Form 2372

groov RIO ENERGY MONITORING UNIT USER'S GUIDE

groov RIO
ENERGY MONITORING UNIT
USER'S GUIDE

for
GRV-R7-I1VAPM-3

Form 2372-240318—March 2024

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 EMU User's Guide
Form 2372-240318—March 2024

Copyright © 2024 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

1: Welcome

WELCOME TO *groov* RIO ENERGY MONITORING!

groov RIO EMUs (EMUs) can monitor the electrical energy used in your facility and then deliver that data to online software applications, control systems, and business systems—using your existing wired or wireless Ethernet network. *groov* RIO EMUs give you the detailed, real-time data you need to analyze energy consumption and reduce energy costs.

Why Monitor Energy?

Typically, managers approve major expenditures only when they know exactly where the money is going. By managing energy in the same way as other business costs—such as people, assets, and inventory—commercial and industrial businesses increasingly find that they can significantly reduce energy costs. Energy management represents a real opportunity to improve the bottom line.

Saving money on energy does not require complex or expensive technology; it requires basic information. That information starts with gathering detailed, real-time data through a *groov* RIO EMU.

Viewing and Using Energy Data

You can view real-time energy data gathered by the *groov* RIO EMUs through:

- Node-RED Dashboards. Add the Node-RED Dashboard nodes to your palette and after configuring a *groov* RIO EMU, wire up your energy channels to Dashboard nodes to create a simple HMI.
- Opto 22's *groov* View to build and view operator interfaces to energy data from a *groov* RIO EMU. Entirely browser-based, *groov* View requires no additional software and no plugins.

You can also incorporate data from a *groov* RIO EMU in control systems based on Opto 22's PAC Project™ software, CODESYS applications, or custom programs.

MORE ABOUT *groov* RIO ENERGY MONITORING UNITS

Opto 22's *groov* RIO EMU is an independent, intelligent Ethernet-based module designed to work at the edge of industrial internet of things (IIoT) applications. Transferring data between electrical circuits, control systems, company software, and cloud services no longer has to be complex and costly, requiring PLCs, programming, and middleware. Instead, ***groov* RIO EMU 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 EMU, 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 electrical circuits and on-premises or cloud-based systems and software.

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

- Place the module almost anywhere. *groov* RIO EMU 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 provide 10–32 VDC power.
- Simplify field connections using the removable terminal connector with spring clamp wire retention. Supports wire sizes 22 to 14 AWG.
- Use web-based software to configure the module and channels: supporting wye or delta configurations, three-phase power monitoring, up to 64 channels of measured and calculated energy data.
- 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 and network activity on the module's LEDs.
- Use embedded software to quickly set up data communications.

groov RIO EMU at the Edge

groov RIO EMU is designed to work at the edge of IIoT applications. Edge devices can bridge the operations technology (OT) world of electrical circuits and the information technology (IT) world of computers and corporate software.

groov RIO EMU'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 EMU channels, security, and communications

Node-RED—Software for creating simple data flows to send data to cloud services, databases, and APIs. Pre-built nodes make flow creation easy.

MQTT—Built-in support for MQTT—an efficient publish/subscribe protocol for exchanging data—through the Data Services MQTT client. Only a simple configuration is needed to publish energy data and subscribe to commands as Sparkplug-B or string payloads.

Modbus® TCP/IP—Support for the well-known industrial protocol. *groov* RIO EMU acts as a Modbus TCP/IP slave right out of the box.

groov RIO EMU as Remote Unit in an Opto 22 Control System

In addition to its use as independent edge EMU for IIoT applications, *groov* RIO EMU can also be used as a remote unit with an Opto 22 *groov* EPIC® processor.

groov RIO EMU is wired to electrical circuits and acts as an I/O unit within the *groov* EPIC's control and I/O network. As an I/O unit, *groov* RIO EMU is compatible with any of the *groov* 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.

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

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

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

C++ or .NET and free SDKs—With your favorite development tool and our free SDKs, you can programmatically access energy data on a *groov* RIO EMU 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 energy data on a *groov* RIO EMU. A Swagger API document is built into *groov* RIO EMU to quickly access REST API calls and evaluate responses.

REQUIREMENTS

Power Requirements

You can supply power to a *groov* RIO EMU 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

Load Wiring

Connect electrical circuits to a *groov* RIO EMU as directed in "Wiring Electrical Circuits" on page 9.

Software Requirements

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

If you are using a *groov* RIO EMU as remote I/O in a system controlled by:

- a PAC Control strategy, you need PAC Project 10.4000 or higher and a *groov* EPIC processor running firmware version 3.3.0 or higher.
- a CODESYS application, you need CODESYS Development System, V3.5 SP17 Patch 1 or newer (32-bit version) with Opto 22 Library Package for CODESYS Development System version 2.0.4.0 installed.

ABOUT THIS GUIDE

This user's guide shows you how to mount your *groov* RIO EMU, how to connect your loads, how to configure the channels, and much more.

What's In This Guide?

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

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

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

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 *groov* RIO EMU to control what services can connect to it.

Chapter 6: Enable Data Services: MQTT and OPC UA introduces you to Data Services and how it helps you configure and manage the Data Services OPC UA server and Data Services MQTT client.

Chapter 7: Configuring groov RIO EMU Module and Channels summarizes the different methods to configure the module and channels and how to select one, then goes into detail on how to configure the module and channels through *groov* Manage: specifying the CT connected to the electrical load, the PT (if used), naming channels, specifying threshold and scaling values, and understanding quality codes.

Chapter 8: Maintaining a groov RIO EMU describes all the tasks you can do to keep your *groov* RIO EMU 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 describes which channel reads input values, which channels calculate different energy and power values, and which channels report summation values for all phases.

Appendix B: Wiring Diagrams lists the wiring diagrams for the GRV-R7-I1VAPM-3.

Appendix C: Understanding Certificates provides background information on how SSL/TSL certificates created authenticated and encrypted connections.

SERVICE AND MAINTENANCE

To keep your *groov* RIO EMU 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 EMU" on page 80.

If you encounter any issues with your *groov* RIO EMU, follow the instructions in "Collecting Information for Product Support" on page 87 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 Energy Monitoring Unit

GATHERING YOUR EQUIPMENT AND INFORMATION

Gathering up all the supplies, information, and equipment you need before you mount and wire your *groov* RIO EMU 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 3.
- The proper CTs to connect the module to your electrical circuit as described in "Wiring Electrical Circuits" on page 9.
- 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 EMU, which helps you connect wires to the correct pins on the terminal connector.

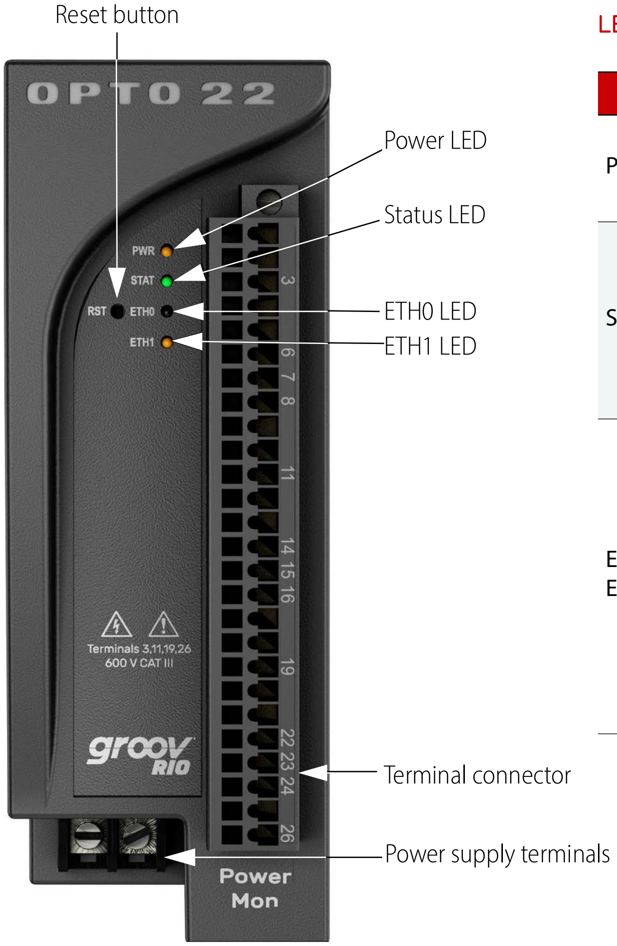
In addition, make sure you have important information about your electrical circuit, like the maximum current to be measured.

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

FAMILIARIZING YOURSELF WITH THE *groov* RIO EMU

Take a look at the *groov* RIO EMU 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.

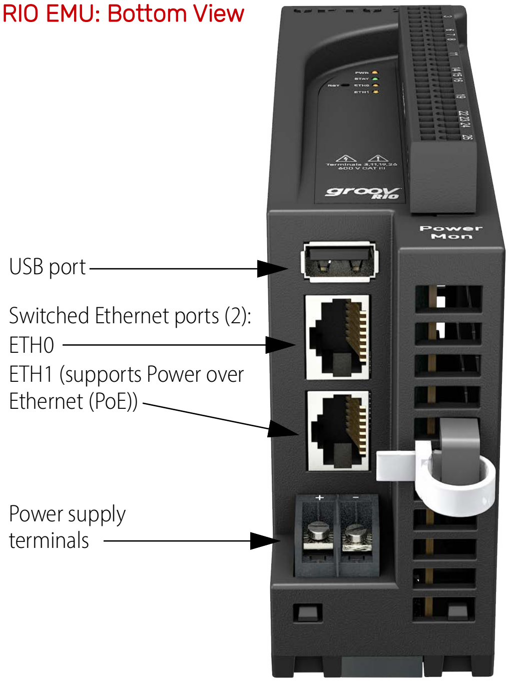
groov RIO EMU: Front View



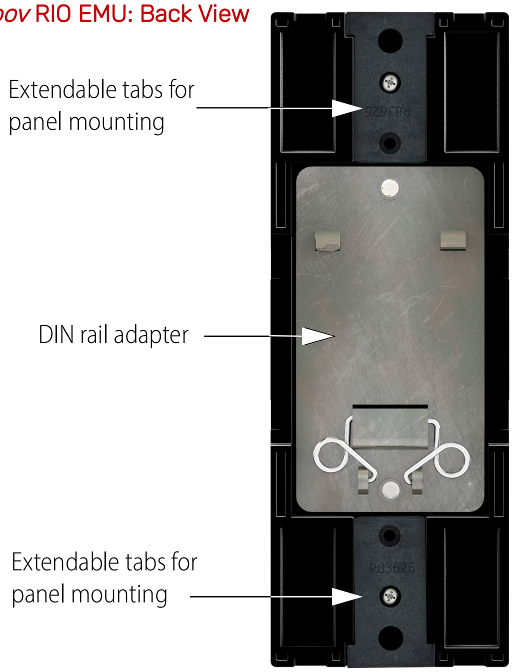
LEDs

<table>
<tr><th>LED</th><th colspan="3">Indicates</th></tr>
<tr><td>PWR</td><td colspan="3">The status of power.
• Solid green—<i>groov</i> RIO is powered on.
• Solid red—<i>groov</i> RIO is restarting.</td></tr>
<tr><td>STAT</td><td colspan="3">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.</td></tr>
<tr><td rowspan="6">ETH0,
ETH1</td><td colspan="3">Network connection speed and whether there is any transmission activity:</td></tr>
<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>

groov RIO EMU: Bottom View


USB port
Switched Ethernet ports (2):
ETH0
ETH1 (supports Power over Ethernet (PoE))
Power supply terminals
Power
Mon
groov RIO

groov RIO EMU: Back View


Extendable tabs for panel mounting
DIN rail adapter
Extendable tabs for panel mounting

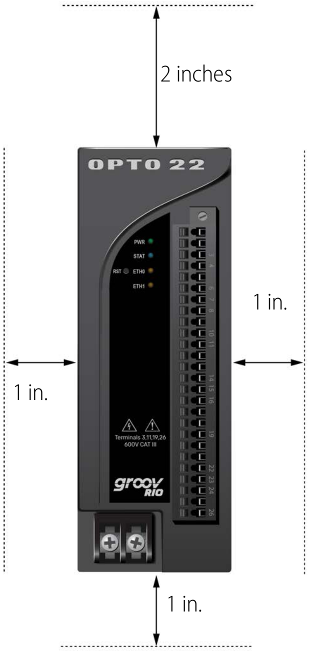
MOUNTING

You can mount a *groov* RIO EMU on DIN rail or a panel.

Choosing a Location

Initial set up (as described in Chapter 3: Initializing a groov RIO EMU) of a *groov* RIO EMU 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 75). Final placement of the *groov* RIO EMU 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 "GRV-R7-I1VAPM-3" on page 94).
- 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 EMU performs as described in the specifications.

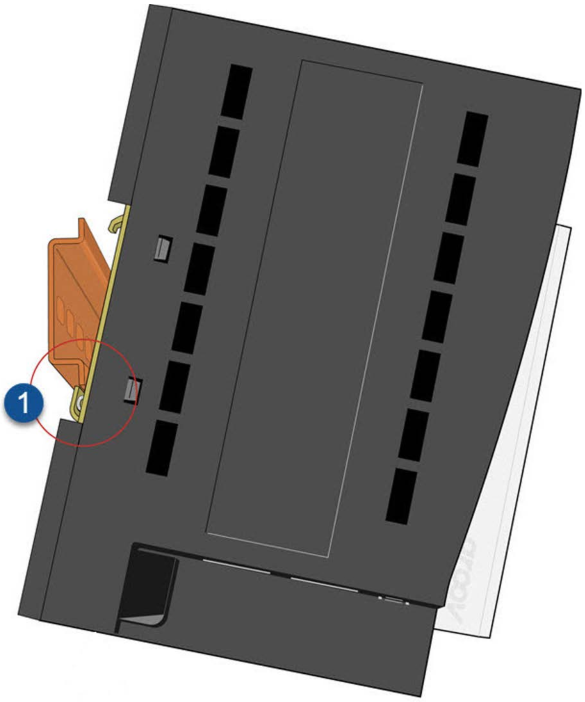
Mounting on DIN Rail

Before mounting your *groov* RIO EMU:

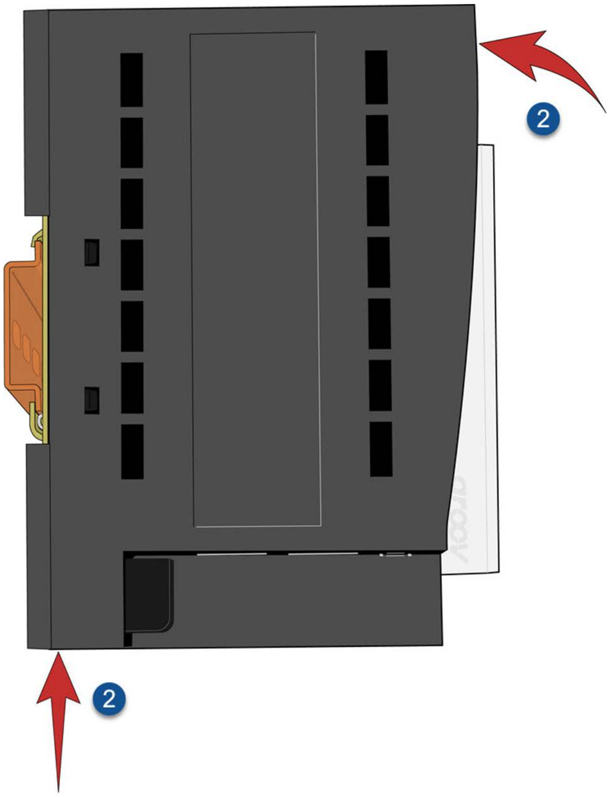
- Ensure that the vents around the module are not obstructed.
- Ensure that the mounting location meets the clearances described above.

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

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.



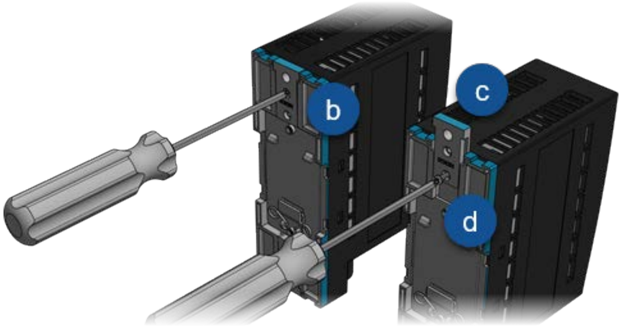
Before you release the module, verify that the top and bottom of the DIN rail adapters have engaged the DIN rail.

Mounting on a Panel

Before mounting your *groov* RIO EMU on a panel:

- Ensure that the vents around the module are not obstructed.
- Review the clearance requirements described in "Choosing a Location" on page 7.

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 page 94.
   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 page 94.
   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 ELECTRICAL CIRCUITS

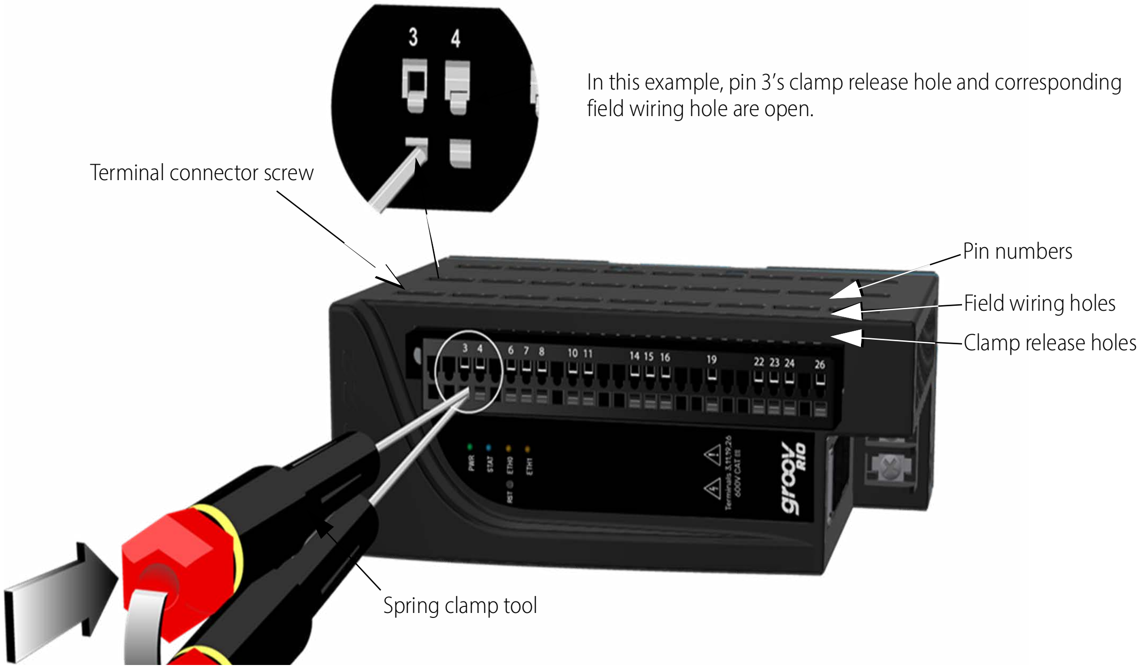
WARNING: DANGER. *Hazardous voltage. Direct wiring involves high voltages and must be done by a* ***qualified electrician****.*

Before you begin wiring, do the following tasks:

- Ensure that you have the spring clamp tool supplied with your *groov* RIO EMU.
- If you are unfamiliar with the names of some of the parts of the *groov* RIO EMU, review the diagrams on page 6.

- It may be easier to insert wires if you remove the terminal connector from the *groov* RIO EMU. To remove the terminal connector, loosen the terminal connector screw at one end of the connector, then pull the connector straight out to remove it.
- If you have never used a spring-clamp wiring system, take a moment to familiarize yourself with the diagram below. The clamp release hole is where you will insert the sprint clamp tool. The field wiring hole is where you will insert your field wires.

  If you look into the field wiring hole, you will see a highly reflective surface. If you can see that surface, that means that the clamp is closed.



In this example, pin 3's clamp release hole and corresponding field wiring hole are open.

You can monitor one 3-phase electrical panel or piece of equipment, or you can monitor three single-phase panels or pieces of equipment. Only a qualified electrician should do the wiring described in the following steps:

1. Install CTs and wire electrical loads.
   - Determine the maximum current to be measured, then choose a CT with:
     - an appropriate secondary and,
     - a primary current rating that can handle both your selected wire size and maximum current.

     For an introduction to selecting CTs, review the Selecting and sizing a current transformer blog on our website (opto22.com).

     UL requires CTs to be CAT III approved. Category III is for measurements performed in a building; for example circuit breakers, wiring, distribution panels, and equipment for industrial use. For more information, review the IEC 61010 standard.

     UL also requires that CTs be **UL Listed Current Transformers for Energy Monitoring**.
   - Verify that the proper safety fuse is connected to each voltage line of each phase, as close to the source as possible. The fuses should be 1 A or less.
   - When the CT is installed, verify that:
     - It is oriented correctly, according to the labeling on the CT.
     - All the CTs are installed in the same direction.
     - Each CT matches its respective voltage tap.

- If loads have a neutral, make sure it's connected.

2. Review the wiring diagram (see"GRV-R7-I1VAPM-3" on page 102) to identify which wires from the CT connect to the correct the pins on the module.
3. Orient the module or terminal connector to match the wiring diagrams in "GRV-R7-I1VAPM-3" on page 102.
4. To make it easier to handle the spring-clamp terminal tool and the field wires, secure the module by doing one of the following:
   - 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.
5. Insert the spring-clamp terminal tool into the clamp release hole, then press and hold down the tool to open the clamp. Look into the field wiring hole. If it is dark, the clamp is open. You can go to step 6. If you can still see the highly reflective surface, gently push down again and maintain downward pressure on the spring-clamp terminal tool. Look into the field wiring hole. If it is dark, the clamp is open.

   Note: If you push down too hard, the spring-clamp terminal tool might pop out of the clamp release hole.

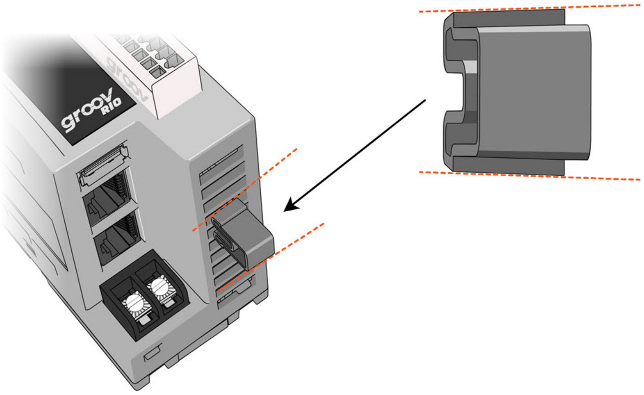
6. Insert the wire into the field wiring hole until it meets complete resistance. Then pull out the spring-clamp terminal tool.
7. Test that the wire is secure by gently pulling on it. If the wire pulls out, repeat steps 5 and 6.

To remove a wire, push the spring-clamp terminal tool into the clamp release hole as described in step 5 above, and then pull the wire out.

Bundling Wires with a Cable Tie Mount

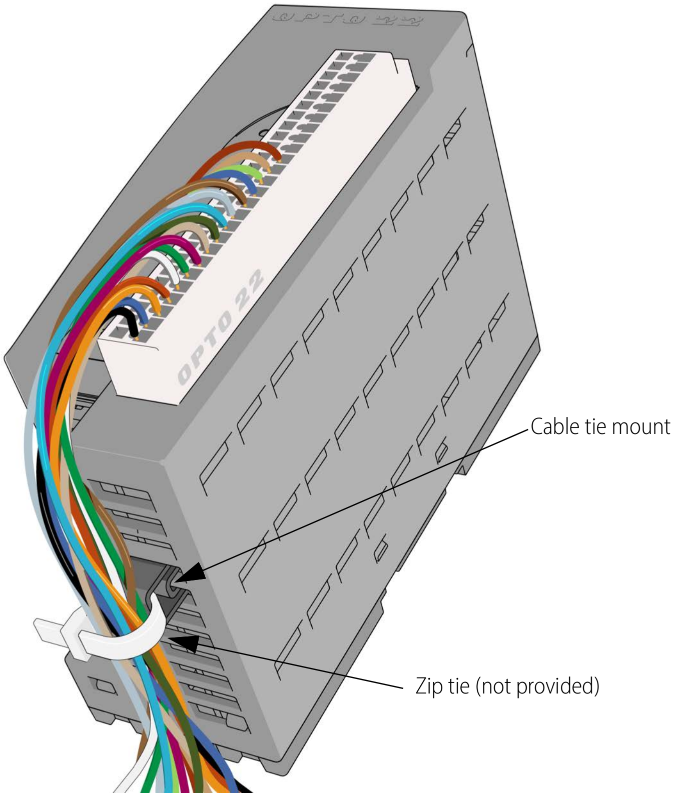
Each *groov* RIO EMU comes with two user-installable cable tie mounts. You only need to attach one mount.

1. Identify the thin side of the mount, then position it over a vent so that the thin side faces the Ethernet network interfaces and is to the right of the PCB, which is visible through the vents (see image on page 6).
2. With one hand, hold the *groov* RIO EMU 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, pull the mount with pliers; 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.

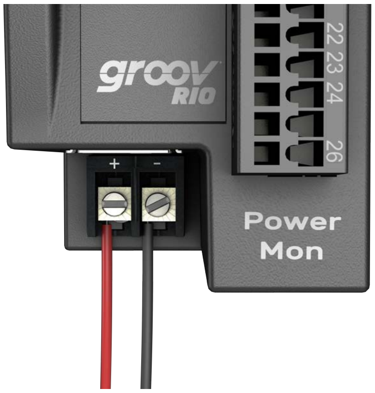
CONNECTING POWER SUPPLY

As mentioned in "Power Requirements" on page 3, you can power a *groov* RIO EMU with either one of the following methods, but not both methods 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) using an Ethernet cable connected to the ETH1 network interface.

External Power Source or Supply

Connect *groov* RIO EMU 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 EMU. 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 EMU and other powered devices (PDs), make sure it has sufficient power available for *groov* RIO EMU 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 EMU.*

SELECTING AN ETHERNET NETWORK INTERFACE TO CONNECT TO A NETWORK

You must begin with a wired Ethernet 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.

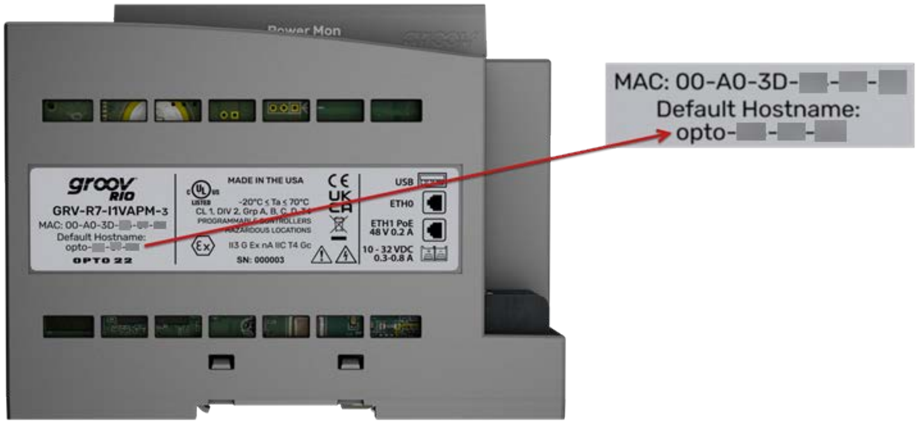
3: Initializing a *groov* RIO EMU

After you connect your *groov* RIO EMU 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.

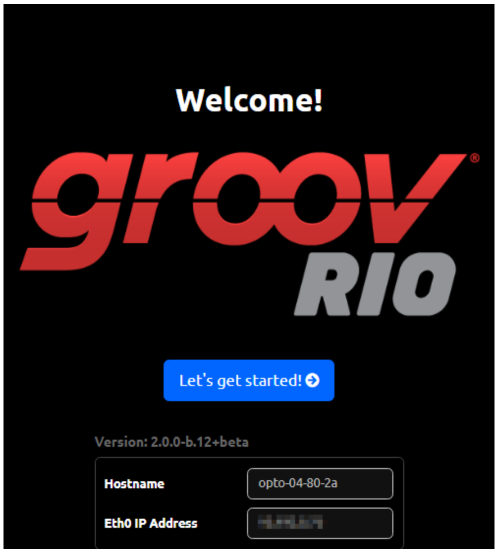
- If your network uses DNS and DHCP to assign and manage IP addresses, go to step 1 (below).
- If your network does not use DNS and DHCP to assign and manage IP addresses, you will need to install and run (on a Windows machine) *groov* Find. *groov* Find is an optional utility program you can use on 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 85.) Make note of the IP address that *groov* Find identifies for your *groov* RIO EMU 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.



Welcome!

Version: 2.0.0-b.12+beta

Hostname opto-04-80-2a

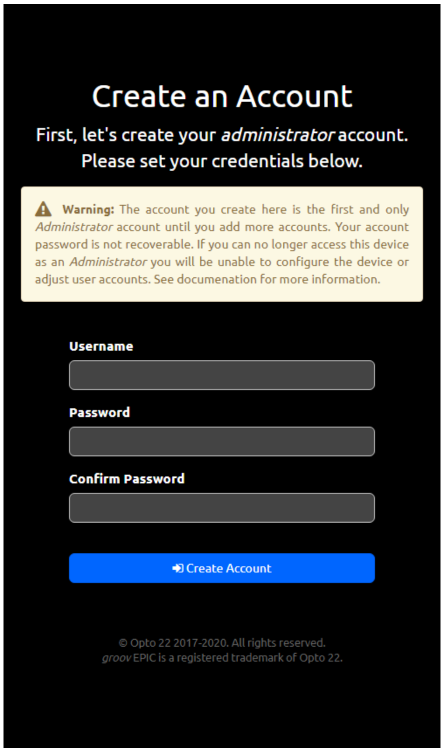
Eth0 IP Address [redacted]

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 EMU is Unreachable" on page 84.

4. Click Let's get started! (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.



Create an Account

First, let's create your *administrator* account. Please set your credentials below.

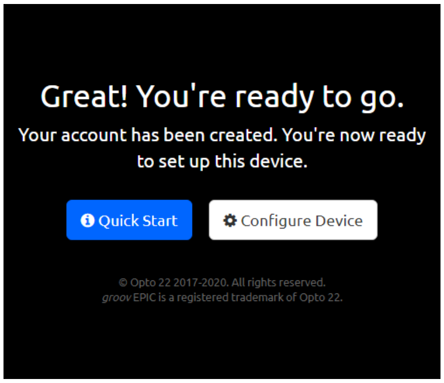
Warning: The account you create here is the first and only *Administrator* account until you add more accounts. Your account password is not recoverable. If you can no longer access this device as an *Administrator* you will be unable to configure the device or adjust user accounts. See documenation for more information.

© 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:



Great! You're ready to go.

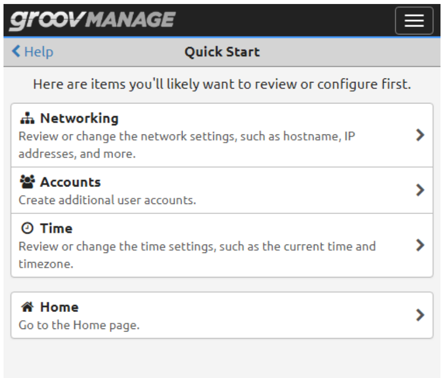
Your account has been created. You're now ready to set up this device.

© Opto 22 2017-2020. All rights reserved.
groov EPIC is a registered trademark of Opto 22.

   – **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.



Here are items you'll likely want to review or configure first.

Networking
Review or change the network settings, such as hostname, IP addresses, and more.

Accounts
Create additional user accounts.

Time
Review or change the time settings, such as the current time and timezone.

Home
Go to the Home 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 EMU'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.

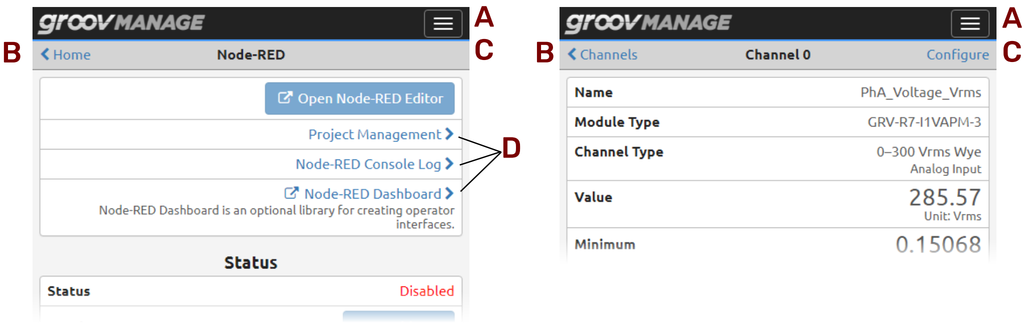
8. In *groov* Manage, click the menu button (☰), then select Info and Help.
9. In the Info and Help page, click About.
10. In the *groov* RIO section, note the version in the System Version field.
11. Log on to opto22.com and enter the part number for your *groov* RIO in the Search box. Select the search result that includes "Firmware" as part of the title; for example GRV-R7-I1VAPM-3 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 configure your module and channels for the electrical load it will be measuring.
    - 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 EMU. Follow the instructions in "Updating Firmware on a groov RIO EMU" on page 80. After you update the firmware, you can continue on to configure your module and channels for the electrical load it will be measuring.

4: Navigating *groov* Manage

When you connect to your *groov* RIO EMU through a web browser, you see *groov* Manage—the "central command" interface to your *groov* RIO EMU 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:



Node-RED Dashboard is an optional library for creating operator interfaces.

Status

Status	Disabled

Name	PhA_Voltage_Vrms
Module Type	GRV-R7-I1VAPM-3
Channel Type	0–300 Vrms Wye Analog Input
Value	285.57 Unit: Vrms
Minimum	0.15068

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.

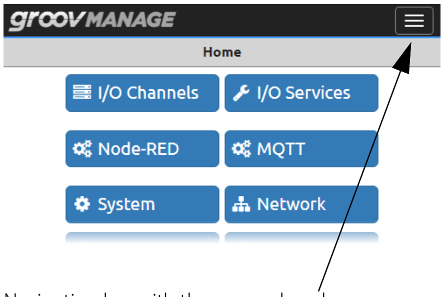
If this area shows the word Save, you must click on it to save any changes you made to settings on the page. If, after saving, the processor must restart an application or service, it displays a message to let you know.

If this area is blank, that means you can't make any changes to this page.

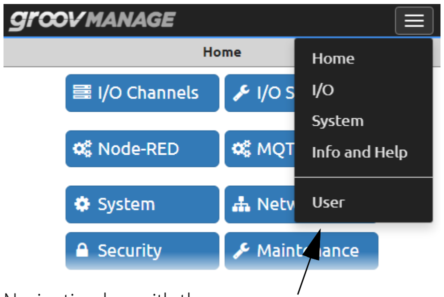
D **Links.** When you see these arrows, it indicates that clicking or tapping on the arrow will open another page that displays more information and provides more functions related to the item. For example, when you click Project Management in the Node-RED page, *groov* Manage displays another page with 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.
- **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

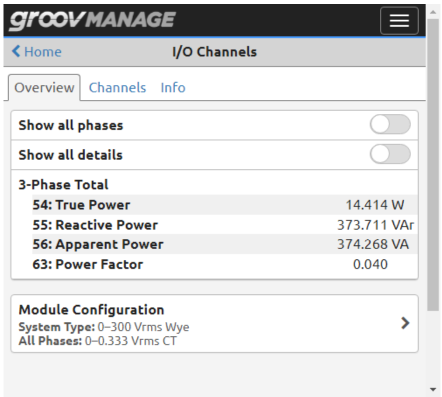
You can navigate through *groov* Manage on a computer or mobile device in much the same way you navigate through any other web application. You can **Drag-and-drop**—a feature commonly used on a computer to visually and easily move files from one location to another. You can drag-and-drop files into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

FINDING INFORMATION ABOUT 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.



Show all phases

Show all details

3-Phase Total

54: True Power	14.414 W
55: Reactive Power	373.711 VAr
56: Apparent Power	374.268 VA
63: Power Factor	0.040

Module Configuration
System Type: 0–300 Vrms Wye
All Phases: 0–0.333 Vrms CT

- **Overview**—This tab provides a way to quickly view real-time values and the current module configuration:
  - Displays the summation values.
  - Provides a way to show or hide the real-time values of all phases or all summation values
  - Displays the current circuit configuration (wye or delta) and provides access to change that configuration.
- **Channels**—This tab provides access to configure any of the 64 channels.
- **Info**—This tab displays the wiring diagram and specification information.

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 the features that Opto 22 provides in *groov* devices to help you with cybersecurity, review *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 EMU will work best with your application and network.
- For a video series on 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 server:

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

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 EMU (see Chapter 3: Initializing a groov RIO EMU).
- You need to understand *permissions* (the ability to access some services and features in *groov* RIO EMU) and determine which permissions you will grant each user, users, or (in the case of 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 EMU. 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 EMU. 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 EMU 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:
    - Change the passwords of other users, including other system-wide administrators.
    - Logout a specific user or all users currently logged into *groov* RIO EMU.
    - Modify the permissions of other users, including other system-wide administrators and, for systems set up to manage user access through LDAP servers, change 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 EMU.
  - Change settings that affect the overall operation of *groov* RIO EMU, 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—Can open the Node-RED editor to build and manage Node-RED flows.
  - Dashboard UI—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)

For more information about *groov* RIO EMU's Data Services OPC UA server, see "Configuring and Enabling OPC UA" on page 58.

Managing Accounts Through LDAP

If your site manages user accounts through a Lightweight Directory Access Protocol (LDAP) service, you can configure your *groov* RIO EMU to connect to the LDAP server, authenticate a user, 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 EMU. Typically, the account you created when you initialized your *groov* RIO EMU has these permissions (review Chapter 3: Initializing a groov RIO EMU).

Note: *This account gives you direct, local access to your groov RIO EMU 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 EMU. To learn more about permissions and how *groov* Manage assigns them to a user, review "Understanding Permissions" on page 24.
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, the account that typically routes authentication requests from LDAP clients to the LDAP server.
   - Connection information like server hostname, 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 27.
   - 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 .
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 29.

6. If you created groups, create permission maps in *groov* Manage as described in "Creating Permission Maps" on page 30.
7. Configure your *groov* RIO EMU 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 31.
8. If your LDAP server requires TLS or LDAPS encryption, update the security certificates as described in "Updating SSL/TLS Certificates" on page 34.
9. Restart the LDAP client and test the connection; review, "Restart LDAP Client and Test Connection" on page 37.

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, and
  - 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 EMU.

  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 24.

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

- **Permissions mapping**—A *groov* RIO EMU system administrator or the LDAP administrator can make changes through any of the following methods:
  - In *groov* Manage, the *groov* RIO EMU 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 EMU 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 31). 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 EMU 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 EMU 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.
- **Start TLS.** 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 Start TLS 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 identify 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

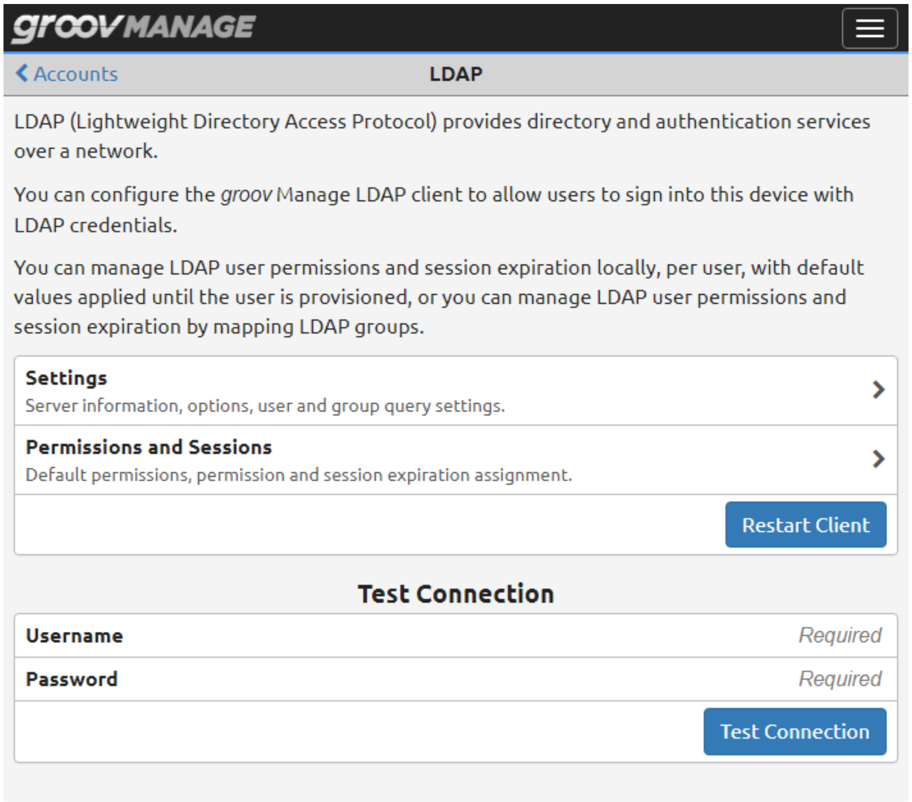
You'll want to work with your LDAP administrator to obtain the following information:

- 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 will be ignored (filtered out). 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 will be 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 EMU with a user ID that has system administrator permission.
2. Click Accounts, then LDAP Settings. *groov* Manage displays the main LDAP page.



groov MANAGE

‹ 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.

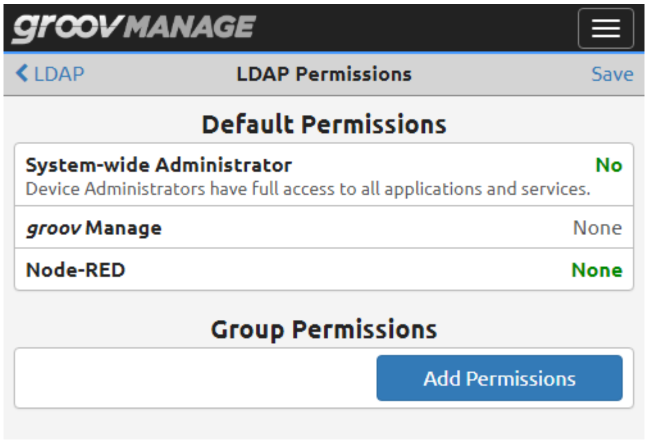
Restart Client

Test Connection

Username	*Required*
Password	*Required*

Test Connection

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



groov MANAGE

‹ LDAP — **LDAP Permissions** — Save

Default Permissions

System-wide Administrator Device Administrators have full access to all applications and services.	No
***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.*

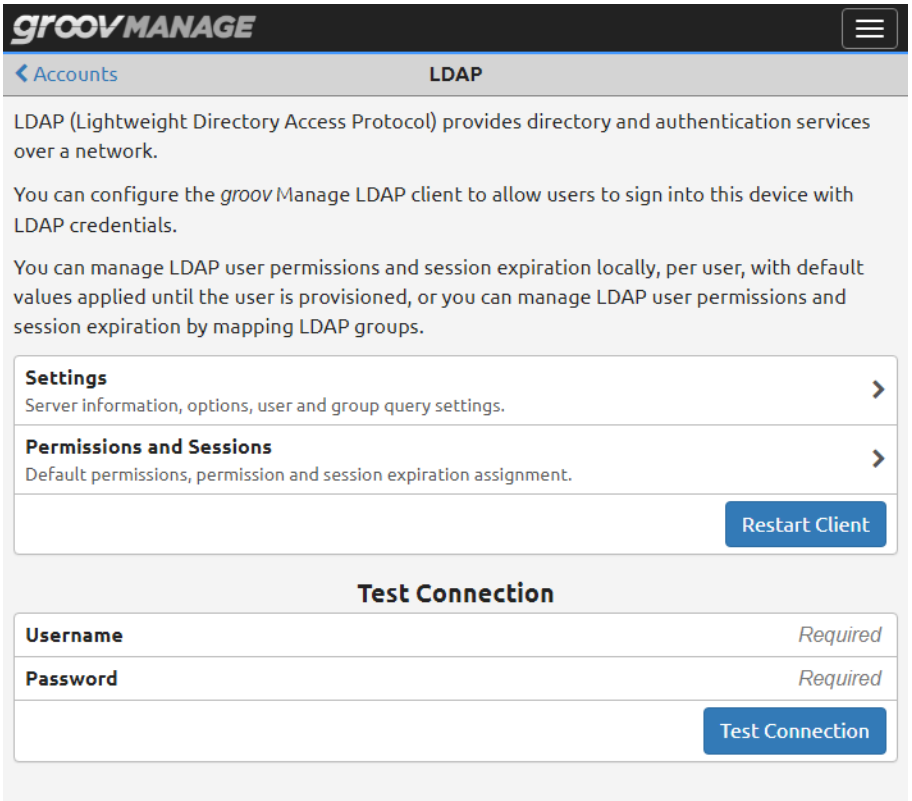
For a list of services and their permissions, see "Understanding Permissions" on page 24.

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 EMU with a user ID that has system administrator permission.
2. Click Accounts, then LDAP Settings. *groov* Manage displays the main LDAP page.



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.

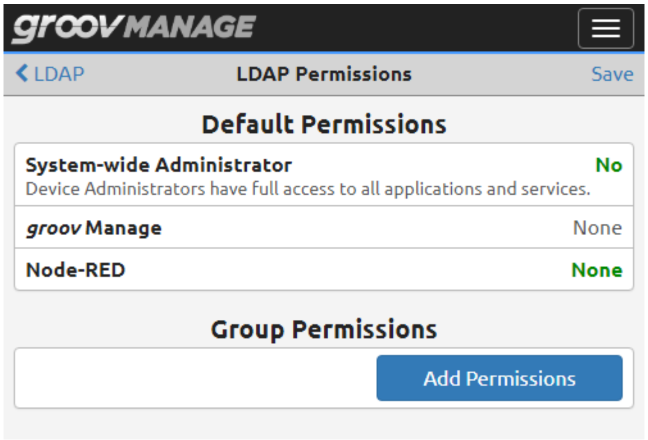
Settings
Server information, options, user and group query settings.

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

Test Connection

Username	*Required*
Password	*Required*

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

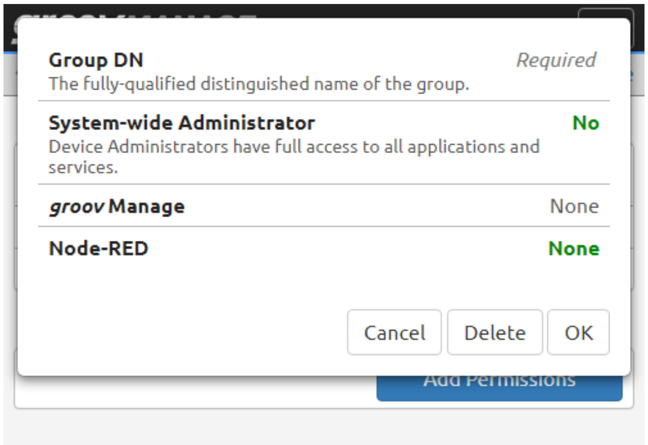


Default Permissions

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

Group Permissions

4. Click Add Permissions in the Group Permissions section.



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

System-wide Administrator **No**
Device Administrators have full access to all applications and services.

groov Manage None

Node-RED **None**

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 25).
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

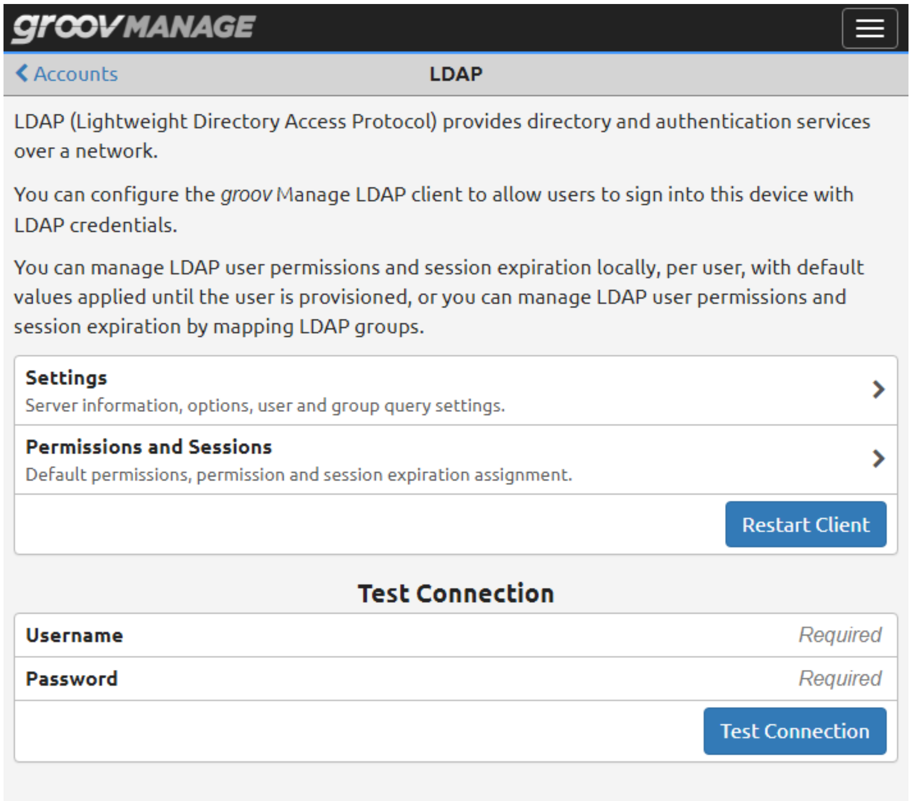
Before you begin, make sure you have the information described in:

- "Information Required to Configure Communication to an LDAP Server" on page 27
- "Information Required to Authenticate Users Through LDAP" on page 28.

Let's get started:

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

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



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.

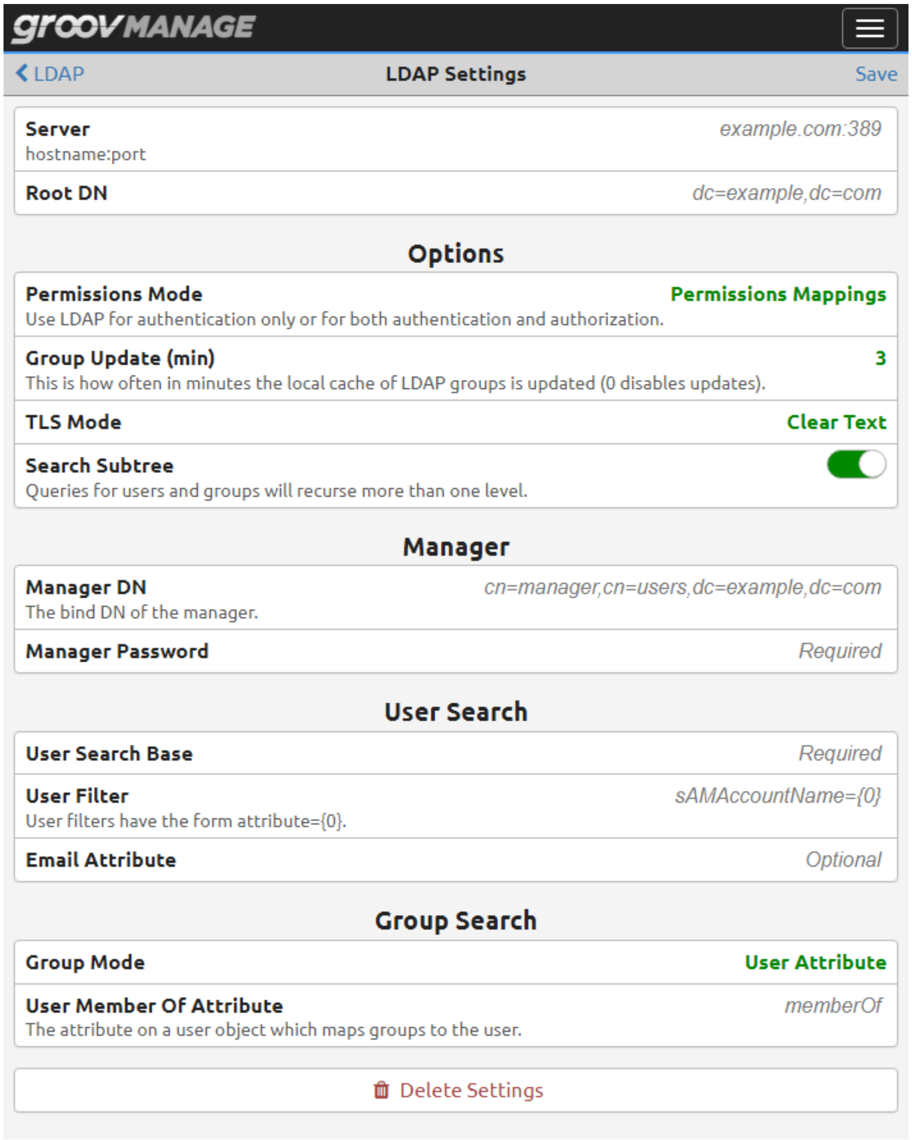
Settings
Server information, options, user and group query settings.

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

Test Connection

Username	*Required*
Password	*Required*

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



groov MANAGE

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

a. Enter the Server and Root DN information you collected in "Information Required to Configure Communication to an LDAP Server" on page 27.

b. In the Options section:

– Set Permissions Mode to either Local Permissions or Permissions Mapping. To understand the difference, see "Understanding How LDAP and groov Manage Authenticate Users and Assign Permissions" on page 26.

– In the Group Update 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 "Information Required to Configure Communication to an LDAP Server" on page 27).

For LDAPS or StartTLS, if you enable the Validate Certificates switch, you can upload the TLS certificate now or later on in step 3 on page 38. 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 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 "Information Required to Authenticate Users Through LDAP" on page 28.

d. In the Group Search section, if Permissions Mode is Local Permissions, do not specify anything for Group Search. If Permissions Mode is 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 "Information Required to Authenticate Users Through LDAP" on page 28 in the fields.

4. Click Save. *groov* Manage validates some of the information and then saves it.

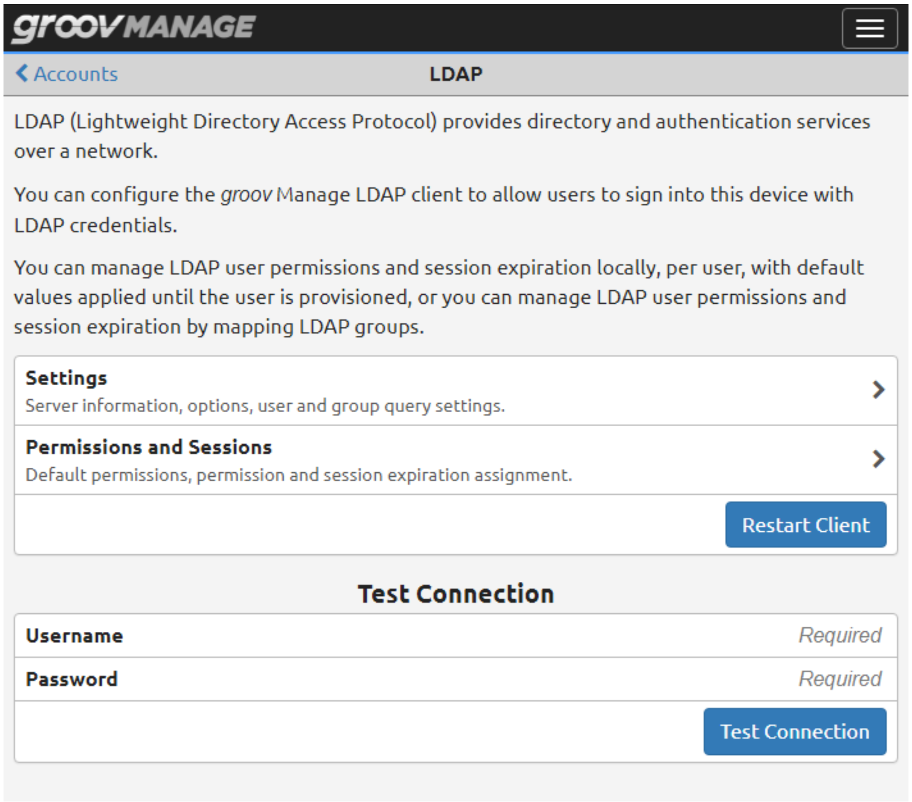
If *groov* Manage finds any invalid information, it highlights (in red) the fields with invalid information and shows a message with guidance on how to fix it. After you fix the information, click Save.

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 EMU. 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 EMU.

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

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



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.

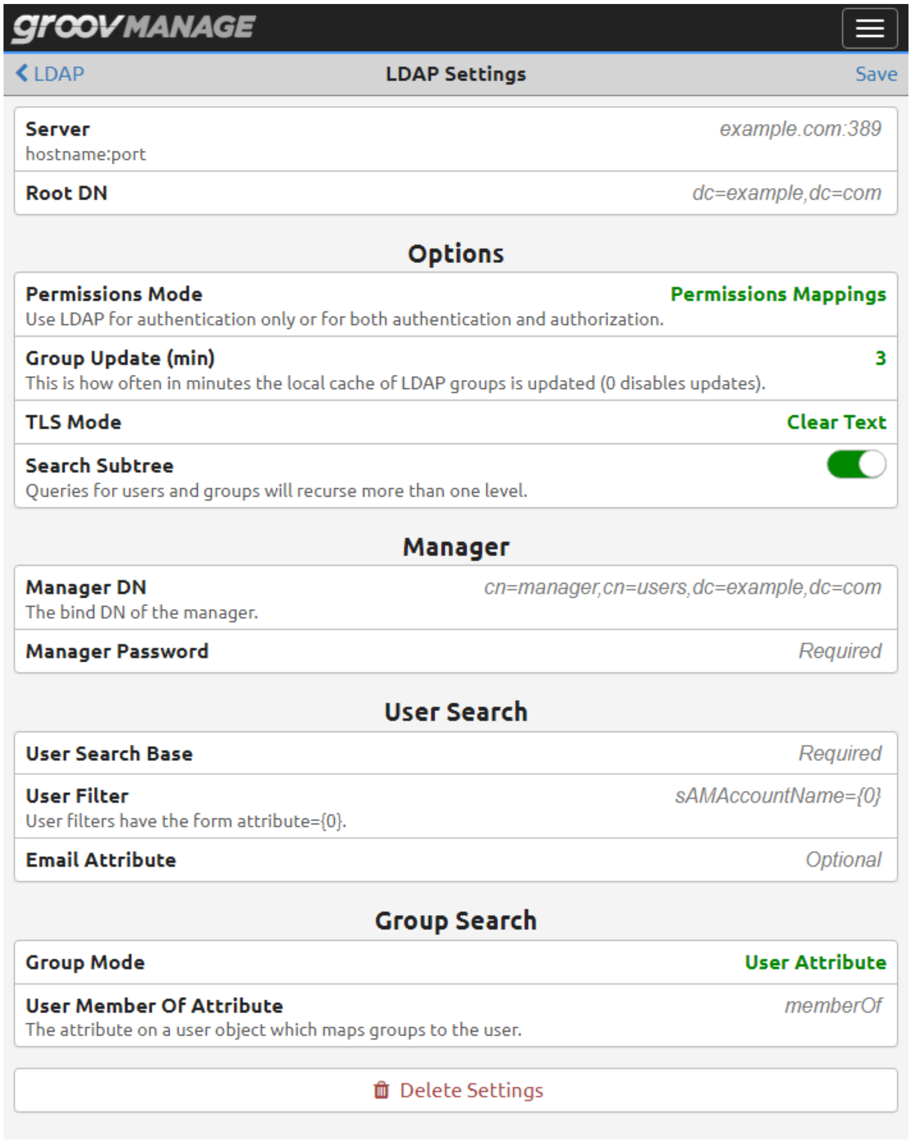
Permissions and Sessions
Default permissions, permission and session expiration assignment.

Test Connection

Username Required

Password Required

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



LDAP Settings

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

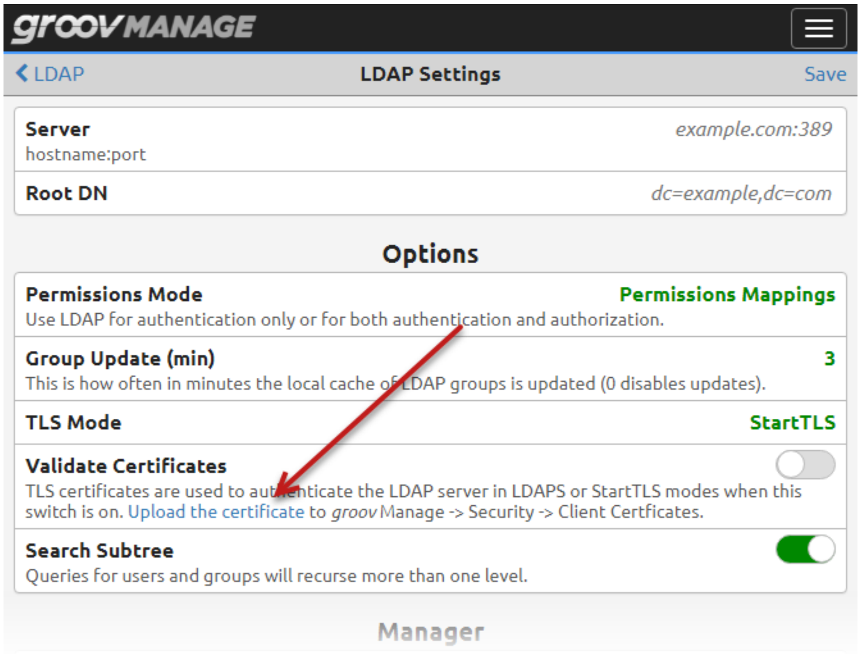
User Member Of Attribute memberOf
The attribute on a user object which maps groups to the user.

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.

6. Click Upload the Certificate.



LDAP | LDAP Settings | Save

Server hostname:port — example.com:389

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).

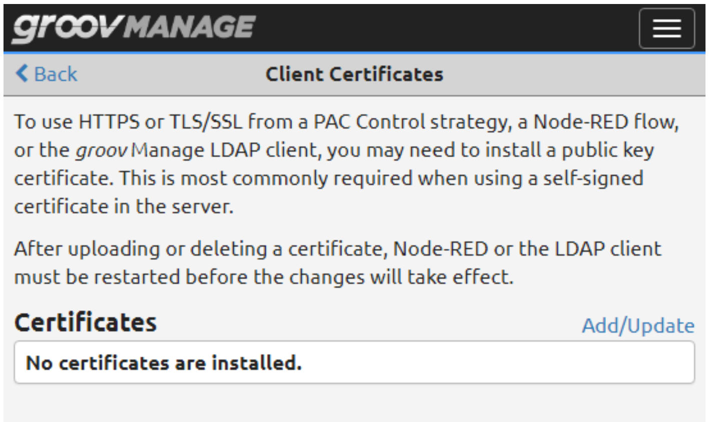
TLS Mode — StartTLS

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 Certficates.

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

Manager

groov Manage displays the Client Certificates page.



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.

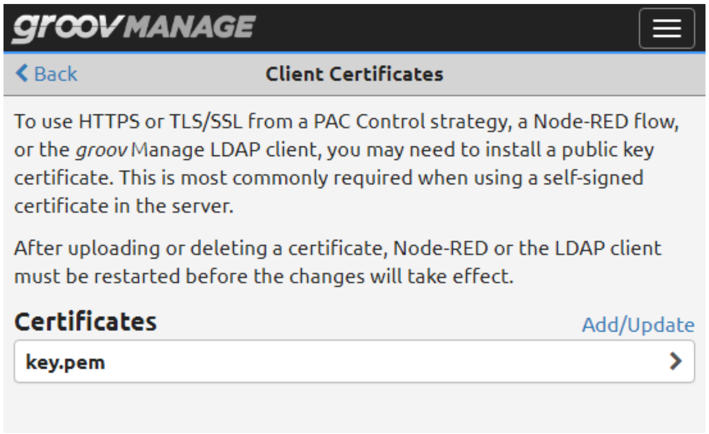
After uploading or deleting a certificate, Node-RED or the LDAP client must be restarted before the changes will take effect.

Certificates — Add/Update

No certificates are installed.

7. Click Add/Update.
8. 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.



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.

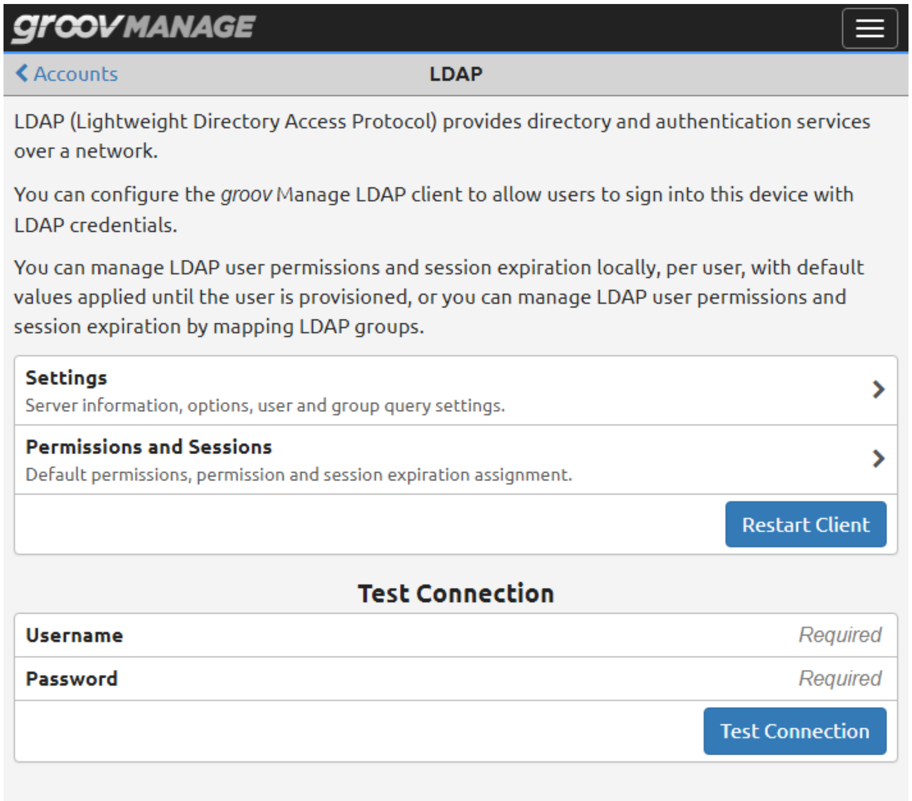
After uploading or deleting a certificate, Node-RED or the LDAP client must be restarted before the changes will take effect.

Certificates Add/Update

key.pem

Restart LDAP Client and Test Connection

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



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.

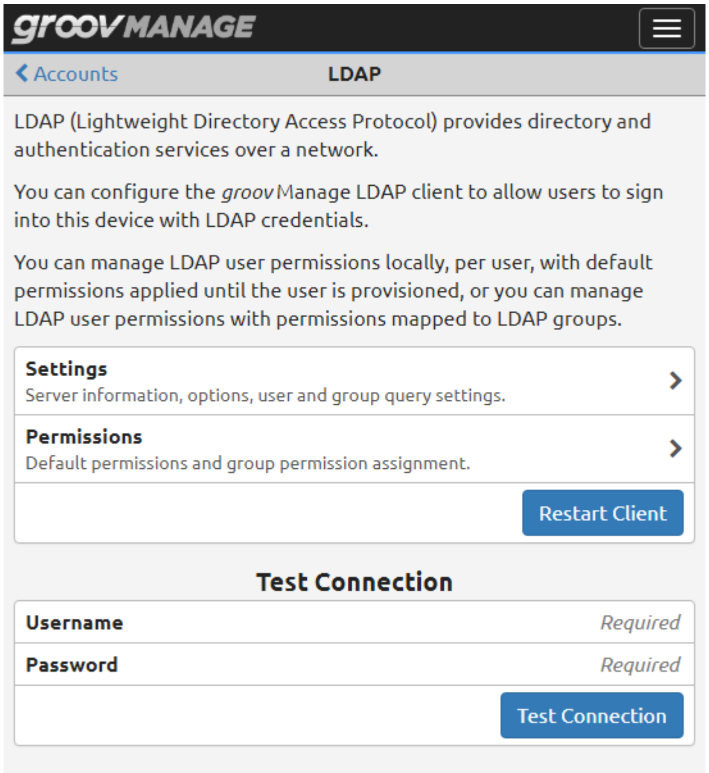
Settings
Server information, options, user and group query settings.

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

Test Connection

Username	*Required*
Password	*Required*

3. In the LDAP page, click Restart Client.



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.

Test Connection

Username	*Required*
Password	*Required*

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 HMIs. You manage these accounts (their creation, deletion, and their access to services/resources) on your *groov* RIO EMU. 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 EMU

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

- encrypt communications and,
- prove the *groov* RIO EMU'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 EMU and client/server applications. To understand how this works, see Appendix C: Understanding Certificates.

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 EMU 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 EMU can trust a server), you need to know which applications on your *groov* RIO EMU operate as clients and which operate as servers. The following applications on your *groov* RIO EMU 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 EMU 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 EMU's trust store.

groov RIO EMU 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 EMU, then install the *groov* RIO EMU'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 39) or CA-verified (see page 40) server certificate created by or for your *groov* RIO EMU 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 EMU is https://process1.acme.com, then type in `process1.acme.com`

Example:

If the URL that others will use to access the *groov* RIO EMU 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 EMU 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 39.

If you have not created a custom self-signed certificate, do that first. See “Creating a Custom Self-Signed Certificate” on page 39.

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 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.

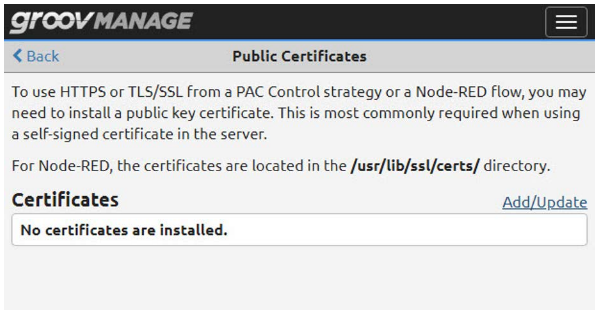
groov RIO EMU as a Client: Adding a Server's Certificate

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 EMU (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 EMU.

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



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

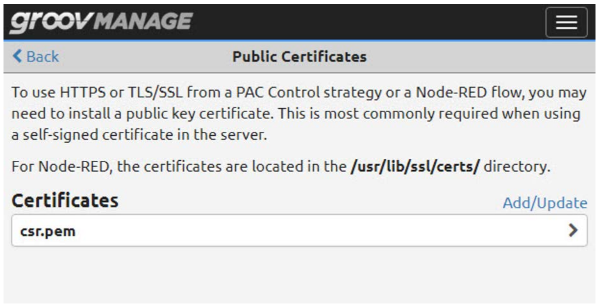
For Node-RED, the certificates are located in the **/usr/lib/ssl/certs/** directory.

Certificates Add/Update

No certificates are installed.

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

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



Public Certificates

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

For Node-RED, the certificates are located in the **/usr/lib/ssl/certs/** directory.

Certificates Add/Update

csr.pem

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

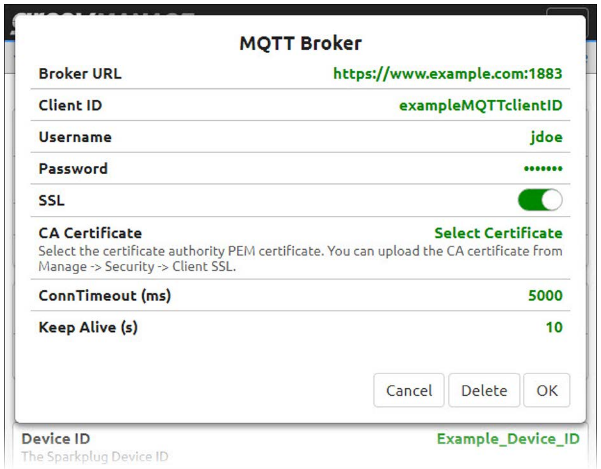
Changing SSL Security Features for Sparkplug

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

- For instructions on creating the certificate, see "Creating or Switching to a CA-verified Certificate" on page 40.
- For instructions on installing the certificate on the processor, see "Uploading a Public Certificate to a groov RIO EMU's Trust Store" on page 43.

After you installed the certificate(s):

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

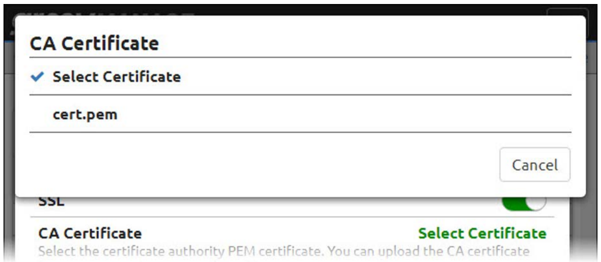


MQTT Broker

Broker URL	https://www.example.com:1883
Client ID	exampleMQTTclientID
Username	jdoe
Password	•••••••
SSL	🟩
CA Certificate Select the certificate authority PEM certificate. You can upload the CA certificate from Manage -> Security -> Client SSL.	Select Certificate
ConnTimeout (ms)	5000
Keep Alive (s)	10

Device ID Example_Device_ID
The Sparkplug Device ID

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



CA Certificate

✓ Select Certificate

cert.pem

Cancel
SSL
CA Certificate
Select Certificate
Select the certificate authority PEM certificate. You can upload the CA certificate

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 EMU contains firewall technology to protect it from unauthorized connections and communication. The *host* firewall on your *groov* RIO EMU can help you open and close ports on each network interface (ETH0, ETH1, WLAN0, TUN0).

Before you configure the host firewall on *groov* RIO EMU, 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	
groov View	443	

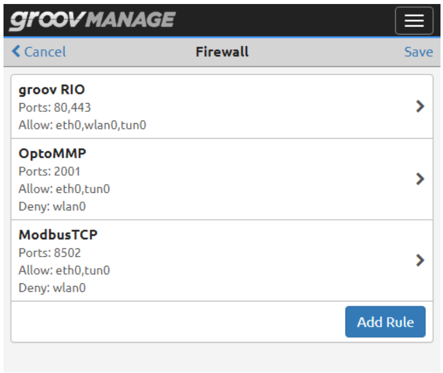
Remember that you want to connect trusted networks to the ETH0 network interface and any untrusted networks to the ETH1 network interface.

Creating a Firewall Rule

When you make changes to the *groov* RIO EMU'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 EMU 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:



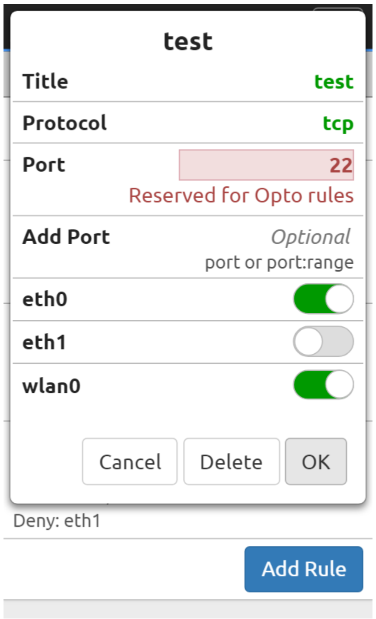
groov RIO
Ports: 80,443
Allow: eth0,wlan0,tun0

OptoMMP
Ports: 2001
Allow: eth0,tun0
Deny: wlan0

ModbusTCP
Ports: 8502
Allow: eth0,tun0
Deny: wlan0

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 (🟩).

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



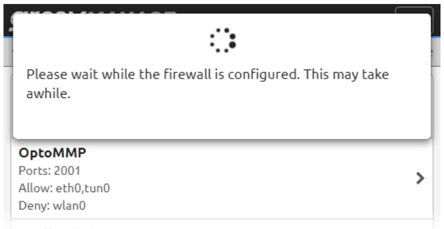
test

Title	test
Protocol	tcp
Port	22 Reserved for Opto rules
Add Port	Optional port or port:range
eth0	●
eth1	○
wlan0	●

Deny: eth1

Fix the error or errors and then click OK.

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



Please wait while the firewall is configured. This may take awhile.

OptoMMP
Ports: 2001
Allow: eth0,tun0
Deny: wlan0

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.

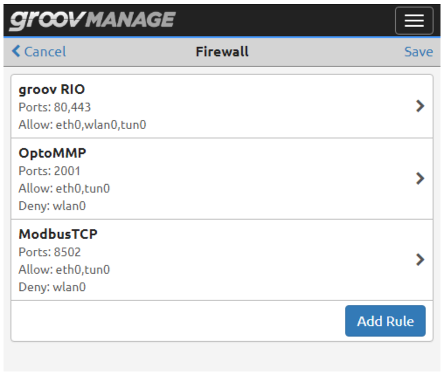
Changing a Firewall Rule

When you make changes to *groov* RIO EMU'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:

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

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

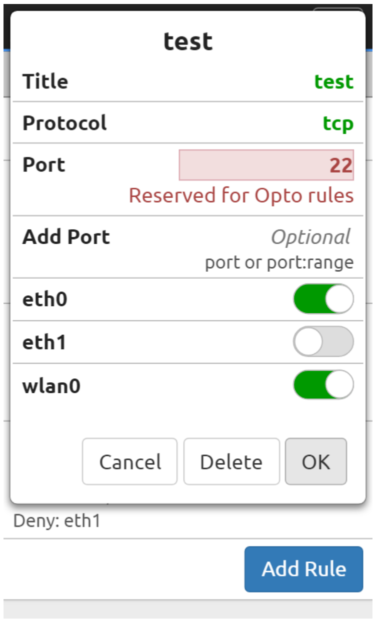


groov RIO
Ports: 80,443
Allow: eth0,wlan0,tun0

OptoMMP
Ports: 2001
Allow: eth0,tun0
Deny: wlan0

ModbusTCP
Ports: 8502
Allow: eth0,tun0
Deny: wlan0

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.



test

Title: test

Protocol: tcp

Port: 22
Reserved for Opto rules

Add Port: Optional
port or port:range

eth0: on

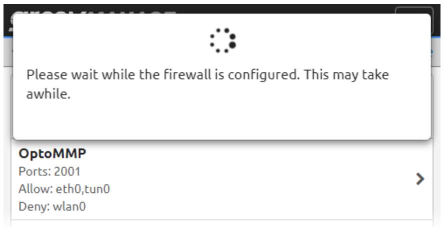
eth1: off

wlan0: on

Deny: eth1

Fix the error or errors and then click OK.

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



Please wait while the firewall is configured. This may take awhile.

OptoMMP
Ports: 2001
Allow: eth0,tun0
Deny: wlan0

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: Enable Data Services: MQTT and OPC UA

Data Services is a runtime that helps you publish (to an MQTT broker) or access (from an OPC UA client) to tag data from the local I/O, PID, and Scratch Pad area of the OptoMMP memory map.

If you aren't familiar with MQTT or OPC UA, you can read the following brief introductions of each protocol:

- "What is MQTT?" on page 52
- "What is OPC UA?" on page 58

OPC UA servers on groov RIO EMUs. The *groov* RIO EMU provides the following OPC UA servers:

- The Data Services OPC UA server, which is described in this chapter.
- Node-RED (by adding third-party OPC UA nodes; refer to their documentation)
- CODESYS OPC UA server (see online help from CODESYS)

MQTT clients on groov RIO EMUs. The *groov* RIO EMU provides the following MQTT clients:

- The Data Services MQTT client, which is described in this chapter.
- Node-RED (by adding third-party MQTT nodes; refer to their documentation)
- CODESYS MQTT client (see online help from CODESYS)

A word on MQTT terminology (client/sever *versus* publisher/subscriber/broker): Although MQTT's 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 EMU and an MQTT broker or OPC UA client. To configure this communication:

1. Enable public access to your local data. By default, local I/O data is not available to MQTT and OPC UA; you must expose it (enable public access). For a summary on how to do this, review "Exposing Data (Public Access)" on page 53.
2. 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 23.
   - If your site requires SSL:

  - For OPC UA, create an SSL server certificate in *groov* Manage, then upload it to the computers or mobile devices running your OPC UA clients. For instructions, review "groov RIO EMU as a Server: Creating Server Certificates" on page 39.
  - For MQTT, obtain the server SSL certificate from the MQTT broker (server) and add it to the Data Services MQTT client on the *groov* RIO EMU. For instructions, review "Uploading a Public Certificate to a groov RIO EMU's Trust Store" on page 43.

3. Create a scanned device to the local I/O, PID, and Scratch Pad. For instructions, review "Add Scan Device For Local I/O, PID, and Scratch Pad" on page 55.
4. To configure the Data Services MQTT client, review "Configuring and Enabling MQTT" on page 52.
5. To configure the Data Services OPC UA server, review "Configuring and Enabling the groov RIO EMU Native OPC UA Server" on page 60.
6. Enable the Data Service runtime and test the connection. For instructions, review "Enabling Data Services and Testing Connections" on page 63.

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 EMU, you must expose the data by enabling *public access*. There are several ways to enable public access:

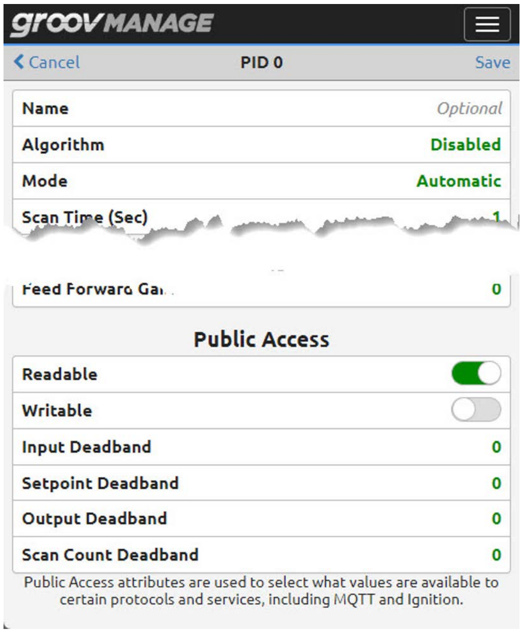
- Through *groov* Manage. Select this method if:
  - you need to expose only a few I/O channels, PID loops, and/or areas of the Scratch Pad, or
  - you want to efficiently expose *all* I/O channels on a module. **Important:** Before you expose all I/O channels, verify that you want and will use data 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 a few channels, review the Public Access section on page 72 of the "Customizing a Channel" section.
  - for all channels at once, review "Changing Some Settings on All Channels at Once" on page 72.
  - for PID loops, review "Enabling Public Access to PID Loops through groov Manage" on page 51.
  - for ScratchPad areas, review "Enabling Public Access to Scratch Pad Area through groov Manage" on page 51.
- Through programming: within your application, enable public access by turning on the correct values through OptoMMP. For instructions, review OptoMMP Protocol Guide (form 1465).

Enabling Public Access of the PID Loops through *groov* Manage

1. Log into your *groov* RIO EMU with an account that has system administrator permission.
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.



PID 0

Name	Optional
Algorithm	Disabled
Mode	Automatic
Scan Time (Sec)	1
Feed Forward Gai	0

Public Access

Readable	☑
Writable	☐
Input Deadband	0
Setpoint Deadband	0
Output Deadband	0
Scan Count Deadband	0

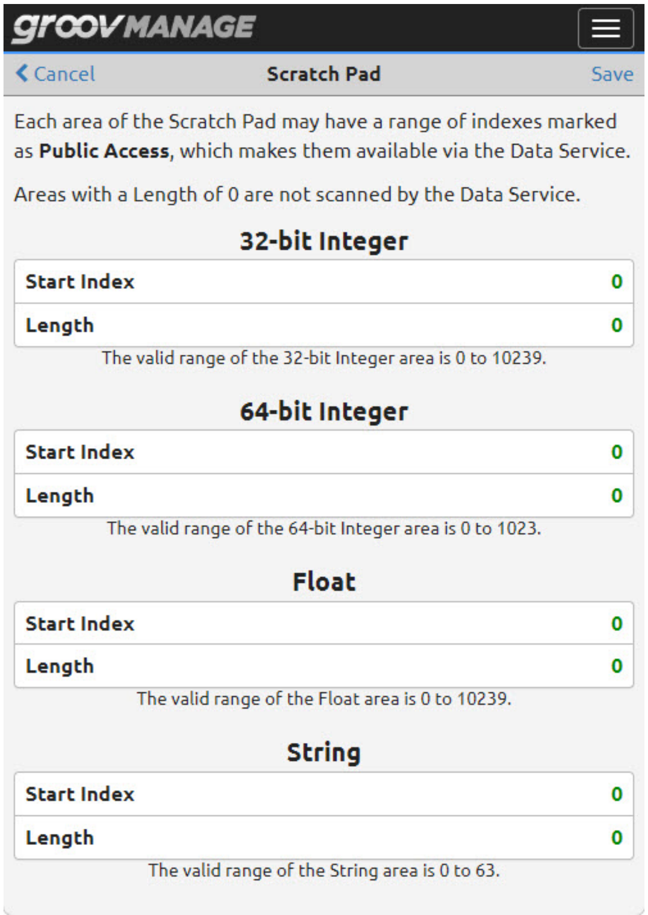
Public Access attributes are used to select what values are available to certain protocols and services, including MQTT and Ignition.

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 EMU with an account that has system administrator permissions.

2. Click I/O > I/O Services > Scratch Pad > Public Access. *groov* Manage displays the public access page for the Scratch Pad area.



Scratch Pad

Each area of the Scratch Pad may have a range of indexes marked as **Public Access**, which makes them available via the Data Service.

Areas with a Length of 0 are not scanned by the Data Service.

32-bit Integer

Start Index	0
Length	0

The valid range of the 32-bit Integer area is 0 to 10239.

64-bit Integer

Start Index	0
Length	0

The valid range of the 64-bit Integer area is 0 to 1023.

Float

Start Index	0
Length	0

The valid range of the Float area is 0 to 10239.

String

Start Index	0
Length	0

The valid range of the String area is 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, 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 Scrath Pad area, review OptoMMP Protocol Guide (form 1465).

3. Click Save.

CREATING A SCANNED DEVICE

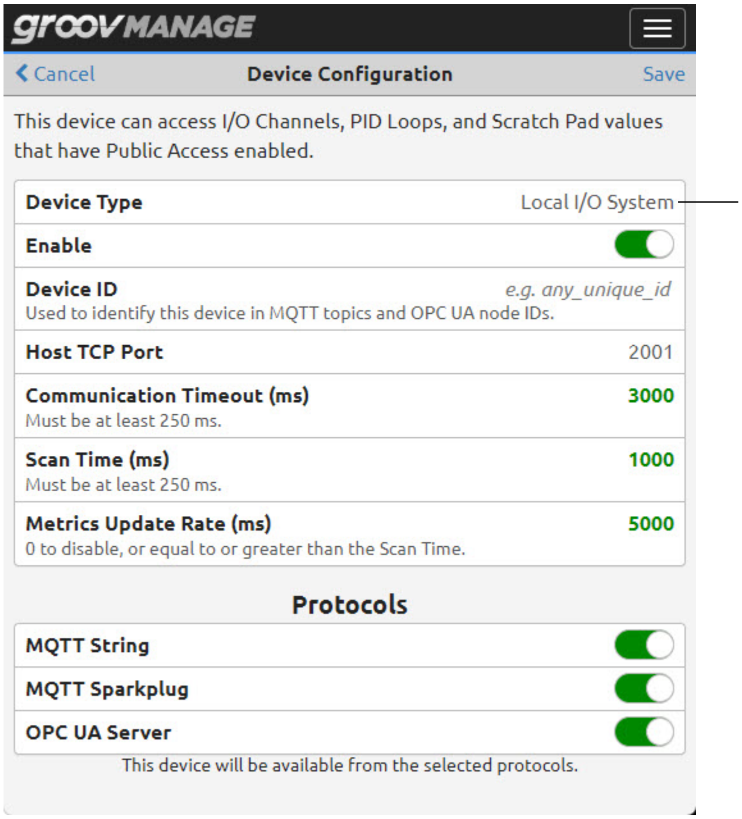
A **scanned** device manages the communication between the local I/O (I/O data, PID loops, and Scratch Pad area of the OptoMMP memory map) and:

- the MQTT broker (through the Data Services MQTT client), and
- OPC UA client (through the Data Services OPC UA server).

[1] Remember that numbering of elements begins with 0.

You can add a label (called a *device ID*) to identify the source of the data (your *groov* RIO EMU) and alter some settings to improve performance and throughput.

1. Log into your *groov* RIO EMU with an account that has system administrator permissions.
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
Enable	●
Device ID Used to identify this device in MQTT topics and OPC UA node IDs.	*e.g. any_unique_id*
Host TCP Port	2001
Communication Timeout (ms) Must be at least 250 ms.	3000
Scan Time (ms) Must be at least 250 ms.	1000
Metrics Update Rate (ms) 0 to disable, or equal to or greater than the Scan Time.	5000

Protocols

MQTT String	●
MQTT Sparkplug	●
OPC UA Server	●

This device will be available from the selected protocols.

For your information.

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 EMU. 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 EMU's hostname.
- If you manage multiple *groov* RIO EMUs, include where it is 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 "Collecting Information About the MQTT Broker" on page 55). 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.

4. Click Save.

CONFIGURING AND ENABLING MQTT

MQTT is a publish/subscribe (pub/sub) protocol that's 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's a great choice for automation applications, visit our website (www.opto22.com), and search for "What is an MQTT broker?"

Contrast this 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 doesn't know when the data changes, so it must request it at regular intervals.

MQTT pub/sub offers three main advantages over client/server for IoT 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 don't have to strain to serve multiple clients. And even remote devices with irregular connections or low bandwidth can publish or subscribe to data. If a publisher can't 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's 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 Paper: Industrial-strength MQTT/Sparkplug B,
  - case studies, and
  - specialized documents (for example, Getting Started with MQTT in groov Products).

Choosing the Right MQTT Client and Payload Type

There are many factors to consider when you include a *groov* RIO EMU into an existing MQTT infrastructure, including the type of payload and client. *groov* RIO EMU provides several different MQTT clients that can publish data in two different payload formats (string and Sparkplug B):

- Data Services MQTT client
- Node-RED (by adding MQTT client nodes)
- 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 EMU for simple data collection and control, or for high-reliability SCADA/IIoT applications.

If you choose the Data Services MQTT client, review "Configuring and Enabling the Data Services MQTT Client" (below). If you choose Node-RED, refer to the documentation provided by the node author for instructions on configuration.

Configuring and Enabling the Data Services MQTT Client

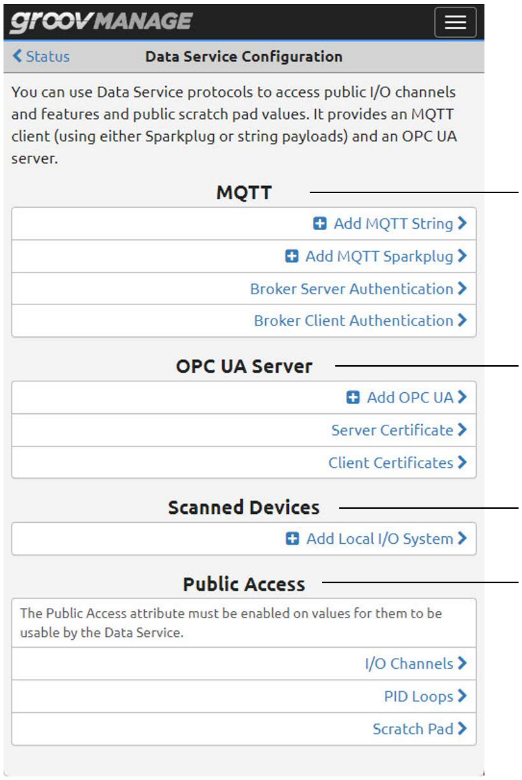
Before you configure and enable the Data Services MQTT client, remember to first finish the following tasks:

- Upload server certificates from your MQTT server (broker) to your *groov* RIO EMU (see "Managing Certificates on your groov RIO EMU" on page 39).
- Create the scanned device (see "Creating a Scan Device" on page 51).

Completing these tasks will make the following steps easier to finish.

1. Log into your *groov* RIO EMU with an account that has system administrator permissions.
2. From the *groov* Manage Home page, click Data Service, then click 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.



groovMANAGE

< Status **Data Service Configuration**

You can use Data Service protocols to access public I/O channels and features and public scratch pad values. It provides an MQTT client (using either Sparkplug or string payloads) and an OPC UA server.

MQTT

- Add MQTT String >
- Add MQTT Sparkplug >
- Broker Server Authentication >
- Broker Client Authentication >

OPC UA Server

- Add OPC UA >
- Server Certificate >
- Client Certificates >

Scanned Devices

- Add Local I/O System >

Public Access

The Public Access attribute must be enabled on values for them to be usable by the Data Service.

- I/O Channels >
- PID Loops >
- Scratch Pad >

Configure the Data Services MQTT clients for each payload type, specify the MQTT broker(s), and (if you haven't already done so) add the certificates (and keys) required by the MQTT broker(s).

Configure the Data Services OPC UA server and create the certificates; see "Configuring and Enabling OPC UA" on page 58.

Create the scanned device. For instructions, review "Creating a Scan Device" on page 51.

Configure public access of the local I/O.

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 "The MQTT String Configuration Page" on page 57 and add the broker(s) as described in "The MQTT Broker Configuration Page" on page 60.

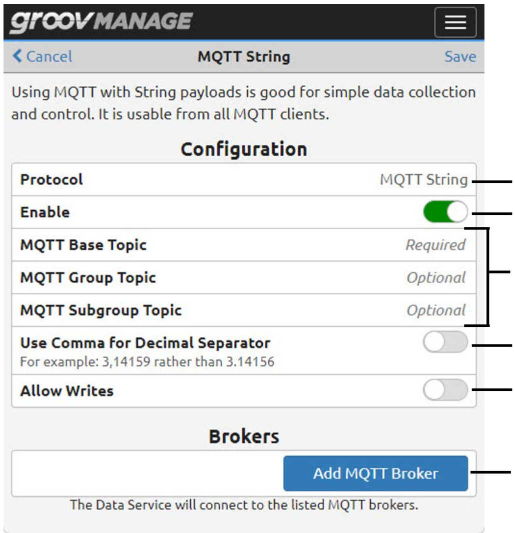
For Sparkplug payloads, click Add MQTT Sparkplug to display the MQTT Sparkplug configuration page and fill out the fields as described in "The MQTT Sparkplug Configuration Page" on page 58 and add the broker(s) as described in "The MQTT Broker Configuration Page" on page 60.

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 "Enabling Data Services and Testing Connections" on page 65.
- If you want to configure the Data Services OPC UA server before enabling Data Service, then review "Configuring and Enabling OPC UA" on page 62.

The MQTT String Configuration Page



Using MQTT with String payloads is good for simple data collection and control. It is usable from all MQTT clients.

Configuration

Protocol	MQTT String
Enable	●
MQTT Base Topic	*Required*
MQTT Group Topic	*Optional*
MQTT Subgroup Topic	*Optional*
Use Comma for Decimal Separator For example: 3,14159 rather than 3.14156	○
Allow Writes	○

Brokers

The Data Service will connect to the listed MQTT brokers.

For your information.

A

B

C

D

For instructions on adding a broker, see "Adding an MQTT Broker" on page 57.

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 EMU 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 EMU 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 module 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.

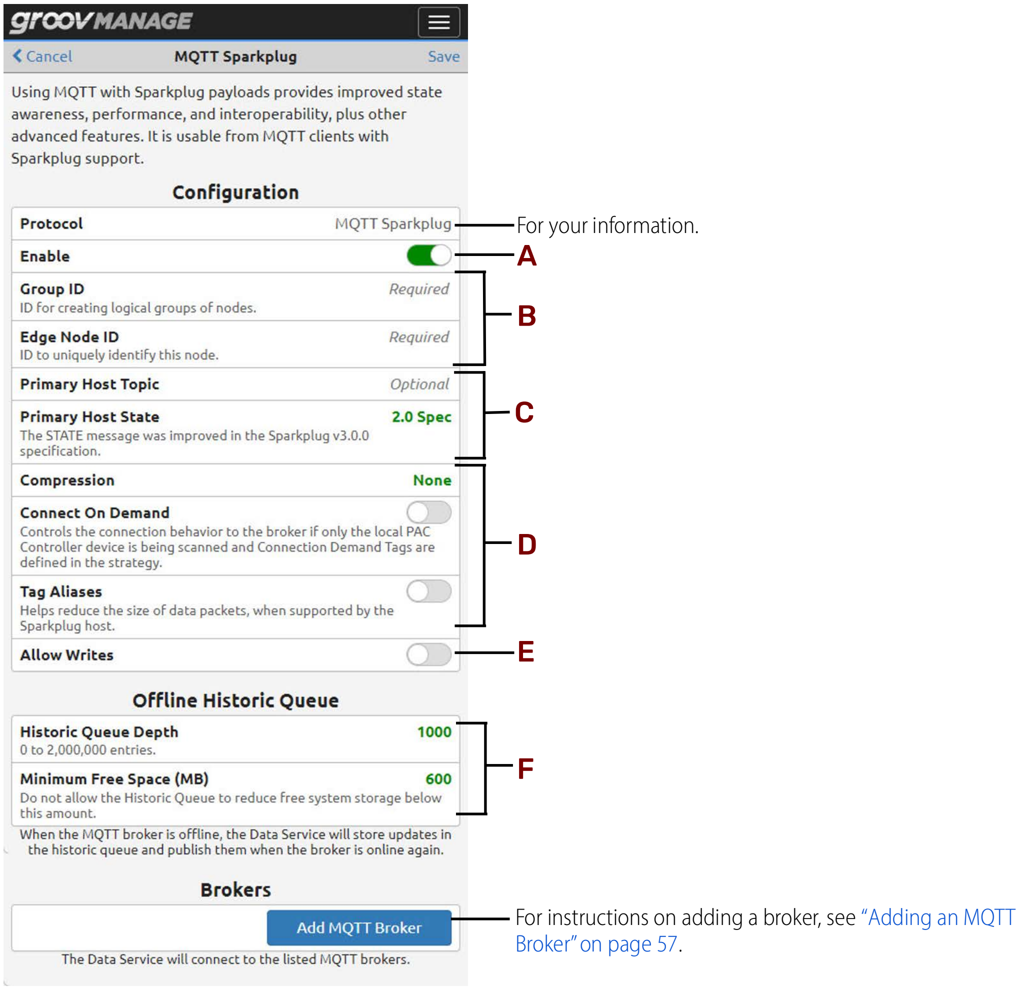
C If your application uses a comma to separate values (for example, pi is denoted as 3,14 instead of 3.14), you'll want to indicate that by enabling the **Use Comma for Decimal Separator** setting.

D **Allow Writes**—Controls whether *groov* RIO EMU 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 Sparkplug Configuration Page



Using MQTT with Sparkplug payloads provides improved state awareness, performance, and interoperability, plus other advanced features. It is usable from MQTT clients with Sparkplug support.

Configuration

Protocol	MQTT Sparkplug
Enable	●
Group ID ID for creating logical groups of nodes.	*Required*
Edge Node ID ID to uniquely identify this node.	*Required*
Primary Host Topic	*Optional*
Primary Host State The STATE message was improved in the Sparkplug v3.0.0 specification.	2.0 Spec
Compression	None
Connect On Demand Controls the connection behavior to the broker if only the local PAC Controller device is being scanned and Connection Demand Tags are defined in the strategy.	○
Tag Aliases Helps reduce the size of data packets, when supported by the Sparkplug host.	○
Allow Writes	○

Offline Historic Queue

Historic Queue Depth 0 to 2,000,000 entries.	1000
Minimum Free Space (MB) Do not allow the Historic Queue to reduce free system storage below this amount.	600

When the MQTT broker is offline, the Data Service will store updates in the historic queue and publish them when the broker is online again.

Brokers

The Data Service will connect to the listed MQTT brokers.

For your information.

For instructions on adding a broker, see "Adding an MQTT Broker" on page 57.

A The MQTT Sparplug protocol is enabled by default; however, you may want to disable it if you want to stop it yet still preserve the configuration information.

B To uniquely identify your *groov* RIO EMU within your MQTT infrastructure, specify a group ID and edge node ID:

- **Group ID**—Identifies the group that your *groov* RIO EMU belongs to.
- **Edge Node ID**—Identifies your *groov* RIO EMU within the group.

If necessary, consult with someone in your organization that assigns IDs within your MQTT infrastructure to determine whether a specific group or edge node ID is assigned to your *groov* RIO EMU, or whether you should follow a particular naming convention when you create these IDs.

C If your MQTT infrastructure monitors the connection status of clients and servers through a primary host application, specify the primary host topic and select the format of the STATE message:

Primary Host Topic—A name, typically characters or numbers, that matches the name used in the primary host application ID of the corresponding server or client application.

Primary Host State—The format (version 3.0 or 2.0 of the Sparkplug specification) of the STATE message.

D The following options can help adjust performance:

- **Compression**—If your MQTT infrastructure supports compression, select the supported algorithm to compress payloads before they are published to the MQTT server.

  Enabling compression can reduce the amount of network traffic; however, Data Service must use additional processing resources to compress the payloads. This may slow down payload publication especially when payloads are larger. For very small payloads, compressing may increase the size of the payloads.
- **Connect on Demand**—Does not apply to *groov* RIO modules.
- **Tag Aliases**—If your MQTT infrastructure implements tag aliasing, enable the Tag Alias switch. Tag aliases help create smaller and more efficient publications by replacing lengthy topic names with a numeric value.

Improving performance by adjusting deadband values. *Adjusting deadband values of I/O tags and PID loop variable tags can improve performance by increasing the amount of change an I/O channel value or PID loop variable goes through before Data Service publishes a topic. To adjust the deadband values:*

- *for I/O channels, review "Customizing a Channel" , specifically the section describing Public Access on page page 72.*
- *for PID loop variables, review "Enabling Public Access of the PID Loops through groov Manage" on page 50.*

E **Allow Writes**—Controls whether your *groov* RIO EMU accepts write requests.

F **Offline Historic Queue**—If the *groov* RIO EMU becomes offline and needs to start saving payloads, the settings in this section help manage storage resources:

- **Historic Queue**—The maximum number of publications that may be saved in user space when the connection to the primary application is not available. The value may range from 0 to 65535. The recommended value is 3600, a value that takes into account the fixed size of memory, which is also utilized by system applications. If the number of publications exceeds this value, the oldest entries are discarded to make room for newer entries.

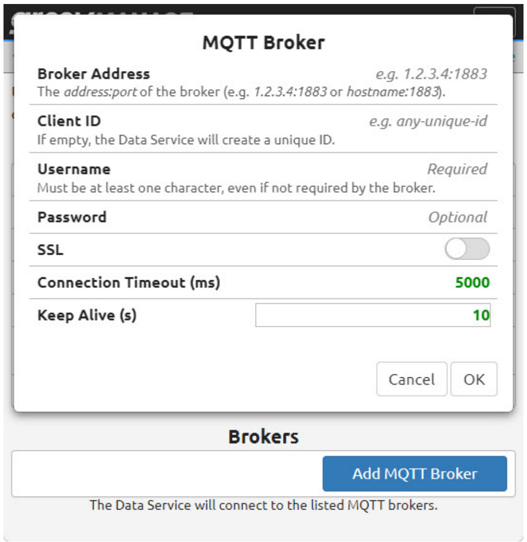
  You may want to change this value after considering the following factors:
  - ***Storage limitations.*** The publications are stored in user space, so when you specify a large value, storage space can be consumed quickly.
  - ***Scan Time and frequency of change in values.*** The following examples show why these two factors can create a large difference in the number of publications created:
    - **Scan Time: 1 millisecond vs 1 second scan time.** In a 2 second time period, the 1 millisecond scan time could create 2000 publications, whereas the 1 second scan time could create only two publications. (The Scan Time is the value you entered when you configured the scanned device; for details, review "Creating a Scanned Device" on page 52.)
    - **A tag that changes value every second versus every hour.** In a 2 hour time period, a tag that changes value every second could create up to 7200 publications, whereas a tag that changes value every hour could create only two publications.

    Scan Time and frequency of change are closely related: a publication is produced only when the value of a tag changes. Working with the examples we described previously: If a tag is scanned every millisecond, but the values changes only every 10 milliseconds, then the number of publications created would be 200, instead of 2000.

    Review your Scan Time and how frequently the values of your tags may change within a given time period to help you estimate how many publications might be created.
  - ***Varying sizes of publications.*** Publications created by the MQTT service on your *groov* RIO EMU can contain many tags or as few as one tag.

– **Minimum Free Space (MB).** The amount of megabytes to leave available in user space. If the historic queue fills up the available space, it deletes the oldest messages to make room for new messages.

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) 10

Brokers

The Data Service will connect to the listed MQTT brokers.

For each broker, you'll 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 "Changing SSL Security Features for Sparkplug" on page 42.
- **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 EMU is in an area with "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 EMU.

CONFIGURING AND ENABLING THE DATA SERVICES OPC UA SERVER

OPC UA is a communications protocol with a long history and established base of implementations in many industrial applications. This client/server architecture has proven reliability and adding your *groov* RIO EMU helps you build upon this reliability and increase the reach of your OPC UA application.

OPC UA Servers on *groov* RIO EMU

groov RIO EMU can run several different OPC UA servers simultaneously:

- The Data Services OPC UA server—built into the *groov* RIO EMU 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 EMU: go to the Opto 22 website (www.opto22.com) and search for Video: OPC UA Quick Start Tutorial.
- For CODESYS users, the *groov* RIO EMU 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, remember to finish the following tasks:

- Upload server certificates from your MQTT server (broker) to your *groov* RIO EMU; for instructions, review "Managing Certificates on your groov RIO EMU" on page 39.
- Create a user account with Data Service OPC UA Server permissions; for instructions, review "Managing User Accounts" on page 23.

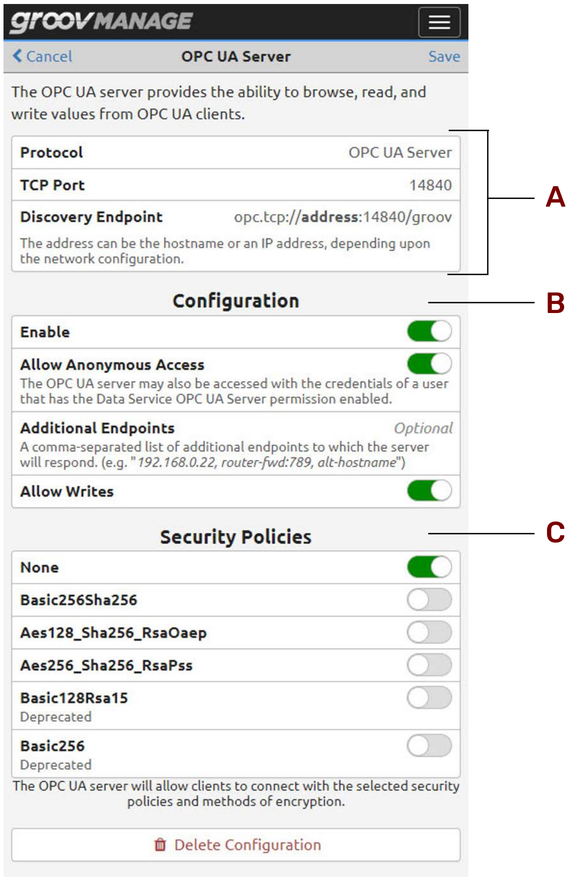
  While it's possible to use an account with System-wide Administrator permission, a security best practice would be to create a separate account with Data Service OPC UA Server permission.

- Create the scanned device; for instructions, review "Creating a Scanned Device" on page 52.

Completing the above tasks will make the following steps smoother.

1. Log into your *groov* RIO EMU with an account that has system administrator permissions.
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.



OPC UA Server

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 — On

Allow Anonymous Access — On
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-fwd:789, alt-hostname*")

Allow Writes — On

Security Policies

None — On
Basic256Sha256 — Off
Aes128_Sha256_RsaOaep — Off
Aes256_Sha256_RsaPss — Off
Basic128Rsa15 — Off
Deprecated
Basic256 — Off
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 will add this URL, replacing **address** with one of the following:

- Hostname—The default hostname of your *groov* RIO EMU (review Chapter 3: Initializing a groov RIO EMU) or, if you changed it, the name you changed it to.
- IP address—The default IP address of *groov* RIO EMU 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 On. Then specify 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 Allow Anonymous Access. This 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 will respond. This is useful when the *groov* RIO EMU is divided from the rest of the network by a firewall router. For example, if the IP address assigned to the *groov* RIO EMU 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 EMU 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.

If you see a message highlighted in yellow with the title "Configuration Issues", that indicates you haven't created the scanned device. For instructions, review "Creating a Scanned Device" on page 52.

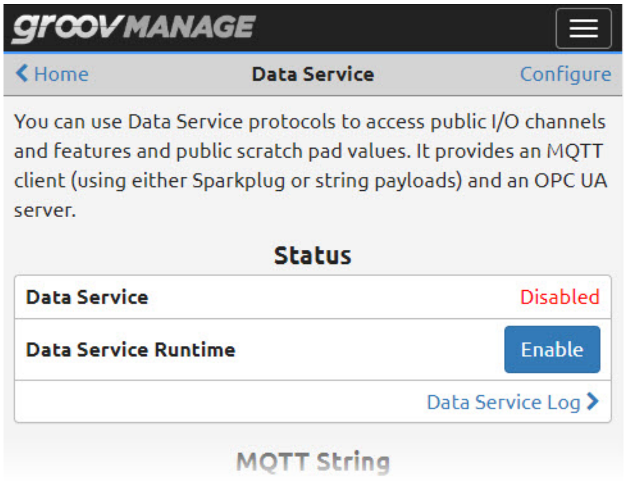
ENABLING DATA SERVICES AND TESTING CONNECTIONS

After you've configured either your Data Services MQTT client or the Data Services OPC UA server, enable Data Services and test your connection:

1. Log into your *groov* RIO EMU with an account that has system administrator permissions.

2. Click Data Service > Configure.

3. In the Status section at the top of the Data Service page, click Enable.



You can use Data Service protocols to access public I/O channels and features and public scratch pad values. It provides an MQTT client (using either Sparkplug or string payloads) and an OPC UA server.

Status

Data Service	Disabled
Data Service Runtime	Enable
	Data Service Log >

MQTT String

After you click Enable:

MQTT—Begins to publish topics.

OPC UA—*groov* Manage configures and opens the port in the firewall through which the OPC UA client will communicate with the Data Services OPC UA server. You can verify this by checking the Firewall page.

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 EMU. 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 "Configuring and Enabling the Data Services OPC UA Server" on page 61 when you configure the OPC UA client.)

If you observe any issues, here are a few suggestions of items to check:

- **Network issues**—Check whether you can ping the server or the client. Check settings like port numbers and whether the firewall is open. *groov* RIO EMU provides several tools to check for some network issues in the Network pages (from the *groov* Manage Home page, click on Network). Also consult with any troubleshooting tools available through your OPC UA client tools.
- **Application issues**—Check that the data is exposed (that you enabled public access); review "Exposing Data (Public Access)" on page 50.

7: Configuring *groov* RIO EMU Module and Channels

SELECTING A METHOD FOR CONFIGURING THE MODULE AND CHANNELS

There are several ways to configure a *groov* RIO EMU module and its channels:

- ***groov* Manage:** If you are using your *groov* RIO EMU as an edge node, where you'll just be transmitting tags to a cloud service (for example, through MQTT, OPC UA, or a Node-RED flow), you'll want to configure the module and the channels through *groov* Manage. The rest of this chapter describes how to do this.
- **PAC Control:** If you are adding your *groov* RIO EMU 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 *groov* RIO EMU as a remote I/O unit to a CODESYS application. The instructions in this chapter do not apply to CODESYS Development System.
- **OptoMMP:** To learn the memory map locations used for I/O configuration, review the OptoMMP Protocol Guide (form 1465).

Important: *Do* ***not*** *combine these methods. Any configuration you make through one method can overwrite configurations made through another method.*

CONFIGURING A *groov* RIO EMU MODULE THROUGH *groov* MANAGE

Remember to do the steps in this section only if you are ***not*** *configuring the module and channels through PAC Control, CODESYS, or OptoMMP.*

The *groov* RIO EMU comes ready to measure 3-phase, 0-500 VAC electrical loads, though it can be customized for other electrical loads:

- Loads with only 1- or 2-phases
- Loads with higher voltages, with the addition of a potential transformer (PT)

Specifying the Type of Current Transformer and Load Connected to the CT

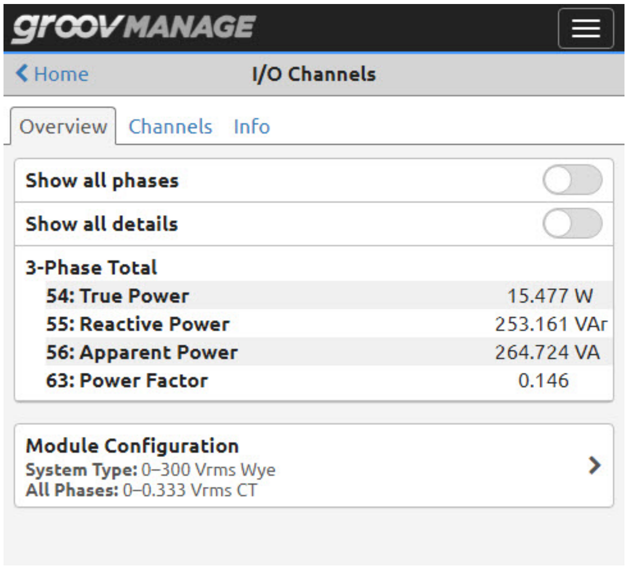
Make sure you know the following about the installed CTs:

- Primary current of each phase CT (if more than 1 phase)
- Secondary or output signal type
- Secondary or output signal range

If you are using a potential transformer, make sure to know its turns ratio.

When you have this information, you can configure the module:

1. Log into your *groov* RIO EMU with a user ID that has system administrator permission.
2. From the *groov* Manage Home page, click I/O. The I/O Channels page displays the current values for power totals and provides access to the module and channel configuration pages.



Show all phases ○

Show all details ○

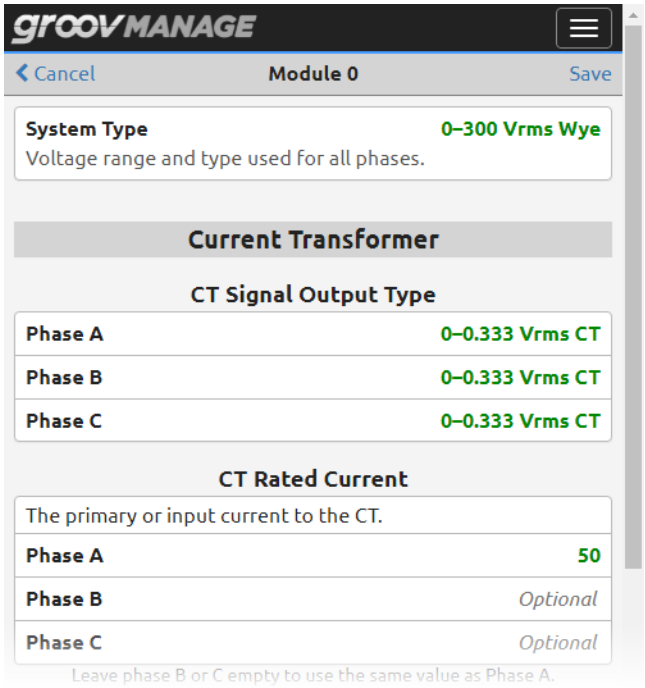
3-Phase Total

54: True Power	15.477 W
55: Reactive Power	253.161 VAr
56: Apparent Power	264.724 VA
63: Power Factor	0.146

Module Configuration
System Type: 0–300 Vrms Wye
All Phases: 0–0.333 Vrms CT

The numbers at the beginning of each row under the 3-Phase Total heading correspond to channel numbers. Notice the jump from 56 to 63. The channels between these two numbers (57 through 62) are energy values (review "Channel Specifications" on page 95). To displays these channels, toggle the Show all details switch.

3. Click the link on the right side of the Module Configuration section. *groov* Manage displays the Module 0 page. The page is very long and the following diagram displays only the top third.



System Type — 0–300 Vrms Wye
Voltage range and type used for all phases.

Current Transformer

CT Signal Output Type

Phase A	0–0.333 Vrms CT
Phase B	0–0.333 Vrms CT
Phase C	0–0.333 Vrms CT

CT Rated Current

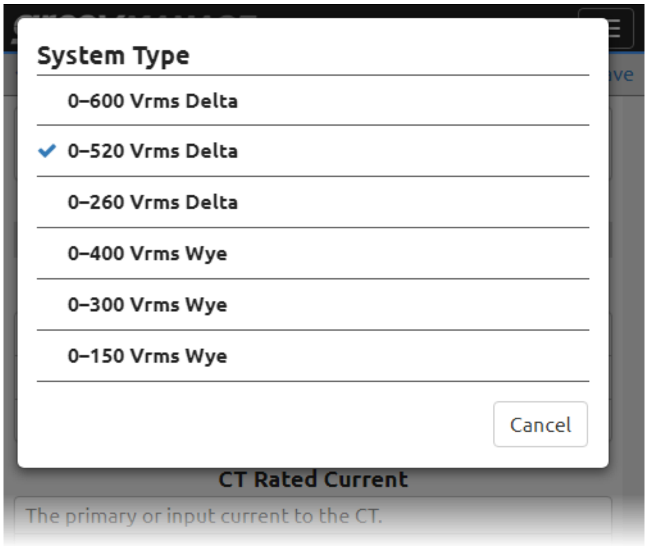
The primary or input current to the CT.

Phase A	50
Phase B	*Optional*
Phase C	*Optional*

Leave phase B or C empty to use the same value as Phase A.

4. Click System Type. Select the System Type that best describes the maximum RMS voltage (V_{rms}) and wiring type of the electrical load.
   - For a Delta circuit, choose a Delta option with the smallest V_{rms} range that is greater than the nominal line-to-line V_{rms} on the electrical load.
   - For a Wye circuit, choose a Wye option with the smallest V_{rms} range that is greater than the nominal line-to-neutral V_{rms} on the electrical load.

   For example, if the module is connected to a three-phase three-wire 480 VAC Delta circuit, choose the 0-520 V_{rms} Delta option.



System Type

- 0–600 Vrms Delta
- ✓ 0–520 Vrms Delta
- 0–260 Vrms Delta
- 0–400 Vrms Wye
- 0–300 Vrms Wye
- 0–150 Vrms Wye

Cancel

CT Rated Current

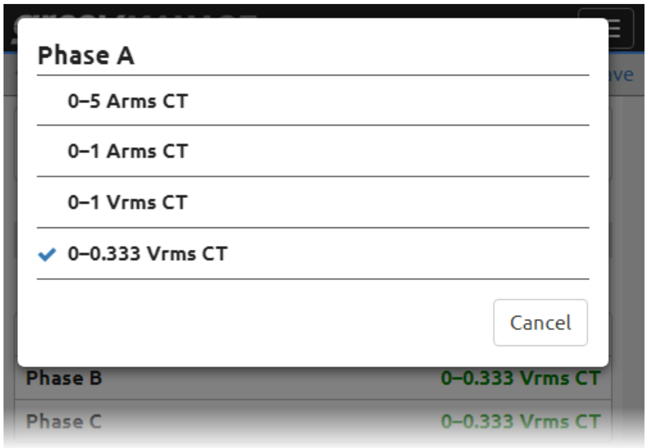
The primary or input current to the CT.

Note: *This field helps groov RIO EMU correctly interpret input values and calculate data values. Selecting the wrong voltage range will not damage the module.*

5. Set the output signal type of the CT and its current rating.

   a. In the CT Signal Output Type section, click the Phase A field. Select the value that corresponds to the CT connected to the module.

   If all phases are using the same CTs, you only have to fill out the Phase A fields; groov Manage will automatically duplicate those values to the Phase B and Phase C fields.



Phase A

- 0–5 Arms CT
- 0–1 Arms CT
- 0–1 Vrms CT
- ✓ 0–0.333 Vrms CT

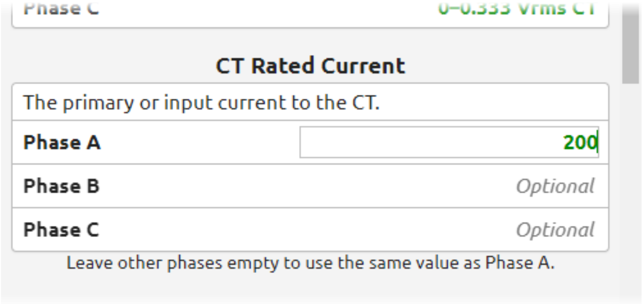
Cancel

Phase B 0–0.333 Vrms CT

Phase C 0–0.333 Vrms CT

   b. In the CT Rated Current section, click the Phase A field. Enter the current rating (maximum scale) for the primary input to the CT, in amps.

For example, if the CT's primary input is 0-200 A with a 0-5 A secondary, when the secondary is at 5 A_{rms}, the primary is measuring 200 A_{rms}, so you would type in 200.



Phase C	0–0.333 Vrms CT

CT Rated Current

The primary or input current to the CT.	
Phase A	200
Phase B	*Optional*
Phase C	*Optional*

Leave other phases empty to use the same value as Phase A.

If all three phases have the same CTs and primary input currents, click Save. You'll see data right away in *groov* Manage.

If the other two phases have different CTs and primary input currents, repeat steps a and b, specifying the corresponding values for each phase.

If you don't need to measure any of the other phases, see "Turning Off Unused Phases" on page 69.

Configuring *groov* RIO EMU Module for Loads Larger than 600 V

Potential transformers (PT) can help drop the voltage output of an electrical load to a level that a current transformer can handle. If a PT is connected to the CT, you need to factor in this drop when you configure the *groov* RIO EMU module so that *groov* Manage displays the correct values.

After you add the information about the electrical load and the CT (see "Specifying the Type of Current Transformer and Load Connected to the CT" on page 65), add the PT information in the Potential Transformer section of the I/O Channels page. Specifically, enter the turns ratio for the potential transformer for each phase. The turns ratio should be calculated as follows:

$$\frac{\texttt{Number of Turns in Primary Winding}}{\texttt{Number of Turns in Secondary Winding}}$$

If a phase does not have a potential transformer, enter 1.0. Remember to click Save to save this configuration.

Setting Current and Voltage Thresholds

Thresholds can help you manage calculations by ignoring values that aren't relevant to your calculations, like overnight values when your energy consumption is at its lowest. Specify threshold values as follows:

- **Minimum current threshold** is the minimum current below which all input values for a phase (except voltage and energy totals) are set to 0.
- **Minimum voltage threshold ratio** is the minimum voltage below which all input values for a phase (except energy totals) are set to 0. Specify this value as a fraction of the full-scale voltage specified in the System Type field.

  For example, if System Type is set to 0-250 V_{rms} Delta, and you specify a minimum threshold voltage ratio of 0.05, input values for this phase will be set to 0 when the voltage measured drops below (520*0.05) = 26 V_{rms}.

1. Log into your *groov* RIO EMU with a user ID that has system administrator permission.
2. From the *groov* Manage Home page, click I/O, then click on Module Configurations.
3. Scroll down to the Advanced Settings section:

- **To set the current threshold,** scroll to the Minimum Current Threshold (A) section. Enter a value in units of RMS amps (A_{rms}). Enter 0.0 (the default) to indicate that the module should use a default minimum current threshold. You cannot set a threshold value lower than the default value implemented by the module.
- **To set the voltage threshold,** scroll to the Minimum Voltage Threshold Ratio section. Enter a value as a fraction of the full-scale voltage specified in the System Type field. Enter 0.0 (the default) to indicate that the module should use a default minimum voltage threshold ratio value. You can not set a minimum threshold value lower than the default value implemented by the module.

  To set all input values for this phase to zero regardless of the measured voltage, set this value to 1.0. (This is also how you turn off a phase, as described in the next section.)

Turning Off Unused Phases

Setting input values on a phase to zero (effectively turning off the measurement of a phase) helps simplify the display of information in *groov* Manage so that you only see values for phases you are measuring:

1. Log into your *groov* RIO EMU with a user ID that has system administrator permission.
2. From the *groov* Manage Home page, click I/O, then click on Module Configurations.
3. Scroll down to the Advanced Settings section, then look for the Minimum Voltage Threshold Ratio section.
4. For each phase that you aren’t using, enter 1.0 in its corresponding field.
5. Click Save.

Customizing a Channel

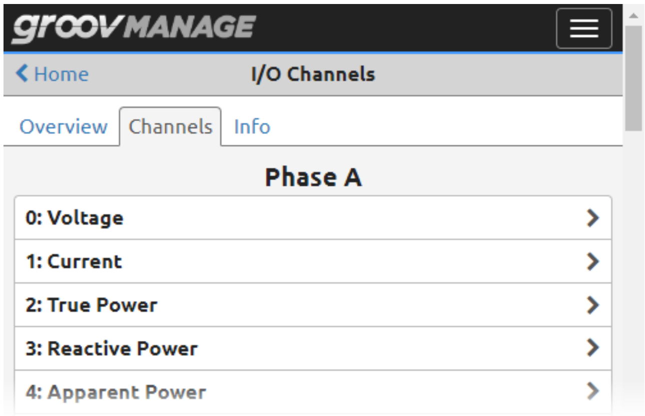
For each channel, you can:

- Assign a unique name. This name can help you identify a channel while viewing it in *groov* Manage, and:
  - If you are using *groov* View, it’s the name you see when you browse through tags on the *groov* RIO EMU.
  - If you are using Data Services, it uses this name to create the tag name. If you don’t assign this channel a name, Data Services creates a generic name.
- Toggle whether *groov* Manage should display quality indicators.
- Customize the scaling to represent different values and units of measure.
- Configure access to the channel tags by third party services like MQTT or Node-RED.

If you don’t need to customize any of these settings, you can skip this section.

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

2. From the *groov* Manage Home page, click I/O, then the Channels tab. *groov* Manage displays the I/O Channels page, which lists all 64 channels divided into four sections: Phase A, Phase B, Phase C, and Totals. This page is long; the image on the following page shows only the first few channels.

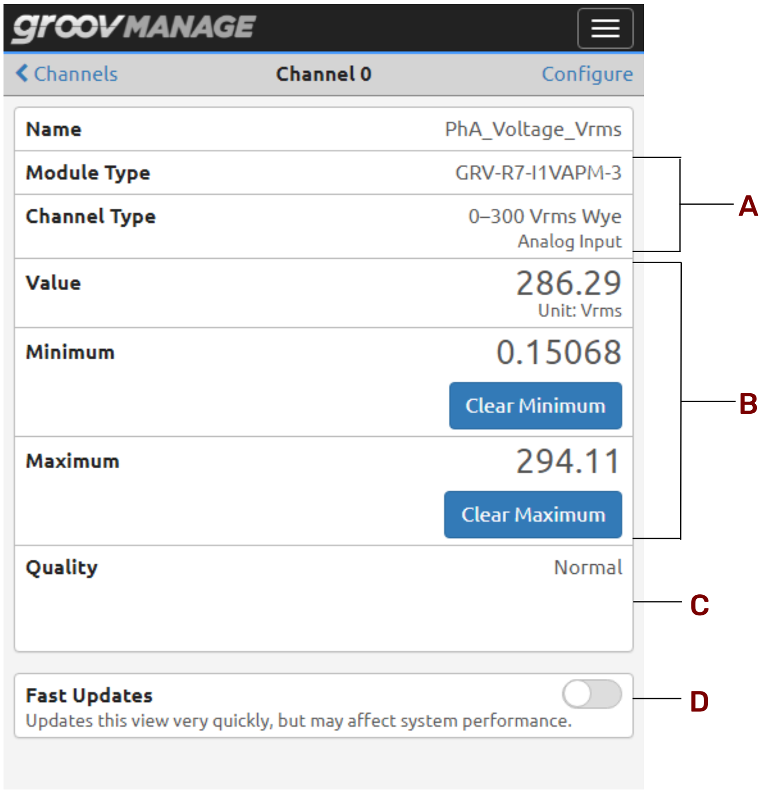


Phase A

0: Voltage
1: Current
2: True Power
3: Reactive Power
4: Apparent Power

From this page, you can get to any channel's status and configuration page.

3. Click the channel you want to modify. *groov* Manage displays the channel status page.



Name	PhA_Voltage_Vrms
Module Type	GRV-R7-I1VAPM-3
Channel Type	0–300 Vrms Wye Analog Input
Value	286.29 Unit: Vrms
Minimum	0.15068
Maximum	294.11
Quality	Normal

Fast Updates
Updates this view very quickly, but may affect system performance.

A *groov* Manage displays Module Type and Channel Type for your reference. (You configured these values in "Specifying the Type of Current Transformer and Load Connected to the CT" on page 65.)

B *groov* Manage displays the following measurements in real-time:

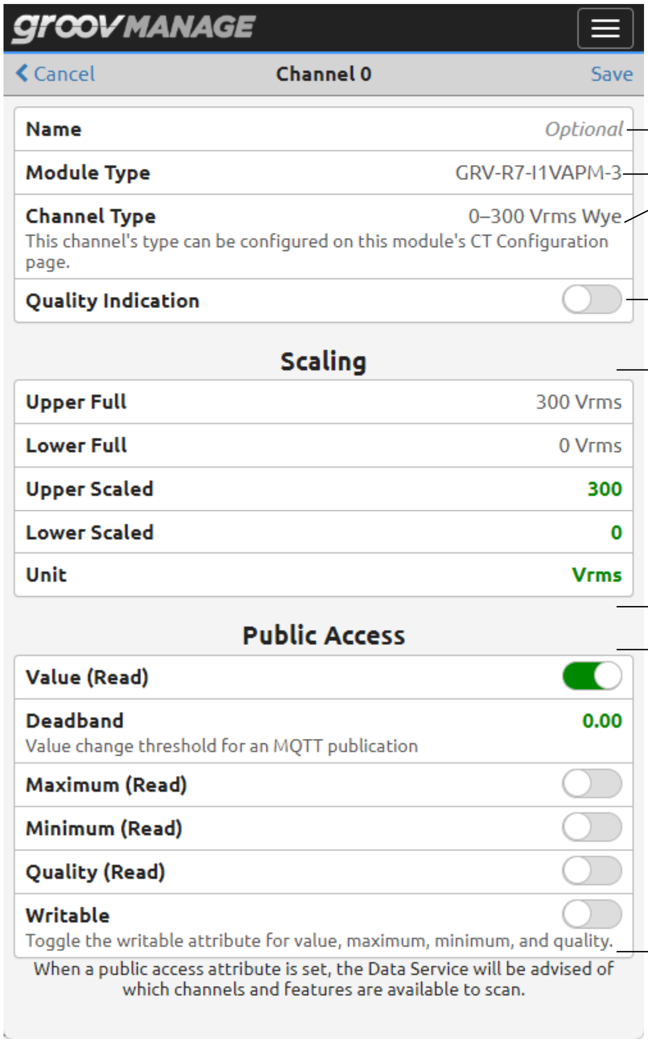
- **Value:** The current value measured or calculated for the channel.
- **Minimum:** The smallest value recorded since the last time this field was cleared. (To clear this value, click Clear Minimum.)

- **Maximum:** The largest value recorded since the last time this field was cleared. (To clear this value, click Clear Maximum.)

C If there any quality issues, *groov* Manage displays them in the Quality field. (For more information, see "Understanding How groov Manage Displays Quality Codes" on page 73.)

D *groov* Manage updates the information on this page several times a second; you can increase this rate by enabling the **Fast Updates** toggle. Afterwards, the information on this page is updated more frequently, though this may affect performance.

4. Click Configure in the top right corner. *groov* Manage displays the channel configuration page.



Name	*Optional*
Module Type	GRV-R7-I1VAPM-3
Channel Type This channel's type can be configured on this module's CT Configuration page.	0–300 Vrms Wye
Quality Indication	○

Scaling

Upper Full	300 Vrms
Lower Full	0 Vrms
Upper Scaled	300
Lower Scaled	0
Unit	Vrms

Public Access

Value (Read)	●
Deadband Value change threshold for an MQTT publication	0.00
Maximum (Read)	○
Minimum (Read)	○
Quality (Read)	○
Writable Toggle the writable attribute for value, maximum, minimum, and quality.	○

When a public access attribute is set, the Data Service will be advised of which channels and features are available to scan.

For your information.

To change channel type, review "Specifying the Type of Current Transformer and Load Connected to the CT" on page 65.

You can modify the following settings:

A **Name**—Text that uniquely identifies this channel; it can be up to 50 characters long and include symbols or spaces. *groov* Manage displays this name on the channels page and saves it when you backup your *groov* RIO EMU settings.

If you are using Data Services, remember the following when you create a name:

- You can use spaces but not tabs.
- Limit your use of symbols to underscores and hyphens. Other characters may have special meaning in some protocols.

For information about where this name is used, see the description of assigning unique names on page 69.

B **Quality Indication**—If you want *groov* Manage to report quality indicators, toggle this switch on. For more information, see "Understanding How groov Manage Displays Quality Codes" on page 73.

C **Scaling**—In the Scaling section, you can assign a custom range of values and unit of measure of the channel to represent the "real world" range of values and unit of measure of the electrical load. For example, if your electrical load is an oven that measure 0 to 200 degrees Fahrenheit, you can scale the readings of a 0 to 300 VAC input channel to display:

- the value 0 degrees Fahrenheit for 0 VAC, and
- the value 200 degrees Fahrenheit for 300 VAC.

A voltage, current, or power value typically has a small variation in accuracy (described in the specification table), which means you want to take the accuracy into account when you specify the scaling values. For example, if you select 0 to 300 V_{rms} Wye as the channel type (which means the input could be anything between 0 to 300 V_{rms}), the specification table indicates that the accuracy of any value can range between +/- 0.35%. That means that if the channel reads a value of 200 V_{rms}, it could actually be between 199.3 and 200.7 V_{rms}. Check the specification table to determine the accuracy ranges for your channel type.

D **Public Access**—Indicate which tags (created by this channel) to make available to services like MQTT and Node-RED.

- **Value**, **Maximum (Read)**, **Minimum (Read)**, and **Quality (Read)**: Toggle these switches on to make their respective tags available. For a description of these tags, see page 70.
- **Deadband:** Specifies how much the value measured must deviate before the Data Service publishes a topic. The deviation is specified as a float, even if the value measured is an integer.
- **Writable:** Toggle this switch on to allow services to write values to this channel.

Changing Some Settings on All Channels at Once

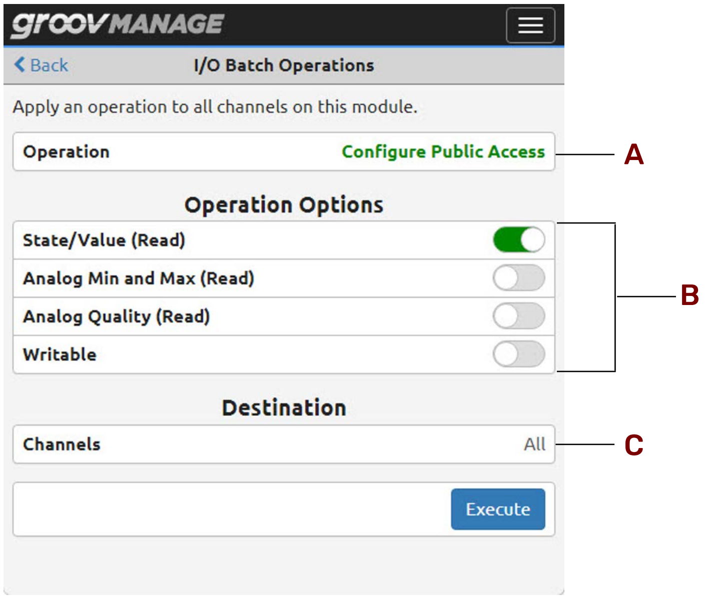
To save you time, you can change the following settings on all channels with just a few clicks, instead of having to edit each individual channel:

- Configure public access so that third party applications (like MQTT, Node-RED, or *groov* View) can:
  - Read state/value; analog minimum, maximum, or both; and quality codes.
  - Write values to the channel.
- Clear the minimum, the maximum, or both.

To change these settings on all channels:

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

2. From the *groov* Manage Home page, click I/O > I/O Services, then I/O Batch Operations.



groov MANAGE

Back — I/O Batch Operations

Apply an operation to all channels on this module.

Operation: Configure Public Access

Operation Options

- State/Value (Read) — on
- Analog Min and Max (Read) — off
- Analog Quality (Read) — off
- Writable — off

Destination

Channels: All

A **Operation**—Select the change you want to make to all channels on the module:

- **Configure Public Access**—Set certain tag values as readable or writable by third party applications like Node-RED or MQTT.
- **Clear Analog Min/Max**—Clear the minimum or maximum analog value stored.

B **Operation Options**—Toggle an option to enable or disable it. The list in this section changes based on what you selected for the Operation field:

Configure Public Access	Clear Analog Min/Max
State/Value (Read)	Clear Minimum
Analog Min and Max (Read)	Clear Maximum
Analog Quality (Read)	
Writable	

C **Destination**—Displays which channels will change when you click Execute. You can't change this field.

3. Click Execute.

UNDERSTANDING HOW *groov* MANAGE DISPLAYS QUALITY CODES

Some channels on the *groov* RIO EMU module can report quality codes, which may indicate common errors like input values that are out of range. *groov* Manage visually indicates when a channel reports a quality code:

- **In the Channels tab.** *groov* Manage highlights the channel (by changing the background to yellow) and displays a short message about the quality code.
- **In the Channel's status page.** The Quality field displays a brief message about the quality code and the quality code number.

The *groov* RIO EMU module reports the following quality codes:

- **5**, analog input (V_{rms}, I_{rms}, and true power) above operating limits. ADC Register overflow.
- **15**, analog input (V_{rms} and I_{rms}) above 110% of range.

8: Maintaining a *groov* RIO EMU

Maintain your *groov* RIO EMUs 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 EMU, 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 processor to factory defaults, you can restore the information that you backed up.

BACKING UP YOUR *groov* RIO EMU SETTINGS

Recommendations vary regarding when and how often you should back up your *groov* RIO EMU:

- 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 EMU 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 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).

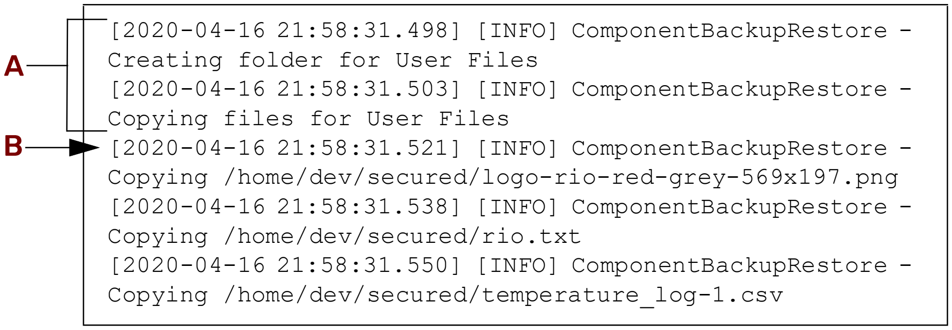
  This also includes sensitive information like the WiFi SSID and pre-shared key, and the OpenVPN server login credentials. If you enable this setting and do not enable encryption by *groov* Manage (review step 4), it's important that you apply your own security or encryption to the backup file to protect 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 EMU that is replacing another *groov* RIO EMU 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 EMU running firmware earlier than version 3.2.0.
   - You ***can*** restore this backup file to any *groov* RIO EMU 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:



```
[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
[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 processor 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 EMU 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 EMU.
- If you selected to have *groov* Manage encrypt the file, you cannot use that file to restore settings to a *groov* RIO EMU running firmware earlier than version 3.2.0.

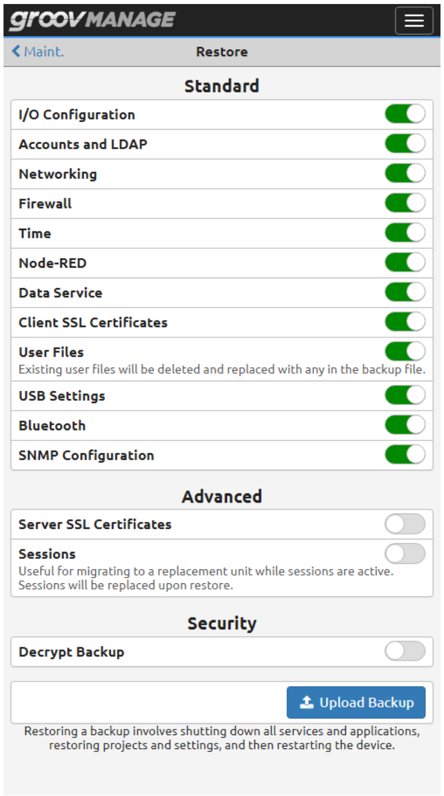
To restore a backup file or specific part of a backup file:

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 EMU 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 EMU firmware.*



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

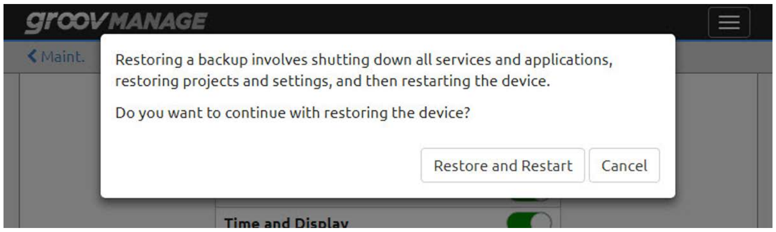
Server SSL Certificates	○
Sessions Useful for migrating to a replacement unit while sessions are active. Sessions will be replaced upon restore.	○

Security

Decrypt Backup	○

Restoring a backup involves shutting down all services and applications, restoring projects and settings, and then restarting the device.

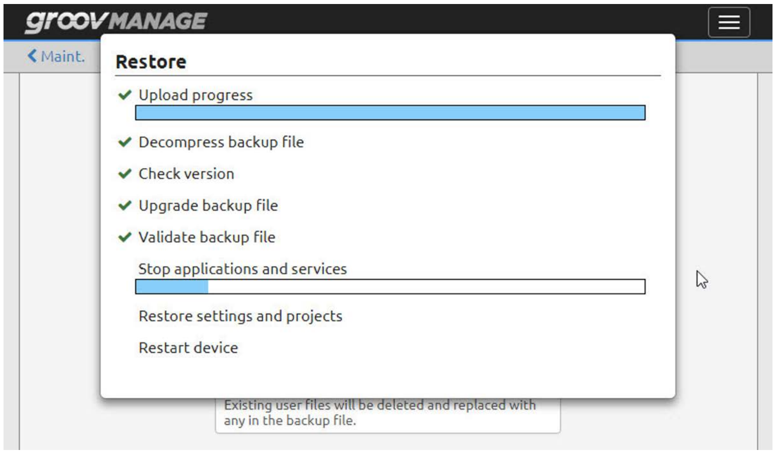
5. Click Upload Backup.
6. Navigate to the folder or media device that contains your backup file.
7. Click Open. *groov* Manage displays the following message, reminding you of what the *groov* RIO EMU will do during the restoration:



Restoring a backup involves shutting down all services and applications, restoring projects and settings, and then restarting the device.

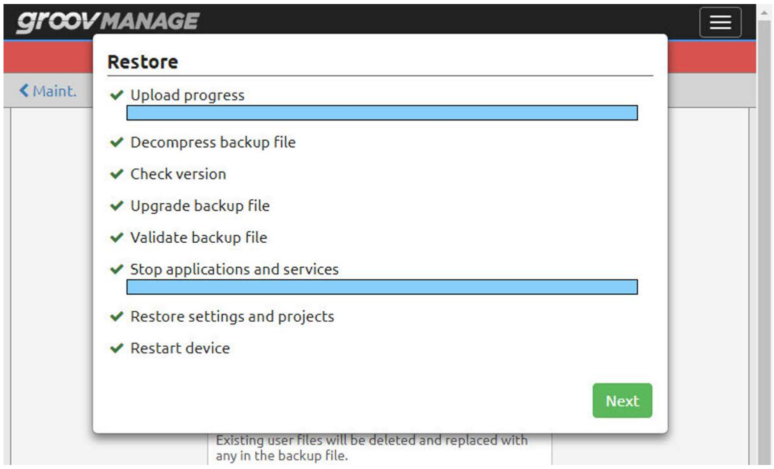
Do you want to continue with restoring the device?

8. Click Restore and Restart. *groov* Manage displays a window that shows the progress of the restoration:



Existing user files will be deleted and replaced with any in the backup file.

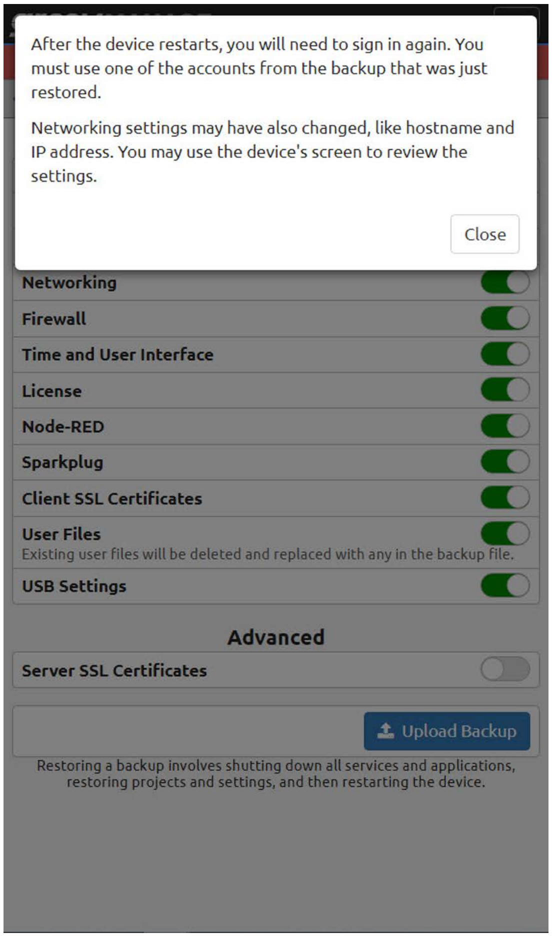
9. When *groov* Manage finishes restoring setting, the window looks like the following:



Existing user files will be deleted and replaced with any in the backup file.

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.



After the device restarts, you will need to sign in again. You must use one of the accounts from the backup that was just restored.

Networking settings may have also changed, like hostname and IP address. You may use the device's screen to review the settings.

Networking ●
Firewall ●
Time and User Interface ●
License ●
Node-RED ●
Sparkplug ●
Client SSL Certificates ●
User Files ●
Existing user files will be deleted and replaced with any in the backup file.
USB Settings ●

Advanced

Server SSL Certificates ○

Restoring a backup involves shutting down all services and applications, restoring projects and settings, and then restarting the device.

11. The *groov* RIO EMU restarts. Wait for the *groov* RIO EMU 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 EMU

Updating firmware on a *groov* RIO EMU keeps it up-to-date with the latest features and fixes. Updating firmware can take 20-30 minutes to complete and your *groov* RIO EMU 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 EMUs daisy-chained together, if you update the firmware on one *groov* RIO EMU, you must update the firmware on all the *groov* RIO EMUs 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 EMU Settings" on page 75). 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 EMU Settings" on page 75.*

2. Go to the Opto 22 website (opto22.com) and enter the part number for your *groov* RIO EMU in the Search box. Select the search result that includes "Firmware" as part of the title; for example GRV-R7-I1VAPM-3 Firmware.

3. Click Download. Save the file to either:

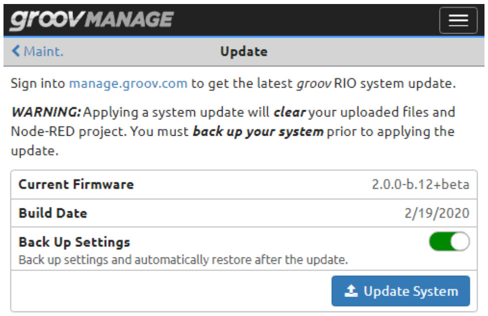
- A computer or mobile device that can connect to your *groov* RIO EMU, or
- Media that you can then install to a computer or mobile device that can connect to your *groov* RIO EMU.

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 EMU 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:



Sign into manage.groov.com to get the latest *groov* RIO system update.

WARNING: Applying a system update will ***clear*** your uploaded files and Node-RED project. You must ***back up your system*** prior to applying the update.

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.	●

- If you leave the Back Up Settings switch on (the default), then all settings are saved before the firmware is upgraded. The *groov* RIO EMU 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.

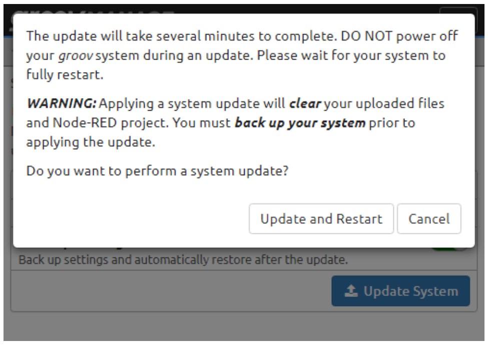
- If you *do not* want the settings saved then restored, click the switch so that it shows gray (○). Turn this setting off if you want to restore your *groov* RIO EMU with settings from a different backup file; for example, the one you created in step 1.

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.



The update will take several minutes to complete. DO NOT power off your *groov* system during an update. Please wait for your system to fully restart.

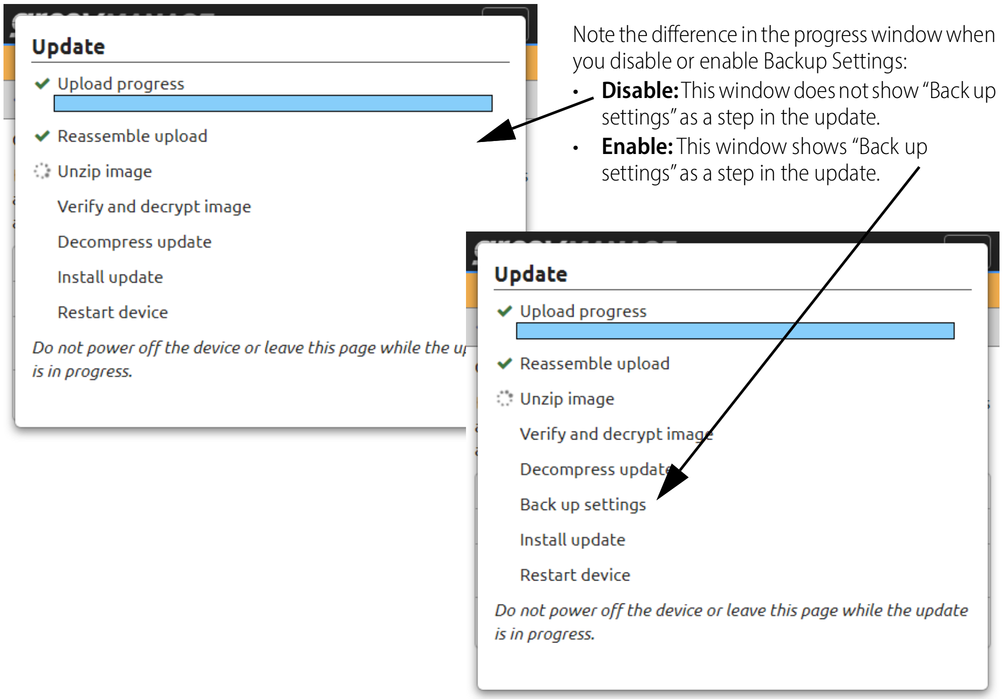
WARNING: Applying a system update will ***clear*** your uploaded files and Node-RED project. You must ***back up your system*** prior to applying the update.

Do you want to perform a system update?

Update and Restart
Cancel
Back up settings and automatically restore after the update.
Update System

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.



Update

- ✓ Upload progress
- ✓ Reassemble upload
- Unzip image
- Verify and decrypt image
- Decompress update
- Install update
- Restart device

Do not power off the device or leave this page while the up is in progress.

Update

- ✓ Upload progress
- ✓ Reassemble upload
- Unzip image
- Verify and decrypt image
- Decompress update
- Back up settings
- Install update
- Restart device

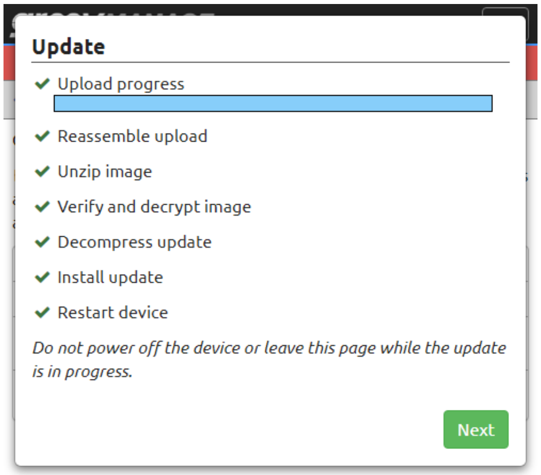
Do not power off the device or leave this page while the update is in progress.

Note the difference in the progress window when you disable or enable Backup Settings:

- **Disable:** This window does not show "Back up settings" as a step in the update.
- **Enable:** This window shows "Back up settings" as a step in the update.

Watch for the banner to turn red, which indicates that the update is finished and that your *groov* RIO EMU is now offline.

11. After a successful install, the Update windows shows all items as checked off and displays the Next button. Click Next.



Update

✓ Upload progress

✓ Reassemble upload

✓ Unzip image

✓ Verify and decrypt image

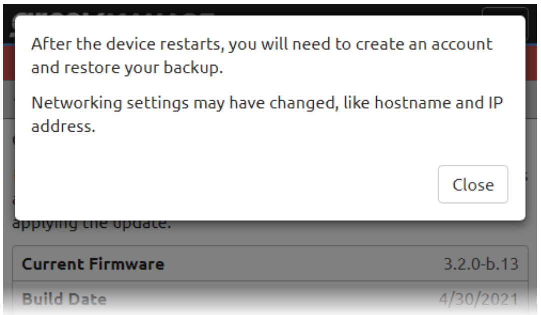
✓ Decompress update

✓ Install update

✓ Restart device

Do not power off the device or leave this page while the update is in progress.

12. Read the instructions on what to do after the *groov* RIO EMU restarts, and then click Close.



After the device restarts, you will need to create an account and restore your backup.

Networking settings may have changed, like hostname and IP address.

applying the update.

Current Firmware 3.2.0-b.13

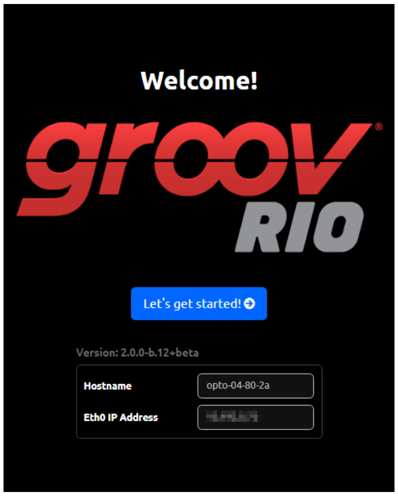
Build Date 4/30/2021

13. If you can see the *groov* RIO EMU, 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.

Welcome screen

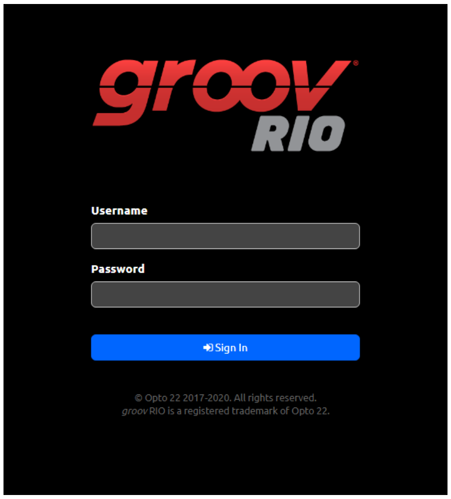


Version: 2.0.0-b.12+beta

Hostname: opto-04-80-2a

Eth0 IP Address: [redacted]

Login screen


groov RIO
Username
Password
Sign In
© Opto 22 2017-2020. All rights reserved.
groov RIO is a registered trademark of Opto 22.

If you see the Welcome! screen (you'll see this screen if you **de**selected the Back Up Settings option in step 6 on page 81):

a. Make a note of the IP address shown in the Eth0 IP Address box. You'll need it in the next few steps.

b. 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.)

c. Click on Configure Device.

d. 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 77).

If you see the login screen (you'll see this screen if you enabled the Back Up Settings option in step 6 on page 81), 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 EMU (review "Downloading and Running groov Find" on page 85).

TROUBLESHOOTING

Browser Reports that URL to *groov* RIO EMU is Unreachable

There are several reasons that a browser may report that it cannot connect to your *groov* RIO EMU 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 EMU'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 EMU. (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 EMU 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.

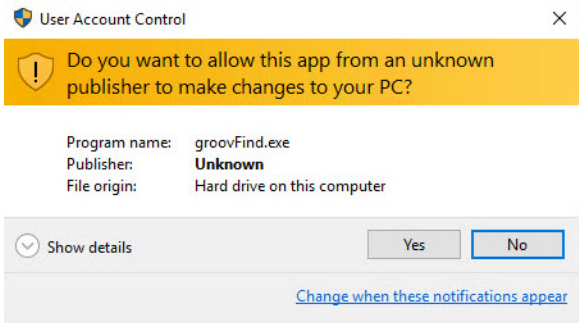
Downloading and Running *groov* Find

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). Save the file to your computer.
2. 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.

   User Account Control

   Do you want to allow this app from an unknown publisher to make changes to your PC?

   Program name: groovFind.exe
   Publisher: **Unknown**
   File origin: Hard drive on this computer

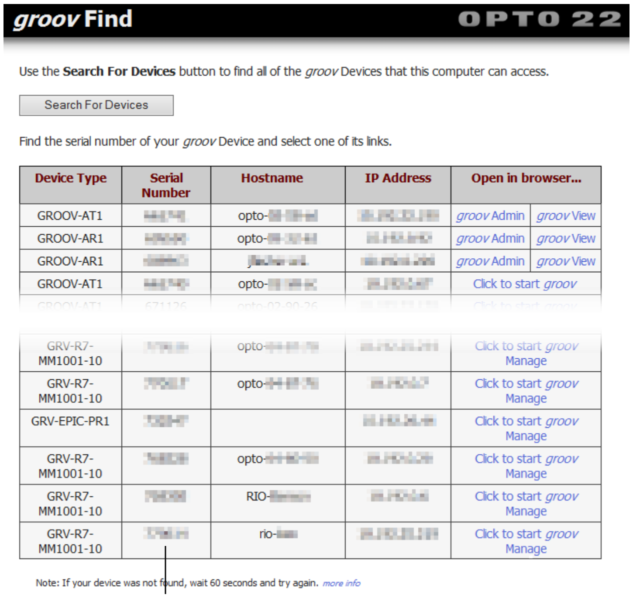
   NOTE 1: *If you are using a Windows account that does not have Administrator privileges (such as Guest), you will need to enter the Administrator User Name and Password in order to use groov Find. If you do not have this information, contact your IT department.*

   NOTE 2: *Clicking Yes permits Find to have temporary administrative privileges to create an additional temporary IP address for each network interface on the computer. This enables 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 will need to assign a static IP address to the groov device in order to maintain communication. If the network does have DNS and DHCP, the temporary IP address is not used and is removed when you exit Find.*

3. Click Yes.

   groov Find opens and automatically searches for *groov* RIOs, *groov* EPICs, and *groov* Boxes on the network.
4. 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.

5. Locate the matching serial number in Find.



Use the **Search For Devices** button to find all of the *groov* Devices that this computer can access.

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	[redacted]	opto-[redacted]	[redacted]	*groov* Admin *groov* View
GROOV-AR1	[redacted]	opto-[redacted]	[redacted]	*groov* Admin *groov* View
GROOV-AR1	[redacted]	[redacted]	[redacted]	*groov* Admin *groov* View
GROOV-AT1	[redacted]	opto-[redacted]	[redacted]	Click to start *groov*
GROOV-AT1	671126	opto-02-90-26	[redacted]	Click to start *groov*
GRV-R7-MM1001-10	[redacted]	opto-[redacted]	[redacted]	Click to start *groov* Manage
GRV-R7-MM1001-10	[redacted]	opto-[redacted]	[redacted]	Click to start *groov* Manage
GRV-EPIC-PR1	[redacted]		[redacted]	Click to start *groov* Manage
GRV-R7-MM1001-10	[redacted]	opto-[redacted]	[redacted]	Click to start *groov* Manage
GRV-R7-MM1001-10	[redacted]	RIO-[redacted]	[redacted]	Click to start *groov* Manage
GRV-R7-MM1001-10	[redacted]	rio-[redacted]	[redacted]	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, then click Search For Devices.

6. Click the link (in the right-most column) to start *groov* Manage.

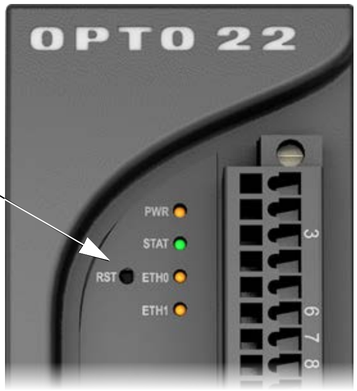
Instructions for Macs:

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 EMU, 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 on the apple menu (top left corner), then select App Store.
   - Click on Finder, then click Applications, then find 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 will open up with the *groov* device's IP address in the URL bar, and then load either *groov* View or *groov* Manage.

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 EMU, which is why it is important that you regularly back up your system. (For instructions, review "Backing up Your groov RIO EMU Settings" on page 75.)

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.


Insert paper clip into RST hole and hold it down for 8 seconds.

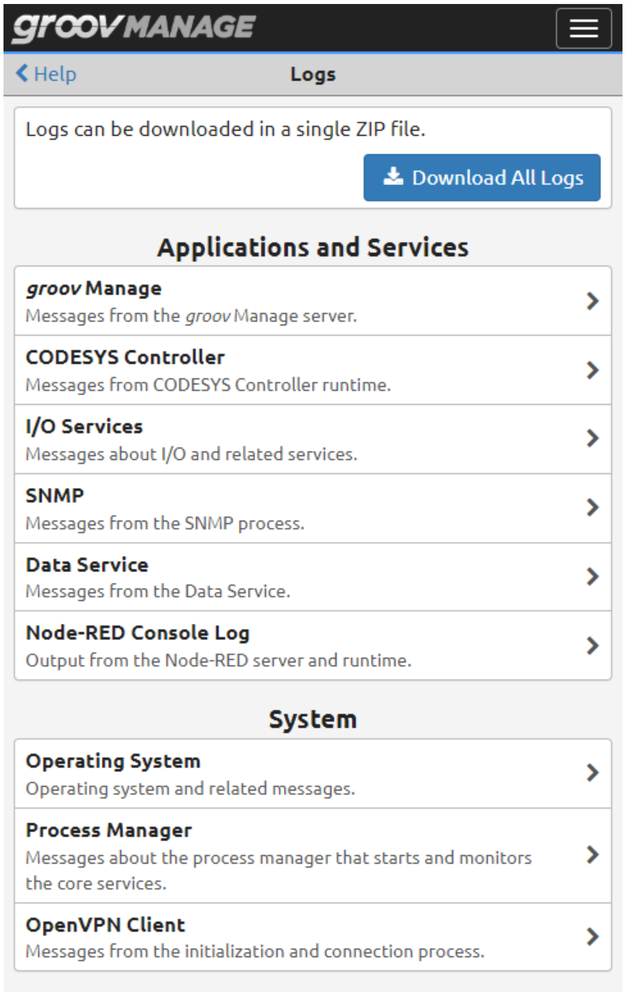
COLLECTING INFORMATION FOR PRODUCT SUPPORT

groov RIO EMU displays messages and collects information in several logs that can help Product Support diagnose and solve issues. If you contact Opto 22 to obtain 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 EMU with a user ID that has system administrator permission.
2. Click Info and Help > Logs. *groov* Manage displays the Logs page.



Logs can be downloaded in a single ZIP file.

Applications and Services

groov Manage
Messages from the *groov* Manage server.

CODESYS Controller
Messages from CODESYS Controller runtime.

I/O Services
Messages about I/O and related services.

SNMP
Messages from the SNMP process.

Data Service
Messages from the Data Service.

Node-RED Console Log
Output from the Node-RED server and runtime.

System

Operating System
Operating system and related messages.

Process Manager
Messages about the process manager that starts and monitors the core services.

OpenVPN Client
Messages from the initialization and connection process.

3. Download either the specific log file(s) (as directed 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.
6. If you are downloading individual logs, repeat steps 3 through 5 for each log that Product Support directs you to download.

If you need to collect information from a screen, you can use the screen capture feature on the computer or mobile device to save (capture) the screens.

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 OptoSupport team member to remotely connect to your *groov* RIO EMU to continue with diagnostics and troubleshooting.

After evaluating the progress of your ticket, your Opto 22 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 EMU by checking the following:

- Verify that your *groov* RIO EMU has an internet connection.
- Verify that, if your internet connection travels through a firewall or router, that the firewall or router does not prevent outbound connections through port 555.

An RSS session typically runs like this:

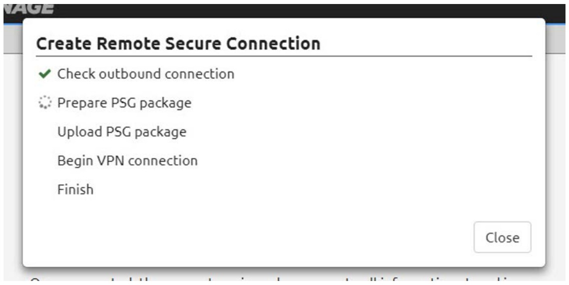
1. At a time agreed upon by you and your OptoSupport team member, you'll initiate a phone call.
2. When instructed, click Create RSC to initiate the session. For detailed instructions and an explanation of what happens during this step, review "Initiating an RSS Session" on page 89.
3. After the session is successfully created, you and your OptoSupport team member will review details of your situation and discuss additional steps. These steps might be:
   – Continue active discussion of the issue over the phone while the OptoSupport team member diagnosis and troubleshoots your *groov* RIO EMU.
   – Agree to a plan of action where you can end the phone call while the OptoSupport team member continues to diagnose and troubleshoot your *groov* RIO EMU.

   If the session is lengthy, part of the plan might include pausing the session and continuing it at a later time. For additional instructions on pausing and resuming a session, review "Pausing and Resuming an RSS Session" on page 90.
4. When it's time to end the RSS session, click Delete RSC. For important information on what happens when you end an RSS session, review "Ending the RSS Session" on page 91.

Initiating an RSS Session

1. The Opto 22 Support team member will ask 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 will ask 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.

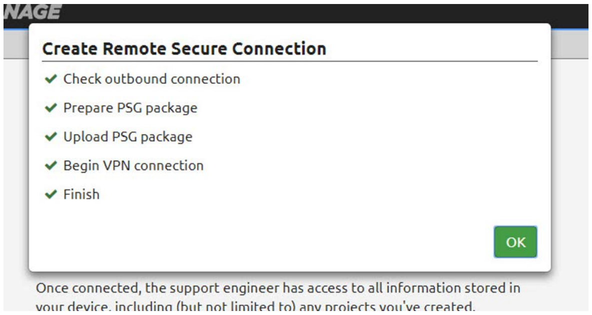
   The first thing you will see is the OptoSupport Remote Support Service Permission and Release Agreement. To proceed with the session, accept the terms of the agreement.
4. After you click Accept, *groov* Manage displays a message to report the steps to create the connection environment:



Create Remote Secure Connection

✓ Check outbound connection
Prepare PSG package
Upload PSG package
Begin VPN connection
Finish

5. When it finishes these steps, click OK to close the message box:



Create Remote Secure Connection

✓ Check outbound connection

✓ Prepare PSG package

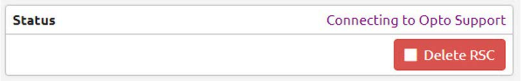
✓ Upload PSG package

✓ Begin VPN connection

✓ Finish

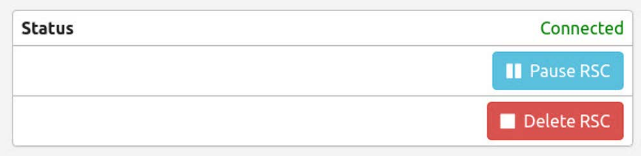
Once connected, the support engineer has access to all information stored in your device, including (but not limited to) any projects you've created.

6. While your *groov* RIO EMU establishes a connection, the Status section of the OptoSupport RSS page displays the following:



Status: Connecting to Opto Support

7. After the connection is established, the Status section of the OptoSupport RSS page displays the following:



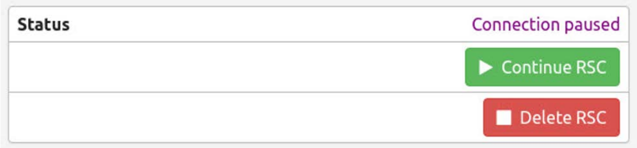
Status: Connected

Do not turn off your *groov* RIO EMU after you start the session. If this happens, you will need to restart this process.

Pausing and Resuming an RSS Session

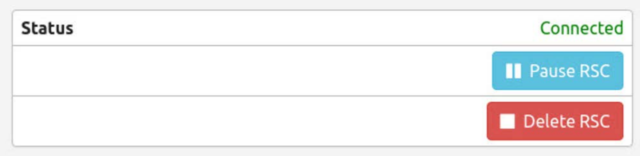
During the course of diagnosis and troubleshooting, you and your OptoSupport team member might agree to pause the session, then resume it at a later time. Pausing the session prevents communication between OptoSupport team member and your *groov* RIO EMU while preserving the information needed to quickly resume the connection.

- 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's 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 EMU created to establish the connection will be erased. If you need to start another RSS session, you'll need to start from the first step in "Initiating an RSS Session" on page 89.

A: Specifications

Specifications are listed on the next page.

GRV-R7-I1VAPM-3

Specification	GRV-R7-I1VAPM-3
Maximum UL61010-3 Measurement Category	Category III 600 VAC
Delta Voltage Input Ranges, V_{rms}	600, 520, 260 (Line-to-Line)
Wye Voltage Input Ranges, V_{rms}	400, 300, 150 (Line-to-Neutral; higher voltages require use of a potential transformer)
Voltage Accuracy (% of range @ 50-60 Hz, excluding voltage transformer)	Wye: ±0.35%, Delta: ±0.5%
Current Transformer (CT) Outputs Supported	5.0 A, 1.0 VAC or 0.3333 VAC
Current Accuracy (% of CT range @ 50-60 Hz, excluding current transformer)	±0.5%
Power Accuracy (% of (Vrms range) * (CT current rating), @ 50-60Hz)	±0.5%
Data Refresh Time	1 s
Step Response Time	1 s
Problem Indication	V_{rms} out of range, I_{rms} out of range
Number of Data Channels	64
Ethernet	Two switched Gigabit ports; daisy-chainable; ETH1 with 802.3af PoE powered device (PD)
USB	One Port, USB 2.0 HS
Memory	1 GB RAM, 4.0 GB disk space
Power Supply	802.3af PoE Class 0 ***or*** 10–32 V DC (but not both)
Power Consumption	4.5 W
Isolation (field to Ethernet / power input)	3600 VAC working, 5400 VAC transient
Isolation (channel-to-channel)	N/A
Minimum *groov* RIO Firmware Version	3.3.0
Minimum *groov* EPIC Firmware Version	3.3.0
Minimum PAC Project Version	10.4000
Minimum Library Package for CODESYS Version	2.0.4.0
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 °C to +70 °C
Temperature (storage)	-40 °C to +85 °C
Relative Humidity (non-condensing)	5–95%
MTBF (minimum, 25 °C)	1.2 Mhrs
Agency Approvals	UL/cUL(Class 1 Div. 2); CE, ATEX(Category 3, Zone 2), RoHS; DFARS; CB Scheme; UKCA
Warranty	30 months

CHANNEL SPECIFICATIONS

Ch	Phase	Description	Details
0	A	V_{rms}	Root-mean-square voltage for the phase in units of V_{rms}, measured relative to the neutral terminal, calculated once per second from 4000 samples. (Review equation to the right.) This value is always positive. This channel can be configured with one of the following channel types: • 0–600 V_{rms} delta • 0–520 V_{rms} delta • 0–260 V_{rms} delta • 0–400 V_{rms} wye • 0–300 V_{rms} wye • 0–150 V_{rms} wye For wye configurations, higher voltages are supported with the addition of a potential transformer. Review wiring diagram on page 101. $V_{rms} = \sqrt{\frac{\sum_{n=1}^{4000} (V^2)_n}{4000}}$
1	A	I_{rms}	Root-mean-square current for the phase in units of A_{rms}, calculated once per second from 4000 samples. (Review equation to the right.) This value is always positive. This channel can be configured with one of the following channel types: • 0–5 A_{rms} CT • 0–1 V_{rms} CT • 0–0.333 V_{rms} CT. $I_{rms} = \sqrt{\frac{\sum_{n=1}^{4000} (I^2)_n}{4000}}$
2	A	True Power	True (or real or active) power for the phase in units of W, calculated once per second from 4000 samples of instant power. (Review equation to the right.) This value can be positive or negative. $P = \frac{\sum_{n=1}^{4000} V_i \times I_i}{4000}$
3	A	Reactive Power	Reactive power for the phase in units of var. This value is calculated once per second from the square root of the apparent power squared minus the true power squared. (Reviewequation to the right.) This value is always positive. $Q = \sqrt{(S^2 - P^2)}$
4	A	Apparent Power	Apparent power for the phase in units of VA, calculated once per second from V_{rms} times I_{rms}. (Review equation to the right.) This value is always positive. $S = V_{rms} \times I_{rms}$
5	A	Power Factor	Ratio of true power to apparent power for the phase, calculated once per second. (Review equation to the right.) This ratio is always between -1.0 and 1.0. $\text{Power Factor} = \frac{P}{S}$
6	A	Peak Voltage	Instantaneous peak voltage over the last second for the phase in units of V. This value can be positive or negative.
7	A	Peak Current	Instantaneous peak current over the last second for the phase in units of A. This value can be positive or negative.
8	A	Frequency	AC line frequency for the phase in units of Hz. This value is updated once per second and is always positive.
9	A	True Power at Fundamental Frequency	True (or real or active) power at the fundamental frequency for the phase in units of W, calculated once per second from a discrete Fourier transform at the fundamental frequency on the voltage and current and multiplying the result. This value can be positive or negative.
10	A	Harmonic True Power	True (or real or active) power in the harmonics for the phase in units of W, calculated once per second by subtracting true power at the fundamental frequency from true power. This value can be positive or negative.

Ch	Phase	Description	Details
11	A	Reactive Power at Fundamental Frequency	Reactive power at the fundamental frequency for the phase in units of var, calculated once per second from a discrete Fourier transform at the fundamental frequency on the voltage and current and multiplying the result. This value can be positive or negative.
12	A	Average Reactive Power	Reactive power for the phase in units of var. This value is updated once per second from the average of 4000 samples of the product of the voltage, shifted 90 degrees, and the current. (Review equation to the right.) This value can be positive (due to a capacitive load) or negative (due to an inductive load). $Q_{avg} = \frac{\sum_{n=1}^{4000} V_{Q_n} \times I_n}{4000}$
13	A	Net Energy	Net energy for the phase, accumulated by adding true power once per second to a signed 64-bit integer in units of mWh. This value can be positive or negative and is stored to non-volatile memory every 30 seconds. This value can be read in three different formats: 32-bit IEEE float in units of kWh, 64-bit signed integer in units of mWh, and 32-bit signed integer in units of mWh. For more details, review "Data Types Required to Read or Write Accumulation and Summation Values" on page 98.
14	A	Positive Energy	Positive energy for the phase, accumulated by adding true power, if it is positive, once per second to a signed 64-bit integer in units of mWh. This value can be positive or negative and is stored to non-volatile memory every 30 seconds. This value can be read in three different formats: 32-bit IEEE float in units of kWh, 64-bit signed integer in units of mWh, and 32-bit signed integer in units of mWh. For more details, review "Data Types Required to Read or Write Accumulation and Summation Values" on page 98.
15	A	Negative Energy	Negative energy for the phase, accumulated by adding true power, if it is negative, once per second to a signed 64-bit integer in units of mWh. This value can be positive or negative and is stored to non-volatile memory every 30 seconds. This value can be read in three different formats: 32-bit IEEE float in units of kWh, 64-bit signed integer in units of mWh, and 32-bit signed integer in units of mWh. For more details, review "Data Types Required to Read or Write Accumulation and Summation Values" on page 98.
16	A	Net Reactive Energy	Net reactive energy for the phase, accumulated by adding reactive power once per second to a signed 64-bit integer in units of mvarh. This value can be positive or negative and is stored to non-volatile memory every 30 seconds. This value can be read in three different formats: 32-bit IEEE float in units of kvarh, 64-bit signed integer in units of mvarh, and 32-bit signed integer in units of mvarh. For more details, review "Data Types Required to Read or Write Accumulation and Summation Values" on page 98.
17	A	Apparent Energy	Apparent energy for the phase, accumulated by adding reactive power once per second to a signed 64-bit integer in units of mVAh. This value can be positive or negative and is stored to non-volatile memory every 30 seconds. This value can be read in three different formats: 32-bit IEEE float in units of kVAh, 64-bit signed integer in units of mVAh, and 32-bit signed integer in units of mVAh. For more details, review "Data Types Required to Read or Write Accumulation and Summation Values" on page 98.
18	B	V_{rms}	For details, see channel 0
19	B	I_{rms}	For details, see channel 1
20	B	True Power	For details, see channel 2
21	B	Reactive Power	For details, see channel 3
22	B	Apparent Power	For details, see channel 4
23	B	Power Factor	For details, see channel 5
24	B	Peak Voltage	For details, see channel 6
25	B	Peak Current	For details, see channel 7
26	B	Frequency	For details, see channel 8

Ch	Phase	Description	Details
27	B	True Power at Fundamental Frequency	For details, see channel 9
28	B	Harmonic True Power	For details, see channel 10
29	B	Reactive Power at Fundamental Frequency	For details, see channel 11
30	B	Average Reactive Power	For details, see channel 12
31	B	Net Energy	For details, see channel 13
32	B	Positive Energy	For details, see channel 14
33	B	Negative Energy	For details, see channel 15
34	B	Net Reactive Energy	For details, see channel 16
35	B	Apparent Energy	For details, see channel 17
36	C	V_{rms}	For details, see channel 0
37	C	I_{rms}	For details, see channel 1
38	C	True Power	For details, see channel 2
39	C	Reactive Power	For details, see channel 3
40	C	Apparent Power	For details, see channel 4
41	C	Power Factor	For details, see channel 5
42	C	Peak Voltage	For details, see channel 6
43	C	Peak Current	For details, see channel 7
44	C	Frequency	For details, see channel 8
45	C	True Power At Fundamental Freq	For details, see channel 9
46	C	Harmonic True Power	For details, see channel 10
47	C	Reactive Power At Fundamental Freq	For details, see channel 11
48	C	Average Reactive Power	For details, see channel 12
49	C	Net Energy	For details, see channel 13
50	C	Positive Energy	For details, see channel 14
51	C	Negative Energy	For details, see channel 15
52	C	Net Reactive Energy	For details, see channel 16
53	C	Apparent Energy	For details, see channel 17
54	All	Total True Power	True power for all 3 phases in units of W, calculated once per second from the sum of true power for each phase. This value can be positive or negative.
55	All	Total Reactive Power	Reactive power for all 3 phases in units of var, calculated once per second from the sum of reactive power for each phase. This value is always positive.
56	All	Total Apparent Power	Apparent power for all 3 phases in units of VA, calculated once per second from the sum of apparent power for each phase. This value can be positive or negative.

Ch	Phase	Description	Details
57	All	Total Net Energy	Net energy for all 3 phases, accumulated by adding the sum of true power for all phases once per second to a signed 64-bit integer in units of mWh. This value can be positive or negative and is stored to non-volatile memory every 30 seconds. This value can be read in three different formats: 32-bit IEEE float in units of kWh, 64-bit signed integer in units of mWh, and 32-bit signed integer in units of mWh. For more details, review "Data Types Required to Read or Write Accumulation and Summation Values" on page 98.
58	All	Total Unsigned Energy	Net energy for all 3 phases, accumulated by adding the sum of the absolute value of true power for each phase once per second to a signed 64-bit integer in units of mWh. This value can be positive or negative (due to rollover) and is stored to non-volatile memory every 30 seconds. This value can be read in three different formats: 32-bit IEEE float in units of kWh, 64-bit signed integer in units of mWh, and 32-bit signed integer in units of mWh. For more details, review "Data Types Required to Read or Write Accumulation and Summation Values" on page 98.
59	All	Total Positive Energy	Positive energy for all 3 phases, accumulated by adding the sum of true power for all phases if this sum is greater than zero once per second to a signed 64-bit integer in units of mWh. This value can be positive or negative (due to rollover) and is stored to non-volatile memory every 30 seconds. This value can be read in three different formats: 32-bit IEEE float in units of kWh, 64-bit signed integer in units of mWh, and 32-bit signed integer in units of mWh. For more details, review "Data Types Required to Read or Write Accumulation and Summation Values" on page 98.
60	All	Total Negative Energy	Negative energy for all 3 phases, accumulated by adding the sum of true power for all phases if the sum is less than zero once per second to a signed 64-bit integer in units of mWh. This value can be positive or negative (due to roll-over) and is stored to non-volatile memory every 30 seconds. This value can be read in three different formats: 32-bit IEEE float in units of kWh, 64-bit signed integer in units of mWh, and 32-bit signed integer in units of mWh. For more details, review "Data Types Required to Read or Write Accumulation and Summation Values" on page 98.
61	All	Total Net Reactive Energy	Net reactive energy for all 3 phases, accumulated by adding the sum of reactive power for all phases once per second to a signed 64-bit integer in units of mvarh. This value can be positive or negative and is stored to non-volatile memory every 30 seconds. This value can be read in three different formats: 32-bit IEEE float in units of kvarh, 64-bit signed integer in units of mvarh, and 32-bit signed integer in units of mvarh. For more details, review "Data Types Required to Read or Write Accumulation and Summation Values" on page 98.
62	All	Total Net Apparent Energy	Positive energy for all 3 phases, accumulated by adding the sum of true power for all phases if this sum is greater than zero once per second to a signed 64-bit integer in units of mVAh. This value can be positive or negative and is stored to non-volatile memory every 30 seconds. This value can be read in three different formats: 32-bit IEEE float in units of kVAh, 64-bit signed integer in units of mVAh, and 32-bit signed integer in units of mVAh. For more details, review "Data Types Required to Read or Write Accumulation and Summation Values" on page 98.
63	All	Average Power Factor	Average power factor for all 3 phases, calculated once per second from the ratio of Total True Power to Total Apparent Power. This value can be positive or negative.

DATA TYPES REQUIRED TO READ OR WRITE ACCUMULATION AND SUMMATION VALUES

The *groov* RIO EMU measures & calculates data (power) values and accumulates energy values for each phase that it monitors. It also sums all of those values into totals called summation values. All these values are provided through 64 channels:

- **Measurement values** are provided through channels 0 & 1 for phase A, 18 & 19 for phase B, and 36 & 37 for phase C:
  - Channels 0, 18, & 36 measure V_{rms}.
  - Channels 1, 19, & 37 measure I_{rms}.
- **Data (power) values** are provided through channels 2-12 for phase A, 20-30 for phase B, and 38-48 for phase C. For each phase, the module provides:
  - True Power
  - Reactive Power
  - Apparent Power
  - Harmonic True Power
  - Power Factor
  - Peak Voltage
  - Peak Current
  - Frequency
  - True Power at Fundamental Frequency
  - Average Reactive Power
  - Reactive Power at Fundamental Frequency
- **Accumulated energy values** for Net, Positive, Negative, Net Reactive, and Apparent energy are provided through channels 13-17 for phase A, 31-35 for phase B, and 49-53 for phase C.
- **Summation values** for True, Reactive, Apparent, Net, Unsigned, Positive, Negative, Net Reactive, and Apparent energy are provided through channels 54-62.
- **Average power factor** is provided through channel 63.

The "Channel Specifications" on page 95 outlines which channel provides each of these values and describes the formulas it uses for calculations.

The accumulated and summation values are stored to non-volatile memory every 30 seconds.

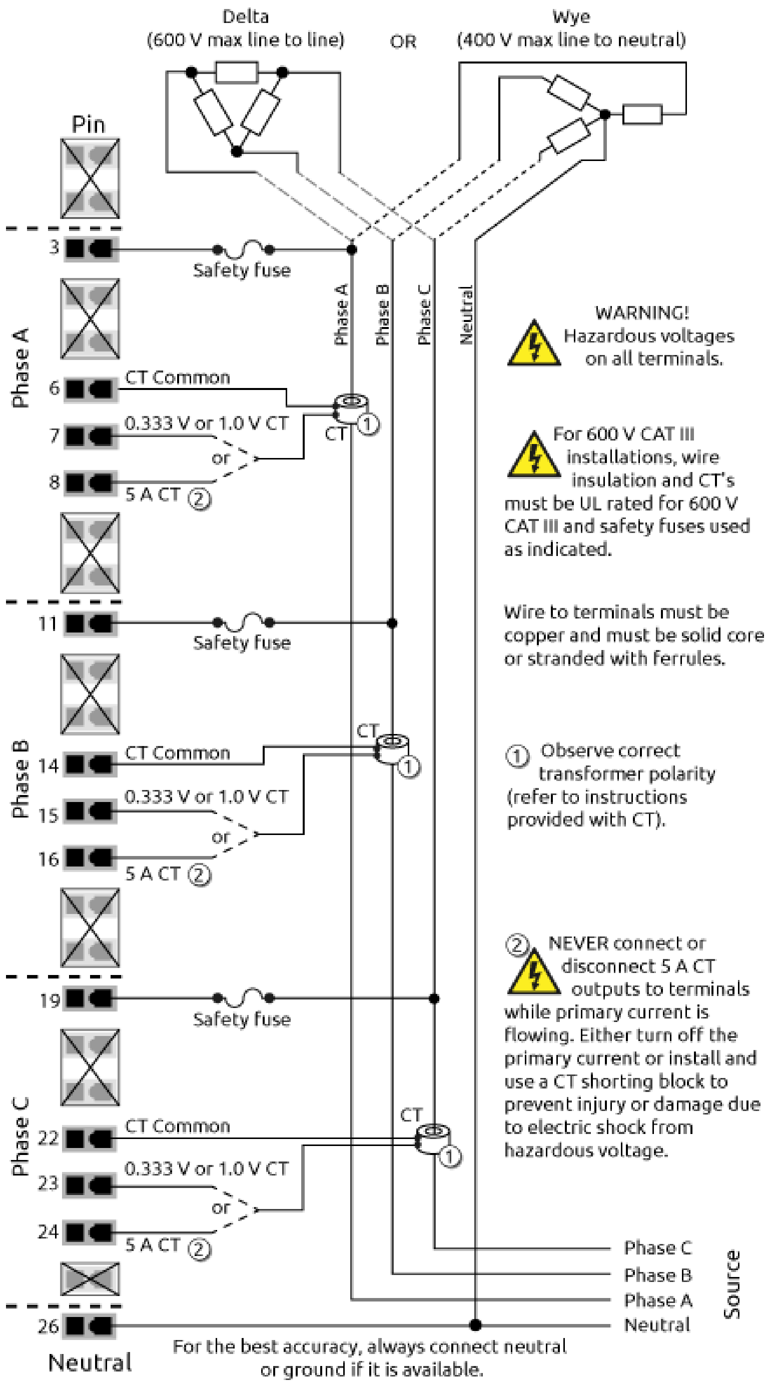
B: Wiring Diagrams

The wiring diagrams begin on the next page.

GRV-R7-I1VAPM-3

The following diagram shows how to correctly wire delta-configured and wye-configured loads without potential transformers. Wye-configured loads above 400 V *require* the use of potential transformers; see wiring diagram on next page.

WARNING: DANGER. *Hazardous voltage. Direct wiring involves high voltages and must be done by a* ***qualified technician****.*



WARNING!
Hazardous voltages
on all terminals.

For 600 V CAT III installations, wire insulation and CT's must be UL rated for 600 V CAT III and safety fuses used as indicated.

Wire to terminals must be copper and must be solid core or stranded with ferrules.

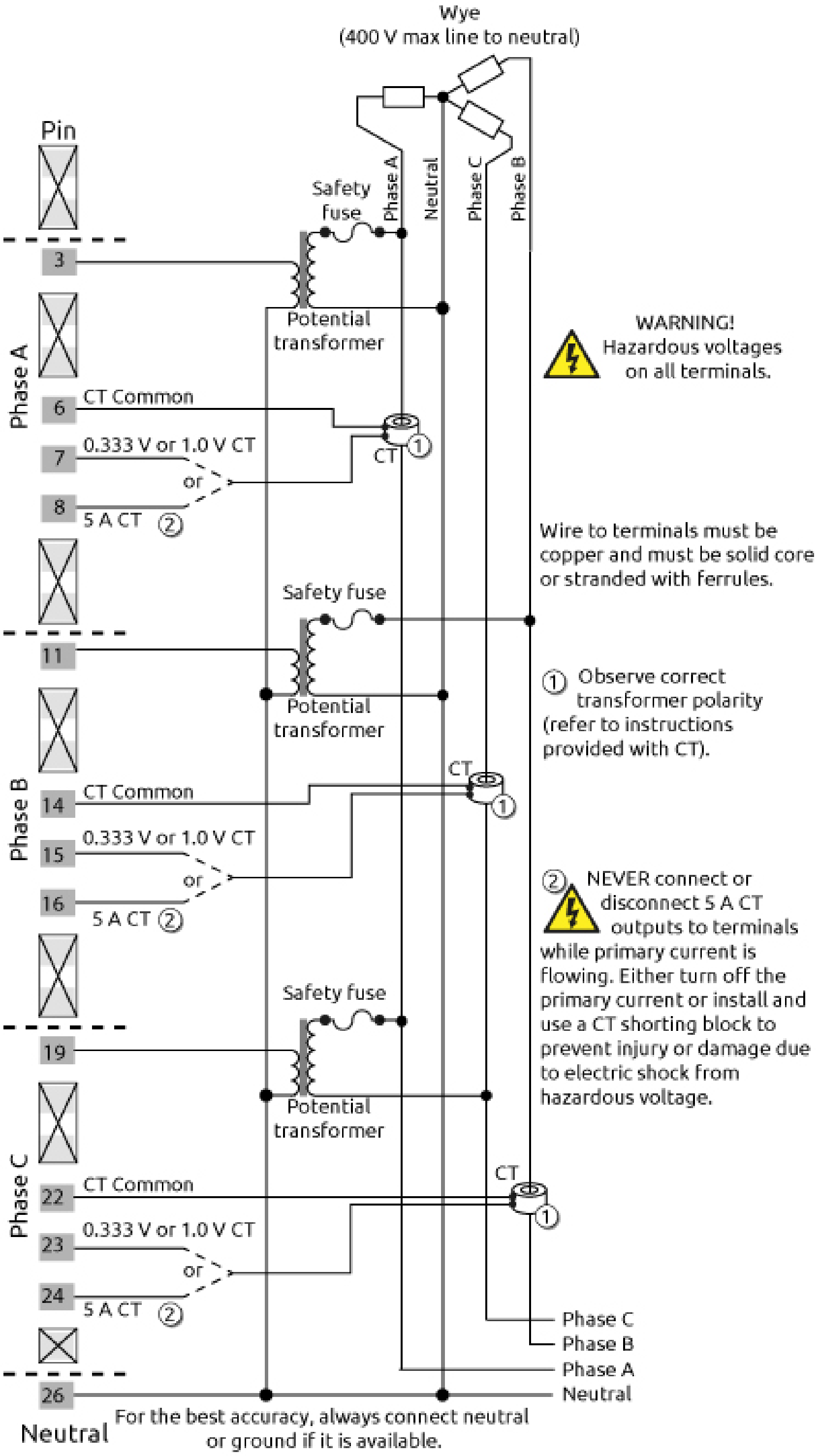
① Observe correct transformer polarity (refer to instructions provided with CT).

② NEVER connect or disconnect 5 A CT outputs to terminals while primary current is flowing. Either turn off the primary current or install and use a CT shorting block to prevent injury or damage due to electric shock from hazardous voltage.

For the best accuracy, always connect neutral or ground if it is available.

The following diagram illustrates how to correctly wire wye-configured loads when using potential transformers. Wye-configured loads over 400 V require potential transformers.

WARNING: DANGER. *Hazardous voltage. Direct wiring involves high voltages and must be done by a* ***qualified technician****.*


Wye
(400 V max line to neutral)
Pin
Safety fuse
Phase A
Neutral
Phase C
Phase B
3
Potential transformer
Phase A
6
CT Common
CT
1
7
0.333 V or 1.0 V CT
or
8
5 A CT
2
WARNING!
Hazardous voltages on all terminals.
Wire to terminals must be copper and must be solid core or stranded with ferrules.
Safety fuse
11
Potential transformer
1 Observe correct transformer polarity (refer to instructions provided with CT).
CT
Phase B
14
CT Common
1
15
0.333 V or 1.0 V CT
or
16
5 A CT
2
2 NEVER connect or disconnect 5 A CT outputs to terminals while primary current is flowing. Either turn off the primary current or install and use a CT shorting block to prevent injury or damage due to electric shock from hazardous voltage.
Safety fuse
19
Potential transformer
CT
Phase C
22
CT Common
1
23
0.333 V or 1.0 V CT
or
24
5 A CT
2
Phase C
Phase B
Phase A
Neutral
26
Neutral
For the best accuracy, always connect neutral or ground if it is available.

C: Understanding Certificates

HOW SSL/TLS CERTIFICATES CREATE TRUST BETWEEN CLIENT AND SERVER

Here's a brief explanation of how an SSL/TLS certificate can help create an encrypted connection and prove a *groov* RIO EMU's identity to client browsers:

1. When you open a browser and type in the *groov* RIO EMU's hostname as `https://hostname`, the "s" at the end of "http" indicates that you are requesting an encrypted, secure connection.
2. The *groov* RIO EMU receives the request, then responds by sending a certificate.
3. The browser receives the certificate, then verifies the information in the certificate:
   – If the browser **can** verify the information in the certificate (which proves the *groov* RIO EMU's identity), then the browser trusts the certificate. The browser creates a session key (which is valid for only this one session and helps create the encryption), then sends the session key to your *groov* RIO EMU.
   – If the browser **cannot** verify the information in the certificate, then the browser may not trust the certificate. The browser displays a warning message to the user (YOU) and may provide some options for handling the situation. One such option may be for the user (YOU) to override the browser's warning and proceed with establishing an encrypted connection.

   Note: *groov RIO EMU accepts only secure, encrypted connections. If you do not override your browser's warning, you will not be able to connect to it.*

The same process is true the other way around, where your *groov* RIO EMU is the client and it wants to request a secure, encrypted connection with a server; for example, an LDAP server.

If you want to learn more about SSL certificates and how they work, you can find several great resources on the Opto 22 website:

- Understanding SSL/TLS and HTTPS, an OptoBlog post
- How to configure SSL/TLS server certificates on *groov* devices, an OptoBlog post
- Video: Cybersecurity: Working with Private Certificate Authorities

Creating Different Scopes of Trust with Certificates

In the scenario described in the previous section, step 2 indicates that your *groov* RIO EMU sends a certificate to your browser. How did your *groov* RIO EMU obtain a certificate? All *groov* RIO EMUs ship with a **default** self-signed certificate. A certificate contains:

- a server name,
- the name of the organization that controls the server,
- a public key, and

- digital signatures of organizations that vouch for the authenticity of the certificate. The certificate can be digitally signed either by a certificate authority (CA) or it can be self-signed.

In the default self-signed certificate shipped with all *groov* RIO EMUs, the server name is the *groov* RIO EMU's hostname, the name of the organization is blank, and the organization vouching for the authenticity of the certificate is the *groov* RIO EMU's hostname, which is what makes this certificate self-signed. For very simple network setups (for example, only one computer or mobile device will ever access your *groov* RIO EMU), the default self-signed certificate may be good enough.

However, for more complex network environments, you may want to create other types of certificates for your *groov* RIO EMU:

- **Custom self-signed**—If you change the hostname of your *groov* RIO EMU, you may need to create a custom self-signed certificate then install it on the clients (the computers and mobile devices) that will access your *groov* RIO EMU.
- **Verified by Private CA**—If you manage or work in a private OT or IT network and you want some or any client within this network to easily and securely access your *groov* RIO EMU, you'll want to create a certificate verified by a private Certificate Authority (CA). If you have a network administrator, work with that person to create this certificate and get it installed on the clients in the network.
- **Verified by Public CA**—If you need to allow clients on the internet to connect to your *groov* RIO EMU, then you want to obtain a certificate verified by a public Certificate Authority (CA). These are rare situations and require careful review by your network administrator and local cybersecurity expert.

How a Browser Trusts Certificates

Step 3 indicates that the browser verifies the authenticity of the certificate. How does it do that? The browser has access to a "trust store": a place (usually in the operating system) that contains certificates whose trust-worthiness has been verified by either a user or a certificate authority (CA). A network administrator typically manages the trust store with the help of utilities provided by the operating system; with the help of a network administrator, you can add certificates to the trust store that you (the user) independently verified. For example, the default self-signed certificate that came with your *groov* RIO EMU will cause your web browser to display the "untrusted site" warning every time you access the *groov* RIO EMU. You can add it to the operating system's trust store to prevent that warning from appearing.

Describing how to manage each client's trust store is outside the scope of this guide; work with your IT administrator if you want to add *groov* RIO EMU certificates to your client's trust store.

In the situation where the *groov* RIO EMU is the client, it has its own trust store that it uses to verify certificates it receives from a server. And, just like a trust store on a computer or a mobile device, its operating system maintains a set of verified certificates and you can add your own verified certificates. Instructions on how to add certificates to the *groov* RIO EMU's trust store are in this guide.

Learning More About SSL/TLS, HTTPS, and Certificate Management

The Opto 22 website contains videos demonstrating many of the concepts and tasks described in this chapter. It also provides blogs that describe a brief history of SSL/TLS and certificates. Review these resources to help further your understanding.

- Technical Note: *groov* EPIC Cybersecurity Design and Best Practices Technical Note

  While the title suggests the document is focused on *groov* EPIC, much of the information also applies to *groov* RIO devices. The document provides an overview of cybersecurity issues applicable to the industrial automation industry and discusses the role of SSL/TLS certificates in cybersecurity.
- OptoBlog: Understanding SSL/TLS and HTTPS

  Provides a basic understanding of the relationship between SSL/TLS and https and how certificates help define that relationship.

- Opto 22 Video: Default Self-signed Certificates

  Introduces certificates and how they play a role in establishing an encrypted connection between your browser and your *groov* RIO EMU. Explains why you see “untrusted” messages from your browser when you connect to your *groov* RIO EMU and how to remove that message by downloading the default self-signed certificates, then adding it to the trust store on your Windows PC.
- Opto 22 Video: Custom Self-signed Certificates

  Reviews the role that certificates play in establishing an encrypted connections, why you would want to create a custom self-signed certificate, and then how to add it to the trust store on your Windows PC.
- Opto 22 Video: Working with Private Certificate Authorities

  How to access a private CA in your company's network and use it to sign a certificate generated by your *groov* RIO EMU..
- *groov* EPIC Developer Guide: Getting a Trusted Connection Between a Web Browser and *groov* EPIC

  Provides a brief introduction to certificates, then a step-by-step guide to create a private CA on your computer, create the client certificates to install into the trust store of your computer, and create the server certificate for a *groov* EPIC. Many of the steps will be similar for a *groov* RIO EMU. This tutorial requires knowledge and experience working with command line terminal programs and text editors.