

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

GROOV BOX USER'S GUIDE

for GROOV-AR1

Form 2104-170424—April 2017

OPTO 22
Automation made simple.

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 2104-170424—April 2017

Copyright © 2015–2017 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, 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*, 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.

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
Automation Made Simple.



Table of Contents

Chapter 1: Welcome	1
Choose Your groov	2
About this Guide	3
System Requirements	3
A Note on Browsers	4
groov Box Communications	4
System Architecture	5
What's In This Guide	7
Product Support	7
Chapter 2: Getting Started	9
What You Will Need	9
In the Box	9
Step 1. Get To Know the groov Box	10
Step 2. Choose a Location	11
Step 3. Mount the groov Box	11
Step 4. Connect to the Network	13
Step 5. Connect the Power Supply	13
Step 6. Turn on the groov Box	14
Step 7. Activate the groov Box and Get the License File	15
Step 8. Open groov	16
Step 9. Create a groov Admin Account	19
Step 10. Install the License File	19
Step 11. Create a groov Build Account	19
Chapter 3: Using groov Admin	21
Opening <i>groov</i> Admin	21
Open <i>groov</i> Admin from <i>groov</i> Build	21
Open <i>groov</i> Admin using the URL	22
Open <i>groov</i> Admin using <i>groov</i> Find (Windows only)	22

Accepting the Security Warning	24
For Chrome	24
For Firefox	24
For Safari	24
For Internet Explorer	24
Logging in	24
Quick Start menu	25
Opening <i>groov</i> View and Build from <i>groov</i> Admin	26
Opening Node-RED Admin from <i>groov</i> Admin	26
Configuring Network Connections	26
Assigning a Static IP Address	27
Changing the Hostname, DNS Servers, or IPv4 Gateway	28
Configuring ETH1 for the Control Network	29
Configuring Wireless Communications	30
Using an AR1 as a Wireless Access Point	33
Updating <i>groov</i> App (Build and View)	34
Backing Up <i>groov</i>	36
Restoring <i>groov</i>	37
Updating <i>groov</i> Admin	39
Updating Node-RED	40
Restarting the <i>groov</i> Box	41
Changing Username and Password	42
Checking System Information	43
Checking Hardware Status	44
Setting the System Time	45

Chapter 4: Using Node-RED47

What is Node-RED?	47
Node-RED in the <i>groov</i> Box	48
Getting Started	48
Requirements	48
Open Node-RED	48
Create a flow	49
Deploy the flow and test	50
Add a Function node	50
Install <i>groov</i> nodes	51
Add a SNAP PAC node	52
Connecting with serial devices	55
Requirements	56
Setting up the serial device	56
Working with nodes	57
Managing nodes	57
Installing nodes	57
Working with flows	58
Exporting a flow	58

Importing a flow	59
Import from the Library	59
Import from a file	59
Debugging your Node-RED project	60
In the Editor	60
In Node-RED Admin	60
Managing security certificates	61
Backing up and restoring your Node-RED project	61
Starting a new Node-RED Project	62
Chapter 5: Using an SSL Certificate	65
Understanding Certificates	65
Certificate Structure	66
Step 1: Back up your <i>groov</i> Project	66
Step 2: Create a Private Key	66
Step 3: Get and Use the Certificate	68
Using a Self-Signed Certificate	68
Finish the Self-Signed Certificate	69
Add the Self-Signed Certificate to a Browser Trust Store on a Computer	70
Install an SSL Certificate on Mobile Devices	73
Using a CA-Signed Certificate on <i>groov</i> Box	74
Finish the CSR	74
Obtain a CA-Signed Certificate	75
Install the CA-Signed Certificate on <i>groov</i> Box	76
Chapter 6: Maintenance and Troubleshooting	79
Maintenance	79
Turning the <i>groov</i> Box On and Off	79
Resetting the <i>groov</i> Box to Factory Defaults	80
Replacing the battery	80
Troubleshooting	81
<i>groov</i> Box is not receiving power	81
Cannot log into <i>groov</i> Box using its hostname	81
<i>groov</i> Box is connected to Ethernet network but doesn't work	82
DHCP (dynamic host configuration protocol) server	82
DNS (domain name server)	82
Computer with more than one NIC	83
Modbus/TCP device, OPC UA server, or Opto 22 SNAP PAC controller can't be found	83
Cannot read from/write to Modbus/TCP device OR Modbus data doesn't make sense	83
"Connection is reset" error in <i>groov</i> Admin	83
Power LED is blinking red	84
Power outage	84
Node-RED flow not working	84
Appendix A: Specifications and Dimensions	85
Specifications	85

Dimensions	86
Appendix B: Connectors and LEDs	87
Connectors and Indicators	87
USB connectors for serial devices	88
LEDs.....	89
Appendix C: Installing an Approved USB WiFi Adapter	91
Index	93

1: Welcome

groov is Opto 22's web-based Internet of Things (IoT) and operator interface system that is *simple, mobile, and connects easily* to automation systems, software, databases, and devices of all kinds.

Simple: *groov* requires only a web browser to connect to devices and build mobile interfaces so you can monitor and control them. *groov* puts ready-made gadgets at your fingertips and requires no programming. Using tags from the built-in Data Simulator, you can test project ideas without connecting to a live machine or system. *groov* makes it simple to build, deploy, and view effective, scalable operator interfaces.



Mobile: Get the free *groov* View app for Android or iOS to view your *groov* interface on your iPhone, iPad, or Android phone or tablet. Or use any brand device, from a smartphone to a web-enabled big-screen TV, and view your *groov* interface using a web browser. *groov* can augment existing human-machine interfaces (HMIs) and SCADA systems by making specific data available to authorized users at any time and in any location. Using event notification, selected personnel can be alerted anywhere about system events based on one or more conditions.

Connects easily: You can connect *groov* to several data sources for monitoring and control in your mobile interface:

- Connect directly to Modbus/TCP devices and Opto 22 SNAP PAC controllers to access their data.
- Connect to PLCs and PACs from other manufacturers, such as Allen-Bradley ControlLogix and CompactLogix, Siemens SIMATIC S7, Schneider Electric Modicon, and GE PACSystems—and to any database or system supported by your server—through an OPC UA (Unified Architecture) server.

- Use your database, a cloud service, or an API (application program interface) to place data in or read data from a *groov* Data Store, where you can access it for use in your mobile interface.
- (GROOV-AR1 *groov* Box only) Use Node-RED (included) to create logical flows for data you use in *groov*. Also connect to serial devices—Modbus RTU/ASCII, weigh scales, and more—via a USB-to-serial converter and Node-RED.

groov brings key data from process control, OEM machines, manufacturing and building systems, and the Internet of Things (IoT) into the hands of those who need it.

Choose Your *groov*

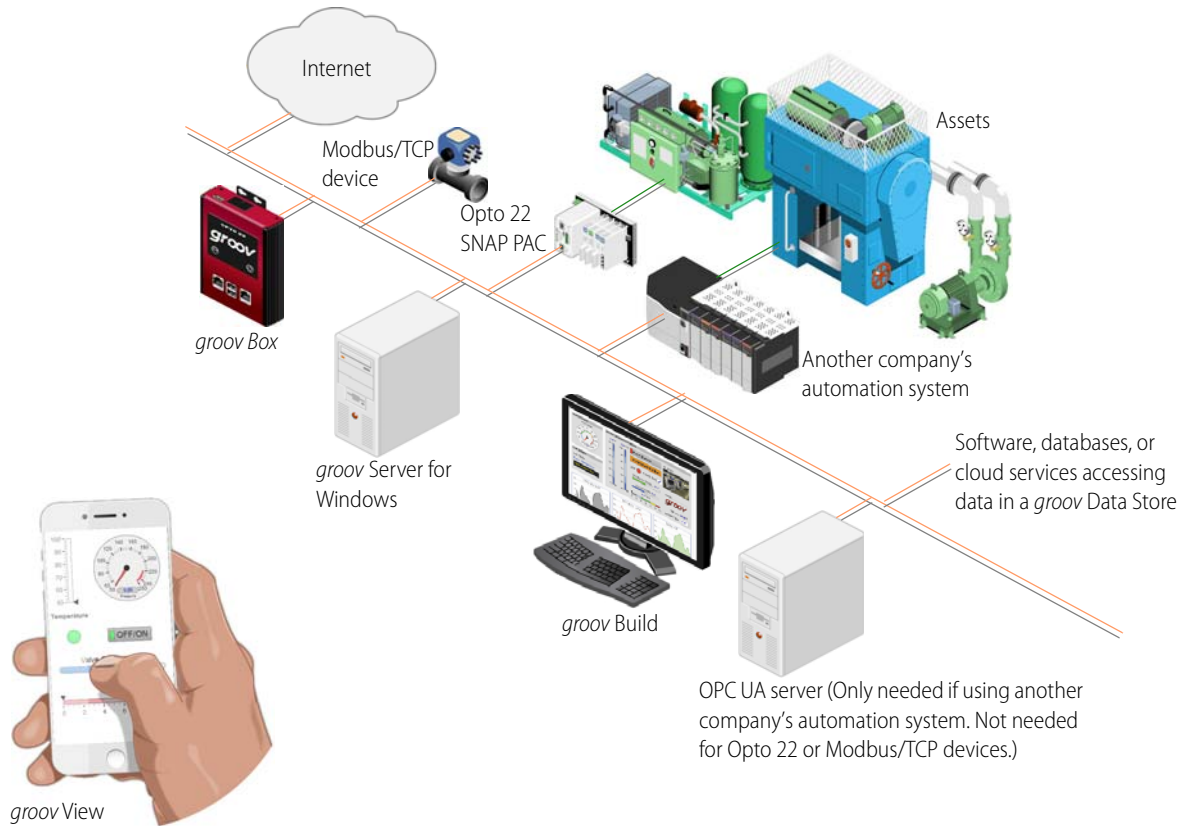
groov is available as either the standalone *groov* Box hardware appliance or the PC-based *groov* Server for Windows software.

***groov* Box** (p/n [GROOV-AR1-BASE](#)) is an industrially hardened appliance that comes preloaded with *groov* software, including *groov* Build for building operator interfaces, *groov* View for using the interfaces you've built, and *groov* Admin for administering the Box itself. It also includes Node-RED, an open-source, multi-platform software tool for wiring together databases, cloud applications, and APIs to produce Internet of Things (IoT) applications quickly and inexpensively. Through Node-RED the *groov* Box can also use a USB-to-serial converter with FTDI chipset to connect to serial devices like weigh scales, Modbus RTU/ASCII devices, and more. The *groov* Box can communicate over a standard Ethernet network or wireless LAN (optional; requires third-party WiFi adapter), or both. See [Appendix C: Installing an Approved USB WiFi Adapter](#).



***groov* Server for Windows** (p/n [GROOV-SVR-WIN-BASE](#)) includes *groov* software (*groov* Build for building operator interfaces and *groov* View for using them) and is ready for installation on a Microsoft® Windows® PC. Once installed, *groov* Server runs as a service on your computer.

Whether you serve *groov* software from a *groov* Box or a computer using *groov* Server for Windows, your *groov* operator interface can be viewed on almost any mobile device or computer. And you can develop on one *groov* and later move your project to another: for example, develop on *groov* Server and then move the project to a *groov* Box.



About this Guide

This user's guide shows you how to install and set up your *groov* Box, 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*, 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 information about building and viewing *groov* interfaces, see [form 2027](#), the *groov User's Guide*.

Additional resources for *groov* are available on groov.com.

System Requirements

For *groov* Box

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

- Any computer with a web browser (does not have to be a Windows PC)
- One or more of the following:
 - 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* API

- An Opto 22 SNAP PAC controller (SNAP PAC S-series, R-series, or SoftPAC, with firmware R9.2a or newer), running a PAC Control strategy
- Any OPC UA-compatible automation system or equipment, plus an OPC UA server and drivers for your equipment
- A database, cloud application, API, or serial device accessible via a Node-RED node (*groov* Box only. Serial device requires a USB-to-serial converter with FTDI chipset, *groov* Admin R1.570.46 or higher, and Node-RED for *groov* Box version 3 or higher)

A Note on Browsers

Thanks to technologies such as HTML5, SVG, and CSS3, modern browsers are now fairly similar. Our browser-based *groov* View and *groov* Build work on a large number of device/operating system/browser combinations, including HDTVs, smartphones and tablets of many shapes and sizes, and computers. We've found Firefox, Chrome, Safari, and Internet Explorer 10 or newer to be generally reliable. If one browser is causing problems for you, however, try another one and let us know what issues you've seen. For Product Support, see [page 7](#).

groov Box Communications

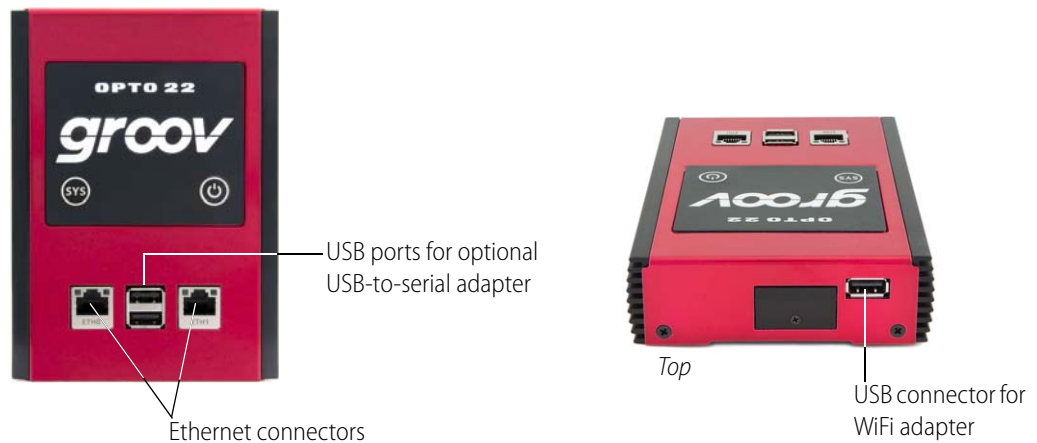
groov uses standard computer networks and protocols. The unit communicates with computer networks over a standard 10/100/1000 Mbps Ethernet network. For use on a wireless network, you must purchase and install a USB WiFi adapter that has been tested and approved by Opto 22. For more information, see [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* 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 33](#).

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* 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 55 for more information.

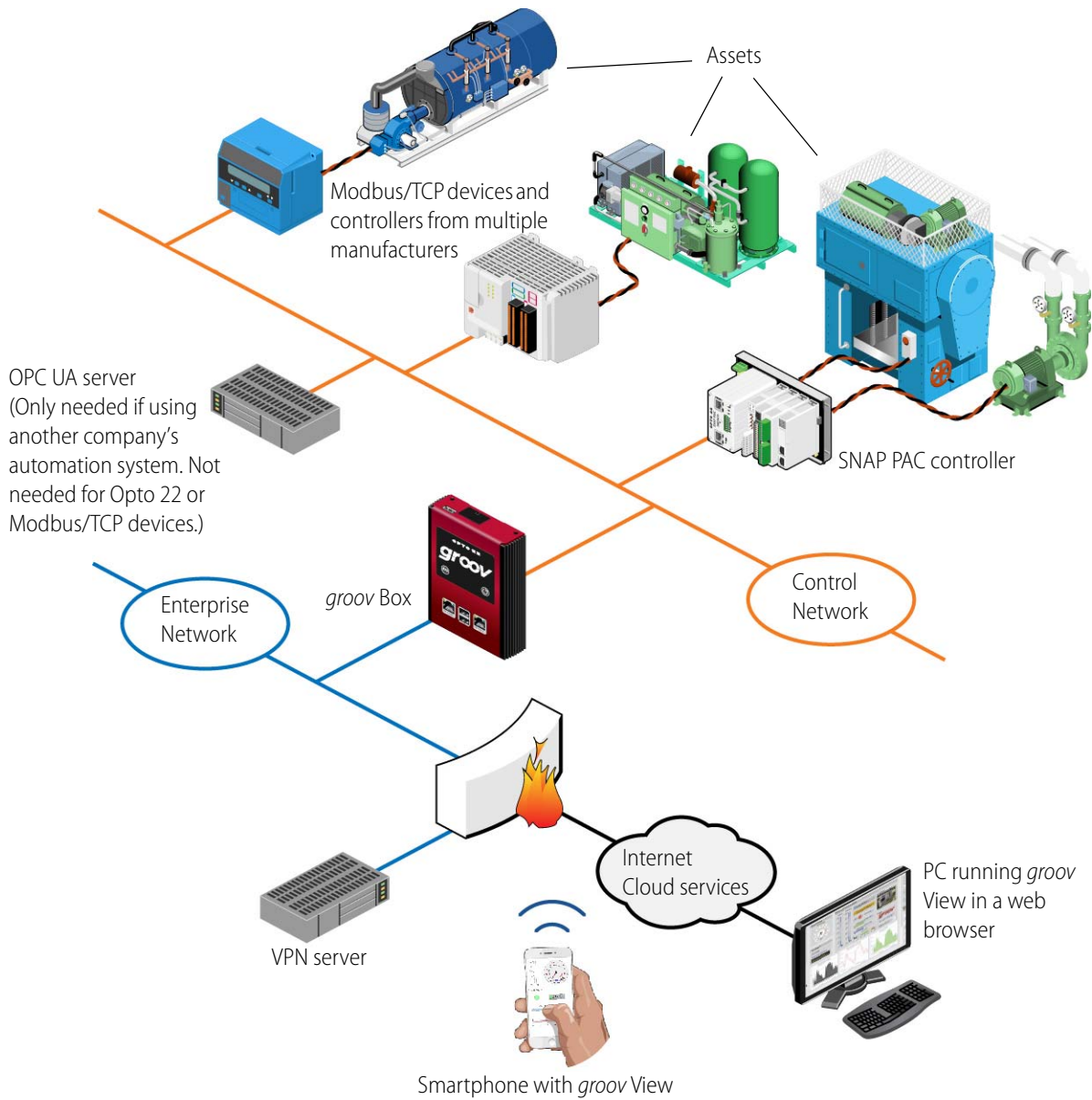


System Architecture

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

The following illustration shows *groov* connected to control systems from other manufacturers as well as a SNAP PAC controller. When accessing *groov* outside *groov*'s network on 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 *groov* is encrypted.



What's In This Guide

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

Chapter 2: Getting Started describes how to get *groov* 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 an SSL Certificate describes using an SSL certificate that is digitally signed either by a certificate authority (CA) or self-signed.

Chapter 6: Maintenance and Troubleshooting provides troubleshooting information and answers questions you might have about *groov*.

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

Appendix B: Connectors and LEDs describes connector and LED functions.

Appendix 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 *groov*, 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	<i>NOTE: Email messages and phone calls to Opto 22 Product Support are grouped together and answered in the order received.</i>
Fax:	951-695-3017	
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 43](#)).
- 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	9
In the Box	9
Step 1. Get To Know the <i>groov</i> Box	10
Step 2. Choose a Location	11
Step 3. Mount the <i>groov</i> Box	11
Step 4. Connect to the Network	13
Step 5. Connect the Power Supply	13
Step 6. Turn on the <i>groov</i> Box	14
Step 7. Activate the <i>groov</i> Box and Get the License File.....	15
Step 8. Open <i>groov</i>	16
Step 9. Create a <i>groov</i> Admin Account.....	19
Step 10. Install the License File.....	19
Step 11. Create a <i>groov</i> Build Account.....	19

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. We recommend Chrome, Firefox, or Internet Explorer 10 or newer as your web browser.

In the Box

These items are included in the box:

- *groov Quick Start for GROOV-AR1*, form 2103
- *groov* Box (GROOV-AR1)
- *groov* CD that includes the *groov User's Guide* (form 2027), the *groov Quick Start for GROOV-AR1* (form 2103), *groov Box User's Guide for GROOV-AR1* (form 2104), and the *groov* Find utility

STEP 1. GET TO KNOW THE GROOV BOX

- 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



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 *groov* Box components shown below. Make sure to put the activation key certificate label 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 85](#) 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 company computer network from your control network, 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.

For mounting on a flat surface:

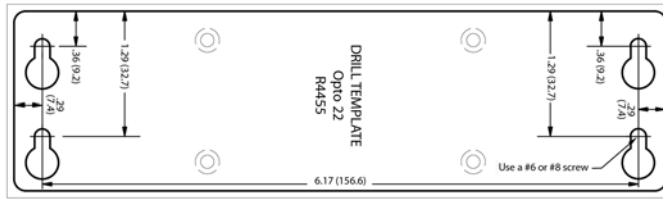
- a. Using the screws provided, install the surface mounting bracket on the back of the *groov* Box.



Surface mounting bracket

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

STEP 3. MOUNT THE GROOV BOX



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

For mounting on a DIN rail:

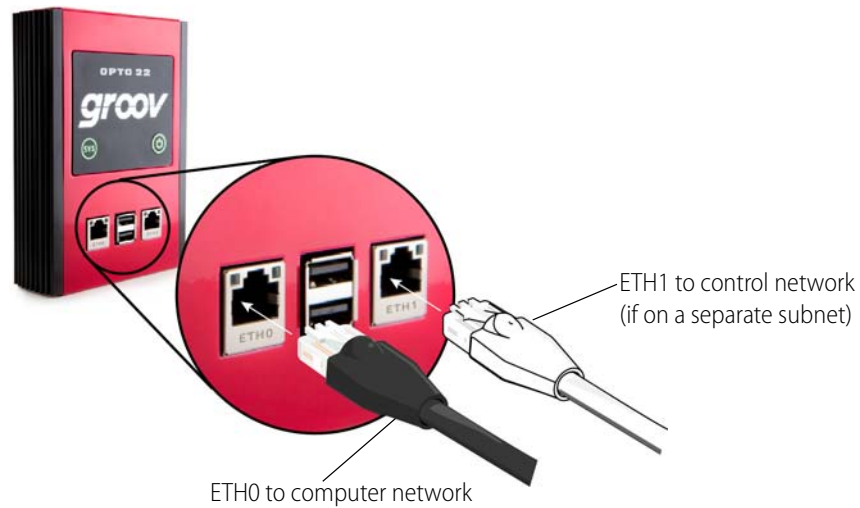
- a. Using the screws provided, install the DIN rail clip on the back of the *groov* Box.



DIN rail clip

- b. Attach the *groov* Box to the DIN rail.

Step 4. Connect to the Network



- a. 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.

- b. 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 enterprise LAN. If your Opto 22 controller, OPC UA server, or Modbus/TCP device is on a different network than 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 27](#).

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:

- a. 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.*

- b. Connect the COM wire from the power supply (normally black) to the – (negative) terminal on the power connector.
- c. 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 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.

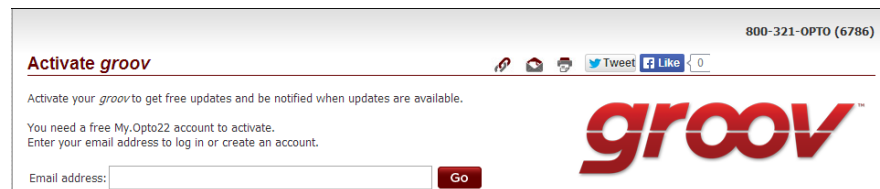


NOTE: Always wait until the SYS LED has stopped blinking before you try to log into groov. Otherwise, you may not be able to use the hostname to log in. If this happens, see page [page 81](#).

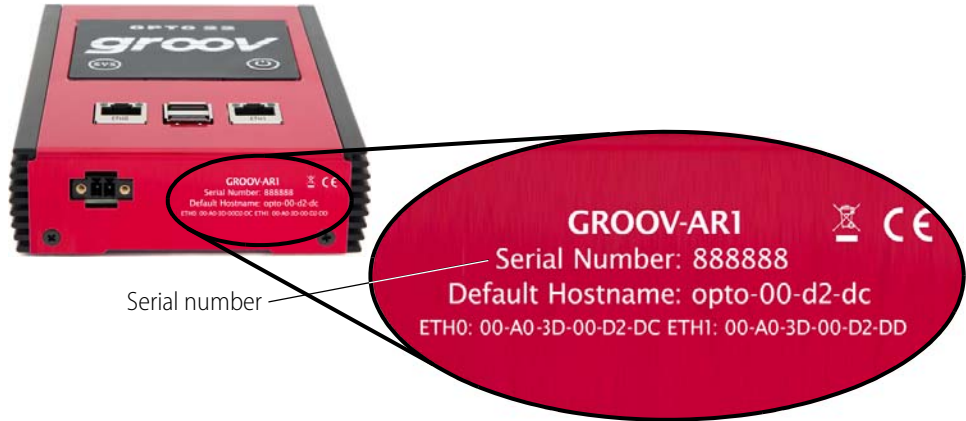
CAUTION: *If you press the button for longer than eight seconds, the groov Box will be reset to default settings. Your project and all passwords will be erased.*

Step 7. Activate the groov Box and Get the License File

- a. Open a web browser. Go to activate.groov.com.



- b. Log in 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.
- c. Follow the on-screen instructions to activate your groov Box and download the license file.
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.



- d. After activating the *groov* Box and downloading the license file, return to this guide and continue with step 8.

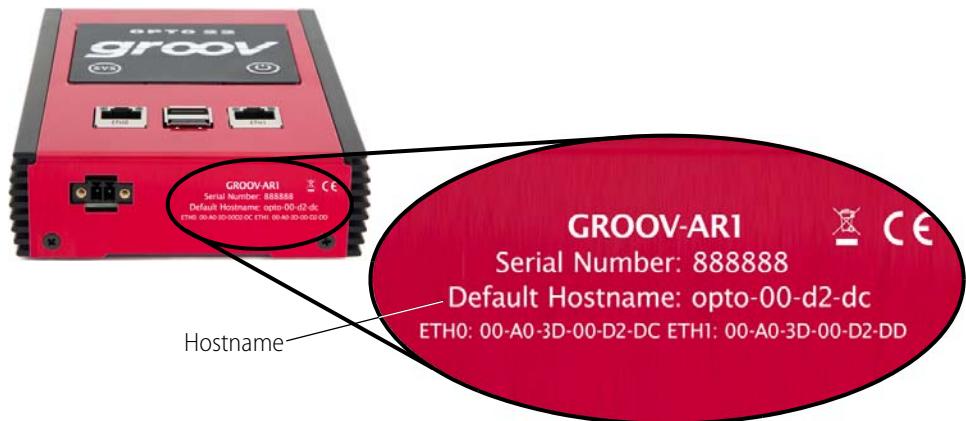
Step 8. Open *groov*

In most cases you'll open *groov* using your web browser. If your network does not have DNS, use *groov* Find from a Windows computer (see [page 17](#)).

Opening *groov* using your web browser:

- a. Make sure the SYS LED on the *groov* Box has stopped blinking.
- b. On your computer, open Firefox, Chrome, or Internet Explorer 10.
- c. 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.

*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*.*

- d. 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 19.

Opening groov 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.

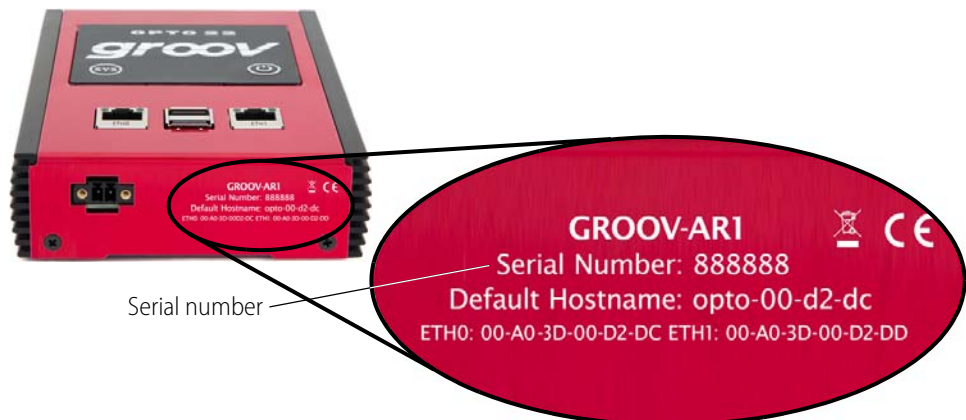
- a. Insert the *groov* CD in your CD-ROM drive, then click the link to copy the Find application file to your computer. *groov* Find can also be downloaded from [groov.com](#) or the [Opto 22 website](#).
- b. Open the Find application file.

A message may appear asking if you want Find to be allowed to make changes to your computer. If it does, click Yes.

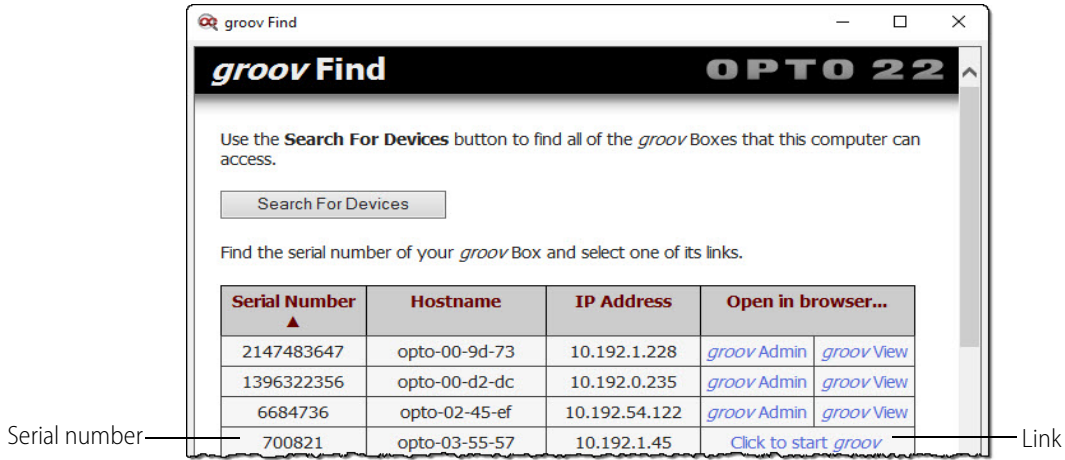
NOTE: If you are using a Windows account that does not have Administrator privileges (such as Guest), a User Account Control dialog box will appear asking for the credentials of an administrator account. To proceed, enter the Administrator User Name and Password. If you do not have this information, contact your IT department.

groov Find opens and automatically searches for *groov* Boxes on the network.

- c. Find the serial number on the bottom of the *groov* Box.




- d. 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.

- e. Click the link "Click to start groov."
- f. 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 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

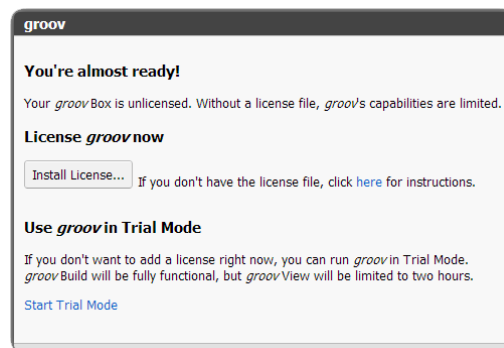
Follow the on-screen instructions to create a username and password for *groov* Admin. The *groov* Admin account is for administrative tasks such as changing or editing the network connections and updating the *groov* Box. (You will create a different account for building your *groov* project.)

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. 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 only work for two hours.

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



- b. Browse to the license file you downloaded in Step 7 ([page 15](#)), and then click Open. Your license is now installed.

Step 11. Create a *groov* Build Account

A *groov* Build account lets you create and edit a project in *groov* Build.

- a. 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.

- b. Click Create *groov* Build Account.
- c. Click Go to *groov* Build. *groov* Build opens in your browser.

If you have any trouble opening *groov*, see Troubleshooting in [form 2027](#), the *groov* User's Guide.

To create and view your mobile operator interface, see instructions in the [groov User's Guide](#).

3: Using *groov* Admin

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

In this chapter:

Opening <i>groov</i> Admin	21
Quick Start menu	25
Opening <i>groov</i> View and Build from <i>groov</i> Admin	26
Opening Node-RED Admin from <i>groov</i> Admin	26
Configuring Network Connections	26
Updating <i>groov</i> App (Build and View)	34
Backing Up <i>groov</i>	36
Restoring <i>groov</i>	37
Updating <i>groov</i> Admin	39
Updating Node-RED	40
Restarting the <i>groov</i> Box	41
Changing Username and Password	42
Checking System Information	43
Checking Hardware Status	44
Setting the System Time	45

Opening *groov* Admin

You can open *groov* Admin in three ways:

- From *groov* Build—see below
- Using the *groov* Admin URL—[page 22](#)
- From *groov* Find (only on a Windows computer)—[page 22](#)

Open *groov* Admin from *groov* Build

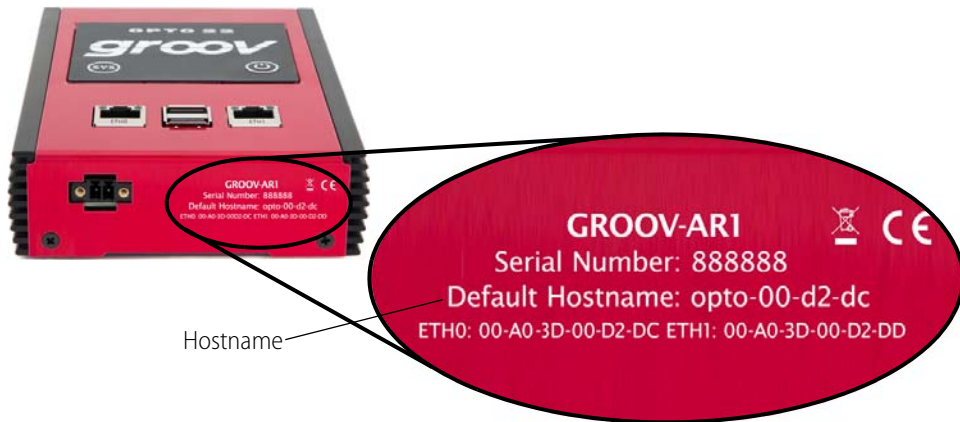
In *groov* Build, choose Configure > *groov* Admin. To log in, see [page 24](#).

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 24](#)).

Open groov Admin using groov Find (Windows only)

groov Find is a utility included on the groov CD 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. You can easily switch from one Box to another, for example when updating groov.

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.

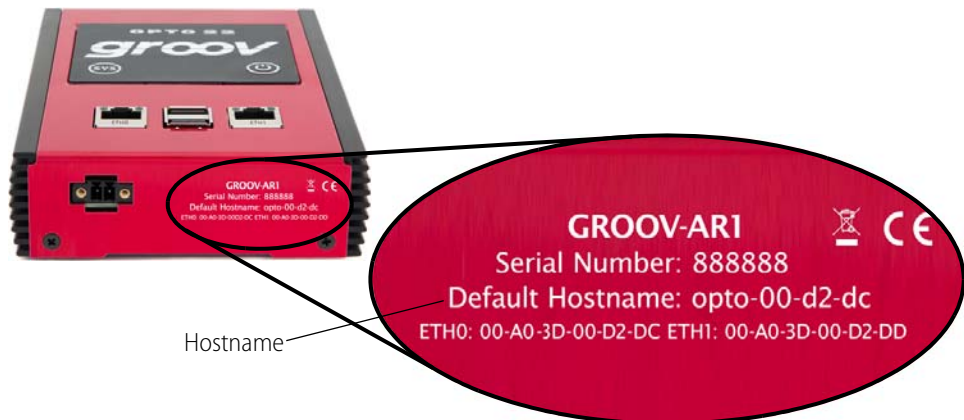
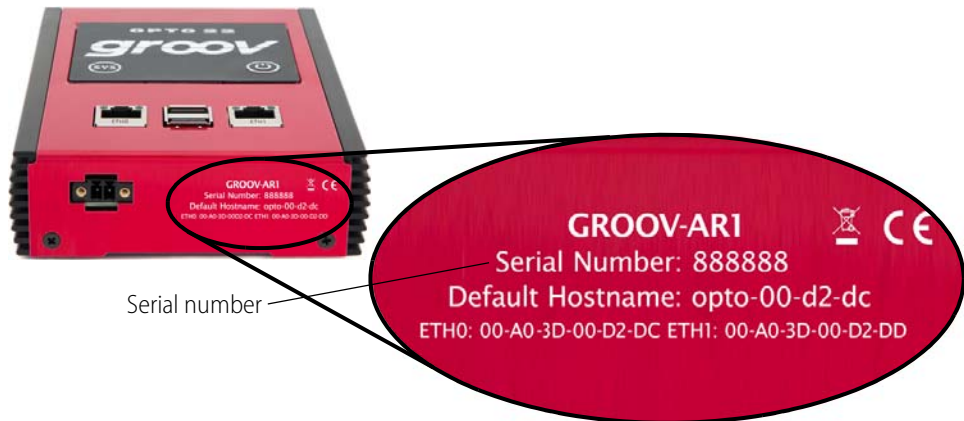
1. Open groov Find. If a message appears asking if you want Find to be allowed to make changes to your computer, click Yes.

NOTE: Clicking Yes permits Find to have temporary administrative privileges to create an additional temporary link-local IP address for each network interface on the computer. This enables Find to locate a groov Box 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 27.) If the network does have DNS and DHCP, the temporary IP address is not used and is removed when you exit Find.

groov Find opens and automatically searches for groov Boxes on the network.

- Locate the serial number on the bottom of the *groov* Box.



- Locate the matching serial number in Find.

Serial number

Link

Serial Number	Hostname	IP Address	Open in browser...
2147483647	opto-00-9d-73	10.192.1.228	groov Admin groov View
1396322356	opto-00-d2-dc	10.192.0.235	groov Admin groov View
6684736	opto-02-45-ef	10.192.54.122	groov Admin groov View
700821	opto-03-55-57	10.192.1.45	Click to start groov

- 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*" on page 16.)
A security warning appears in your web browser.

5. Accept the security warning (if you need help, see the next section).
6. Log in (see [page 24](#)).

Accepting 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 68.

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 *groov* Box” on page 74.

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

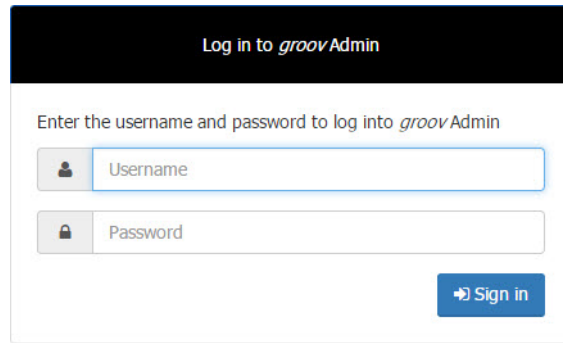
Click Continue.

For Internet Explorer

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

Logging 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.



Log in to *groov* Admin

Enter the username and password to log into *groov* Admin

Username

Password

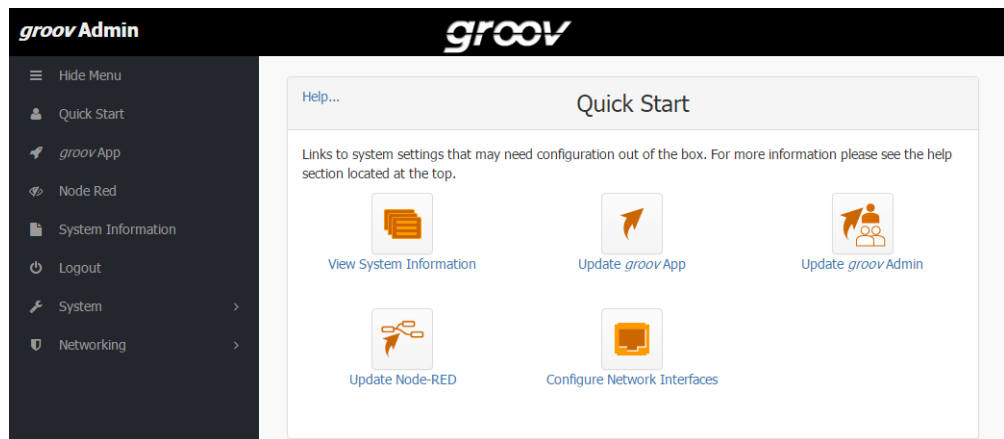
Sign in

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 43.](#)

 **Update *groov* App**
Update *groov* Build and View. See [“Updating *groov* App \(Build and View\)” on page 34.](#)

 **Update *groov* Admin**
Update *groov* Admin itself with the latest version. See [“Updating *groov* Admin” on page 39.](#)

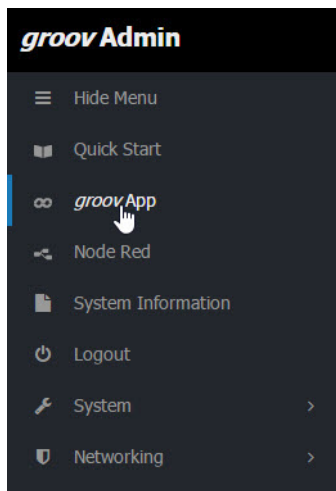
 **Update Node-RED**
Update Node-RED software running on the *groov* Box. See [“Updating Node-RED” on page 40.](#)

 **Configure Network Interfaces**
Configure IP settings for the wired and optional wireless Ethernet interfaces: ETH0, ETH1, and WLAN0. See [“Configuring Network Connections” on page 26.](#)

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

Opening *groov* View and Build from *groov* Admin

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

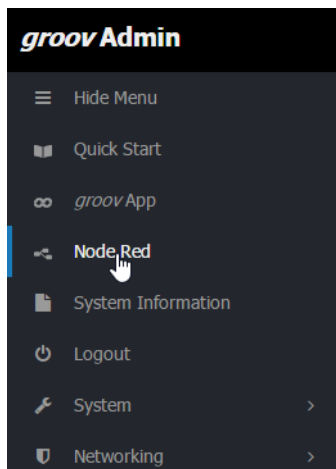


Your *groov* project opens in *groov* View. To get to *groov* Build, in View click the gear icon in the upper right and choose Switch to *groov* Build.

For information on using *groov* Build and View, see [form 2027](#), the *groov* 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.

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 27
- “Changing the Hostname, DNS Servers, or IPv4 Gateway” on page 28
- “Configuring ETH1 for the Control Network” on page 29
- “Configuring Wireless Communications” on page 30
- “Using an AR1 as a Wireless Access Point” on page 33

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.

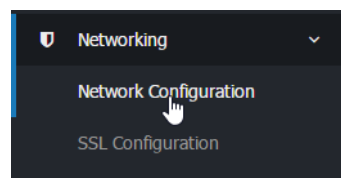
Assigning a Static IP Address

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: 255.255.225.0
 - **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.

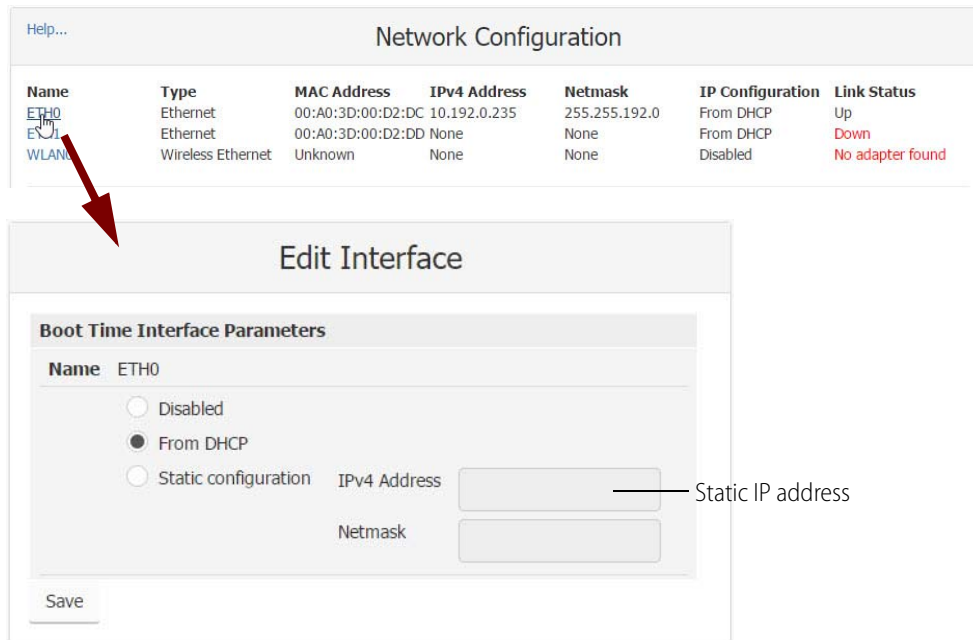


OR:



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.



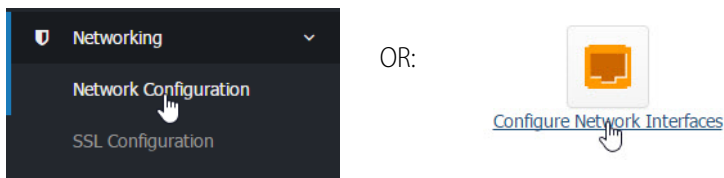
3. Select Static configuration. Enter the static IP Address and Netmask.
4. Click Save.

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:

DNS servers:

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

IPv4 Gateway:

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

- 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.

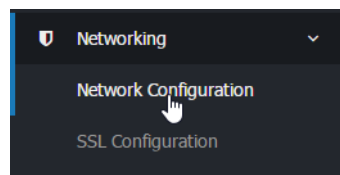
NOTE 2: Any changes to this interface may make your system inaccessible via your current wired or wireless connection. Be sure to write down the new hostname or other changes.

- Click Save.

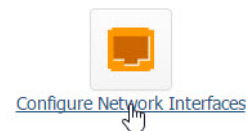
Configuring ETH1 for the Control Network

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.

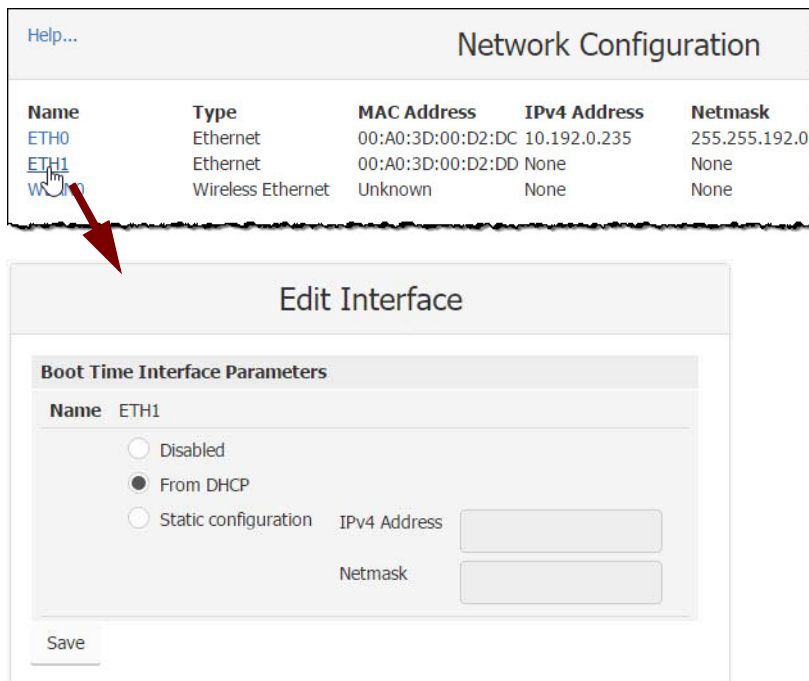
- In the left navigation bar choose Networking > Network Configuration, or click the Configure Network Interfaces button in Quick Start.



OR:



- Click ETH1.



- 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.

- 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.

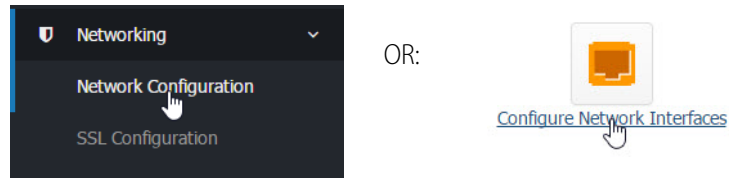
Before you begin, get the following information from your IT Department:

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

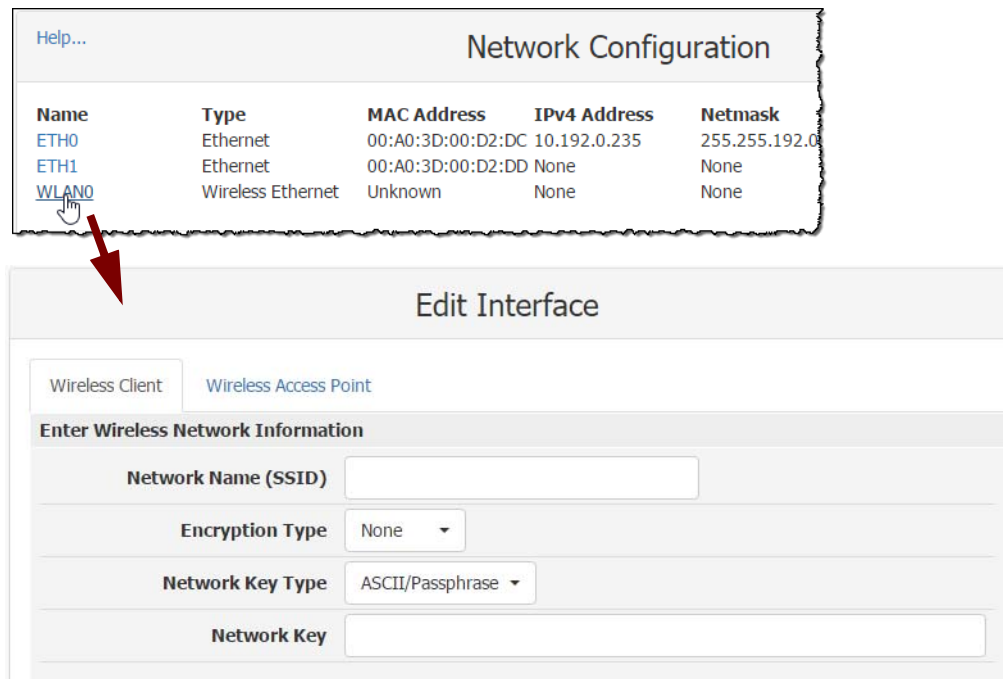
Security—Encryption type (WPA or WPA2), network key input type (hex or ASCII), and password

Password—To access the wireless network

- 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.



2. Click WLAN0.



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.

- 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.

- 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

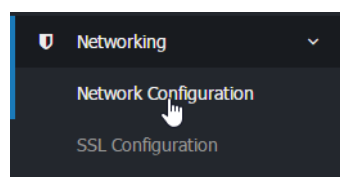
groov's SoftAP (Software Access Point) feature allows you to use your *groov* Box as an access point in order to create a private wireless network with WPA2-PSK security. This is particularly useful for connecting a phone or tablet to the *groov* App when there is no other wireless network available. 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:

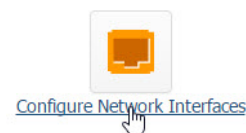
- Netis WF2119S
- Netis WF2116

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

1. Follow the instructions on page 91 to install your Netis WiFi adapter.
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. In the Network Configuration page, click WLAN0.
3. Scroll down to Boot Time Interface Parameters and make sure that WLAN0 is Disabled.
4. Scroll back up and click the Wireless Access Point tab.

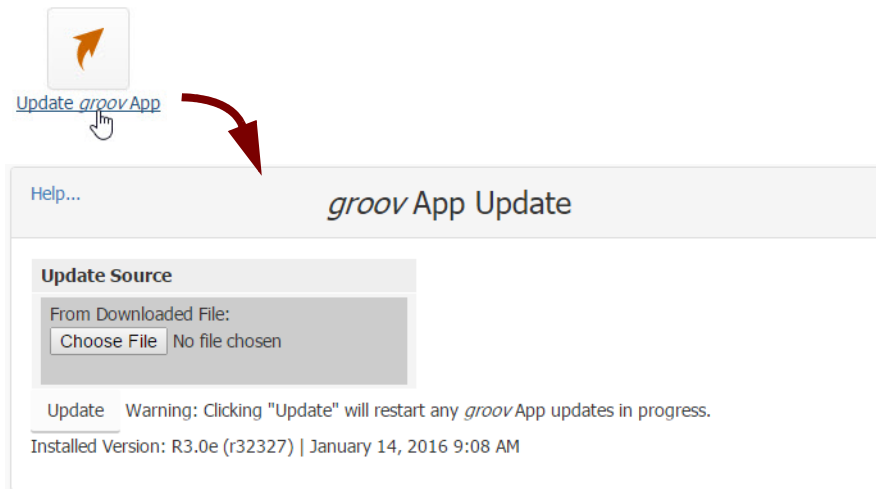
The screenshot shows the 'Edit Interface' configuration page. At the top, there are two tabs: 'Wireless Client' and 'Wireless Access Point', with the latter being selected. Below the tabs is the 'Software Access Point Configuration' section. It includes an 'Enable?' section with radio buttons for 'Yes' and 'No', where 'No' is selected. Below that are input fields for 'Static IPv4 Address' (172.16.0.1), 'Network Name (SSID)' (groov-ar1_1396322356), and 'Network Key' (ahbu708131). There is also a 'Channel' dropdown menu set to 'Nothing selected' and a link to 'Execute WiFi Sight Survey'. A 'Save' button is located at the bottom left of the form.

5. Next to **Enable?**, choose Yes.
6. 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.
7. 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](#).

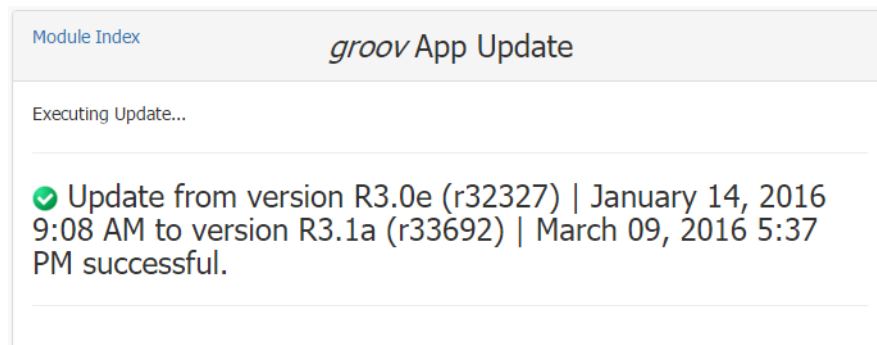
Updating *groov* App (Build and View)

1. Before updating *groov*, back up your project using *groov* Build (see form [2027, the groov User’s Guide](#)) or *groov* Admin (see [page 36](#)).
2. Make sure the *groov* Box is activated. See “[Step 7. Activate the groov Box and Get the License File](#)” on [page 15](#).
3. Go to manage.groov.com and follow directions to download the latest *groov*App update file and save it to your computer.
4. Open *groov* Admin.
5. Click Quick Start and then the Update *groov* App 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

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

NOTE: To back up Node-RED, see page 61.

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

If you have two *groov* Boxes or Servers at different versions of *groov* 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 *groov* at R3.3b to a *groov* at R3.3a should be OK, but moving from R3.3 to R3.2 is not likely to work. It's safest to keep your *groovs* at the same release.

To restore *groov* from the backup file, see ["Restoring groov" on page 37](#).

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

- *SMTP account info (including password)*
- *User email accounts (does not include the groov 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.

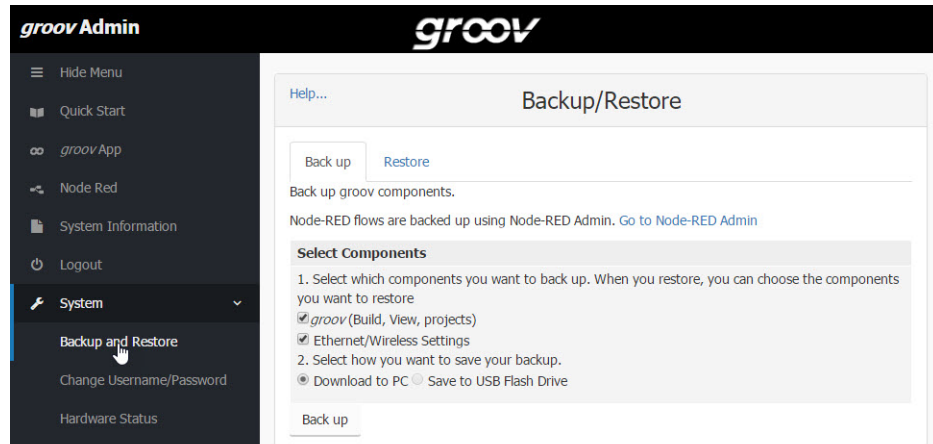
Also, be aware that if you send project files to Opto 22, our personnel will have access to the information listed above.

Follow these steps to back up groov:

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



USB connectors for backing up and restoring using a flash drive



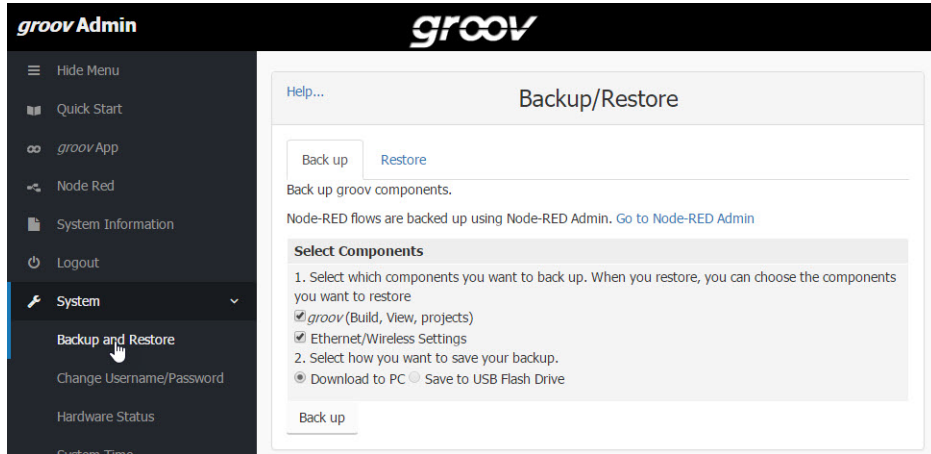
2. Click the Back up tab.
3. Select the components you want to back up.
groov (Build, View, projects) saves the *groov* App (Build and View) and your project.
Ethernet/Wireless Settings saves any settings you've configured for ETH0, ETH1, and the wireless network, including IP, Subnet, Gateway, Hostname, 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.
6. 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.
7. 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*

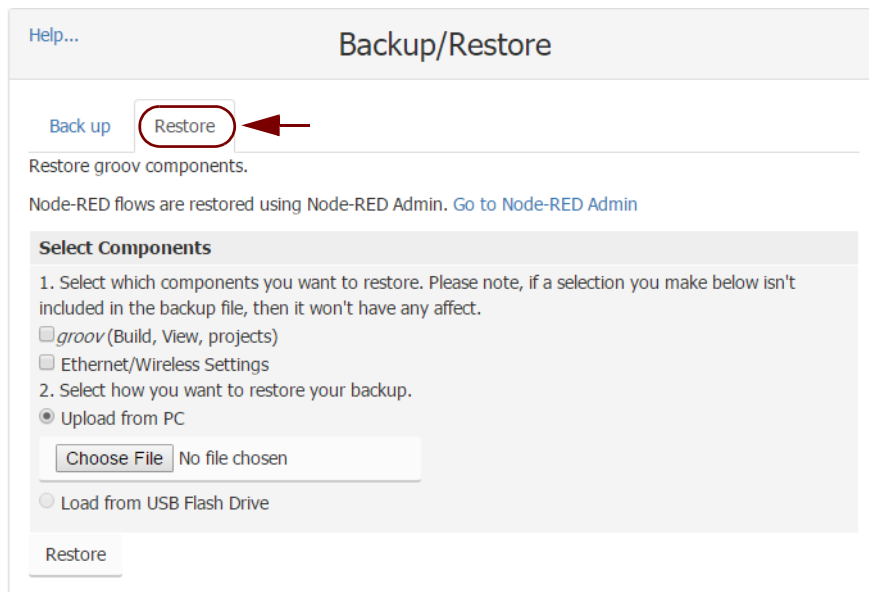
Use the following instructions to restore *groov* components from a backup file saved on a computer or USB flash drive (see “Backing Up *groov*” on page 36).

NOTE: To restore Node-RED, see page 61.

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



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* software and the project you built in *groov*. **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.

- Click Restore, and then wait while the files are uploaded. It may take several minutes.

Updating *groov* Admin

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

- Go to manage.groov.com and follow directions to download and save the latest *groov* Admin update file to your computer.
- If the Quick Start menu is not open, in the left navigation bar, click Quick Start.



Update *groov* Admin

- 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

- Click Choose File and locate the update file you downloaded. Highlight the file, and click Open.
- 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. Be patient and don't click away from this page until you see the success message:

Update *groov* Admin

Updating *groov* Admin... ✔ Success.



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

[← Back](#)

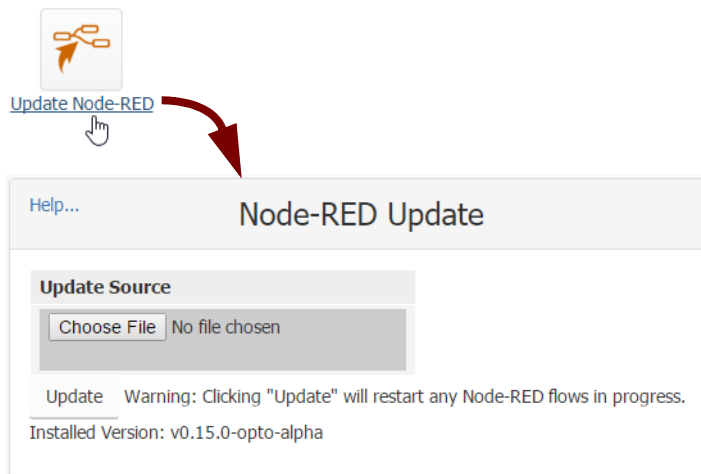
*NOTE: Your *groov* Box must be restarted for the update to take effect. While the *groov* Box is restarting, all of your users will be disconnected, and you will not be able to continue working in *groov*.*

- 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,” below.) 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. You and your users will be able to use *groov* View and *groov* Build once the *groov* Box has fully restarted and the SYS LED has stopped flashing.

Updating Node-RED

- Before updating, back up your Node-RED project using Node-RED Admin (see “Backing up and restoring your Node-RED project” on page 61).
- Log into manage.groov.com and follow directions to download and save the latest Node-RED update file to your computer.
- Open *groov* Admin.
- Click Quick Start and then the Update Node-RED button.



- 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* Build.
- 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. You and your users will be able to use *groov* View and *groov* Build once the *groov* Box has fully restarted and the SYS LED has stopped flashing.


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* Build. 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

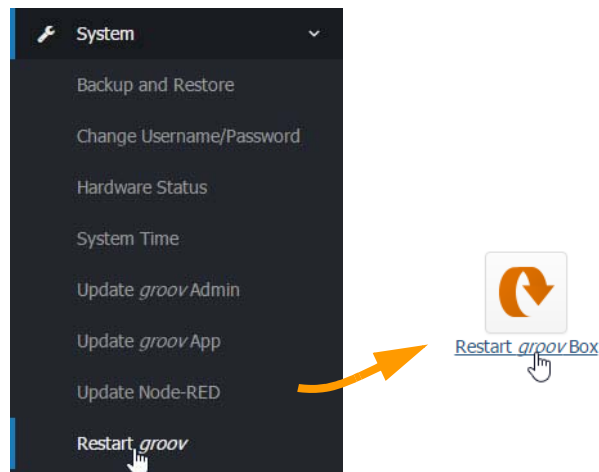
Updating *groov* Admin...  Success.



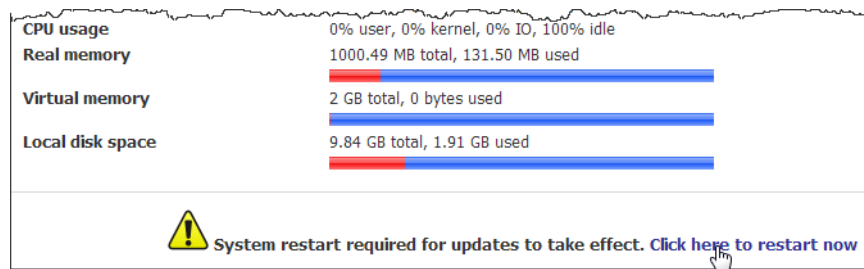
System restart required for updates to take effect. [Click here to restart now.](#)

[← 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.”



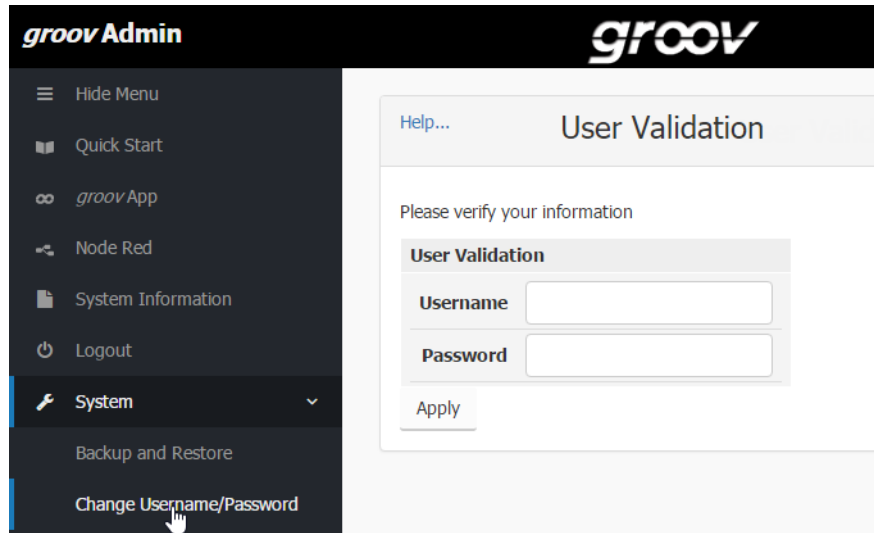
- **Hardware restart:** Press the On/Off button briefly and wait for the *groov* Box to turn off. Then briefly press the On/Off button again to power it back up.

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 and *groov* Build once the *groov* Box has fully restarted and the SYS LED has stopped flashing.

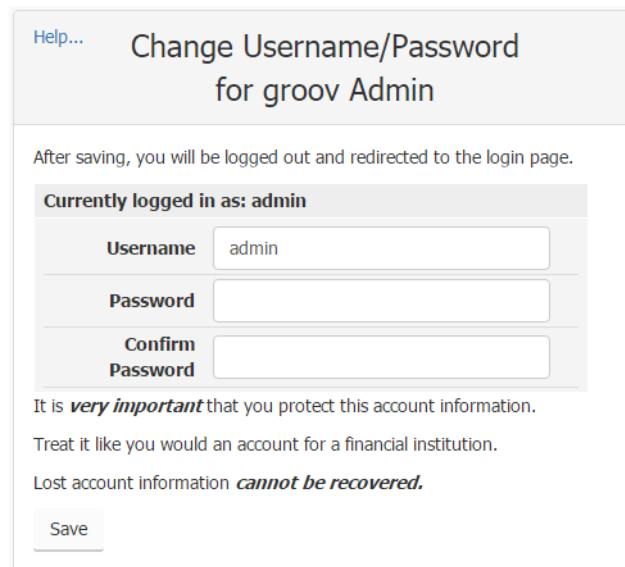
Changing Username and Password

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* Build.

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.



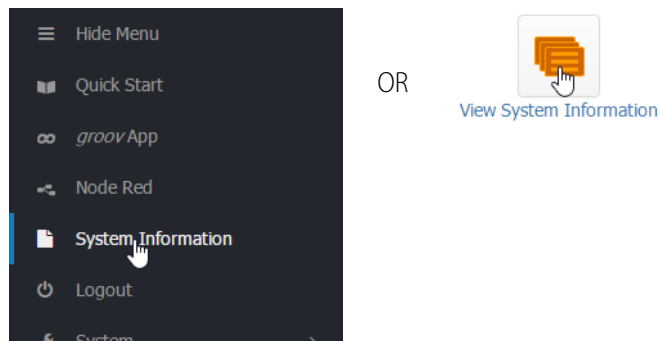
3. Enter the new username and the password in both boxes.

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.



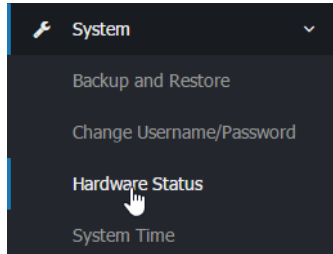
The following information is provided.

System Information	
System Hostname	opto-09-32-60
Activation key	Visit: activate.groov.com to activate your Groov box
groov Serial Number	695531
groov Part Number	GROOV-AR1
groov Image Version	31
groov Admin Version	1.570.46
groov App Version	R3.3b (r39719) January 04, 2017 3:08 PM
Node-RED Update Version	3
Power-Loss Tolerant File System:	Yes
Hardware Date	December 31, 2013
Time on System	Thu Apr 6 19:25:46 2017
System Uptime	1 days, 1 hours, 00 minutes
CPU Load Averages	0.17 (1 min) 0.32 (5 mins) 0.34 (15 mins)
CPU Usage	3% user, 1% kernel, 0% IO, 96% idle
Real Memory	1000.38 MB total, 263.34 MB used
Virtual Memory	256 MB total, 0 bytes used
Local Disk Space	12 GB total, 1.94 GB used

OPTO 22

Checking Hardware Status

- 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

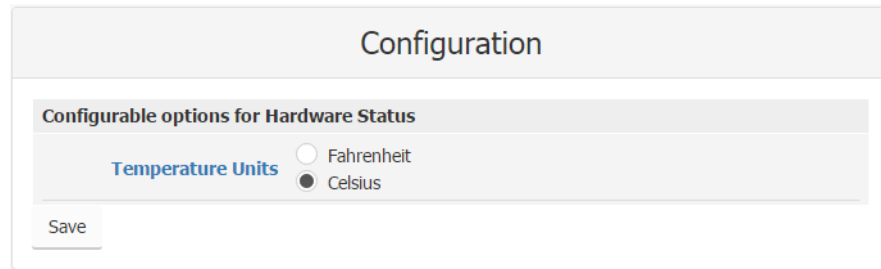
If any value is out of range, it is displayed in red and a message appears. Here are the values:

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 <i>groov</i> Box
Battery Voltage:	Voltage of the battery that maintains the date and time

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

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

3. Select either Fahrenheit or Celsius.



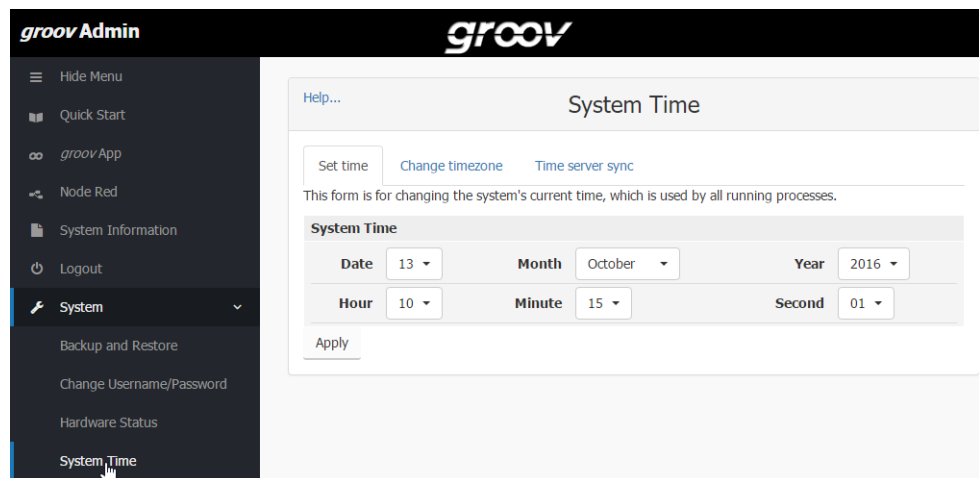
The screenshot shows a 'Configuration' window with a section titled 'Configurable options for Hardware Status'. Under this section, there is a label 'Temperature Units' followed by two radio button options: 'Fahrenheit' (which is currently selected) and 'Celsius'. Below these options is a 'Save' button.

4. Click Save.

Setting the System Time

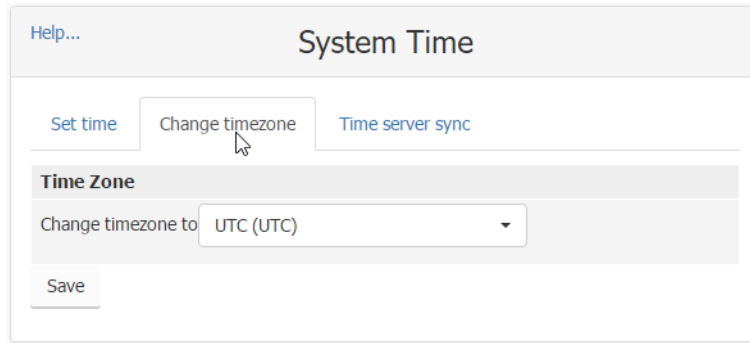
You can set the time and time zone used by the *groov* Box. You can also set the Box to synchronize with a specific time server.

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



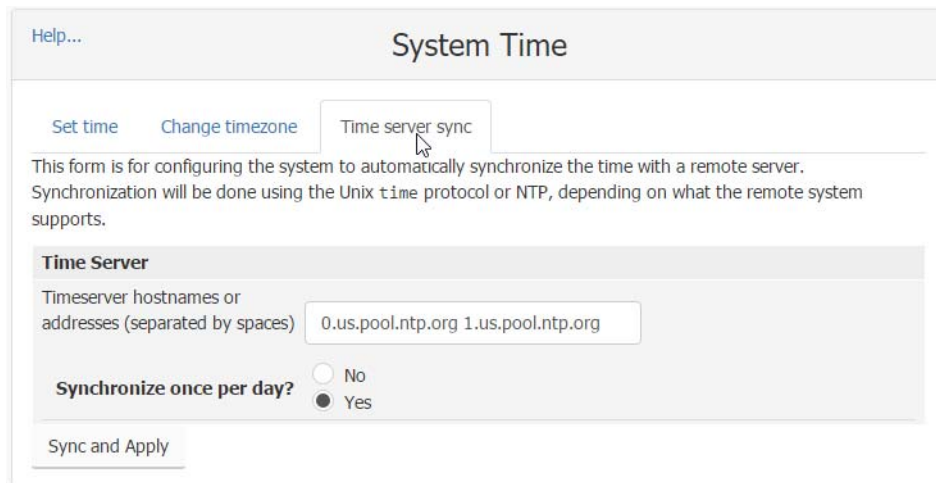
The screenshot shows the 'groov Admin' interface. On the left is a dark navigation sidebar with a 'System' menu item highlighted. The main content area is titled 'System Time' and contains several tabs: 'Set time', 'Change timezone', and 'Time server sync'. Below the tabs, there is a text box stating: 'This form is for changing the system's current time, which is used by all running processes.' Underneath, there is a 'System Time' section with a grid of dropdown menus for 'Date' (13), 'Month' (October), 'Year' (2016), 'Hour' (10), 'Minute' (15), and 'Second' (01). An 'Apply' button is located at the bottom of this section.

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.



4. In the drop-down list, select a time zone, and then click Save. Reboot the *groov* Box to use the new time zone throughout *groov*.
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.



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.

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* and for Opto 22 SNAP PAC programmable automation controllers. SNAP PACs are reliable industrial-grade controllers used in thousands of applications worldwide. The Node-RED nodes provide access to data in *groov* Data Stores and SNAP PACs. 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?	47
Getting Started	48
Connecting with serial devices	55
Working with nodes	57
Working with flows	58
Debugging your Node-RED project	60
Managing security certificates	61
Backing up and restoring your Node-RED project	61
Starting a new Node-RED Project	62

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 SNAP PAC nodes, *groov* 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 55 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 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).

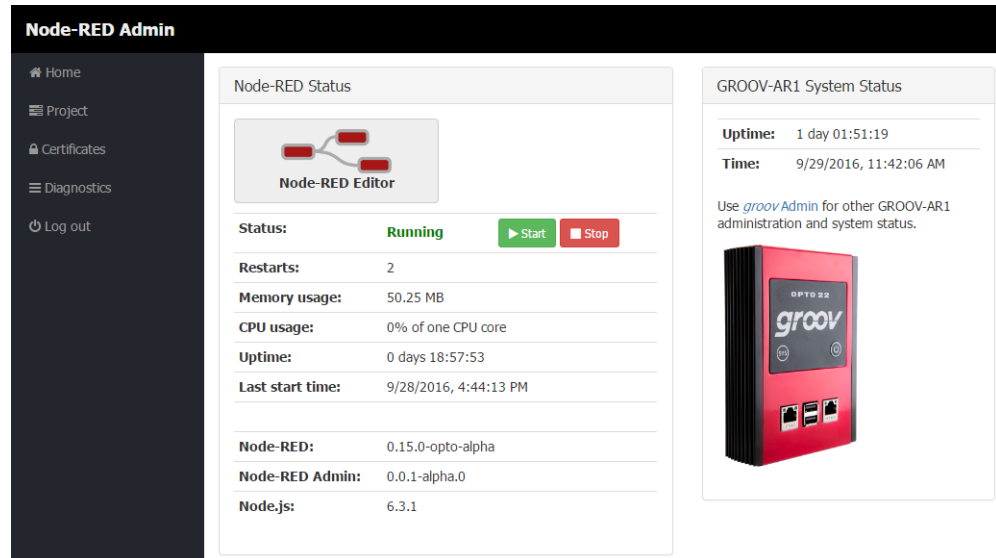
Open Node-RED

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`

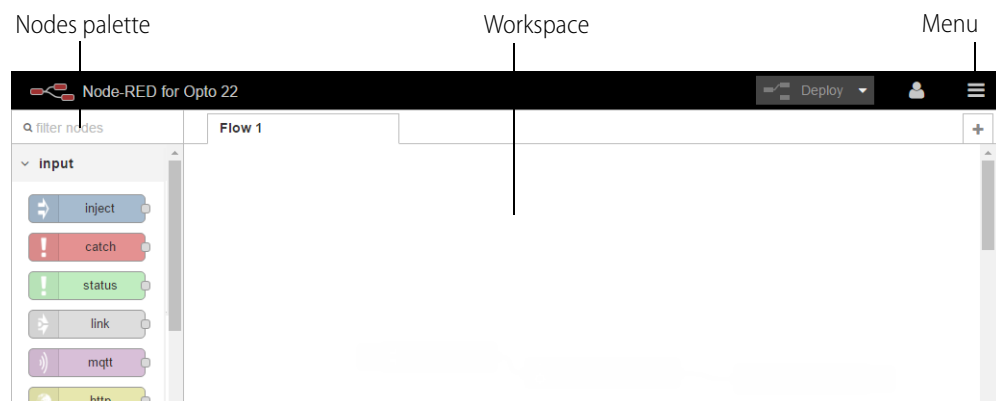
NOTE: This URL using port 3000 takes you to Node-RED Admin. In the future, if you want to go directly to the Node-RED Editor, use port 1880: `https://[hostname]:1880`

You can also open Node-RED Admin from within groov Admin. See [page 26](#).


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:

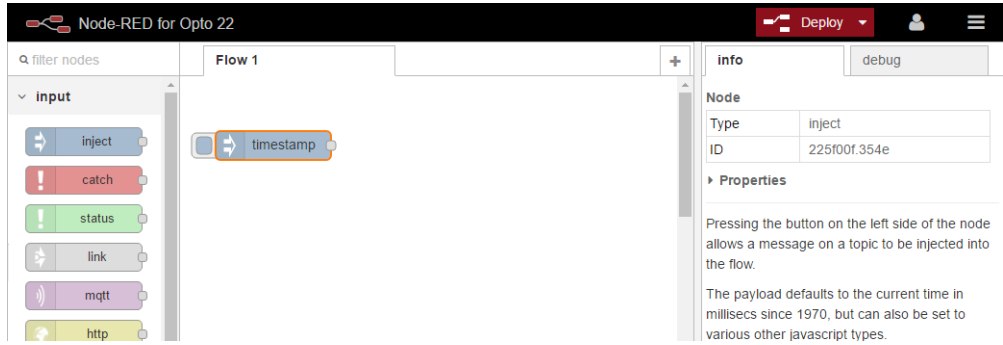


3. Click the Node-RED Editor button to open Node-RED.

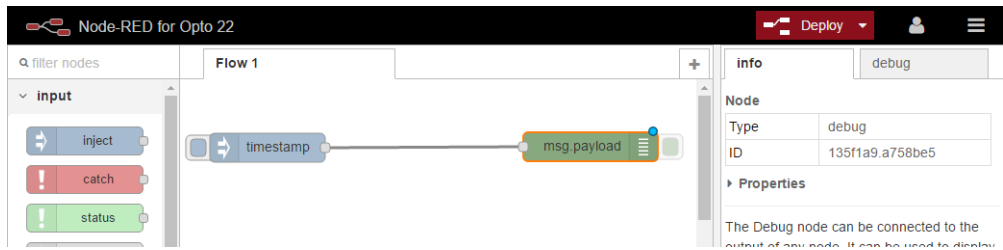


Create a flow

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.

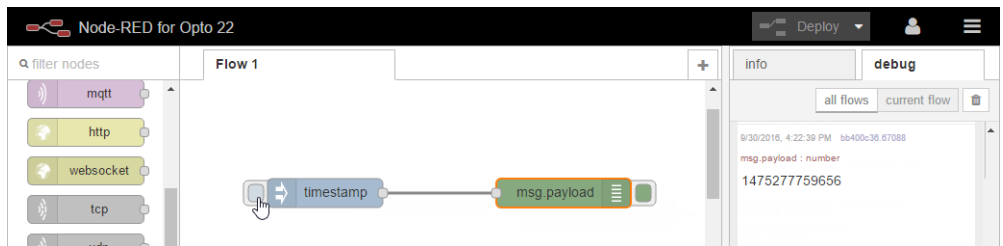


Deploy the flow and test

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:

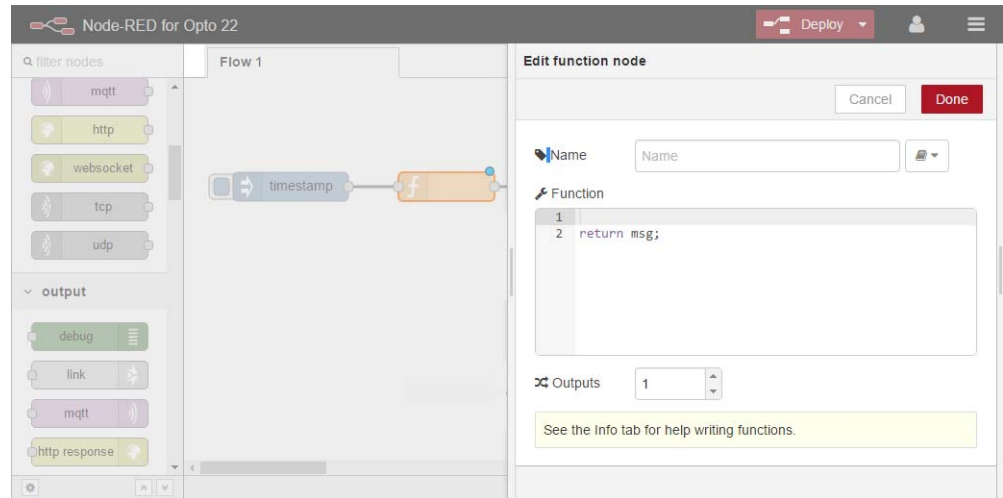


This number is a timestamp representing the number of milliseconds since January 1, 1970. This is the default payload of the Inject node.

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.

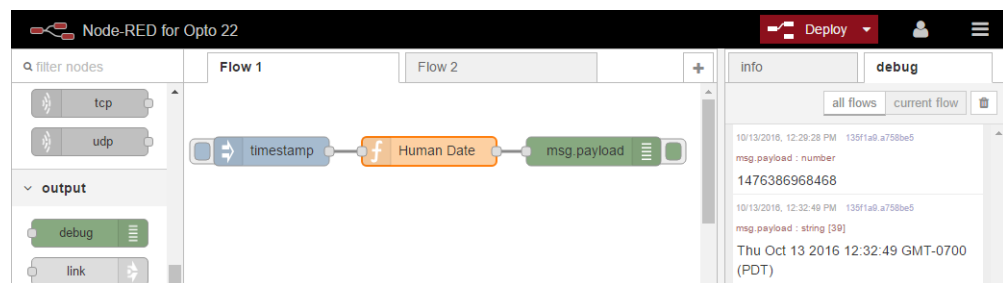


3. In the Name field, type Human Date.
4. Copy the following code into the Function field:


```
// 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:

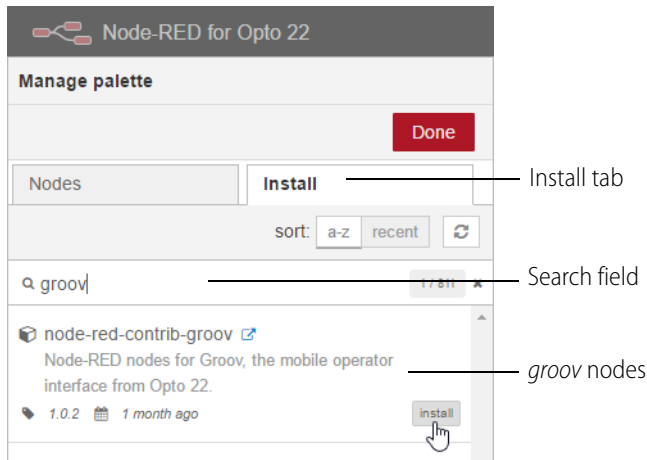


Install groov nodes

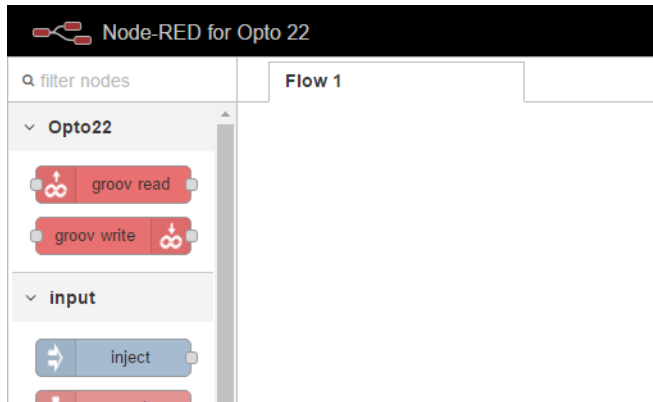
Your *groov* Box must have access to the Internet in order to install nodes.

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 nodes appear at the top of the nodes palette:



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

Add a SNAP PAC node

For this section, you’ll need to have an Opto 22 [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, with the PAC’s RESTful API configured. See the SNAP PAC REST API Quick Start instructions on [developer.opto22.com](#).

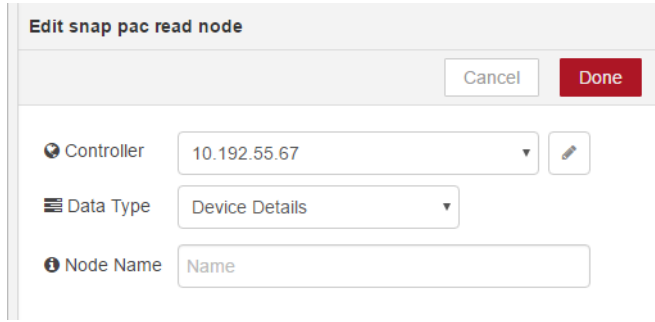
1. Install Node-RED nodes for SNAP PAC controllers, just as you installed the *groov* node. (Menu > Manage palette > Install tab. Search for `node-red-contrib-pac`.)
2. Make sure you have an inject and a debug node in the workspace.

3. Near the top of the Nodes palette, click the *snap pac read* node and drag it to the workspace, in between inject and debug (msg.payload).
The snap pac read node lets you read I/O and variable data on the SNAP PAC controller.
4. Wire the snap 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 snap pac node to edit it.

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

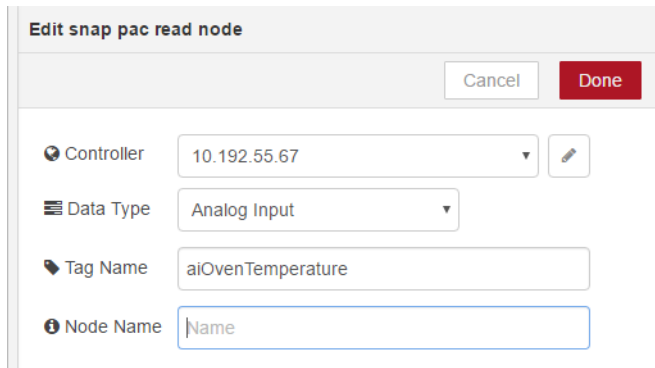
8. Complete the fields:
 - a. For PAC Address, choose the protocol (HTTPS is strongly recommended because it is secure) and enter the PAC's IP address.
 - b. Enter the API Key ID and Value to allow access to the PAC's API. (You must have already set this up for the PAC. See steps on developer.opto22.com.)
 - 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 61 to add the certificates to the *groov* Box.)
 - d. Click Add.

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

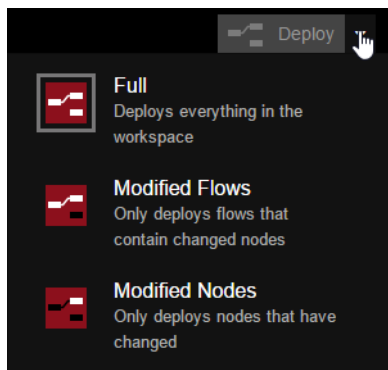


9. Choose the Data Type from the dropdown list.

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



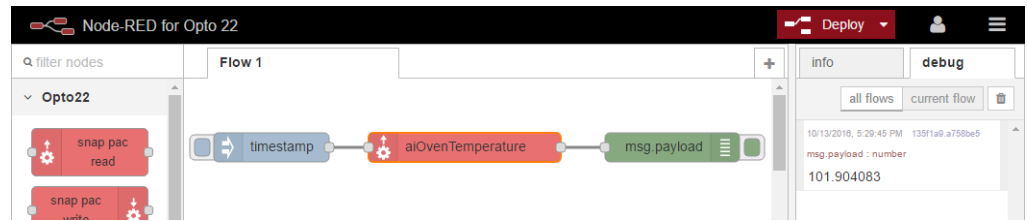
- a. **Tag Name**—Enter the exact I/O point or variable name from the PAC Control strategy running on this controller. If you leave this field blank, you'll receive values for all tags of this type (in this example, all analog inputs).
 - b. **Start Index** and **Length**—For a table, enter the starting 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).

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

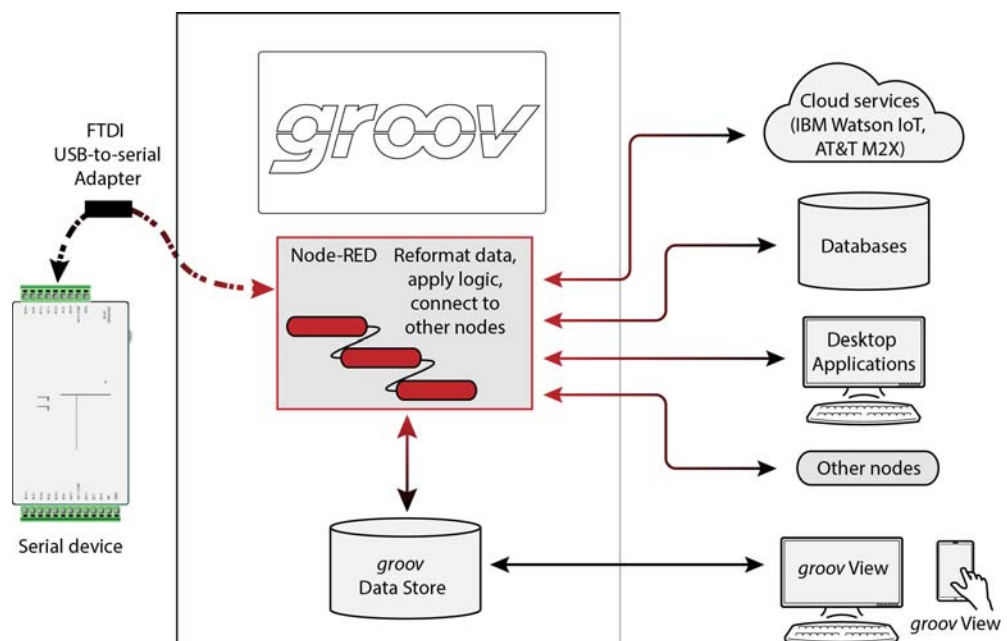


Connecting with serial devices

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* 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* Data Store, and use it in your *groov* 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

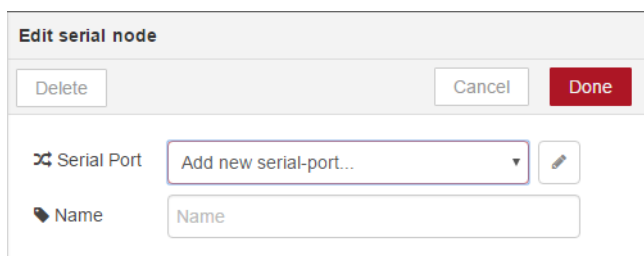
To use serial devices with the groov Box, you will need:

- *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 88](#)).
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 88](#).

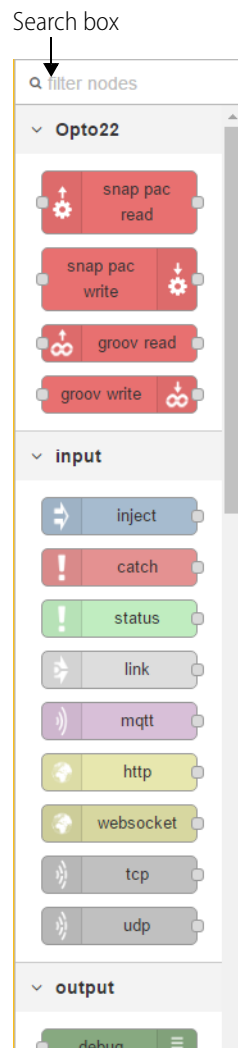
For serial devices connected through a USB hub, see address information on [page 88](#).

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

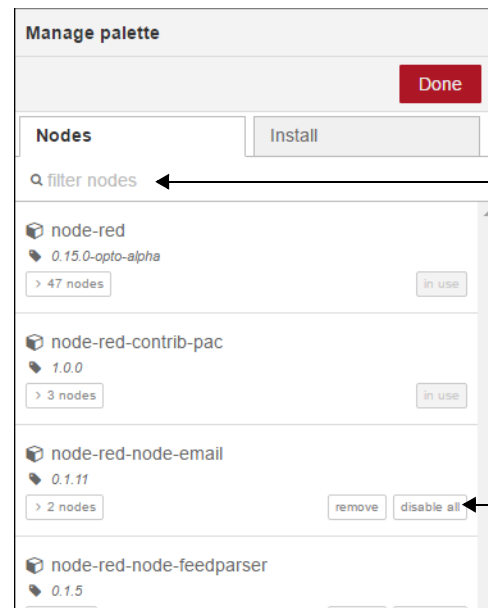


In the nodes palette on the left side of the workspace, you see all the nodes built into the program. You can scroll down to find the one you want or search for it by typing into the search box at the top. For example, if you type `tw` into the search box you'll find the Twitter node.

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.

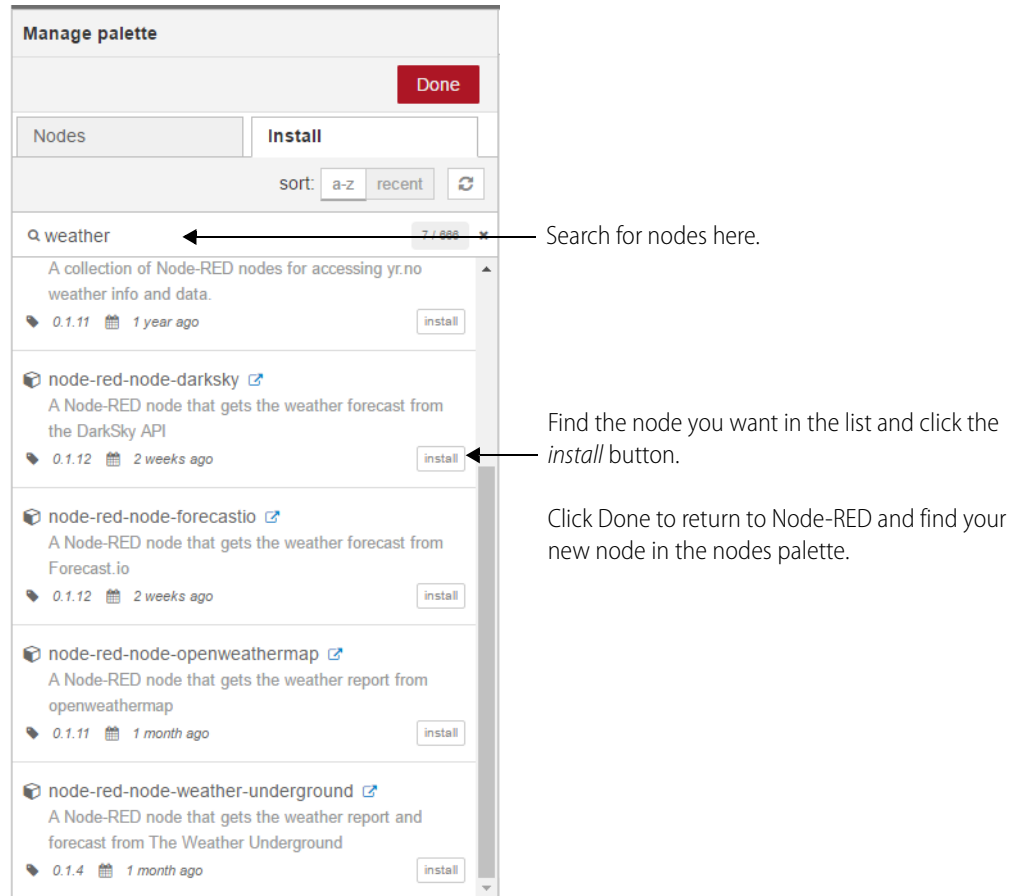
To disable or remove nodes, choose the one you want in the list and click the button.

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

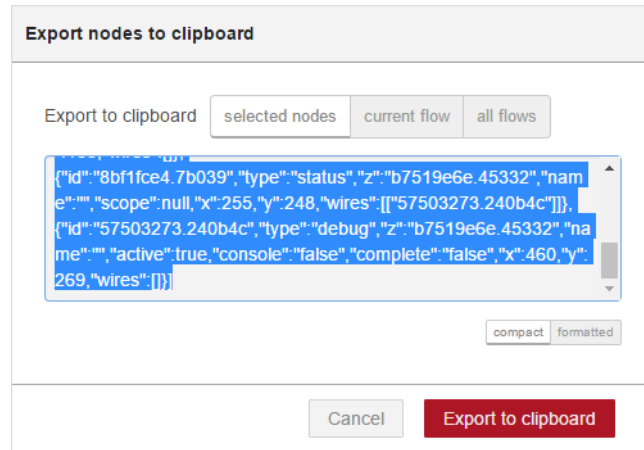
You can have one or many flows in your Node-RED project.

- **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.)

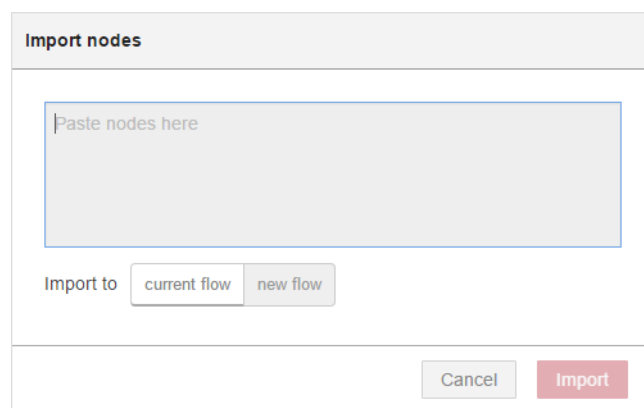
Import from the Library

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.



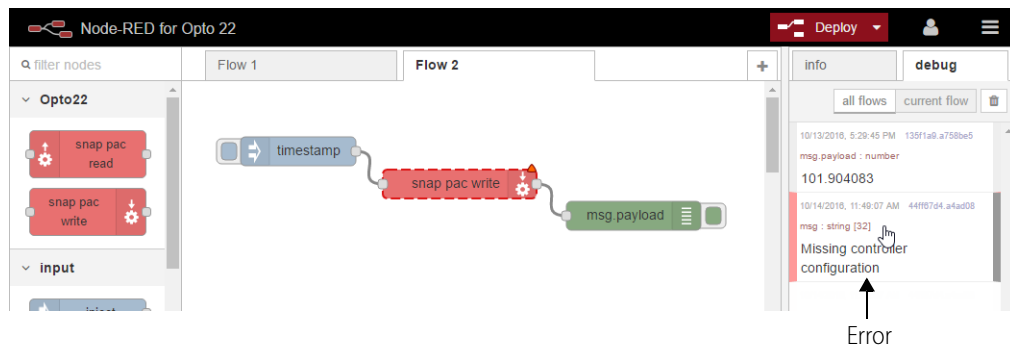
3. Paste the data into the field. Choose whether to import into the flow that's open on the workspace or to create a new flow.
4. Click Import.

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:



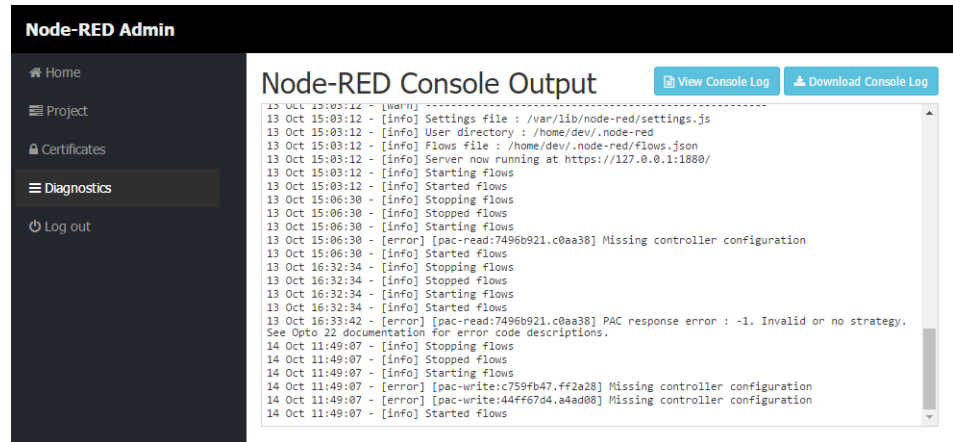
To see which node the error occurred in, hover over the error or click it to highlight the node (the node is surrounded with a dotted orange line).

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.

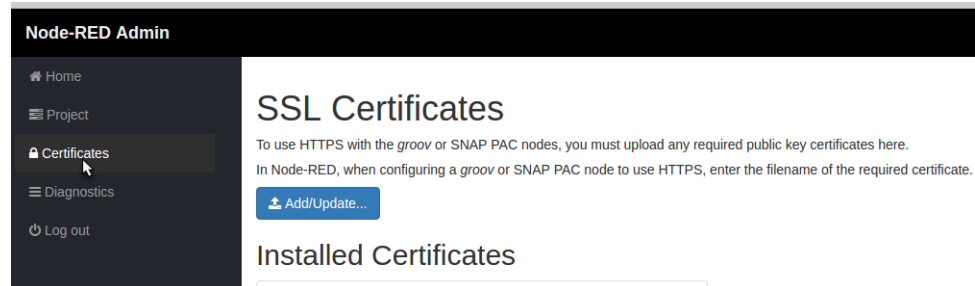


- To save a copy of the log, click Download Console Log. To view only the log in a separate browser tab, click View Console Log.

Managing security certificates

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

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



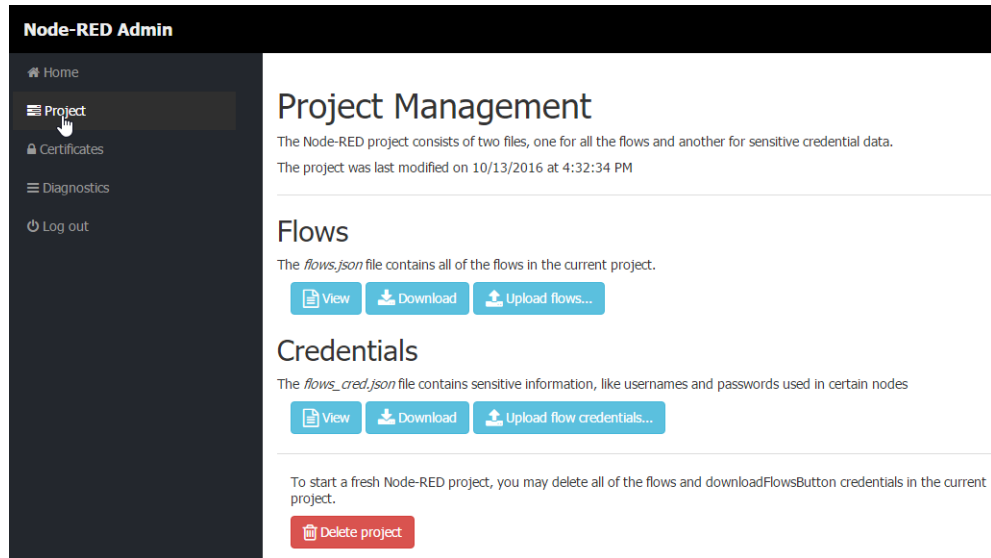
- If you've already added one or more certificates, you'll see a list of those installed.
- Click Add/Update. Navigate to the location of your SNAP PAC public key certificate. Click Open. The certificate appears in the list of Installed Certificates.

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.

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

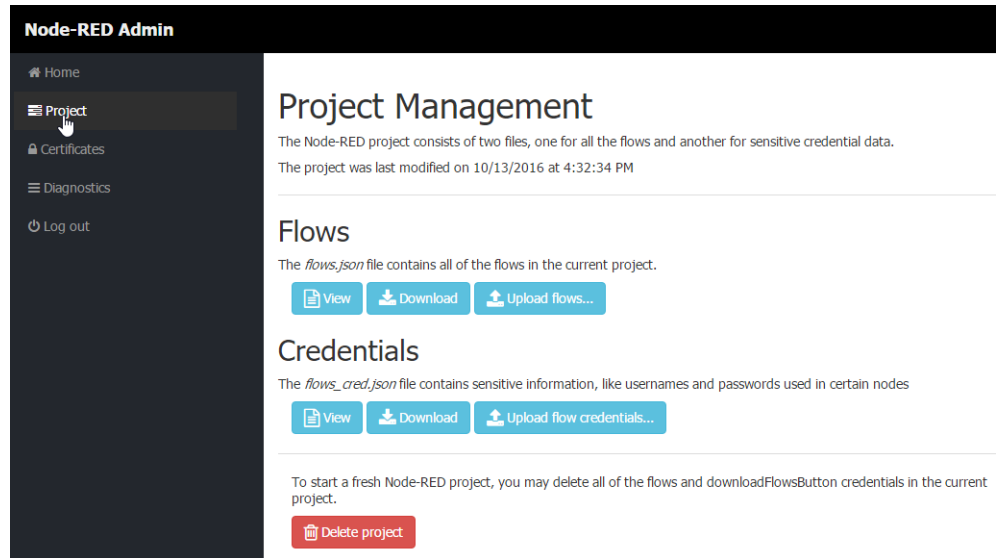
Backing up and restoring can take several minutes. Wait until the process is finished.

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 40.)

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.



The screenshot shows the Node-RED Admin interface. On the left is a dark sidebar with navigation links: Home, Project (highlighted with a mouse cursor), Certificates, Diagnostics, and Log out. The main content area is titled "Project Management" and contains the following sections:

- Project Management:** A heading followed by text stating "The Node-RED project consists of two files, one for all the flows and another for sensitive credential data." and "The project was last modified on 10/13/2016 at 4:32:34 PM".
- Flows:** A heading followed by text stating "The `flows.json` file contains all of the flows in the current project." Below this are three buttons: "View", "Download", and "Upload flows..."
- Credentials:** A heading followed by text stating "The `flows_cred.json` file contains sensitive information, like usernames and passwords used in certain nodes". Below this are three buttons: "View", "Download", and "Upload flow credentials..."
- Delete Project:** A red button with a trash icon and the text "Delete project".

Below the screenshot, there are two numbered steps:

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 an SSL Certificate

Understanding Certificates

Like other web servers that contain sensitive data—for example, your bank—*groov* uses an SSL/TLS certificate to (1) encrypt communications and (2) prove *groov*'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 *groov*. To avoid the warning you can install the self-signed certificate in all the browser certificate stores used to access *groov*. However, whether or not the certificate is installed in the certificate stores, communication between *groov* 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>groovs</i> 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>groovs</i> , or the set of browsers that will access <i>groovs</i> is unknown or changes frequently, or 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> administrator has demonstrated the validity of the certificate (e.g. by providing the certificate thumbprints).	Trusted by those who trust the <i>groov</i> administrator enough to install or let him or her install the certificate in their browser certificate store	Trusted by everyone

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* Project

IMPORTANT: Before starting any certificate process, back up your *groov* project. See “[Backing Up groov](#)” on page 36 for instructions. Certificates can be tricky, and you want to make sure you can recover if needed.

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

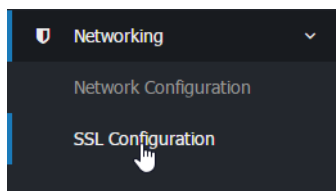
Step 2: Create a Private Key

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*. (See also, “[Changing the Hostname, DNS Servers, or IPv4 Gateway](#)” on page 28.) 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* in client browsers is <https://process1.acme.com>, then you enter `process1.acme.com`

If you have multiple *groovs* with fully qualified hostnames all with the same domain, another option is to create a self-signed wildcard certificate. For example, if you have two *groovs* with the hostnames *groov1.foo.com* and *groov2.foo.com*, you can create a certificate that has the hostname **.foo.com*. The same private key and certificate are then installed on all the *groovs*.

Server name: Enter the hostname of this *groov* Box that client browsers will use to access *groov*. (See also, “[Changing the Hostname, DNS Servers, or IPv4 Gateway](#)” on page 28.) 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 client browsers will use to access this *groov* Box is:

<https://process1.acme.com>, enter `process1.acme.com`

If the URL client browsers will use to access this *groov* Box is:

<https://mobilehmi>, enter `mobilehmi`

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* 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

```

-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKwggggkAgEAAoIBAQRFRq1SuiFghET
QeRA0ykygYKqj5q5qX74qmNL5npz2S5yM6nLkCyf4wZuiJi2Cc4h+dC+g41RLKu
QeSEStm+32n3qCSdGIGKf+OVRUU6eCT2whqps3z28Uox66Zkb2yxtM0Kpftq3m
VS+3AumzEWS1iE7v2p6b0mDghadH+C34fdKv5q1Vq3TII073VgLOTowCwPHEFy+
j5Kf2k7Uhxu11wz7KXZ0NRdBYEdybh0qgw/0Pwmi+Pwpp4Hwz0W7kXhaci5b
-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIIEBzCCBzggGjSgQwSMBGACGCSqGSIb3DQEBCwUQIMIGYMQewCQYD
VQOCeFJUwEELMAG1UECAwQOCeEATAEgNlBhMCFRlBw7dNobMSEwHwYDQk
DBhPFRFIDlyI69u1G9w4G8cMDA+ZD1+ZGMaDDMMEgN/Ba+MA0UzEEMMQGA1UE
AwwMTEYyE2DCC4eLjEwNDEgM4GCSqGSIb3DQEQJARYZEMjYXJyQ09wH3AM5j
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE REQUEST-----
MIIC3jCCAcFCAQwzZgcCahBqNBAITA1VTMqewCQYDQIDhJDQTERMA8GAIUE
BewIVG7cZRN1bGEkITAfBqN/BaoMGE5Q7E8gHjIgb24gb2B0by0wMCIkM1kTeEM
MboGAIUECwERNwMR7wFYUvQQDDA0KGIUMI4H1jAumITAM8MwHjI7Ro2IhveN
Aq8Fk7aZ8McJab380cDjLan8vTCCAIwDQYJgE2Ihw3QGE8B0AggFAEDCC
KQcQpPBRAM8Gc7WkTNRMPSEDS8DNJ6G0...84Pj...Y0...MaET...XELJ/
y0Gp/yScVwKFDac4RSDUaij/pu6UCawEAa8AMAGC8qG0IeSDQECW0AA41B
Aq48njKlhnge1eqI9k73J2KuF66Fq38UNJ3gHd2iJHjwo9Qc3nVq4T/WaUgHys
KmmG6Wrdw/pqmNjhbNLTp0Wq8cH/vrE1769nCS8EUV/ZED7a5av7/kyuT0ZR
OwdI7wv8M5ocJHd3j2mMa18aj7e48q96828wHv1e6JELLINg9vPDE8ai
eN4S1aPaF8P8T02/GOWI TRSTCTIPaD6cF27ab7/TrasEUP0V9+22K/2mb+end0
Jgo88F8ka18n1a1h8F88KQc0hIRakvaJY+2bFjYgEqlfa1LLNCHMwGTVaogc
NIR8QxKjQil+fIDM8SHjKjLd
-----END CERTIFICATE REQUEST-----

```

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 *groov* Box" on page 74.

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 69

[“Add the Self-Signed Certificate to a Browser Trust Store on a Computer” on page 70](#)

[“Install an SSL Certificate on Mobile Devices” on page 73](#)

Finish the Self-Signed Certificate

When you created the private key ([“Step 2: Create a Private Key” on page 66](#)), 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.

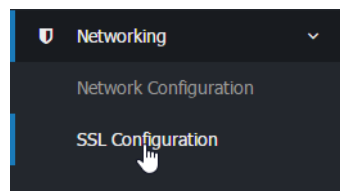


For Internet Explorer 10: Click “Continue to this website (not recommended).”



For Safari: Click Continue.

3. When *groov* Admin returns, select Networking > SSL Configuration.



4. Click the Current Certificate tab, then select “PEM format.”



The certificate's text appears.

```
-----BEGIN CERTIFICATE-----
MIIEBTCCAu2gAwIBAgIJAMz8yixPBBGyMA0GCSqGSIb3DQEBCwUAMIGYMQswCQYD
VQQGEwJVUzELMAkGA1UECAwCQ0ExETAPBgNVBAcMCFRlbWVjZDwXhMSEWwYDVQK
DBhPUFRPIDIyIG9uIG9wdG8tMDAtZDI1ZGMxDDAKBgNVBAsMA0VuzZEWMBQGA1UE
AwNMTkyLjE2OC4wLjEwNDEgMB4GCSqGSIb3DQEJARYRZHNjYXJyQG9wdHAYMi5j
b20wHhcNMTUwMjEwMjEzNTU3WheNNDUwMjEwMjEzNTU3WjCBMDELMAkGA1UEBhMC
VVMxCzAJBgNVBAGMAkNBMRewDwYDVQQHDAhUZW11Y3VsYTEhMB8GA1UECgwY1BU
TyAyMiBvbiBvcHRvLTAwLWQyLWRjMQwwCgYDVQQLDANFbmcxFjAUBGNVBAMMDTE5
Mi4xNjgumC4xMDQxIDAeBgkqhkiG9w0BCQEWEWRzY2FycyBvcHRwMjIuY292MIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApGMvd+ATfSBegut+qy0C20QP
HJspbae+OP1mK18LRSXGmOkC1+U12qMf7vPpOkFD21Xmg/ytBOCfcjPuxriGCh5
3RF7mdF4RbaZOTnF7Y3cqdBtQ087UPUfAsv6BXyLXA3qlFMnnspl+Jzh8l/dNwN/
twIS0rgrDf1j3ugGdV0e4wzZ+SGqoYiIVkASUzV5a3+2SCfojRYxmvvSnfew9Lg4
GWUJMTW0qmpCwXgBOIasXzyvxxwIO4zqZEygbVhnlTjCgSxhnm/86O7s61Rh7Fd
zt1lEj8X/T/oDceFp7Na48fKUGggjo7ubcYEWiAnWpLbA/8Ldfw4mDoSok2bhQID
AQAbolAwTjAdBgNVHQ4EFgQUb+2Tvx3Rpg3b9ZB1hwrZiIitutsWHDVROjBBGw
FoAub+2Tvx3Rpg3b9ZB1hwrZiIitutsWHDVROTBaUwAwEB/zANBgkqhkiG9w0B
AQsFAAOCAQEAA71G7qjadOdWHLdBwA0VMu85uHzi+NUDLQDVoyJQ2+TVEOgC4m+x
p2wuf/c4+RAvTOeNzxYgvt2iVcmH1vyZWW0VJ3OIXSfgdgkLjN7xioYW58jttq0G
g4xGAsN1opxG4Nut9ubjYLSjibF71iGzu4d5/PLhQDHqAUIWkk+sHyQDiWASgeh0
Spft39SKnNgBLBASwRcnmasqylTYwh1D9AHWXA2VI3h0xCv1qxhKhjRKRWA5bqrg
c5fm0eXf3cGe/XYaDn9iWdt/7fHnJz7ACncXVXxjTdf8L2ZCa9ge2y4E/+ox0Yj
Cg801mjL70Bjs96jP9YbWJO+BOGbkhtjw==
-----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.

5. 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 66](#)..)

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 *groov*. 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 71](#)

"OS X" on [page 72](#)

Windows

Internet Explorer & Chrome

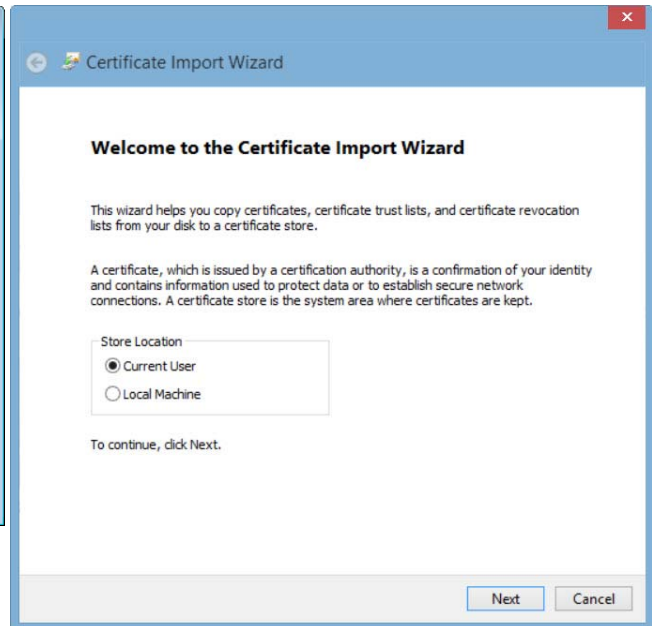
1. In Windows file explorer, locate the `<server name>.cer` file you created in the previous step.
2. Right-click on the file and choose Install Certificate.

The Certificate Import Wizard appears.

Windows 7



Windows 8



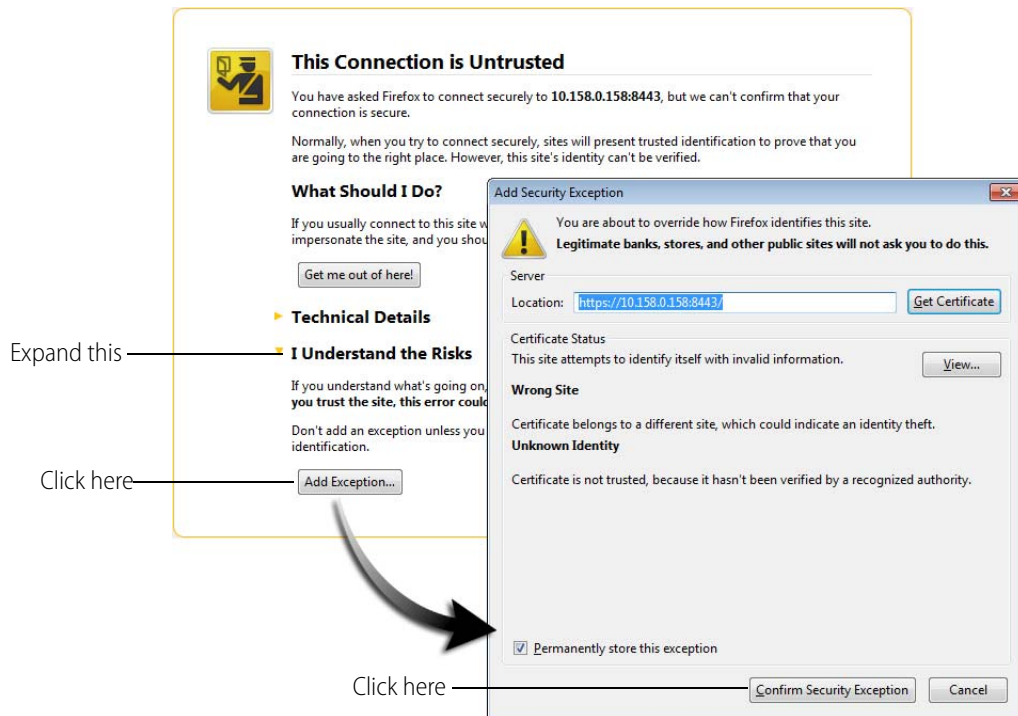
3. (Windows 8 only) If you are administrator of local machine, choose the Local Machine certificate store so this certificate will be trusted by all user accounts. Otherwise it will only be trusted by the current user account.
4. Click Next.
5. Select "Place all certificates in the following store."
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 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."
5. Click Confirm Security Exception.

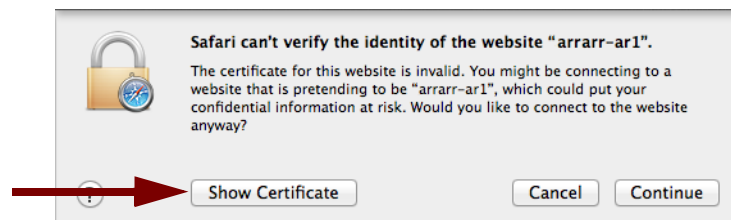


6. To verify the certificate was installed correctly, open Firefox and enter the hostname specified on the certificate. If the browser does not generate an untrusted site warning, the certificate was installed correctly.

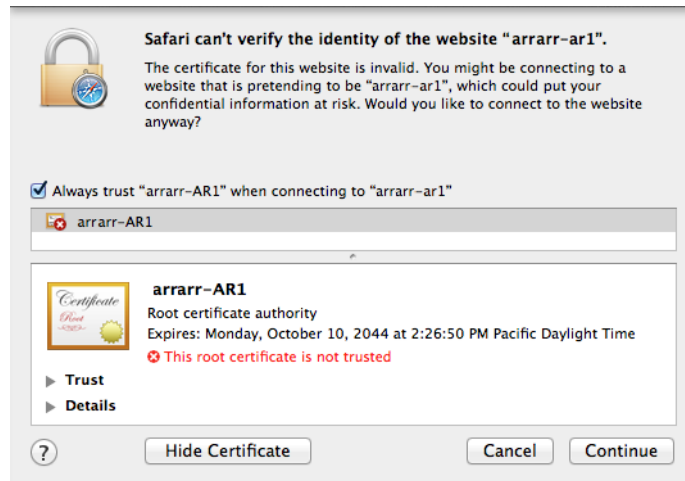
OS X

Safari and Chrome

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



2. Click Show Certificate to reveal the full details:



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 73](#)
- [“Android Devices” on page 74](#)

iOS Devices

1. Email the *<server name>.cer* file you created previously (see [“Step 2: Create a Private Key” on page 66](#)) 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 66](#)) 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 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 74](#))

[“Obtain a CA-Signed Certificate”](#) (see [page 75](#))

[“Install the CA-Signed Certificate on groov Box”](#) (see [page 76](#))

Finish the CSR

When you created the private key ([“Step 2: Create a Private Key” on page 66](#)), 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.

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-----
MIIC3jCCAcYCAQAwZGxkCzAJBgNVBAYTA1VTMQswCQYDVQQIDAJDQTERMA8GA1UE
BwwIVGVtZW50bGExITAFBgNVBAoMGE9QVE8gMjIgb24gb3B0by0wMC1kMi1kYzEM
MAoGA1UECwwDRW5nMRYwFAYDVQQDDA0xOTIuMTY4LjAuMTA0MSAwHgYJKoZIhvcN
AQkBFhFkc2NhcjAb3B0cDIyLmNvbTCCASIdQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBANWp3jKqPrlMtZFX0c5bJ3WiBt9ZifLe2cMgr7xg3z0pTEeKPFiqt32
hvJnsIyCr45C6rMCQVbiV9vxtaLHBN39DItS7gO6WrNq9kbYnUnkSVwE/fr8toPk
MdzVxmIt877A3ZtcEI3YxnFLSxsNcGOD4BFajoyNWLHMDN5Qnxyfv034czvLM/E
kKbfo/zZAJjMCWrBeFEUFNxDwOsf2cfreFtbMyeB1oQy65bB3RRSxRC21BOAMi
bi+eRIAvmIf8YrpgijyPRdJOpnBVNfe8GLR6gh13SXPwuVborCv18UXCqHwQtg0J
YHanWnzsaBPTVfqLmzHc00DbdbiV+LUCAwEAAAAMA0GCSqGSIb3DQEBCwUAA4IB
AQDBvZEJPCu1pm03hmQZeKQp3OLIUwF120ctXZK3GNzUaqo0Rv92emV4HW3TrYlw
iYrbe+bsaBDg4DN93sF6bEwr6ryKBCvGuBIES5nLgZsml+DeAat1kLFVWqTBhwg
BY032tiBn/j8E+hx0M5zq8nIHPS8OPQ1RkyTbABu7Tmmj8Q7WmymdgdzcCT+rpN
FS99Xfepkq/s7YrCs3b2iMj35UMTztimyg13fQ2I56byMcbZLQ69Baq8qwYpvooi
N0HQXUdTQNwXi+pdDnGpSxsmb5UnZ2kDcF7cHvDCrFBBpFGruXA0ER5Ik0ZixMBB
d3Xoxd/9VxOtja7u0Q/xvwxJ
-----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 66](#).)

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.

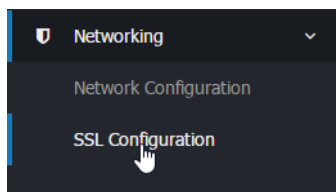
To paste the text into a text field on the CA’s website, open your `.csr` file in a text editor such as Notepad, select all of the text and press CTRL+C to copy the text to the clipboard.

```
-----BEGIN CERTIFICATE REQUEST-----  
MIICjTCCAXUCAQAwSDELMakGA1UEBhMCdXMxITAfBgNVBAoMGE9QVE8gMjIgb24g  
b3B0by0wMi0yYS1hNjEwMBQGA1UEAwNb3B0by0wMi0yYS1hNjCCASIdQYJKoZI  
hvcNAQEBBQADggEPADCCAQoCggEBAPnEPMiUKONk5YKpt4jw183qShIKHpOIbE  
c3D4IpSa0eliPjbyIxsesY68DmqcXEvPXzSxyjeFVHKgDdOgrQIVhrAtUWn4aLCU  
sNI9GbcCOft1dLRxxceyI1DeVQD5KI6DR2xCGnqvMwpc8tzbJksYWroPjCRFwVi7  
V5oG405YGsqxBQAVKiQBRyjTJUkKDu/HGb5WtVYUoieogUllnhnttpH71Kk2iZ+K  
ZgXss8W017v9/I4nsc9sFTq8Iclg9G9tsfsjX+S46UfVmeu2ExYzbz3dvTJF6mzC  
z9mL5Q5Sy6RZT56ksJGM2GVaQo9sfHcgjdYJlbaEpM9nYXfDgg8CAwEAAaAAMA0G  
CSqGSIb3DQEBBQUAA4IBAQCvRm0AQVeMyj6LC7YBLCP5iGnlFM++PH3rZjwrJi2b  
rOdgStAeYLMewo+XU/8G5pMojnwhfvBnBbukovA7gi77my0JBvQPLJBQ8u9GQ1EU  
GY7r19gcn9uncW6FzkH0WNkvCC6Ps5lqPUgcBQE9+/aI10MRWNdwLVZn21HKYMH  
+H/8dPftbsUzoHvHBjNZG5WPaJwrdrnOSvdltOuPl/TBuOKIDTmqjYoUANtyjQnc  
U745b/kU8RQuNsylvk6aFmNP7oWgIou7CgWQ09ZfFcEGATn3+QDXH15tlpYOGljMM  
7UD2Y6ue9s5sxxv2ME6V2BAP6V8DcSWDq78NhQcwkj/X  
-----END CERTIFICATE REQUEST-----
```

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

Install the CA-Signed Certificate on groov Box

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



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

The screenshot shows the 'SSL Encryption' page with the 'Upload certificate' tab selected. The page contains three main sections for inputting certificate data:

- Private key text:** A text area for pasting the private key, with a 'Choose File' button below it.
- Certificate text:** A text area for pasting the certificate, with a 'Choose File' button below it. A radio button is selected for 'Combined with private key'.
- Chained certificate text:** A text area for pasting chained certificates, with a 'Choose File' button below it. Radio buttons are present for 'No chained certificate' and 'Entered below ..'.

At the bottom of the form is a 'Save' button. A red arrow points to the 'Upload certificate' tab in the top navigation bar.

- Under "Private key text," click Browse and specify the `<server name>.key` file you created and saved in "Step 2: Create a Private Key" on page 66.

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

- Under "Certificate text" click "Entered below," then click Browse and specify the file containing the signed certificate that was obtained from the CA.
- If your CA used intermediate CA certificates, they should all be contained in a single file.

The certificate may or may not include an intermediate certificate file. If you are not sure if your CA used intermediate CA certificates, ask your CA. Or, to find out if the file is a part of the chained certificate path, open up the server certificate in Windows and click the tab that says certificate path. It should show you the chained path and where the intermediate files should be placed.

For example, if you obtained your signed certificate from StartSSL™, the certificate was downloaded to a file named `sub.class1.server.ca.pem`.

- Under "Chained certificate text," select "Entered below."

- b.** Click Browse and specify the file containing all the intermediate CA certificates in the certificate chain between your certificate and the root CA certificate. For a StartSSL class 1 free certificate this is *sub.class1.server.ca.pem*.
- 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.

6: 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 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 *groov*. Otherwise, you may not be able to use the hostname to log in. If this happens, see [page 81](#).

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 project. To keep your project, make sure you have backed it up (see [page 36](#)) before you reset the Box.

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

1. 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.
2. 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.*

3. 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.

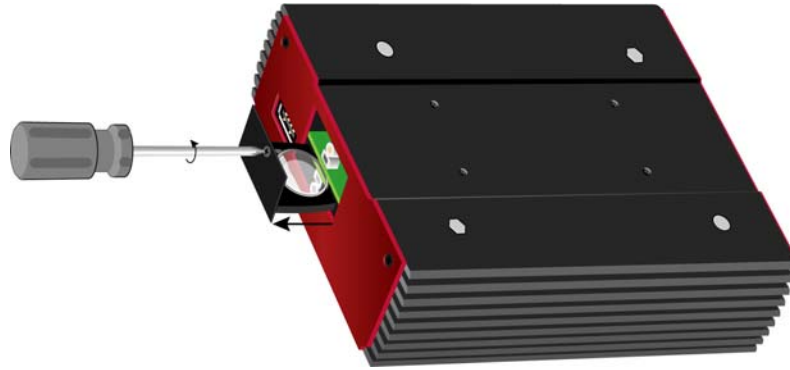
*NOTE: Always wait until the SYS LED has stopped blinking before you try to log into *groov*. Otherwise, you may not be able to use the hostname to log in. If this happens, see [page 81](#).*

4. 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`
5. Accept the security warnings. When *groov* opens, follow the onscreen instructions to create a *groov* Admin account. **Remember** your username and password!
6. When prompted, install your license.
7. Follow instructions to create a *groov* Build account. **Remember** this username and password, too; login information **cannot be recovered** if lost.
8. Click Go to *groov* Build. When Build opens, choose Help > Check for Updates. Log into `manage.groov.com` using your My.Opto22 credentials, and locate your Box in the list. Under details for the Box, click Show.
9. Download upgrades for both *groov* Admin and *groov* App, and install them (see [“Updating *groov* Admin” on page 39](#) and [“Updating *groov* App \(Build and View\)” on page 34](#)).

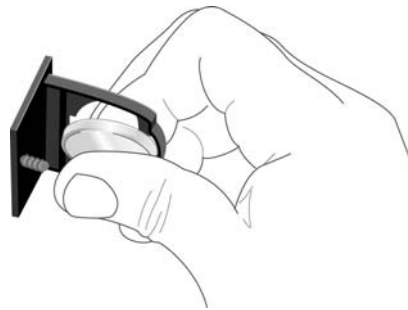
Replacing the battery

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.



- Using your fingers, pop out the old battery.



- 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 85](#).
- 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 *groov*. 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 and locate the IP address of the *groov* you want to log into. Log into *groov* using the 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 *groov* 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 89.)
- 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 *groov* 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.
- 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 [page 83](#).

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 (on the CD that came with the *groov* Box)
- to assign the static IP address to the Box. See “[Assigning a Static IP Address](#)” on [page 27](#).

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 *groov*. 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 (on the CD that came with the *groov* Box). See “[Open groov Admin using groov Find \(Windows only\)](#)” on [page 22](#).

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 *groov* 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* 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 29](#) to configure the ETH1 connection.
3. Now try configuring your tag server or controller again. This time *groov* 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* Build, choose [Configure > Devices and Tags](#) and locate your device in the list. Follow instructions in the [groov Build and 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 13). If power is OK, replace the battery (see page 80).



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:

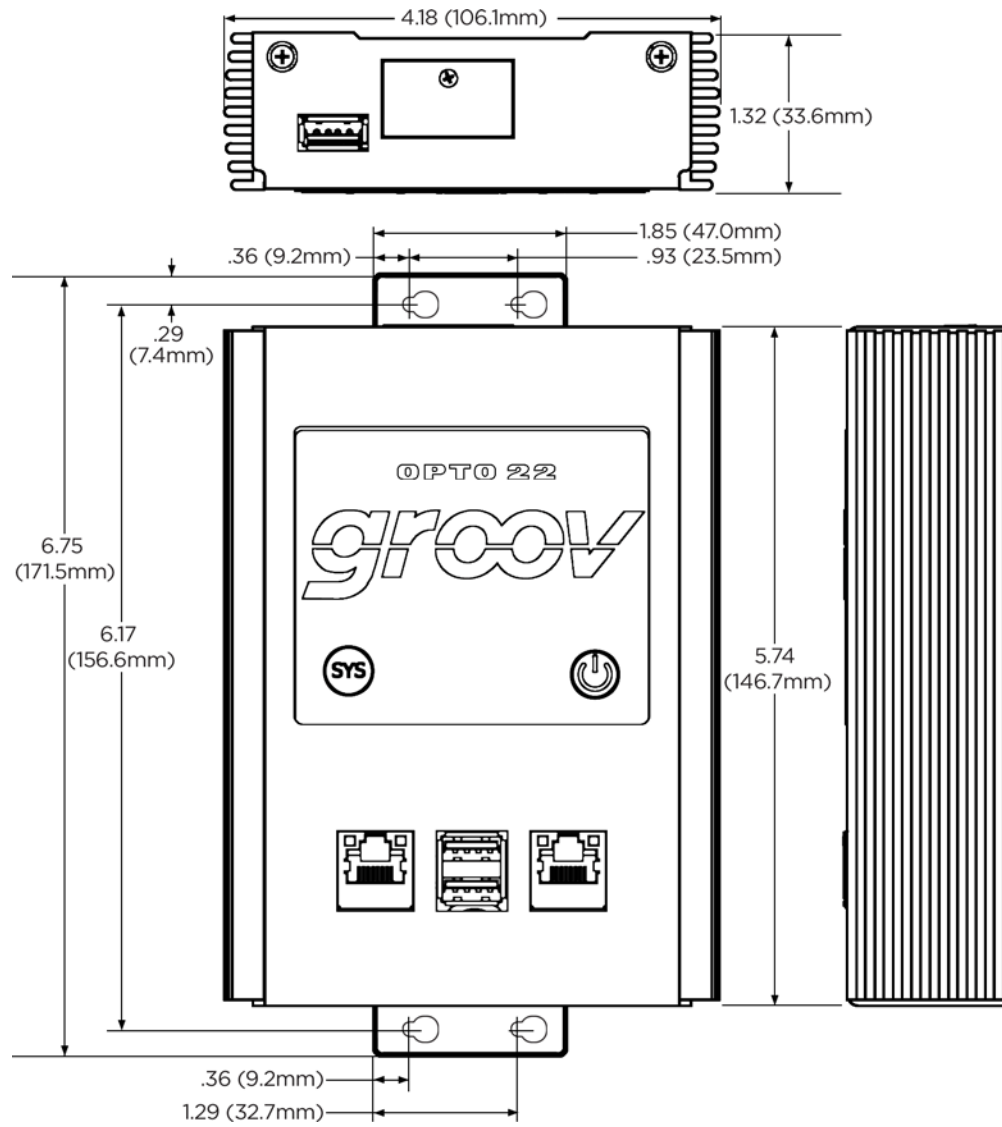
- [Node-RED website](#)
- Opto 22 developer website at developer.opto22.com
- [Opto 22 Node-RED forum](#)

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)
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 known as WPA Personal) WPA2 PSK (also known as 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



B: Connectors and LEDs

Connectors and Indicators



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

USB connectors. Can be used for:

- Backing up and restoring groov. See [“Backing Up groov” on page 36](#) and [“Restoring groov” on page 37](#).
- Connecting to serial devices using an FTDI USB-to-serial converter and Node-RED. See [“USB connectors for serial devices” on page 88](#) and [“Connecting with serial devices” on page 55](#).



Top

USB connector, used for:

- WiFi adapter. See Appendix C: Installing an Approved USB WiFi Adapter on page 91 and [“Configuring Wireless Communications” on page 30](#).
- Serial device. See [“USB connectors for serial devices” on page 88](#) and [“Connecting with serial devices” on page 55](#).

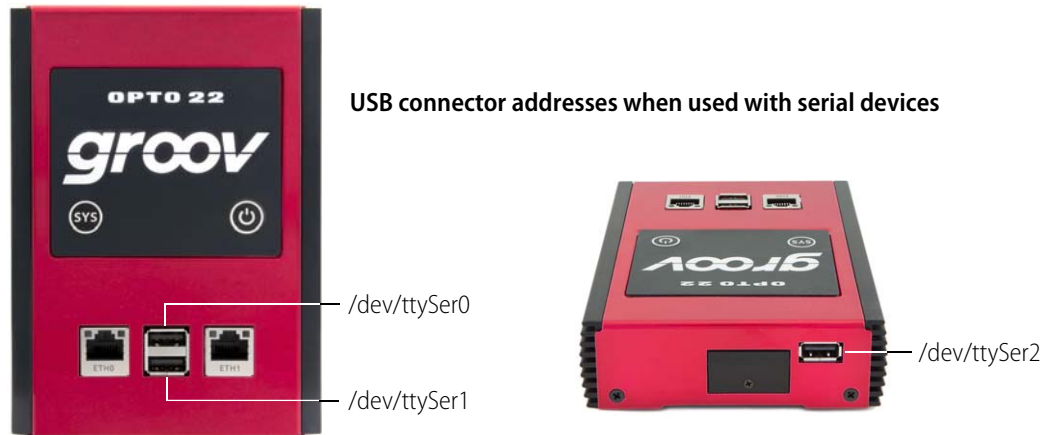


Bottom

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.

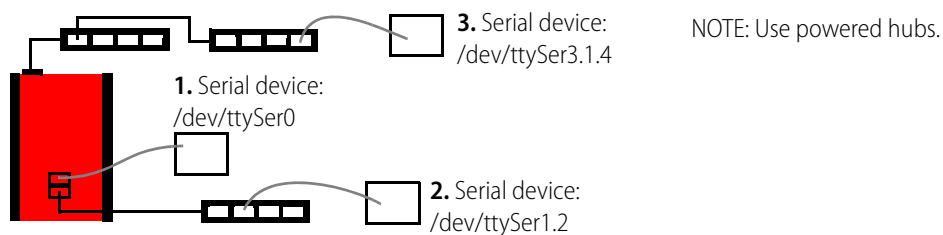


If you're using a USB hub, the address looks like this:

`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:



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.

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
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 84)
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 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 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 21](#).
5. Configure wireless communications as described on [page 30](#).



Index

A

- access point, wireless, 30
- activate groov Box, 15
- architecture, system, 5

B

- backing up
 - groov project, 36
 - Node-RED project, 61
- battery, replacing, 80
- browsers, 4, 9, 16, 24

C

- CCMP, 32
- certificate
 - CA-signed, 74
 - for Node-RED, 61
 - self-signed, 68
- changing
 - groov Admin password or username, 42
 - network configuration, 26
- Chrome, 24
- Client Options dialog, 29
- communications, 4
- connecting to groov, 13
 - troubleshooting, 82
- connecting to network, 13
- connection is reset error, 83
- connectors on the groov Box, 87
- control network, 5
- controller not found, 83
- credentials
 - uploading, downloading, 61

D

- data, Modbus, troubleshooting, 83
- debugging Node-RED project, 60
- default network settings, 80
- device not found, 83
- DHCP, 26, 80, 82
- DIN rail clip, 12
- DNS, 16, 26, 29, 82
- downloading Node-RED project, 61

E

- encryption, 31
- enterprise network, 5
- environmental requirements, 85
- error, connection is reset, 83
- Ethernet connectors, 4, 13, 80
- Ethernet interfaces, 87
- exporting
 - flow in Node-RED, 58
 - node, 58

F

- Find, 17
- Firefox, 24
- flow
 - exporting, 58
 - importing, 59
 - library, 59
 - uploading, downloading, 61
- function node, 50

G

- groov
 - backing up, 36
 - restoring project from backup, 37

- groov Admin
 - logging in, 83
 - opening, 21
 - quick start, 25
 - updating, 25
- groov Box
 - connecting to serial devices, 55
 - connectors, 87
 - LEDs, 89
 - power outage, 84
 - reset to factory defaults, 80
 - turn on/off, 79
- groov Build and View
 - opening from groov Admin, 26
 - updating, 34
- groov Find, 17, 22
- groov nodes, 47

H

- hardware status, 44
- help
 - Opto 22 Product Support, 7
 - Product Support, 7
- hostname
 - changing, 29
 - troubleshooting, 81, 82

I

- importing flow in Node-RED, 59
- installing
 - groov Box, 11
 - Node-RED nodes, 57
- Internet Explorer, 24
- IP address
 - DHCP server, 82
 - DNS, 82
 - static, 27
- IPv4 Gateway, 29

L

- LEDs
 - blink codes, 89
 - location, 89
- library in Node-RED, 59
- license file, 15

M

- memory, 85

- Modbus troubleshooting, 83
- mounting groov Box, 11

N

- network
 - configuring, 26
 - connecting, 13
 - control, 5
 - enterprise, 5
 - interface card (NIC), 82
 - key, 32
 - LEDs, 89
 - troubleshooting, 82
- node
 - exporting, 58
 - importing, 59
 - library, 59
- Node-RED, 47
 - backing up, 61
 - debugging, 60
 - editor, 48
 - exporting a flow, 58
 - function node, 50
 - groov nodes, 47
 - importing a flow, 59
 - installing nodes, 57
 - opening, 26, 48
 - Opto 22 SNAP PAC node, 47
 - Opto 22 SNAP PAC nodes, 52
 - restoring, 61
 - security certificates, 61
 - serial devices, 55, 88
 - updating, 40
- Node-RED Admin
 - opening from groov Admin, 26

O

- On/Off button, 79
- opening
 - groov Admin, 21
 - groov Build and View from groov Admin, 26
 - Node-RED, 48
- operating temperature, 85
- Opto 22 Product Support, contacting, 7

P

- password
 - changing, for groov Admin, 42

- power
 - connector, 87
 - outage, 84
 - red LED, 84
 - requirements, 13, 85
 - troubleshooting, 81
- private key, 77
- processor, 85
- project, groov
 - backing up, 36
 - restoring from backup, 37
- project, Node-RED
 - backing up, 61
 - restoring, 61

Q

- quick start
 - groov Admin, 25
 - Node-RED, 48

R

- replacing battery, 80
- resetting groov Box, 80
- restarting groov Box, 41
- restoring
 - groov project, 37
 - Node-RED project, 61
 - to older groov version, 36

S

- Safari, 24
- security
 - CA-signed certificate, 75
 - certificate, 61, 74
 - self-signed certificate, 68
 - warning, 17, 24
- self-signed certificate, 68
- serial devices
 - addresses for node, 88
 - connecting to groov Box, 55
- server, synchronize time with, 46
- session timer, 25
- setting system time, 45
- SNAP PAC node
 - security certificates, 61
 - using in Node-RED, 52
- SNAP PAC nodes, 47
- SoftAP, 33

- specifications, 85
- SSID, 31
- SSL certificate, 74
 - buying CA-signed, 75
 - using in Node-RED, 61
- static IP address, 16
 - assigning, 27
- storage temperature, 85
- synchronize time with remote server, 46
- SYS LED, 89
- system
 - architecture, 5
 - information, 25, 43, 48
 - time, setting, 45

T

- Technical Support. *See* Opto 22 Product Support, 7
- temperature and humidity, 85
- time
 - server, 45
 - setting, 45
 - zones, 45
- TKIP, 31
- troubleshooting
 - cannot connect to groov, 82
 - device or controller not found, 83
 - DNS (domain name server), 82
 - hostname, 81
 - Modbus device or data, 83
 - Opto 22 Product Support, 7
 - power, 81
 - red power LED, 84

U

- updating
 - groov Admin, 39
 - groov App, 34
 - Node-RED, 40
- uploading Node-RED project, 61
- USB connectors, 87
 - serial device addresses, 88
- USB flash drive
 - back up to, 36
 - restore from, 37
- username, changing, for groov Admin, 42

V

- version, restoring to older groov version, 36

W

WEP, 31

wired network, 4

wireless

access point, 30

communications, 30

LAN, 4

specifications, 85

WPA, 31