

Configuring Channel Features (Device Parameters)

1. If you haven't started CODESYS Development System, start it and open your project.
2. Open or select the Devices view, then expand the Ethernet branch of your *groov* RIO.
3. Double-click the device (channel) you want to configure. CODESYS Development System opens the object view for that device. Check that the Parameters tab is selected.
4. Find the parameter (feature) you want to configure:
 - **For devices (channels) with scaling:** If you want to set scaling values, first determine the upper and lower ends of the scale. For example, if your input range is ± 150 mV and it is connected to a tank that can hold 1000 liters, you can set the lower end of the scale (-150 mV) to represent 0 liters and the upper end of the scale ($+150$ mV) to represent 1000 liters. With a signal type of Analog In ± 150 mv (for example, on a GRV-R7-MM1001-10):
 - On the Upper Scaled row, double-click the Value cell and enter 1000.
 - On the Lower Scaled row, double-click the Values cell and enter 0.
 To set default scaling, leave the Value cells blank or enter 0.
 - **For devices (channels) with clamping:** If you want to limit the output sent out from the device (channel), first determine the upper and lower end of that range. For example, suppose you want the output range to be 5–15 mA. On a signal type of Analog Out 0-20 mA (for example, on a GRV-R7-MM1001-10), to limit the range to 5–15 mA:
 - On the Upper Clamp row, double-click the Value cell and enter 15.
 - On the Lower Clamp row, double-click the Value cell and enter 5.
 To set no clamping, set both Values cells to 0.

- **For devices (channels) with counting:** If you want to use the counting feature, you must select it. On the Feature row, double-click the Value cell to display the drop-down arrow.

Parameter	Type	Value	Default Value	Unit	Description
Channel Configuration					
Channel Type	DWORD	16 #50000068	16 #50000068		
Feature	Enumera...	None	None		

Click the arrow to display a list, then select Counter.

Parameter	Type	Value	Default Value	Unit	Description
Channel Configuration					
Channel Type	DWORD	16 #50000068	16 #50000068		
Feature	Enumera...	None	None		

5. Repeat [step 4](#) for each device (channel) you want to configure.

Remember to save your project periodically.

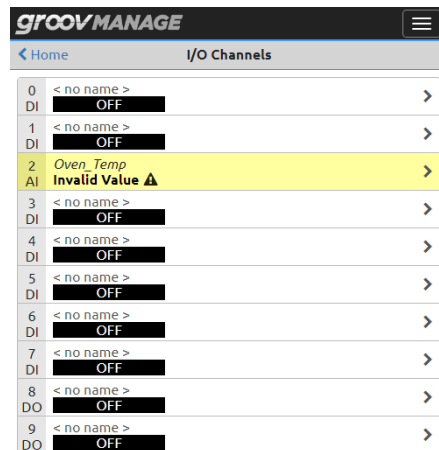
If you haven't already done so, wire your field devices to your RIO as described in ["Wiring Field Devices"](#) on [page 11](#).

UNDERSTANDING HOW QUALITY ERRORS ARE REPORTED

Some signal types on a *groov* RIO can report quality errors, which are common errors like input values that are out of range. *groov* Manage can show you that there is a quality error in the I/O Channels page by highlighting the channel yellow and showing brief message about the quality error.

Viewing Information About a Quality Error

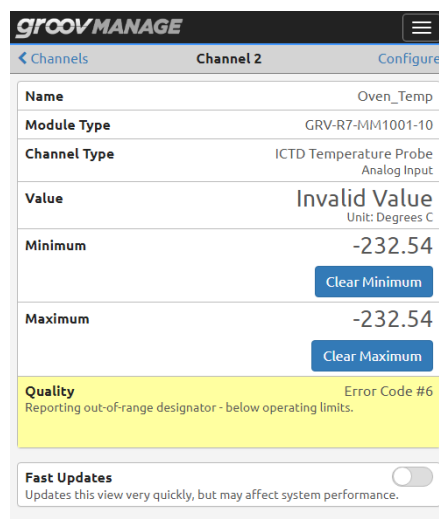
1. Log into your *groov* RIO with a user ID that has administrator privileges.
2. Click I/O Channels. *groov* Manage displays the list of channels and highlights the channel that is reporting the quality error with a yellow background.



GROOVMANAGE		Menu
< Home		I/O Channels
0	< no name > DI OFF	>
1	< no name > DI OFF	>
2	Oven_Temp AI Invalid Value ⚠	>
3	< no name > DI OFF	>
4	< no name > DI OFF	>
5	< no name > DI OFF	>
6	< no name > DI OFF	>
7	< no name > DI OFF	>
8	< no name > DO OFF	>
9	< no name > DO OFF	>

Click on that channel.

3. *groov* Manage displays the specific information about that channel:



GROOVMANAGE		Menu
< Channels		Channel 2 Configure
Name	Oven_Temp	
Module Type	GRV-R7-MM1001-10	
Channel Type	ICTD Temperature Probe Analog Input	
Value	Invalid Value Unit: Degrees C	
Minimum	-232.54	Clear Minimum
Maximum	-232.54	Clear Maximum
Quality	Error Code #6 Reporting out-of-range designator - below operating limits.	
Fast Updates	Updates this view very quickly, but may affect system performance. ☐	

The Quality field shows you a message with an error code number and a possible reason for the error. This information can help you troubleshoot problems with a field device wired to that specific channel.

9: Creating and Updating PID Loops

PID loops (or simply PIDs) are used to drive an input (a process variable) toward a particular value (the setpoint) and keep the input very close to that value by controlling an output. For example, consider temperature control, where the input is a measurement of ambient temperature, the setpoint is the desired temperature, and the output is a heater. The PID for this system will use a mathematical formula that controls the output to maintain a desired temperature, efficiently adjust to changes in setpoint, and compensate for changes in load, such as the influx of cold air. In this example, a temperature sensor (analog input), a thermostat (analog input), and a heater control (analog output) are components of one system, controlled by a PID loop.

This chapter assumes that you are already familiar with using PIDs. PID calculations are complex and the physical qualities of systems suitable for PID control differ greatly. You may be familiar with creating and managing PIDs through control programs like PAC Control; however, this chapter explains how to create and manage a PID through *groov* Manage, independent of any control program. If you configured a PID loop through PAC Control, you can review the current settings, as well as tune the PID.

PIDs can control isolated systems or be part of cascaded systems where one loop controls the setpoints or input variables of others. For maximum flexibility, you can set any PID input, setpoint, or output through *groov* Manage.

UNDERSTANDING HOW A PID WORKS

A proportional integral derivative (PID) control system (often referred to as a PID loop) monitors a process variable, compares the variable's current value to a desired value (a setpoint), and calculates an output to correct error between the setpoint and the variable. Because the calculation is complex, it is done by a mathematical formula that is adjusted (tuned) for each PID loop. The mathematical formulas vary, but all PID systems share these fundamental concepts:

- They evaluate a process variable against its setpoint.
- They control an output to correct the process variable.
- The output comprises proportional, integral, and derivative calculations.
- The effect of proportional, integral, and derivative calculations is modified by user-determined P, I, and D constants.
- The P, I, and D constants need to be tuned for each system.

PIDS AND CONTROL PROGRAMS

Once configured and initialized, a PID operates until the module loses power.

Each PID loop must be individually configured and tuned.

Configuration steps start in [“Configuring a PID Loop” on page 115](#). For information about PAC Control logic commands to read and write various PID parameters, see [PAC Control User’s Guide](#) (form 1700).

PID LOOPS ON *groov* RIO

groov RIO UIO provide 4 PID loops.

In *groov* Manage, you can configure each of the PID loops with unique settings for a large number of parameters. For a simple PID loop, you must configure at least the following:

- Input (the process variable being monitored)
- Setpoint (the desired value)
- Output (the I/O point that effects change in the system)
- Scan time (how often the PID loop is run)
- PID algorithm used (four algorithms are available; see [“Understanding PID Algorithms”](#) below).
- Valid range for input
- Upper and lower clamps for output
- Minimum and maximum change for output

You can also configure the following parameters if necessary:

- Forced output value or use of manual mode if input goes out of range
- Feed forward gain
- Square root of input

In *groov* RIO UIO, the derivative is applied only to the process variable (the input) and not to the setpoint. This means you can change the setpoint without causing spikes in the derivative term. These PIDs also prevent integral windup by back calculating the integral without the derivative term. The feed forward term (“bias”) is added before output clamping and has a tuning factor.

If desired, you can cascade PIDs by simply using the output channel of one PID loop as the input channel for another.

UNDERSTANDING PID ALGORITHMS

When you configure a PID loop, choose one of these algorithms:

- Velocity (Type C)
- ISA
- Parallel
- Interacting

You may also see the following obsolete algorithms:

- Velocity (Type B) Obsolete
- ISA (Obsolete)
- Parallel (Obsolete)
- Interacting (Obsolete)

Do not use these algorithms on *groov* RIO.

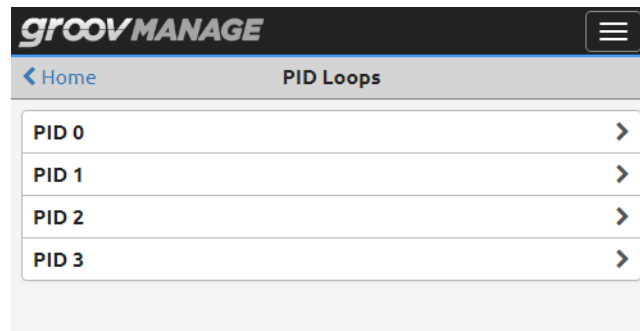
CONFIGURING A PID LOOP

Important: If you configure a PID loop through your control program, you may not be able to use these instructions:

- *If you configure PID loops through PAC Control and then configure PID loops through groov Manage (by following the instructions in this section), the configurations you made through groov Manage will be overwritten or lost whenever you download your PAC Control strategy or restart it.*
- *If you run a CODESYS application, it cannot access these PID loops directly.*

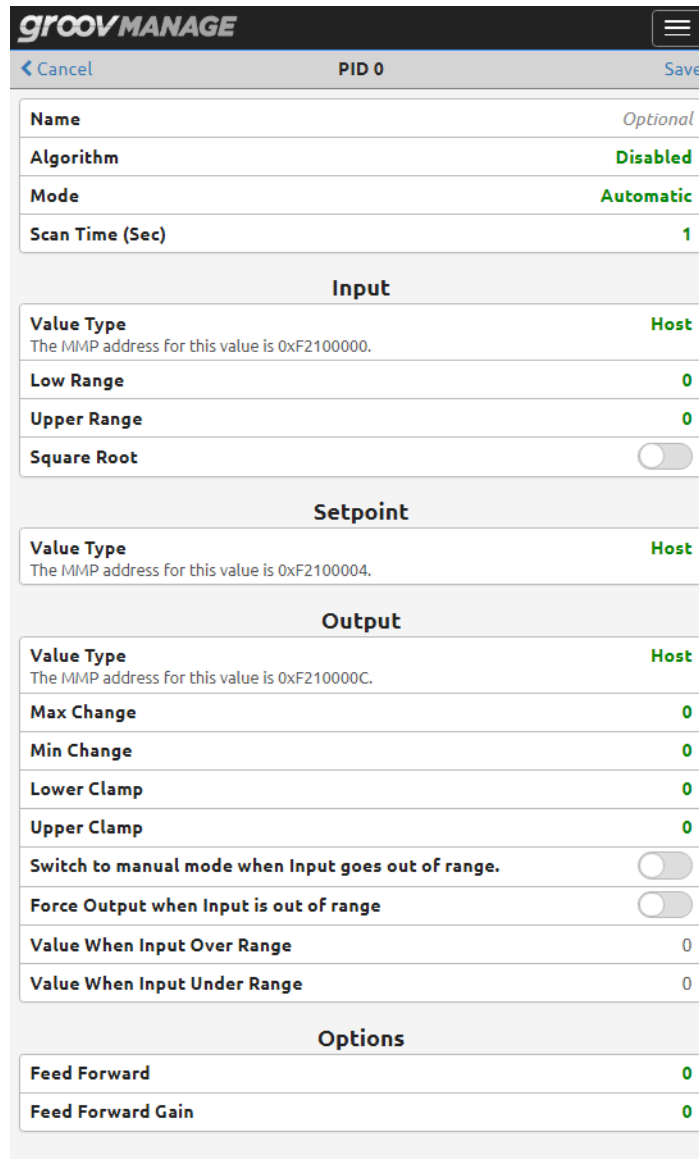
Before you configure a PID loop, make sure you first configure the I/O points that will be used by the PID loop.

1. Log into your *groov* RIO UIO with a user ID that has administrator privileges.
2. Click PID Loops. *groov* RIO UIO supports 4 PID loops, so you will see 4 rows in the PID Loops page, numbered sequentially, beginning with 0.



3. Click on the lowest unconfigured PID loop number. As an example, we will start with PID 0.

- Click Configure. *groov* Manage displays the configuration page.



PID 0	
Name	Optional
Algorithm	Disabled
Mode	Automatic
Scan Time (Sec)	1
Input	
Value Type	Host The MMP address for this value is 0xF2100000.
Low Range	0
Upper Range	0
Square Root	☐
Setpoint	
Value Type	Host The MMP address for this value is 0xF2100004.
Output	
Value Type	Host The MMP address for this value is 0xF210000C.
Max Change	0
Min Change	0
Lower Clamp	0
Upper Clamp	0
Switch to manual mode when Input goes out of range.	☐
Force Output when Input is out of range	☐
Value When Input Over Range	0
Value When Input Under Range	0
Options	
Feed Forward	0
Feed Forward Gain	0

Fill out the fields and select options as follows:

Name. Type a unique, descriptive name for the PID.

Algorithm. Choose algorithm: Velocity, ISA, Parallel, or Interacting. For details on algorithms, see [“Understanding PID Algorithms” on page 114](#).

Mode. Choose whether you want the PID initialized automatically or manually. The main difference between Automatic and Manual mode is that in Manual mode, the PID loop stops its mathematical calculation. In both modes, the PID's output value is still copied to the analog output.

- **Automatic:** The PID makes calculations based on the difference between the input and the setpoint resulting in changes to the output, which causes the input to move toward the setpoint.
- **Manual mode:** The PID stops making changes to the output, but continues to write the PID output to the configured destination for the PID output. Manual mode allows control program logic or an

operator to control the PID output, which in turn is written by the PID loop to the configured destination of the PID output.

NOTE: If the value of the analog channel or configured destination is changed, it will be overwritten by the PID output.

Scan Time (sec). Enter a scan time to determine how often the input is scanned and the PID output is calculated. There are many factors you need to consider when calculating a scan time; the Opto 22 website (www.opto22.com) provides several resources to help you calculate an appropriate scan time. (Enter “PID” in the search box of the website.) You should also consider other PIDs and tasks competing for the I/O processor’s power.

In the **Input** section:

- Select from where the PID receives its input: Input Channel, Output Channel, MMP address, Host, or PID Output.
 - If the PID’s process variable comes from an input channel on the same unit, select Input Channel. Enter the channel number (or click on the + or - signs) to indicate which channel on the module is the input channel.

The screenshot shows a configuration window titled "Input". It contains a table with two rows. The first row has "Value Type" in the left column and "Input Channel" in the right column. The second row has "Channel Index" in the left column and a control element in the right column consisting of a minus sign, the number "0", and a plus sign.

Input	
Value Type	Input Channel
Channel Index	⊖ 0 ⊕

- If the PID’s process variable comes from an output channel on the same unit, select Output Channel. Enter the channel number (or click on the + or - signs) to indicate which channel on the module is the output channel.

This screenshot is identical to the previous one, showing the "Input" configuration window with "Input Channel" selected and "Channel Index" set to 0.

Input	
Value Type	Input Channel
Channel Index	⊖ 0 ⊕

- If the PID’s process variable comes from an MMP address on the MMP server, select MMP Address. Enter the MMP address in the MMP Address field.

The screenshot shows a configuration window titled "Input". It contains a table with three rows. The first row has "Value Type" in the left column and "MMP Address" in the right column. The second row has "MMP Address" in the left column and "0x00000000" in the right column. The third row has "Low Range" in the left column and "0" in the right column.

Input	
Value Type	MMP Address
MMP Address	0x00000000
Low Range	0

- If the PID’s process variable comes from a control program, select Host.
 - For custom control programs, make sure the control program writes the input value to the MMP address listed underneath Value Type.
 - For PAC Control strategies, use the Set PID Input command.

CONFIGURING A PID LOOP

- In the following diagram, the MMP address shown is for PID 0:

Input	
Value Type	Host
The MMP address for this value is 0xF2100000. 	
Low Range	0

- If the PID's process variable is the output of another PID on this module (a cascading control loop), select PID Output. Enter the PID loop number (or click on the + or - signs) to indicate which loop contains the input value.

Input	
Value Type	PID Output
PID Output	 0 
Low Range	0

- **Square Root.** (Optional) Check this box if the error should be calculated based on the square root of the process variable (applies to flow control systems where volumetric flow is proportional to the square root of a signal from a flow transducer).
- **Low/Upper Range.** Set the valid range of the process variable by entering the low range and the upper range. (See Output section for optional responses to out-of-range input.)

In the **Setpoint** section, choose the source for the setpoint: Input Channel, Output Channel, MMP address, Host, or PID output.

- To control the setpoint using a device (on the same module) such as a potentiometer, select Input Channel. Enter the channel number (or click on the + or - signs) to indicate which channel on the module is the input channel.
- To control the setpoint from an output channel on the same unit, select Output Channel. Enter the channel number (or click on the + or - signs) to indicate which channel on the module is the output channel.
- To control the setpoint through a control program, select Host.
 - For custom control programs, make sure the control program writes the setpoint value to the MMP address listed underneath Value Type.
 - For PAC Control strategies, use the Set PID Setpoint command.
- To control the setpoint value through an MMP address on the MMP server, select MMP Address. Enter the MMP address in the MMP Address field.
- If another PID loop will control the setpoint, select PID Output. Enter the PID loop number (or click on the + or - signs) to indicate which loop contains the setpoint value.

In the **Output** section:

- Choose the destination for the PID output: Output Channel, MMP address, or Host.
 - If the destination is an output channel, select Output Channel. Enter the channel number (or click on the + or - signs) to indicate which channel on the module is the output channel.
 - If the output should be sent to an MMP address on the MMP server, select MMP Address. Enter the MMP address in the MMP Address field.

–If the output should be sent to a control program, select Host. Make sure the control program reads the output value from the MMP address listed underneath Value Type. In the following diagram, the MMP address shown is for PID 0:

The screenshot shows a configuration window titled "Output". It has two main sections. The first section is labeled "Value Type" and has a dropdown menu set to "Host". Below this, it says "The MMP address for this value is 0xF210000C." with a red arrow pointing to the address. The second section is labeled "Max Change" and has a value of "0" entered.

- **Min Change/Max Change.** (Optional) Enter minimum and maximum change values. The output won't respond until the minimum change is reached (for example, you may not want a heater to turn on to correct a 1 degree error). Maximum change prevents too drastic a change in output (for example, you could limit the increase in a pump's output to prevent pipe breakage). The default for both minimum and maximum is zero, which disables the feature.
- **Lower Clamp/Upper Clamp.** Enter upper and lower clamp values to prevent the output from exceeding a desirable range. These values should equal the range of the output channel, if used. Or choose values to make sure that the output device doesn't shut off (for example, keeping a circulation pump running regardless of the PID output) or that the output never reaches a destructively high setting (for example, keeping a motor below maximum).
- Choose how the PID should respond if the input goes out of range:
 - To have the control program logic or an operator respond, click Switch to manual mode when Input goes out of range.
 - To force the output to a specific value, click Force Output when Input is out of range.
 For either option, enter the range values in the Value When Input Over Range and Value When Input Under Range fields.

NOTE: If both switches are enabled (forced output and manual mode), the output will be forced and the PID put into manual mode; but if the PID is already in manual mode, the output will not be forced.

If neither switch is enabled and the PID input goes out of range (as defined by Low/Upper Range) then the output will freeze, but only while the input is out of range.

In the **Options** section, it's optional to specify values for **Feed Forward/Feed Forward Gain**. Enter values if you need to offset the module output in your application. These values are constants that are multiplied and added to the module output; often they are not used in PIDs.

CHANGING A PID LOOP

You can change the PID loop's configuration.

1. Log into your *groov* RIO UIO with a user ID that has administrator privileges.
2. Click PID Loops. *groov* Manage displays the PID Loops page, listing all the configured and unconfigured PID loops.
3. To change the PID loop's configuration, click the PID loop number, then click Configure. *groov* Manage opens the configuration page. Change the fields as necessary. For help in completing the fields, see ["Configuring a PID Loop" on page 115](#).

DISABLING A PID LOOP

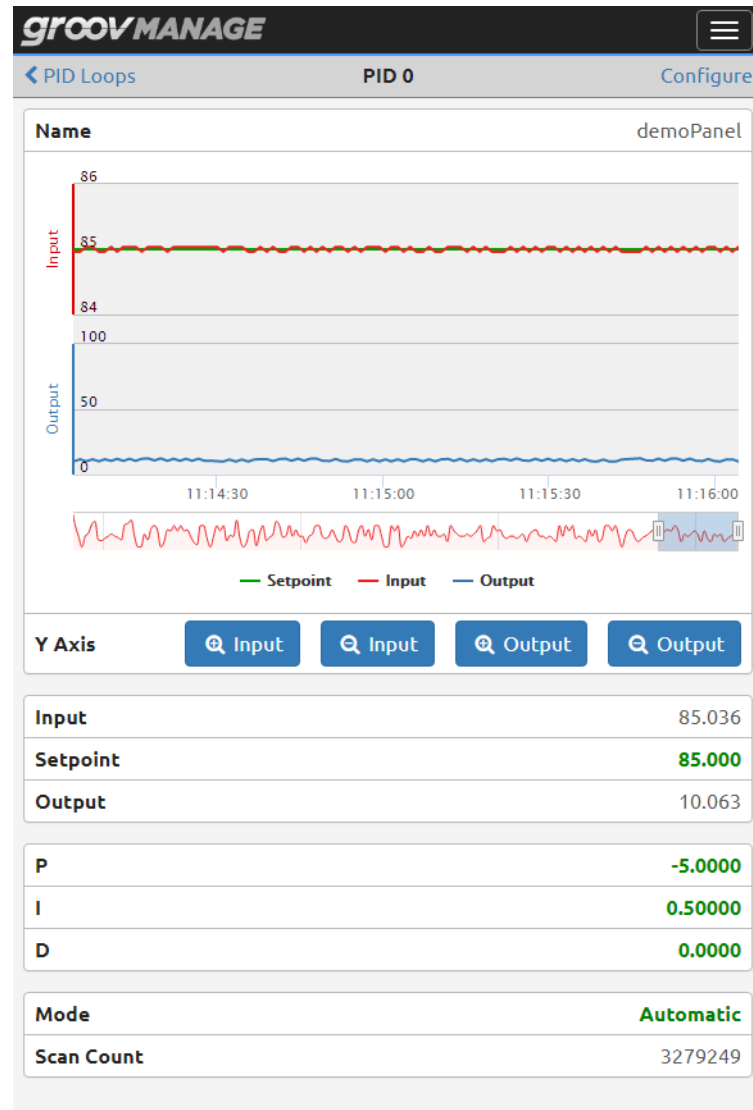
If you no longer need to run a specific loop, you can disable it. All the settings you selected and information you entered will remain.

1. Log into your *groov* RIO UIO with a user ID that has administrator privileges.
2. Click PID Loops. *groov* Manage displays the PID Loops page, listing all the PID loops.
3. Click on a PID loop number. *groov* Manage displays the PID Loop <number> page.
4. Click Configure.
5. Click Algorithm, then select Disable.
6. Click Save. The PID will stop running.

INSPECTING A PID

1. Log into your *groov* RIO UIO with a user ID that has administrator privileges.
2. Click PID Loops. *groov* Manage displays the PID Loops page, listing all the PID loops.

- Click on a PID loop number. *groov* Manage displays the PID Loop <number> page. The following example is for PID Loop 0:



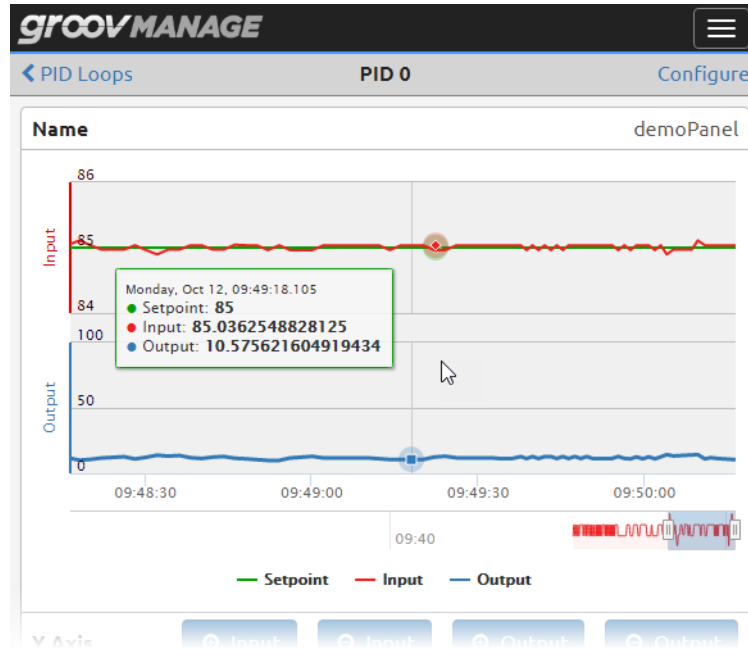
You can change PID parameters, view specific channel values on the chart, or adjust the scale of the chart.

Changing PID Parameters

To change the value of any of the PID parameters, click on the name of the parameter and enter a new value. You'll see the changes reflected in the chart on the top half of the screen.

View Specific Values on the Chart

Move the cursor so that it hovers over a specific point on the chart. *groov* Manage displays the values for that point:



Adjusting the Scale of the Charts

There are a few ways to adjust the scale of the charts so that you can see a longer time period, view a specific segment of time, or to adjust the view of only the input chart or the output chart. Note that you can only do this through a browser on a desktop computer or laptop; you can't adjust the scales through a mobile device or a tablet.

To view a longer length of time, click and hold the left endpoint of the slider below the chart and move it further away from the right endpoint. This increases the amount time shown on the chart.

To view a specific segment of time, click and hold in the center (blue area) of the slider and then move the slider to the specific range of time you want. You may want to adjust the endpoints to narrow or increase the time segment.

To adjust the view of only the input portion of the chart, click on the  Input or  Input buttons.

To adjust the view of only the output portion of the chart, click on the  Output or  Output buttons.

10: Enabling Data Services—MQTT and OPC UA

If you are not familiar with MQTT or OPC UA, you can read the following brief introductions of each protocol:

OPC UA servers on groov RIO UIOs. The *groov* RIO UIO provides the following OPC UA servers:

- The Data Services OPC UA server, which is described in this chapter.
- (GRV-R7-MM2001-10 only) Ignition®/Ignition Edge® OPC UA server (see the online help from Inductive Automation®)
- Node-RED (by adding third-party OPC UA nodes; refer to their documentation)
- (GRV-R7-MM2001-10 only) CODESYS® OPC UA server (see online help from CODESYS)

MQTT clients on groov RIO UIOs. The *groov* RIO UIO provides the following MQTT clients:

- The Data Services MQTT client, which is described in this chapter.
- (GRV-R7-MM2001-10 only) Ignition MQTT client (with the addition of the Cirrus Link® MQTT transmission module; see online help from Inductive Automation)
- Node-RED (by adding third-party MQTT nodes; refer to their documentation)
- (GRV-R7-MM2001-10 only) CODESYS MQTT client (see online help from CODESYS)

A word on MQTT terminology (client/sever versus publisher/subscriber/broker): Although the MQTT publish-subscribe architecture is different from the typical client-server architecture, the terms *client* and *server* are still used to describe the relationship between devices or software communicating via MQTT. The MQTT broker functions as a server. The devices or software that publish or subscribe to data function as clients. This terminology is also consistent with the MQTT 5.0 standard.

OVERVIEW OF CONFIGURING AND ENABLING DATA SERVICE

The Data Service runtime enables communication between the data on your *groov* RIO UIO and an MQTT broker or OPC UA client. To configure this communication:

1. Configure the following cybersecurity features to create secure, authenticated connections to the MQTT broker (server) and/or the OPC UA clients:
 - For OPC UA, create and configure user accounts with the Data Services OPC UA Server permission. These accounts are dedicated for this communication. For instructions on creating accounts, review [“Managing User Accounts” on page 25](#).
 - If your site requires SSL:
 - For OPC UA, create an SSL server certificate in *groov* Manage, and then upload it to the computers or mobile devices running your OPC UA clients. For instructions, review [“groov RIO as a Server: Creating Server Certificates” on page 41](#).

EXPOSING DATA (PUBLIC ACCESS)

- For MQTT, obtain the server SSL certificate from the MQTT broker (server) and add it to the *groov* RIO UIO's trust store. [“groov RIO as a Client: Adding a Server's Certificate” on page 43](#)
- 2. To configure the Data Services MQTT client, review [“Configuring and Enabling the Data Services MQTT Client” on page 130](#).
- 3. To configure the Data Services OPC UA server, review [“Configuring and Enabling the Data Services OPC UA Server” on page 133](#).
- 4. Enable the Data Service runtime and test the connection. For instructions, review .

EXPOSING DATA (PUBLIC ACCESS)

For the Data Services MQTT client to publish data or for an OPC UA client to access data on your *groov* RIO UIO, you must expose the data by enabling *public access*. There are several ways to enable public access:

- Through *groov* Manage. Select this method if:
 - you need to expose only a few I/O channels, PID loops, and/or areas of the Scratch Pad, or
 - you want to efficiently expose *all* I/O channels on a module. **Important:** Before you expose all I/O channels, verify that you want and will use data from all I/O channels. For services like MQTT, this can create lots of data transmission, which can fill your network bandwidth.

To enable public access through *groov* Manage:

- for all channels at once, review .
 - for PID loops, review .
 - for Scratch Pad areas, review .
- Through programming: within your application, enable public access by turning on the correct values through OptoMMP. For instructions, review the [OptoMMP Protocol Guide](#) (form 1465).

Enabling Public Access of the PID Loops through *groov* Manage

1. Log into your *groov* RIO UIO with a user ID that has system administrator privileges.
2. Click **I/O > I/O Services > PID Loops**.
3. Click the loop you want to expose.
4. Click **Configure**.

5. Scroll down to the **Public Access** section.

The screenshot shows the **groovMANAGE** interface for **PID 0**. At the top, there are buttons for **< Cancel** and **Save**. Below the title bar, there are four input fields: **Name** (with a note "Optional"), **Algorithm** (set to **Disabled**), **Mode** (set to **Automatic**), and **Scan Time (Sec)** (set to **1**). Below these is a **Feed Forward Gain** field set to **0**. The **Public Access** section is highlighted and contains five toggle switches: **Readable** (turned on), **Writable** (turned off), **Input Deadband** (set to **0**), **Setpoint Deadband** (set to **0**), **Output Deadband** (set to **0**), and **Scan Count Deadband** (set to **0**). A note at the bottom states: "Public Access attributes are used to select what values are available to certain protocols and services, including MQTT and Ignition."

6. Click **Readable**. *groov* Manage displays additional options.
7. If you want to allow applications to write values to the PID loop, click **Writable** to enable it.
8. Adjust deadband values to control how often Data Service publishes a topic due to a change in value of each PID variable. The larger the value, the more change a variable undergoes before Data Services publishes a topic. You may want to periodically evaluate these values to determine if they are providing the information needed by your application. All values must be non-negative values.
9. Click **Save**.

Enabling Public Access of the Scratch Pad Area through *groov* Manage

1. Log into your *groov* RIO UIO with a user ID that has system administrator privileges.

CREATING A SCANNED DEVICE

2. Click **I/O > I/O Services > Scratch Pad > Public Access**. *groov* Manage displays the public access page for the Scratch Pad area.

The screenshot shows the 'groovMANAGE' interface for the 'Scratch Pad' area. At the top, there are 'Cancel' and 'Save' buttons. Below the header, a text block explains that areas marked as 'Public Access' are available via the Data Service and that areas with a length of 0 are not scanned. The page is divided into four sections: '32-bit Integer', '64-bit Integer', 'Float', and 'String'. Each section contains two input fields: 'Start Index' and 'Length', both currently set to '0'. Below each section, a note specifies the valid range for that data type: 0 to 10239 for 32-bit Integer and Float, 0 to 1023 for 64-bit Integer, and 0 to 63 for String.

Area	Start Index	Length	Valid Range
32-bit Integer	0	0	0 to 10239
64-bit Integer	0	0	0 to 1023
Float	0	0	0 to 10239
String	0	0	0 to 63

For each area (**32-bit Integer**, **64-bit Integer**, **Float**, and **String**) of the Scratch Pad, indicate how many elements of the area to expose by specifying the index of the first element (as a decimal) in the **Start Index** field and the number of elements (as a decimal) in the **Length** field. For example:

- If you want to enable public access to 5 elements (beginning with the fourth element) of the 32-bit Integer area: in the **32-bit Integer** section, specify **3**¹ in the **Start Index** field and **5** in the **Length** field.
- If you want to enable public access to all the elements of the String area: in the **String** section, enter **63** in the **Length** field.

To learn how memory is organized in the Scratch Pad area, review the [OptoMMP Protocol Guide](#) (form 1465).

3. Click **Save**.

CREATING A SCANNED DEVICE

A *scanned* device manages the communication between the local I/O (I/O data, PID loops, and the Scratch Pad area of the OptoMMP memory map) and:

¹Remember that numbering of elements begins with 0.

- the MQTT broker (through the Data Services MQTT client), and
- OPC UA client (through the Data Services OPC UA server).

You can add a label (called a *device ID*) to identify the source of the data (your *groov* RIO UIO) and alter some settings to improve performance and throughput.

1. Log into your *groov* RIO UIO with a user ID that has system administrator privileges.
2. Click **Data Service > Configure**.
3. In the **Scanned Devices** section, click **Add Local I/O System**. *groov* Manage displays the Device Configuration page:

groovMANAGE

[Cancel](#) **Device Configuration** [Save](#)

This device can access I/O Channels, PID Loops, and Scratch Pad values that have Public Access enabled.

Device Type	Local I/O System	For your information.
Enable	☒	
Device ID	e.g. any_unique_id Used to identify this device in MQTT topics and OPC UA node IDs.	
Host TCP Port	2001	
Communication Timeout (ms)	3000 Must be at least 250 ms.	
Scan Time (ms)	1000 Must be at least 250 ms.	
Metrics Update Rate (ms)	5000 0 to disable, or equal to or greater than the Scan Time.	

Protocols

MQTT String	☒
MQTT Sparkplug	☒
OPC UA Server	☒

This device will be available from the selected protocols.

4. Configure the settings as follows:
 - Enable**—The scanned device is enabled by default.
 - Device ID**—Enter a name that helps uniquely identify the source of data: your *groov* RIO UIO. Remember the following as you create a name:
 - Allowed characters are A through Z, a through z, 0 through 9, underscores (_), spaces, and dashes (-). While it may be possible to use other symbols, remember that other systems (like brokers, protocols, operating systems, etc.) may have different or special meanings for these symbols.
 - The character encoding determines the maximum length of the name; for example, if characters are encoded in UTF-8, the name must not exceed 65,535 bytes.
 - The device ID becomes part of an MQTT Sparkplug® tag, MQTT String topic, and an OPC UA tag.
- Some useful information to have in the device ID:
- Your *groov* RIO UIO's hostname.
 - If you manage multiple *groov* RIO UIOs, include where they are located. For example, Bldg_1.
 - If you are limiting the scan to a specific protocol, include the name of the protocol. For example, OPC-UA.

Host TCP Port—You cannot change this value. *groov* Manage displays it for your reference.

Communication Timeout (ms)—The number of milliseconds that the scanned device takes to connect to and then wait for a response from the MQTT server. The default value is 3000 milliseconds. The minimum is 1000; the maximum is 30,000.

Some factors to consider when you adjust this value:

- The volume of tags created by the local I/O, PID, and Scratch Pad.
- The stability of the network connection. If you are transmitting through a cellular network, which may be more lossy than a hard-wired connection, you may want to increase this value.
- If you are using the MQTT protocol, compare this value to the communication timeout value for the MQTT broker (see). In general, you want the connection timeout value of the scanned device to be smaller than the communication timeout value to the MQTT broker.

Scan Time (ms)—The number of milliseconds the scanned device waits to read the tags of the local I/O, PID, and Scratch Pad. The default is 1000 milliseconds. The minimum is 250.

Metrics Update Rate (ms)—The number of milliseconds between scans of performance-related tags. The default is 5000 milliseconds. To disable the publication of these tags, enter **0**. A higher value means fewer publications of these types of tags. If you are using the MQTT protocol, a larger value can help reduce the volume of data the MQTT broker receives. Performance-related metrics can include:

- Actual scan times.
- Writing queue depth, which is the volume of pending write requests that the scan device needs to process. This metric can help you evaluate the scanned device's performance. For example, if the value is consistently high, the scanned device may have a performance issue or the MQTT broker or OPC UA client may be sending too many write requests.

Protocols—The scanned device can communicate with up to three protocols at once. Enable the ones needed by your application and disable unused protocols.

5. Click **Save**.

CONFIGURING AND ENABLING MQTT

MQTT is a publish/subscribe (pub/sub) protocol that is suited to many IIoT applications because of its architecture.

In a pub/sub architecture, a central source (called a *broker*) receives and distributes data. MQTT clients can publish data to the broker or subscribe to get data from a broker (or both). Clients can publish (send) data when it changes. Clients can subscribe (receive) this data from the broker. To view a video that explains how an MQTT broker works and why it is a great choice for automation applications, visit our website (www.opto22.com), and search for “What is an MQTT broker?”

Contrast the MQTT architecture with a client/server architecture. With this architecture, the client and server must be connected because the client requests data directly from the server. The client does not know when the data changes, so it must request it at regular intervals.

MQTT pub/sub offers three main advantages over client/server for IIoT applications:

- Network traffic is reduced overall because data is published only when it changes, rather than at regular intervals.
- Because the broker is a central source that manages data, servers do not have to strain to serve multiple clients. Even remote devices with irregular connections or low bandwidth can publish or subscribe to data. If a publisher cannot connect to the broker, for example, the publisher can optionally buffer its data and send it at a later time.
- For data publishers and subscribers, there is another important advantage: data is published and subscriptions are initiated through an outbound connection. Most firewalls block inbound traffic

requests (for example, an external OPC client requesting data from an internal OPC server), but they allow outbound connections over secure TCP ports.

For more information about the protocol, see mqtt.org. Opto 22 provides a wide-range of resources on our website (www.opto22.com) to help you learn about working with MQTT and Opto 22 devices:

- Video resources like the [MQTT Videos](#) series
- Online training like the [Moving IIoT Data with MQTT Strings and Sparkplug B](#) course
- Additional documents like:
 - white papers such as [White Paper: Industrial-strength MQTT/Sparkplug B](#) (form 2357)
 - case studies
 - specialized documents such as [Getting Started with MQTT in groov Products](#) (form 2350)

Choosing the Right MQTT Client and Payload Type

There are many factors to consider when you include a *groov* RIO UIO into an existing MQTT infrastructure, including the type of payload and client. The *groov* RIO UIO provides several different MQTT clients that can publish data in two different payload formats (string and Sparkplug B):

- Data Services MQTT client
- (GRV-R7-MM2001-10 only) Ignition/Ignition Edge (requires the purchase of an appropriate Ignition license)
- Node-RED (by adding MQTT client nodes)
- (GRV-R7-MM2001-10 only) CODESYS

To help you choose the MQTT client and payload format best suited for your application, review *Getting Started with MQTT in groov Products* (form 2350), which describes important factors that can influence which client and payload format you choose. It also provides examples that explain how to configure a *groov* RIO UIO for simple data collection and control, or for high-reliability SCADA/IIoT applications.

After reviewing that document, you can get more information in this guide about:

- Configuring and enabling the Data Services MQTT client, which is described in this chapter.
- Configuring and enabling the Ignition/Ignition Edge MQTT client, which is described in ADD CHAPTER.

For information on configuring the CODESYS MQTT client, refer to the CODESYS documentation. For information on configuring the Node-RED MQTT client nodes, refer to the documentation provided by the node author.

Running Multiple MQTT Clients on a *groov* RIO UIO

You can run the following Ignition/Ignition Edge MQTT clients simultaneously:

- MQTT client publishing Sparkplug B payloads
- MQTT client publishing string payloads

You can also run all of the MQTT clients on a *groov* RIO UIO simultaneously: Data Services, Ignition/Ignition Edge, CODESYS, and Node-RED.

MQTT on *groov* RIO. One of the features of MQTT is that the data (payload) it transmits can be in a format best suited for the application. *groov* RIO can transmit payloads formatted to meet the Sparkplug-B specification or formatted as strings. In addition, RIO offers several features and capabilities to suit a variety of application requirements.

Review the following list of features and capabilities and select the option that best suits your application:

- **MQTT with string payloads**—Select this option if:
 - Your application requires that the payload be formatted as a string.
 - Your application is simple, perhaps monitoring or controlling only a few devices.

- Your application requires automation data from *groov* RIO, but not from other PLCs.
- You are looking for a cost-effective option. This option does not require the purchase of additional licenses.

With this option, you will need to:

- Convert data within your application. With payloads formatted as strings, you will need to add logic to your application to convert strings to the correct data type, when necessary.
- Define the topic namespace.
- **MQTT with Sparkplug payloads published from *groov* RIO**—Select this option if:
 - Your application requires that the payload be formatted to comply with the Sparkplug specification.
 - Your application requires automation data from *groov* RIO, but not from other PLCs.
 - You are looking for a cost-effective option. This option does not require the purchase of additional licenses.

With this option, you'll be able to queue data into RAM if network connectivity is lost, which will then be transmitted when the service is available. However, because the queued data is stored in RAM, it can be lost when power is cycled or space runs out.

Keep in mind that you will need to:

- Define the topic namespace.
- Provide the MQTT configuration information through *groov* Manage and then enable the service.

Note that you cannot combine these two options; you must choose one or the other.

- For MQTT with string payloads, see [“Configuring and Enabling MQTT with String Payloads” on page 61](#).
- For MQTT with Sparkplug payloads published from *groov* RIO, see [“Configuring and Enabling MQTT with Sparkplug Payloads from *groov* RIO” on page 63](#).

Configuring and Enabling the Data Services MQTT Client

Before you configure and enable the Data Services MQTT client, complete the following tasks to make the process easier:

- Upload server certificates from your MQTT server (broker) to your *groov* RIO UIO (see).
- Create the scanned device (see).

To configure and enable the Data Services MQTT client:

1. Log into your *groov* RIO UIO with a user ID that has system administrator privileges.
2. From the *groov* Manage Home page, click **Data Service > Configure**. *groov* Manage displays the Data Service Configuration page.

Each section of the page provides access to additional pages to configure the Data Services MQTT client, the Data Services OPC UA server, and to create the scanned device, as well as access to the pages that help you enable public access to the local data.

3. Configure the client and add the broker(s):
 - **For String payloads**—click **Add MQTT String** to display the MQTT String configuration page and fill out the fields as described in and add the broker(s) as described in .
 - **For Sparkplug payloads**—click **Add MQTT Sparkplug** to display the MQTT Sparkplug configuration page and fill out the fields as described in and add the broker(s) as described in .

Note: You can add multiple brokers for each payload type.

4. Click **Status** to return to the Status page.
 - If you are done, enable Data Service and test your connections (review .
 - If you want to configure the Data Services OPC UA server before enabling Data Service, then review .

The MQTT String Configuration Page

- A** The MQTT String protocol is enabled by default; however, you may want to disable it if you want to stop it and preserve the configuration information.
- B** The Data Service creates one topic per tag with that data represented as 7-bit ASCII. The topic namespace uniquely identifies your *groov* RIO UIO in your MQTT infrastructure and is made up of the following topics:
 - **MQTT Base Topic**—Data Service prefixes the base topic to the MQTT topic.
 - **MQTT Group Topic**—(Optional) Identifies the group that your *groov* RIO UIO belongs to.
 - **MQTT Subgroup Topic**—(Optional) Identifies a subdivision within the group.

If necessary, consult with someone that assigns topic names to determine if the will be assigned a specific set of topic names, and whether you should follow a particular naming convention.

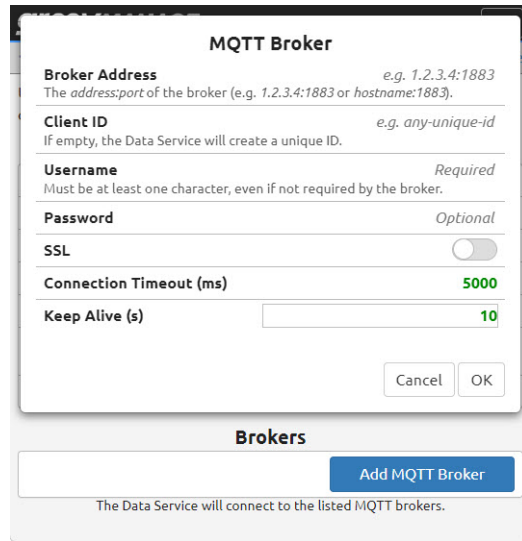
There are two additional topics that trigger special actions, which you write between the base topic and the group topics:

 - **write** to indicate that a topic is to write a value to a tag.
 - **special** to indicate that the Data Service should publish all tags.
- C** If your application uses a comma to separate values (for example, pi is denoted as 3,14 instead of 3.14), you want to indicate that by enabling the **Use Comma for Decimal Separator** setting.
- D** **Allow Writes**—Controls whether *groov* RIO UIO accepts write requests.

Supported Data Types. MQTT string payloads support only the following data types:

Data Type		Examples
Boolean		true, false
32-bit IEEE 754 Float		3.141596e0 (If the Use Comma for Decimal Separator field is enabled, the value would be 3,141596e0.)
32-bit Integer		123456
64-bit Integer		-34359738368
String		"MQTT is fun!" (Data Service includes any quote or double quote marks that are part of the string; it does not add extra marks when it creates the topic.)

The MQTT Broker Configuration Page



MQTT Broker

Broker Address *e.g. 1.2.3.4:1883*
The address:port of the broker (e.g. 1.2.3.4:1883 or hostname:1883).

Client ID *e.g. any-unique-id*
If empty, the Data Service will create a unique ID.

Username *Required*
Must be at least one character, even if not required by the broker.

Password *Optional*

SSL ☐

Connection Timeout (ms) **5000**

Keep Alive (s)

Cancel OK

Brokers

The Data Service will connect to the listed MQTT brokers.

For each broker, you need to provide the following information:

- **Broker Address**—The hostname or IP address of the MQTT broker, followed by a colon, and then the port number.
- **Client ID**—This is optional. Only enter a client ID if one was supplied. If you do not enter a client ID, the Data Service generates one. For guidance on whether to create a client ID or use the one generated by Data Service, review your MQTT provider's requirements.
- **Username**—The username you need to access the broker.
- **Password**—The password you need to access the broker. Not all MQTT infrastructures require a password; check with your system administrator regarding passwords to the MQTT brokers.
- **SSL**—If your MQTT server requires SSL, make sure you upload the correct SSL certificate (before you begin configuring the MQTT service), as described in .
- **Connection Timeout (ms)**—The default connection timeout value is 5000 milliseconds. You can adjust this value to account for slower or faster infrastructures. (For example, if your *groov* RIO UIO is in an area with a lossy or slow connection, you may want to increase this value.) The minimum is 1000; the maximum is 30,000.
- **Keep Alive (s)**—The number of seconds between heartbeats. If there is no heartbeat for longer than the keep alive time, the Data Services MQTT client closes the connection to the broker. The broker automatically publishes the Sparkplug Last Will and Testament of your *groov* RIO UIO.

CONFIGURING AND ENABLING THE DATA SERVICES OPC UA SERVER

OPC UA is a communications protocol with a long history and an established base of implementations in many industrial applications. This client/server architecture has proven reliability and adding your *groov* RIO UIO helps you build upon this reliability and increase the reach of your OPC UA application.

OPC UA Servers on *groov* RIO

groov RIO UIO can run several different OPC UA servers simultaneously:

- The Data Services OPC UA server—built into the *groov* RIO UIO firmware—is configured and enabled through Data Service. The rest of this chapter describes this server. You can also view a video that

explains how to configure the Data Services OPC UA server on a *groov* RIO UIO: go to the Opto 22 website (www.opto22.com) and search for [Video: OPC UA Quick Start Tutorial](#).

- GRV-R7-MM2001-10 only: For CODESYS® users, the *groov* RIO UIO firmware ships with CODESYS OPC UA server. You must purchase and install the [CODESYS OPC UA Server SL](#) license to enable this server. You must also configure the CODESYS Development System to support OPC UA features. For detailed instructions, review the CODESYS online help.
- For Node-RED users, you can download OPC UA Node-RED nodes to give Node-RED flows and messages access to your data. For detailed instructions, review the Node-RED information provided by the OPC UA Node-RED node contributor.

Configuring and Enabling the Data Services OPC UA Server

Before you configure and enable the Data Services OPC UA server, complete the following tasks to make the process easier:

- Upload server certificates from your OPC UA server to your *groov* RIO UIO; for instructions, review .
- Create a user account with Data Service OPC UA Server permissions; for instructions, review .

While it is possible to use an account with system-wide Administrator permission, a security best practice would be to create a separate account with Data Service OPC UA Server permission.

- Create the scanned device; for instructions, review .

To configure and enable the Data Services OPC UA server:

1. Log into your *groov* RIO UIO with a user ID that has system administrator privileges.
2. From the *groov* Manage Home page, click **Data Service**.

3. In the **OPC UA** section, click **Add OPC UA**. *groov* Manage displays the OPC UA Server configuration page.

groovMANAGE

[Cancel](#) **OPC UA Server** [Save](#)

The OPC UA server provides the ability to browse, read, and write values from OPC UA clients.

Protocol	OPC UA Server
TCP Port	14840
Discovery Endpoint	opc.tcp://address:14840/groov

The address can be the hostname or an IP address, depending upon the network configuration.

Configuration

Enable ☒

Allow Anonymous Access ☒
The OPC UA server may also be accessed with the credentials of a user that has the Data Service OPC UA Server permission enabled.

Additional Endpoints Optional
A comma-separated list of additional endpoints to which the server will respond. (e.g. "192.168.0.22, router-fw:789, alt-hostname")

Allow Writes ☒

Security Policies

None ☒

Basic256Sha256 ☐

Aes128_Sha256_RsaOaep ☐

Aes256_Sha256_RsaPss ☐

Basic128Rsa15 ☐
Deprecated

Basic256 ☐
Deprecated

The OPC UA server will allow clients to connect with the selected security policies and methods of encryption.

[Delete Configuration](#)

- A** The top part of the page provides important reference information. Copy and save the **Discovery Endpoint** URL; when you configure your OPC UA clients, you add this URL, replacing **address** with one of the following:
- Hostname—The default hostname of your *groov* RIO UIO (review) or, if you changed it, the name you changed it to.
 - IP address—The default IP address of *groov* RIO UIO or, if your network configuration required modifications, the IP address assigned to it by your network administrators.
- B Configuration**—Make sure the **Enable** switch is green (turned on), and specify the configuration options as follows:
- Allow Anonymous Access**—If you are using *groov* View and obtaining tag data through the Data Services OPC UA server, you must enable this option. It still permits access to specific users that have the Data Service OPC UA Server permission.
- Additional Endpoints**—You can create a list (separated by commas) of additional endpoints. When OPC UA clients use these endpoints, the Data Services OPC UA server responds. This is useful when the *groov* RIO UIO is divided from the rest of the network by a firewall router. For example, if the IP address assigned to the *groov* RIO UIO by the router differs from the one assigned by the DHCP server, specify the address assigned by DHCP server in this field.
- The format of the each endpoint must be one of the following:

- hostname:port_number
- ip_address:port_number

Allow Writes—Controls whether *groov* RIO UIO accepts write requests.

C Security Policies—Enable the encryption policy that you want applied to connections to the Data Services OPC UA server:

- None
- Basic256Sha256
- Aes128_Sha256_RsaOaep
- Aes256_Sha256_RsaPss
- Basic128Rsa15 (Deprecated)
- Basic256 (Deprecated)

Make sure that your OPC UA clients support and enable the same encryption policy. If you do not want any encryption policy applied, enable **None**.

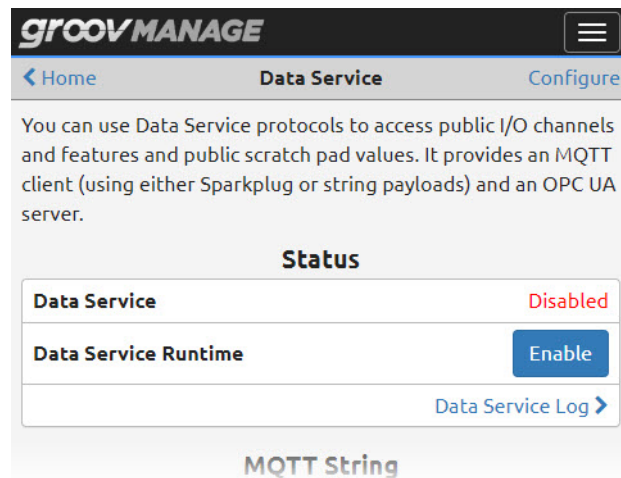
4. Click **Save**. After *groov* Manage validates the information you selected, it displays the Data Service page.

Note: If you see a message highlighted in yellow with the title “Configuration Issues”, it indicates you have not created the scanned device. For instructions, review .

ENABLING DATA SERVICES AND TESTING CONNECTIONS

After you have configured either the Data Services MQTT client or the Data Services OPC UA server, enable Data Services and test your connection:

1. Log into your *groov* RIO UIO with a user ID that has system administrator privileges.
2. Click **Data Service > Configure**.
3. In the **Status** section at the top of the Data Service page, click **Enable**.



After enabling the Data Service Runtime:

- **MQTT**—Begins to publish topics.
- **OPC UA**—*groov* Manage configures and opens the port in the firewall through which the OPC UA client communicates with the Data Services OPC UA server. You can verify this by checking the Firewall page in *groov* Manage.

When these changes are done, *groov* Manage displays **Running** (in green) in the **Data Service** field.

4. Test your connections:

- **MQTT**—Open up an MQTT client and configure it to subscribe to the data published by your *groov* RIO UIO. Refer to your MQTT client's documentation for instructions on configuring it to subscribe to data from a device.
- **OPC UA**—Configure your OPC UA client to connect to the Data Services OPC UA server, and look for your data. Refer to your OPC UA client's documentation for instructions on configuring it to connect to an OPC UA server. (Remember to use the **Discovery Endpoint** you copied from when you configure the OPC UA client.)

If you observe any issues, here are a few suggested items to check:

- **Network issues**—There are a few items you can check on your *groov* RIO UIO:
 - For OPC UA clients, the Data Services page (from the *groov* Manage Home page, click **Data Service**) displays the IP addresses of connected clients.
 - Check the *groov* RIO UIO's network connection status in the Network page (from the *groov* Manage Home page, click **Network > Status**) to verify that your **Link Status** is **Connected**.
 - Check the firewall settings, verifying the port numbers and whether the firewall is open.
 - The *groov* RIO UIO provides several tools in the Network page (from the *groov* Manage Home page, click **Network**) that can help you troubleshoot some network issues.
 - Check the Data Service logs (from the *groov* Manage Home page, click **Info and Help > Logs > Data Service**) for any authentication failures.

Remember to consult with any troubleshooting tools available through your OPC UA client tools or MQTT server, as well as your network administrator.

- **Application issues**—Check that the data is exposed (that you enabled public access); review .

11: Developing Node-RED Flows

If you are new to Node-RED, it might be helpful to review our Automation 101 video introducing Node-RED: [Intro to Node-RED: Part 1 - Fundamentals](#). (You can find other videos in the Support > Videos section of our website, www.opto22.com.) The “[Learning to Develop a Node-RED Flow](#)” section (below) will take you through a hands-on approach to learning how to develop a Node-RED flow. However, before you can begin those exercises or do anything else with Node-RED on your *groov* RIO, make sure you:

- Enabled Node-RED as described in “[Enabling Node-RED](#)” on page 94.
- Configured the channels on your RIO by one of the following methods:
 - As described in [Chapter 8: Configuring I/O](#).
 - Configured through a PAC Control strategy.
 - Configured through a custom control program.

FOR EXPERIENCED Node-RED DEVELOPERS

If you have experience developing Node-RED flow and just want to know which node to install to access I/O on your *groov* RIO, it is **node-red-contrib-groov-io**. This node can also access I/O on *groov* I/O modules mounted on an EPIC chassis.

You might also find the following nodes helpful:

- **node-red-contrib-groov**. Nodes to access a Data Store in a *groov* View project.
- **node-red-contrib-pac**. Nodes to access tags and strategy information from a PAC Control strategy running on a *groov* EPIC processor or SNAP PAC controller.

These are the URLs to access the Node-RED Editor in *groov* RIO:

- `https://[your groov RIO's hostname]/node-red`
- `https://[your groov RIO's IP address]/node-red`

NOTE: Starting in *groov* RIO firmware version 4.1.0, support for the FlowFuse Dashboard (also known as the Node-RED Dashboard 2.0) was added. You can have both the Node-RED Dashboard 1.0 and the FlowFuse Dashboard (Node-RED Dashboard 2.0) installed simultaneously. If you have Node-RED projects using both Node-RED Dashboards, *groov* Manage will open Dashboard 1.0. Note that the endpoints for 1.0 contain “/node-red/ui” in the URL while 2.0 endpoints have “/node-red/dashboard” in the URL. For more information, visit the Opto 22 Developer website (<https://developer.opto22.com>).

LEARNING ABOUT Node-RED ON RIO

Opto 22 provides Node-RED nodes to access *groov* RIO I/O; the same nodes can also access I/O on a *groov* EPIC processor. Opto 22 also provides Node-RED nodes to access data in *groov* View Data Stores, as well

as nodes to access strategy information from PAC Control strategies running on *groov* EPIC processors or SNAP PAC controllers. For more information on nodes, see developer.opto22.com.

Node-RED Editor. You can include one or many flows in your Node-RED project, which you build in the standard, browser-based Node-RED Editor. You can access the editor directly through a URL or navigate to it through *groov* Manage.

Debugging. With few programming restraints, it's easy to accidentally introduce bugs into your flow. The Node-RED Editor can help you debug flows. If Node-RED crashes, it automatically restarts. You can also start and stop Node-RED yourself from within *groov* Manage.

Files. Your Node-RED project consists of two files: the main file with all your flows, and a separate file containing all the sensitive credential information used by some nodes, such as usernames and passwords for an email node. *groov* RIO provides ways to backup and restore Node-RED projects, either separately or as part of the complete backup and restore.

LEARNING TO DEVELOP A Node-RED FLOW

If you are new to Node-RED, this section takes you step-by-step through the following exercises:

- Learning the different ways to open the Node-RED Editor in *groov* RIO.
- Creating a basic flow to display a timestamp; deploying the flow, operating a node, and observing its behavior; then enhancing the flow to modify the format of the timestamp.
- Adding nodes that can collect data from your RIO, a *groov* View Data Store, and a PAC Control strategy.
- Creating and deploying a flow that accesses tag values from a fictional PAC Control strategy.

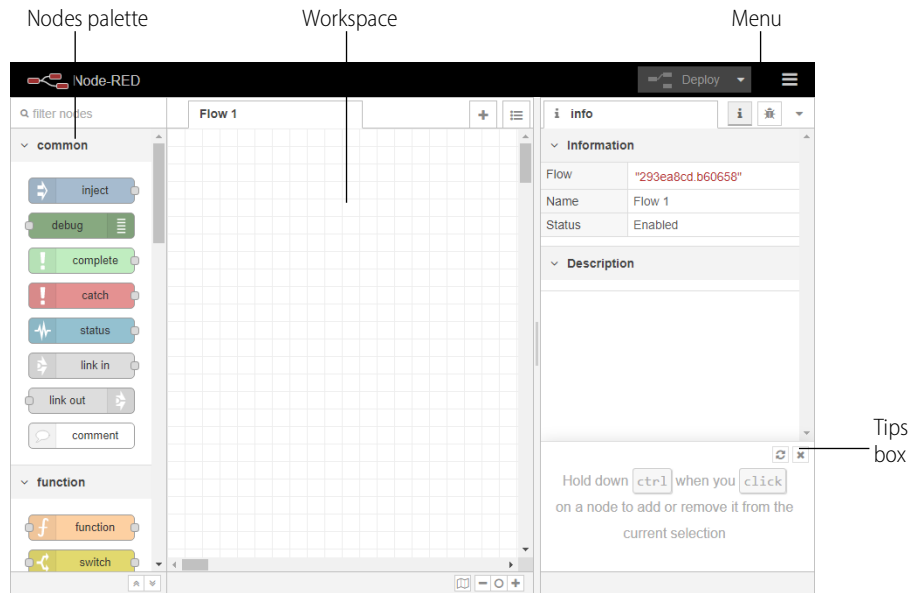
Before you start these exercises, make sure you enable Node-RED (see “Enabling Node-RED” on page 94) and that your *groov* RIO has access to the Internet.

Opening the Node-RED Editor

You can open the Node-RED editor with either of the following methods:

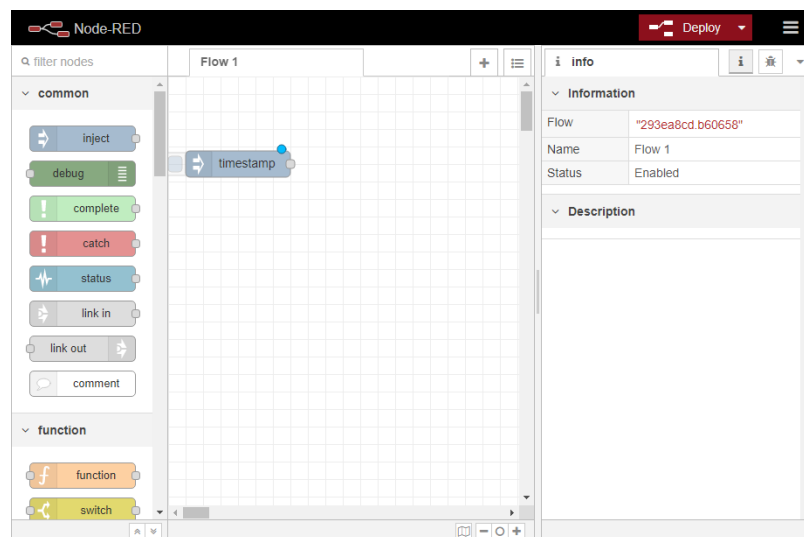
- Open a web browser and enter either of the following in the URL bar:
 - `https://[your groov RIO's hostname]/node-red`
 - `https://[your groov RIO's IP address]/node-red`Don't forget the “s” in **https**. Examples:
 - `https://opto-00-d2-da/node-red`
 - `https://192.0.2.20/node-red`
- If you are in *groov* Manage, click the menu button () , then select Home. From the Home page, click on Node-RED, then Open Node-RED Editor.

If you are new to the Node-RED Editor, take a moment to review the following diagram to familiarize yourself with the different parts of the editor.



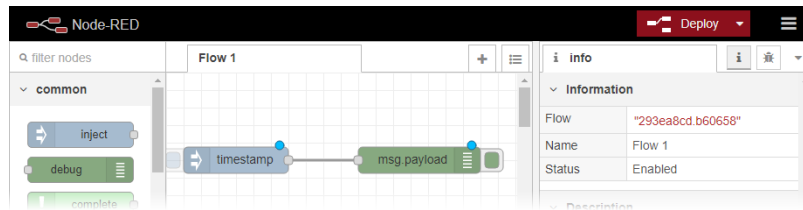
Creating a Flow

1. In the Nodes palette on the left, locate the *inject* node. Click and hold on it, then drag it to the workspace. The inject node lets you inject messages into a flow, either by clicking the button on the node or by setting a time interval between injects.
The **info** tab on the right side-bar displays information about the inject node's properties and a description of what it does:



- You might want to close the Tips box so that you can see more information in the **info** tab.
2. Scroll down in the Nodes palette and locate the *debug* node. Drag it to the workspace.

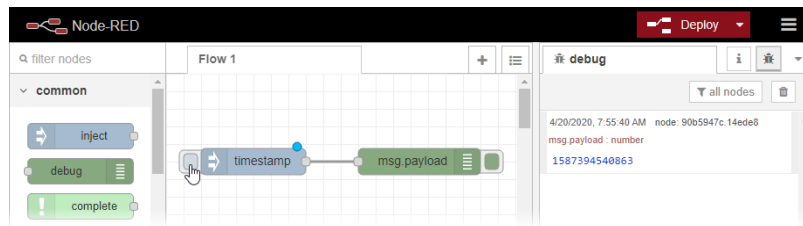
3. Wire the inject and debug nodes together by dragging from the output port of inject to the input port of debug.



Deploying the Flow and Testing It

The nodes exist only in the editor and must be deployed to the server.

1. Click the Deploy button in the upper right.
 2. In the right-sidebar, select the **debug** tab. (If you can't see the debug tab, click )
 3. Click the button on the left side of the inject node.
- Numbers appear in the sidebar:

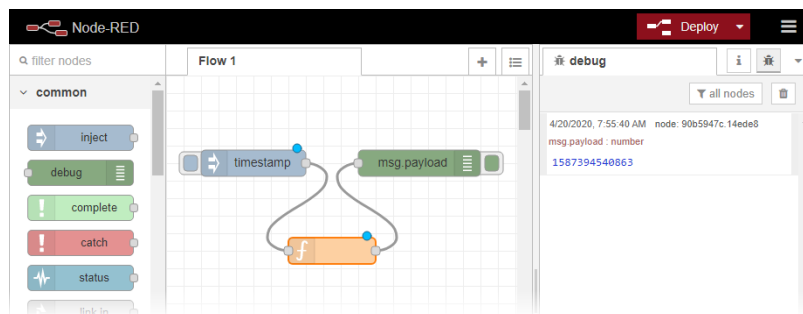


This number is a timestamp representing the number of milliseconds since January 1, 1970. This is the default payload of the Inject node.

Adding a Function Node

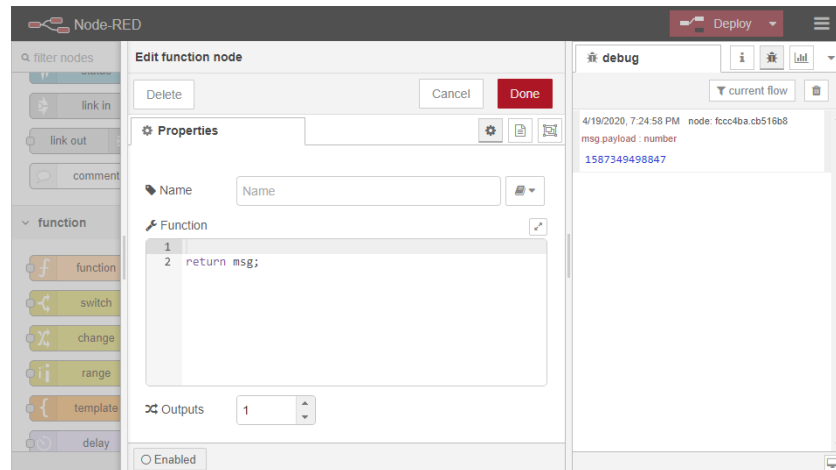
Let's make the timestamp more readable by using a Function node. Function nodes let you pass each message through a JavaScript function. If you don't know JavaScript, you may be able to find code you need using an Internet search.

1. Find the function node in the Nodes palette.
2. Click and hold on the function node, then drag it to the workspace, placing it between the inject and debug nodes. When the wire between the inject node and debug node becomes a dashed line, let go of the mouse button. The Node-RED editor automatically wires the Function node to the inject node and the debug (msg.payload) node.



If you didn't see a dashed line:

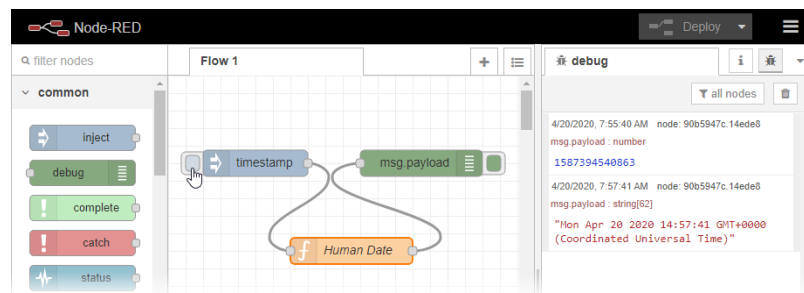
- a. Drop the function node near the inject and debug node.
 - b. Delete the existing wire by selecting it and pressing Delete on the keyboard.
 - c. Add a wire to link the output of the inject node to the input of the function node.
 - d. Add a wire to link the output of the function node to the input of the debug (msg.payload) node.
3. Double-click the Function node to edit it. The Node-RED editor displays the Edit function node panel.



4. In the Name field, type Human Date.
5. Copy the following code into the Function field, at line 1:


```
// Create a Date object from the payload
var date = new Date(msg.payload);
// Change the payload to be a formatted Date string
msg.payload = date.toString();
```
6. Leave this code in place at the end:

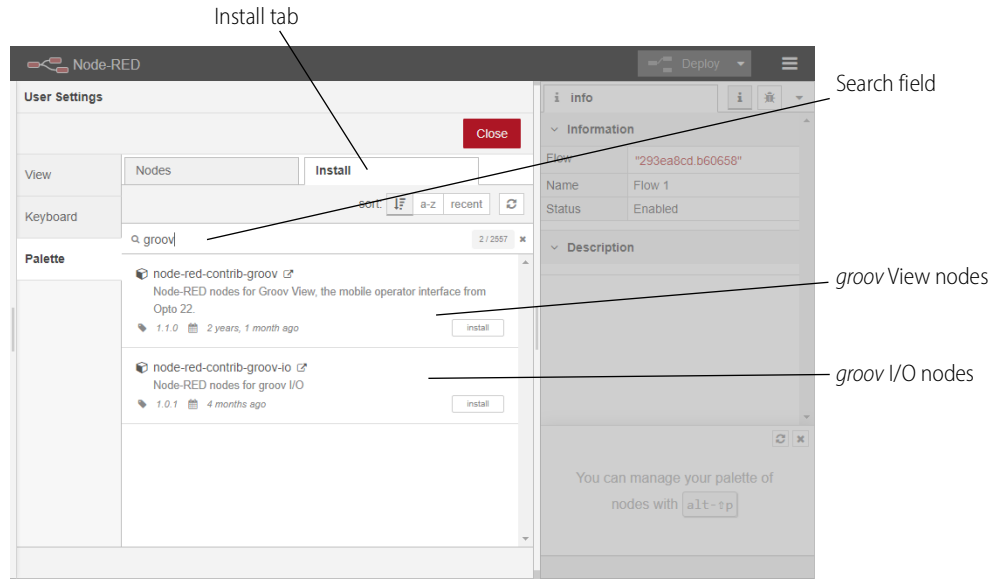

```
return msg;
```
7. Click Done to close the edit dialog box and then click the Deploy button.
8. Now when you click the Inject button, the message in the sidebar shows a more readable time stamp:



Installing groov I/O Nodes

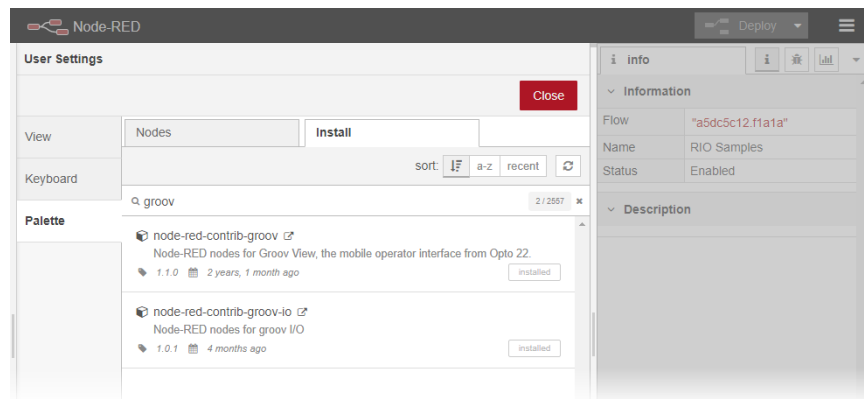
groov I/O nodes can read and write data from your RIO or from I/O modules on an EPIC.

1. Click the menu button (☰), then select Manage palette.
2. Click the Install tab.
3. In the search field, enter groov.



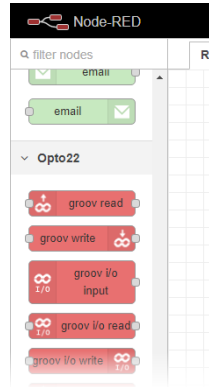
4. Find `node-red-contrib-groov-io` in the list and click the Install button next to it.
5. The Node-RED Editor displays a message about checking dependencies and reviewing node documentation. Click Install. When installation is finished, the small Install button changes color to gray and changes text to Installed.

While you are here, you can also install the groov View nodes. This will help you save some steps in the next section, “Installing groov View Nodes to Access Data Stores” on page 143. The following image shows both nodes installed.



6. Click Close.

The new *groov* I/O and *groov* View nodes appear in the nodes palette, under the heading Opto22.

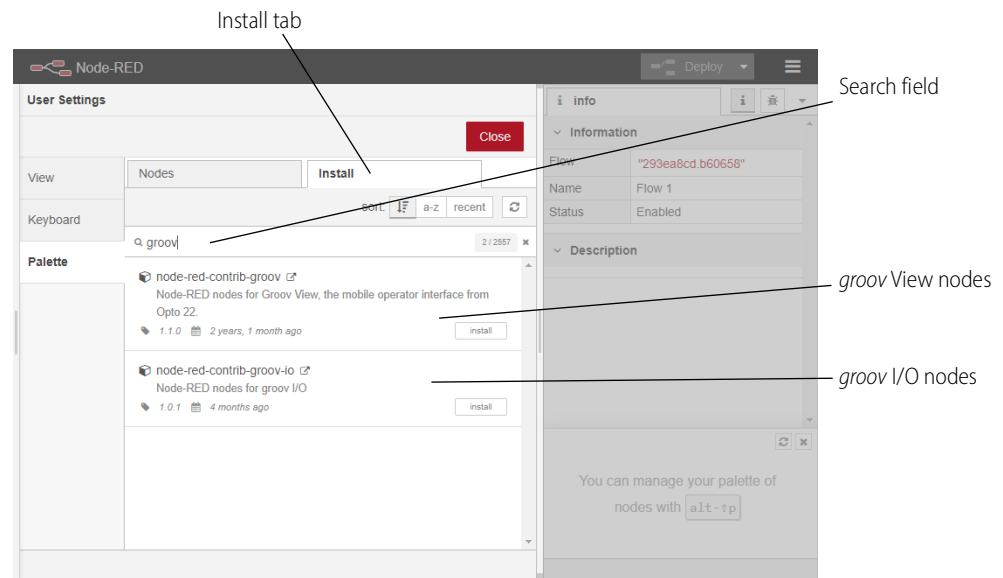


Installing *groov* View Nodes to Access Data Stores

*groov*View nodes can read and write data from a *groov*View Data Store. For an introduction to Data Stores and how to create them in *groov*View, see “Adding a Data Store” in the [groovView User's Guide](#) (form 2027). After you create the Data Store in *groov*View, you can access the Data Store in your Node-RED flow by accessing the *groov*View project that contains the Data Store.

If you already installed the node-red-contrib-groov nodes to the Node palette when you went through “Installing groov I/O Nodes” on page 141, you can skip to the next section.

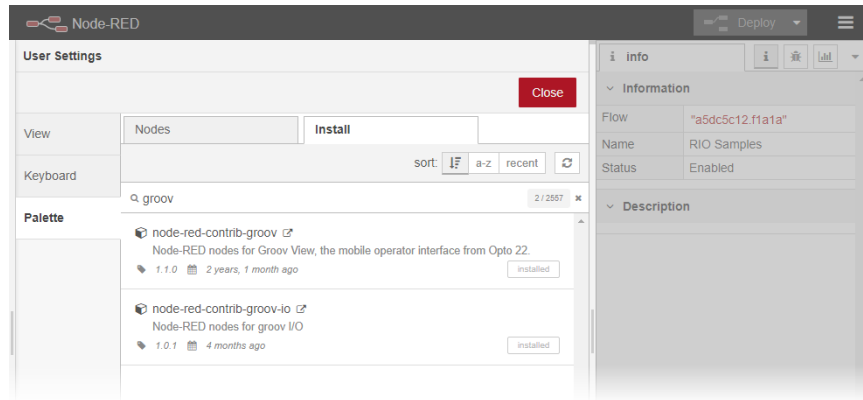
1. Click the menu button (☰), then select Manage palette.
2. Click the Install tab.
3. In the search field, enter `groov`.



4. Find `node-red-contrib-groov` in the list and click the Install button next to it.

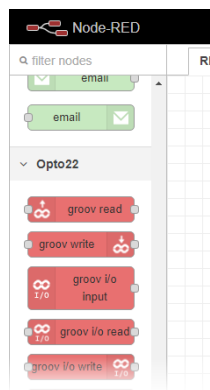
The Node-RED Editor displays a message about checking dependencies and reviewing node documentation. Click Install. When installation is finished, the small Install button changes color to gray and changes text to Installed.

The following image shows both groov I/O and groov View nodes installed.



5. Click Close.

The new *groov* I/O and *groov* View nodes appear in the nodes palette, under the heading Opto22.



Installing Opto 22 PAC Control Nodes

For this section, you'll add nodes to establish real-world communication with *groov* View Data Stores and tags in PAC Control strategies. You need either of the following:

- An Opto 22 *groov* EPIC processor running a PAC Control strategy, or
- a [SNAP PAC S-series or R-series industrial controller](#) with firmware R9.5 or higher, running a PAC Control R9.5 or higher strategy.

For either of these options, you need to complete the configuration instructions on developer.opto22.com. At the website, click on Node-RED for PAC Control, then expand Getting Started.

- For the *groov* EPIC processor, click on *groov* EPIC Controller Configuration.
- For the SNAP PAC controller, click SNAP PAC Controller Configuration.

As you complete the processor or controller configuration, make sure to save the following information:

- API Key Name and Value (for SNAP PAC)
- API Key (for *groov* EPIC)
- Path and file name to the SSL Certificate

After you set everything up and gathered this information, you can start:

1. Install Node-RED for PAC Control nodes just as you installed the *groov* View nodes. (Menu > Manage palette > Install tab. Search for `node-red-contrib-pac`.)
2. Make sure you have an inject and a debug node in the workspace.

3. Near the bottom of the Nodes palette, click and hold on the pac read node and drag it to the workspace, in between inject and debug (msg.payload).
The pac read node lets you read I/O and variable data in the PAC Control strategy.
4. Wire the pac node to the inject node and debug node, in the same way you wired the Function node.
5. Click the node and click the **info** tab to see helpful information about the node.
6. Double-click the pac read node to edit it.

Edit pac read node

Delete Cancel Done

node properties

Device Add new pac-device...

Data Type Device Details

Value msg.payload

Topic Do not alter

Node Name Name

7. Click the pencil at the right of the Controller field.

Edit pac read node > Add new pac-device config node

Cancel Add

Address HTTPS IP address

API Key Name Key name for SNAP; blank for Groov EPIC

API Key Value Value (secret)

SSL Certificates (PEM format)

CA or Self-Signed Path to CA certificate

Public Key Path to certificate (blank for self-signed)

8. Complete the fields:
 - a. For Address, choose a protocol and enter the IP address of the *groov* EPIC processor or the SNAP PAC controller.
 - b. For the API Key Name and API Key Value fields:
 - If you are accessing tags from a PAC Control strategy running on a SNAP PAC Controller, enter the API Key Name and Value you obtained when you configured the controller (as described on the previous page).
 - If you are accessing tags from a PAC Control strategy running on a *groov* EPIC processor, enter the API Key into the API Key Value field. Leave the API Key Name field blank.
 - c. For the SSL Certificates (PEM format) fields:
 - If you selected HTTPS as the protocol, read the information in the **info** tab to determine what to enter in these fields.
 - If you selected any other protocol, you can leave these fields blank.
 - d. Click Add.

The Node-RED editor returns you to the Edit pac read node panel, where your node is now configured to access the I/O and variable data in the PAC Control strategy running on the *groov* EPIC processor or the SNAP PAC controller:

Edit pac read node

Delete Cancel Done

node properties

Device 192.0.2.20

Data Type Digital Input

Tag Name Leave blank to get all tags

Value msg.payload

Topic Do not alter

Node Name Name

9. Choose the Data Type from the dropdown list.

The data type determines what other fields appear. In this example we chose Analog Input, so a field appears for Tag Name.

Edit pac read node

Delete Cancel Done

node properties

Device 192.0.2.20

Data Type Analog Input

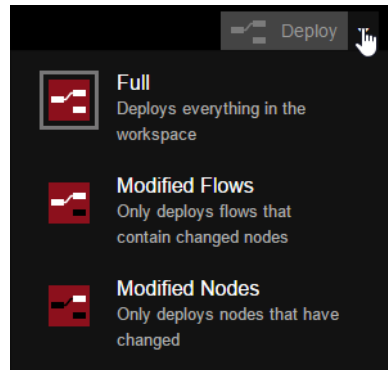
Tag Name aiOvenTemperature

Value msg.payload

Topic Do not alter

Node Name Name

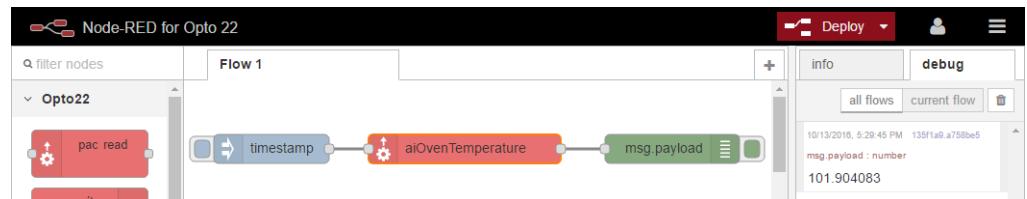
- a. **Tag Name**—Enter the exact I/O point or variable name from the PAC Control strategy running on this controller. If you leave this field blank, you'll receive values for all tags of this type (in this example, all analog inputs).
 - b. **Start Index and Length**—For a table, enter the starting index and length of the data you want to use.
 - c. **Node Name**—(Optional) By default, the tag name is used for this node. If you want to give it a different name, enter it here.
 - d. Click Done.
10. Click the down arrow next to Deploy to see your choices.



You can deploy everything, or if you don't want to disturb running flows, you can choose to deploy only the changed flows or changed nodes.

The gray box around the icon shows what will happen when you click the Deploy button. In this example, everything is deployed (Full).

11. Click Deploy. Now click the inject button and see what message appears in the debug tab. You should see the data from your PAC Control strategy. Here's how our example looks:



12: Maintaining a *groov* RIO

Maintain your *groov* RIO modules up-to-date and running smoothly by:

- Backing up your information regularly to make it easier to restore in the event of a reset or a firmware update.
- Applying firmware updates to apply the latest features, enhancements, and bug fixes.

If you encounter issues while operating your *groov* RIO, here are a few things you can do:

- You can troubleshoot some issues and, if you can't resolve your issues, there are some steps you can take to help Product Support solve your issues.
- If you had to restore your module to factory defaults, you can restore the information that you backed up.

BACKING UP YOUR *groov* RIO SETTINGS

Recommendations vary regarding when and how often you should back up your *groov* RIO:

- Before you apply a firmware update.
- Before you change configuration, like channel function.
- Periodically; for example, weekly or monthly.

Whichever recommendation you follow, the *groov* Manage Backup feature can save valuable configuration information, which you can then restore at a future date.

Note: *The backup feature saves only the first 10 MB of user files, which are files that either you uploaded manually to the module or were placed there by control programs.*

Save your backup to a storage medium (for example, a folder on a computer or a USB drive) that you can secure. The backup file may contain sensitive information that you'll want to protect. After you select a storage medium:

1. On a computer or mobile device that is connected to the storage medium where you want to save your back up file, log into your *groov* RIO UIO with a user ID with system administrator permission.
2. Click Maintenance > Backup.
3. On the Backup page, select the information you want to back up by clicking the corresponding switch so that it shows green (). By default, *groov* Manage backs up everything except Server SSL Certificates and active sessions (see "[Session Management](#)" on page 39). If you do not want certain information backed up, click the switch so that it shows grey ().
 - **I/O Configuration**—Save all the I/O channel configurations.
 - **Accounts and LDAP**—All local user accounts and passwords, plus each user account's permissions. For LDAP, the server information, settings for the user and group queries, and the default permissions for user and groups.

- **Networking**—Saves all of the following:
 - Hostname
 - The settings for the Ethernet 0 (ETH0) and WiFi.
 - The settings for the OpenVPN Tunnel 0.
 - The settings for the Network Options (DNS server IP address(es) and domain name(s), gateway IP address, the DNS order, and the gateway order).

This also includes sensitive information like the WiFi SSID and pre-shared key, and the OpenVPN server login credentials. If you enable this setting and do not enable encryption by *groov* Manage (review [step 4](#)), it's important that you apply your own security or encryption to the backup file to protect this information.

- **Firewall**—The firewall settings you selected, as well as any rules you created.
- **Time**—The time zone and time servers configurations.
- **Node-RED**—All your Node-RED projects and any nodes that you installed. Part of a Node-RED project can include a credentials file, which can contain sensitive information like user names, passwords, and security keys. If you enable this setting and do not enable encryption by *groov* Manage (review [step 4](#)), it's important that you apply your own security or encryption to the backup file to protect this information.
- **Data Service**—The configuration information for any MQTT clients and OPC UA servers that you may have created.
- **Client SSL Certificates**—All client SSL certificates you uploaded.
- **User Files**—Only the first 10 MB of files you uploaded manually or were placed there by control programs. After you create the backup file, you can review the log file to see which user files were stored in the backup file and which were not, as described in [step 8](#).
- **USB Settings**—The enable and automount settings you chose.
- **Bluetooth**—The enable setting you chose.
- **SNMP Configuration**—The two configuration files that contain the external host names and the Opto MIB definition.
- **Server SSL Certificates**—The server SSL certificates include sensitive information, like the web server's private key. If you enable this setting and do not enable encryption by *groov* Manage (review [step 4](#)), it's important that you apply your own security or encryption to the backup file to protect this information.
- **Sessions**—Save active user sessions; this is so users with active sessions do not have to log back in. This is useful if you are restoring settings to a *groov* RIO UIO that is replacing another *groov* RIO UIO that you are removing from active service.

4. In the Security section, select whether you want *groov* Manage to encrypt the backup file. If you toggle this switch on, note the following:
 - You **cannot** restore this backup file to any *groov* RIO UIO running firmware earlier than version 3.2.0.
 - You **can** restore this backup file to any *groov* RIO UIO running the same firmware.

Be aware that if you send a backup file without encryption to Opto 22, our personnel will have access to all the information in that file.

5. Click Download Backup.
6. Navigate to the folder or media where you want to store the backup file. *groov* Manage includes the date and time (in UTC) that you ran the backup as part of the file name. If you want to give it a different name, change the name in the File name field. Click Save.

NOTE: Some browsers might automatically download the file to a specific folder. Check your browser's downloads settings to determine where the browser stored the backup file.

7. If you did not select the option to have *groov* Manage encrypt the backup file, Opto 22 recommends that you apply some form of security on the backup file.
8. (Optional) Remember that *groov* Manage does not back up all user files. To check which user files were not included in the backup:
 - a. In *groov* Manage, click the menu button () , then select Info and Help.
 - b. Click Logs > *groov* Manage.
 - c. Review the log file for the list of user files that were and were not included in the backup file. Look for lines like the following:

A — [2020-04-16 21:58:31.498] [INFO] ComponentBackupRestore - Creating folder for User Files

[2020-04-16 21:58:31.503] [INFO] ComponentBackupRestore - Copying files for User Files

B — [2020-04-16 21:58:31.521] [INFO] ComponentBackupRestore - Copying /home/dev/secured/logo-rio-red-grey-569x197.png

[2020-04-16 21:58:31.538] [INFO] ComponentBackupRestore - Copying /home/dev/secured/rio.txt

[2020-04-16 21:58:31.550] [INFO] ComponentBackupRestore - Copying /home/dev/secured/temperature_log-1.csv

- A**—These lines indicate when *groov* Manage started backing up user files.
- B**—This line indicates the first user file that *groov* Manage backed up.
- d. Compare the list of files in the log with the list of files in the Internal Drive section of the Files page. (From the *groov* Manage Home page, click System > Files.) Note any differences and download the files that were not included in the backup.

RESTORING A BACKUP OR SPECIFIC SETTINGS FROM A BACKUP FILE

There are a few reasons why you may want to restore all or part of a backup:

- If you had to restore your module to factory settings, a backup can help you quickly restore a previously-saved configuration.
- You might want to restore a prior configuration or a specific part of a prior configuration; for example, only the firewall settings.
- After you apply an update, restoring a backup can help you quickly restore a previously-saved configuration.

When you want to restore a backup file, remember the following:

- You can restore a subset of the settings stored in a backup file; for example, only the firewall settings and the user accounts.
- When you restore from a backup file, the *groov* RIO UIO shuts down all services and applications, restores the projects and settings, and then restarts. Make sure to schedule the restoration during a time that minimizes its impact on your applications and equipment.
- The user accounts and passwords that are restored do not include any user accounts that you created after you created the backup file. Make sure you know the user account and password of any administrator account saved in the backup file so you can use that account and password when you log into the *groov* RIO UIO.
- If you selected to have *groov* Manage encrypt the file, you cannot use that file to restore settings to a *groov* RIO UIO running firmware earlier than version 3.2.0.

To restore a backup file or specific part of a backup file:

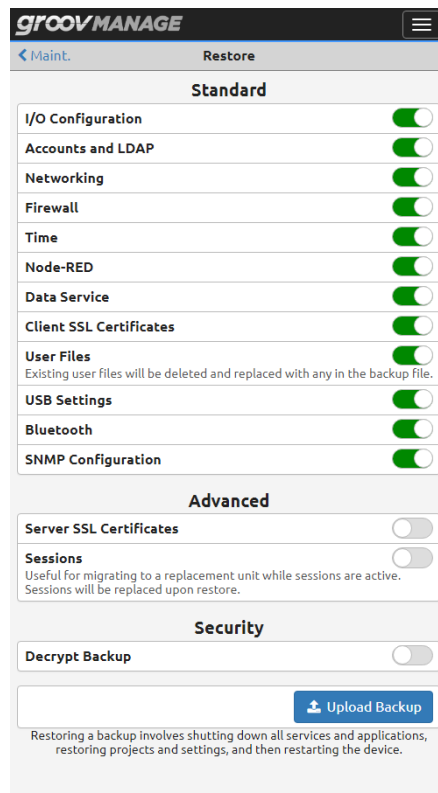
RESTORING A BACKUP OR SPECIFIC SETTINGS FROM A BACKUP FILE

1. Locate the media or folder that contains the backup file and remove any security you may have applied to the file.
2. On a computer or mobile device that contains the folder or is connected to the medium that contains the backup file, log into your *groov* RIO UIO with a user account that has system administrator permission.
3. Click Maintenance > Restore.
4. In the Restore page, select or deselect the settings you want to restore:
 - If you want to restore a setting, leave the switch green ().
 - If you do not want to restore a setting, click the switch so that it shows gray ().

Remember that if you selected to have *groov* Manage encrypt the backup file, enable the Decrypt Backup switch.

NOTE: If you select a setting that doesn't contain any information in the backup, nothing will be restored for that setting. This can happen if:

- When you created the backup, you deselected the setting.
- You select a setting that was not available in previous versions of the *groov* RIO UIO firmware.



groovMANAGE

← Maint. Restore

Standard

- I/O Configuration 
- Accounts and LDAP 
- Networking 
- Firewall 
- Time 
- Node-RED 
- Data Service 
- Client SSL Certificates 
- User Files 
Existing user files will be deleted and replaced with any in the backup file.
- USB Settings 
- Bluetooth 
- SNMP Configuration 

Advanced

- Server SSL Certificates 
- Sessions 
Useful for migrating to a replacement unit while sessions are active.
Sessions will be replaced upon restore.

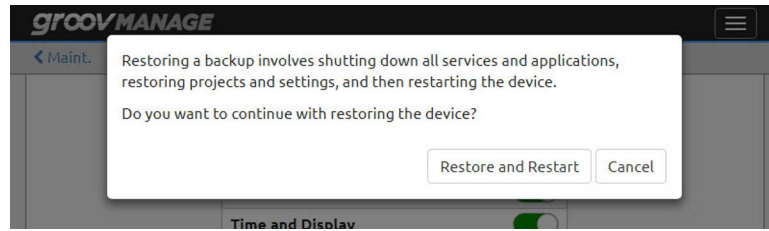
Security

- Decrypt Backup 

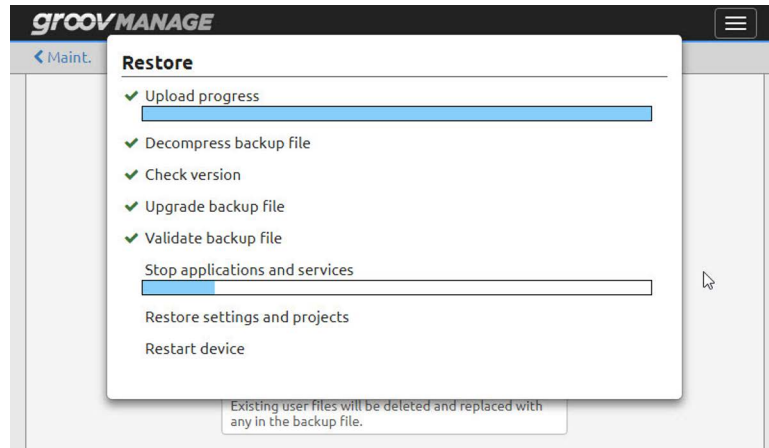
 Upload Backup

Restoring a backup involves shutting down all services and applications, restoring projects and settings, and then restarting the device.

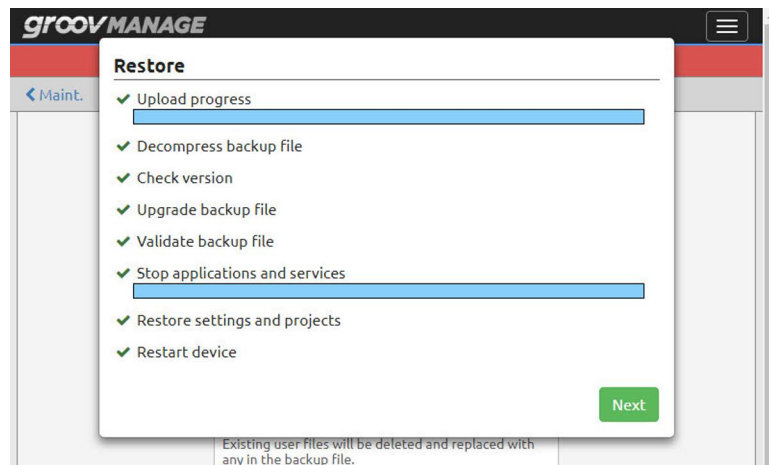
5. Click Upload Backup.
6. Navigate to the folder or media device that contains your backup file.
7. Click Open. *groov* Manage displays the following message, reminding you of what the *groov* RIO UIO will do during the restoration:



8. Click Restore and Restart. *groov Manage* displays a window that shows the progress of the restoration:

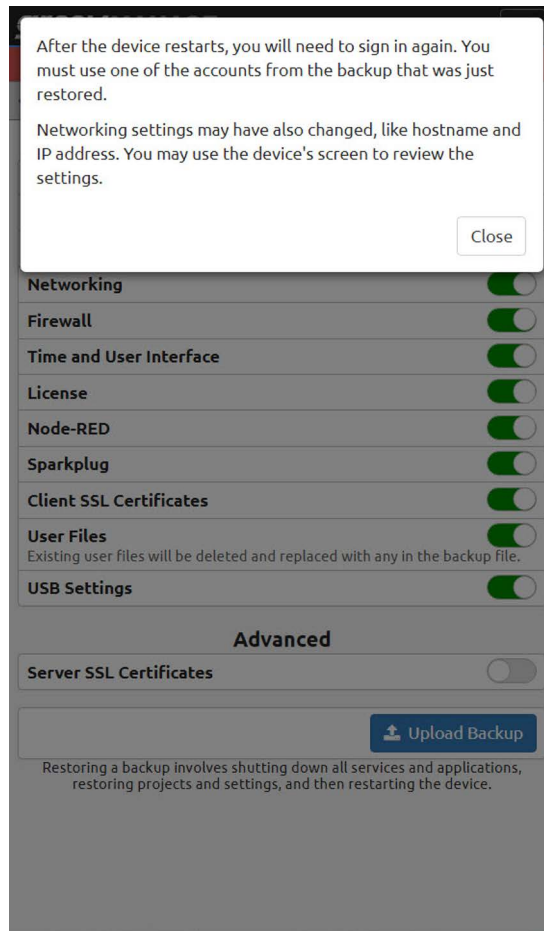


9. When *groov Manage* finishes restoring setting, the window looks like the following:



Click Next.

10. *groov* Manage displays a message that gives you a few tips about what you might need to do next. Read the message and then click Close.



11. The *groov* RIO UIO restarts. Wait for the *groov* RIO UIO login screen and log back in with any user account that has system administrator permission and was stored in the backup file.
12. Review the configuration settings such as I/O, date and time, and network to determine whether you need to update the values of those settings or make other changes.
13. Because the backup files contain only the first 10 MB of user files, if there were any additional files that weren't included in those 10 MB, upload them.

UPDATING FIRMWARE ON A *groov* RIO

Updating firmware on a *groov* RIO UIO keeps it up-to-date with the latest features and fixes. Updating firmware can take 20-30 minutes to complete and your *groov* RIO UIO will be restarted, so schedule the update during a time when it minimizes impact to your applications and equipment. If you have several *groov* RIO UIOs daisy-chained together, if you update the firmware on one *groov* RIO UIO, you must update the firmware on all the *groov* RIO UIOs in the chain.

Downloading and Installing the Firmware File

1. If you haven't done so recently, create a backup file (review "Backing up Your groov RIO Settings" on page 149). Keep this file handy and secure.

Note: *groov Manage provides you the option to automatically create a backup before it installs the firmware. However, if you have an excess of 10 MB of user files, or you don't want certain settings saved in the backup, manually create a backup following the directions in "Backing up Your groov RIO Settings" on page 149.*

2. Go to the Opto 22 website (opto22.com) and enter the part number for your groov RIO UIO in the Search box. Select the search result that includes "Firmware" as part of the title; for example GRV-R7-MM1001-10GRV-R7-I1VAPM-3 Firmware.
3. Click Download. Save the file to either:
 - A computer or mobile device that can connect to your groov RIO UIO, or
 - Media that you can then install to a computer or mobile device that can connect to your groov RIO UIO.

Important: *If you are updating multiple models of groov RIOs (for example, a GRV-R7-MM1001-10 and a GRV-R7-I1VAPM-3), pay attention to the file name. The part number of each model is pre-pended to the firmware file name. For example, the firmware file for GRV-R7-MM1001-10 begins with grv-r7-mm1001-10.*

4. Log into your groov RIO UIO with a user account that has system administrator permission. If you downloaded the file to an external storage medium, make sure that storage medium is connected to your computer.
5. From the groov Manage Home page, click Maintenance > Update.
6. On the Update page, decide whether you want groov Manage to create a backup file and, after the firmware upgrade, restore the settings stored in the backup file:

Current Firmware	2.0.0-b.12+beta
Build Date	2/19/2020
Back Up Settings Back up settings and automatically restore after the update.	
☒ Update System	

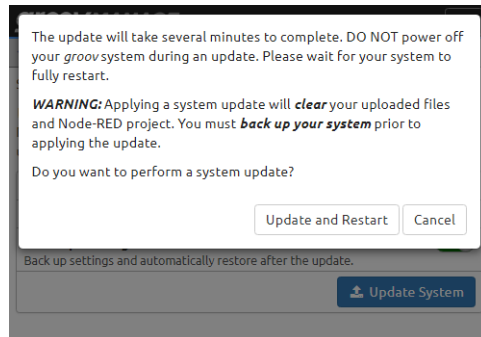
- If you leave the Back Up Settings switch on (the default), then all settings are saved before the firmware is upgraded. The groov RIO UIO restores the settings after it restarts. Leaving this setting on will also save you some steps later on.

If you created a backup file in step 1, note that the information in that backup file may not be the same as what groov Manage stores in the backup it creates as part of this step.

- If you *do not* want the settings saved then restored, click the switch so that it shows gray (). Turn this setting off if you want to restore your groov RIO UIO with settings from a different backup file; for example, the one you created in step 1.
7. Click Update System.
 8. Navigate to the storage medium or folder where you saved the file you downloaded in step 3.

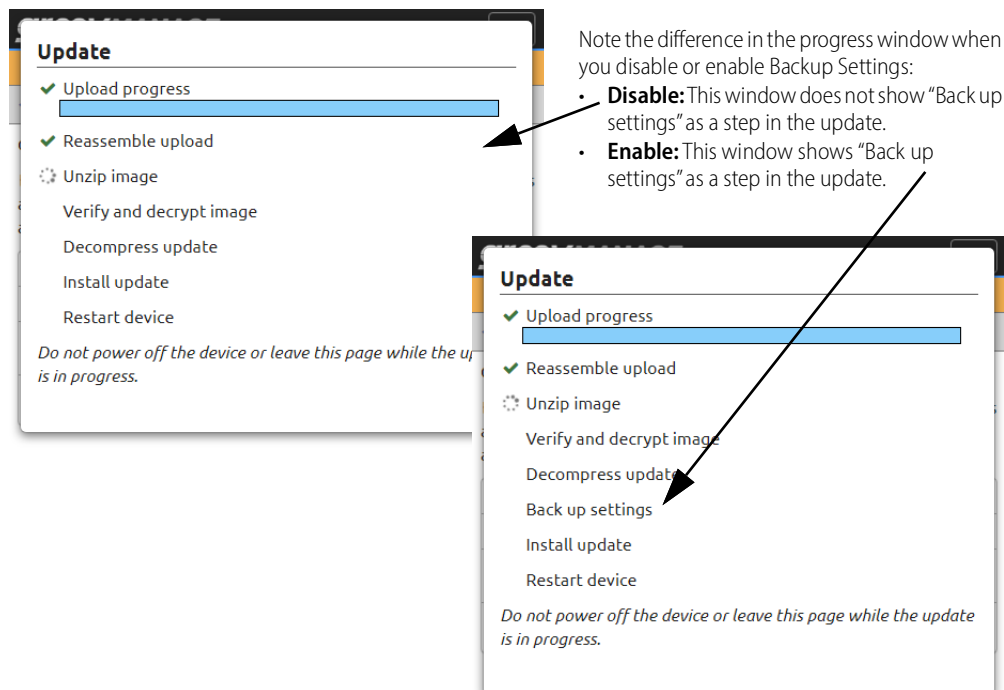
9. Click Open.

groov Manage displays a message to remind you that the firmware update clears all your settings and projects, giving you one more opportunity to cancel and perform that important backup.



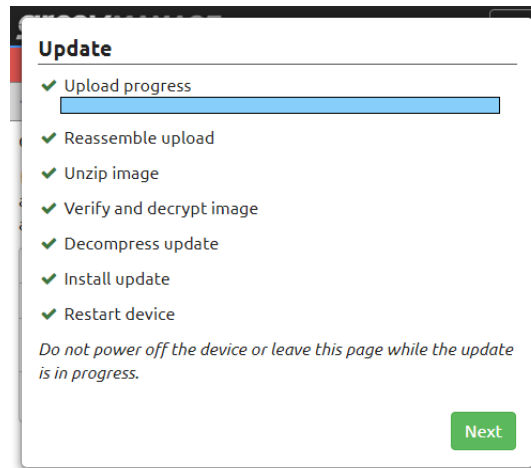
10. If you are ready to proceed with the update, click Update and Restart.

groov Manage displays an Update window, which shows you the progress of the update. The update can take 10 to 20 minutes to complete. During that time, the banner (now behind the Update window) changes color to yellow.

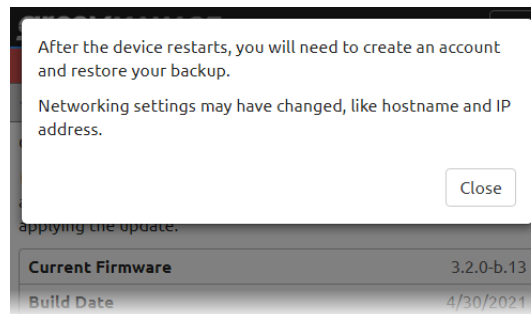


Watch for the banner to turn red, which indicates that the update is finished and that your *groov* RIO UIO is now offline.

11. After a successful install, the Update windows shows all items as checked off and displays the Next button. Click Next.



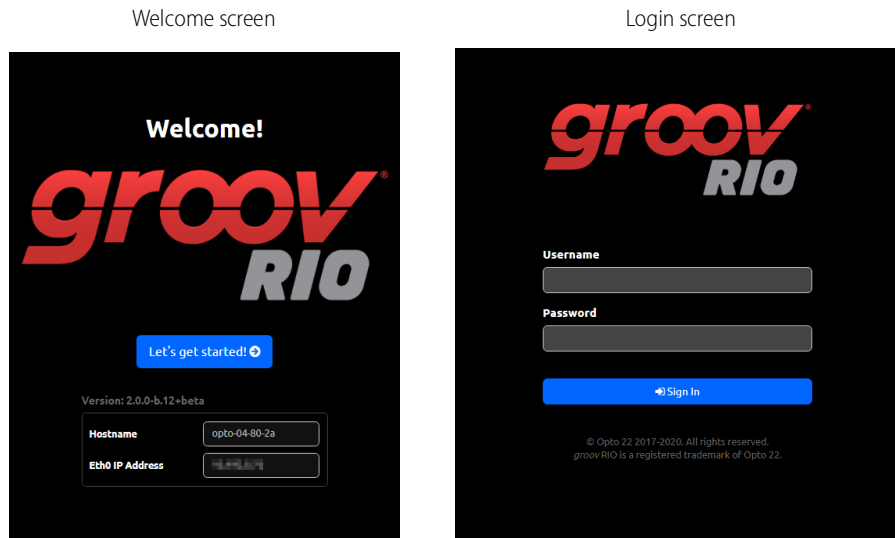
12. Read the instructions on what to do after the *groov* RIO UIO restarts, and then click Close.



13. If you can see the *groov* RIO UIO, look at the STAT LED. When it is solid green, the restart is finished and the browser refreshes. If you can't see the module, you will know that the restart is done when the browser refreshes.

Note: If the browser doesn't refresh after about 5 minutes, refresh it manually. (Each browser has a different key or combination of keys for refreshing: F3, F5, or CTRL+R are some examples.)

14. When the restart is done, you'll see one of the following screens.



If you see the Welcome! screen (you'll see this screen if you **d**eselected the Back Up Settings option in [step 6](#) on [page 155](#)):

- Make a note of the IP address shown in the Eth0 IP Address box. You'll need it in the next few steps.
- Click Let's get started! and create a system administrator account and password. (It does not have to match any that might be stored in a backup file; however, you still do have to remember to store it in a safe location for later recall.)
- Click on Configure Device.
- If you want to restore a backup file, do that now (for instructions, review ["Restoring a Backup or Specific Settings from a Backup File"](#) on [page 151](#)).

If you see the login screen (you'll see this screen if you enabled the Back Up Settings option in [step 6](#) on [page 155](#)), log into your *groov* RIO with a user account that has system administrator permission.

If you see neither screen (likely because your network settings were not backed up as part of the update), use *groov* Find to get the IP address or hostname of the *groov* RIO UIO (review ["Downloading and Running groov Find"](#) on [page 159](#)).

TROUBLESHOOTING

Browser Reports that URL to *groov* RIO UIO is Unreachable

There are several reasons that a browser may report that it cannot connect to your *groov* RIO UIO through its hostname; some of those reasons may be physical connectivity issues, some may be network configuration issues. Here are a few things to check:

- For wired Ethernet connections, verify that the Ethernet cable that you inserted into the *groov* RIO UIO's Ethernet port is connected to the network.
- Make sure the STAT LED is solid green before you attempt to connect to your *groov* RIO UIO. (For a diagram that shows you where the STAT LED is located, review [page 8](#).)
- Check that the LED of the Ethernet port (ETH0 or ETH1) is showing link speed and activity. (For an explanation of LED activity, review [page 8](#).)
- If the *groov* RIO UIO is connected to a network that does not automatically assign IP addresses to new devices (which typically means the network is not managed by a DHCP server), download *groov* Find to

help you locate your *groov* RIO on your network (see below). You *must* use *groov* Find if your network does not have DNS.

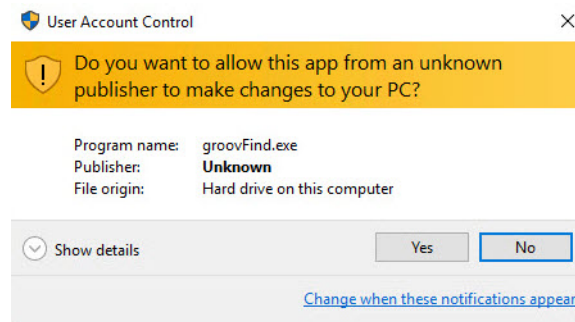
Downloading and Running *groov* Find

groov Find is an application available on the Opto 22 website (for Windows® PCs) or the Mac® App Store (for Mac computers) that can help you locate *groov* RIOs, *groov* EPICs, and *groov* Boxes on your network.

Instructions for PC Users:

1. Download [groov Find](#) from our website (go to www.opto22.com and enter `groov Find` in the search box).
2. Save the file (`groovFind.exe`) to your computer.
3. Open the `groovFind.exe` file.

If you have User Account Control (UAC) turned on, Windows displays a message asking you to allow *groov* Find to make changes to your computer.



NOTE 1: If you are using a Windows account that does not have Administrator privileges (such as Guest), you need to enter the Administrator username and password to use *groov* Find. If you do not have this information, contact your IT department.

NOTE 2: Clicking **Yes** permits *groov* Find to have temporary administrative privileges to create an additional temporary IP address for each network interface on the computer. This enables *groov* Find to locate a *groov* device on a network that does not have DNS and DHCP. If the network does not have DNS and DHCP, you need to assign a static IP address to the *groov* device to maintain communication. If the network does have DNS and DHCP, the temporary IP address is not used and is removed when you exit *groov* Find.

4. Click **Yes**.
groov Find opens and automatically searches for *groov* RIOs, *groov* EPICs, and *groov* Boxes on the network.
5. Locate the serial number on the *groov* device.
 - On *groov* EPIC, open the LCD display and look at the label on the back of the display.
 - On a *groov* Box, find the label on the bottom of the Box.
 - On a *groov* RIO, the label is on the module's side. The serial number is indicated by **SN**.

6. Locate the matching serial number in *groov* Find.

Use the **Search For Devices** button to find all of the *groov* Devices that this computer can access.

Search For Devices

Find the serial number of your *groov* Device and select one of its links.

Device Type	Serial Number	Hostname	IP Address	Open in browser...
GROOV-AT1	...	opto-...	...	groov Admin groov View
GROOV-AR1	...	opto-...	...	groov Admin groov View
GROOV-AR1	...	...	...	groov Admin groov View
GROOV-AT1	...	opto-...	...	Click to start groov
GROOV-AT1	...	opto-...	...	Click to start groov
GRV-R7-MM1001-10	...	opto-...	...	Click to start groov Manage
GRV-R7-MM1001-10	...	opto-...	...	Click to start groov Manage
GRV-EPIC-PR1	...	...	...	Click to start groov Manage
GRV-R7-MM1001-10	...	opto-...	...	Click to start groov Manage
GRV-R7-MM1001-10	...	RIO-...	...	Click to start groov Manage
GRV-R7-MM1001-10	...	rio-...	...	Click to start groov Manage

Note: If your device was not found, wait 60 seconds and try again. [more info](#)

Serial number

If you do not see the serial number right away, wait 60 seconds, and then click **Search For Devices**.

7. Click the link (in the right-most column) to start *groov* Manage.

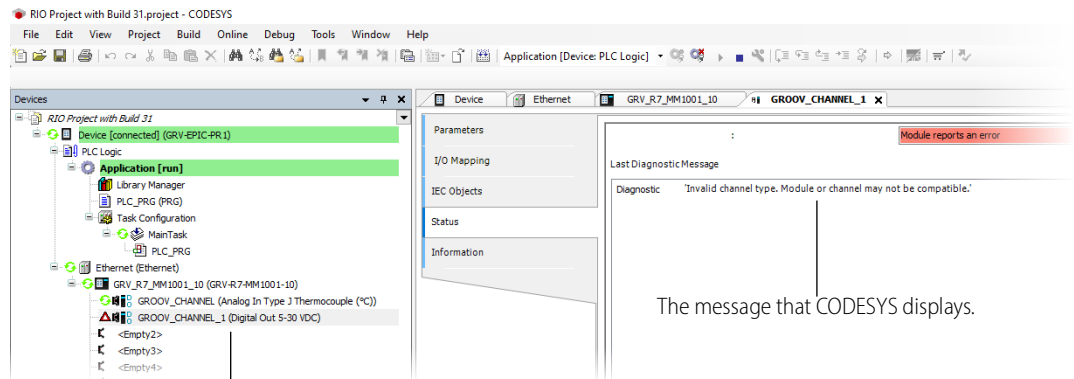
Instructions for Macs:

1. Locate the serial number on the *groov* device.
 - On *groov* EPIC, open the LCD display and look at the label on the back of the display.
 - On a *groov* Box, find the label on the bottom of the Box.
 - On a *groov* RIO UIO, the label is on the module's side. The serial number is indicated by **SN**.
2. On your Mac, go to the Mac App Store.
 - Click the apple menu (top left corner) and select **App Store**.
 - Click **Finder > Applications** and click **App Store**.
3. In the store, enter *opto 22* in the search box.
4. Click **Get** on the *groov* Find app. If requested, enter your Apple Store ID and password.
5. Click **Open** to start the *groov* Find app. Within a few moments, *groov* Find begins locating *groov* RIOs, *groov* EPICs, and *groov* Boxes on your network and displays them in a list.
6. Under the **Serial Number** column, locate the serial number of your *groov* device and select it.
7. At the bottom of the window, click either **Open groov View** or **Open groov Manage**. Your default browser opens with the *groov* device's IP address in the URL bar, and then loads either *groov* View or *groov* Manage.

CODESYS: "Invalid Channel Type. Module or channel may not be compatible."

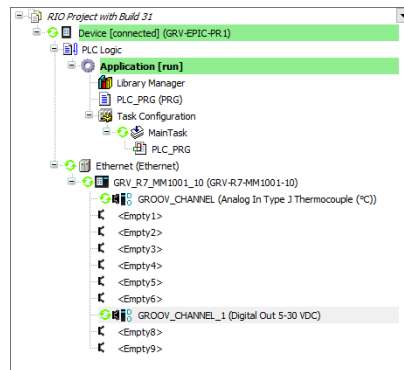
There are certain combinations of signal types that aren't supported on GRV-R7-MM1001-10 (for details, see [KB88975](#)). CODESYS does not prevent you from creating these combinations, so you might not know you

created one until you try to download your project. When this happens, you'll see the following messages on the channels that are incorrectly configured:



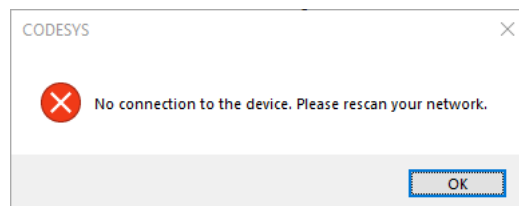
A GRV-R7-MM1001-10 with an unsupported combination of signal types on channels 0 & 1.

To correct this problem, move the problematic signal type to another channel based on guidance given in [KB88975](#). In this example, we moved the digital sinking output from channel 1 to channel 7:



CODESYS: Can't Connect to *groov* RIO Module

You may see this message from the CODESYS Development System when you are trying to connect (**Online > Login**) to the *groov* RIO UIO or it may appear as you are debugging your application:



This could be caused by several different reasons:

- **Physical disconnection**—Check for the following:
 - Is the *groov* RIO UIO turned off?
 - Is the Ethernet cable disconnected?

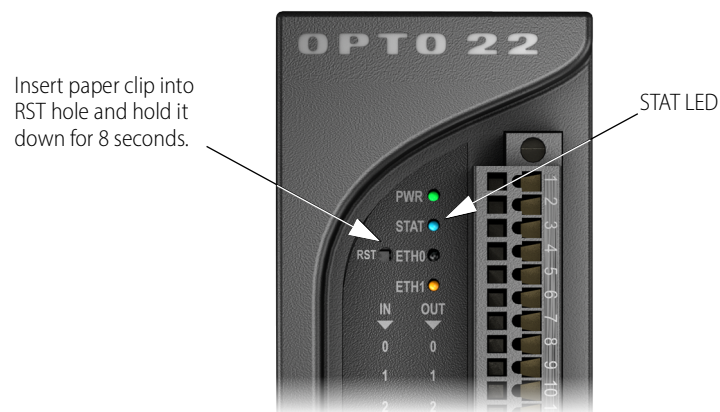
RESETTING TO FACTORY DEFAULTS

- Is the module in independent mode? If so, did the Ethernet cable get moved to a different Ethernet network interface on the module? If so, check your firewall settings. For instructions, see [“Configuring the Firewall” on page 45](#).
- If you are connecting to the *groov* RIO UIO through WiFi, was the WiFi adapter removed?
- **Network instability**—Check for the following:
 - If you are connecting to the *groov* RIO UIO through WiFi, is the WiFi adapter experiencing connectivity problems?
 - Is the network experiencing instability issues?
- ***groov* RIO UIO configuration issues**—Check for the following:
 - If you did not license the CODESYS Runtime Engine, you have been running in two-hour trial mode and the two hours might be up. You can do one of two things:
 - Enable the CODESYS Runtime Engine for another two hours (see).
 - Obtain and apply the GRV-LIC-CRE-RIO license, which removes the two-hour time limit (see).
 - Was the CODESYS Runtime Engine on the *groov* RIO UIO disabled? To enable it, see .
 - Was the Ethernet cable plugged into ETH1 and you did not modify the module’s firewall to open a port for CODESYS on ETH1? To open the port, see .
 - If you are connecting to the *groov* RIO UIO through WiFi, did you modify the module’s firewall to open a port for CODESYS on wlan0? To open the port, see .

RESETTING TO FACTORY DEFAULTS

You might have to reset to factory defaults if instructed to do so by product support. A reset to factory defaults erases all the changes you made to the *groov* RIO UIO, which is why it is important that you regularly back up your system. (For instructions, review [“Backing up Your groov RIO Settings” on page 149](#).)

Insert a paper clip into the RST hole and push down for approximately 8 seconds. Release the button when the STAT LED alternates between red and green.



COLLECTING INFORMATION FOR PRODUCT SUPPORT

groov RIO UIO displays messages and collects information in several logs that can help Opto 22’s Product Support diagnose and solve issues. If you contact Opto 22 for help, the Product Support team will direct you on what specific information to collect and how to send it to them.

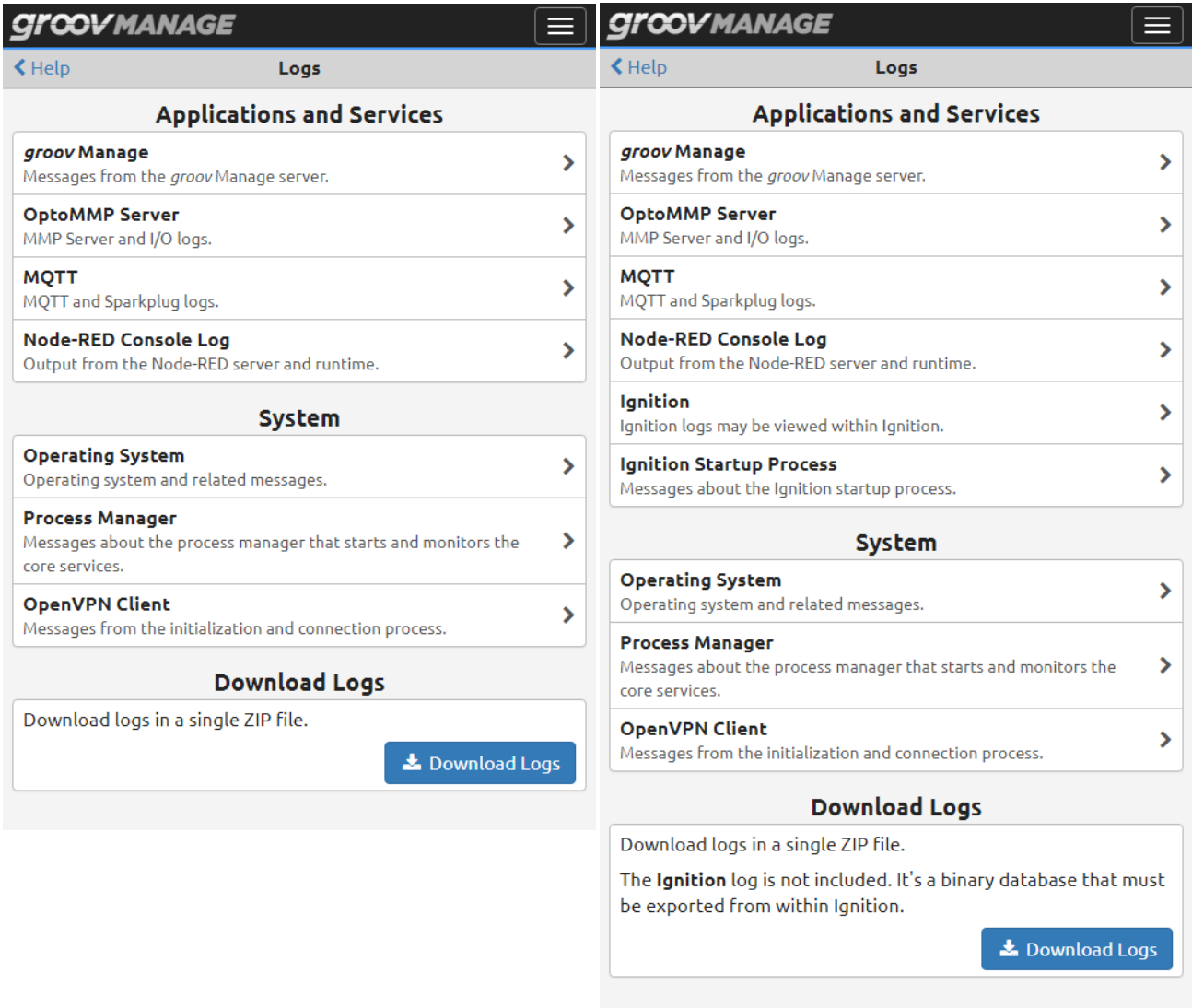
You might want to create a new folder on your computer or mobile device with the name of the Opto 22 ticket number, if you have one, and store the log files and additional information into that folder.

If Product Support directs you to send log files:

1. On a computer or mobile device, log into your *groov* RIO UIO with a user ID that has system administrator privileges.
2. Click **Info and Help > Logs**. *groov* Manage displays the Logs page.

GRV-R7-MM1001-10

GRV-R7-MM2001-10



3. Download either the specific log file(s) requested by Product Support or all of the logs:
 - If you want to download individual logs, click on the application, service, or system name. *groov* Manage displays the log file's page. At the top of the page, click **Download**.
 - If you want to download all the log files, click **Download All Logs**.
4. Navigate to a folder on your computer or mobile device where you want to save the log. You might also want to make note of the name of the log file or modify it to something else.
5. Click **Save**.

CONDUCTING AN OPTOSUPPORT REMOTE SUPPORT SERVICE (RSS) SESSION

6. If you are downloading individual logs, repeat steps 3 through 5 for each log that Product Support directs you to download.

Send this information to Opto 22 as directed by Product Support.

CONDUCTING AN OPTOSUPPORT REMOTE SUPPORT SERVICE (RSS) SESSION

An OptoSupport Remote Support Service (RSS) session can help expedite the resolution of your support ticket by allowing an Opto Product Support team member to remotely connect to your *groov* RIO UIO to continue with diagnostics and troubleshooting.

After evaluating the progress of your ticket, your Opto 22 Product Support team member might determine that your situation would benefit from an RSS session and discuss with you these benefits and the goals of the session. If you agree with this option, our team member will schedule a time to start a Remote Support Service (RSS) session.

Before beginning the session, it's important that you prepare your *groov* RIO UIO by checking the following:

- Verify that your *groov* RIO UIO has an internet connection.
- If your internet connection travels through a firewall or router, verify that the firewall or router does not prevent outbound connections through port 555.

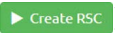
An RSS session typically runs like this:

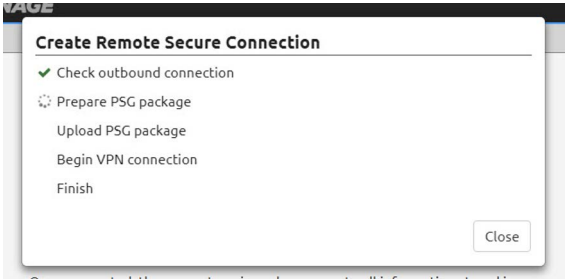
1. At a time agreed upon by you and your Opto Support team member, you initiate a phone call.
2. When instructed, click **Create RSC** to initiate the session. For detailed instructions and an explanation of what happens during this step, review ["Initiating an RSS Session" on page 164](#).
3. After the session is successfully created, you and your Opto Support team member review the details of your situation and discuss additional steps. These steps might be:
 - Continue active discussion of the issue over the phone while the Opto Support team member diagnoses and troubleshoots your *groov* RIO UIO.
 - Agree to a plan of action where you can end the phone call while the Opto Support team member continues to diagnose and troubleshoot your *groov* RIO UIO.

If the session is lengthy, part of the plan might include pausing the session and continuing it at a later time. For additional instructions about pausing and resuming a session, review ["Pausing and Resuming an RSS Session" on page 165](#).

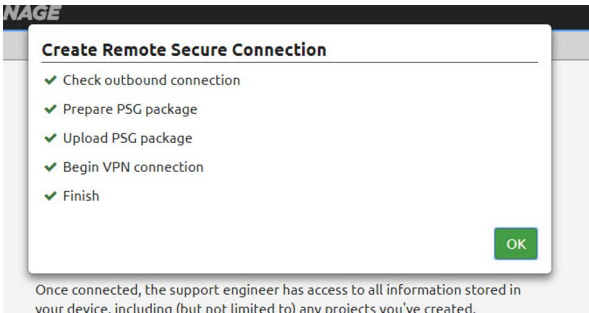
4. When it is time to end the RSS session, click **Delete RSC**. For important information about what happens when you end an RSS session, review ["Ending the RSS Session" on page 166](#).

Initiating an RSS Session

1. The Opto 22 Support team member asks you to navigate to the OptoSupport RSS page, if you haven't already done so. (From the *groov* Manage home page, click or tap **Info and Help** > **OptoSupport RSS**.)
2. The Opto 22 Support team member asks for the serial number listed on the OptoSupport RSS page. This information is necessary for the connection to be successful.
3. When instructed by the Opto 22 Support team member, click **Create RSC** ().
4. The OptoSupport Remote Support Service Permission and Release Agreement appears. To proceed with the session, click **Accept** to accept the terms of the agreement.
groov Manage displays a status message of the steps to create the connection environment:



5. When all steps are complete, click **OK** to close the message box:



While your *groov* RIO UIO establishes a connection, the **Status** section of the OptoSupport RSS page displays the following:



After the connection is established, the **Status** section of the OptoSupport RSS page displays the following:



Do **not** turn off your *groov* RIO UIO after you start the session. If this happens, you will need to restart this process.

Pausing and Resuming an RSS Session

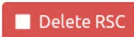
During the diagnosis and troubleshooting, you and your Opto Support team member might agree to pause the session and resume it at a later time. Pausing the session prevents communication between the Opto Support team member and your *groov* RIO UIO while preserving the information needed to quickly resume the connection.

CONDUCTING AN OPTOSUPPORT REMOTE SUPPORT SERVICE (RSS) SESSION

- To pause a session, click **Pause** in the OptoSupport RSS page (**Info and Help > OptoSupport RSS**). *groov* Manage displays a message confirming the pause. Click **OK** to close the message. The OptoSupport RSS page updates the **Status** section to indicate the RSS session is paused:

Status	Connection paused
	
	

- To resume a session, click **Continue RSC** in the OptoSupport RSS page (**Info and Help > OptoSupport RSS**). After the connection is re-established, the OptoSupport RSS page updates the **Status** section to indicate the RSS session is active (connected).

Status	Connected
	
	

Ending the RSS Session

When it is time to end the RSS session, click **Delete RSC** in the OptoSupport RSS page (**Info and Help > OptoSupport RSS**). All of the information that your *groov* RIO UIO created to establish the connection is erased. If you need to start another RSS session, you need to start from the first step in ["Initiating an RSS Session" on page 164](#).

A: Specifications

GRV-R7-MM1001-10, GRV-R7-MM2001-10

You can configure GRV-R7-MM1001-10 and GRV-R7-MM2001-10 with any combination of the following inputs and outputs:

- Up to 2 electromechanical relays
- A combination of up to 8:
 - discrete or analog inputs
 - discrete or analog outputs

Not all types of discrete and analog I/O are supported on all channels; the specifications table on [page 169](#) lists which channels support which channel types. Features are listed on the next page.

Features

GRV-R7-MM1001-10 GRV-R7-MM2001-10		Signal Type					
	DI: • Discrete • Switch Input, Powered	DI: • Discrete • Switch Input, Powered	DO: • DC Sinking	DO: • Form C Mech. Relay	AI: • Voltage • ICTD • Thermistor • Resistor	AI: • Current • Thermocouple • Millivolt	AO: • Voltage • Current
Channels	0-1	2-7	0-7	8-9	0-7	0-3	4-7
Features							
On/off State	•	•	•	•			
On/off Latching	•						
Counting	•						
On/off Totalization	•						
Frequency Measurement	•						
Period Measurement	•						
Pulse Measurement	•						
Scaling					•	•	•
Offset and Gain					•	•	
Minimum/Maximum Values					•	•	
Average Filter Weight					•	•	
Simple Moving Average							
Analog Totalizing					•	•	
Output Pulsing / TPO			•				
Ramping							•
Clamping							•
Watchdog Timeout Value			•	•			•
Quality Indication					•	•	•

SPECIFICATIONS

Specification		GRV-R7-MM1001-10 GRV-R7-MM2001-10
Voltage Input		
Available Channels		0–7
Input Range		0–10 V DC
Over-range Limit		0–11 V DC
Resolution		0.5 mV
Accuracy		±0.05% of range (±5 mV)
Gain Temperature Coefficient		30 ppm/°C
Offset Temperature Coefficient		15 ppm/°C
Input Impedance		> 425 kOhms
Data Refresh Time		550 ms
50 / 60 Hz rejection		> 90 dB
Current Input		
Available Channels		0–3
Input Range		0–20 mA, 4–20 mA
Over-range Limit		0.0–20.8 mA, 2.0–20.8 mA
Recommended Fuse		32–40 mA, Fast Acting (for example, Eaton S500-32-R)
Resolution		1.0 µA
Accuracy		±0.05% (±10 µA)
Gain Temperature Coefficient		30 ppm/°C
Offset Temperature Coefficient		15 ppm/°C
Input Voltage Drop (±10%)		0.9 V @ 4 mA, 2.0 V @ 20 mA, 25 °C
Equivalent Input Impedance (±10%)		225 Ohms @ 4 mA, 100 Ohms @ 20 mA, 25 °C
Data Refresh Time		550 ms
50 / 60 Hz rejection		> 90 dB
ICTD Input		
Available Channels		0–7
Input Range with ICTD Probe		–40 to +100 °C
Resolution		0.04 °C
Accuracy with ICTD Probe		±1.0 °C (1.8 °F)
Gain Temperature Coefficient		30 ppm/°C
Offset Temperature Coefficient		60 ppm/°C
Data Refresh Time		550 ms
50 / 60 Hz rejection		> 90 dB

CONTINUED ON NEXT PAGE.

SPECIFICATIONS

Specification		GRV-R7-MM1001-10 GRV-R7-MM2001-10	
Thermocouple Input			
Available Channels	0–3 (see Note)		
Nominal Input Range	-75 to +75 mV		
Full Scale Range	-78 to +78 mV		
Input Resolution	3 microvolts		
Input Impedance	> 1 megohm		
Data Refresh Time	550 ms		
50 / 60 Hz rejection	> 90 dB		
Thermocouple ITS90 Types	± Accuracy / Resolution		
B: 90 °C to 1,820 °C	7 °C / 0.4 °C		
E: -80 °C to 1,000 °C	2 °C / 0.1 °C		
J: -100 °C to 1,200 °C	2 °C / 0.1 °C		
K: -80 °C to 1,372 °C	2 °C / 0.1 °C		
N: -100 °C to 1,300 °C	3 °C / 0.1 °C		
R: 100 °C to 1,768 °C	7 °C / 0.3 °C		
S: 100 °C to 1,768 °C	7 °C / 0.3 °C		
T: -60 °C to 400 °C	3 °C / 0.1 °C		
Note: To achieve the best thermocouple accuracy when also using current outputs or discrete outputs, always configure thermocouples on the lowest channel numbers and outputs on the highest channel numbers.			
Millivolt Input			
Available Channels	0–3		
Input Ranges	±150 mV, ±75 mV, ±25 mV		
Over-range Limits	±165.0 mV, ±78.0 mV, ±27.5 mV		
Resolution	10 µV, 3 µV, 2 µV		
Accuracy	±0.1% of Full Scale (±150 µV) ±0.1% of Full Scale (±75 µV) ±0.2% of Full Scale (±50 µV)		
Input Impedance	> 1 MOhms		
Data Refresh Time	550 ms		
50 / 60 Hz rejection	> 90 dB		

CONTINUED ON NEXT PAGE.

Specification		GRV-R7-MM1001-10 GRV-R7-MM2001-10
Thermistor Input (Requires firmware version 3.0.0 or later)		
Available Channels	0–7 (see Note)	
Input Range (Ohm)	0-400 k	
Accuracy (Ohm @ Range)	greater of 3 Ohm or 0.5%@0-25k, 400@25k–50k, 900@50k–75k, 1.5k@75k–100k, 5k@100k–200k, 20k@200k–400k	
Gain Temperature Coefficient	500 ppm/°C	
Resolution (Ohm @ Range)	0.5@0–1k, 1@1k–5k, 2@5k–10k, 5@10k–25k, 50@25k–100k, 200@100k–200k, 700@200k–400k	
Power Dissipation @ Resistance (µW @ Ohm)	375@1k, 950@5k, 1075@10k, 875@25k, 600@50k, 450@75k, 350@100k, 200@200k, 100@400k	
Predefined Thermistor Curves	Accuracy (°C) @ Range (°C)	
2252	0.2 °C @ -40 °C to 70 °C	
	2.5 °C @ 70 °C to 150 °C	
3K	0.2 °C @ -40 °C to 70 °C	
	2.5 °C @ 70 °C to 150 °C	
10K type 2	0.75 °C @ -40 °C to -20 °C	
	0.2 °C @ -20 °C to 120 °C	
	0.6 °C @ 120 °C to 150 °C	
10k type 3	0.5 °C @ -40 °C to -20 °C	
	0.3 °C @ -20 °C to 120 °C	
	0.6 °C @ 120 °C to 150 °C	
Custom	depends on curve	
Data Refresh Time	550 ms	
Note: To achieve the best thermistor accuracy when also using current outputs, always configure thermistors on the lowest channel numbers and current outputs on the highest channel numbers.		
0–400 kOhm Input (Requires firmware version 3.0.0 or later)		
Available Channels	0–7 (see Note)	
Input Range (Ohm)	0–400k	
Accuracy (Ohm @ Range)	greater of 3 Ohm or 0.5%@0-25k, 400@25k–50k, 900@50k–75k, 1.5k@75k–100k, 5k@100k–200K, 20k@200k–400k	
Gain Temperature Coefficient	500 ppm/°C	
Resolution (Ohm @ Range)	0.5@0–1k, 1@1k–5k, 2@5k–10k, 5@10k–25k, 50@25k–100k, 200@100k–200k, 700@200k–400k	
Power Dissipation @ Resistance (µW@Ohm)	375@1k, 950@5k, 1075@10k, 875@25k, 600@50k, 450@75k, 350@100k, 200@200k, 100@400k	
Data Refresh Time	550 ms	
Note: To achieve the best resistance accuracy when also using current outputs, always configure the 0-400 kOhm channel type on the lowest channel numbers and current outputs on the highest channel numbers.		

CONTINUED ON NEXT PAGE.

SPECIFICATIONS

Specification		GRV-R7-MM1001-10 GRV-R7-MM2001-10	
Discrete DC Input			
Available Channels	0–7		
Input Voltage Range	5–30 V DC		
Minimum ON Voltage	5.0 V		
Maximum OFF Voltage	1.5 V		
Input Impedance	> 425 KOhms		
Max. Input Frequency (50% square wave)	10000 Hz		
Switch Input, Powered			
Available Channels	0–7		
Open Circuit Voltage (Switch Open)	10.5 V (minimum)		
Channel Current Limit	1.1 mA max.		
Channel Operating Current	0.63 mA typical		
Minimum Off Resistance	10000 Ohms		
Maximum On Resistance	1200 Ohms		
Minimum ON Voltage	5 V		
Maximum OFF Voltage	1.5 V		
Maximum Continuous Survivable Input Voltage	32 V		
Input Impedance	> 425 KOhms		
Max. Freq. (50% square wave)	10000 Hz		
Discrete Counter Input			
Available Channels	0–1		
Input Voltage Range	5–30 V DC		
ON Threshold	5 V		
OFF Threshold	1.5 V		
Input Impedance	> 425 KOhms		
Max. Frequency (50% square wave): State, Latches, Counter	10000 Hz		
Max. Frequency (50% square wave): On/Off pulse width, Period, Frequency	2000 Hz		
Max. Frequency (50% square wave): On/Off totalization	750 Hz		
Pulse Width Measurement Resolution	100 microseconds		
Pulse Width Measurement Error (50% square wave)	0.1%	0 to	20 Hz
	1%	21 to	200 Hz
	5%	201 to	2000 Hz
Period/Frequency Error (50% square wave)	0.05%	0 to	20 Hz
	0.1%	21 to	200 Hz
	1%	201 to	2000 Hz

CONTINUED ON NEXT PAGE.

Specification	GRV-R7-MM1001-10 GRV-R7-MM2001-10
Discrete DC Sinking Output	
Available Channels	0–7 (4–7 if using any thermocouple inputs)
Line Voltage Range	5–30 V DC
Maximum Continuous Current	1.0 A
Peak Current (< 10 ms)	4.0 A
Recommended Fuse / Circuit Breaker	1 A at 30 V DC
Output Voltage Drop	175 mV at 1 A
Off-State Leakage (per channel)	< 80 μ A at 24 V, -20 to +70 °C
Peak Blocking Voltage	32 V
TPO Period (min, max, resolution)	0.004, 4294967, 0.001
Turn On / Off Time	20 ms nominal
Form C Relay Output	
Available Channels	8, 9
Line Voltage Range	0–250 V AC or 5–30 V DC
Clamp Voltage	440 V nominal
Current Rating	5 A per channel
Surge Current	6 A peak for 1 second
Recommended Fuse / Circuit Breaker	5 A at 250 V AC / > 30 V DC per channel
Initial Contact Resistance	< 100 milliohms
Turn On Time	8 ms
Turn Off Time	4 ms
Operating Life (to specification)	Min. 30,000 cycles at max. ratings
Mechanical Life	Min. 10,000,000 cycles
Voltage Output	
Available Channels	4–7
Range	0–10 V
Resolution	2.5 mV
Accuracy	$\pm 0.3\%$ of range (± 30 mV)
Gain Temperature Coefficient	50 ppm/°C
Offset Temperature Coefficient	20 ppm/°C
Output Slew Rate	> 15 V/ms
Minimum Load Resistance	7.5 kOhms
Output Impedance	< 10 Ohms
Short-circuit Current	20 mA
Data Refresh Time	Nominal 20 ms. Proportional to I/O scan time.

CONTINUED ON NEXT PAGE.

SPECIFICATIONS

Specification		GRV-R7-MM1001-10 GRV-R7-MM2001-10
Current Output		
Available Channels	4–7	
Output Range	0–20 mA	
Resolution	5 μ A	
Accuracy	$\pm 0.325\%$ of range ($\pm 65 \mu$ A)	
Gain Temperature Coefficient	60 ppm/ $^{\circ}$ C	
Output Slew Rate	> 10 mA/ms	
Maximum Loop Resistance	700 Ohms	
Data Refresh Time	Nominal 20 ms. Proportional to I/O scan time.	
Common Specifications		
Ethernet	Two 10/100/1000 Mbps ports; ETH1 supports 802.3af PoE (PD). <i>Configurable Modes:</i> Switched Mode (default): Supports daisy-chaining via internal 2-port switch. Independent Mode: Ports operate as separate logical interfaces for dual-network isolation.	
USB	One Port, USB 2.0 HS	
Memory	GRV-R7-MM1001-10: 1 GB RAM, 4.0 GB disk space GRV-R7-MM2001-10: 2 GB RAM, 7.0 GB disk space	
Power Supply	10–32 V DC or 802.3af PoE Class 0 (ETH1)	
Power Consumption	10 W	
Max. Survivable Input (channels 0 - 7)	32 V DC	
Isolation (between channels 0 - 7)	None	
Isolation (between channel 8 or 9 and all others)	3000 V AC _{rms} 1 min.	
Isolation (field to Ethernet / power input)	1500 V AC _{rms} 1 min.	
Minimum <i>groov</i> RIO Firmware Version	GRV-R7-MM1001-10: N/A GRV-R7-MM2001-10: 3.0.0	
Minimum <i>groov</i> EPIC Firmware Version	GRV-R7-MM1001-10: 2.0.0 (3.0.0 for Thermistors) GRV-R7-MM2001-10: 3.0.0	
Minimum PAC Project Version	GRV-R7-MM1001-10: 10.3000 (10.3003 for Thermistors) GRV-R7-MM2001-10: 10.3003	
Minimum Library Package for CODESYS Version	GRV-R7-MM1001-10: 2.0.0.0 (2.0.1.0 for Thermistors) GRV-R7-MM2001-10: 2.0.1.0	
Field Connector Wire Size	28–14 AWG	
Torque, field connector screw	2.5 in-lb (0.28 N-m)	
Power Connector Wire Size	22–14 AWG	
Torque, DC power connector screws	7.0 in-lb (0.79 N-m)	
Torque, panel mount tab screw	2.0 in-lb (0.23 N-m)	
Temperature (operating)	-20 $^{\circ}$ C to +70 $^{\circ}$ C	
Temperature (storage)	-40 $^{\circ}$ C to +85 $^{\circ}$ C	
Relative Humidity (non-condensing)	5–95%	
MTBF (minimum, 25 $^{\circ}$ C)	1.2 Mhrs	

Specification		GRV-R7-MM1001-10 GRV-R7-MM2001-10
Agency Approvals	UL/cUL(Class 1 Div. 2); CE, ATEX(Category 3, Zone 2), RoHS; DFARS; CB Scheme; UKCA	
Warranty	30 months	

Wiring Assignments

These assignments apply to the thermocouple input signal type.

Type	-	+	Range
B	Red	Gray	+90 °C to +1,820 °C
E	Red	Purple	-80 °C to +1,000 °C
J	Red	White	-100 °C to +1,200 °C
K	Red	Yellow	-80 °C to +1,372 °C
N	Red	Orange	-100 °C to +1,300 °C
R,S	Red	Black	100 °C to +1,768 °C
T	Red	Blue	-60 °C to +400 °C

B: Wiring Diagrams

WIRING FIELD DEVICES

Diagrams are readily available to help you wire field devices to *groov* RIO.

- Basic wiring diagrams are shown on the following page for all channels. Note instructions on fusing and power.
- You can also find wiring diagrams for each channel type in *groov* Manage. At the *groov* Manage homepage, choose I/O Reference > *groov* RIO Mixed Signal, Multifunction > [RIO part number] and select the signal type to see how to wire it.

groov RIO Explorer

The [groov RIO Explorer](#) is an online, interactive tool that can help you select and track which combinations of functions (input or output) and signal types (analog, discrete, voltage, current, ICTD, thermocouple, etc.) you can assign to specific channels.

For instructions on how to use it, see [Appendix C: groov RIO Explorer](#) on [page 179](#).

GRV-R7-MM1001-10, GRV-R7-MM20001-10

Review the notes along the bottom of the wiring diagram for additional instructions on fusing, power, and selecting supported combinations of signals for some channels.

			INPUT							OUTPUT						
Channel	Internal Wiring	Pin	Discrete		Voltage	Current ²	Analog			Discrete ^{1,3}	DC Sinking ^{1,3}	Analog	Current / Voltage	Mechanical Relay		
			Discrete	Switch Input, Powered			ICTD	Thermistor/Resistor	Thermocouple/Millivolt ³					Form C-NO ¹	Form C-NC	
Ch 0		1														
		2														
		3														
Ch 1		4														
		5														
		6														
Ch 2		7														
		8														
		9														
Ch 3		10														
		11														
		12														
Ch 4		13														
Ch 5		14														
		15														
Ch 6		16														
		17														
Ch 7		18														
		19														
Ch 8		20													— NC	
		21													— COM	— COM
		22													— NO	
Ch 9		23													— NC	
		24													— COM	— COM
		25													— NO	
		26													— NO	

Notes:

1. You must supply external fusing.
2. Opto 22 recommends adding external fusing. Review the specification table for specific ratings. Compatible with an externally powered or self powered transmitter. Wiring for externally powered transmitter is shown on channels 0 and 1. Wiring for a self powered transmitter is shown on channels 2 and 3.
3. Thermocouple inputs and discrete sinking outputs cannot be mixed on channels 0-3.

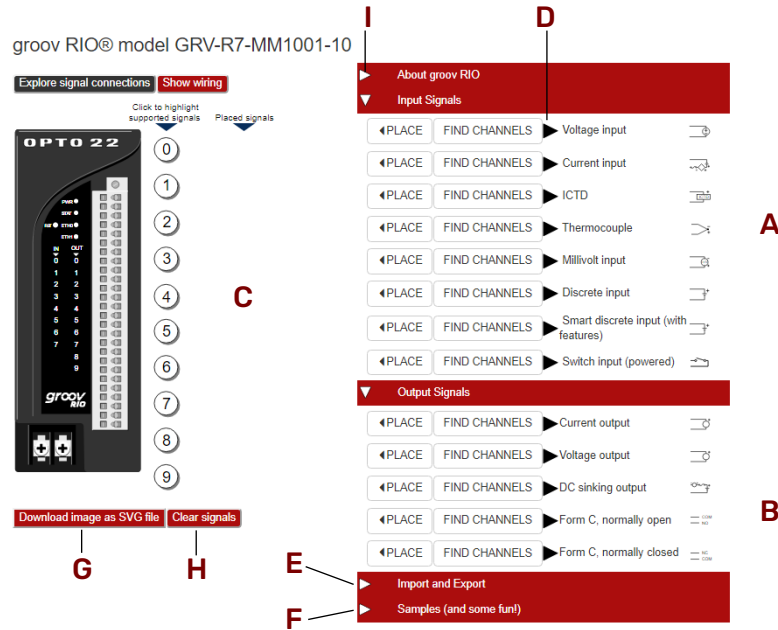
C: *groov* RIO Explorer

The [groov RIO Explorer](#) is an online app that helps you see different combinations and arrangements of channel configurations and their associated wiring diagrams. With the app, you can:

- Identify which channels support a specific combination of function (input or output) and signal type (analog, discrete, voltage, current, ICTD, thermocouple, etc.).
- Move any signal that you placed on one channel to another supported channel.
- Avoid assigning a combination of function and signal type to a channel that does not support that particular combination.
- See a wiring diagram of the combination you built, plus different ways to arrange that combination.
- Export or import a combination into text description.
- See samples of wiring configurations from over 61,000 possible combinations.

THE *groov* RIO EXPLORER

Open the online app by opening a browser and going to www.opto22.com/products/groov-RIO-Explorer. Here's an overview of what you can see and do in the window:



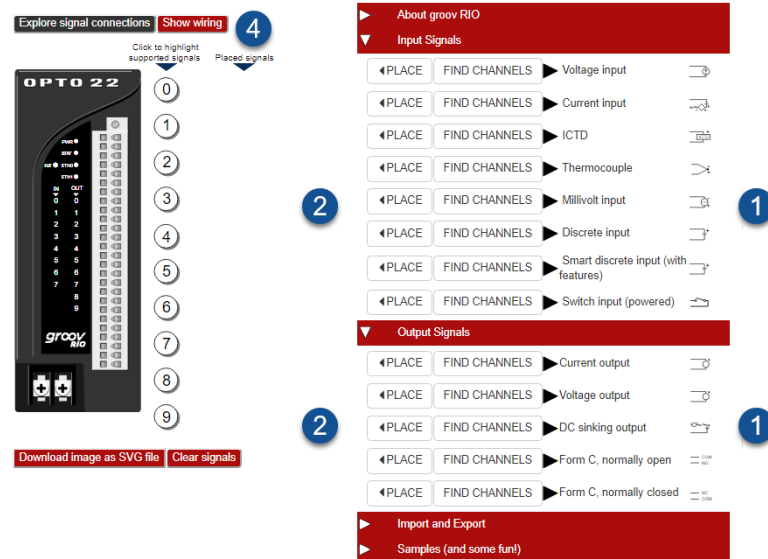
- A** Signal types available for inputs.
- B** Signal types available for outputs.
- C** When you place a signal, it's shown in this column, next to the channel you selected or the first channel number that supports that signal.
- D** To view specifications for the signal type, click the triangle next to it.
- E** To access import and export functions, click the triangle to open this section.
- F** To see sample configurations and different arrangements for your own or sample configurations, click the triangle.
- G** To download your wiring diagram as a Scalable Vector Graphic, click Download image as SVG file.
- H** To remove all the signals you placed on the RIO Explorer and start over, click Clear signals.
- I** To see specifications for this *groov* RIO unit, click the triangle.

Now let's see how to assign channels to match the configuration you want.

Assigning Functions and Signals to a Channel

Follow the steps below to assign a function (input or output) and signal type to a channel.

groov RIO® model GRV-R7-MM1001-10



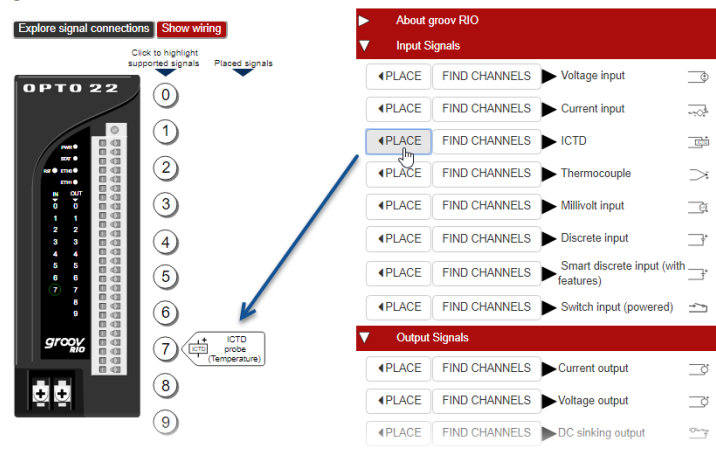
1. Look through the options on the right. Look in either the input or the output list and choose the signal type you need.

For example, if you need an ICTD input, look in the Input Signals list and find ICTD. If you need a voltage output, look in the Output Signals list and find Voltage Output.

2. Click Place next to the function and signal type you need.

The Explorer places that function and signal on a channel that supports that combination. For example, your ICTD input might appear like this:

groov RIO® model GRV-R7-MM1001-10



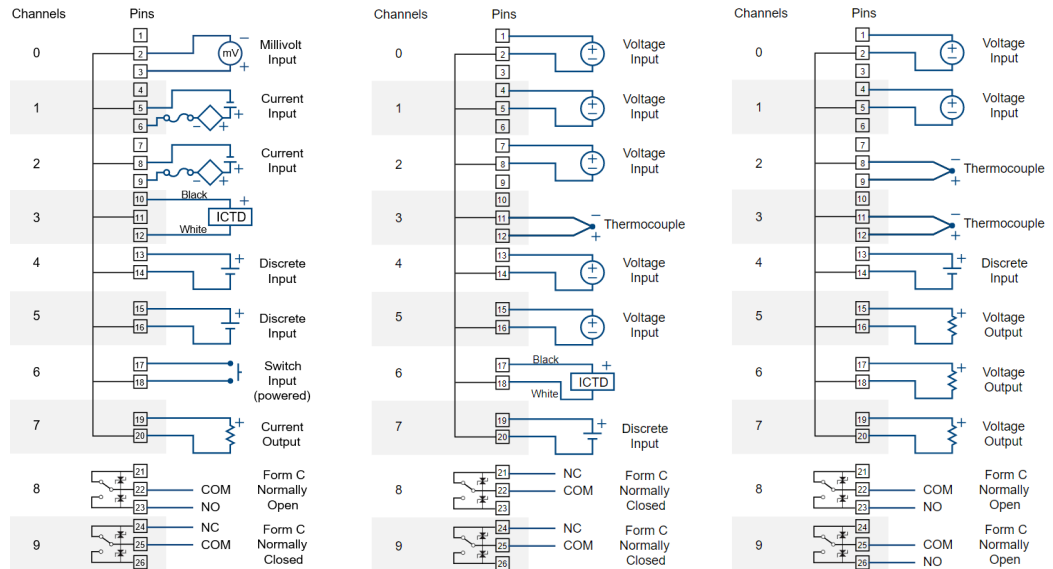
If you don't like where the Explorer placed your signal, see ["Moving and Deleting Signals"](#) on page 182.

- Repeat the previous steps for each additional channel you want to configure.

The Explorer will not let you place functions and signals into channels that don't support them.

- Click Show wiring to see a diagram that illustrates wiring for all your selections.

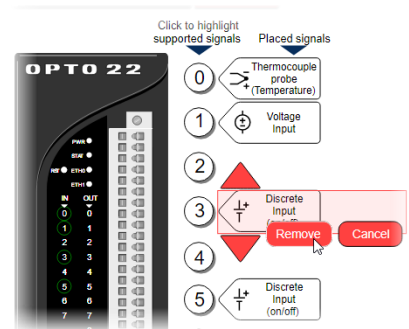
Below are three examples of images of wiring diagrams created by the *groov* RIO Explorer for function and signal type assignments made to channels on a GRV-R7-MM1001-10.



- If you want to save your wiring diagram as a re-sizable image file, click Download image as SVG file. To leave the wiring diagram, click Explore signal connections.

Moving and Deleting Signals

- To move a signal, click on the placed signal. Click the up or down arrow to move the signal to another available channel that supports that signal. (The Explorer can "hop" over assigned channels, if necessary.)
- To delete the signal, click a placed signal and then click Remove.

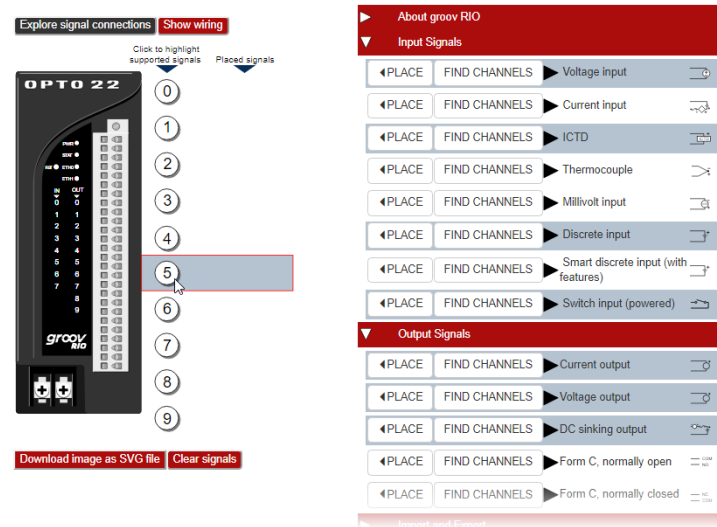


Viewing Possible Signals and Channels

To see which functions and signals you can place on a channel, click the channel number. The RIO Explorer highlights all the functions and signal types that you can assign to that channel.

In the example that follows, when you click the number for channel 5, the RIO Explorer highlights Voltage input, ICTD, Discrete input, and Switch input (powered) under the Input Signals section; Current output, Voltage output, and DC sinking output under the Output Signals section. You can assign any of those to channel 5.

groov RIO® model GRV-R7-MM1001-10



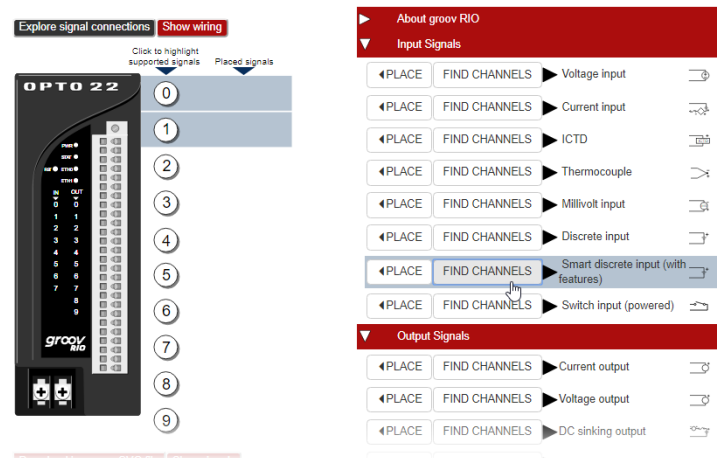
The screenshot shows the groov RIO Explorer interface. On the left, a vertical list of channels (0-9) is shown. Channel 5 is highlighted in blue. Above the list, a button labeled 'Click to highlight supported signals' is visible. To the right of the channel list, a red box highlights the 'Placed signals' section. Below the channel list, there are two buttons: 'Download image as SVG file' and 'Clear signals'.

On the right side of the interface, there are two main sections: 'Input Signals' and 'Output Signals'. The 'Input Signals' section lists various signal types with 'PLACE' and 'FIND CHANNELS' buttons. The 'Output Signals' section lists various output types with 'PLACE' and 'FIND CHANNELS' buttons.

To see which channels can be configured with a specific function and signal, find the function and signal in the lists at right. Click the FIND CHANNELS button, and the Explorer highlights the channels that support that combination.

For example, if you want to see which channels will accept a smart discrete input with features like counting, latching, and totalization, click its Find Channels button. Channels 0 and 1 are highlighted, so you can place that signal on either (or both) of those channels.

groov RIO® model GRV-R7-MM1001-10



The screenshot shows the groov RIO Explorer interface. On the left, a vertical list of channels (0-9) is shown. Channels 0 and 1 are highlighted in blue. Above the list, a button labeled 'Click to highlight supported signals' is visible. To the right of the channel list, a red box highlights the 'Placed signals' section. Below the channel list, there are two buttons: 'Download image as SVG file' and 'Clear signals'.

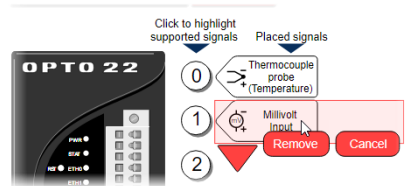
On the right side of the interface, there are two main sections: 'Input Signals' and 'Output Signals'. The 'Input Signals' section lists various signal types with 'PLACE' and 'FIND CHANNELS' buttons. The 'Output Signals' section lists various output types with 'PLACE' and 'FIND CHANNELS' buttons.

Replacing a Signal

1. Click the placed signal.
2. On the right side of the Explorer, find your new function and signal type.

EXPORTING AND IMPORTING COMBINATIONS OF FUNCTIONS AND SIGNALS

3. Click Place next to the new signal.



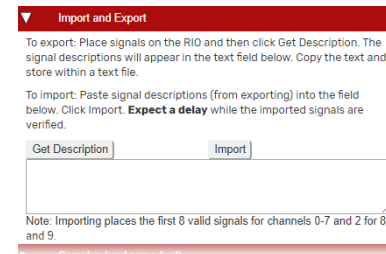
4. Click Replace.

EXPORTING AND IMPORTING COMBINATIONS OF FUNCTIONS AND SIGNALS

Once you have your *groov* RIO configured in the Explorer, you may want to save the signal combination by exporting it to a text file. Exported configurations can be imported later to view or work on.

Exporting

1. To export a combination, click Import and Export to expand that section.
2. Click Get Description.
The Explorer places abbreviations for the functions and signal types in the text box. (See below for the abbreviations used.)
3. Copy the text, paste it into a text file, and save it.



The following abbreviations identify functions and signal types:

Inputs	Outputs
ai_voltage	ao_current
ai_mv	ao_voltage
ai_current	do_sinking
ai_ictd	do_formc_no
ai_thermocouple	do_formc_nc
di_discrete	
di_smart_discrete	
di_switch_powered	

- **ai**—analog input
- **ao**—analog output
- **di**—discrete input
- **do**—discrete output

Importing

1. To import a combination, click Import and Export to expand the section.
2. Paste all the text from the text file you saved into the box. Click Import Configuration.

The RIO Explorer assigns the functions and signals to the channels, verifying that they are correct. There may be a delay while verifying.

Note that the channels may not end up in the same order you originally configured.

You can also type function/signal abbreviations into the field, and the Explorer will place them. It uses the first eight valid signals for channels 0-7 and the first two for channels 8 and 9. (Any text not in the correct abbreviation format is ignored.) So for example, to import channel assignments like the first wiring diagram on [page 182](#), you could type the following into the text box:

```
ai_mv, ai_current, ai_current, ai_ictd, di_discrete, di_discrete,
di_switch_powered, ao_current, do_formc_no, do_formc_nc
```

WORKING WITH SAMPLES

The *groov* RIO Explorer comes loaded with 61,260 wiring combinations! To access those samples, click Samples (and some fun!) to expand that section.

▼ Samples (and some fun!)

Here is a sample configuration using a practical mix of signals:

[Load Sample Configuration](#)

To see any of the 61260 wiring possibilities, select or enter a value from 0 to 61259:

[load combination](#)

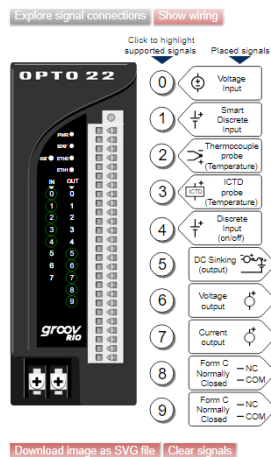
Most combination of signals on a groov RIO can be rearranged using the same signals but changing the channel placement.

To have the alternative arrangements calculated, choose this button.

(Expect a delay while arrangements are calculated.)

[Calculate arrangements for this combination](#) Arrangements: ▼

One sample in particular can give you a good idea of the versatility of GRV-R7-MM1001-10. To see it, click Load Sample Configuration. The Explorer replaces any signals in the Placed signals area with the signals that are in the sample configuration.



Samples are numbered 0 to 61259. Type in any number in that range in the text box, then click Load Combination to view that sample configuration. Have some fun with the numbers: enter a special date, the final score of your favorite football game, or the altitude of your favorite mountain.

How many ways are there to wire the same combination of functions and signals? For many samples or even for a configuration that you created, the arrangement of functions and signals on the channels can be changed. Seeing another way to wire the same signals can be useful if you have space constraints. The *groov* RIO Explorer can calculate the number of ways a particular combination can be rearranged. To learn that number and view the arrangements, click Calculate Arrangements for this Combination.

The RIO Explorer displays the result along with a drop-down list. Click the drop-down list and select any number, and the Explorer shows that arrangement. You can scroll through the numbers by pressing the up and down arrows on the keyboard. You'll see the Explorer update the image with each new arrangement.