

***groov* BOX**
USER'S GUIDE
FOR GROOV-AR1

groov BOX USER'S GUIDE

for GROOV-AR1

Form 2104-220518—May 2022

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 Box User's Guide
Form 2104-220518—May 2022
Copyright © 2015–2022 Opto 22.
All rights reserved.
Printed in the United States of America.

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

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

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

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

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

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

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

Opto 22
Your Edge in Automation.

Table of Contents

Chapter 1: Welcome	1
System Requirements	2
Everything you can do with the <i>groov</i> Box	3
<i>groov</i> Box Communications	4
System Architecture	4
<i>groov</i> Box System Architecture	5
About this Guide	5
What's In This Guide	6
Product Support	6
Chapter 2: Getting Started	7
What You Will Need	7
In the Box	7
Step 1. Get To Know the <i>groov</i> Box	8
Step 2. Choose a Location	8
Step 3. Mount the <i>groov</i> Box	9
Mounting on a flat surface:	9
Mounting on a DIN rail:	9
Step 4. Connect to the Network	10
Step 5. Connect the Power Supply	11
Step 6. Turn on the <i>groov</i> Box	11
Step 7. Activate the <i>groov</i> Box and Get the License File	12
Step 8. Open <i>groov</i> View	13
Opening <i>groov</i> View using your web browser	13
Opening <i>groov</i> View using <i>groov</i> Find	14
Step 9. Create a <i>groov</i> Admin Account	16
Step 10. Install the License File	16
Step 11. Create a <i>groov</i> View Account	16
Chapter 3: Using <i>groov</i> Admin	17
Opening <i>groov</i> Admin	17
Open <i>groov</i> Admin from Build mode	17
Open <i>groov</i> Admin using the URL	17
Open <i>groov</i> Admin using <i>groov</i> Find (Windows only)	18

Accept the Security Warning	20
For Chrome	20
For Firefox	20
For Safari	20
For Internet Explorer	20
Log in	20
Quick Start menu	21
Opening <i>groov</i> View from <i>groov</i> Admin	21
Opening Node-RED Admin from <i>groov</i> Admin	22
Opening Ignition Edge from <i>groov</i> Admin	22
Configuring Ignition Edge	23
Configuring Network Connections	23
Assigning a Static IP Address	24
Changing the Hostname, DNS Servers, or IPv4 Gateway	25
Configuring ETH1 for the Control Network	25
Configuring Wireless Communications	26
Using an AR1 as a Wireless Access Point	29
Updating <i>groov</i> View	30
Backing Up <i>groov</i> View and Network Settings	32
Restoring <i>groov</i> View and Network Settings	33
Updating <i>groov</i> Admin	34
Updating Node-RED	36
Restarting the <i>groov</i> Box	36
Changing Username and Password	37
Checking System Information	39
Checking Hardware Status	40
Setting the System Time	41

Chapter 4: Using Node-RED 43

What is Node-RED?	43
Node-RED in the <i>groov</i> Box	44
Getting Started	44
Requirements	44
Open Node-RED	44
Create a flow	45
Deploy the flow and test	46
Add a Function node	46
Install <i>groov</i> View nodes	47
Add an Opto 22 PAC Control node	48
Connecting with serial devices	51
Requirements	51
Setting up the serial device	52
Working with nodes	53
Managing nodes	53
Installing nodes	53
Working with flows	54
Exporting a flow	54

Importing a flow	55
Import from the Library	55
Import from a file	55
Debugging your Node-RED project	56
In the Editor	56
In Node-RED Admin	56
Managing security certificates	57
Backing up and restoring your Node-RED project	57
Starting a new Node-RED Project	58

Chapter 5: Using Ignition Edge 59

What is Ignition Edge?	59
Ignition Edge in the <i>groov</i> Box	59
OPC UA drivers included with Ignition Edge in the <i>groov</i> Box	60
<i>groov</i> EPIC and SNAP PAC drivers	60
Getting Started	60
Requirements	60
Configure Ignition Edge	61
Configure a device in Ignition Edge	66
Add the internal OPC-UA server to <i>groov</i> View	67
Add a gadget connected to an Ignition Edge tag	68
Add other devices (Allen-Bradley, Siemens, Modbus)	69
Configure tags manually	70
Using MQTT	73
MQTT and the <i>groov</i> Box	73
Install the MQTT Transmission module	73
Configure the MQTT broker	74
Configure MQTT tags	74
Managing Ignition Edge	75
Restart the Trial	75
License Ignition Edge	76
Activate Offline	78
Unactivate Ignition Edge license	80
Change Ignition Edge password	80
Back up and restore Ignition Edge project	81
Restore Ignition Edge project	82
Use Ignition Edge Designer or Edge Panel	82
Ignition Edge Plugins	84
Check Ignition Edge license and modules	84
Add Quarantined Modules	85

Chapter 6: Using an SSL Certificate 87

Understanding Certificates	87
Certificate Structure	88
Step 1: Back up your <i>groov</i> View Project	88
Step 2: Create a Private Key	88
Step 3: Get and Use the Certificate	90

Using a Self-Signed Certificate	90
Finish the Self-Signed Certificate	90
Add the Self-Signed Certificate to a Browser Trust Store on a Computer	91
Install an SSL Certificate on Mobile Devices	94
Using a CA-Signed Certificate on the <i>groov</i> Box	95
Finish the CSR	95
Obtain a CA-Signed Certificate	96
Install the CA-Signed Certificate on the <i>groov</i> Box	97
Chapter 7: Maintenance and Troubleshooting	99
Maintenance	99
Turning the <i>groov</i> Box On and Off	99
Resetting the <i>groov</i> Box to Factory Defaults	100
Applying a <i>groov</i> Edge license option	100
Transferring a <i>groov</i> Box to someone else	101
Replacing the battery	101
Troubleshooting	102
<i>groov</i> Box is not receiving power	102
Cannot log into <i>groov</i> Box using its hostname	102
<i>groov</i> Box is connected to Ethernet network but doesn't work	102
DHCP (dynamic host configuration protocol) server	103
DNS (domain name server)	103
Computer with more than one NIC	103
Modbus/TCP device, OPC UA server, or Opto 22 SNAP PAC controller can't be found	103
Cannot read from/write to Modbus/TCP device OR Modbus data doesn't make sense	104
"Connection is reset" error in <i>groov</i> Admin	104
Power LED is blinking red	104
Power outage	104
Node-RED flow not working	105
Errors in Build mode when using Ignition Edge	105
No data in <i>groov</i> View for gadgets using Ignition Edge tags	105
Ignition Edge OPC-UA and MQTT documentation	105
Ignition Edge shows license is temporary and valid for only seven days	106
Time zone change not shown in Ignition Edge	106
Appendix A: Specifications and Dimensions	107
Specifications	107
Dimensions	108
Appendix B: Connectors, Ports, and LEDs	109
Connectors	109
USB connectors for serial devices	110
Ports	111
LEDs	111
Appendix C: Installing an Approved USB WiFi Adapter	113
Index	115

1: Welcome

NOTE: The groov Box is a legacy product as of June 2021 and is not recommended for new development. For new industrial internet of things (IIoT) projects that do not require local I/O, we recommend a groov EPIC processor (GRV-EPIC-PR1 or GRV-EPIC-PR2) on a chassis zero (GRV-EPIC-CHS0, with no I/O slots). groov EPIC has a larger form factor and is more expensive, but it offers more RAM, groov View, more recent versions of Node-RED and Ignition Edge® from Inductive Automation®, an integral color touchscreen, and secure shell access. In addition, groov EPIC future-proofs your IIoT project with the ability to add I/O, real-time control, and full Ignition.

The groov® Edge Appliance (groov Box) is an Opto 22 internet of things (IIoT) and operator interface appliance that provides visualization, data handling, and connectivity to automation systems, software, databases, and devices of all kinds—all in a compact, industrially hardened box suited to the edge of the network.

Visualization: From pumps and processes, to production data, to the weather, your world is full of things you need to view, monitor, or control. With browser-based groov View, you can easily build an operator interface to see and interact with exactly what you need. Show data from sensors and automation systems, cloud applications, databases, web services, and more. Securely view the interface you build on any brand device, from a smartphone to a computer to a web-enabled big-screen TV.

To build your interface, just drag, drop, and tag. No tag limits; no user licenses required.

Set up authorized users and groups. Define events based on one or more conditions, and automatically alert selected personnel anywhere when events occur. groov View can augment existing human-machine interfaces (HMIs) and SCADA systems by making specific data visible to authorized users at any time and in any location.

Data Handling: The key to IIoT usefulness is getting the data out of where it's trapped and into the systems and software where it's needed. With the groov Edge Appliance, you can use standard internet and IT-compatible tools to manipulate and move data between things in the real world and computer systems and software on premises or in the cloud.

Key tools are built into the groov Box and ready for use: Node-RED, an IIoT rapid application development environment; RESTful APIs to groov View Data Stores; and Ignition Edge® from Inductive Automation®, with



SYSTEM REQUIREMENTS

OPC UA and MQTT. You can place the secure *groov* Box at the network's edge in harsh industrial environments and know you have the tools right there to acquire data, move it, and act on it.

Connectivity: The *groov* Box simplifies the connections you need to accomplish your IoT goals. Connect to all kinds of devices and systems to monitor and control them and move data between them.

- Connect directly to Modbus/TCP devices, Opto 22 *groov* EPIC® processors, *groov* RIO units, SNAP PAC controllers, and SNAP PAC I/O units to access their data.
- Use Node-RED (included) to create logical flows for data. Exchange data with cloud applications, IoT platforms, on-premises databases, and external web services. Also connect to serial devices—Modbus RTU/ASCII, weigh scales, and more—via a USB-to-serial converter and Node-RED.
- Use our secure RESTful API from your database, cloud service, or business application to place data in or read data from a *groov* Data Store, where you can access it for your use.
- Connect to PLCs and PACs from other automation manufacturers using OPC UA:
 - With the internal Ignition Edge server and drivers, connect to Allen-Bradley® and Siemens® PLC systems, plus others (requires Ignition Edge license, GROOV-LIC-EDGE).
 - With an external OPC-UA server such as Kepware Technologies' KepServerEX®, connect to any system or database your server and drivers support.
- Publish and subscribe data from devices connected to the *groov* Box to brokers, using the lightweight MQTT transport protocol. MQTT creates a high-performance communications architecture ideal for getting the data that's trapped behind firewalls into SCADA software like Ignition Enterprise (requires Ignition Edge license, GROOV-LIC-EDGE).

The *groov* Box brings data from process control, OEM machines, manufacturing and building systems, and the internet of things (IoT) to the people and systems that need it.

NOTE: The groov Box is compatible with groov EPIC, groov RIO, and the SNAP PAC System, and all can be used in combination to meet the needs of your application.

SYSTEM REQUIREMENTS

To build operator interfaces with *groov* View, you'll need:

- Any computer with a web browser (does not have to be a Windows PC; see the [groov View Readme](#) for current browsers supported)
- One of the following:
 - *groov* EPIC
 - *groov* Server for Windows
 - a legacy *groov* Box Edge Appliance

You can connect to any of the following devices or services to get and send data:

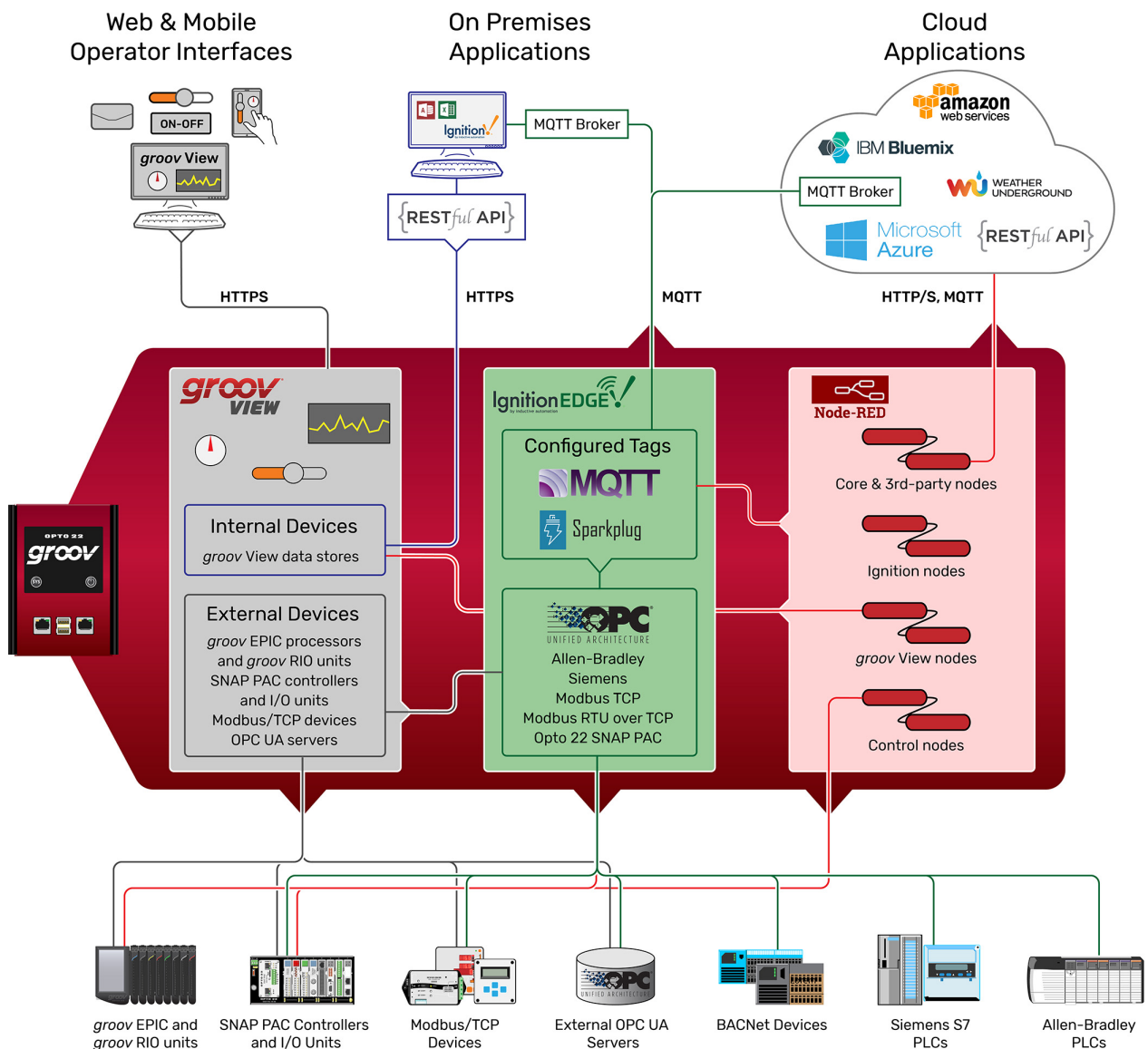
- A Modbus/TCP device
- A database, online service, or software program to get data from or put data into a Data Store using the *groov* View API
- An Opto 22 *groov* EPIC processor or SNAP PAC controller (SNAP PAC S-series, R-series, or SoftPAC, with firmware R9.2a or newer), running a PAC Control strategy
- An Opto 22 *groov* EPIC I/O unit
- An Opto 22 *groov* RIO unit
- An Opto 22 SNAP PAC I/O unit
- (*groov* EPIC or legacy *groov* Box only) A database, cloud application, API, or serial device accessible via a Node-RED node. (For a *groov* Box, see requirements in the user's guide.)
- OPC UA-compatible automation system or equipment. Ignition Edge supplies an internal server and drivers for *groov* EPIC or a legacy *groov* Box. An external OPC-UA server is required for *groov* Server; an external server and additional drivers may be required for your equipment.

NOTE: Browser-based groov View software works on a large number of device/operating system/browser combinations, including HDTVs, smartphones and tablets, and computers. Check the [groov View Readme](#) for supported browsers for your version of groov View. If one browser is causing problems for you, try another one and let us know what issues you've seen. For Product Support, see [page 6](#).

EVERYTHING YOU CAN DO WITH THE *groov* BOX

Congratulations on choosing the *groov* Box! This compact industrial box is designed for harsh environments and is ideal for industrial internet of things applications at the edge of the network. Because it includes not only *groov* View but also Node-RED and Ignition Edge with MQTT, the *groov* Box gives you the modern tools you need to make your IoT projects a reality.

The diagram below illustrates how data can move easily between the devices and software at the top, and the industrial systems and equipment at the bottom. You can use the open standards and methods that work best for your skills and situation: *groov* devices and tags, tags in Ignition Edge, and nodes in Node-RED flows. (You'll need a *groov* Edge license to fully use Ignition Edge for OPC UA and MQTT.) With all these tools in the same box, configuration and security are simplified.



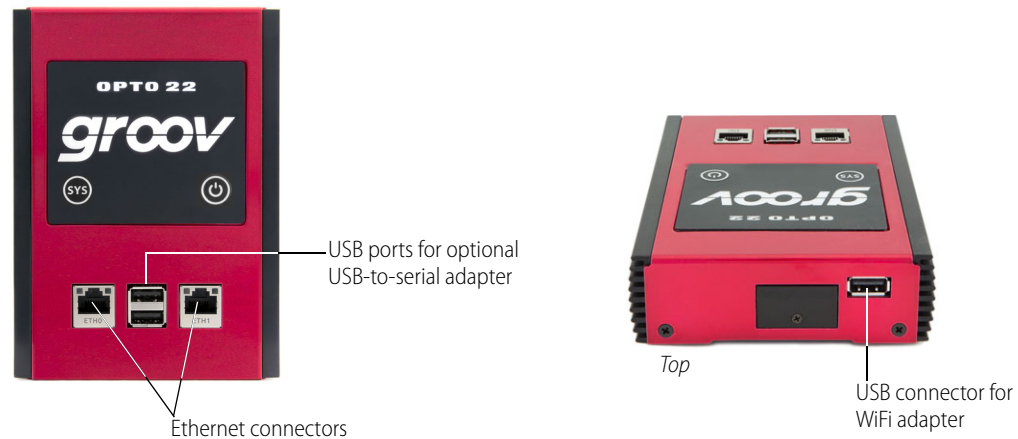
groov BOX COMMUNICATIONS

groov uses standard computer networks and protocols. The unit communicates with computer networks over a standard 10/100/1000 Mbps Ethernet network. For use on a wireless network, you must purchase and install a USB WiFi adapter that has been tested and approved by Opto 22. For more information, see [Appendix C: Installing an Approved USB WiFi Adapter](#).

With two independent wired Ethernet network interfaces plus an optional independent wireless interface, the unit gives you the flexibility to monitor devices in hard-to-reach areas and to set up networking suited to your business.

In addition, you can use your *groov* Box as an access point in order to create a private wireless network with WPA2-PSK security. This is particularly useful for connecting a phone or tablet to *groov* View when there is no other wireless network available. SoftAP can be used by any WiFi-capable device. Your *groov* Box can be connected to either a wireless or Ethernet network. See [“Using an AR1 as a Wireless Access Point” on page 29](#).

Using a USB-to-serial converter and Node-RED in the *groov* Box, you can also connect to serial devices. You can use data from these devices in your *groov* View operator interface or anything with a Node-RED node, for example a database or a cloud-based service such as IBM Watson IoT. See [“Connecting with serial devices” on page 51](#) for more information.

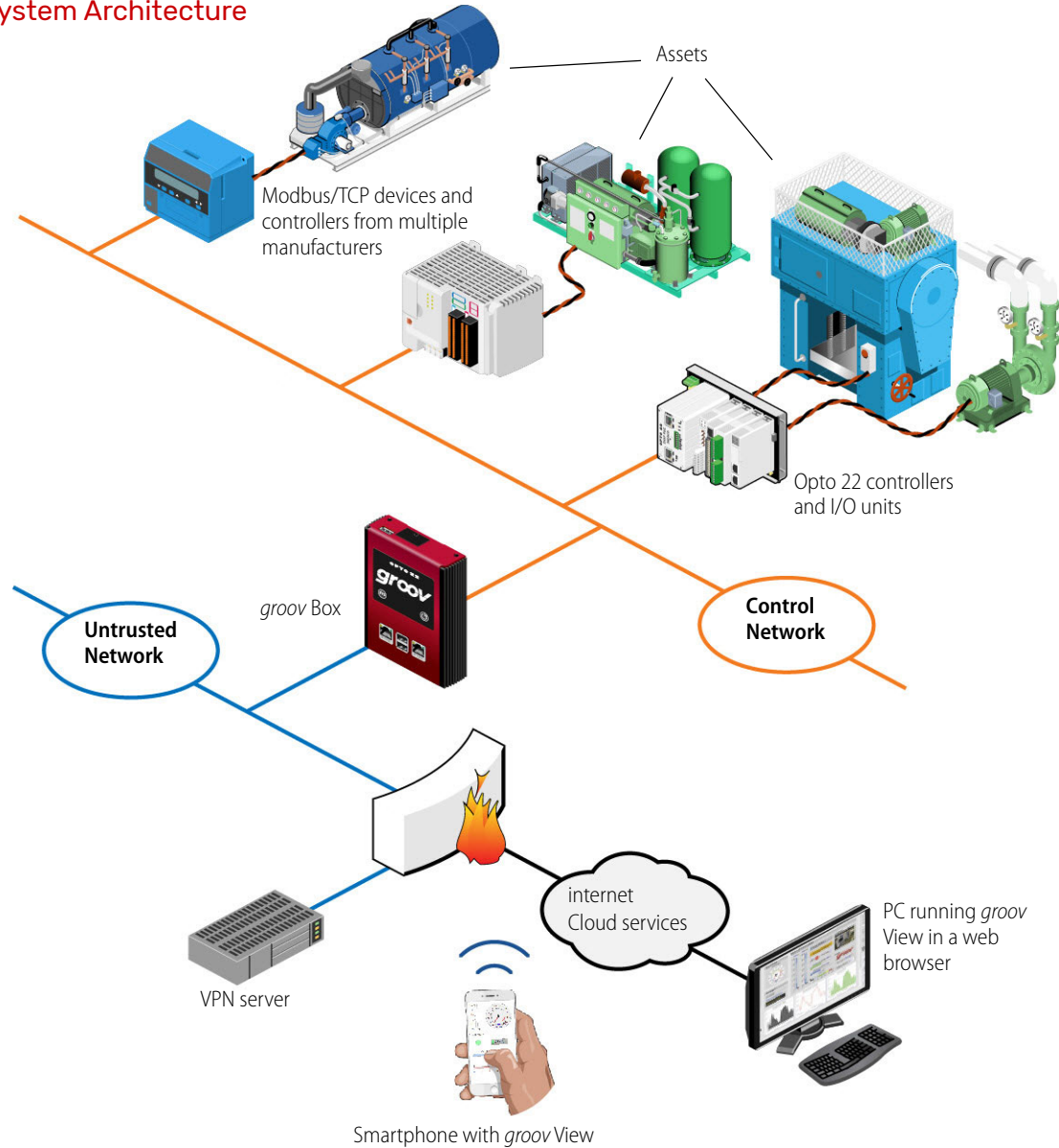


SYSTEM ARCHITECTURE

When you first set up your *groov* Box, the PC you use must reside on the same network (broadcast domain) as the Box. In a quick and easy setup, the development PC and smartphone or tablet running *groov* View all reside within the same domain as the Box. The controller or other device that supplies data to the *groov* Box can also be on the same network, or it can be on a separate control network as shown below. For more information, see form 2161, the [Guide to Networking groov](#).

The following illustration shows the *groov* Box connected to control systems from other manufacturers as well as an Opto 22 controller and I/O units. (The illustration shows a SNAP PAC controller, but the *groov* Box is also compatible with *groov* EPIC and *groov* RIO.) When accessing the *groov* Box outside the Box's network, over the internet, we recommend a VPN (Virtual Private Network) connection for security. The HTTPS (HTTP plus TLS/SSL) in your browser shows that all data exchanged between your browser and the *groov* Box is encrypted.

groov Box System Architecture



ABOUT THIS GUIDE

This user's guide shows you how to install and set up your *groov* Box, how to get started with Node-RED and Ignition Edge, and how to use the *groov* Admin and Node-RED Admin software. *groov* Admin provides the tools to back up and restore your project, update *groov* and Ignition Edge, set up wired and wireless networking, and more. Node-RED Admin includes tools for debugging, backing up, and restoring Node-RED flows, nodes, and credentials. For other information:

- For information about building and viewing *groov* View interfaces, see form 2027, the [groov View User's Guide](#). You can also find [groov View videos](#) and other resources on our website.
- For information about Node-RED, visit nodered.org. Also see [Node-RED videos](#) on our website.
- For Ignition Edge, see inductiveautomation.com.

What's In This Guide

Chapter 1: Welcome (this chapter) introduces this user's guide and the *groov* Box.

Chapter 2: Getting Started describes how to get your *groov* Box up and running quickly.

Chapter 3: Using *groov* Admin describes how to use *groov* Admin to back up and restore *groov*, manage the network connections, access system information, and more.

Chapter 4: Using Node-RED introduces the open-source tool Node-RED (included in the *groov* Box) and shows you how to use Node-RED Admin to manage your nodes and flows.

Chapter 5: Using Ignition Edge gets you started with the OPC UA server and MQTT communications option included in your *groov* Box.

Chapter 6: Using an SSL Certificate describes using an SSL certificate that is digitally signed either by a certificate authority (CA) or self-signed.

Chapter 7: Maintenance and Troubleshooting provides troubleshooting information and answers questions you might have about the *groov* Box.

Chapter A: Specifications and Dimensions provides technical specifications and dimensions.

Chapter B: Connectors, Ports, and LEDs describes connector and LED functions.

Chapter C: Installing an Approved USB WiFi Adapter provides a list of USB WiFi adapters Opto 22 has tested and approved for use with GROOV-AR1-BASE, and installation instructions.

PRODUCT SUPPORT

If you have any questions about your *groov* Box, you can call, fax, or e-mail 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

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

Email: support@opto22.com

Opto 22 website: www.opto22.com

When calling for technical support, be prepared to provide the following information about your system to the Product Support engineer:

- *groov* Image version and *groov* Admin version. Click the System Information icon in the Admin Quick Start (see [page 39](#)).
- A description of your system equipment:
 - Computer type, speed, memory, and operating system
 - Browser type and version
 - OPC UA server type and configuration
- A description of the network
- Specific error messages or other diagnostic indications

2: Getting Started

This chapter shows you how to install the *groov* Box and set up the *groov* Admin software.

In this chapter:

What You Will Need	7
In the Box	7
Step 1. Get To Know the <i>groov</i> Box	8
Step 2. Choose a Location	8
Step 3. Mount the <i>groov</i> Box	9
Step 4. Connect to the Network	10
Step 5. Connect the Power Supply	11
Step 6. Turn on the <i>groov</i> Box	11
Step 7. Activate the <i>groov</i> Box and Get the License File	12
Step 8. Open <i>groov</i> View	13
Step 9. Create a <i>groov</i> Admin Account	16
Step 10. Install the License File	16
Step 11. Create a <i>groov</i> View Account	16

WHAT YOU WILL NEED

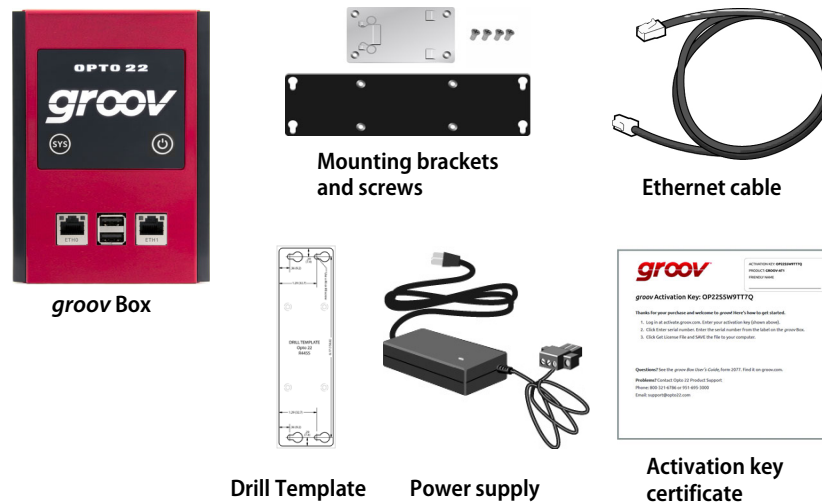
In order to set up your *groov* Box and do the activities in this chapter, you will need a computer with a web browser on the same network you'll use for the *groov* Box. You'll need a recent web browser: Chrome, Firefox, Edge, or Safari. See the [groov View Readme](#) for current supported browsers.

IN THE BOX

These items are included in the box:

- *groov* Quick Start for GROOV-AR1, form 2103
- *groov* Box (GROOV-AR1)
- Ethernet cable
- Power supply unit
- One DIN clip and one flat surface mounting bracket (includes four screws)
- Drill template for the mounting bracket
- Activation key certificate

STEP 1. GET TO KNOW THE GROOV BOX



You'll need the activation key for step 7 when you activate your *groov* Box, so make sure to **put your activation key certificate in a safe place**.

STEP 1. GET TO KNOW THE *groov* BOX

To set up the *groov* Box, you'll use the components shown below. Make sure to put the activation key certificate in a safe place. You'll need the activation key later when you activate your *groov* Box.



STEP 2. CHOOSE A LOCATION

The *groov* Box is a fanless industrial appliance made to operate in tough environments (see specs on [page 107](#) for temperature and humidity). Some location considerations:

- Make sure there is room around the front, top, and sides of the *groov* Box to allow air to flow freely around the device. Also, you need to be able to see the information on the bottom.
- If you plan to use the two Ethernet network interfaces on the *groov* Box to separate your control network from an untrusted network (for example, a network with internet access), place it where you can connect to both networks. (For more on networking, see the [Guide to Networking groov](#), form 2161).
- If you're connecting to a wireless LAN through a WiFi adapter in the top USB port, choose a location where the signal is constant and strong. Wireless networks can be unreliable unless carefully designed and periodically checked.

- If you're a machine builder or OEM and including a *groov* Box in your machine, the same basic ideas apply: check specs, check security, and then install. Make sure you have network access to the Box for updates.

STEP 3. MOUNT THE *groov* BOX

Mounting brackets are provided for you to attach the *groov* Box to a flat surface or a DIN rail. If there will be vibration at the *groov* Box installation site, make sure to mount the device to a flat surface for a secure installation.

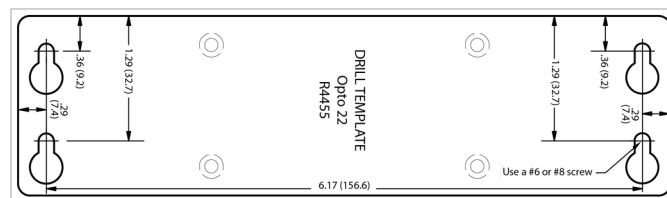
Mounting on a flat surface:

1. Using the screws provided, install the surface mounting bracket on the back of the *groov* Box.



Surface mounting bracket

2. Using the hole template provided, drill holes for #6 or #8 screws in the mounting surface.



3. Secure the device to a flat surface with #6 or #8 screws.

Mounting on a DIN rail:

1. Using the screws provided, install the DIN rail clip on the back of the *groov* Box.

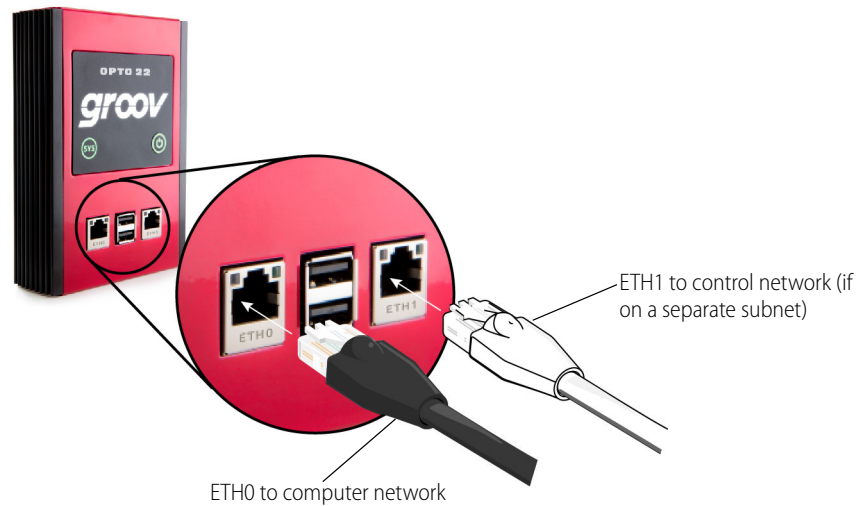
STEP 4. CONNECT TO THE NETWORK



DIN rail clip

2. Attach the *groov* Box to the DIN rail.

STEP 4. CONNECT TO THE NETWORK



1. Connect an Ethernet cable from ETH0 to your computer's network.

NOTE: Opto 22 recommends connecting ETH0 to a network with DHCP and DNS services. If you do not have these services, you'll need to manually configure networking.

2. The two independent Ethernet connectors (ETH0 and ETH1) have separate IP addresses that can be used to segment a control system's network from the company LAN. If your Opto 22 controller, OPC UA server, or Modbus/TCP device is on a different network from your computer, connect ETH0 to your computer's network and ETH1 to the other network.

If you are using both ETH0 and ETH1, make sure they have IP addresses on different subnets. In some situations, this may require configuring a static IP address for the *groov* Box to avoid communication errors. For more information, see ["Assigning a Static IP Address" on page 24](#).

For detailed information on setting up your network and setting up communications over the Internet, see form 2161 the [Guide to Networking groov](#).

STEP 5. CONNECT THE POWER SUPPLY

Your *groov* Box requires a power supply with an output of 8–36 VDC, 24 VDC @ 500 mA. You can use the power supply that comes with the *groov* Box, or provide your own. In either case, we recommend using a UPS (uninterruptible power supply) for backup power and surge protection.

If you are using the power supply that came with the *groov* Box, do the following:

Plug the small connector on the power supply into the power terminal on the bottom of the *groov* Box, and tighten the screws. Plug the other end into a standard 120 or 240 VAC outlet.



If you are using your own power supply, do the following:

1. With the power supply off or unplugged, connect the + (positive) lead from the power supply (normally red) to the + (positive) terminal on the power connector.

CAUTION: Reversing wire polarity may cause damage to your *groov* Box. This damage is not covered by Opto 22's warranty. If you are not certain about the polarity of the wires on your power supply, check with a meter.

2. Connect the COM wire from the power supply (normally black) to the – (negative) terminal on the power connector.
3. Plug the power supply into a standard 120 or 240 VAC outlet.

STEP 6. TURN ON THE *groov* BOX

Firmly press the On/Off button only until the SYS LED lights up (in about one second), then release. Take a look at the LNK ACT light for ETH0; if the cable is properly connected, the LNK ACT light should be on or blinking.

STEP 7. ACTIVATE THE GROOV BOX AND GET THE LICENSE FILE



CAUTION: If you press the button for longer than eight seconds, the groov Box will be reset to default settings. Your project and all passwords will be erased.

NOTE: Always wait until the SYS LED has stopped blinking before you try to log into groov. Otherwise, you may not be able to use the hostname to log in. If this happens, see [page 102](#).

STEP 7. ACTIVATE THE *groov* BOX AND GET THE LICENSE FILE

1. Open a web browser. Log into manage.groov.com using your email address and your My.Opto22 password.

You may have set up your free My.Opto22 account when you purchased your *groov* Box. If you don't have a My.Opto22 account, enter your email address and other information, and the account will be created.

Manage groov

What would you like to do?

Activate a new *groov* product, option, or training

- > *groov* EPIC
- > *groov* Box Edge Appliance
- > *groov* Server for Windows
- > License or maintenance renewal
- > *groov* EPIC Premium Factory Training

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

ACTIVATE

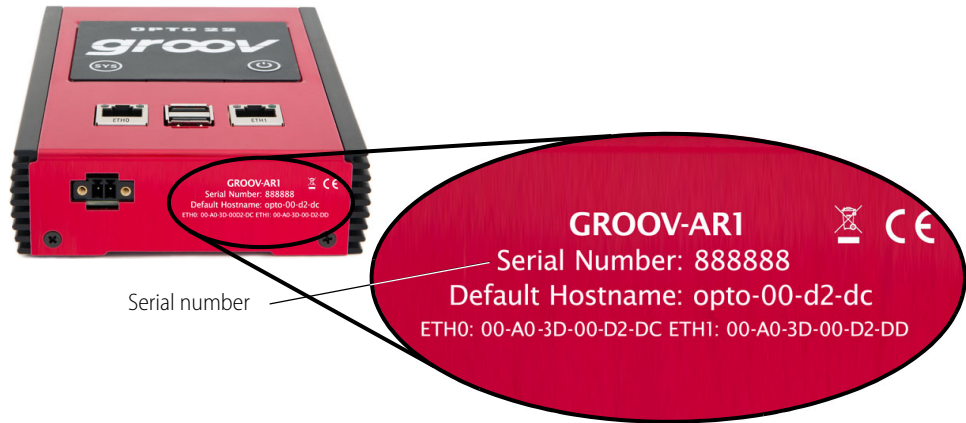
Manage existing *groov* products

- > Complete your activation by adding a MAC address or serial number
- > Get *groov* updates and see the latest README files
- > Download your license file
- > Change or cancel your *groov* EPIC Premium Factory Training class
- > Manage your *groov* maintenance
- > See all your *groov* products in one place
- > Transfer a *groov* product to someone else

MANAGE

2. Click the Activate button.
3. Follow the on-screen instructions to activate your *groov* Box.

The activation key is printed on the activation key certificate included with the *groov* Box. When asked to enter the serial number, you'll find it on the label on the bottom of the device.



4. If you also purchased a *groov* Edge license for OPC UA or MQTT use, activate the Edge license in the same way, applying it to the *groov* Box.
5. From the *groov* Profile page, click the Download license file button and save the file to your computer. If you activated an Edge license, copy the license number and save it.
6. After activating the *groov* Box and downloading the license file, return to this guide and continue with step 8.

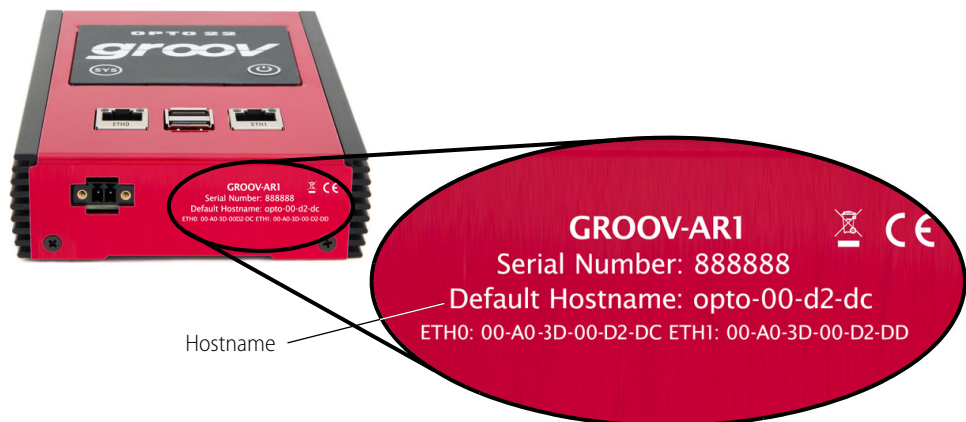
STEP 8. OPEN *groov* VIEW

In most cases you'll open *groov* View using your web browser. If your network does not have DNS, use *groov* Find from a Windows computer (see [page 14](#)).

Opening *groov* View using your web browser

1. Make sure the SYS LED on the *groov* Box has stopped blinking.
2. On your computer, open a web browser (like Firefox, Chrome, Safari, Edge, or Internet Explorer 11).
3. Enter `https://` and your *groov* Box's hostname as the URL. The hostname is printed on the bottom of the *groov* Box.

For example, if the hostname is `opto-00-d2-dc`, you type
`https://opto-00-d2-dc`



Make sure you type `https`. The **s** indicates it is a secure (encrypted) connection.

STEP 8. OPEN GROOV VIEW

NOTE: If you've assigned a static IP address to the groov Box, or if your network doesn't provide DHCP and DNS services, use the IP address instead of the hostname to open groov View.

4. Accept the security warning as described below.



For Chrome:

- Click "Advanced" to expand the initial screen.
- Click "Proceed to <hostname> (unsafe)."



For Firefox:

- Expand "I Understand the Risks."
- Click Add Exception to open the Add Security Exception dialog box.
- Select "Permanently store this exception."
- Click Confirm Security Exception.



For Internet Explorer 10 or newer: Click "Continue to this website (not recommended)."

For Safari: Click Continue.

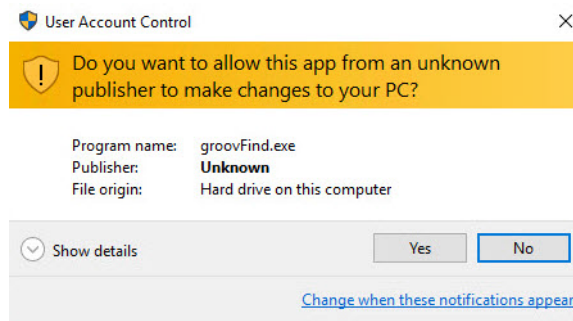
The **Welcome to groov** window opens in your web browser. Now go to ["Step 10. Install the License File" on page 16.](#)

Opening groov View using groov Find

If your network does not have DNS, use a Windows computer with groov Find to locate the groov Box on your network.

1. [Download groov Find from our website](#) (click the link or go to www.opto22.com and search on groov Find). Save the file to your computer.
2. Open the Find application file.

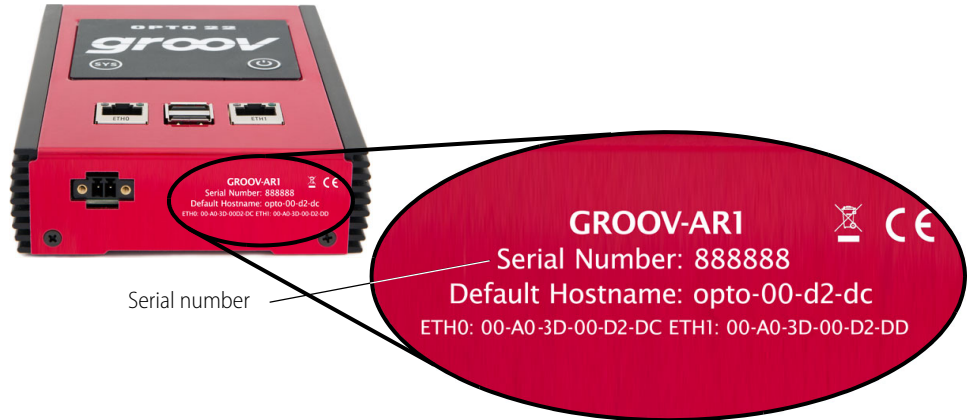
If you have User Account Control (UAC) turned on, a message appears asking if you want Find to be allowed to make changes to your computer.



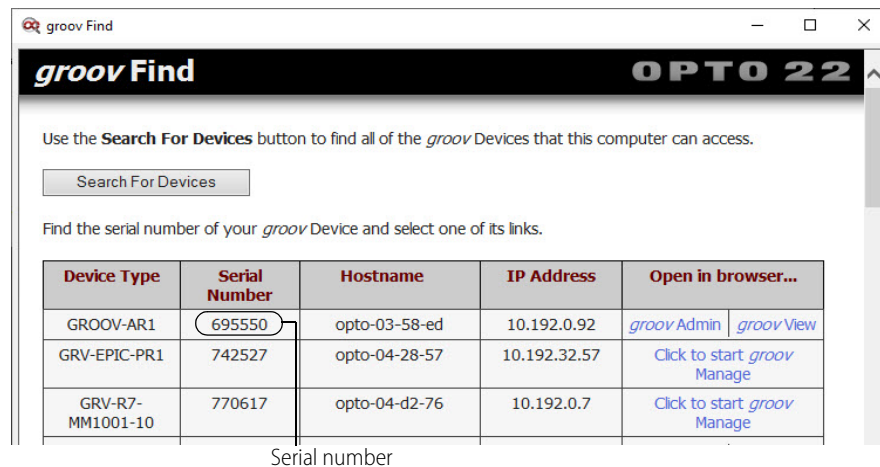
NOTE 1: If you are using a Windows account that does not have Administrator privileges (such as Guest), you will need to enter the Administrator User Name and Password in order to use groov Find. If you do not have this information, contact your IT department.

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. (See ["Assigning a Static IP Address" on page 24.](#)) 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* devices on the network, including *groov* Boxes, *groov* EPICs, and *groov* RIO units.
4. Find the serial number on the bottom of the *groov* Box.



5. Locate the matching serial number in Find.



If you do not see the serial number right away, wait 60 seconds and click Search For Devices.

6. Click the link for *groov* View.
When your browser connects to *groov* View for the first time, the browser will display a *security warning*. This is normal behavior.
7. Accept the security warning as described below.



For Chrome: Click "Proceed anyway."



For Firefox:

- Expand "I Understand the Risks."
- Click Add Exception to open the Add Security Exception dialog box.
- Select "Permanently store this exception."
- Click Confirm Security Exception.

STEP 9. CREATE A GROOV ADMIN ACCOUNT



For Internet Explorer 10 or newer:
Click "Continue to this website (not recommended)."



For Safari: Click Continue.

The **Welcome to *groov*** window opens in your web browser.

STEP 9. CREATE A *groov* ADMIN ACCOUNT

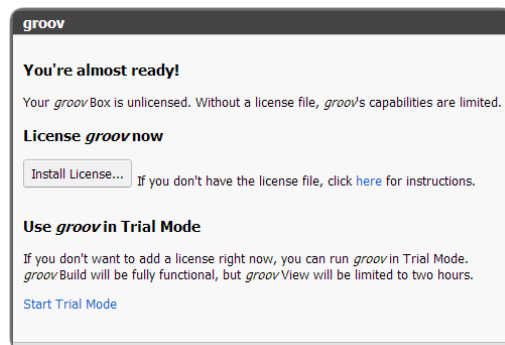
Follow the on-screen instructions to create a username and password for *groov* Admin. (Do not include spaces in the username or password.) The *groov* Admin account is for administrative tasks such as changing or editing the network connections and updating the *groov* Box. (You will create a different account for your *groov* View project.)

CAUTION: Write down your Username and Password, and keep them in a safe place. You will need this information each time you log in. If you lose your login information, you will have to reset the *groov* Box to factory defaults, which will erase your project. For security, there is **no password recovery** option.

STEP 10. INSTALL THE LICENSE FILE

Make sure to install your license file. Without an installed license, *groov* will work for only two hours.

1. When prompted to add a license file to *groov*, click Install License.



2. Browse to the license file you downloaded in Step 7 (page 12), and then click Open.

Your license is now installed.

STEP 11. CREATE A *groov* VIEW ACCOUNT

A *groov* View account lets you use *groov* View to create, edit, and use an operator interface.. (Remember, your *groov* View account is different from the *groov* Admin account you created in Step 9.)

1. When prompted, enter a new username and password. Enter the password again to confirm.

IMPORTANT: Remember your username and password! There is no way to recover it if you lose it.

2. Click Create *groov* View Account.
3. Click Go to Build mode. Build mode opens in your browser.

If you have any trouble opening *groov* View, see Troubleshooting in the [groov View User's Guide, form 2027](#). To create and view your mobile operator interface, see instructions in the [groov View User's Guide](#).

3: Using *groov* Admin

With *groov* Admin, you can back up and restore your projects and project settings, update software and firmware, set up wired and wireless networking, and more.

In this chapter:

Opening <i>groov</i> Admin.....	17
Quick Start menu	21
Opening <i>groov</i> View from <i>groov</i> Admin	21
Opening Node-RED Admin from <i>groov</i> Admin	22
Opening Ignition Edge from <i>groov</i> Admin	22
Configuring Ignition Edge.....	23
Configuring Network Connections.....	23
Updating <i>groov</i> View.....	30
Backing Up <i>groov</i> View and Network Settings.....	32
Restoring <i>groov</i> View and Network Settings.....	33
Updating <i>groov</i> Admin	34
Updating Node-RED	36
Restarting the <i>groov</i> Box	36
Changing Username and Password.....	37
Checking System Information.....	39
Checking Hardware Status.....	40
Setting the System Time.....	41

OPENING *groov* ADMIN

You can open *groov* Admin in three ways:

- From Build mode—see below
- Using the *groov* Admin URL—[page 17](#)
- From *groov* Find (only on a Windows computer)—[page 18](#)

Open *groov* Admin from Build mode

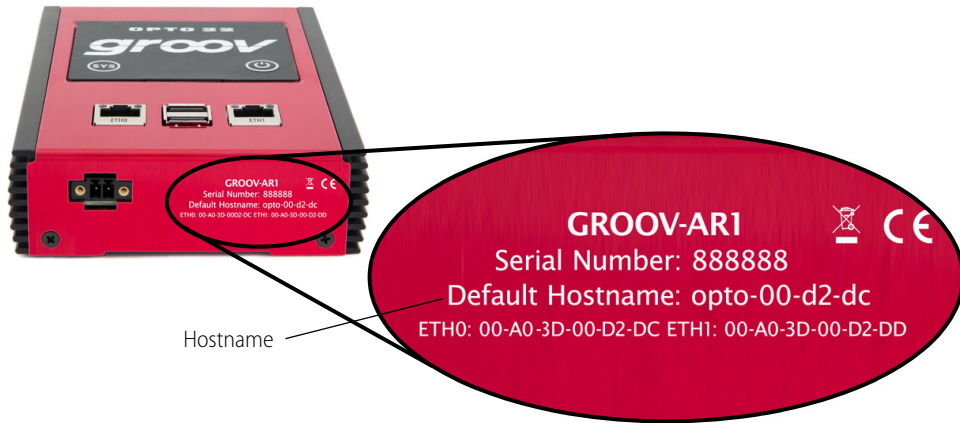
In Build mode, choose Configure > *groov* Admin. To log in, see [page 20](#).

Open *groov* Admin using the URL

1. In your web browser, enter `https://hostname:10000`

For example:

`https://opto-00-d2-dc:10000/`
 hostname port 10000



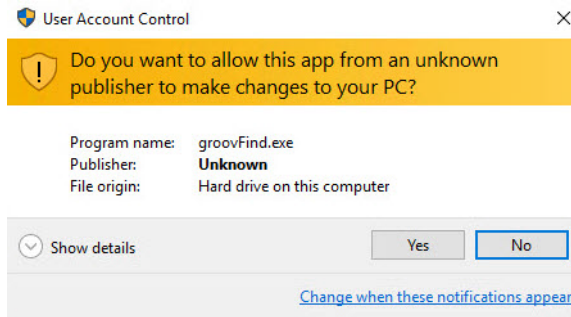
2. When groov Admin opens, log in (see [page 20](#)).

Open groov Admin using groov Find (Windows only)

groov Find is a utility that locates your groov Box on the network and provides a link so that you can access the groov applications. It is useful if you have multiple groov Boxes, because it finds and lists them all. (It also finds all groov EPICs and groov RIO units.) You can easily switch from one Box to another, for example when updating.

NOTE: You need to have Administrator privileges on your Windows account to use groov Find. If you do not have this information, contact your IT department.

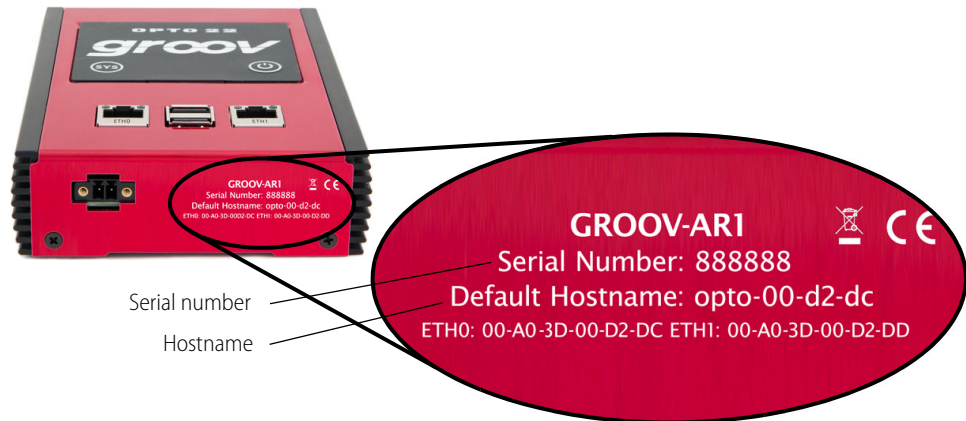
1. [Download groov Find from our website](#) (go to www.opto22.com and search on groov Find). Save the file to your computer.
2. Open the Find application file.
 If you have User Account Control (UAC) turned on, a message appears asking if you want Find to be allowed to make changes to your computer.



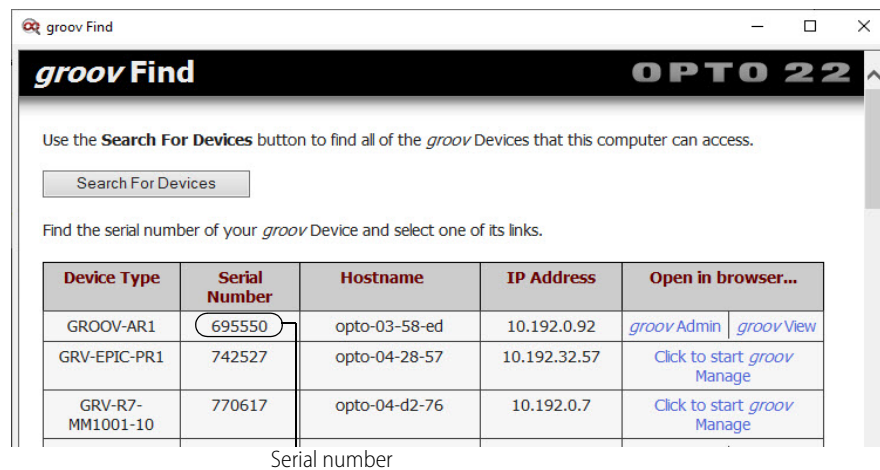
NOTE 1: If you are using a Windows account that does not have Administrator privileges (such as Guest), you will need to enter the Administrator User Name and Password.

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 Box in order to maintain communication. (See “Assigning a Static IP Address” on page 24.) 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 devices on the network.
4. Locate the serial number on the bottom of the groov Box.



5. Locate the matching serial number in Find.



If you do not see the serial number right away, wait 60 seconds and click Search For Devices.

6. Click the groov Admin link. (If it isn't there, click the link “Click to start groov” to start the initial setup on the groov Box. See “Step 8. Open groov View” on page 13.)
A security warning appears in your web browser.
7. Accept the security warning (if you need help, see the next section).
8. Log in (see page 20).

Accept the Security Warning

groov uses the TLS/SSL (Transport Layer Security/Secure Sockets Layer) to protect your data by encrypting data exchanged between your browser and the *groov* Box. When a computer or mobile device attempts to access *groov*, your browser will issue a security warning unless the appropriate SSL security certificate is installed on the device.

If your computer resides in the same domain as the *groov* Box, you can safely accept the warning because your data is protected by the 256-bit encryption. However, if you want to avoid seeing the security warning, you can install the self-signed certificate on your computer and other devices that access *groov*. See [“Using a Self-Signed Certificate” on page 90](#).

If your computer or other device will access *groov* from outside *groov*’s network or over the Internet, Opto 22 strongly recommends you obtain an SSL Certificate from a third-party company that is authorized to confirm your user’s ID. See [“Using a CA-Signed Certificate on the *groov* Box” on page 95](#).

To accept the security warning, see the section below for your browser.

For Chrome

- Click “Advanced” to expand the initial screen.
- Click “Proceed to <hostname> (unsafe).”

For Firefox

1. Expand “I Understand the Risks.”
2. Click Add Exception to open the Add Security Exception dialog box.
3. Select Permanently store this exception.
4. Click Confirm Security Exception.

For Safari

Click Continue.

For Internet Explorer

Click “Continue to this website (not recommended).”

Log in

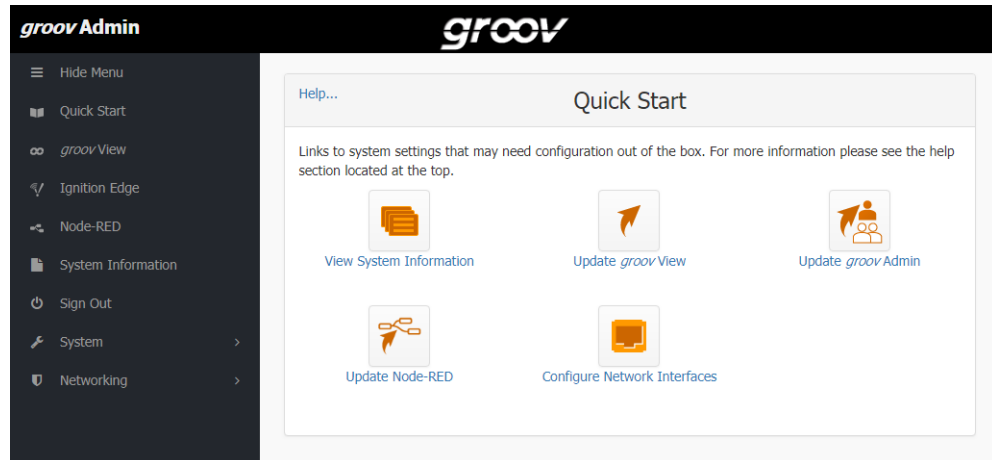
CAUTION: There is no password recovery option. Write down your Username and Password, and keep it in a safe place. You will need this information each time you log in. If you lose your login information, you will have to reset the *groov* Box back to factory defaults, which will erase your project.

1. Enter the *groov* Admin account Username and Password.
2. Click Sign in to open *groov* Admin.

NOTE: There is a session timer of 10 minutes. If you don't do anything for 10 minutes, you will be logged out and have to log in again.

QUICK START MENU

groov Admin opens at the Quick Start menu.



The quick start buttons take you directly to some of the more common actions in *groov* Admin.



View System Information

Check system information and see usage statistics. [“Checking System Information” on page 39.](#)



Update *groov* View

Update *groov* View. See [“Updating groov View” on page 30.](#)



Update *groov* Admin

Update *groov* Admin itself with the latest version. See [“Updating groov Admin” on page 34.](#)



Update Node-RED

Update Node-RED software running on the *groov* Box. See [“Updating Node-RED” on page 36.](#)



Configure Network Interfaces

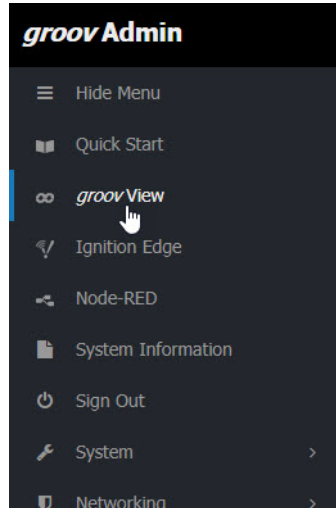
Configure IP settings for the wired and optional wireless Ethernet interfaces: ETH0, ETH1, and WLAN0. See [“Configuring Network Connections” on page 23.](#)

To return to the Quick Start menu, in the left navigation bar, click Quick Start.

OPENING *groov* VIEW FROM *groov* ADMIN

To go to *groov* View, in the left navigation bar, click *groov* View.

OPENING NODE-RED ADMIN FROM GROOV ADMIN

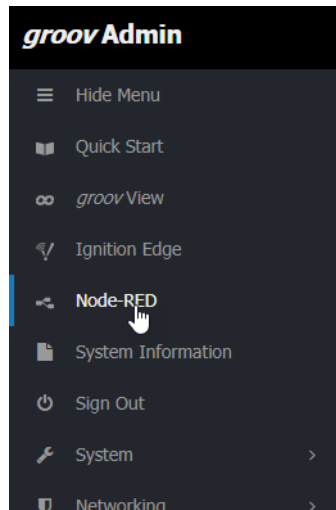


Your *groov* project opens in *groov* View. To get to Build mode, in View click the gear icon in the upper right and choose Switch to Build mode.

For information on using *groov* View, see [form 2027](#), the *groov* View User's Guide.

OPENING NODE-RED ADMIN FROM *groov* ADMIN

To go to Node-RED Admin (or Node-RED), in the left navigation bar, click Node-RED.

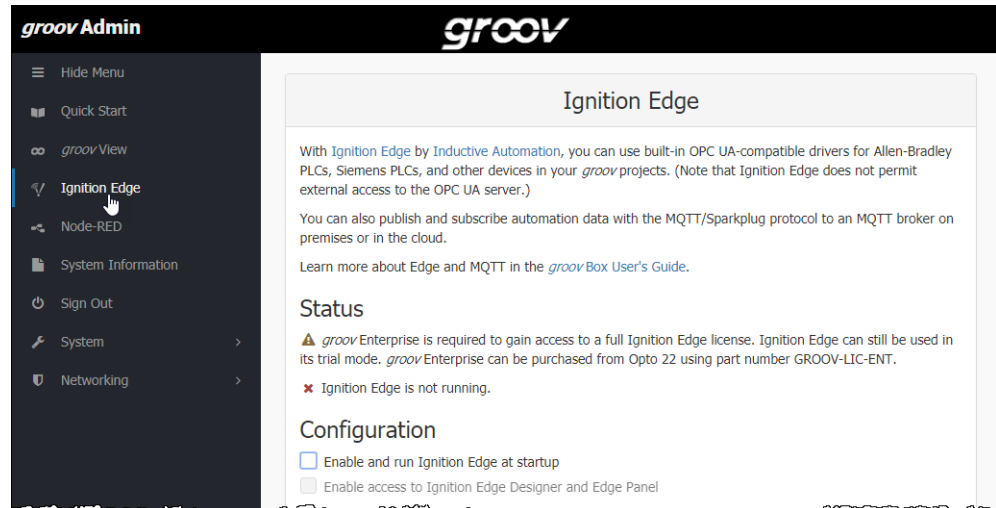


Node-RED Admin opens. You'll need to log in; use your *groov* Admin username and password.

For more information on Node-RED and Node-RED Admin, see [Chapter 4: Using Node-RED](#).

OPENING IGNITION EDGE FROM *groov* ADMIN

1. To go to Ignition Edge, in the left navigation bar, click Ignition Edge.



2. If Edge is already running, click Open Ignition Edge.
3. If Edge is not running, check Enable and run Ignition Edge. Wait for the message that all changes are done, and then click Back. Return to the screen shown above and click Open Ignition Edge.

For more information, see [Chapter 5: Using Ignition Edge](#).

CONFIGURING IGNITION EDGE

See the following sections for more information about configuring Ignition Edge:

- ["License Ignition Edge" on page 76](#)
- ["Use Ignition Edge Designer or Edge Panel" on page 82.](#)

CONFIGURING NETWORK CONNECTIONS

groov is designed to work with a network that has a Dynamic Host Configuration Protocol (DHCP) server and a Domain Name Server (DNS). If your network has DHCP and DNS, you do not need to assign an IP address to the *groov* Box; you just plug it in and the IP address is assigned automatically. This is the recommended method for setting up the *groov* Box.

However, if you need to customize your network connections for *groov* after the initial setup, *groov* Admin provides the tools to do that.

This section includes the following topics:

- ["Assigning a Static IP Address" on page 24](#)
- ["Changing the Hostname, DNS Servers, or IPv4 Gateway" on page 25](#)
- ["Configuring ETH1 for the Control Network" on page 25](#)
- ["Configuring Wireless Communications" on page 26](#)
- ["Using an AR1 as a Wireless Access Point" on page 29](#)

To set up your network, see form 2161, the [Guide to Networking groov](#). This guide provides detailed information on how to make your *groov* network more secure. It also describes how to directly communicate with *groov* over the Internet using a virtual private network (VPN) or with port forwarding (PF). A VPN is recommended because it is more secure.

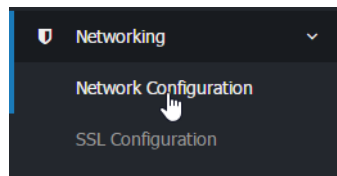
Assigning a Static IP Address

If you do not have a DHCP server, you'll need to configure a static address to either ETH0 or ETH1. Otherwise there may be communication errors.

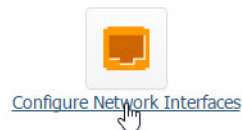
NOTE: If you are using a laptop computer to assign a static IP address, make sure you disable Windows' Internet Connection Sharing (ICS). If you don't, the laptop will act like a DHCP server and assign a dynamic address.

You'll need to get the following networking information from your IT department:

- **IPv4 address**—A unique, fixed (static) IP address.
For example: 172.18.234.1
 - **Netmask**—Identifies the subnetwork.
For example: 255.255.0.0
 - **Gateway** (optional)—Identifies the route to the Internet.
For example: 172.18.1.1
1. In the left navigation bar choose Networking > Network Configuration, or click the Configure Network Interfaces button in Quick Start.



OR:



2. Click the wired Ethernet connection you want to configure.

NOTE: Use ETH0 as the main network connection. Only use ETH1 if you have segmented networks.

 The image shows two parts of the network configuration interface. The top part is a table titled 'Network Configuration' with columns: Name, Type, MAC Address, IPv4 Address, Netmask, IP Configuration, and Link Status. The bottom part is the 'Edit Interface' form for the selected interface.

Name	Type	MAC Address	IPv4 Address	Netmask	IP Configuration	Link Status
ETH0	Ethernet	00:A0:3D:00:D2:DC	10.192.0.235	255.255.192.0	From DHCP	Up
ETH1	Ethernet	00:A0:3D:00:D2:DD	None	None	From DHCP	Down
WLAN0	Wireless Ethernet	Unknown	None	None	Disabled	No adapter found

 The 'Edit Interface' form shows 'Boot Time Interface Parameters' for the selected interface 'ETH0'. It has three radio buttons: 'Disabled', 'From DHCP' (which is selected), and 'Static configuration'. To the right of these are input fields for 'IPv4 Address' and 'Netmask'. A red arrow points from the 'ETH0' row in the table to the 'Edit Interface' form. A label 'Static IP address' points to the 'IPv4 Address' input field.

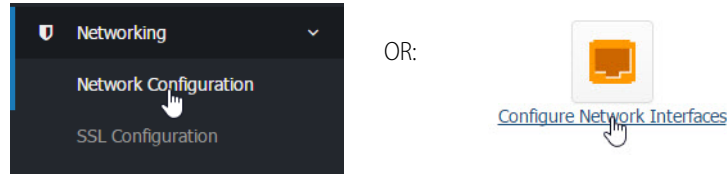
3. Select Static configuration. Enter the static IP Address and Netmask.
4. Click Save.

Changing the Hostname, DNS Servers, or IPv4 Gateway

In order to identify the *groov* Box more easily on the network, you might want to change the hostname from the default. And, depending on your network setup, you might need to change the DNS Servers or IPv4 Gateway.

NOTE: Keep in mind that any changes to this interface may make your system inaccessible via your current wired or wireless connection. Be sure to write down the new hostname or other changes.

1. In the left navigation bar choose Networking > Network Configuration, or click the Configure Network Interfaces button in Quick Start.



The Network Configuration page opens.

[Help...](#)

Network Configuration

Name	Type	MAC Address	IPv4 Address	Netmask	IP Configuration	Link Status
ETH0	Ethernet	00:A0:3D:00:D2:DC	10.192.0.235	255.255.192.0	From DHCP	Up
ETH1	Ethernet	00:A0:3D:00:D2:DD	None	None	From DHCP	Down
WLAN0	Wireless Ethernet	Unknown	None	None	Disabled	No adapter found

Client Options

Hostname

☒ Obtain IP address(es) for the DNS server(s) automatically
☐ Use the following IP address(es) for the DNS server(s)

DNS servers

☒ Obtain an IP address for the gateway automatically
☐ Use the following IP address for the gateway

IPv4 Gateway

2. In the Client Options are, change the hostname, DNS servers, or IPv4 Gateway as necessary.

NOTE 1: A hostname cannot have spaces or special characters.

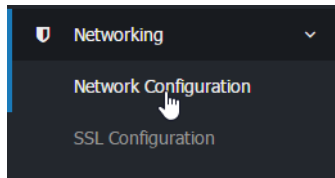
NOTE 2: Any changes to this interface may make your system inaccessible via your current wired or wireless connection. Be sure to write down the new hostname or other changes.

3. Click Save.

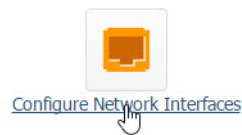
Configuring ETH1 for the Control Network

If your computer is on a different network than the control network, you need to configure ETH1 by assigning it an IP address and subnet appropriate for the control network.

1. In the left navigation bar choose Networking > Network Configuration, or click the Configure Network Interfaces button in Quick Start.



OR:



2. Click ETH1.

Network Configuration				
Name	Type	MAC Address	IPv4 Address	Netmask
ETH0	Ethernet	00:A0:3D:00:D2:DC	10.192.0.235	255.255.192.0
ETH1	Ethernet	00:A0:3D:00:D2:DD	None	None
WLAN	Wireless Ethernet	Unknown	None	None

Edit Interface

Boot Time Interface Parameters

Name

ETH1

☐ Disabled
 ☒ From DHCP
 ☐ Static configuration

IPv4 Address

Netmask

Save

3. If the network has DNS and DHCP, select "From DHCP." If it doesn't, enter a static IP Address and Netmask.

NOTE: If you are using static addresses, ETH1 must be on a different subnet than ETH0.

4. Click Save.

Configuring Wireless Communications

If you want to use your *groov* Box on a wireless network, you must purchase and install a USB WiFi adapter that has been tested and approved by Opto 22. See [Appendix C: Installing an Approved USB WiFi Adapter](#).

You can configure the *groov* Box to connect to a wireless network through an access point using the 802.11b, 802.11g, and 802.11n protocols.

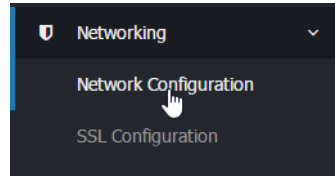
Before you begin, get the following information from your IT Department:

SSID—Name of the wireless network access point you want the *groov* Box to join

Security—Encryption type (WPA or WPA2), network key input type (hex or ASCII), and password

Password—To access the wireless network

1. With the *groov* Box connected via ETH0, in *groov* Admin's left navigation bar choose Networking > Network Configuration, or click the Configure Network Interfaces button in Quick Start.



OR:



2. Click WLAN0.

Name	Type	MAC Address	IPv4 Address	Netmask
ETH0	Ethernet	00:A0:3D:00:D2:DC	10.192.0.235	255.255.192.0
ETH1	Ethernet	00:A0:3D:00:D2:DD	None	None
WLAN0	Wireless Ethernet	Unknown	None	None

Wireless Client

Wireless Access Point

Enter Wireless Network Information

Network Name (SSID)

Encryption Type

None

Network Key Type

ASCII/Passphrase

Network Key

3. Enter the Network Name (SSID).

The SSID is a text string from 1 to 32 characters used to uniquely identify the wireless network. This should match the SSID of the access point you want to connect to.

NOTE: If the SSID contains one or more spaces, enclose the SSID with quotation marks. For example, enter "Opto 22" instead of Opto 22.

4. Select the Encryption Type.

This is the type of encryption used to encrypt any packet sent or received between the access point and the groov Box.

- **None**—No encryption used.
- **WEP64**—Use WEP encryption with a 5 digit ASCII or 10 digit hexadecimal key. WEP has been deprecated by IEEE and should not be used in new installations.
- **WEP128**—Use WEP encryption with a 13 digit ASCII or 26 digit hexadecimal key.

NOTE: WEP is not secure and has been deprecated by the Institute of Electrical and Electronics Engineers (IEEE). Do not use WEP in new installations unless it is the only option available. Use WPA or WPA2 instead.

- **WPA**—Use TKIP encryption (RC4) with an 8 to 63 digit ASCII or 64 digit hexadecimal key.
- **WPA2**—Use CCMP encryption (AES) with an 8 to 63 digit ASCII or 64 digit hexadecimal key.

5. Choose the Network Key Type.

Select ASCII or Hexadecimal keys. Typically, WEP uses hexadecimal keys and WPA uses ASCII keys.

6. Enter the Network Key.
Use the key for the Encryption Type selected above. This is a write-only field.
7. Scroll down to the Boot Time Interface Parameters section.

Boot Time Interface Parameters

Name

WLAN0

☒ Disabled
 ☐ From DHCP
 ☐ Static configuration

IPv4 Address

Netmask

Save

8. Select From DHCP.
If the wireless network does not have a DHCP server, assign a static IP address and netmask.
9. Click Save.
Wait till you see the following message.

Network Configuration

Restarting network services. Please wait...Finished

[Back](#)

Congratulations. You're connected!

10. If ETH0 and WLAN are on the same subnet, disconnect the cable from ETH0.
You need to disable ETH0 because the *groov* Box will continue to communicate over ETH0 as long as it is connected on the same subnet and enabled.

NOTE: If you are using a control network and an enterprise network, and ETH0 is on a different subnet, you can leave it connected.

- a. In the Network Configuration page, click ETH0.

Edit Interface

Boot Time Interface Parameters

Name

ETH0

☐ Disabled
 ☒ From DHCP
 ☐ Static configuration

IPv4 Address

Netmask

Save

- b. Select Disabled, then click Save.

- c. Click the Back button, and notice that in the Network Configuration page, ETH0 is disabled (Down) and WLAN0 is enabled (Up).

Network Configuration						
Name	Type	MAC Address	IPv4 Address	Netmask	IP Configuration	Link Status
ETH0	Ethernet	00:A0:3D:00:D2:DC	10.192.0.235	255.255.192.0	From DHCP	Down
ETH1	Ethernet	00:A0:3D:00:D2:DD	None	None	From DHCP	Down
WLAN0	Wireless Ethernet	Unknown	None	None	Disabled	Up

Using an AR1 as a Wireless Access Point

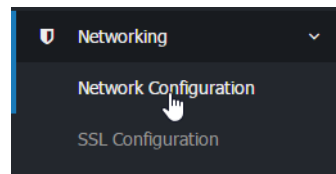
groov's SoftAP (Software Access Point) feature allows you to use your *groov* Box as an access point in order to create a private wireless network with WPA2-PSK security. This is particularly useful for connecting a phone or tablet to the *groov* Box when there is no other wireless network available. SoftAP can be used by any WiFi-capable device. Your *groov* Box can be connected to either a wireless or Ethernet network.

In order to use SoftAP, you will need one of the following WiFi adapters:

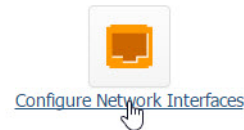
- Netis WF2119S
- Netis WF2116

These are the *only* WiFi adapters tested and approved for this feature.

1. Follow the instructions on [page 113](#) to install your Netis WiFi adapter.
2. With the *groov* Box connected via ETH0, in *groov* Admin's left navigation bar choose Networking > Network Configuration, or click the Configure Network Interfaces button in Quick Start.



OR:



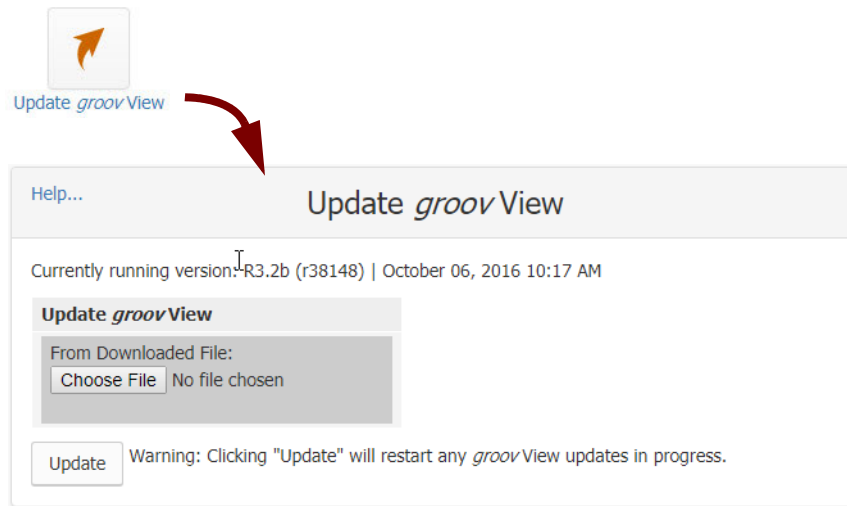
3. In the Network Configuration page, click WLAN0.
4. Scroll down to Boot Time Interface Parameters and make sure that WLAN0 is Disabled.
5. Scroll back up and click the Wireless Access Point tab.

6. Next to **Enable?**, choose Yes.
7. Edit the following parameters as necessary:
 - **Static IPv4 Address**—Use an IP address that is not on the same subnet as ETH0 or ETH1.
 - **Network Name (SSID)**—Enter a name between 1 and 32 characters.
 - **Network Key**—Enter a key between 8 and 63 characters.
 - **Channel**—The WiFi Channel should be between 1 and 14, depending on the geographic region. Click *Execute WiFi Sight Survey* to display a table of detectable WiFi access points and populate the Channel field with the quietest channel available.
8. Click Save.

Now you're ready to connect your wireless device to your new wireless network using the Network Name and Network Key. For information about using a mobile device with *groov*, see form 2105, the [Setting Up groov Mobile Apps Technical Note](#).

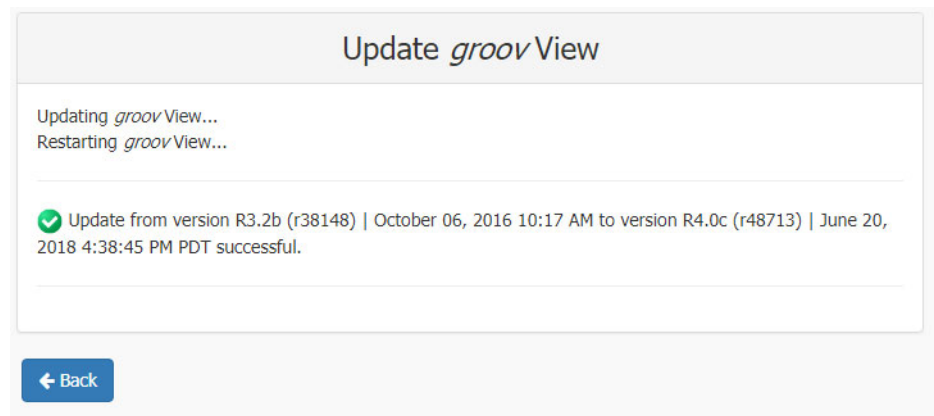
UPDATING *groov* VIEW

1. Before updating *groov* View, back up your project (see [page 32](#)).
2. Make sure the *groov* Box is activated. See “[Step 7. Activate the groov Box and Get the License File](#)” on [page 12](#).
3. Go to manage.groov.com and follow directions to download the latest *groov* View update file and save it to your computer.
4. Open *groov* Admin.
5. Click Quick Start and then the Update *groov* View button.



6. Click Choose File, navigate to the update file you downloaded, and then click Open.
7. Click Update.

Wait while the application is installed and restarted automatically, which may take several minutes. When the operation is complete, a success message appears.



BACKING UP *groov* VIEW AND NETWORK SETTINGS

During backup, project components are saved to a file on your computer or a USB flash drive. You should back up *groov* View frequently. There is no automatic backup.

NOTE: To back up Node-RED, see [page 57](#).

To back up Ignition Edge, see [page 81](#).

groov View project backups are interchangeable among the *groov* Box, *groov* EPIC, and *groov* Server. So you can restore to *groov* EPIC a project you backed up from a *groov* Box, and vice versa.

If you have two *groov* Boxes, EPICs, or Servers at different versions of *groov* View and you want to move a project to the older version, it will usually work only between lettered versions. For example, moving a project from a product running *groov* View at R3.3b to one running *groov* View at R3.3a should be OK, but moving from R3.3 to R3.2 is not likely to work. As much as possible, it's safest to keep your *groov* products at the same release.

To restore from the backup file, see “[Restoring *groov* View and Network Settings](#)” on [page 33](#).

IMPORTANT: Your *groov* View project files are not encrypted or masked in any way. This means that most of the project information in them (except for the *groov* View user passwords) can be read, including the following:

- SMTP account info (including password)
- User email accounts (does not include the *groov* View user passwords, which are securely encrypted before being stored)
- Device addresses
- Tag address information (PAC tag names, Modbus addresses, OPC node-id, etc.)

Opto 22 recommends that you secure your backup files using file- or disk-based encryption provided either by the operating system or other software/hardware.

Also, be aware that if you send project files to Opto 22, our personnel will have access to the information listed above.



USB connectors for backing up and restoring using a flash drive

Follow these steps to back up:

1. In the left navigation bar, choose System > Backup and Restore.

Help...

Backup/Restore

Back up

Restore

Back up groov components.

Node-RED flows are backed up using Node-RED Admin. [Go to Node-RED Admin](#)

Select Components

1. Select which components you want to back up. When you restore, you can choose which components to restore

☐ groov (Build, View, project)

☐ Ethernet/Wireless Settings

2. Select how you want to save your backup. To save to a flash drive, first insert the drive into a USB slot on the front of the *groov* Box.

☒ Download to PC ☐ Save to USB Flash Drive

Back up

2. Click the Back up tab.
3. Select the components you want to back up.
groov (Build, View, projects) saves *groov* View, Build mode, and your project.
Ethernet/Wireless Settings saves any settings you've configured for ETH0, ETH1, and the wireless network, including IP, Subnet, Gateway, Hostname, SSID, Wireless Network Key, etc.
4. Do one of the following:
 - Select Download to PC.
 - Insert a USB drive into a USB slot on the front of the *groov* Box. Select Save to USB Flash Drive. (The option is not available until you insert the USB drive. If necessary, refresh the page.)
5. Click Back up.
 - If saving to the PC, save the file (don't open it).
 The backup file is downloaded to your computer; wait for it to finish.
 - If saving to a USB flash drive, the file is downloaded to your USB drive. When you see the prompt to Eject the USB drive, click Eject. Wait for the prompt that says it's OK to remove the flash drive before you take it out of the *groov* Box.

RESTORING *groov* VIEW AND NETWORK SETTINGS

Use the following instructions to restore *groov* View components and network settings from a backup file saved on a computer or USB flash drive (see “[Backing Up groov View and Network Settings](#)” on page 32).

NOTE: To restore Node-RED, see [page 57](#). To restore Ignition Edge, see [page 81](#).

1. In the menu tree, click System, and then click Backup and Restore.

Help... Backup/Restore

Back up Restore

Back up groov components.

Node-RED flows are backed up using Node-RED Admin. [Go to Node-RED Admin](#)

Select Components

1. Select which components you want to back up. When you restore, you can choose which components to restore

☐ *groov* (Build, View, project)

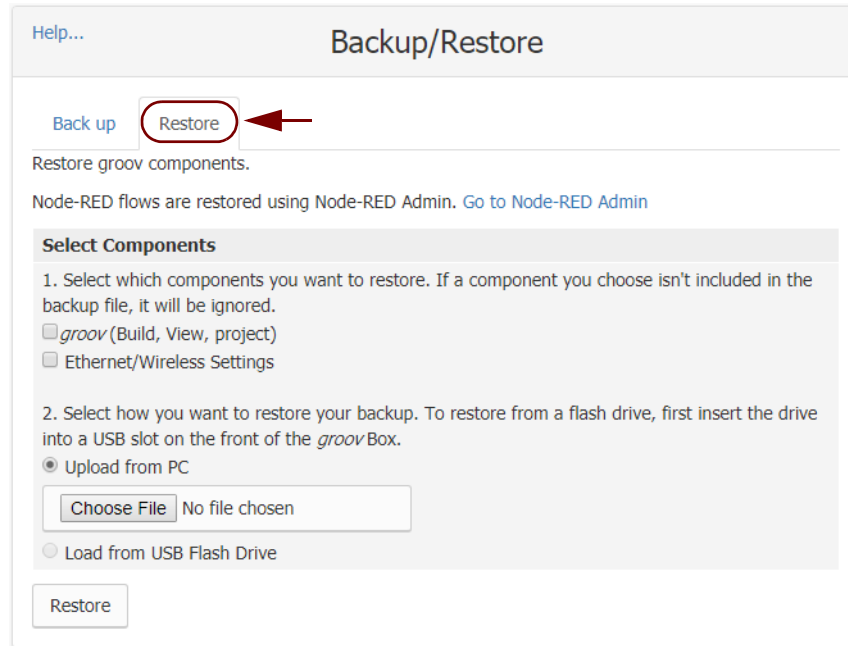
☐ Ethernet/Wireless Settings

2. Select how you want to save your backup. To save to a flash drive, first insert the drive into a USB slot on the front of the *groov* Box.

☒ Download to PC ☐ Save to USB Flash Drive

Back up

2. Click the Restore tab.



3. Select the components you want to restore. If you choose a component that isn't included in the backup file, it won't be restored.
groov (Build, View, projects) restores the *groov* View software and the project you built in *groov* View.
Ethernet/Wireless Settings restores any settings you've configured for ETH0, ETH1, and the wireless network, including IP, Subnet, Gateway, Hostname, SSID, Wireless Network Key, etc.
4. Do one of the following:
 - To restore from your PC, select Upload from PC, then click Choose File and locate your backup file.
 - To restore from a USB flash drive, insert the drive with the backup file into a slot on the front of the *groov* Box. (The option is not available until you insert the USB drive. If necessary, refresh the page.) Click Load from USB Flash Drive, then click the browse button and select your backup file.
5. Click Restore, and then wait while the files are uploaded. It may take several minutes.

UPDATING *groov* ADMIN

When you update *groov* Admin, your *groov* View configuration settings are kept. Updates for Ignition Edge software are included in *groov* Admin updates.

1. **IMPORTANT:** If you are using Ignition Edge, before you update *groov* Admin, do two things:
 - a. Back up your Ignition Edge project following the steps on [page 81](#).
 - b. Deactivate your Ignition Edge license following the steps in "[Unactivate Ignition Edge license](#)" on [page 80](#).
2. Log into manage.groov.com, click Manage, locate your *groov* Box in the list, and click Manage.
3. In Latest Releases, click the Filename for *groov* Admin to download and save the latest *groov* Admin update file to your computer.
4. If the Quick Start menu is not open, in the left navigation bar, click Quick Start.

Update *groov* Admin

5. Click Update *groov* Admin.

[Help...](#)

Update *groov* Admin

Update *groov* Admin

Currently running version: 1.570.43

When you update *groov* Admin, All of your configuration settings are kept

To get the update file, go to manage.groov.com. Follow directions and save the *groov* Admin update file to your computer.

Update *groov* Admin

From file:

No file chosen

6. Click Choose File and locate the update file you downloaded. Highlight the file, and click Open.
7. Click Update.

The application file is downloaded and installed. **The update process may take several minutes.** It may not look like anything is happening, but it is. A small note in the lower-left corner of the screen shows progress while the file is loaded to the *groov* Box. Be patient and don't click away from this page until you see the success message.

NOTE: If you have reset your groov Box to factory defaults and your original groov Admin version is 1.570.41 or lower, your Update groov Admin page may become blank for awhile and later show an "updating" message. Continue to wait. It can take as long as 15 minutes to completely update on an older Box.

Update *groov* Admin

Updating *groov* Admin... Success.

System restart required for updates to take affect. [Click here to restart now.](#)

[Back](#)

NOTE: Your groov Box must be restarted for the update to take effect. While the groov Box is restarting, all of your users will be disconnected, and you will not be able to continue working in groov View.

8. When the success message appears, click "Click here to restart now" or click Back to restart later. (To restart later, see "[Restarting the groov Box](#)" on page 36.) Wait while it restarts, which may take several minutes.

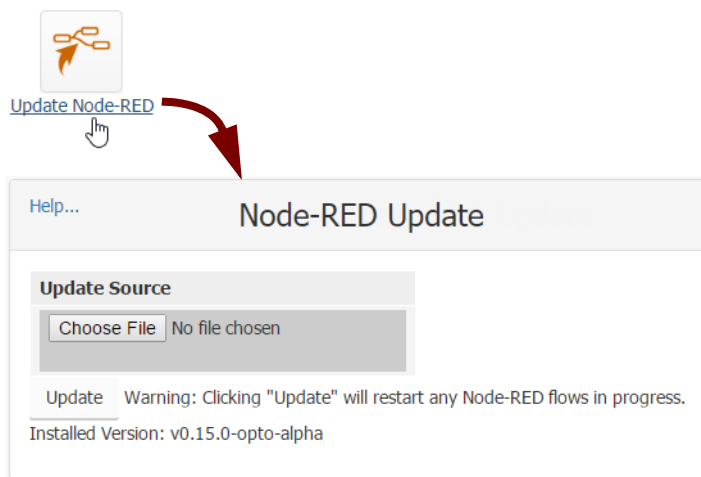
During the restart, if you can see the *groov* Box, you'll notice its LED lights go off and then come back on, and the SYS LED flash in different colors. Wait until the SYS LED has completely stopped flashing. At that point the *groov* Box has fully restarted, and you and your users will be able to use *groov* View.

9. Refresh the page to see the new *groov* Admin version.

10. If you are using Ignition Edge, restore your Edge project following steps on [page 82](#), and reactivate your license as shown in [“License Ignition Edge” on page 76](#).

UPDATING NODE-RED

1. Before updating, back up your Node-RED project using Node-RED Admin (see [“Backing up and restoring your Node-RED project” on page 57](#)).
2. Log into [manage.groov.com](#), click Manage, locate your *groov* Box in the list, and click Manage.
3. In Latest Releases, click the Filename for Node-RED to download and save the latest Node-RED update file to your computer.
4. Open *groov* Admin.
5. Click Quick Start and then the Update Node-RED button.



6. Click Choose File, navigate to the update file you downloaded, and then click Update. Wait while Node-RED is updated, which may take several minutes.
The *groov* Box must be restarted in order for updates to take effect. While it is restarting, all users are disconnected, and you won't be able to work in *groov* View.
7. To restart, click the message “Click here to restart now.” Wait until the Box is fully restarted before continuing.
If you can see the *groov* Box, you'll see its LED lights go off and then come back on, and the SYS LED flash in different colors. Wait until the SYS LED has completely stopped flashing. At that point the *groov* Box has fully restarted, and you and your users will be able to use *groov* View.

RESTARTING THE *groov* BOX

While the *groov* Box is restarting, all users are disconnected, and you won't be able to continue working in *groov* View. The *groov* Box must be restarted in order for updates to take effect.

To restart the *groov* Box, do one of the following:

- **After updating** *groov* Admin, click the message “Click here to restart now.”

Update *groov* Admin

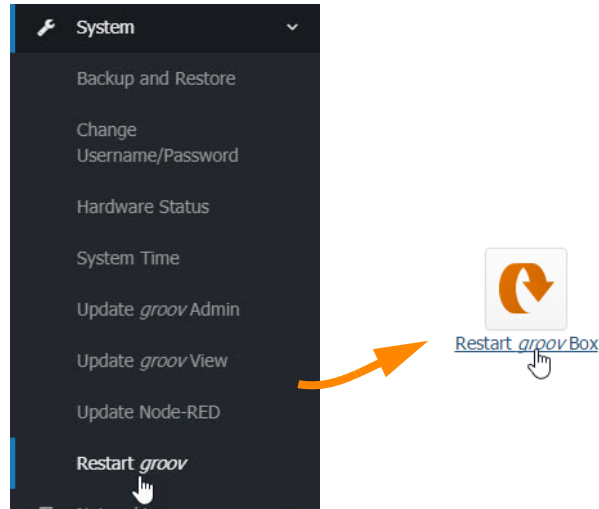
Updating *groov* Admin... Success.



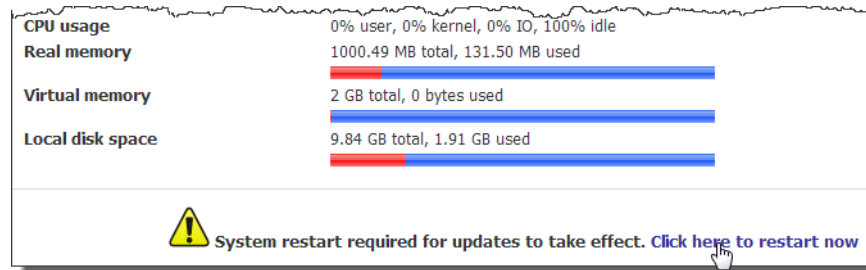
System restart required for updates to take affect. [Click here to restart now.](#)

[Back](#)

- In the left navigation bar, choose System > Restart *groov* and then click the Restart *groov* Box button.



- If you've updated but not restarted the Box, click System Information, and then click "Click here to restart now."



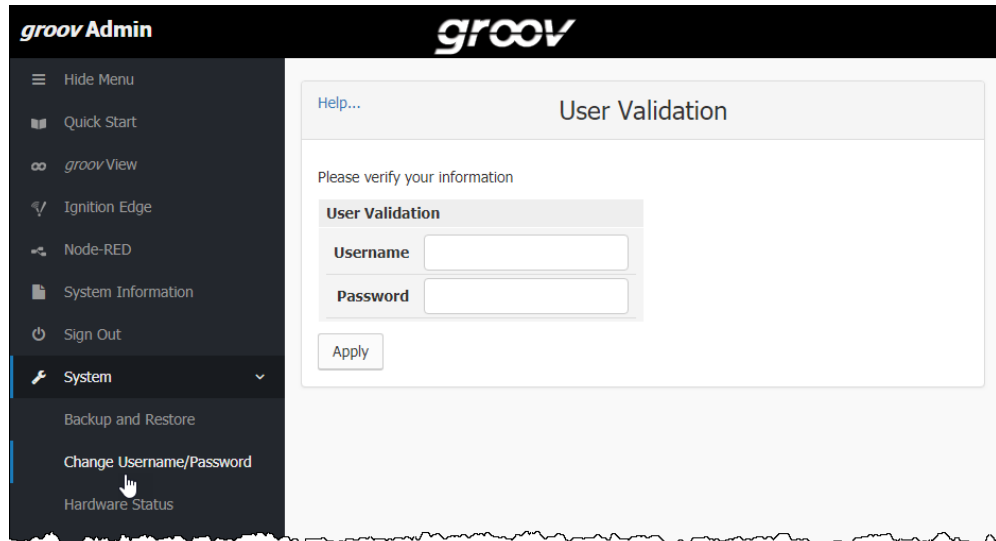
- **Hardware restart:** Press the On/Off button briefly and wait for the *groov* Box to turn off. Then briefly press the On/Off button again to power it back up.

During a restart, if you can see the *groov* Box, you'll notice that its LED lights go off and then come back on. You and your users will be able to use *groov* View once the *groov* Box has fully restarted and the SYS LED has stopped flashing.

CHANGING USERNAME AND PASSWORD

For *groov* Admin there is only one user; you cannot add more than one username. However, you can change the username or password for the *groov* Admin user. This change does not affect any usernames or passwords in *groov* View.

1. In the left navigation bar, choose System > Change Username/Password.



2. Enter your current username and password to verify your identity, and click Apply.

The screenshot shows a dialog box titled 'Change Username/Password for groov Admin'. It includes a 'Help...' link. Below the title, it states: 'After saving, you will be logged out and redirected to the login page.' There is a section 'Currently logged in as: admin' with three input fields: 'Username' (containing 'admin'), 'Password', and 'Confirm Password'. Below these fields, a warning message reads: 'It is **very important** that you protect this account information. Treat it like you would an account for a financial institution. Lost account information **cannot be recovered**.' At the bottom is a 'Save' button.

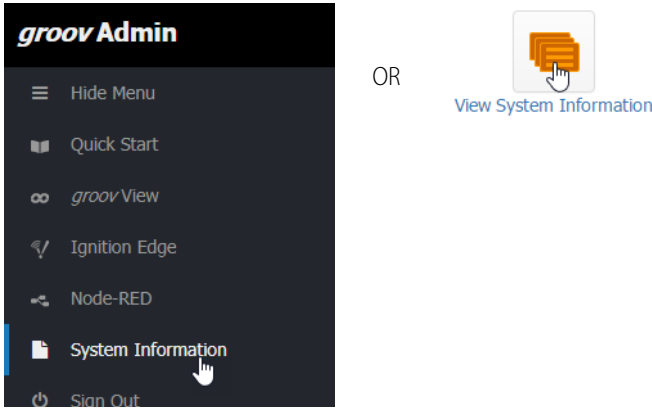
3. Enter the new username and the password in both boxes. Do not include spaces in the username or password.

CAUTION: Write down your new Username and Password, and keep it in a safe place. You will need this information each time you log in. If you lose your login information, you will have to restore the groov Box back to factory defaults, erasing your project. There is no password recovery option.

4. Click Save.
The login dialog box appears.
5. Log in using the new username and password.

CHECKING SYSTEM INFORMATION

In the left navigation bar, choose System Information in the menu tree, or click the System Information icon in Quick Start.



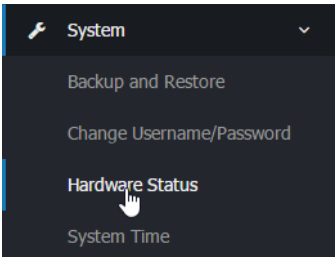
The following information is provided.

System Information

System Hostname	opto-00-00-00
Activation key	4F2FVRYVWQKT-1DEV
groov Serial Number	234567
groov Part Number	GROOV-AR1
groov Image Version	36
groov Admin Version	1.570.50.48435
groovView Version	R3.2b (r38148) October 06, 2016 10:17 AM
Node-RED Update Version	2
Power-Loss Tolerant File System	No
Hardware Date	December 31, 2013
Time on System	Fri Jun 22 17:12:06 2018
System Uptime	1 days, 1 hours, 09 minutes
CPU Load Averages	0.24 (1 min) 0.31 (5 mins) 0.28 (15 mins)
CPU Usage	0% user, 0% kernel, 0% IO, 100% idle
Real Memory	1000.38 MB total, 235.73 MB used
Virtual Memory	2 GB total, 0 bytes used
Local Disk Space	9.84 GB total, 2.28 GB used
SSD FW Version	S9FU02.8
SSD Serial Number	DC11076618EE03130279
SSD Power On Hours	12295
SSD Avg/Max Erase Counts	306/3639

CHECKING HARDWARE STATUS

- 1. To check the status of the internal components in the *groov* Box, in the left navigation bar, choose System > Hardware Status.



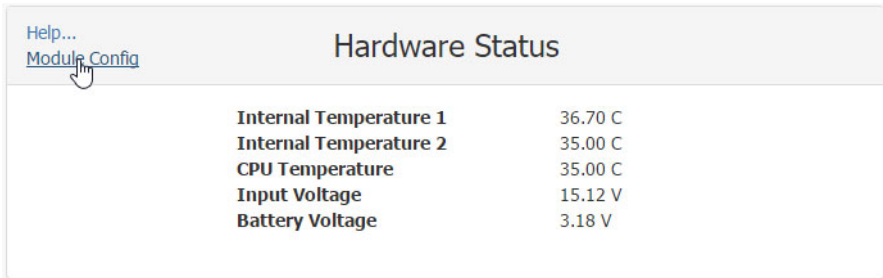
The following information is provided:

Hardware Status	
Internal Temperature 1	36.70 C
Internal Temperature 2	35.00 C
CPU Temperature	35.00 C
Input Voltage	15.12 V
Battery Voltage	3.18 V

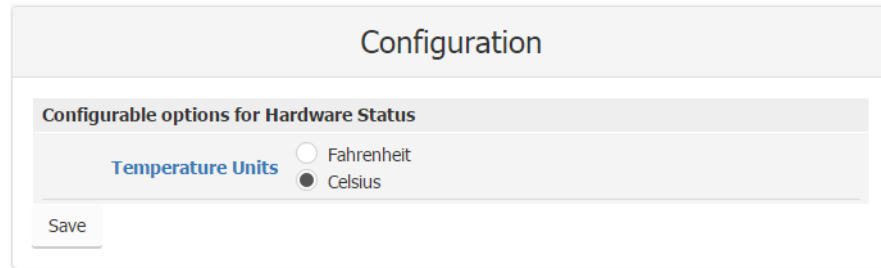
If any value is out of range, it is displayed in red and a message appears. Here are the values:

- Internal Temperature 1: Temperature of the internal PCB located near the battery
- Internal Temperature 2: Temperature of the internal PCB located near the power supply
- CPU Temperature: Temperature of the CPU
- Input Voltage: Main power supply for the *groov* Box
- Battery Voltage: Voltage of the battery that maintains the date and time

- 2. To change the temperature units (Fahrenheit or Celsius) shown in Hardware Status, click Module Config under Help on the left-hand side.



- 3. Select either Fahrenheit or Celsius.



Configuration

Configurable options for Hardware Status

Temperature Units ☐ Fahrenheit ☒ Celsius

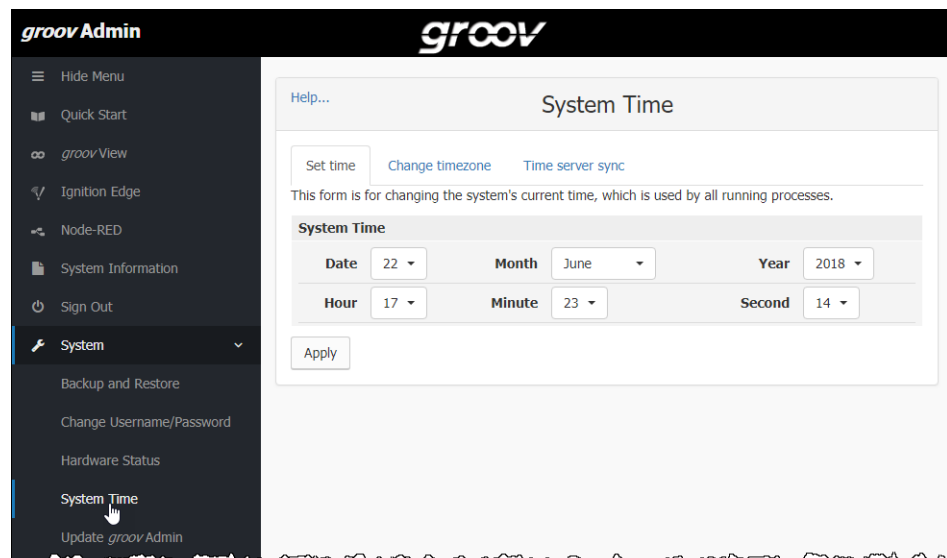
[Save](#)

4. Click Save.

SETTING THE SYSTEM TIME

You can set the time and time zone used by the *groov* Box. You can also set the Box to synchronize with a specific time server.

1. In the left navigation bar, choose System > System Time.



groov Admin **groov**

Help... **System Time**

[Set time](#) [Change timezone](#) [Time server sync](#)

This form is for changing the system's current time, which is used by all running processes.

System Time

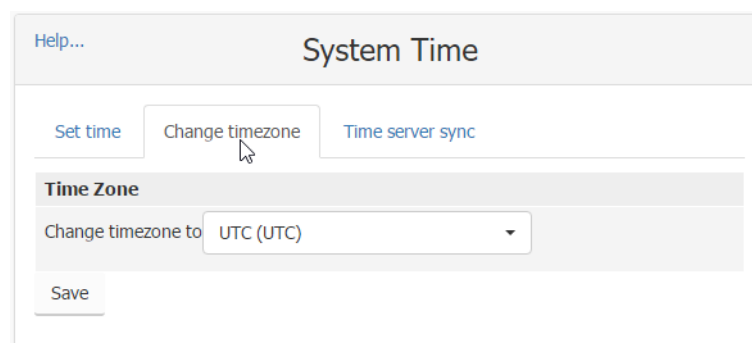
Date	22	Month	June	Year	2018
Hour	17	Minute	23	Second	14

[Apply](#)

System (selected)

- Backup and Restore
- Change Username/Password
- Hardware Status
- System Time**
- Update groov Admin

2. Set the time and date and then click Apply.
3. To change the time zone from the default of UTC (Coordinated Universal Time), click the Change timezone tab.



Help... **System Time**

[Set time](#) [Change timezone](#) [Time server sync](#)

Time Zone

Change timezone to UTC (UTC)

[Save](#)

SETTING THE SYSTEM TIME

4. In the drop-down list, select a time zone, and then click Save. Restart the *groov* Box to use the new time zone.
5. To set up the *groov* Box to automatically synchronize the time with a remote server, click the Time server sync tab.

Synchronization uses the Unix time protocol or NTP, depending on the remote system.

Help... System Time

Set time Change timezone Time server sync

This form is for configuring the system to automatically synchronize the time with a remote server. Synchronization will be done using the Unix time protocol or NTP, depending on what the remote system supports.

Time Server

Timeserver hostnames or addresses (separated by spaces) 0.us.pool.ntp.org 1.us.pool.ntp.org

Synchronize once per day? ☐ No ☒ Yes

Sync and Apply

6. Enter the hostnames or addresses of the time server(s). Separate servers by a space.
7. Click Yes next to "Synchronize once per day."
8. Click Sync and Apply.

4: Using Node-RED

Included in your *groov* Box is [Node-RED](#), an open-source, multi-platform software program that lets you wire together devices, databases, cloud applications, and APIs (application program interfaces) with simple logic flows.

NOTE: Because the groov Box is a legacy product as of June 2021, updates are no longer provided for Node-RED.

Because Node-RED is included in the *groov* Box, you do not have to download and install it on a computer or embedded device. You can just log in and start using it. A tool called Node-RED Admin is included for easier debugging, backups, and certificate administration.

Node-RED nodes are available for *groov* View and for Opto 22 *groov* EPIC and SNAP PAC controllers. These are reliable industrial-grade controllers used in thousands of applications worldwide. The Node-RED nodes provide access to data in *groov* View Data Stores and controllers. For more information on nodes, see developer.opto22.com.

NOTE: Node-RED is not included in the original GROOV-AT1 groov Box nor on groov Server for Windows. It is included only with GROOV-AR1 Boxes.

In this chapter:

What is Node-RED?	43
Getting Started	44
Connecting with serial devices	51
Working with nodes	53
Working with flows	54
Debugging your Node-RED project	56
Managing security certificates	57
Backing up and restoring your Node-RED project	57
Starting a new Node-RED Project	58

WHAT IS NODE-RED?

Node-RED is a visual tool originally designed at IBM® Emerging Technologies to connect hardware devices, APIs, and online services. Many people use it for Internet of Things (IoT) applications.

In Node-RED you connect prebuilt *nodes* (provided by device manufacturers or software developers) together to make a *flow*. The flow provides the logic to accomplish your goal. You can also add *function* nodes containing JavaScript.

Node-RED in the *groov* Box

Node-RED Editor. You can include one or many flows in your Node-RED project, which you build in the standard Node-RED Editor. You can access the editor directly or from Node-RED Admin.

Because Node-RED is a general-purpose programming environment, you have the freedom to create the flows you like using any nodes you choose. Opto 22 control nodes (for *groov* EPIC or SNAP PAC controllers), *groov* View Data Store nodes, and a wide variety of other nodes are easy to install.

Serial nodes are available for Node-RED. Using an FTDI USB-to-serial adapter, you can connect one or more serial devices to the *groov* Box and use their data in your flows. See [“Connecting with serial devices” on page 51](#) for more information.

Debugging. With few programming restraints, it’s easy to write bugs into your flow. The Node-RED Admin tool can help you debug flows. If Node-RED crashes, it is automatically restarted. You can also start and stop Node-RED yourself from within the Node-RED Admin tool.

Files. Your Node-RED project consists of two files: the main file with all your flows, and a separate file containing all the sensitive credential information used by some nodes, such as usernames and passwords for an email node. In the *groov* Box these files are treated separately to maintain security, and the Node-RED Admin tool provides ways to work with them.

GETTING STARTED

The included Node-RED Admin tool provides access to Node-RED as well as debugging, security certificate processing, and backups.

Requirements

- A GROOV-AR1 Box with *groov* Admin v1.570.44 or higher (Updates are available at manage.groov.com.)
- A computer that can communicate with the *groov* Box
- For real-world communication with an industrial controller, an Opto 22 *groov* EPIC processor running a PAC Control strategy, or a SNAP PAC R-series or S-series controller with firmware R9.5 or higher, with its built-in RESTful API configured (see Quick Start steps on developer.opto22.com).

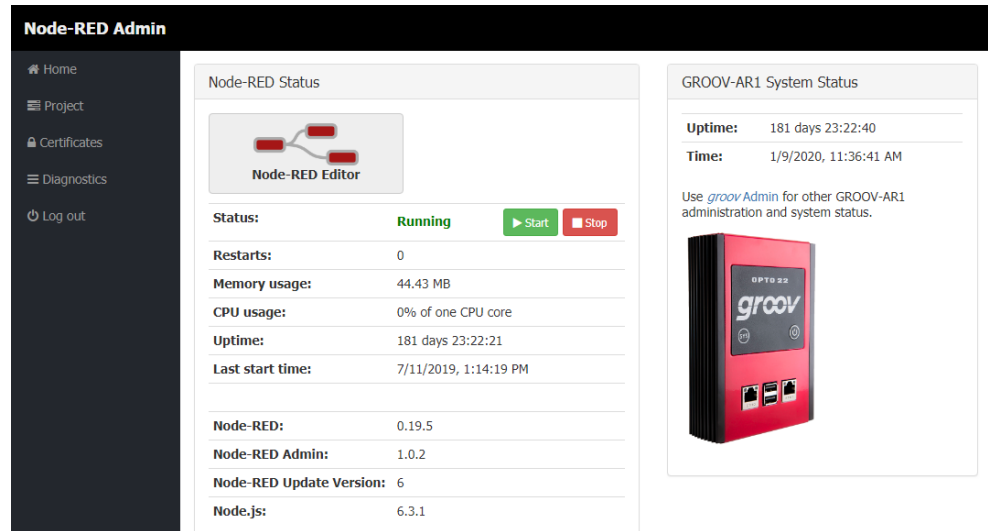
Open Node-RED

1. Open a web browser and enter: `https://[your groov Box's hostname]:3000`
Don’t forget the “s” in https. Example: `https://opto-00-d2-da:3000`

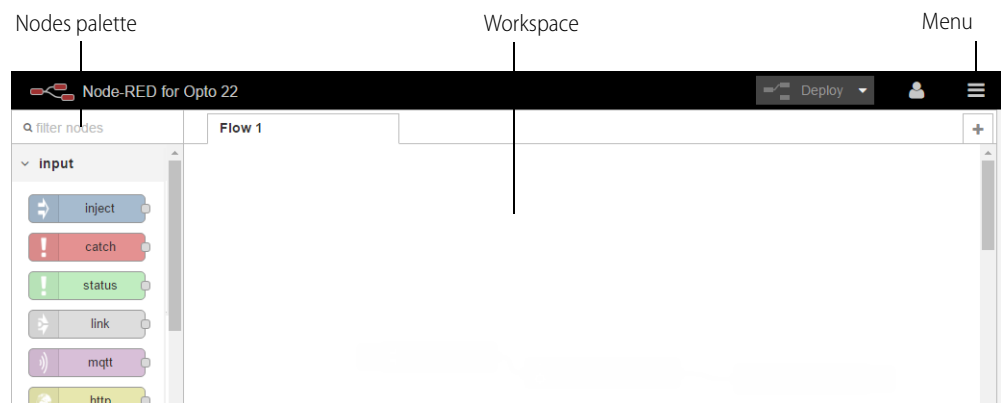
NOTE: This URL using port 3000 takes you to Node-RED Admin. In the future, if you want to go directly to the Node-RED Editor, use port 1880: `https://[hostname]:1880`

*You can also open Node-RED Admin from within *groov* Admin. See [page 22](#).*

2. Log in using your username and password for *groov* Admin.
The Node-RED Admin homepage appears. Status for your Node-RED project appears in the middle column, and status for the *groov* Box appears in the right-hand column:

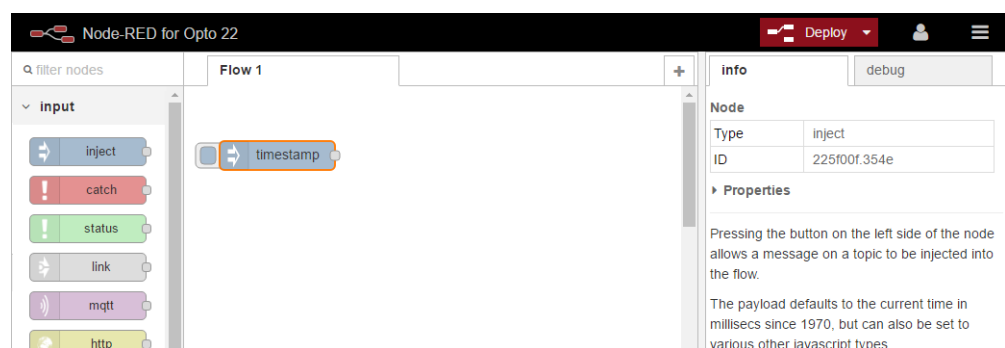


3. Click the Node-RED Editor button to open Node-RED.

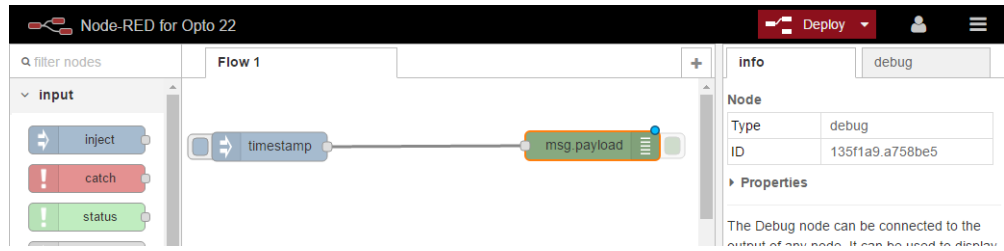


Create a flow

1. In the Nodes palette on the left, locate the *inject* node. Drag it to the workspace.
The inject node lets you inject messages into a flow, either by clicking the button on the node or by setting a time interval between injects.
2. Open the right sidebar (click Ctrl-Space, or click Menu ☰ > View > Show sidebar) and select the **info** tab. Click the inject node to see information about its properties and a description of what it does:



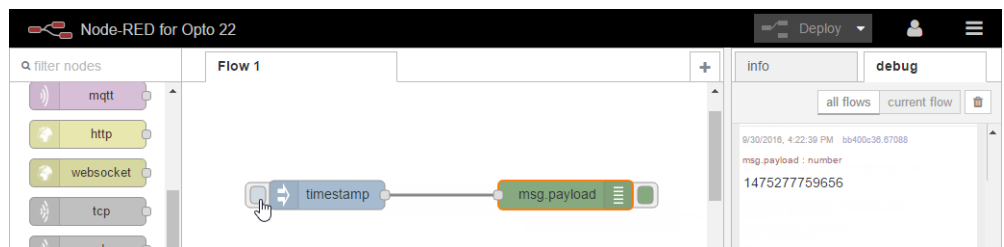
3. Scroll down in the Nodes palette and locate the *debug* node. Drag it to the workspace.
4. Wire the inject and debug nodes together by dragging from the output port of inject to the input port of debug.



Deploy the flow and test

The nodes exist only in the editor and must be deployed to the server.

1. Click the Deploy button in the upper right.
2. In the sidebar, select the **debug** tab. Click the button on the inject node. Numbers appear in the sidebar:

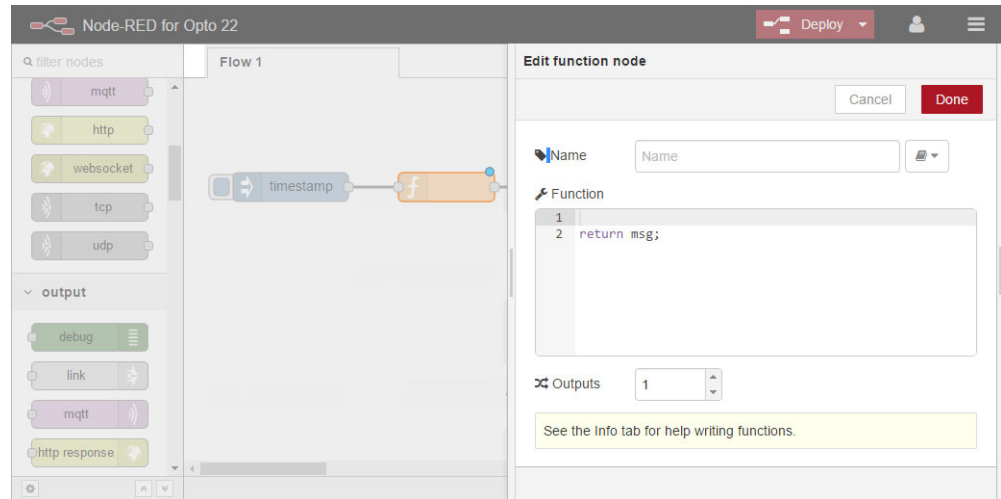


This number is a timestamp representing the number of milliseconds since January 1, 1970. This is the default payload of the Inject node.

Add a Function node

Let's make the timestamp more readable by using a Function node. Function nodes let you pass each message through a JavaScript function. If you don't know JavaScript, you may be able to find code you need using an Internet search.

1. Drag the Function node to the workspace between the Inject and Debug nodes. If you need to delete the existing wire, select it and press Delete on the keyboard. Add new wires if necessary to link the three nodes.
2. Double-click the Function node to edit it.



3. In the Name field, type Human Date.
 4. Copy the following code into the Function field:



```
// Create a Date object from the payload
var date = new Date(msg.payload);
// Change the payload to be a formatted Date string
msg.payload = date.toString();
```
 5. Leave this code in place at the end:

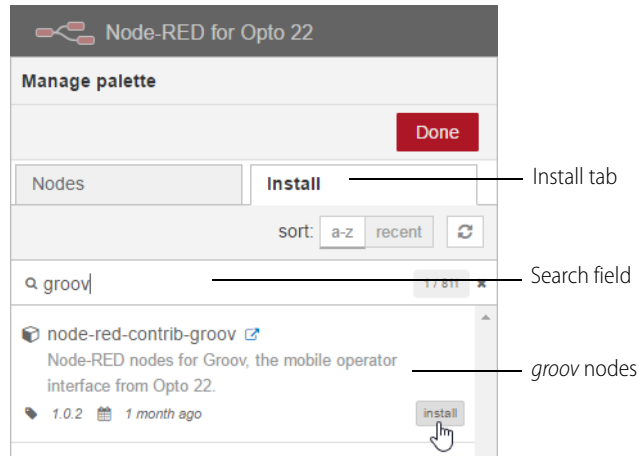

```
return msg;
```
 6. Click Done to close the edit dialog box and then click the Deploy button.
- Now when you click the Inject button, the message in the sidebar shows a more readable time stamp:



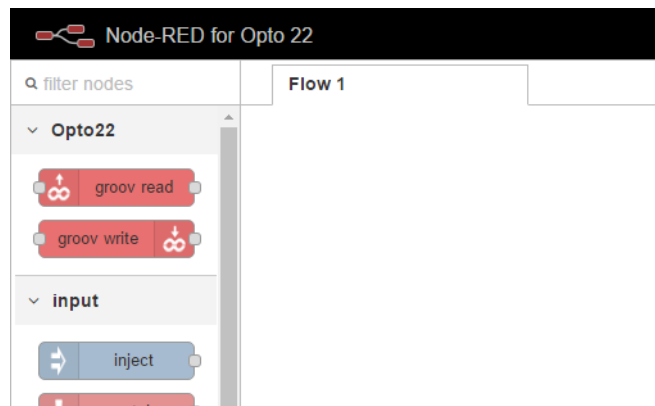
Install groov View nodes

Your *groov* Box must have access to the internet in order to install nodes.

1. Choose Menu  > Manage palette.
2. Click the Install tab.
3. In the search field, enter `groov`.



4. Find `node-red-contrib-groov` in the list and click the Install button next to it.
5. Click Install. When installation is finished and the button changes to read Installed, click Done.
The new *groov* View nodes appear at the top of the nodes palette:



If you have a *groov* View Data Store, you can use a *groov* View node to read or write data in the Store. For help, see “Adding a Data Store” in the [groov View User's Guide](#). For complete instructions to use the node, see “[groov Nodes](#)” on developer.opto22.com.

Add an Opto 22 PAC Control node

For this section, you'll need to have an Opto 22 *groov* EPIC processor running a PAC Control strategy, or a SNAP PAC S-series or R-series industrial controller with firmware R9.5 or higher, running a PAC Control R9.5 or higher control strategy. Make sure the RESTful API is configured. On developer.opto22.com, see the [PAC Control REST API instructions for groov EPIC](#) or the [SNAP PAC REST API Quick Start instructions](#).

1. Install Node-RED for PAC Control nodes just as you installed the *groov* node. (Menu > Manage palette > Install tab. Search for `node-red-contrib-pac`.)
2. Make sure you have an inject and a debug node in the workspace.
3. Near the top of the Nodes palette, click the *pac read* node and drag it to the workspace, in between inject and debug (`msg.payload`).
The *pac read* node lets you read I/O and variable data in the PAC Control strategy.
4. Wire the *pac* node to the other nodes in the flow.
5. Click the node and click the info tab to see helpful information about using it.

6. Double-click the Opto 22 node to edit it.

7. Click the pencil at the right of the Controller field.

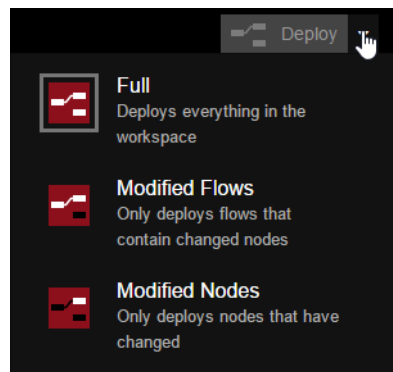
8. Complete the fields:
 - a. For PAC Address, choose the protocol (HTTPS is strongly recommended because it is secure) and enter the EPIC's or PAC's IP address.
 - b. Enter the API Key ID and Value to allow access to the PAC Control API. (You must have already set this up for the controller. See steps on developer.opto22.com.)
 - c. If you are using HTTPS as recommended, enter the SSL certificate information. (You must have already created the certificates. See [“Managing security certificates” on page 57](#) to add the certificates to the *groov* Box.)
 - d. Click Add.

You return to the edit box, where your controller is now configured:

9. Choose the Data Type from the dropdown list.

The data type determines what other fields appear. In this example we chose Analog Input, so a field appears for Tag Name.

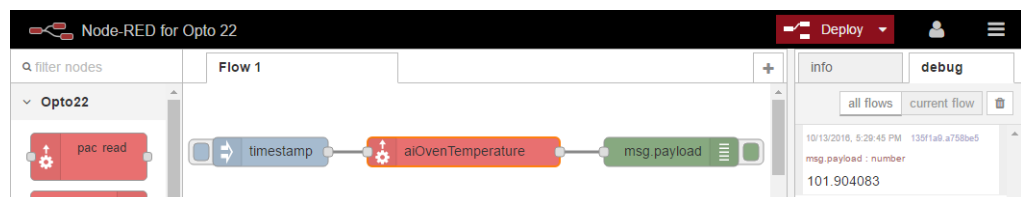
- a. **Tag Name**—Enter the exact I/O point or variable name from the PAC Control strategy running on this controller. If you leave this field blank, you'll receive values for all tags of this type (in this example, all analog inputs).
 - b. **Start Index** and **Length**—For a table, enter the starting index and length of the data you want to use.
 - c. **Node Name**—(Optional) By default, the tag name is used for this node. If you want to give it a different name, enter it here.
 - d. Click Done.
10. Click the down arrow next to Deploy to see your choices.



You can deploy everything, or if you don't want to disturb running flows, you can choose to deploy only the changed flows or changed nodes.

The gray box around the icon shows what will happen when you click the Deploy button. In this example, everything is deployed (Full).

11. Click Deploy. Now click the inject button and see what message appears in the debug tab. You should see the data from your Opto 22 controller. Here's how our example looks:

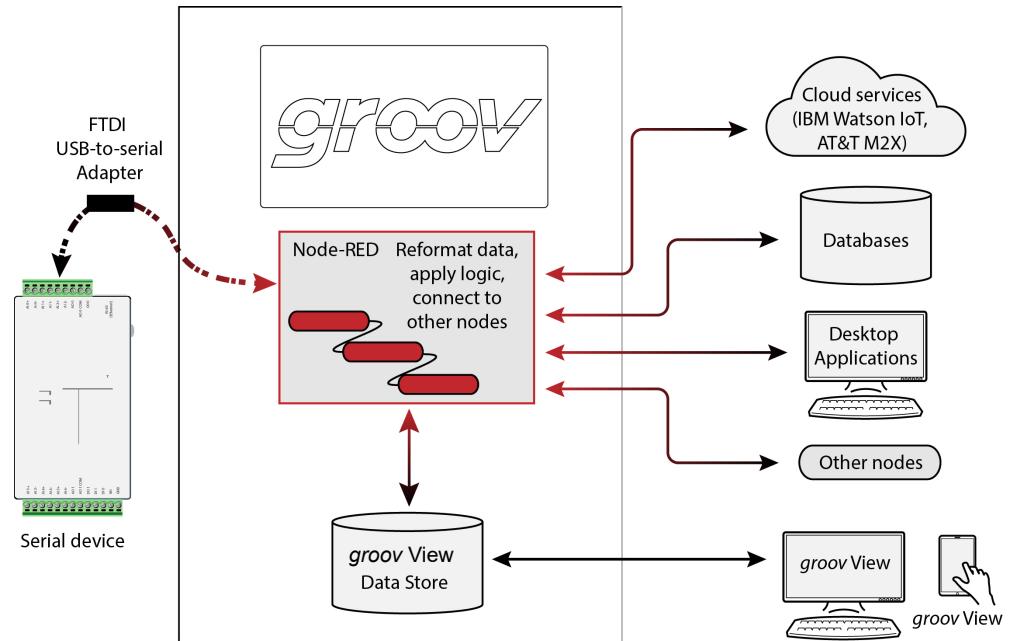


CONNECTING WITH SERIAL DEVICES

Several serial nodes are available for Node-RED. You can attach one or more serial devices to the *groov* Box and use serial nodes to communicate with them. You can connect to RS-232, RS-485, or RS-422 serial devices (2-wire or 4-wire). Three USB ports are available on the *groov* Box. If you need to connect to additional devices, use a USB hub.

Data from connected serial devices can be used in your flows and can also be included in your *groov* View operator interface. For example, you can:

- Get data from a Modbus RTU device, reformat it if necessary in your flow, put it in a *groov* View Data Store, and use it in your *groov* View operator interface for technicians to monitor.
- Log data from weigh scales in your company database for tracking.
- Send data from legacy serial manufacturing equipment to a cognitive computing application, such as IBM Watson IoT, to analyze for predictive maintenance.
- Monitor facility energy usage through serial devices, correlate it with temperature data from local sensors, and project future usage based on forecasts from an online weather service.
- Write data from a company database to serial devices.



Requirements

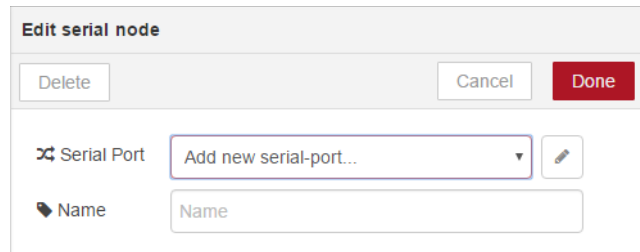
To use serial devices with the *groov* Box, you will need:

- *groov* Admin 1.570.46 or higher
- Node-RED for *groov* Box version 3 or higher
- An RS-232, RS-485, or RS-422 serial device (2-wire or 4-wire)
- A USB-to-serial converter with FTDI chipset, appropriate for the serial device you want to connect to. We recommend single-port adapters.
- If you use a USB hub, use a powered hub.

NOTE: FTDI-compatible adapters are not likely to work. Use an adapter with a genuine FTDI chip, for example B&B Electronics model USOPTL4 or Gearmo US-485422.

Setting up the serial device

1. Connect the converter from the serial device to one of the USB ports on the front or top of the *groov* Box (diagram on [page 110](#)).
2. In Node-RED, drag your serial node to the workspace and double-click it to edit it.



3. Click the pencil at the right of the Serial Port field.
4. In the Add New dialog box, click the magnifying glass to discover the serial devices you have connected to your *groov* Box.

In this example, two serial devices are connected, both to the front of the Box:



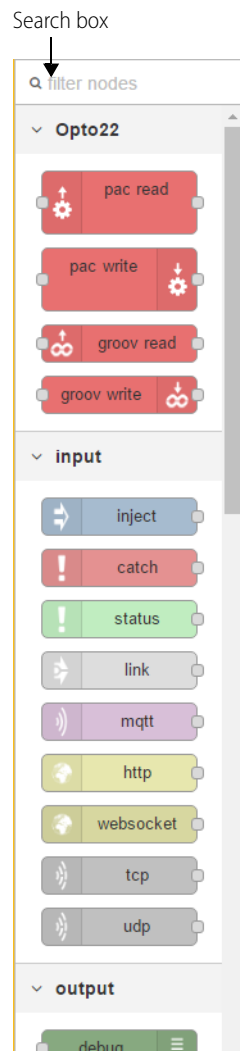
/dev/ttySer0 is the top USB port on the front of the *groov* Box.
/dev/ttySer1 is the bottom USB port on the front of the Box.
 See diagram on [page 110](#).

For serial devices connected through a USB hub, see address information on [page 110](#).

5. Choose the device you want, and then enter the Settings (baud rate, data bits, and so on) that apply to it. Make any other changes necessary for the node and then click Add.
6. Back in the Edit dialog box, give the new serial port a name and click Done.
 Your serial device is ready to use in Node-RED.

IMPORTANT: Remember that the address of the port you added in the node is the address of the USB connector on the *groov* Box or hub, not the address of the serial device. If you unplug a device from one connector and plug it into a different one, you will need to change the device's address in the node.

WORKING WITH NODES

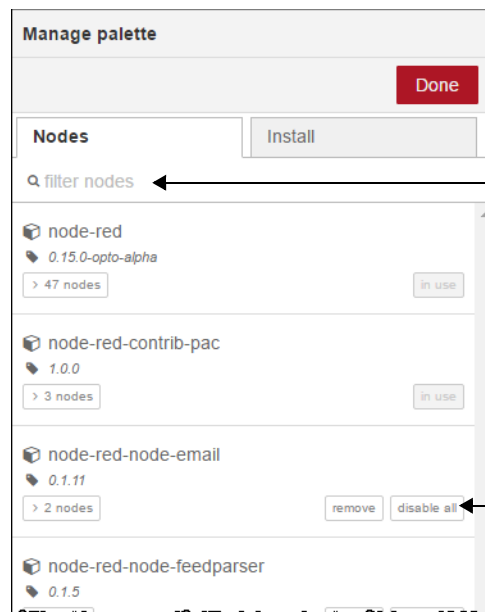


In the nodes palette on the left side of the workspace, you see all the nodes built into the program. You can scroll down to find the one you want or search for it by typing into the search box at the top.

Managing nodes

You can remove or disable nodes you don't want and install additional nodes you want to use.

To manage nodes, choose Menu  > Manage palette. You see a list of the nodes built into Node-RED:




Type here to search for existing nodes.

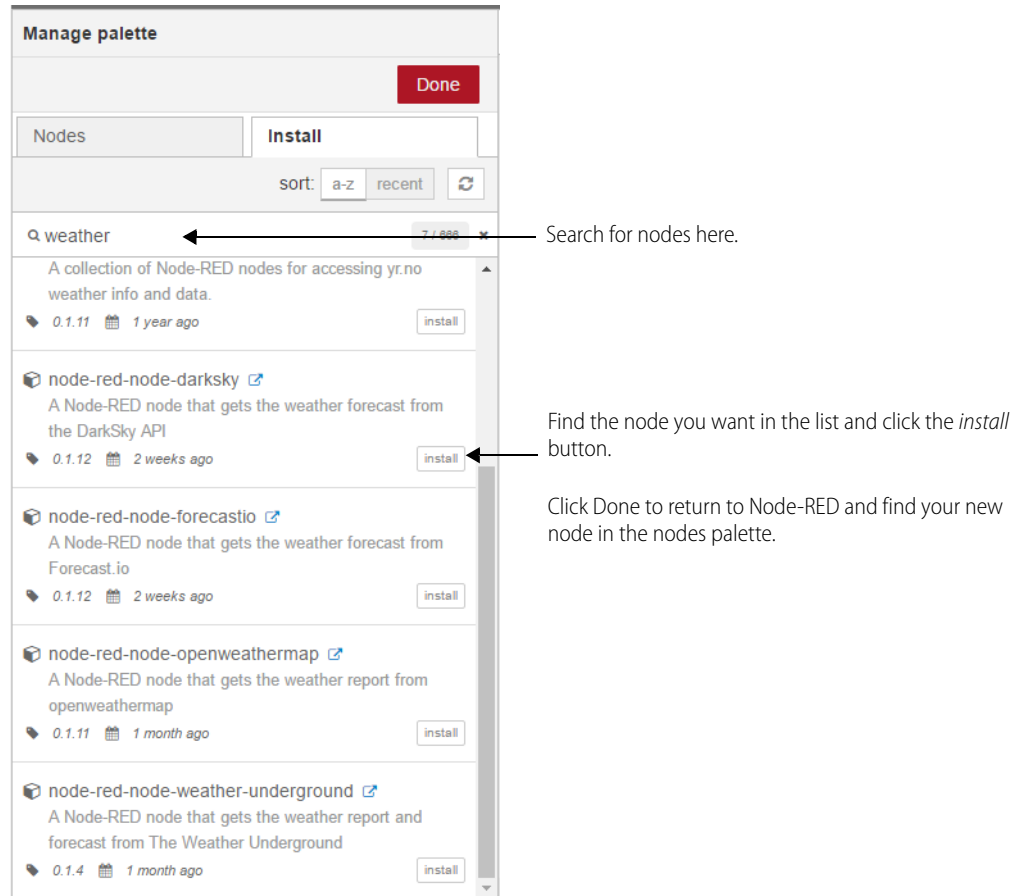
To disable or remove nodes, choose the one you want in the list and click the button.

Installing nodes

Many Node-RED nodes are available, and you can easily install the ones you want. For example, you may want to use nodes for a weather service or for mysql.



To install nodes, choose Menu  > Manage palette. Click the Install tab.

In the search box, enter the node you're looking for. In this example we entered: `weather`



WORKING WITH FLOWS

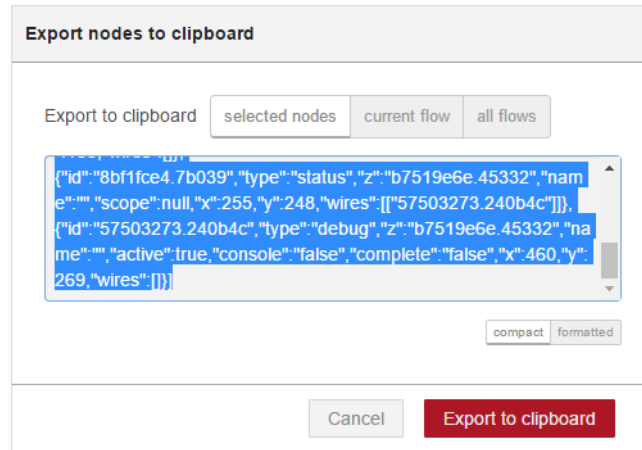
You can have one or many flows in your Node-RED project.

- **To name a flow**, choose Menu  > Flows > Rename.
- **To add a new flow**, click the plus sign  in the upper-right corner of the workspace.
- **To delete a flow**, choose Menu > Flows > Delete.

Exporting a flow

It's easy to export flows or nodes. Exporting lets you share a flow you've built with others or store it for future use.

1. With the flow open in the workspace, highlight one or more nodes (to export just part of a flow, highlight only the nodes to export).
2. To store, choose Menu > Export > Library. Give the file a name so you can find it later.
3. To save to a text file for sharing, choose Menu > Export > Clipboard



4. Choose whether to export only the highlighted nodes, the current flow, or all flows in the project.
5. Click Export to clipboard.
6. Paste the contents of the clipboard into a text file and save it.

Importing a flow

Importing lets you use flows or nodes you've saved or other people have built, so you can build what you need faster. (A good source of flows is the [OptoForum](#), where Opto 22 customers ask and answer questions and share code samples and tips.)

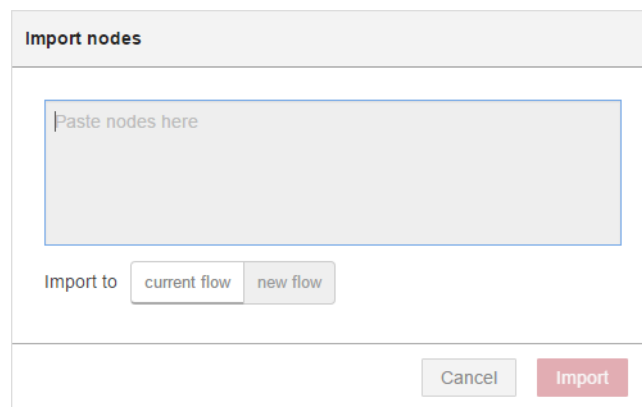
Import from the Library

If you've already saved flows or nodes, open the flow you want to import to. Choose Menu > Import > Library and choose the filename you want.

The saved flow or node immediately appears in the workspace.

Import from a file

1. Make sure the data you want to import is in a text file. Copy the contents of the file.
2. In the workspace, choose Menu > Import > Clipboard.



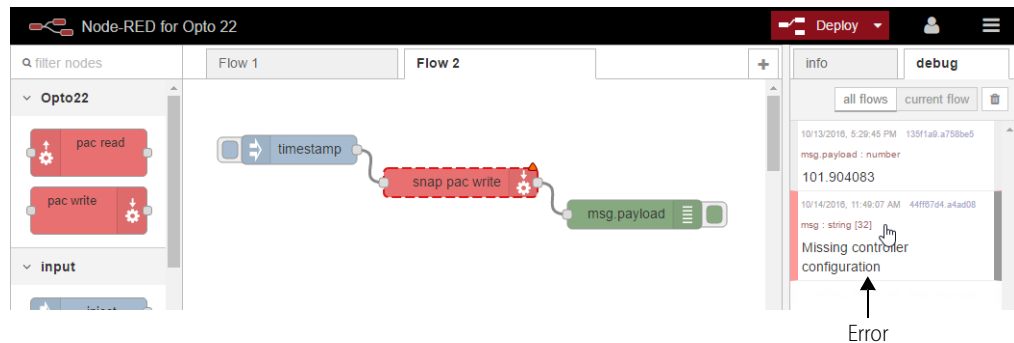
3. Paste the data into the field. Choose whether to import into the flow that's open on the workspace or to create a new flow.
4. Click Import.

DEBUGGING YOUR NODE-RED PROJECT

In the Editor

Within the Node-RED Editor, the debug tab helps you debug your flow.

In this example, we forgot to configure the SNAP PAC controller in the middle node. When we injected, an error was returned in the debug tab:



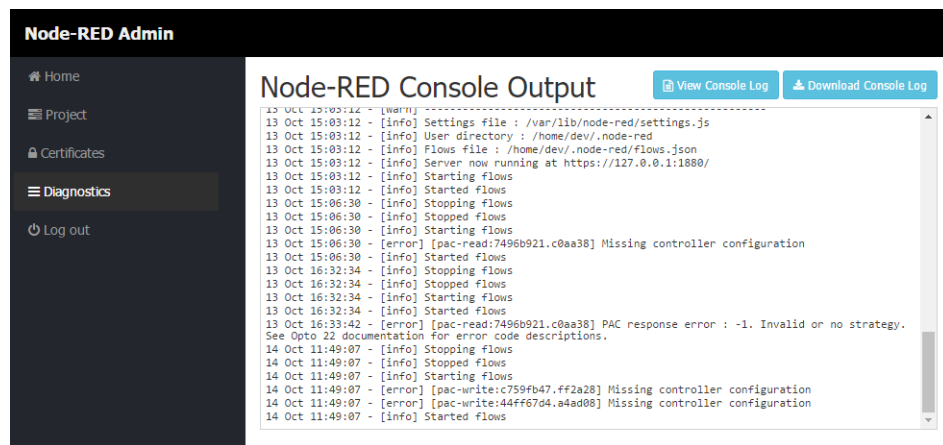
To see which node the error occurred in, hover over the error or click it to highlight the node (the node is surrounded with a dotted orange line).

Note: If the problem node is in another flow, hovering won't highlight the node; but if you click the error you'll be taken to the flow and the node highlighted.

In Node-RED Admin

Node-RED Admin keeps a running log of events that you can view or download to help debug problems.

1. In the left nav bar in Node-RED Admin, select Diagnostics.

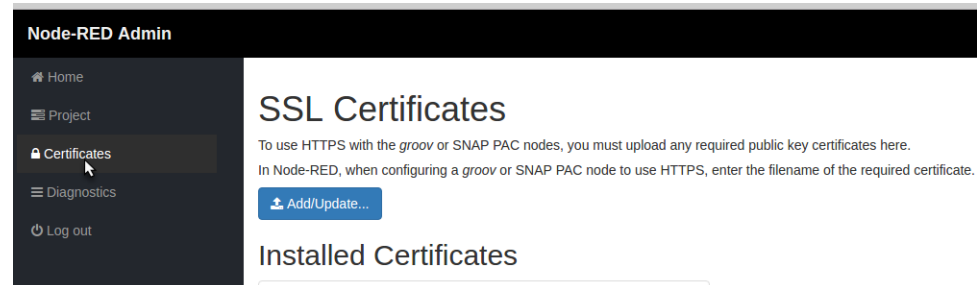


2. To save a copy of the log, click Download Console Log. To view only the log in a separate browser tab, click View Console Log.

MANAGING SECURITY CERTIFICATES

SSL security certificates must exist on the *groov* Box before you can connect to Opto 22 controllers using Node-RED. You can upload and manage these certificates from within Node-RED Admin.

1. In the left nav bar in Node-RED Admin, select Certificates.



If you've already added one or more certificates, you'll see a list of those installed.

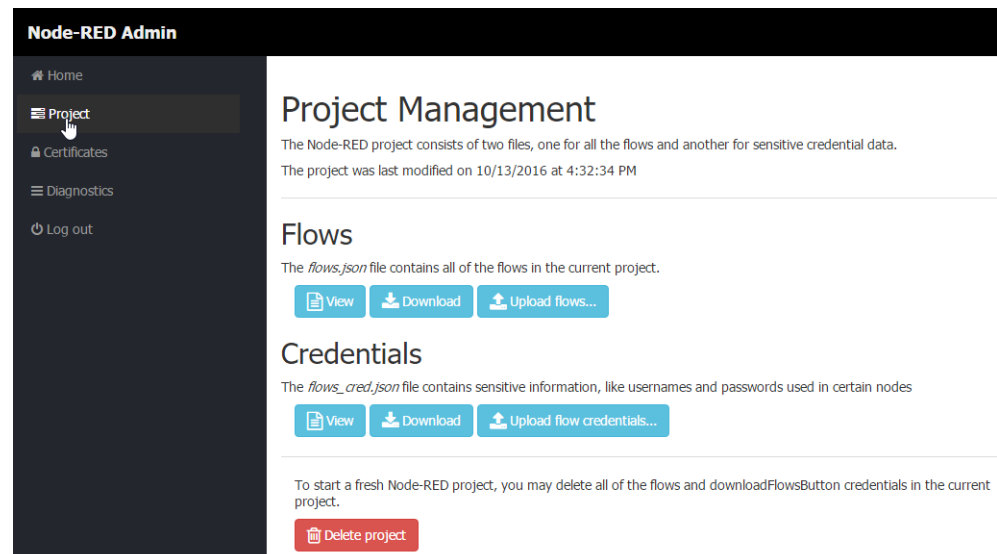
2. Click Add/Update. Navigate to the location of your Opto 22 controller's public key certificate. Click Open. The certificate appears in the list of Installed Certificates.

BACKING UP AND RESTORING YOUR NODE-RED PROJECT

You'll want to back up your Node-RED project to make sure you have a copy. Backing up just means downloading the files to your computer, so you can upload them later if you need to.

The project consists of two files: one for all your flows and the other for sensitive credential information like the username and password required for some nodes. We recommend you back up both.

1. In the left nav bar in Node-RED Admin, select Project.



2. To see what each file looks like, click the *View* button under Flows or Credentials.
3. To back up your Node-RED project, click *Download* under Flows or Credentials and save the file in a safe place on your computer.

STARTING A NEW NODE-RED PROJECT

4. To restore your project, click *Upload flows* or *Upload flow credentials*. Navigate to the location of the backed-up file and click Open.

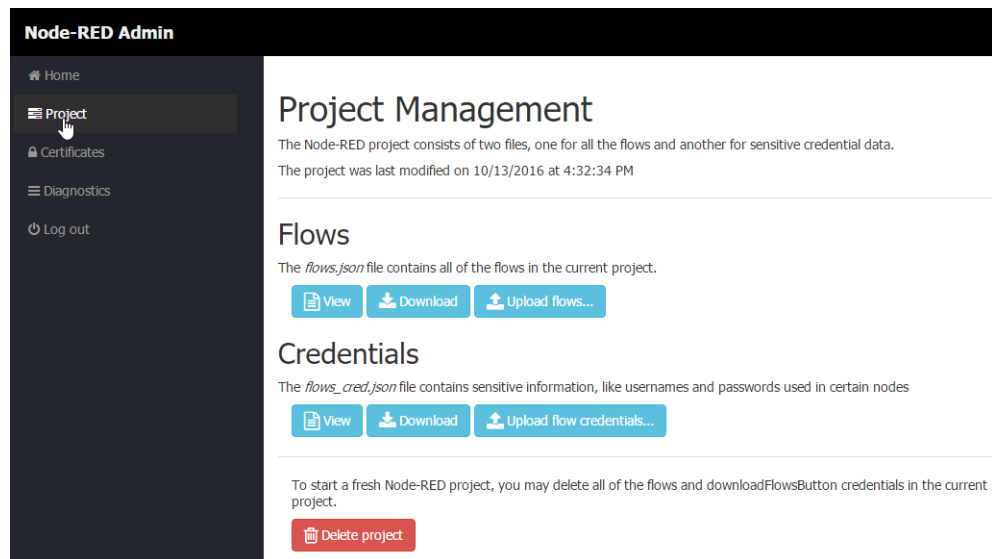
Backing up and restoring can take several minutes. Wait until the process is finished.

NOTE: If you have updated Node-RED since your last Node-RED backup, restoring will take you back to a previous version. Update Node-RED again after restoring (see ["Updating Node-RED"](#) on page 36.)

STARTING A NEW NODE-RED PROJECT

You can only have one Node-RED project at a time, although that project can contain multiple flows. If you decide to start over and create a new project, you can delete all flows and credentials in the existing project.

1. In the left nav bar in Node-RED Admin, select Project.



2. Scroll down and click the red Delete Project button.
3. To verify that you really want to start over, click Delete and Restart.

5: Using Ignition Edge

This chapter introduces Ignition Edge, available in the *groov* Box and designed so you can use OPC UA and MQTT at the edge of the network for your IoT applications.

NOTE: Because the groov Box is a legacy product as of June 2021, updates are no longer provided for Ignition Edge.

What is Ignition Edge?	60
Getting Started	60
Using MQTT	73
Managing Ignition Edge	75

WHAT IS IGNITION EDGE?

Available in your *groov* Box is Ignition Edge, an internet of things (IoT) software application developed by Inductive Automation for the network's edge, with OPC-UA drivers for Allen-Bradley and Siemens PLCs, SNAP PACs, and other automation equipment.

Because Ignition Edge is included in the *groov* Box, you can use its tags—in your *groov* View operator interface, Node-RED flows, and MQTT communications—for your IoT projects:

- Without having to purchase a separate OPC-UA server
- Without requiring a PC at the network's edge

Note that the OPC-UA server in Ignition Edge is used by Ignition applications and by *groov* View. The server is available only to internal applications.

Ignition Edge in the *groov* Box

In the Opto 22 *groov* Box, Ignition Edge provides two key connectivity tools for IoT applications—OPC UA and MQTT.

- Ignition Edge includes an internal **OPC-UA** server and drivers for a number of commonly used PLCs, plus Modbus devices communicating over TCP. (See [“OPC UA drivers included with Ignition Edge in the groov Box” on page 60.](#)) Additional drivers may be available for purchase from Inductive Automation and their partners.
- Ignition Edge also includes an **MQTT** Transmission module. MQTT is a transport protocol highly useful in IoT applications because of its architecture. For more information, see [“Using MQTT” on page 73.](#)

You can use Ignition Edge in the *groov* Box for two-hour trial periods and reset the trial as often as you wish. To use Ignition Edge fully, you will need to purchase an Ignition Edge license, part number [GROOV-LIC-EDGE](#).

The *groov* Box with Ignition Edge is especially useful for the plant floor, geographically dispersed locations, and OEMs, because everything is included in one compact, secure, industrial appliance.

With Ignition Edge in the *groov* Box:

- Data from many PLCs becomes easier to access for IoT applications.
- Authorized operators can monitor and control these PLC systems from your *groov*View operator interface.
- All data in Ignition Edge can be published and subscribed to via MQTT.
- Node-RED flows can use tags from the Ignition Edge tag database.
- It's easy to add other Inductive Automation products:
 - Other Ignition Edge-compatible modules
 - Additional drivers like DNP3, Omron®, and TCP/UDP
 - Ignition Edge Panel or Enterprise

OPC UA drivers included with Ignition Edge in the *groov* Box

Opto 22 controllers:

- *groov* EPIC
- SNAP PAC

Allen-Bradley PLCs:

- Logix: ControlLogix® and CompactLogix™ firmware v21 and higher
- ControlLogix firmware v20 and lower
- CompactLogix firmware v20 and lower
- SLC™ 5/05
- PLC-5®
- MicroLogix™ 1100, 1200, 1400, 1500

Siemens PLCs:

- S7-300
- S7-400
- S7-1200
- S7-1500

Other drivers:

- Modbus/TCP devices
- Devices that support Modbus RTU over TCP
- Other drivers you have purchased

groov EPIC and SNAP PAC drivers

Ignition Edge in the *groov* Box includes drivers for Opto 22 *groov* EPIC and SNAP PAC systems, which help you:

- Publish EPIC and SNAP PAC system data via MQTT.
- Connect other Inductive Automation applications to *groov* EPIC and SNAP PAC systems.

You can add drivers to the *groov* EPIC system by downloading and installing the Opto 22 *groov* EPIC and SNAP PAC Driver module, which is a product of Cirrus Link Solutions. For details, see the Cirrus Link Documentation webpage

(<https://docs.chariot.io/display/CLD/Opto+22+groov-EPIC+and+SNAP+PAC+Driver>). However, note that you don't need to use this driver to use *groov* EPIC or SNAP PAC controller tags in your *groov*View operator interface. Instead, configure the *groov* EPIC or SNAP PAC controller in *groov*View, so *groov*View communicates with the *groov* EPIC or SNAP PAC system directly.

GETTING STARTED

This section gives you basic steps to get started using Ignition Edge. For a lot more information on using Ignition Edge, visit [Inductive University](#).

Requirements

- A GROOV-AR1 Box with *groov* Admin v1.570.47 or higher (Updates are available at [manage.groov.com](#).)
- A computer that can communicate with the *groov* Box
- One or more devices supported by the drivers included with Ignition Edge in the *groov* Box (see list on [page 60](#))

NOTE: If you want to read PAC Control R10.0a (or higher) tag names with Ignition Edge or Ignition Designer, be sure to:

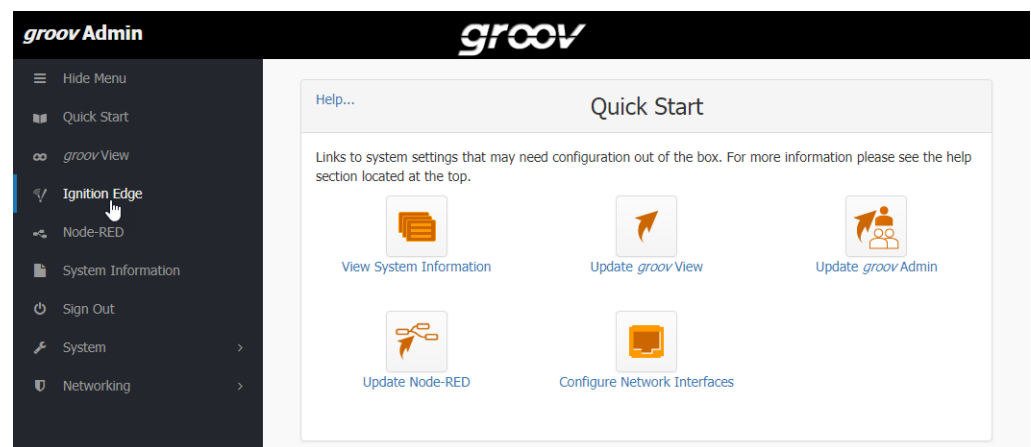
- *Configure PAC Control Strategy tags with public tag access using PAC Control R10.0a or newer.*
- *Install version 3.4.2 (or higher) of the Opto 22 groov EPIC and SNAP PAC Driver module.*

For details, see [KB87534](#).

To get you started, the following steps use a simulated device that is included in Ignition Edge.

Configure Ignition Edge

1. Open a web browser and enter: `https://[your groov Box's hostname]:10000`
Or open *groov Admin* from within Build mode (Configure > *groov Admin*).
2. Log in with your *groov Admin* username and password to open the Quick Start menu.



NOTE: If Ignition Edge does not appear in the left navigation panel, refresh your browser window. If it still does not appear, make sure you have installed groov Admin v1.570.47 or higher. (Click System Information to check.)

3. In the left navigation panel, click Ignition Edge.

Ignition Edge

With [Ignition Edge](#) by [Inductive Automation](#), you can use built-in OPC UA-compatible drivers for Allen-Bradley PLCs, Siemens PLCs, and other devices in your *groov* projects. (Note that Ignition Edge does not permit external access to the OPC UA server.)

You can also publish and subscribe automation data with the MQTT/Sparkplug protocol to an MQTT broker on premises or in the cloud.

Learn more about Edge and MQTT in the [groov Box User's Guide](#).

Status

✓ *groov* Enterprise is licensed and enabled. To get your Ignition Edge license key, email Opto 22 at pcs@opto22.com and include your *groov* Serial number: E1937S

✗ Ignition Edge is not running.

Configuration

☐ Enable and run Ignition Edge at startup

☐ Enable access to Ignition Edge Designer and Edge Panel

Designer is not needed to configure Allen-Bradley and SNAP PAC drivers and use their data in *groov*.

Designer is needed to:

- Configure tags for Siemens PLC and Modbus drivers
- Create MQTT Transmission tags
- Update MQTT brokers with tag configurations and changes
- Use advanced features of Ignition Edge, including Panel and EAM

CAUTION: Ignition Edge Designer and Edge Panel require an insecure TCP port to be exposed by the *groov* Box firewall. Opto 22 recommends that if you check this option, you also:

1. Connect the *groov*Box only to a trusted network that blocks external requests to TCP port 8088.
2. Configure Ignition Edge to use SSL to limit the functionality available on the insecure TCP port.

NOTE: Ignition Edge Panel is an optional feature available for separate purchase. If you use it, be sure to allow connections only over HTTPS (see Ignition Edge Panel manual for details).

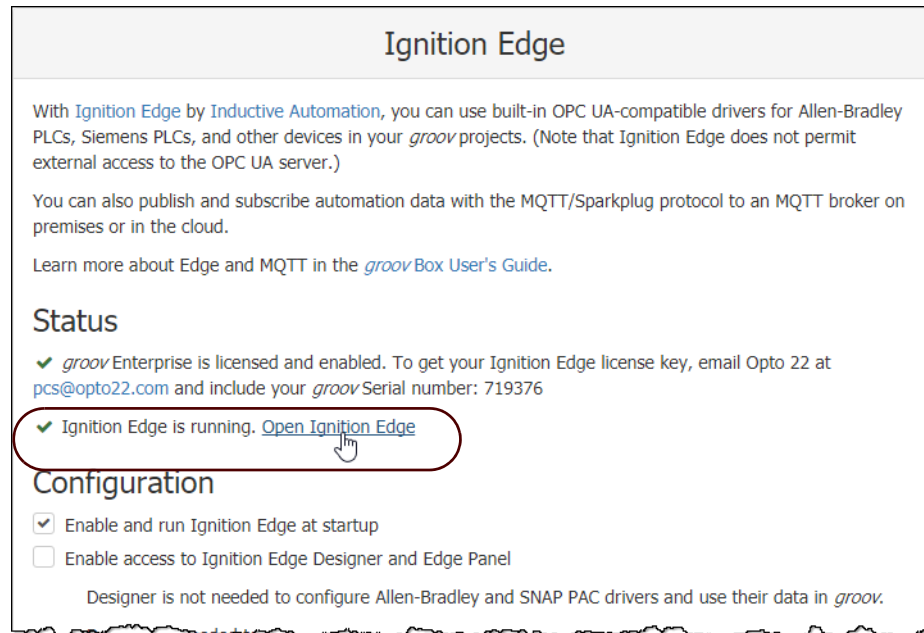
The Status section on this page shows you whether you already have a *groov* Enterprise license, which fully enables Ignition Edge. However, you can use Ignition Edge for a two-hour trial without licensing it. You can restart the trial as often as you want. These Getting Started steps use the free trial.

This section also shows you whether Ignition Edge is currently running.

4. In the **Configuration** section, check Enable and run Ignition Edge at startup.
5. For this example, do not check Enable access to Ignition Edge Designer and Edge Panel.
6. Click Save.
7. Read the software license and click Accept to continue. Wait until the message in the image below appears.



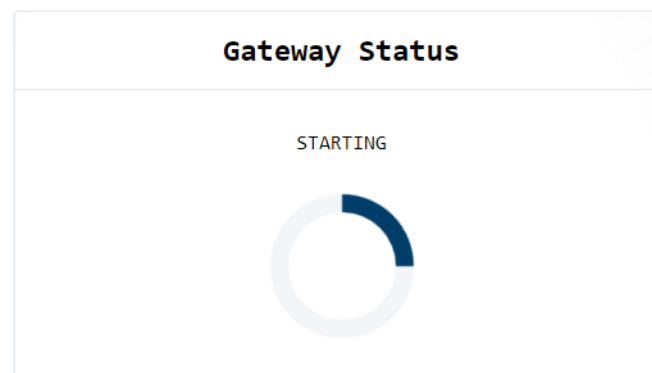
8. Click Back and notice that Ignition Edge is now running.



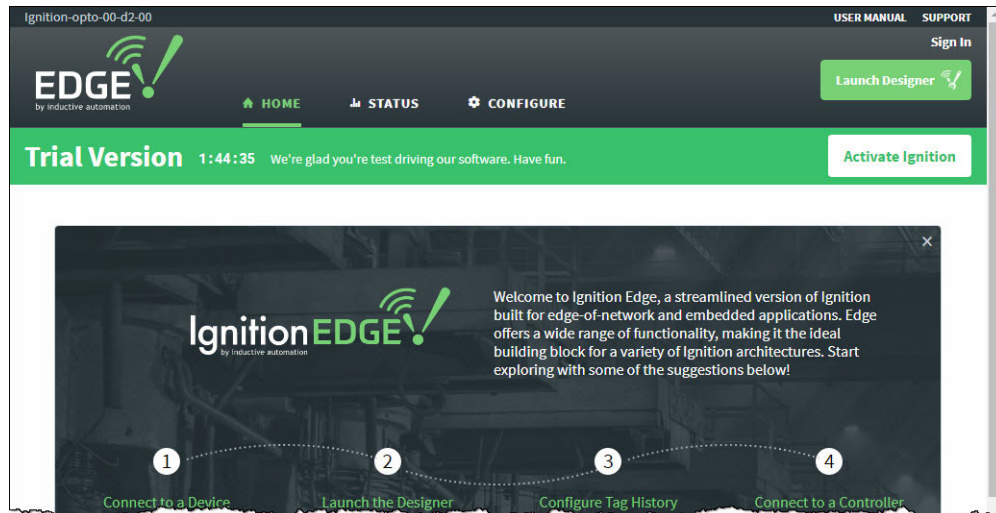
9. Click Open Ignition Edge.

NOTE: In the future, you can open Ignition Edge from this page in groov Admin, or you can go directly to Ignition Edge in your web browser by entering as the URL: `https://[your groov Box's hostname]:8043`. Don't forget the "s" in https. Example: `https://opto-00-d2-da:8043`

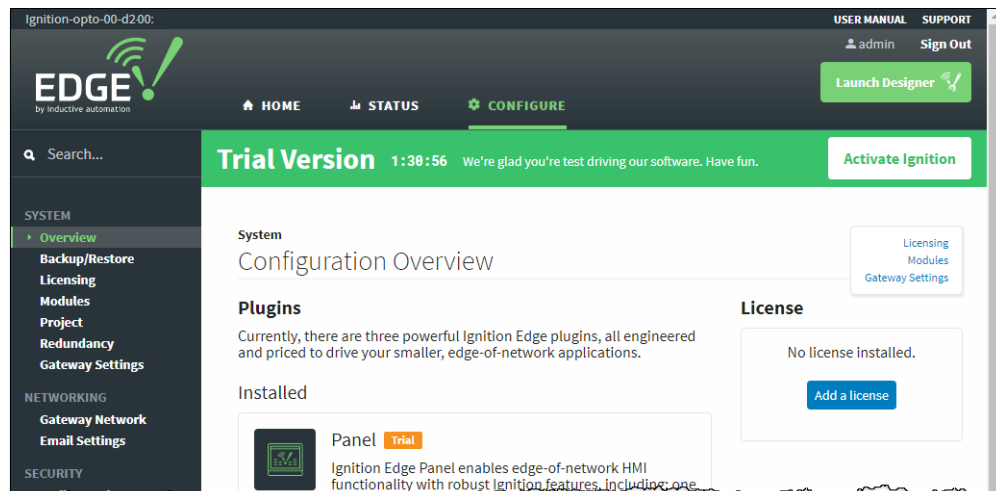
10. Wait while Ignition Edge starts. (It may take a few minutes initially.)



The Ignition Edge gateway webpage appears, showing the trial running.



11. In the top navigation bar, click Configure.
12. Sign in using the default username `admin` and password `password` and press Enter. (When you license Ignition Edge for full use, you will change your Ignition Edge password following the steps on [page 80](#).)



13. In the left navigation panel, scroll down and choose OPC-UA Server > Settings.

Settings

Authentication

Authentication Profile: opcua-module
The name of the authentication profile to authenticate against.

Allowed Roles: ReadWrite
Separate multiple roles with a comma (ex: Administrator,user,manager)

Allow Anonymous Access: ☒ Allow users to connect whether or not they possess authentication credentials.
(default: false)

Server

Server Port: 4096
The port on the local machine the server will run on. Requires a module restart to take effect.

Minimum: 100
The lowest rate (in milliseconds) that the server will accept for reading data sources. Requires a module restart to take effect.

14. Change only the following:
 - a. Under Authentication, check the box to Allow Anonymous Access.
Allowing anonymous access does not create a security issue, because the Ignition Edge OPC server is on the same box as *groov* View.
 - b. Under Expose Configured Tags, check the box to Expose Tag Providers (allows the server to get tags automatically for some manufacturers' devices).
15. Scroll to the bottom of the page and click Save Changes.
16. In the left nav, choose System > Gateway Settings.

Ignition-opto-00-d2-dc

USER MANUAL SUPPORT

admin Sign Out

Launch Designer

EDGE by Inductive automation

HOME STATUS CONFIGURE

Search...

Trial Version 1:52:13 We're glad you're test driving our software. Have fun. Activate Ignition

SYSTEM

- Overview
- Backup/Restore
- Licensing
- Modules
- Project
- Redundancy
- Gateway Settings

NETWORKING

- Gateway Network
- Email Settings

SECURITY

- Audit Log Viewer
- Users, Roles
- Service Security

Gateway Settings

Settings Homepage Config

Gateway Settings

System Name: Ignition-opto-00-d2-dc
The name of this Ignition system, used to differentiate this system from others in a larger architecture.
(default:)

17. Scroll down and check the box next to Use SSL:

Use SSL: ☒ Turns on SSL encryption when communicating with the Gateway. It is highly recommended that you purchase an SSL certificate from a certificate authority if you turn this feature on.
(default: false)

Because Ignition Edge is in the *groov* Box and it includes a self-signed certificate, a purchased certificate may not be necessary. See [Chapter 6: Using an SSL Certificate](#) for more information on certificates.

18. Scroll to the bottom of the page and click Save Changes.

Configure a device in Ignition Edge

1. In the left nav, choose OPC-UA Server > Devices.

Devices

Name	Type	Description	Enabled	Status
No Devices				
→ Create new Device...				

2. Click Create New Device.

You see all the device types whose drivers are included in Ignition Edge in the *groov* Box. If your application requires a device type not listed, you can contact Inductive Automation to see if a driver is available for it. For this example, we'll use one of the demo devices.

Add Device Step 1: Choose Type

☒
Allen-Bradley Logix Driver
Connect to Allen-Bradley Logix family devices, including devices with firmware v21+.

☐
Allen-Bradley MicroLogix
Connect to MicroLogix 1100 and 1400 series PLCs.

☐
Allen-Bradley PLC5
Connect to PLC5s via Ethernet.

☐
Allen-Bradley SLC
Connect to SLC 5/05s via Ethernet.

☐
Legacy Allen-Bradley CompactLogix
Connect to CompactLogix firmware v20 and prior processors.

☐
Legacy Allen-Bradley ControlLogix
Connect to ControlLogix firmware v20 and prior processors.

☐
Modbus RTU over TCP

3. For this example, scroll down and choose the Simulators Dairy Demo Simulator. Click Next.

New Device

General

Name

Description

Enabled

☒ (default: true)

Create New Device

4. Give the demo a name and optional description, and click Create New Device.

Devices

✓ Successfully created new Device "Dairy Demo"

Name	Type	Description	Enabled	Status	
Dairy Demo	Simulators Dairy Demo Simulator		true	Connected	delete edit

→ Create new Device...

The DairySim device is listed and its status shows as Connected.

5. Back up your Ignition Edge project: in the left navigation panel, choose System > Backup/Restore.

System Backup / Restore

Backup Restore Legacy Upgrade

Download Backup ↓

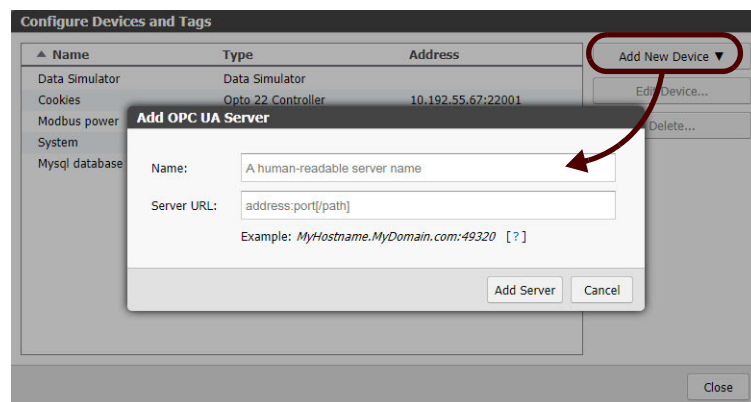
Backs up the *user data* inside this Ignition Gateway server. This includes all projects, drivers, images, and configuration, but not the modules.

6. Click Download Backup and save the file to your computer.
7. Continue with the next section.

Add the internal OPC-UA server to *groov* View

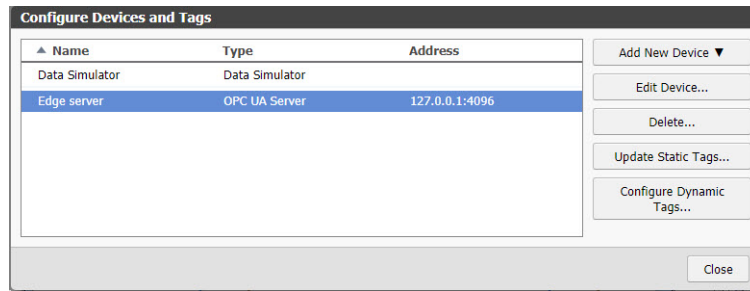
For help in using *groov* View, see the [groov View User's Guide](#).

1. Open a new tab in your browser and open *groov*: `https://[your groov Box's hostname]`
2. Click the gear icon in the upper right and choose Switch to Build mode.
3. Choose Configure > Devices and Tags. Click Add New Device (upper right) and click OPC UA Server.

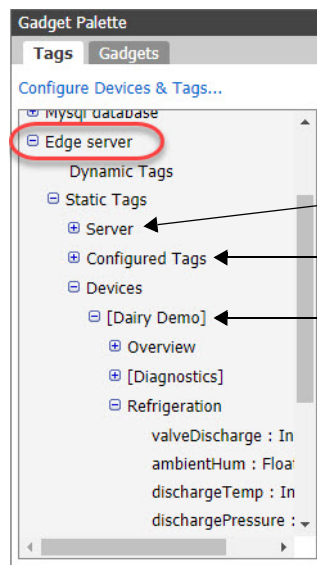


4. Enter a name for your Ignition Edge server. For the Server URL, enter: `127.0.0.1:4096`
The URL uses the loopback address, because *groov* View and the server are in the same box. The 4096 specifies the port *groov* View uses to communicate with the server.
5. Click Add Server.

Your new server is added to *groov* View's list of devices:



- Click Close.
- Back in Build mode, find your new server in the Gadget Palette (lower right corner, in the Tags tab). Click the plus sign next to the server's name to see the tags in this device. Keep opening the tree by clicking the plus signs next to Static Tags > Devices > [Dairy Demo] > Refrigeration.



You can configure multiple devices in the server. Devices and their tags appear in the tree, but their location depends on how their tags are created.

Server tags show the status of the Ignition Edge OPC-UA server itself.

Under Configured tags you'll find tags you manually configured in the server (from devices whose tags were *not* imported automatically).

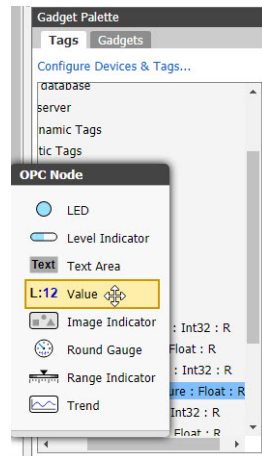
The Dairy Demo is the device you configured in the Ignition Edge server. The server automatically imported its tags, so all of them are shown here.

You'll find a folder under Devices for each device whose tags were imported by the server.

Add a gadget connected to an Ignition Edge tag

- Add a new page to your *groov* View project, or open an existing page to add new gadgets.

- In the Gadget Palette, under Refrigeration, select dischargePressure. Highlight the Value gadget.



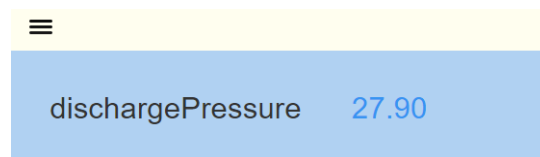
- Drag the Value gadget onto your page.

NOTE: If you receive an error, the Ignition Edge trial period may have expired. Open another browser tab, go to [https://\[your groov Box's hostname\]:8043](https://[your groov Box's hostname]:8043) and restart the trial. (See [page 75](#) for help.)

- Expand the gadget's width so you can see the full tagname.



- Choose File > Save All Changes and Switch to *groov* View. Watch the value change in *groov* View. *groov* View updates data from OPC-UA servers (or from any source) at a fixed rate of once per second.



NOTE: If you see a yellow triangle on the gadget and no value is shown, click the yellow triangle to see what's wrong. Some possibilities:

- Your groov View trial period may have expired. Unless your groov Box has an Edge license, you are using a free trial for OPC UA, and that trial expires two hours after you first look at your operator interface in groov View. To restart the trial, just restart the Box. (See [page 36](#) for steps.)*
- Your Ignition Edge trial period may have expired. Open another browser tab, go to [https://\[your groov Box's hostname\]:8043](https://[your groov Box's hostname]:8043) and restart the trial. (See [page 75](#) for help.)*

Add other devices (Allen-Bradley, Siemens, Modbus)

Take another look at the list of [OPC UA drivers included with Ignition Edge in the groov Box](#). If you have any of this equipment, you can use their tags in your *groov* View operator interface, Node-RED flows, and MQTT communications.

Tags for these devices are brought into Ignition Edge in two different ways:

- Some, like Opto 22 controllers and most Allen-Bradley devices, support tag browsing. That means all tags on the device are automatically pulled into the server and available immediately in *groov* View.
- Others, like Siemens and Modbus devices, do not support tag browsing. You manually add each tag you want to use to the server.

To add another device:

1. Go back to the tab with the Ignition Edge gateway webpage. Or open a new browser tab and enter: `https://[your groov Box's hostname]:8043`
2. Make sure the Trial Version is still running (to restart, click the Reset Trial button).
3. In the left nav, choose OPC-UA Server > Devices.
4. Click Create new Device. Choose the appropriate driver for your hardware. Scroll down and click Next.
5. Give your new device a name and optional description. Make sure Enabled is checked. Fill in the hostname or IP address of your device and then click Create New Device.
Your device appears in the list.
6. If your device is an A-B PLC, go back to Build mode and test the new device by adding a gadget, just as you did with the Dairy Demo.
7. If your device is Siemens or Modbus, follow steps in [“Configure tags manually,”](#) next.

Configure tags manually

You need to manually add tags using Ignition Edge Designer if any of the following applies:

- You are using MQTT.
- You are using Ignition Edge OPC-UA tags in Node-RED flows.
- Your device does not support tag browsing.
- You want to reduce the number of tags you see for Opto 22 controllers and Allen-Bradley PLCs when building your *groov* View interface.

CAUTION: *To configure tags manually, you must temporarily open an insecure TCP port on the groov Box. Before opening it, make sure that:*

- *The groov Box is connected only to a trusted network that blocks external connection requests to TCP port 8088*
- *You have checked the “Use SSL” box in the Ignition Edge Gateway Settings (see [step 16 on page 65](#)).*

1. Open a web browser and enter: `https://[your groov Box's hostname]:10000`
Or open *groov* Admin from within Build mode (Configure > *groov* Admin).
2. Log in with your *groov* Admin username and password.
3. In the left navigation panel, click Ignition Edge.

Ignition Edge

With [Ignition Edge](#) by [Inductive Automation](#), you can use built-in OPC UA-compatible drivers for Allen-Bradley PLCs, Siemens PLCs, and other devices in your *groov* projects. (Note that Ignition Edge does not permit external access to the OPC UA server.)

You can also publish and subscribe automation data with the MQTT/Sparkplug protocol to an MQTT broker on premises or in the cloud.

Learn more about Edge and MQTT in the [groov Box User's Guide](#).

Status

- ✓ *groov* Enterprise is licensed and enabled. To get your Ignition Edge license key, email Opto 22 at pcs@opto22.com and include your *groov* Serial number: E1937S
- ✓ Ignition Edge is running. [Open Ignition Edge](#)

Configuration

☒ Enable and run Ignition Edge at startup

☐ Enable access to Ignition Edge Designer and Edge Panel

Designer is not needed to configure Allen-Bradley and SNAP PAC drivers and use their data in *groov*.

Designer is needed to:

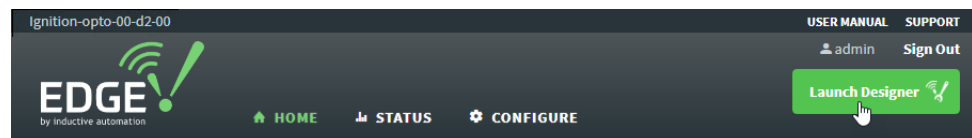
- Configure tags for Siemens PLC and Modbus drivers
- Create MQTT Transmission tags
- Update MQTT brokers with tag configurations and changes
- Use advanced features of Ignition Edge, including Panel and EAM

CAUTION: Ignition Edge Designer and Edge Panel require an insecure TCP port to be exposed by the *groov* Box firewall. Opto 22 recommends that if you check this option, you also:

1. Connect the *groov*Box only to a trusted network that blocks external requests to TCP port 8088.
2. Configure Ignition Edge to use SSL to limit the functionality available on the insecure TCP port.

NOTE: Ignition Edge Panel is an optional feature available for separate purchase. If you use it, be sure to allow connections only over HTTPS (see Ignition Edge Panel manual for details).

4. Make sure Ignition Edge is running. Under Configuration, click Enable access to Ignition Edge Designer and Edge Panel. Then click Save.
5. When the changes are marked as done, click Back. Click Open Ignition Edge.
6. When the Ignition Edge gateway page opens, click the Launch Designer button in the upper right.

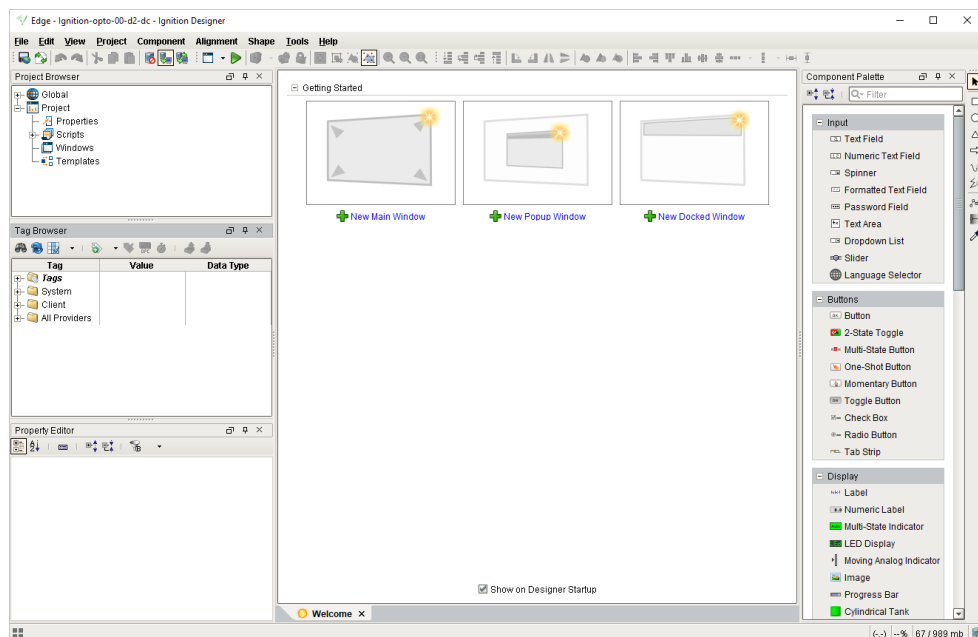


NOTE: Ignition Edge Designer is not web-based software, but a program you download from the gateway page to your computer and run locally. It requires Java to run. If you don't have Java, you can install it from the [Java website](#).

7. Save the file to your computer. Double-click it to open it. At the security warning, click Continue.



8. Log into Ignition Edge Designer using your Ignition Edge credentials. (If you have not changed them, the defaults are: admin and password)



9. To add tags for a device, follow the instructions provided by Inductive Automation:
 - [Instructions for Siemens](#)
 - [Instructions for Modbus](#)
10. For MQTT tags, set up folders for topics and put tags in them, following instructions in [documentation from Cirrus Link](#).
11. When you have finished adding tags, choose File > Save and Publish.
12. **IMPORTANT:** When you have finished configuring tags and saved them, go back to *groov* Admin. In the left navigation panel, click Ignition Edge. Uncheck "Enable access to Ignition Edge Designer and Edge Panel" and click Save to close the insecure port.
13. Remember to back up your Ignition Edge project to make sure all your tags are saved (see [page 81](#)).

USING MQTT

One of the advantages of having Ignition Edge in the *groov* Box is that you can use the Message Queue Telemetry Transport (MQTT) in your IoT application. MQTT is a publish/subscribe (pub/sub) protocol that's suited to many IoT applications because of its architecture.

In a pub/sub architecture, a central source, called a broker, stores all data. MQTT clients can publish data to the broker or subscribe to get data from it (or both). Clients who publish data send it only when the data changes. Clients who subscribe to data automatically receive it from the broker only when it changes.

Contrast this with a client/server architecture. There 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 and sent only when it changes, rather than at regular intervals.
- Because the broker is a central source with stored 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 subscriber is offline, for example, the broker buffers the data and sends it at a later time.
- For data publishers, there's another important advantage: data is published using an outbound connection. Most firewalls block inbound traffic (for example, an external OPC client requesting data from an internal OPC server), but they allow outbound connections over secure TCP ports.

See mqtt.org for more information about the protocol.

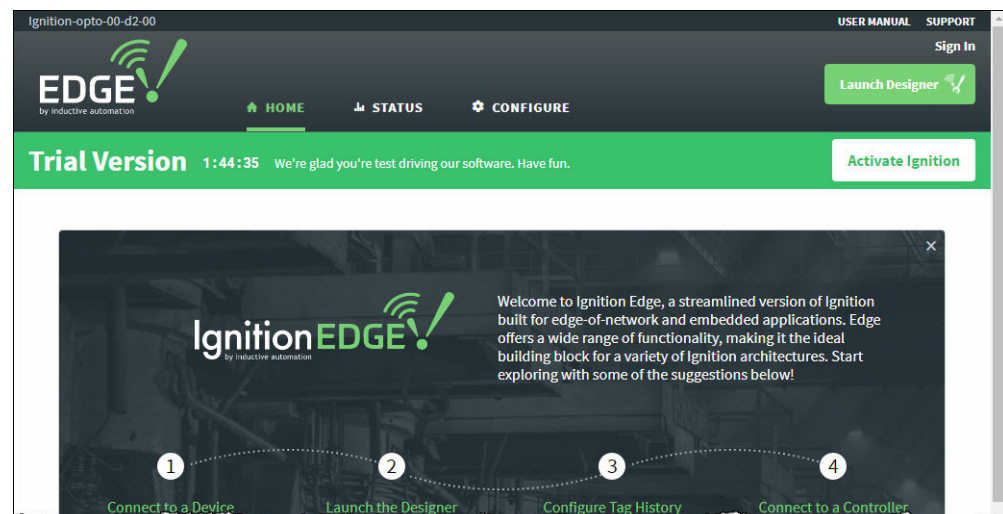
MQTT and the *groov* Box

Ignition Edge in the *groov* Box gives you access to an MQTT Transmission module built by a third party, [Cirrus Link Solutions](#). This module uses the Sparkplug open MQTT client specification. More information and documentation are available on the [Cirrus Link website](#).

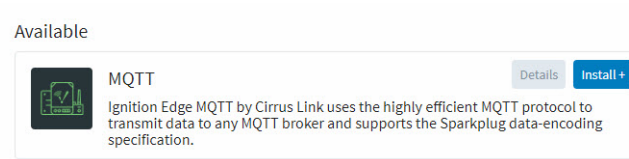
You will also need an MQTT broker, which you can locate on your premises or in the cloud; information is available online to set one up.

Install the MQTT Transmission module

1. Open the Ignition Edge gateway page: `https://[your groov Box's hostname]:8043`



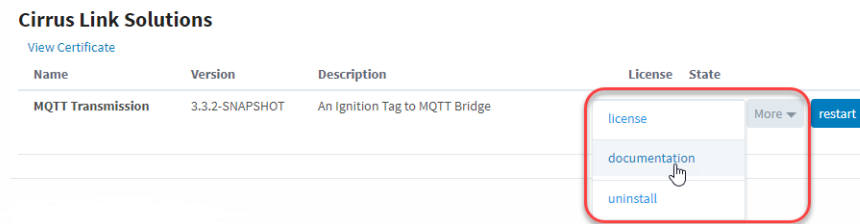
2. In the top navigation, click Configure. Scroll down till you see the MQTT plugin.



3. Click Install. In the next page, scroll down to find Quarantined modules and click the install button for MQTT Transmission. Then follow directions on the screen to accept the license.
4. Check "I want to add this certificate to my trusted certificates and install the module" and then click the button to install.

When the success message appears, you can scroll down and see the MQTT Transmission module listed under Cirrus Link Solutions.

5. To see documentation for the module, click More > documentation.



Configure the MQTT broker

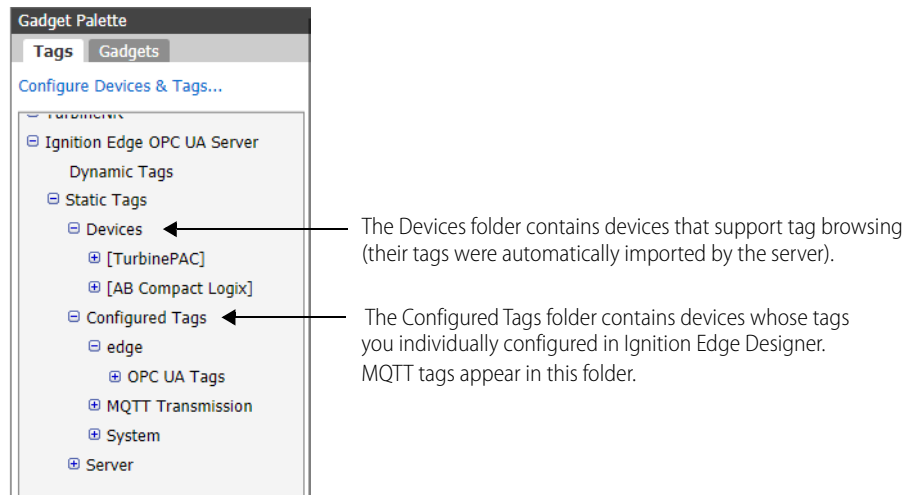
You will need an MQTT broker to handle published data and send it to subscribers. The broker can reside either locally or in the cloud. If you don't have a broker, check online for instructions to set one up. These steps show you how to configure a broker you've already set up.

1. In the Ignition Edge gateway page left navigation, choose MQTT Transmission > Settings.
2. Follow [instructions from Cirrus Link](#) to enter the URL and credentials for the MQTT broker.

Configure MQTT tags

1. Configure tags for MQTT following the steps in ["Configure tags manually" on page 70](#).

NOTE: The MQTT tags you create are individually configured tags. When you look for them in groov View, they'll appear in the Configured Tags folder:



2. When you have finished configuring your MQTT broker and tags, remember to back up your Ignition Edge project (see [page 81](#).)
3. To use the MQTT module, see [documentation from Cirrus Link](#).

MANAGING IGNITION EDGE

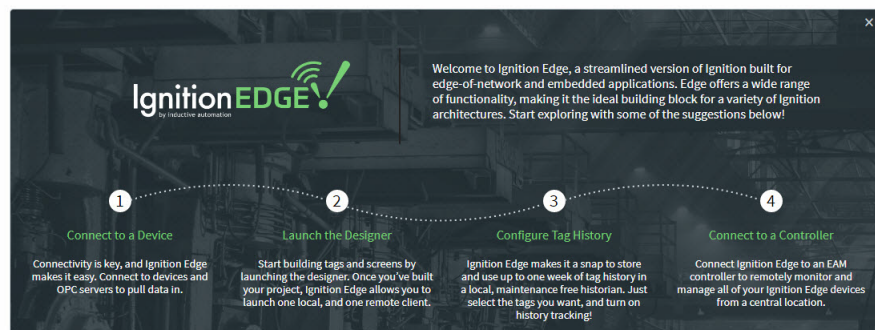
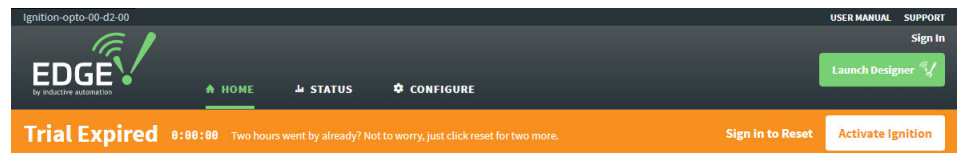
In this section:

Restart the Trial	75
License Ignition Edge	76
Unactivate Ignition Edge license	80
Change Ignition Edge password	80
Back up and restore Ignition Edge project	81
Use Ignition Edge Designer or Edge Panel	82
Ignition Edge Plugins	84
Check Ignition Edge license and modules	84
Add Quarantined Modules	85

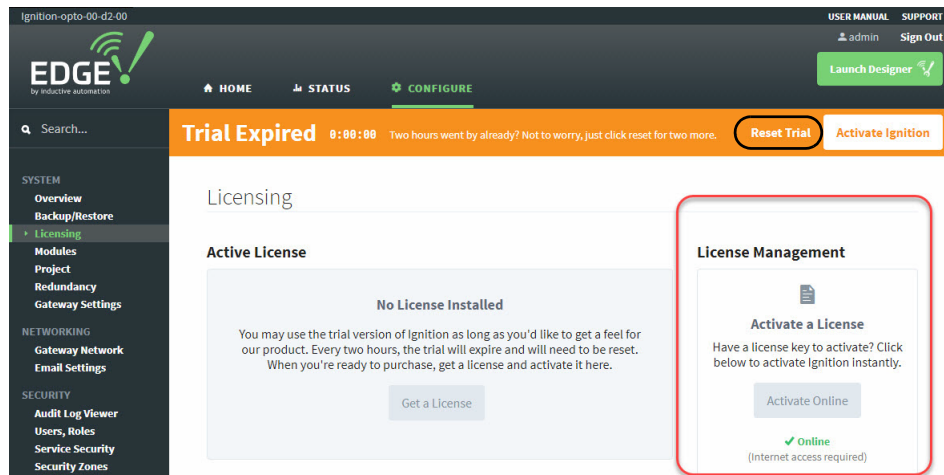
Restart the Trial

If your *groov* interface stops reporting values on gadgets you've attached to Ignition Edge, your two-hour trial may have expired. You can reset it as often as you want.

If the trial has expired, the banner color in the Ignition Edge gateway webpage changes from green to orange:



1. Click Activate Ignition to start the trial period again. Enter the username and password if asked. (If you've changed it, enter your credentials. If you haven't changed it, enter the defaults `admin` and `password` and press Enter.)



2. To start the two-hour trial again, click Reset Trial.
3. To enter your Ignition Edge license now, see “[License Ignition Edge](#),” next.

License Ignition Edge

You can use Ignition Edge for a two-hour trial without licensing it, and you can repeat the trial. But to use Ignition Edge fully, you must license it.

1. Purchase a *groov* Ignition Edge license ([GROOV-LIC-EDGE](#)).
You'll receive a certificate with an Activation Key for the license.
2. Log into [manage.groov.com](#) with your MyOpto username and password.
3. Click Activate, enter your activation key, and follow instructions to apply it to your *groov* Box. Make sure you choose the correct Box!
4. Copy the Ignition Edge License number shown on the *groov* Box profile page.
5. Open the Ignition Edge gateway page: `https://[your groov Box's hostname]:8043`
6. If you have not already changed your username and password from the defaults (`admin` and `password`), do so now:
 - a. In the Ignition Edge gateway webpage, click the Configure tab.
 - b. In the left navigation panel, choose Security > Users, Roles.

User Sources

Name	Type	Description	
default	Internal	This is the default and always present internal authentication profile.	manage users edit
opcua-module	Internal	OPC-UA clients will authenticate against this profile by default.	More ▼ edit

→ [Create new User Source...](#)

→ [Verify an Authentication Profile...](#)

- c.** For the default user, click the manage users button.

Manage Users and Roles for Profile 'default'

Users		Roles		
Username	Name	Roles	Contact Info	Schedule
admin		Administrator		Always
Edit Delete				

- d.** Click Edit and complete the following fields:
 - Username: enter new username
 - Check Change Password?
 - Password/Password: enter new password
 - (Optional) First Name/Last Name and Language: enter or change as necessary
 - e.** Scroll to the bottom of the screen and click Save Changes.
 - f.** In the top right corner of the page, click Sign Out. Then sign back in using your new username and password.
 - 7.** Click Activate Ignition (upper right).

Ignition-opto-00-d2-00

USER MANUALSUPPORTadminSign OutLaunch Launcher

HOMESTATUSCONFIGURE

Trial Expired0:00:00Two hours went by already? Not to worry, just click reset for two more. Reset TrialActivate Ignition

SYSTEMOverviewBackup/RestoreLicensingModulesProjectRedundancyGateway SettingsNETWORKINGGateway NetworkEmail SettingsSECURITYAudit Log ViewerUsers, RolesService SecuritySecurity Zones

LicensingActive LicenseNo License InstalledYou may use the trial version of Ignition as long as you'd like to get a feel for our product. Every two hours, the trial will expire and will need to be reset. When you're ready to purchase, get a license and activate it here.Get a License

License ManagementActivate a LicenseHave a license key to activate? Click below to activate Ignition instantly.Activate OnlineOnline(Internet access required)

- Under License Management at the right, if your *groov* Box has internet access, click Activate Online. If your *groov* Box does not have internet access, go to [“Activate Offline” on page 78](#).

Licensing / Activate Online

Activate Your Ignition License

Already have an Ignition license key? You're in the right place. Use this form to activate your 6-digit license key.

Note that for each license key, only one Ignition Gateway instance is allowed to be activated at a given time. If you want to activate Ignition on a different server, you must first unactivate the previous server.

Enter license key

✓ **Online**

Internet access required

- To activate online, enter the Ignition Edge license key you copied in [step 4](#), and click Activate. A confirmation message appears, stating that your license was successfully activated.


Licensing

License NNN-NNN successfully activated

Activate Offline

Use these steps if your *groov* Box does not have internet access.

- In the Ignition Edge gateway page, click Activate Ignition. Scroll down and find No Internet Connection?



No Internet Connection?

No problem! You can start or continue the offline activation process by creating an activation request file for Ignition.

- Click Activate Offline.

Licensing / Activate Offline

Activate Ignition Offline

If you do not have an internet connection on this gateway, or if you are behind a firewall, proxy or anti-virus software which is preventing online activation, Ignition will not be able to contact the activation server and an offline activation may be necessary.

Follow the steps below to manually activate Ignition on your machine:

1

Download Offline Activation Request

Enter your license key below, then download and save the activation request file somewhere convenient.

(a USB thumbdrive, for example)

Download Activation Request

2

Upload To Our Website & Download Your License File

Transfer your activation request file to a computer with an internet connection, then upload it at:

<https://links.inductiveautomation.com/activation>

3

Return Here & Upload License File

Our website will provide you with the necessary license.ipl file for your Ignition activation here.

Choose .ipl file to upload

No file chosen

Activate

Please note that you need to have access to a machine with internet access as part of this process, but this does not have to be the machine on which you are trying to activate Ignition.

3. Under 1, enter the Ignition Edge license key you copied. Click Download Activation Request.
4. Save the Request (a text file) to your computer.
If your computer is not online, you can save the file to a flash drive and take it to a computer that does have an internet connection. The next few steps require internet access.
5. Under 2, click the link to Inductive Automation.

Activate or Unactivate Ignition

Activate Ignition

Download the activation request file (activation_request.txt) from the Ignition Gateway and save it somewhere convenient. Once saved, browse for the file below then click Upload Activation File to proceed with your request.

Activation File

No file chosen

Upload Activation File

6. In the Activate Ignition section, click Choose File, find the text file you just downloaded, and open it. Then click Upload Activation File. A license file is downloaded; save it to your computer.
7. Go back to the gateway page. Under 3, click Choose File, find the license file, and open it. Click Activate.

A confirmation message appears, stating that your license was successfully activated.

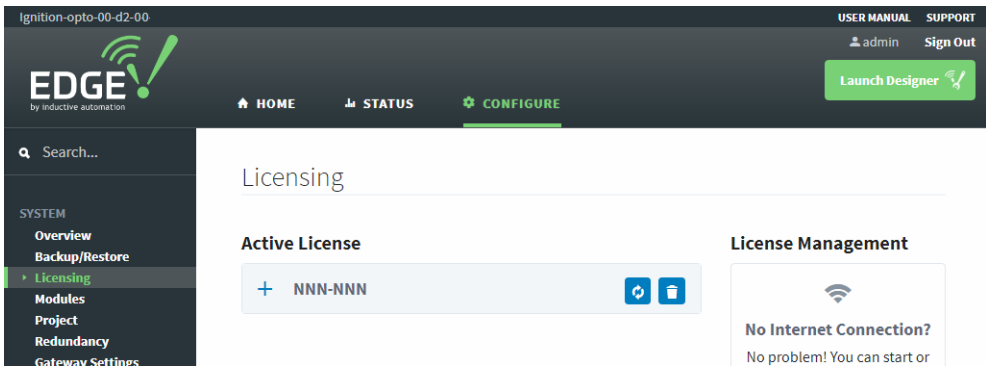
Licensing

License NNN-NNN successfully activated

Unactivate Ignition Edge license

Before you update *groov* Admin or reset your *groov* Box to factory defaults, be sure to deactivate your Ignition Edge license. Then when the update or reset is finished, activate the license again. By deactivating and then reactivating, you avoid having to contact Ignition Edge to have the license reinstated.

1. Open the Ignition Edge gateway page: `https://[your groov Box's hostname]:8043`
2. Click the Configure tab. In the left navigation panel, choose System > Licensing.



3. **IMPORTANT:** Make sure you have a record of your license number, so you can reactivate it later.
4. To deactivate, click the trash can button next to your license number.
5. To confirm, click Yes, Unactivate.

When you're ready to activate your license again, follow steps in ["License Ignition Edge"](#) on page 76.

Change Ignition Edge password

You can change your username and password for Ignition Edge whenever you want to. Be sure you change them when you license Ignition Edge (see [page 76](#)).

1. In the Ignition Edge gateway webpage, click the Configure tab.
2. In the left navigation panel, choose Security > Users, Roles.

User Sources

Name	Type	Description	
default	Internal	This is the default and always present internal authentication profile.	manage users edit
opcua-module	Internal	OPC-UA clients will authenticate against this profile by default.	More edit

→ [Create new User Source...](#)

→ [Verify an Authentication Profile...](#)

- For the default user, click the manage users button.

Manage Users and Roles for Profile 'default'

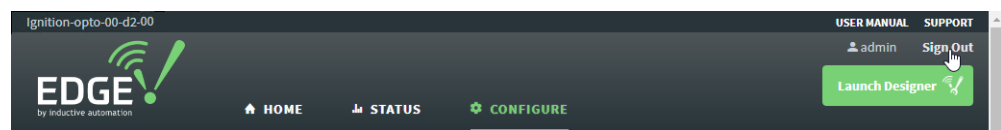
Users

Roles

Username	Name	Roles	Contact Info	Schedule	
admin		Administrator		Always	<a>Edit <a>Delete

→ Add User

- Click Edit and complete the following fields:
 - Username: enter new username
 - Check Change Password?
 - Password/Password: enter new password
 - (Optional) First Name/Last Name and Language: enter or change as necessary
- Scroll to the bottom of the screen and click Save Changes.
- In the top right corner of the page, locate Sign Out.



- Click Sign Out. Then sign back in using your new username and password.

Back up and restore Ignition Edge project

Remember to back up your Ignition Edge project when you first configure Ignition Edge, devices, and tags, and also when you change configurations.

- Open the Ignition Edge gateway page: `https://[your groov Box's hostname]:8043`
- Click the Configure tab.
- In the left nav, choose System > Backup/Restore.

System Backup / Restore

Backup

Restore

Legacy Upgrade

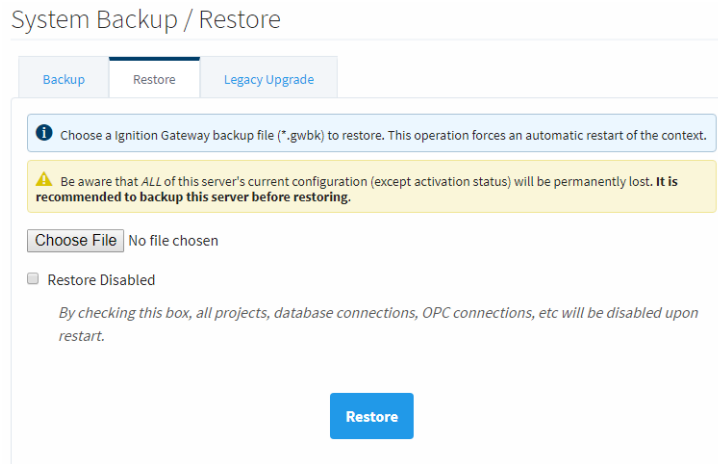
Download Backup

Backs up the *user data* inside this Ignition Gateway server. This includes all projects, drivers, images, and configuration, but not the modules.

- Click Download Backup and save the file to your computer.

Restore Ignition Edge project

1. Open the Ignition Edge gateway page: `https://[your groov Box's hostname]:8043`
2. Click the Configure tab.
3. In the left nav, choose System > Backup/Restore.
4. Click the Restore tab.



5. Click Choose File and locate the backup file you saved to your computer. Then click Restore.

Use Ignition Edge Designer or Edge Panel

You can access Ignition Edge Designer from the Ignition Edge gateway page if you need to use it. Designer is **not** needed to configure Allen-Bradley and SNAP PAC drivers and use their data in *groov* View.

Designer **is** needed to:

- Configure tags for Siemens PLC and Modbus drivers (see ["Configure tags manually" on page 70](#))
- Create MQTT Transmission tags (see ["Using MQTT" on page 73](#))
- Configure and update MQTT brokers with tag configurations and changes
- Use Ignition Edge OPC-UA tags in Node-RED flows
- Use advanced features of Ignition Edge, including Panel and EAM. Ignition Edge EAM, Panel, and the Vision module are available for separate purchase from Inductive Automation.

CAUTION: *Ignition Edge Designer and Edge Panel require an insecure TCP port to be exposed by the groov Box firewall. Opto 22 recommends that while you are using Designer or Panel, you:*

- *Connect the groov Box only to a trusted network that blocks external requests to TCP port 8088.*
- *Make sure you configure Ignition Edge to use SSL (see [step 16 on page 65](#)).*

1. Open a web browser and enter: `https://[your groov Box's hostname]:10000`
Or open *groov* Admin from within Build mode (Configure > *groov* Admin).
2. Log in with your *groov* Admin username and password.
3. In the left nav, click Ignition Edge.

Ignition Edge

With [Ignition Edge](#) by [Inductive Automation](#), you can use built-in OPC UA-compatible drivers for Allen-Bradley PLCs, Siemens PLCs, and other devices in your *groov* projects. (Note that Ignition Edge does not permit external access to the OPC UA server.)

You can also publish and subscribe automation data with the MQTT/Sparkplug protocol to an MQTT broker on premises or in the cloud.

Learn more about Edge and MQTT in the [groov Box User's Guide](#).

Status

✓ *groov* Enterprise is licensed and enabled. To get your Ignition Edge license key, email Opto 22 at pcs@opto22.com and include your *groov* Serial number: E1937S

✓ Ignition Edge is running. [Open Ignition Edge](#)

Configuration

☒ Enable and run Ignition Edge at startup

☐ Enable access to Ignition Edge Designer and Edge Panel

Designer is not needed to configure Allen-Bradley and SNAP PAC drivers and use their data in *groov*.

Designer is needed to:

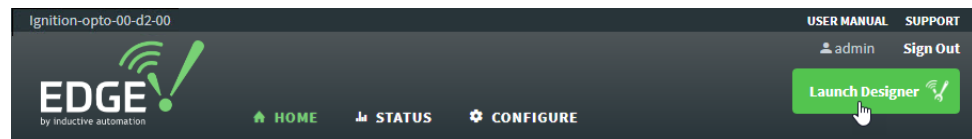
- Configure tags for Siemens PLC and Modbus drivers
- Create MQTT Transmission tags
- Update MQTT brokers with tag configurations and changes
- Use advanced features of Ignition Edge, including Panel and EAM

CAUTION: Ignition Edge Designer and Edge Panel require an insecure TCP port to be exposed by the *groov* Box firewall. Opto 22 recommends that if you check this option, you also:

1. Connect the *groov*Box only to a trusted network that blocks external requests to TCP port 8088.
2. Configure Ignition Edge to use SSL to limit the functionality available on the insecure TCP port.

NOTE: Ignition Edge Panel is an optional feature available for separate purchase. If you use it, be sure to allow connections only over HTTPS (see Ignition Edge Panel manual for details).

4. Make sure Ignition Edge is running. Under Configuration, click Enable access to Ignition Edge Designer and Edge Panel. Then click Save.
5. When the changes are marked as done, click Back. Click Open Ignition Edge.
6. When the Ignition Edge gateway page opens, click the Launch Designer button in the upper right.



NOTE: Designer is not web-based software, but a program you download from the gateway page to your computer and run locally. It requires Java to run. If you don't have Java, you can install it from the [Java website](#).

7. Log into Designer using your Ignition Edge credentials. (If you have not changed them, use the default username `admin` and password `password`.)
8. To use Designer:
 - a. If you are configuring tags for Siemens PLC and Modbus drivers, see [“Configure tags manually” on page 70](#).
 - b. If you are using MQTT, see [“Using MQTT” on page 73](#).

- c. For other uses, follow Ignition's instructions.
9. When you have finished using Designer or Panel, return to *groov* Admin and uncheck the box to disable access and close the insecure port.

Ignition Edge Plugins

The Ignition Edge gateway Configure page shows plugin options you may be interested in:

- Ignition Panel (free trial included; to purchase, contact Inductive Automation)
- Ignition Enterprise (free trial included; to purchase, contact Inductive Automation)
- **Ignition Edge MQTT by Cirrus Link**—If you plan to use the MQTT protocol, you'll want this module. See [“Using MQTT” on page 73](#)

Check Ignition Edge license and modules

You can see which Ignition Edge modules you have licensed, and which are available.

1. Open the Ignition Edge gateway page: `https://[your groov Box's hostname]:8043`
2. Click the Status tab.
3. In the left nav under Systems, click Modules.

You see all the modules you have. In the License column, the modules that show “Activated” are licensed, and those that show “Trial” are not. The Status column shows which modules are currently running.

The screenshot shows the Ignition Edge gateway interface. The top navigation bar includes 'HOME', 'STATUS' (selected), and 'CONFIGURE'. The left sidebar shows 'SYSTEMS' with 'Modules' selected. The main content area displays 'Systems Modules' with a 'Licensing Configuration' button. It shows 'Running Modules' (9/9) and 'Licensed Modules' (7/9). A 'License Details' table shows the license key, version, and edition. Below this is a table of modules with columns for Name, Version, License, and Status. At the bottom, there is a section for 'Quarantined Modules' with columns for Name, Version, and Quarantine Reason.

Name	Version	License	Status
Alarm Notification	4.9.4 (b2017082918)	Activated	✓ RUNNING
Allen-Bradley Driver	4.9.4 (b2017082911)	Activated	✓ RUNNING
Enterprise Administration	2.9.4 (b2017082911)	Trial	✓ RUNNING
Logix Driver	3.9.4 (b2017082911)	Activated	✓ RUNNING
Modbus Driver	5.9.4 (b2017082911)	Activated	✓ RUNNING
OPC-UA	4.9.4 (b2017082911)	Activated	✓ RUNNING
Siemens Drivers	4.9.4 (b2017082911)	Activated	✓ RUNNING
Tag Historian	2.9.4 (b2017082911)	Activated	✓ RUNNING
Vision	9.9.4 (b2017082918)	Trial	✓ RUNNING

Name	Version	Quarantine Reason
MQTT Transmission	3.4.6 (b2019030100)	Certificate has not been accepted. License has not been accepted.
Opto 22 groov EPIC and SNAP PAC Driver	3.4.6 (b2019030100)	Certificate has not been accepted. License has not been accepted.

At the bottom are modules that are available to license. See [“Add Quarantined Modules” on page 85](#).

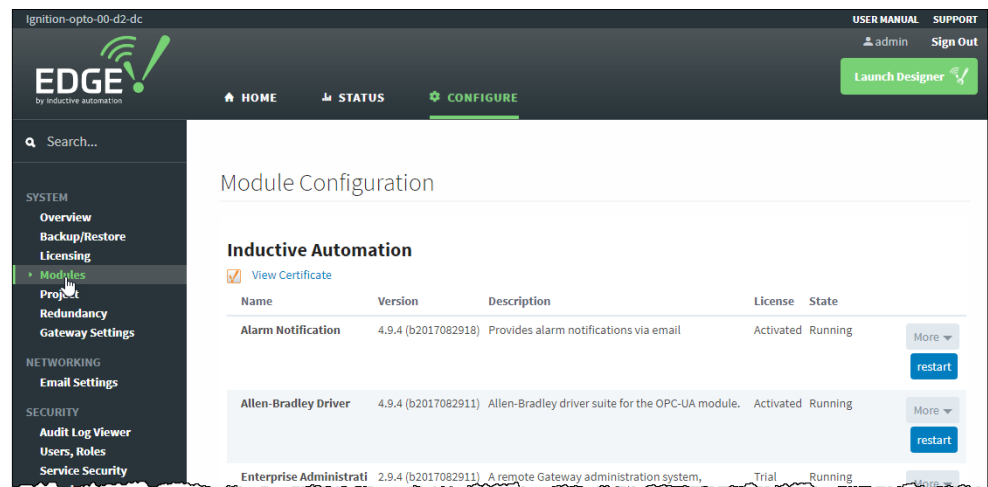
Add Quarantined Modules

Two modules are included in Ignition Edge on the *groov* Box but not enabled until you install them:

- MQTT Transmission—for using the MQTT protocol with Sparkplug messaging. See [“Using MQTT” on page 73](#).
- Opto 22 *groov* EPIC and SNAP PAC Driver—for using *groov* EPIC or SNAP PAC programmable automation controller tags with MQTT or with other Ignition software.

To install a quarantined module:

1. In the Ignition Edge gateway webpage, click the Configure tab. In the left navigation bar under System, click Modules.




2. Scroll down till you see Quarantined Modules.

Quarantined Modules

Name	Version	Description	Quarantine Reason	
MQTT Transmission	3.4.6 (b2019030100)	An Ignition Tag to MQTT Bridge	Certificate has not been accepted. License has not been accepted.	delete install
Opto 22 groov EPIC and SNAP PAC Driver	3.4.6 (b2019030100)	A driver for communicating with groov EPIC and SNAP PAC series controllers	Certificate has not been accepted. License has not been accepted.	delete install

3. Click the Install button next to the module you want to add. Click confirm when asked.
4. Read the license and check the box at the bottom of the page. Click Accept License.

Module Certificate

 This certificate has been signed by a trusted Certificate Authority.

Not Valid Until	3/14/17 12:00:00 AM
Not Valid After	5/25/20 11:59:59 PM
Subject Name	Cirrus Link Solutions
Issuer Name	thawte SHA256 Code Signing CA
Thumbprint	[31 EC 97 F5 4D C5 EB A8 B5 DD A8 1F 8B 00 18 F6 E2 2D CD 53]

This module's certificate has been signed by a trusted Certificate Authority.

☐ I want to add this certificate to my trusted certificates and install the module

Add Certificate and Install Module

5. Check the box to add the certificate and install the module, and then click the button. You see a success message, and when you scroll down you find the installed module is no longer quarantined. It's ready to use.

6: Using an SSL Certificate

UNDERSTANDING CERTIFICATES

Like other web servers that contain sensitive data—for example, your bank—the *groov* Box uses an SSL/TLS certificate to (1) encrypt communications and (2) prove the Box's identity to client browsers. This certificate contains the server name, the name of the organization that controls the server, and digital signatures of organizations that vouch for the authenticity of the certificate. The certificate is digitally signed either by a *certificate authority* (CA) or it is *self-signed*.

The default certificate type (a self-signed certificate) and configuration will cause your web browser to issue an untrusted site warning when accessing the *groov* Box. To avoid the warning you can install the self-signed certificate in all the browser certificate stores used to access the Box. However, whether or not the certificate is installed in the certificate stores, communication between the Box and client browsers is always encrypted.

Here's a comparison of the certificate types:

	Self-Signed Certificate (default)	Self-Signed Certificate installed on all browser certificate stores	CA-Signed Certificate
Best Use	For one or two <i>groov</i> products and a small set of client browsers that remain pretty much the same, and users who trust that your certificate is valid	Same as default, plus it avoids seeing the untrusted site warning from the browser	Use with a system with many <i>groov</i> products or where the set of browsers that will access them is unknown or changes frequently, or for users who will not trust your self-signed certificate
Cost	Free	Free	Public CA-signed certificates cost anywhere from \$9 to \$100 or more per year
Ease of Configuration	Easiest configuration	Must install in the browser certificate store for every browser that accesses the server	More complex initial configuration because a certificate authority signature must be obtained
Untrusted Site Warning	Browser raises untrusted site warning. (But communication is still encrypted.)	No untrusted site warning from browser	No untrusted site warning from browser. Trusted by all major browsers.
Trust Level	Trusted by those to whom the <i>groov</i> Box administrator has demonstrated the validity of the certificate (e.g. by providing the certificate thumbprints).	Trusted by those who trust the <i>groov</i> Box administrator enough to install or let him or her install the certificate in their browser certificate store	Trusted by everyone

STEP 1: BACK UP YOUR GROOV VIEW PROJECT

Certificate Structure

Whether you use a self-signed or CA-signed certificate, your certificate contains 3 parts:

Private Key—The private key is secret. Put it in a very safe place and make sure it remains secure.

Server Certificate—The server or hostname certificate is generated by the self-signed certificate process or is obtained via the CA (Certificate Authority).

Intermediate Certificate (chain.cert)—A certificate signed by a CA may or may not include this intermediate certificate as part of a chained certificate path.

STEP 1: BACK UP YOUR *groov* VIEW PROJECT

IMPORTANT: Before starting any certificate process, back up your *groov* View project. See [“Backing Up *groov* View and Network Settings” on page 32](#) for instructions. Certificates can be tricky, and you want to make sure you can recover if needed.

After you’ve backed up your *groov* View project, follow steps in the next section to create a private key.

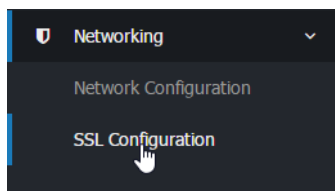
STEP 2: CREATE A PRIVATE KEY

Follow the steps below to generate the following components.

- **Private Key:** This must be kept secret and never shared. Keep a copy of it in a safe and secure place. There is also a **Public Key** included in the signed certificate. You will not handle the public key using *groov* Admin.
- **Signed Certificate:** Contains identification information, the public key, and a digital signature. Identification information includes the server name and the name of the organization that controls the server. The self-signed certificate is digitally signed by the Private Key to establish authenticity. The Certificate is automatically installed on the *groov* Box.
- **Certificate Signing Request (CSR).** If you want to use a CA-signed certificate, you will need this CSR.

To generate a private key:

1. In *groov* Admin, select Networking > SSL Configuration.



2. Click the Create certificate tab.
3. Fill in the Create SSL key form as follows:

Server name: Enter the [fully qualified domain name](#) (or *hostname*) of this *groov* Box that client browsers will use to access *groov*. (Also see [“Changing the Hostname, DNS Servers, or IPv4 Gateway” on page 25.](#)) 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.

For example, if the URL you will use to access *groov* View in client browsers is <https://process1.acme.com>, then you enter `process1.acme.com`

Email address: (optional) Enter the email address of the person responsible for administering this certificate.

Department: Use this field to differentiate between divisions within an organization. For example, you might enter "Engineering" or "Manufacturing." If applicable, you can enter the DBA (doing business as) name in this field.

Organization: The legally registered name of your business. This business must be the legally registered owner of the domain name.

City or Locality: Name of the city or locality where your organization is located. Spell out the name of the city or locality. Do not abbreviate.

State: Full name of the state, province, region, territory where your organization is located. 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. [Click here for](#) a complete list of ISO country codes.

RSA key size: Both the public key and the private key. The recommended key size is 2048 bits. Avoid key sizes smaller than 2048 bits.

Days before expiry: Enter the number of days before the self-signed certificate is expired and has to be replaced. It's up to the *groov* Box administrator how many days to enter. For example, if you want the certificate to be valid for 10 years, enter 3650.

- 4.** Click Create Now.

groov Admin creates the following and displays them all in the same window:

- New private key
- Self-signed certificate
- Certificate signing request (CSR) to obtain a CA-signed certificate

[illegible]

At this point, the new self-signed certificate is installed on the *groov* Box and network services restarts.

5. Copy the **private key** portion of text in its entirety, including the title portion

"==== Private Key =====" and paste it to a file named `<server name>-key.pem` (where `<server name>` is replaced by the server name value you entered on the Create SSL key form.) **Save this file in a secure place** and do not share it with anyone.

IMPORTANT: Do not lose the private key! You will need it if you are using a CA-signed certificate. Also, you must keep a copy of it to restore later in case you commission a replacement groov Box or have to restore the Box to factory defaults. You cannot go back and get it again.

6. Continue with the next section.

STEP 3: GET AND USE THE CERTIFICATE

For a **self-signed certificate**, continue with [“Using a Self-Signed Certificate,”](#) below.

For a **CA-signed certificate**, see [“Using a CA-Signed Certificate on the groov Box”](#) on page 95.

Using a Self-Signed Certificate

A self-signed certificate encrypts communications, but does not include a digital signature from a commercial CA. It is free and easy to configure, but if you want to avoid having your users see an untrusted site warning every time they use *groov*, you must install the self-signed certificate in the browser certificate store for every browser that will access *groov*. This type of certificate is a good solution for a small set of *groovs* and a small set of client browsers that you can configure.

Follow these steps to use a self-signed certificate:

[“Finish the Self-Signed Certificate”](#) on page 90

[“Add the Self-Signed Certificate to a Browser Trust Store on a Computer”](#) on page 91

[“Install an SSL Certificate on Mobile Devices”](#) on page 94

Finish the Self-Signed Certificate

When you created the private key ([“Step 2: Create a Private Key”](#) on page 88), you also created a self-signed certificate. Continue with these steps to finish.

1. **IMPORTANT:** *Before proceeding*, wait for the SYS LED on the *groov* Box to stop blinking green, then make sure to refresh your browser.
It might take some time, but eventually you should see the security warning. (The security warning appears because the new certificate that was just installed on the *groov* Box is not trusted by the browser.)
2. Accept the security warning as described below.



For Chrome: Click “Proceed anyway.”



For Firefox:

- Expand “I Understand the Risks.”
- Click Add Exception to open the Add Security Exception dialog box.
- Select “Permanently store this exception.”
- Click Confirm Security Exception.

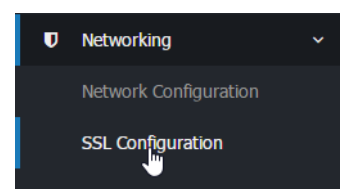


For Internet Explorer 10: Click “Continue to this website (not recommended).”



For Safari: Click Continue.

3. When *groov* Admin returns, select Networking > SSL Configuration.
4. Click the Current Certificate tab, then select “PEM format.”



Help... **SSL Encryption**

Current certificate [Create certificate](#) [Upload certificate](#)

This section shows the details of the current *groov* Admin SSL certificate, and allows it to be downloaded so that it can be accepted by your browser.

Details of current certificate			
Authority name	opto-00-d2-dc	Organization	groov on opto-00-d2-dc
Issuer name	opto-00-d2-dc	Issuer organization	groov on opto-00-d2-dc
Valid until	Mar 24 20:27:52 2046 GMT	Certificate type	Self-signed
Download certificate	PEM format PKCS12 format CSR		



The certificate's text appears.

```
-----BEGIN CERTIFICATE-----
MIIEBTCCAu2gAwIBAgIJAMz8yixPBBGyMA0GCSqGSIb3DQEBCwUAMIGYMawCQYD
VQQGEwJVUzELMAkGA1UECAwCQ0ExETAPBgNVBACMCFRlbWVjdWxhbmSEwHwYDVQK
DBhPUFRPIDIyIG9uIG9wdG8tMDAtZDItZGMxDDAKBgNVBAsMA0VuzZEWMBQGA1UE
AwwNMTkyLjE2OC4wLjEwNDEgMB4GCSqGSIb3DQEJARYRZHNjYXJyYyYyYyYyYyYy
b20wHhcNMTUwMjEwMjEzNTU3WhcNNDUwMjEwMjEzNTU3WjCBMDELMAkGA1UEBhMC
VVMxCzAJBgNVBAGMAkNBMRFEwYDVQQHDAhUZW11Y3VsYTEhMB8GA1UECgwYT1BU
TyAyMiBvbiBvcHRvLTAwLWQyLWRjMQwwCgYDVQQQLDANFmckFjAUBgNVBAMMDTE5
Mi4xNjguMCA4xMDQxIDAeBgkqhkiG9w0BCQEWERzY2FyckBvcHRvMjE1Y29tMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApmvdtAtfSBegut+qy0C20QP
HJspbae+OP1mKl8LRSXGmOkC1+U12qMf7vVpokFD21Xmg/ytBOCfcjPuxriGCh5
3RF7mdF4RBaZOTnF7Y3cqdBtQ087UPUfAsv6BXyLXA3qlFMnnspl+Jrh81/dNwN/
twIS0rgrDf1j3ugGdV0e4wzZ+SGqoYiIVkASUzV5a3+2SCfojRYxmvvSnfew9Lg4
GWUJMTW0qmpCwXgBOIasXzyvxxwIO4zqZEygbVhnlTjCgSxhnm/8607s61Rh7Fd
Zt11vEj8X/T/oDceFp7Na48fKUGggj07ubcYEWiAnWpLbA/8LdfW4mDoSk2bhQID
AQABolAwTjAdBgNVHQ4EFgQUb+2Tvx3Rpg3b9ZB1hwrZiIitutsWwHwYDVROjBBGw
FoAub+2Tvx3Rpg3b9ZB1hwrZiIitutsWwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0B
AQsFAAOCAQEAA71G7qjadOdWHldBwA0VMu85uHzi+NUDLQDVoyJQ2+TVEOgC4m+x
p2wuf/c4+RAvTOeNzxYgvt2iVCmH1vyZW0VJ3OIXSfgdgkLjN7xioYW5SjttqOG
g4xGAsN1opxG4Nut9ubjYLSjibF71iGzu4d5/PLhQDHQAUIWHk+sHyQDiWASgeH0
Spft39SKnNgBLBASwRCnmasqylTYwh1D9AHWAZVI3h0xCv1qxhKhjRKRWA5bqrG
c5fm0eXf3cGe/YYaDn9iWdt/7fHnJZ7ACncXQVXxjTdf81Z2Ca9ge2y4E/+ox0Yj
Cg801mjL70Bjs96jP9YbWJO+BOGbkhoTjw==
-----END CERTIFICATE-----
```

If you have multiple certificates and have any doubt about whether this is the right one, open up the certificate in Windows. When the certificate wizard/explorer opens, you can see the hostname the certificate was created for.

- Copy the certificate text and paste it to a file named `<server name>.cer` (where `<server name>` is replaced by the server name value you entered on the Create SSL key form in [step 3](#) on [page 88](#).)

Add the Self-Signed Certificate to a Browser Trust Store on a Computer

To prevent the untrusted site warning in browsers, the self-signed certificate must be added to the trust store for each browser used to access the *groov* Box or *groov* View. This section describes how to add a self-signed certificate on a computer. [Step 3](#) describes how add a self-signed certificate on a mobile device.

See the section below for the client computer's operating system.

["Windows" on page 91](#)

["OS X" on page 93](#)

Windows

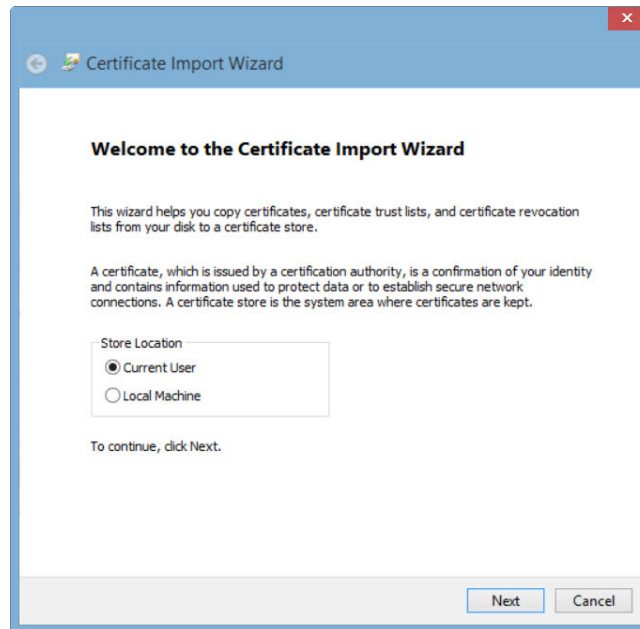
Internet Explorer & Chrome.

- In Windows file explorer, locate the `<server name>.cer` file you created in the previous step.

STEP 3: GET AND USE THE CERTIFICATE

2. Right-click on the file and choose Install Certificate.
The Certificate Import Wizard appears.

Windows 8



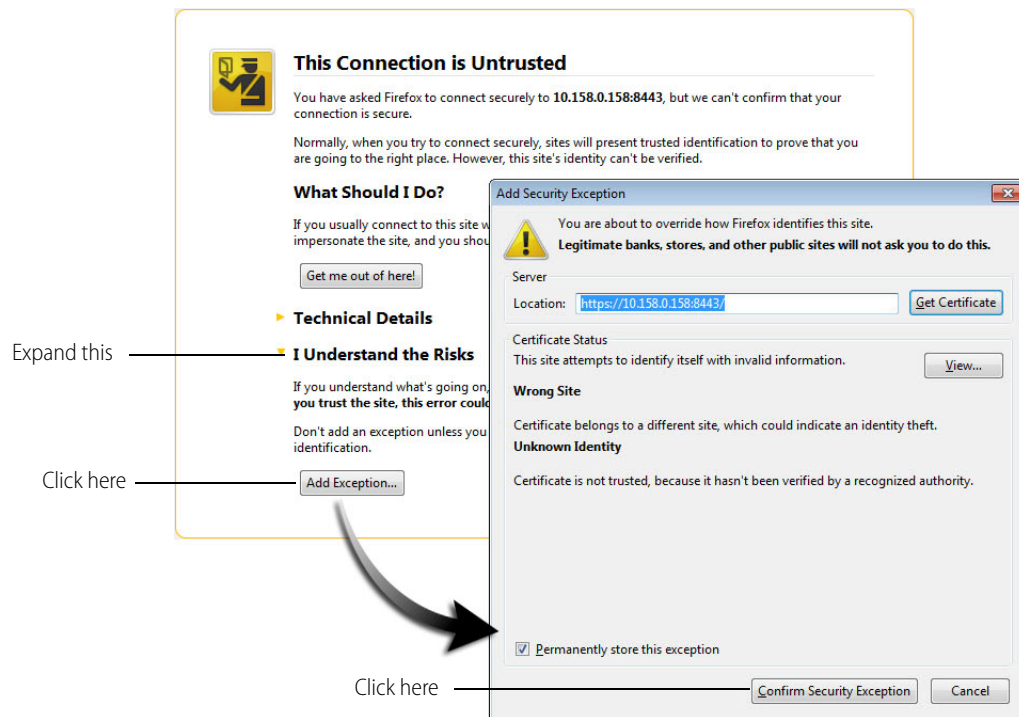
3. (Windows 8 only) If you are administrator of local machine, choose the Local Machine certificate store so this certificate will be trusted by all user accounts. Otherwise it will only be trusted by the current user account.
4. Click Next.
5. Select "Place all certificates in the following store."
6. Click Browse to open the Select Certificate Store dialog box.
7. Select Trusted Root Certification Authorities, and then click OK.
8. Click Next.
9. Click Finish.
10. A security warning alerts you that certificate installation is a risk if you don't trust the certificate.
11. Click Yes to affirm that you trust the self-signed certificate.
12. To verify the certificate was installed correctly, open Internet Explorer or Chrome and enter the hostname specified on the certificate. If the browser does not generate an untrusted site warning, the certificate was installed correctly.

Firefox.

The self-signed certificate is added to the certificate store by adding a security exception. Firefox will present several warnings about creating a security exception for a self-signed certificate, but because you created and control the private key and certificate and installed the private key on the server, you can trust that the certificate identifies your server.

1. Open Firefox and enter `https://<server name>`
A warning appears that says, "This Connection is Untrusted."
2. Expand "I Understand the Risks."
3. Click Add Exception to open the Add Security Exception dialog box.
4. Select "Permanently store this exception."

- Click Confirm Security Exception.

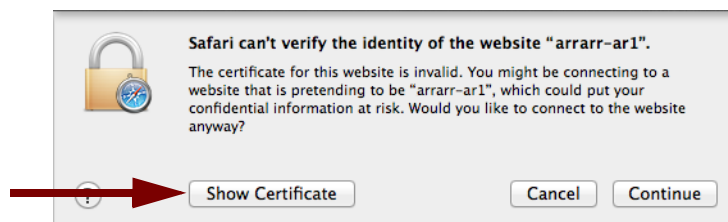


- To verify the certificate was installed correctly, open Firefox and enter the hostname specified on the certificate. If the browser does not generate an untrusted site warning, the certificate was installed correctly.

OS X

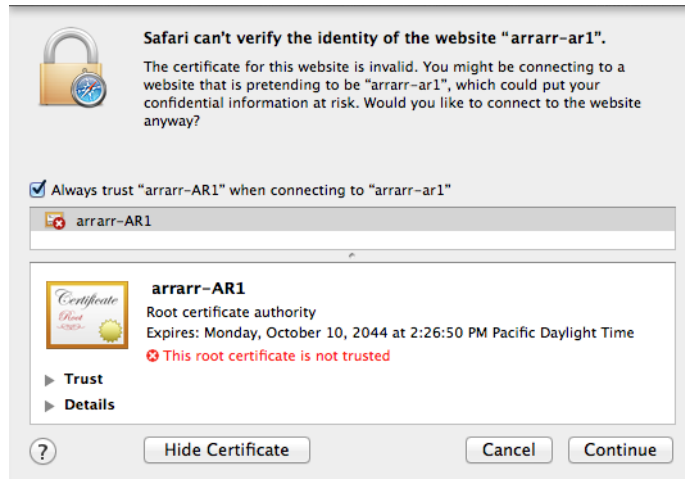
Safari and Chrome.

- Open Safari and enter `https://<server name>` to open this dialog box:



- Click Show Certificate to reveal the full details:

STEP 3: GET AND USE THE CERTIFICATE



3. If the certificate looks good to you, check the "Always trust <server name> when connecting to <server name>" and click Continue. You will be asked to provide your password to authorize the addition of this certificate to your keychain, after which the browser and the Hosted Projects window will accept the SSL certificate as valid.
4. To verify the certificate was installed correctly, open a browser and enter the hostname specified on the certificate. If the browser does not generate an untrusted site warning, the certificate was installed correctly.

Install an SSL Certificate on Mobile Devices

When you open the operator interface in a browser on a smart phone or tablet, a security warning will appear unless you have installed a self-signed SSL certificate. See the section below for the device's operating system.

- ["iOS Devices" on page 94](#)
- ["Android Devices" on page 94](#)

iOS Devices.

1. Email the <server name>.cer file you created previously (see ["Step 2: Create a Private Key" on page 88](#)) to an email account accessible from iOS.
2. On the iOS device, open the email message containing <server name>.cer.
3. Tap on <server name>.cer
4. A message appears, "The authenticity of <server name> cannot be verified..."
5. Click Install.
6. Click Install Now.
7. Click Done.
8. To verify the certificate was installed correctly, open a browser and enter the hostname specified on the certificate. If the browser does not generate an untrusted site warning, the certificate was installed correctly.

Android Devices.

1. Email the <server name>.cer file you created previously (see ["Step 2: Create a Private Key" on page 88](#)) to an email account accessible from Android.
2. On the Android device, open the email and click the <server name>.cer file to install the certificate.
3. When prompted for a certificate name, type in a name. Make sure "Credential use:" is set to "VPN and apps."
4. Click OK.

5. To verify the certificate was installed correctly, open a browser and enter the hostname specified on the certificate. If the browser does not generate an untrusted site warning, the certificate was installed correctly.

Using a CA-Signed Certificate on the *groov* Box

A **CA-signed certificate** contains identification information, the public key, and a digital signature. Identification information includes the server name and the name of the organization that controls the server. The certificate is digitally signed by a CA to establish authenticity. The Certificate is installed on the *groov* Box or Server.

To obtain the certificate, you send the certificate signing request (CSR) to the Certificate Authority (CA) of your choice. The CA verifies the identification information and signs the CSR, which then becomes a CA-signed Certificate. Follow these steps to obtain and use the certificate.

[“Finish the CSR”](#) (see [page 95](#))

[“Obtain a CA-Signed Certificate”](#) (see [page 96](#))

[“Install the CA-Signed Certificate on the *groov* Box”](#) (see [page 97](#))

Finish the CSR

When you created the private key ([“Step 2: Create a Private Key” on page 88](#)), you also created a certificate signing request (CSR). Continue with these steps to finish.

1. **IMPORTANT:** *Before proceeding*, wait for the SYS LED on the *groov* Box to stop blinking green, then make sure to refresh your browser.

It might take some time, but eventually you should see the security warning. (The security warning appears because the new self-signed certificate that was just installed on the *groov* Box is not trusted by the browser.)

2. Accept the security warning as described below.



For Chrome: Click “Proceed anyway.”



For Firefox:

- Expand “I Understand the Risks.”
- Click Add Exception to open the Add Security Exception dialog box.
- Select “Permanently store this exception.”
- Click Confirm Security Exception.



For Internet Explorer 10: Click “Continue to this website (not recommended).”



For Safari: Click Continue.

3. Select the Current Certificate tab, then click the CSR hyperlink at the bottom of the dialog box.

STEP 3: GET AND USE THE CERTIFICATE

[Help...](#)

SSL Encryption

[Current certificate](#) [Create certificate](#) [Upload certificate](#)

This section shows the details of the current *groov* Admin SSL certificate, and allows it to be downloaded so that it can be accepted by your browser.

Details of current certificate

Authority name	opto-00-d2-dc	Organization	groov on opto-00-d2-dc
Issuer name	opto-00-d2-dc	Issuer organization	groov on opto-00-d2-dc
Valid until	Mar 24 20:27:52 2046 GMT	Certificate type	Self-signed
Download certificate	PEM format PKCS12 format CSR		



```
-----BEGIN CERTIFICATE REQUEST-----
MIIC3jCCACyCAQAwGzgxChZABGNVBAUYTAUVTMQswCQYDVQQIDAJDQTERMA8GA1UE
BwwIVGVtZWlnbGEyITAFBgNVBAoMGE9QVE8mJlIgb24gb3B0by0wMC1kMi1kYzEM
MAoGA1UECwwDRW5nNMRyWFAYDVQDDA0eX0tIUUMTY4JlAuMTA0MSAwHgYJKoZIhvcC
AQKBFHkx2NhcnJAb3B0dCIyLmNvbTCCASIwDQYJKoZIhvcNAQBQAAGGADPADC
CgQCGgEBANpw3jkqPrImtZXfK0c5bj3W1bt9zifLe2cMgr7xg3Q2EKePfIqst32
hvJnsIyCr45C6rMCQvbiV9vxatLHBN39DIts7gO6WrNq9kbYUnkSWvE/fr8toPk
MdZVmxi877A3ZctIEI3YxnFLSxsNcGOD4BFajoyNWlHMND5Onxyfv034czvLM/E
kKbf0/zZAjMcwRBeFuFNXdWosF2cfreFTDByhloQy65b3BRRSxrC21BOAMi
bi+eRIAWInFI8YrgpijYPrdJOpnBVNFhe8GLR6ghl3SPXuPVBoRCvl8UXCqHwQtogJ
YHANwnzsabPTVFqlmzHco0DbdbivHLUCAWEAAaAMA0GCsgSGtb3DQEBCWUA41B
AQDBvZEJPculpm3hmQZekQp3OLIUwF120ctXZK3GNzUaqoRv9r2emV4HW3TrYlw
iYrbe+bsaBDg4DN93SF6BEwr6ryKBCvGUbieS5nLGzsm1+DeAat1kLFVFWQgtBhwg
BY032tiBn/j8E+hXOM5zg8nIHPS8OPQLRkytAbAU7Tmmj8Q7WmymdgdZccT+rpn
FS99Xfepkq/s7YrCs3b2imJ35UMTztimygl3fQ2I56byMbCbZLQ69BaqqwYpvooi
N0HQXUDtQNwXi+pdDnGsxsmb5Unz2kdCF7chVDcRFBBpFGruXA0ER5Ik0ziXMBB
d3Xoxd/V9Xotja7u0Q/vXcdJ
-----END CERTIFICATE REQUEST-----
```

4. Copy and paste the entire text to a file named `<server name>.csr` (where `<server name>` is replaced by the server name value you entered on the Create SSL key form in [step 3](#) on [page 88](#).)

Obtain a CA-Signed Certificate

When filling out a form for a certificate authority, keep in mind that an SSL certificate can be used with any operating system. If you are asked to select an operating system, you can select “other” if that is an option, but it’s OK to select some other operating system.

1. Open the .csr file you created in the previous section.
2. Provide the text of the CSR to the certificate authority in whatever form they require, whether it's a text file or just text pasted into a text field.

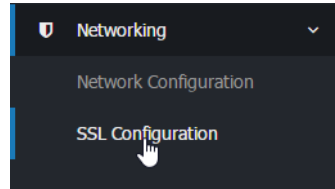
To paste the text into a text field on the CA's website, open your .csr file in a text editor such as Notepad, select all of the text and press Ctrl+ C to copy the text to the clipboard.

```
-----BEGIN CERTIFICATE REQUEST-----
MIICjTCCAXUCAQAwSDElMAkGA1UEBhMCdXMxITAfBgNVBAAoMGE9QVE8gMjIgb24g
b3B0b0y0wMi0yYS1hNjEwMBQGA1UEAwwNb3B0b0y0wMi0yYS1hNjEwMBQGA1UE
hvcNAQEBBQADgQEAPADCCAQoCgGEBAPNEPMIUKONk5YKpt4jwttl83qShIKhPFOIBe
c3D4Ipsa0e1IipJjIXsesY68DmqcXEVFXmZCgxyjFVHKdDOgrQIVhrAtUwn4aLcU
sNI9GbcCoftlDlRxxceYIlDeVxKI6DR2KXnqgMwpc8tzbJksYwPcjCRFWvi7
V5oG405YgsqxBQAVKIBRYtJtUKDU/HGb5WtVYUoieoguLlnhnttpH71k2iz+K
ZgXsa8W017v9/I4nsc9sFTq8Iclg9G9tsf8jX+S46UfVmeu2ExYzb3dvTF6mzc
2mL5Q5Sy6R2T56ksJGMZGvAQo9sFhcggYdJtIbAEPm9NyxDFdg8CAwEAAaAAMA0G
CSqGSIb3DQEBBQUAAIIBAQCgRm0aYmYj6LC7YBLCP5iGnlFm++PH3rZjwrJi2b
rOdgsItbAELMewc+XU/8G5pMojnwqhfVbNBbukova7gi77mYJBvQJLUBQ8u9GQLE
GY7r19gcn9uncw6FzkH0WNkvCC6Ps1lqPUgCBQE9+/aI10MRWNdVVLVZn21HKYMH
+/H/SdPfTbSuzoHvHBJN2G5WPAJwdrnOsVdLTOuPl/TBuOKIDTmqjYoUANTyjqnc
U745b/kU8RQUNsyvk6aFmNP7oWgTou7CGwQ09ZFFcEGATn3+QDXH15tlpYOGljMM
7UD2Y6uE9s5sxx2ME6V2BAP6vk8DcSWDq78NhQewkj/X
-----END CERTIFICATE REQUEST-----
```

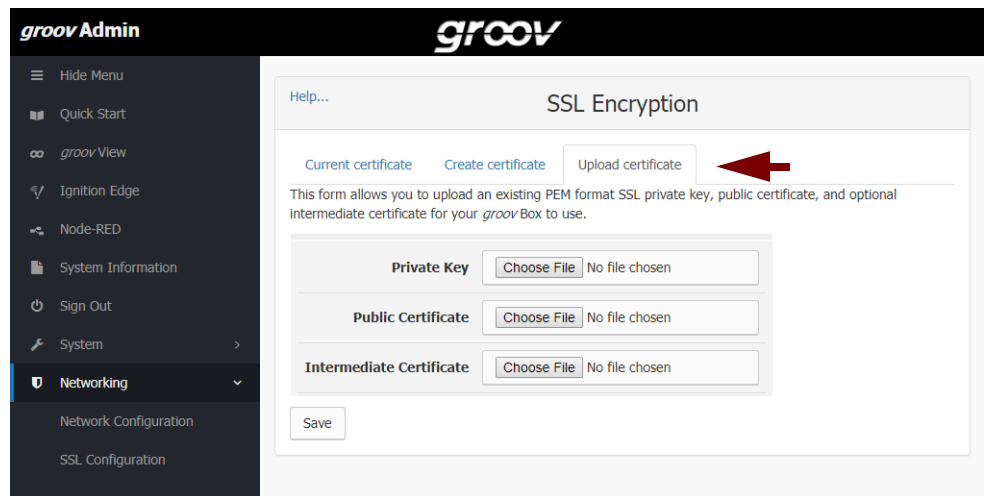
3. Finish the transaction with the certificate authority and receive your new SSL certificate.

Install the CA-Signed Certificate on the *groov* Box

1. In *groov* Admin, select Networking > SSL Configuration.



2. Click the Upload certificate tab on the SSL Encryption page.



3. Under "Private key," click Choose File and specify the `<server name>.key` file that you created and saved in ["Step 2: Create a Private Key" on page 88](#). If you are running *groov* Admin v1.570.50 or later and the certificate you are uploading was created with the private key that is already installed on the *groov* Box, then you can skip this step.

IMPORTANT: Remember to keep the Private Key private. If it is compromised, security is no longer guaranteed.

4. Under "Public Certificate," click Choose File and specify the file you received from the CA.
5. If the SSL certificate you received from the CA included an Intermediate Certificate (chain.cert), under "Intermediate Certificate," click Choose file and specify the file you received from the CA.
6. Click Save to complete the process.

The browser pauses for a few seconds while the certificates are applied to the *groov* Box. When the certificates have been installed successfully, a confirmation message appears.

7. To verify the certificate was installed correctly, use a browser to access the *groov* Box using the hostname specified on the certificate. If the browser does not generate an untrusted site warning, the certificate was installed correctly.

7: Maintenance and Troubleshooting

MAINTENANCE

Turning the *groov* Box On and Off



Turning the Box On

1. Check to make sure that the *groov* Box is plugged in and receiving power.
2. Firmly press the On/Off button only until the SYS LED lights up (in about one second), then release. Take a look at the LNK ACT light for ETH0; if the cable is properly connected, the LNK ACT light should be on or blinking.

CAUTION: If you press the button for longer than eight seconds, the *groov* Box will be reset to default settings. Your project and all passwords will be erased.

NOTE: Always wait until the SYS LED has stopped blinking before you try to log into the *groov* Box. Otherwise, you may not be able to use the hostname to log in. If this happens, see [page 102](#).

Turning the Box Off

With the *groov* Box on, press the On/Off button. The SYS LED will blink blue and then turn off. Always allow the *groov* Box to turn off completely before removing power.

Resetting the *groov* Box to Factory Defaults

Resetting the *groov* Box returns the Box to its default network settings and erases all your data, including your *groov* View, Node-RED, and Ignition Edge projects.

CAUTION: *When the groov Box is reset to factory default settings, your projects and all passwords are erased.*

1. **IMPORTANT:** Back up your *groov* View project (page 32), your Node-RED project (page 57), and your Ignition Edge project (page 81). Also, unactivate your Ignition Edge license following steps on page 80.
2. Turn the *groov* Box off by pressing the On/Off button briefly (the SYS LED blinks blue and then turns off). Make sure the Box is still plugged in and receiving power.
3. Press and hold the On/Off button for at least eight seconds, until the SYS LED is blinking red and green. Then release the button.

The reset defaults operation can last several minutes. When the process is complete, the *groov* Box powers off.

NOTE: Do not remove power from the groov Box or turn it off while the SYS LED is blinking red and green. If you do, you'll need to repeat the reset defaults operation from step 1.

4. Firmly press and release the On/Off button to turn on the *groov* Box.
groov is now in the same state it was in when shipped from the factory.

NOTE: Always wait until the SYS LED has stopped blinking before you try to log into the groov Box. Otherwise, you may not be able to use the hostname to log in. If this happens, see page 102.

5. Wait until the SYS LED has stopped blinking, and then open your web browser and type `https://` plus the *groov* Box's hostname (find it on the bottom of the Box).
Example: `https://opto-01-d2-cd`
6. Accept the security warnings. When *groov* View opens, follow the onscreen instructions to create a *groov* Admin account. **Remember** your username and password! They **cannot be retrieved**.
7. When prompted, install your license.
8. Follow instructions to create a *groov* View account. **Remember** this username and password, too; login information **cannot be recovered** if lost.
9. Click Go to Build mode. When Build opens, choose Help > Check for Updates. Log into manage.groov.com using your My.Opto22 credentials, click Manage, and locate your Box in the list. Click Manage next to its name.
10. From the Box's profile page, download updates for *groov* Admin, *groov* View, and Node-RED (if you use it), and then install them (see "Updating *groov* Admin" on page 34, "Updating *groov* View" on page 30, and "Updating Node-RED" on page 36).
11. Restore your *groov* View project (page 33), your Node-RED project (page 57), and your Ignition Edge project (page 81), and reactivate your Ignition Edge license (page 76).

Applying a *groov* Edge license option

A *groov* Edge license is required for:

- Using the Ignition Edge internal OPC-UA server & drivers in the *groov* Box
- Using MQTT in Ignition Edge

You can purchase the *groov* Edge license, part number [GROOV-LIC-EDGE](#), at the same time you buy the *groov* Box, or you can buy it later. Then follow the steps in "License Ignition Edge" on page 76 to activate and apply it.

Transferring a *groov* Box to someone else

In some situations, you may need to transfer ownership of a *groov* Box to someone else. For example, if you are a system integrator or OEM, you may need to transfer *groov* Boxes to your customers so they can install updates or licenses.

IMPORTANT: *When you transfer the groov Box to someone else, you will no longer be able to see or manage it in your list of groov products on manage.groov.com. Only the new owner will be able to do that.*

To transfer a *groov* Box:

1. Log into manage.groov.com with your MyOpto username and password.
2. Click Manage.
3. In your list of *groov* products, find the Box you want to transfer and click the Manage button next to it.
4. At the bottom of the Box's Profile page, click Transfers.
5. Enter the email address of the person you are transferring the Box to (the transferee) and double-check to make sure it is the correct address. Then click Transfer *groov*.

You receive a confirmation email. If you've made an error, you can cancel the transfer unless the transferee has already accepted it.

The transferee receives an email asking them to accept or decline the transfer at manage.groov.com. If they don't already have a free MyOpto account, they will need to register for an account.

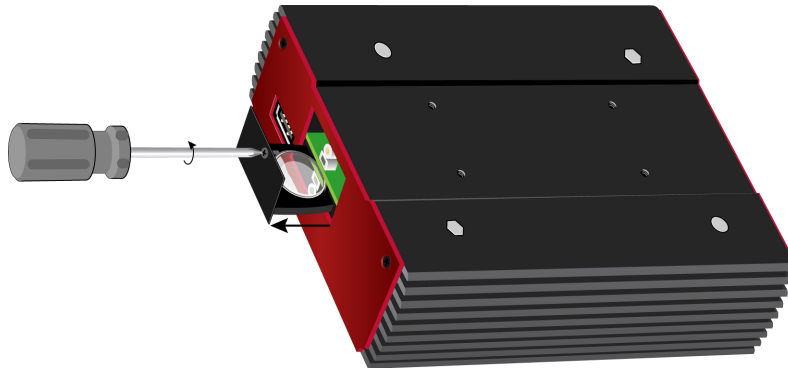
When the transferee accepts the transfer, the *groov* Box disappears from your list and appears in their list.

If you have any problems with the transfer, contact Opto 22 Product Support (see [page 6](#)).

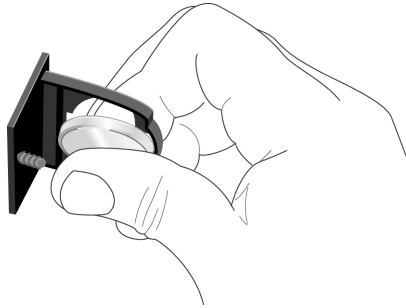
Replacing the battery

If the power LED blinks red and power to the *groov* Box is adequate, replace the battery. The battery maintains the Date and Time. You'll need a BR2032 button cell lithium battery with a nominal voltage of 2.8 volts.

1. On the top of the *groov* Box, unscrew the captive screw, and pull out the battery holder.



2. Using your fingers, pop out the old battery.



3. Put in the new battery, push in the holder, and secure the captive screw.

TROUBLESHOOTING

groov Box is not receiving power

- Make sure you are using either the power supply that came with *groov* Box or else a power supply with the appropriate specifications. See [Appendix A: Specifications and Dimensions](#) on [page 107](#).
- Check that the power supply is securely attached to the *groov* Box and that the power supply is receiving power.

Cannot log into *groov* Box using its hostname

When starting a *groov* Box, always wait until the SYS LED has stopped blinking before you try to access it. Otherwise, you might not be able to log in using the hostname. If this happens, try one of the following methods to log in:

Method 1: Open *groov* Find (see [page 18](#)) and locate the IP address of the *groov* Box you want to log into. Log in using the Box's IP address. After some time passes, you should be able to log in again using the hostname.

Method 2: Open a command prompt and enter `ipconfig /flushdns`. Then log into the Box using the hostname.

groov Box is connected to Ethernet network but doesn't work

- Make sure the *groov* Box has been turned on, and the LNK ACT LED for the connected Ethernet interfaces are lit. (See ["LEDs" on page 111](#).)
- Make sure you've typed the URL accurately and included the "s": `https://` plus the *groov* Box hostname or IP address. Check the label on the bottom of the *groov* Box, where the hostname is printed. URL examples:
 - `https://opto-06-51-f2`
 - `https://192.168.11.2`
- If you cannot connect to the *groov* Box on the network, make sure the Ethernet cable is connected to ETH0, which must be used for initial setup and configuration. After that, either ETH0 or ETH1 may be used.
- Check the [groov View Readme](#) for current supported browsers, and make sure you're using one of them.
- Make sure that the *groov* Box and the computer are connected to the same network. If you still can't reach the Box, your network is set up differently. That's OK. Find out the following information about your network and your computer:
 - Does your network have a DHCP server? See below.

- Does your network have a DNS server? See below.
- Does your computer have more than one network interface card (NIC)? See below.

DHCP (dynamic host configuration protocol) server

A DHCP server automatically assigns IP addresses to devices on the network, which is what the *groov* Box expects. If you have no DHCP, work with your IT Department to choose a static IPv4 address for the *groov* Box. To assign the fixed IP address, you'll need:

- a Windows PC on the same network subnet as the *groov* Box
- *groov* Find utility (download from www.opto22.com)

Assign the static IP address to the Box. See “[Assigning a Static IP Address](#)” on page 24.

Once you've assigned the static IP address, open your web browser and for the URL enter https:// plus the IP address you assigned to the Box. For example: `https://182.154.1.68`

DNS (domain name server)

A DNS (domain name server) keeps track of the unique hostname for each device on the network, so you can find it by name even if its IP address changes. If your network has no DNS, you won't be able to access the *groov* Box using its hostname, but you can access it using its IP address.

To determine the IP address, you'll need:

- a Windows PC on the same network subnet as the *groov* Box
- *groov* Find utility (download from www.opto22.com). See “[Open groov Admin using groov Find \(Windows only\)](#)” on page 18.

Once you've found your *groov* Box in *groov* Find, click the link to set up the Box. Also make a note of the IP address shown, so later you can use it in your web browser instead of the hostname: for the URL enter https:// plus the Box's IP address. For example: `https://192.168.1.220`

Computer with more than one NIC

More than one NIC can cause a problem when you're trying to communicate with the *groov* Box using your browser and the *groov* Box's hostname.

Each NIC communicates on a separate network subnet. You may have one network subnet set up for your computers and a second one set up for your control system, for example (this is a pretty common scenario, and in fact we recommend it for security).

Make sure you're trying to reach the *groov* Box using the NIC for the network subnet it is on. You could unplug the Ethernet cable from your controller network NIC to force the PC to look for the *groov* Box on the computer network. Then try again using your browser and the *groov* Box's hostname.

If your control system and your computers are on separate network subnets, you'll need to set up ETH1 on the *groov* Box in order to reach your control system. See the next question.

Modbus/TCP device, OPC UA server, or Opto 22 SNAP PAC controller can't be found

Are your control system and your computers on separate network subnets? We recommend this setup for security reasons, and the *groov* Box is designed to work this way. Here's what to do so *groov* View can find your OPC UA server, Opto 22 SNAP PAC controller, or Modbus/TCP device:

1. Plug the control network into ETH1 on the *groov* Box. (Remember, your computer network is plugged into ETH0. The two Ethernet network interfaces on the Box are independent, so that keeps the two network subnets separate.)

2. Follow the steps in [“Configuring ETH1 for the Control Network” on page 25](#) to configure the ETH1 connection.
3. Now try configuring your tag server or controller again. This time *groov* View should be able to find it.

Cannot read from/write to Modbus/TCP device OR Modbus data doesn’t make sense

Modbus/TCP devices, though based on a standard protocol, may be set up differently from one another. Some use zero-based addressing and some use one-based addressing. Some devices don’t support all Modbus functions. Modbus/TCP devices also vary in the way they present float data. And device documentation sometimes doesn’t specify how the device is set up.

If you’re having trouble reading or writing to your device, or if the data is clearly wrong, you probably need to change settings for your Modbus device. In *groov* View, choose Configure > Devices and Tags and locate your device in the list. Follow instructions in the [groov View User’s Guide](#) to understand and change settings. You may need to try different combinations of settings to see what works.

“Connection is reset” error in *groov* Admin

If you see this error, it just means that *groov* Admin has timed out. For security reasons, if you have not interacted with *groov* Admin in 10 minutes, you must log in again. Refresh the page and log in.

Power LED is blinking red

If the power LED blinks red, either power to the *groov* Box is outside normal range, or the Box’s battery needs replacing. Check to make sure the power supply to the *groov* Box is adequate (see [“Step 5. Connect the Power Supply” on page 11](#)). If power is OK, replace the battery (see [page 101](#)).



Power outage

If power to the *groov* Box is removed, such as when there is a power outage, when the power is restored the *groov* Box **may** return to the state it was in prior to the power being removed. That is, if it was on, it may power up, and if it was off, it will likely remain off.

However, to avoid potential problems we recommend that you use a UPS (uninterruptible power supply) with the *groov* Box for backup power and surge protection.

Node-RED flow not working

Node-RED is open-source software, and troubleshooting it is beyond the scope of this user's guide. But a good thing to try if your flow used to work, but now doesn't, is to redeploy it.

For example, if you upgrade to a newer version of Node-RED for the *groov* Box, some nodes you're using may have changed or been removed. If they've been removed, you'll need to reinstall them, but changes can also affect the way your flow works.

Make sure there are no unwanted changes, and then try doing a full deploy (a partial deploy may not be enough). If the Deploy button is grayed out, move a block or make some other small change to the flow.

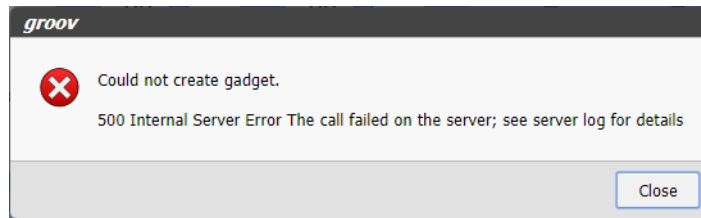
Console Log. The log can also help with troubleshooting. Open Node-RED Admin and choose Diagnostics in the left navigation bar to see the console log.

Additional resources for using Node-RED:

- [Node-RED website](#)
- Opto 22 developer website at developer.opto22.com
- [Opto 22 Node-RED forum](#)

Errors in Build mode when using Ignition Edge

If you're working in Build mode and receive an error while trying to create a gadget for an Ignition Edge tag, the Ignition Edge trial period may have expired. Here's an example of an error like this:



To fix it, open another browser tab, go to `https://[your groov Box's hostname]:8043` and restart the trial. (See [page 75](#) for help.)

No data in *groov* View for gadgets using Ignition Edge tags

If you're in *groov* View and gadgets for Ignition Edge tags show a yellow triangle and no data, click the yellow triangle to see what's wrong.

- Your *groov* View trial period may have expired. Unless your *groov* Box has an Edge license (see [page 100](#)), you are using a free trial for OPC UA, and that trial expires two hours after you first look at your operator interface in *groov* View. To restart the trial, just restart the Box. (See [page 36](#) for steps.)
- Your Ignition Edge trial period may have expired. If so, go to `https://[your groov Box's hostname]:8043` and restart the trial. (See [page 75](#) for help.)

Ignition Edge OPC-UA and MQTT documentation

Instructions for using Ignition Edge, Ignition Edge Designer, and the MQTT Transmission module are beyond the scope of this guide, since these products are owned by other companies. Here are some document links:

- Configure OPC UA tags for Siemens: <https://docs.inductiveautomation.com/display/DOC79/Siemens>
- Configure OPC-UA tags for Modbus: <https://docs.inductiveautomation.com/display/DOC79/Modbus>

- Set up folders and configure tags for MQTT:
<https://docs.chariot.io/display/CLD/Sending+OPC+Tag+Data+with+Transmission>
- Using the MQTT Transmission module: <https://docs.chariot.io/display/CLD/MT%3A+Configuration>

Ignition Edge shows license is temporary and valid for only seven days

If you have updated *groov* Admin or reset your *groov* Box to factory defaults, and you did not deactivate your Ignition Edge license before updating or resetting, you may see a message in Ignition Edge that your license was previously activated and is now temporarily valid for a week.

If you see this message, contact Ignition Edge at the number shown in the message and explain the situation, so they will reinstate the license.

To avoid this problem, always deactivate your Edge license before updating *groov* Admin or resetting the *groov* Box to factory defaults. See “[Unactivate Ignition Edge license](#)” on page 80.

Time zone change not shown in Ignition Edge

You set up your time zone in *groov* Admin (see [page 41](#)). If you are running Ignition Edge and change the time zone, Ignition Edge does not automatically update it. To update it, restart the Ignition Edge Gateway.

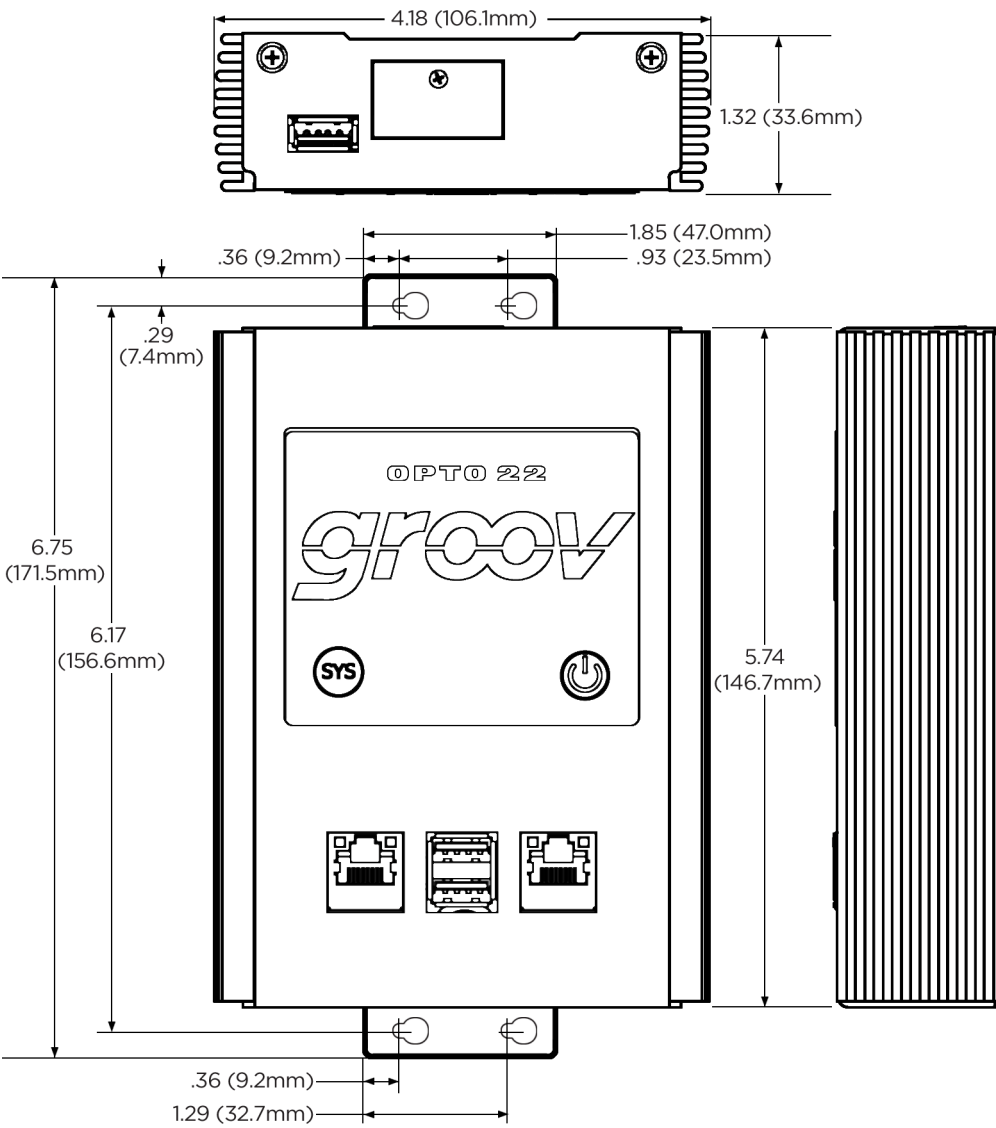
A: Specifications and Dimensions

SPECIFICATIONS

Ethernet Communication (wired)	Two independent 10/100/1000 Mbps RJ-45 connectors, each with a separate IP address (separate subnets). Supports Auto MDI-X (crossover cable not needed).
Ethernet Comm (wireless)	802.11 b/g/n (optional; requires purchase of a third-party commercial USB WiFi adapter that has been tested and approved by Opto 22)
Security (wireless)	WEP64 WEP128 WPA PSK (also called WPA Personal) WPA2 PSK (also called WPA2 Personal)
Backup battery	BR2032 button cell lithium battery with a nominal voltage of 2.8 volts. Lasts 8 years at 25 °C. This battery maintains the date and time.
Power Consumption	8-36 VDC, 24 VDC @ 500mA (Power supply included; input 100-240 VAC. Use international adapter if needed.)
Housing	Compact and sturdy metal. Fanless operation.
USB	USB 2.0 (three: used for backing up, restoring, WiFi, and connecting to serial devices via a USB-to-serial converter with an FTDI chipset)
Indicators	Ethernet interfaces (2): Link/Activity and Speed System: SYS & PWR
Operating Temperature	0 to 70 °C (32 to 158° F)
Storage Temperature	-20 to +80 °C (-4 to 176° F)
Operating Humidity	10% to 90% relative humidity, non-condensing
Storage Humidity	5% to 95% relative humidity, non-condensing
Agency Approvals	CE, RoHS, DFARS
Warranty	30 months

DIMENSIONS

DIMENSIONS



B: Connectors, Ports, and LEDs

CONNECTORS



USB connectors. Can be used for:

- Backing up and restoring. See [“Backing Up groov View and Network Settings” on page 32](#) and [“Restoring groov View and Network Settings” on page 33](#).
- Connecting to serial devices using an FTDI USB-to-serial converter and Node-RED. See [“USB connectors for serial devices” on page 110](#) and [“Connecting with serial devices” on page 51](#).

Independent 10/100/1000 Mbps Ethernet interfaces (RJ-45 connectors)



Top

USB connector, used for:

- WiFi adapter. See [Appendix C: Installing an Approved USB WiFi Adapter on page 113](#) and [“Configuring Wireless Communications” on page 26](#).
- Serial device. See [“USB connectors for serial devices” on page 110](#) and [“Connecting with serial devices” on page 51](#).

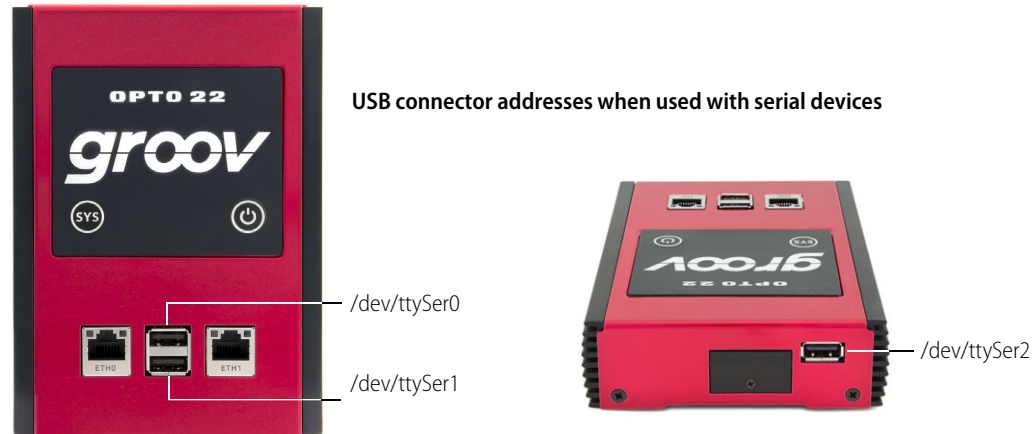


Bottom

Power connector

USB connectors for serial devices

When used for connecting to serial devices with a USB-to-serial converter with FTDI chipset, each USB connector on the *groov* Box shows a specific address in Node-RED. **The address is for the connector, not for the serial device.** If you unplug a device from one connector and plug it into a different one, you will need to change the device's address in the node. Connector addresses are shown below.

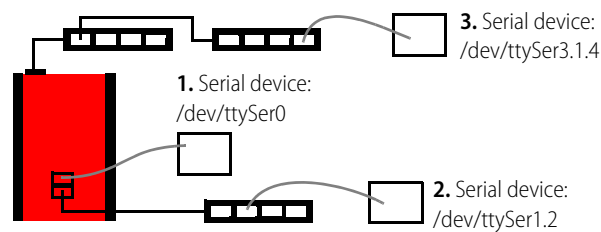


If you're using a USB hub, the address looks like this:

`ttySer<connector>.[<tier 1 port number>].[<tier 2 port number>]`

- `<connector>` indicates the 0, 1, or 2 connector on the *groov* Box, as shown above.
- `[<tier 1 port number>]` for a USB hub connected to the AR1, indicates the USB hub port number where the converter is plugged in.
- `[<tier 2 port number>]` is for a second USB hub connected to the first hub. You can add additional tiers if needed, using the same pattern.

Examples:



NOTE: Use powered hubs.

1. USB-to-serial converter is attached to the top USB connector on the front of the groov-AR1: `/dev/ttySer0`
2. Converter is attached to port 2 of a USB hub attached to the bottom connector on the front of the groov-AR1: `/dev/ttySer1.2`
3. Converter is attached to port 4 of a USB hub attached to port 1 of a USB hub attached to the USB connector on the top of the groov-AR1: `/dev/ttySer3.1.4`

Remember that the address indicates the connectors, not the serial device. If you move a device, be sure you change the device's address in the node.

PORTS

The following ports are used for communication in the *groov* Box:

Port	How used	Example/Notes
443 or 8443	Basic communication with <i>groov</i> View	Default is 443.
10000	Open <i>groov</i> Admin	https://[groov Box hostname]:10000
1880	Open Node-RED Editor	https://[groov Box hostname]:1880
3000	Open Node-RED Admin	https://[groov Box hostname]:3000
4096	<i>groov</i> View communication with Edge (inside the Box)	127.0.0.1:4096
8043	Open Ignition Edge Gateway	https://[groov Box hostname]:8043
8088	Download Ignition Edge Designer project file	CAUTION: This is an insecure port. If you need to open it temporarily for configuring tags, close it as soon as possible. While it is open we strongly recommend that you connect the <i>groov</i> Box only to a trusted network that blocks external connection requests to TCP port 8088. Also, configure Ignition Edge to use SSL for the user interface. See page 82 .

LEDS

The *groov* Box's LEDs use color and blinking to show status information.



LED	What it shows	Color	What it means
SYS	<i>groov</i> Box status	Off	<i>groov</i> Box is turned off
		Green	<i>groov</i> Box is turned on
		Blinking green	<i>groov</i> Box is booting up
		Blinking blue	<i>groov</i> Box is shutting down
		Blinking red and green	Default settings are being restored
		Blinking red	Restoration to default settings failed

LED	What it shows	Color	What it means
On/Off	Power to Box	Green	<i>groov</i> Box is turned on
		Blinking red	Input power is outside normal range or battery is low (see “Power LED is blinking red” on page 104)
SPEED	Ethernet link speed	Off	10 Mbps
		Green	100 Mbps
		Orange	1000 Mbps
LINK ACT	Ethernet network activity	Off	No Ethernet link
		Green	There is an Ethernet link, but no activity
		Blinking green	There is a link and activity

C: Installing an Approved USB WiFi Adapter

If you want to use the *groov* Box on a wireless network, you must purchase and install one of the following USB WiFi adapters that Opto 22 has tested and approved for use with GROOV-AR1. Unapproved WiFi adapters should not be used.

- Netis WF2119S
- Netis WF2116
- Rosewill RNX-N150UBE
- Patriot Memory PCUSBW1150

Install the WiFi adapter and restart the *groov* Box as follows:

1. If the *groov* Box is on, press the On/Off button firmly but briefly to turn it off.

CAUTION: *If you press the button for longer than eight seconds, the *groov* Box will be restored to default settings. Your project and all passwords will be erased.*

2. Insert the WiFi adapter into the USB connector on the top of the device.



3. Firmly press the On/Off button. The Power LED will turn on. Wait until the SYS LED has stopped blinking and is solid green.
4. Open *groov* Admin as described on [page 17](#).
5. Configure wireless communications as described on [page 26](#).

Index

A

- access point, wireless, 26
- activate
 - groov Box, 12
 - Ignition Edge license, 76
- architecture, system, 4

B

- backing up
 - groov View project, 32
 - Ignition Edge project, 81
 - Node-RED project, 57
- battery, replacing, 101
- browsers, 3, 7, 13, 20

C

- CCMP, 27
- certificate
 - CA-signed, 95
 - for Node-RED, 57
 - self-signed, 90
- changing
 - groov Admin password or username, 37
 - Ignition Edge password or username, 80
 - network configuration, 23
 - owner of groov Box, 101
- Chrome, 20
- Client Options dialog, 25
- communications, 4
- configuring
 - Ignition Edge, 61
 - OPC and MQTT tags, 70
- connecting to groov Box, 10
- connecting to groov Box and groov View
 - troubleshooting, 102
- connecting to network, 10

- connection is reset error, 104
- connectors on the groov Box, 109
- control network, 4
- controller not found, 103
- credentials
 - uploading, downloading, 57

D

- data, Modbus, troubleshooting, 104
- deactivate Ignition Edge license, 80
- debugging Node-RED project, 56
- default network settings, 100
- Designer, 82
- device not found, 103
- DHCP, 23, 100, 103
- DIN rail clip, 9
- DNS, 13, 23, 25, 103
- downloading Node-RED project, 57

E

- Edge, *see* Ignition Edge, 59
- encryption, 27
- enterprise network, 4
- environmental requirements, 107
- EPIC processors, 2
- error, connection is reset, 104
- Ethernet connectors, 4, 10, 100
- Ethernet interfaces, 109
- exporting
 - flow in Node-RED, 54
 - node, 54

F

- Find, 14
- Firefox, 20

- flow
 - exporting, 54
 - importing, 55
 - library, 55
 - uploading, downloading, 57
- function node, 46

G

- groov Admin
 - logging in, 104
 - quick start, 21
 - updating, 21
- groov Box
 - connecting to serial devices, 51
 - connectors, 109
 - LEDs, 111
 - power outage, 104
 - reset to factory defaults, 100
 - turn on/off, 99
- groov EPIC, 2
- groov EPIC driver for Ignition Edge, 60
- groov EPIC nodes, 43
 - using in Node-RED, 48
- groov Find, 14, 18
- groov RIO units, 2
- groov View
 - backing up, 32
 - opening from groov Admin, 21
 - restoring project from backup, 33
- groov View nodes, 43

H

- hardware status, 40
- help
 - Opto 22 Product Support, 6
 - Product Support, 6
- hostname
 - changing, 25
 - troubleshooting, 102, 103

I

- Ignition Edge
 - back up project, 81
 - changing password, 80
 - Designer, 70, 82
 - documentation links, 105
 - drivers included, 60
 - getting started, 60
 - groov EPIC driver, 60
 - install modules, 85

- licensing, 76, 84, 106
- modules installed, 84
- no data in groov View, 105
- opening, 22, 61
- overview, 59
- Panel, 82
- reset trial period, 75
- restore project, 81
- SNAP PAC driver, 60
- time zone change, 106
- troubleshooting, 105
- unactivate license, 80
- Vision, 82

- importing flow in Node-RED, 55
- installing
 - groov Box, 9
 - Ignition Edge modules, 85
 - Node-RED nodes, 53
- Internet Explorer, 20
- IP address
 - DHCP server, 103
 - DNS, 103
 - static, 24
- IPv4 Gateway, 25

L

- LEDs
 - blink codes, 111
 - location, 111
- library in Node-RED, 55
- license file
 - for groov View, 12
 - for Ignition Edge, 76
- licensing
 - Ignition Edge, 84, 106

M

- memory, 107
- Message Queue Telemetry Transport, 73
- Modbus troubleshooting, 104
- mounting groov Box, 9
- MQTT, 73
 - broker, 74
 - documentation links, 105
 - tags, 74

N

- network
 - configuring, 23
 - connecting, 10

- control, 4
- enterprise, 4
- interface card (NIC), 103
- key, 27
- LEDs, 111
- troubleshooting, 102
- node
 - exporting, 54
 - importing, 55
 - library, 55
- Node-RED, 43
 - backing up, 57
 - debugging, 56
 - editor, 44
 - exporting a flow, 54
 - flow not working, 105
 - function node, 46
 - groov View nodes, 43
 - importing a flow, 55
 - installing nodes, 53
 - opening, 22, 44
 - Opto 22 controller nodes, 43, 48
 - restoring, 57
 - security certificates, 57
 - serial devices, 51, 110
 - updating, 36
- Node-RED Admin
 - opening from groov Admin, 22

O

- On/Off button, 99
- OPC UA server
 - adding to groov View, 67
 - configuring tags manually, 70
 - Ignition Edge, 59
 - tag browsing, 70
- opening
 - groov View from groov Admin, 21
 - Ignition Edge, 22, 61
 - Node-RED, 44
- operating temperature, 107
- Opto 22 Product Support, contacting, 6

P

- PAC Control nodes, 43
 - security certificates, 57
 - using in Node-RED, 48
- Panel, 82
- password
 - changing, for groov Admin, 37
 - changing, for Ignition Edge, 80

- power
 - connector, 109
 - outage, 104
 - red LED, 104
 - requirements, 11, 107
 - troubleshooting, 102
- private key, 97
- processor, 107
- project, groov View
 - backing up, 32
 - restoring from backup, 33
- project, Node-RED
 - backing up, 57
 - restoring, 57

Q

- quick start
 - groov Admin, 21
 - Ignition Edge, 60
 - Node-RED, 44

R

- replacing battery, 101
- resetting
 - groov Box, 100
 - Ignition Edge trial, 75
- restarting groov Box, 36
- restoring
 - groov View project, 33
 - Ignition Edge project, 81
 - Node-RED project, 57
 - to older groov View version, 32
- RIO units, 2

S

- Safari, 20
- security
 - CA-signed certificate, 96
 - certificate, 57, 95
 - self-signed certificate, 90
 - warning, 14, 20
- self-signed certificate, 90
- serial devices
 - addresses for node, 110
 - connecting to groov Box, 51
- server, synchronize time with, 42
- session timer, 21
- setting system time, 41
- SNAP PAC driver for Ignition Edge, 60
- SoftAP, 29

- Sparkplug, 73
- specifications, 107
- SSID, 27
- SSL certificate, 95
 - buying CA-signed, 96
 - using in Node-RED, 57
- static IP address, 14
 - assigning, 24
- storage temperature, 107
- synchronize time with remote server, 42
- SYS LED, 111
- system
 - architecture, 4
 - information, 21, 39, 44
 - time, setting, 41

T

- Technical Support. *See* Opto 22 Product Support, 6
- temperature and humidity, 107
- time
 - server, 41
 - setting, 41
 - zones, 41
 - zones and Ignition Edge, 106
- TKIP, 27
- transferring a groov Box, 101
- troubleshooting
 - cannot connect to groov Box or groov View, 102
 - device or controller not found, 103
 - DNS (domain name server), 103
 - hostname, 102
 - Ignition Edge, 105
 - Modbus device or data, 104

- Opto 22 Product Support, 6
- power, 102
- red power LED, 104

U

- updating
 - groov Admin, 34
 - Node-RED, 36
- uploading Node-RED project, 57
- USB connectors, 109
 - serial device addresses, 110
- USB flash drive
 - back up to, 32
 - restore from, 33
- User Account Control, 14, 18
- username, changing, for groov Admin, 37

V

- version, restoring to older groov View version, 32
- Vision, 82

W

- WEP, 27
- wired network, 4
- wireless
 - access point, 26
 - communications, 26
 - LAN, 4
 - specifications, 107
- WPA, 27