GROOV BOX USER'S GUIDE FOR GROOV-AT1[Obsolete]

GROOV BOX USER'S GUIDE FOR GROOV-AT1

OPTO 22

Automation made simple.

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

This product is obsolete.

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.

groov Box

groov View

Internet

Opto 22 SNAP PAC controller

groov Server for Windows

groov Build

Assets

Another company's automation system

OPC-UA tag server (only needed if using another company's automation system)
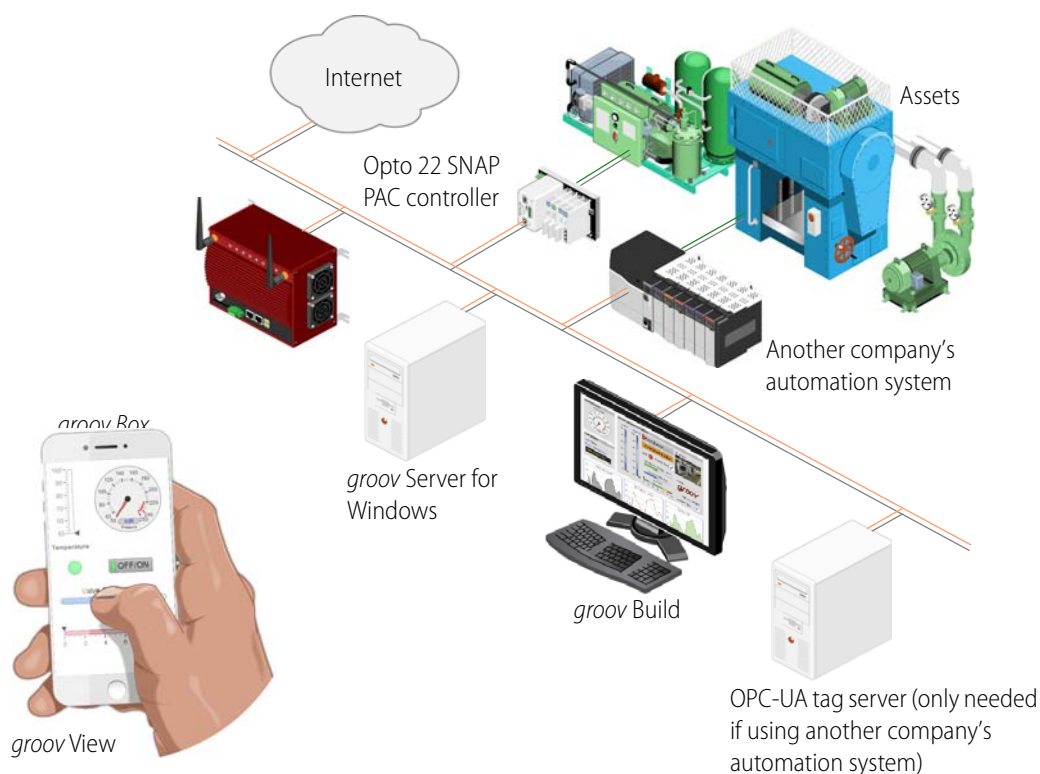
Choose Your *groov*

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

groov Box 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. The *groov* Box communicates over a standard Ethernet network or wireless LAN (local area network), or both.

groov Server for Windows 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. For more information on *groov* Server, see form 2078, the *groov Server for Windows User's Guide*.

Whether you store and serve *groov* software on a *groov* Box or on a computer using *groov* Server for Windows, an operator interface you develop with *groov* can be viewed on almost any mobile device or computer.

About this Guide

NOTE: The GROOV-AT1 is OBSOLETE and no longer available.

This user's guide shows you how to install and set up your *groov* Box, part number **GROOV-AT1**. (If your groov Box is the newer model with part number GROOV-AR1, see form 2104, the *groov Box User's Guide for GROOV-AR1*, instead of this guide.)

This guide also shows you how to use the *groov* Admin software. *groov* Admin provides the tools to update *groov*, set up wired and wireless networking, and more.

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

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

- Any computer with a modern web browser. This does not have to be a Windows PC.
- One or more of the following:

– A Modbus device that communicates over Ethernet

– An Opto 22 SNAP PAC System (SNAP PAC S-series, R-series, with firmware R9.2a or newer or SoftPAC, running a PAC Control strategy)

– Any OPC UA-compatible automation system or equipment, plus an OPC UA server and drivers for your equipment.

groov and KEPServerEX: If you are building a *groov* interface for an OPC UA-compatible system and don't already have an OPC UA server installed, the KEPServerEX communication platform from Kepware Technologies is recommended by Opto 22 and tested to work with *groov*. For more information, see www.kepware.com/Products/products_OPCServers.asp and www.kepware.com/Support_Center/doc_auto_tag.asp

A Note on Browsers

Thanks to technologies such as HTML5, SVG, and CSS3, web browsers are now fairly similar. Our browser-based *groov* View and *groov* Build work reliably on a large number of device/OS/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 .

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 or over an 802.11b, g, or n wireless LAN (local area network), or over both.

With two independent wired Ethernet network interfaces plus an 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.

This product is obsolete.

Wireless antenna

Ethernet connectors

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 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, a VPN (Virtual Private Network) connection is recommended for security. The HTTPS (HTTP plus TLS/SSL) in your browser shows that all data exchanged between your browser and *groov* is encrypted.

Assets

Modbus/TCP devices and controllers from multiple manufacturers

OPC UA server (Only needed if using another company's automation system. Not needed for Opto 22 or Modbus/TCP devices.)

SNAP PAC controller

groov Box

Enterprise Network

Control Network

Internet

PC running *groov* View in a web browser

VPN server

Smartphone with *groov* View

Assets

Control systems from other manufacturers

OPC UA server

SNAP PAC controller is recommended for running the PAC Control strategy and managing assets

groov Box

Enterprise Network

Control Network

Internet

PC running *groov* View in a modern browser

VPN server

Smartphone with View

This product is obsolete.

This product is obsolete

What's In This Guide

Here's what is in this user's guide:

Chapter 1: Welcome 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 5: Using an SSL Certificate describes using an SSL certificate that is digitally signed either by a certificate authority (CA) or self-signed.

Chapter 5: Maintenance and Troubleshooting provides troubleshooting information and answers questions you might have about *groov*.

Appendix A: Specifications and Dimensions provides technical specifications and *groov* Box dimensions.

Appendix B: Connectors, Indicators, and LEDs describes connector names and what the status and activity LEDs mean.

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
Fax:	951-695-3017
Email:	support@opto22.com
Opto 22 website:	www.opto22.com

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

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

- *groov* version and *groov* Admin version. Click the System Information icon (see).
- A description of your system equipment:
    - Computer type, speed, memory, and operating system
    - If used, Modbus/TCP device manufacturer and model
    - If used, SNAP PAC controller model and firmware version
    - If used, OPC UA server type and configuration
- A description of the network
- Specific error messages or other diagnostic indications

2: Getting Started

In this chapter you'll find instructions on how to install the *groov* Box and set up the *groov* Admin software.

In this chapter:

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. For the best experience, we recommend Chrome, Firefox, or Internet Explorer 10 or newer.

In the Box

These items are included in the box:

- *groov Quick Start*, form 2063
- *groov* Box
- 2 extra fan filters
- *groov* Box wireless antennas

This product is obsolete.

- *groov* CD that includes the *groov User's Guide* (form 2027), the *groov Quick Start* (form 2063), *groov Box User's Guide* (form 2077), and the *groov* Find utility
- Ethernet cable
- Power supply unit
- Activation key certificate

Antennas
(attach before use)

CD

Spare fan filters

***groov* Box**

Ethernet cable

Power supply

Activation key certificate
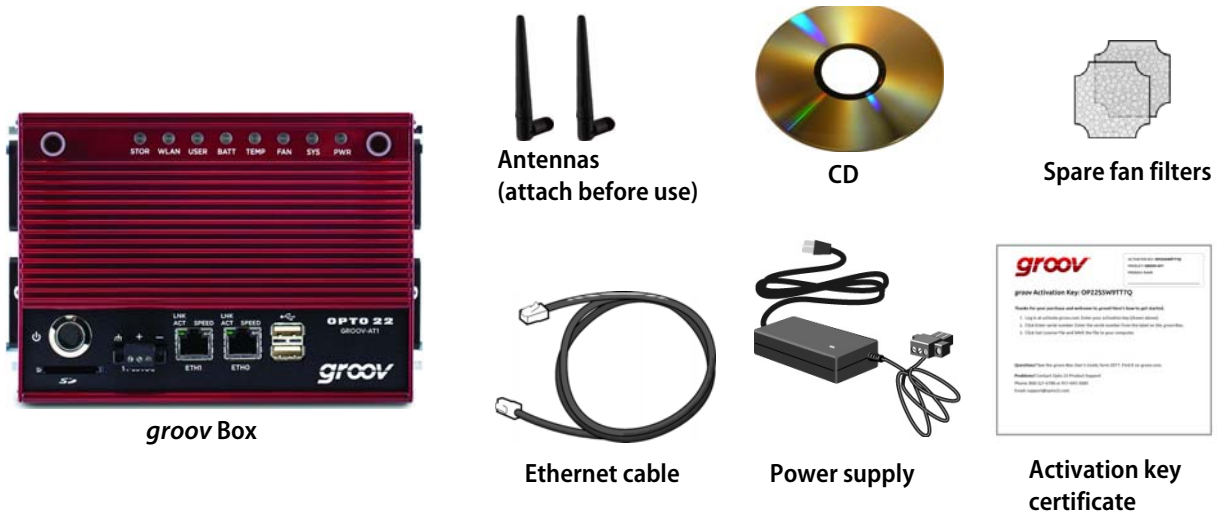
Step 1: Get To Know the *groov* Box

To set up the *groov* Box, you'll use the *groov* Box components shown below. Make sure to peel the label from the Activation Key certificate and affix it to the top of the *groov* Box.

Affix the Activation Key label here.

LEDs

Airflow

Mounting tab

On/Off button

Power terminal

ETH0

Step 2: Choose a Location

Locate a suitable wall or panel near a standard 120VAC or 240VAC wall outlet and the wired Ethernet network(s) your computer is on. If your controller, Modbus/TCP device, or OPC UA server is on a different network than your computer, connect ETH0 to your computer's network and ETH1 to the other network. (Also see page 63.)

Allow room around the front, top, and sides of the *groov* Box. Air needs to flow freely though the fans on the sides, and you need to be able to see the information on the top.

Step 3: Mount the *groov* Box

You can mount the *groov* Box on a flat surface using the four mounting tabs, or you can mount it on a DIN rail using the DIN rail clips provided on the back of the *groov* Box. Use #8 screws with the mounting tabs. If there will be vibration at the *groov* Box installation site, make sure to use the mounting tabs for a secure installation.

Method 1:
Mount to a flat surface using the mounting tabs

Method 2:
Mount to a DIN rail
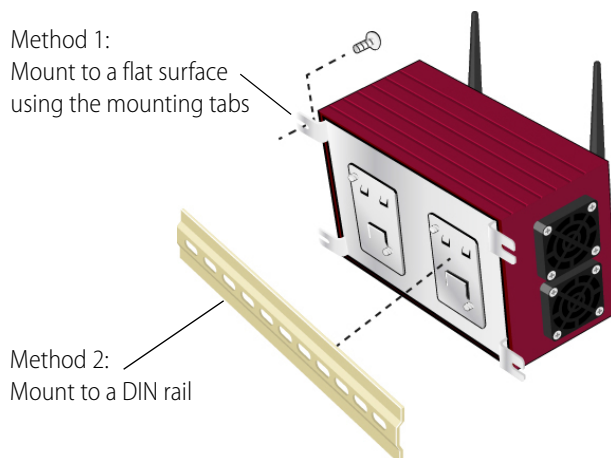
Step 4: Connect to the Network

ETH1 to control network

ETH0 to computer network

ETH1 to control network
(if on a separate subnet)

ETH0 to computer 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. See "Troubleshooting" on page 61.

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 controller, ModbusTCP device, or OPC UA server is on a different network than your computer, connect ETH0 to your computer's network and ETH1 to the other network.

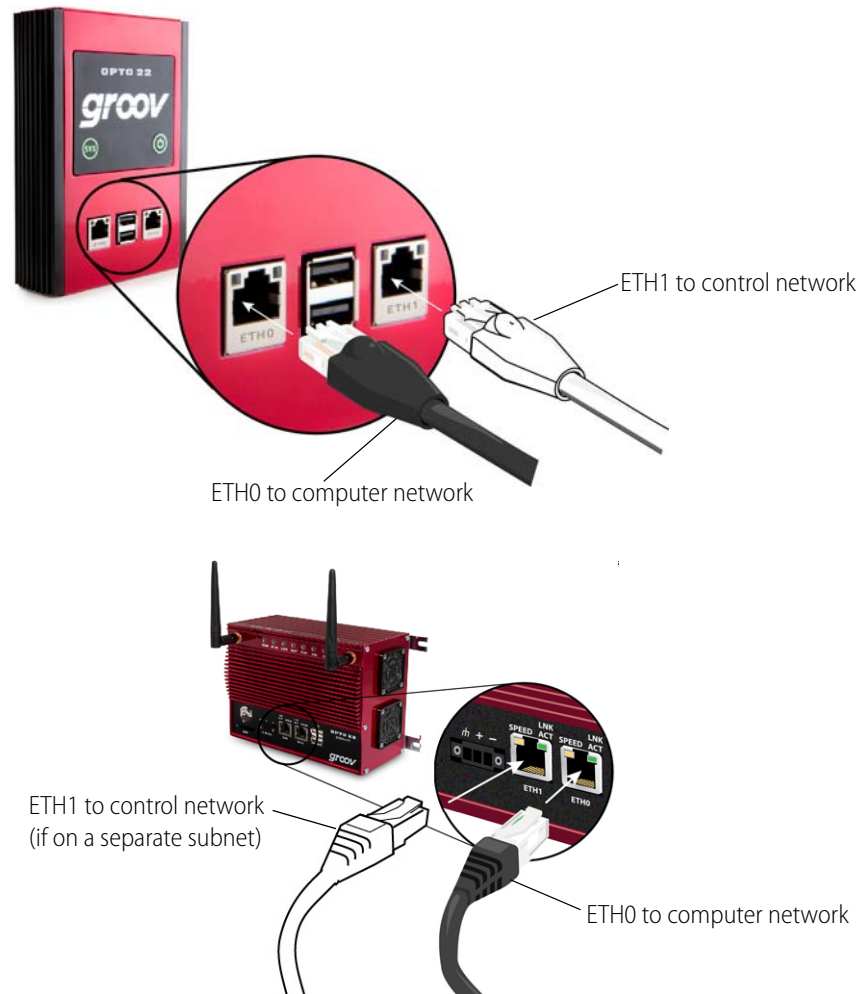If you are using both ETH0 and ETH1, make sure they have IP addresses on different subnets. In some situations, this may require configuring a static IP address. Otherwise there may be communication errors. For more information, see "Assigning a Static IP Address" on page 25.

For detailed information on setting up your network and setting up communications over the Internet, see form 1796, the *Guide to Networking Opto 22 Products*.

Step 5: Connect the Power Supply

Your *groov* Box requires a power supply with an output of 14-36 VDC, 24 VDC @ 1 amp. 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 terminal marked 14–36 VDC, tighten the screws. Plug the other end into a standard 120 or 240 VAC outlet. The LED marked PWR will light solid green.
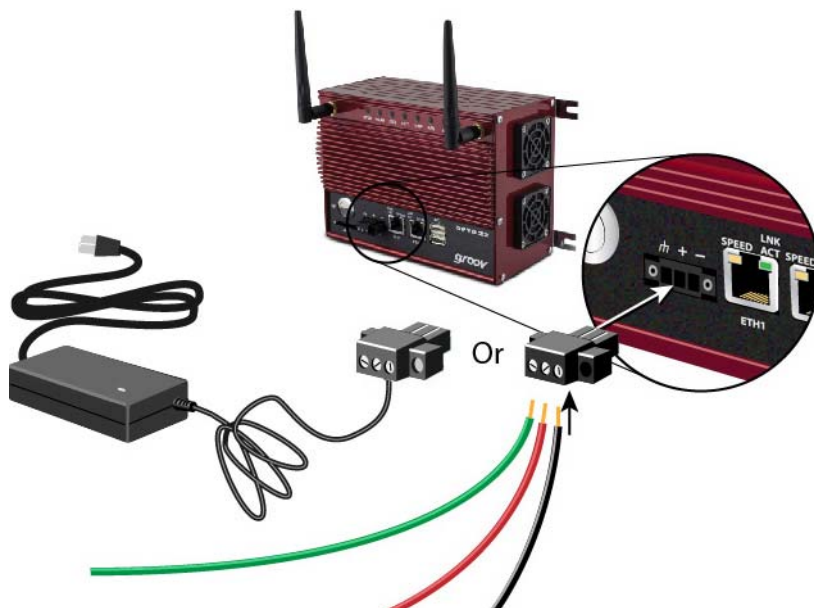
If you are using your own power supply, do the following:

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. Connect a lead from a known earth/chassis ground to the (ground) terminal on the power connector.

Step 6: Turn on the *groov* Box

Briefly press and release the On/Off button. **Wait** until the SYS LED has stopped blinking and is solid green. Also, 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 .

Step 7: Activate the *groov* Box and Get the License File

You'll need the activation key printed on the certificate included with your *groov* Box.

a. Open a web browser (Firefox or Chrome recommended). Go to activate.groov.com.
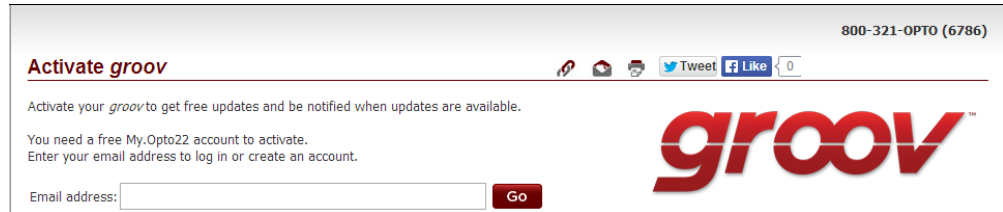
b. Log in using your email address and your My.Opto22 password.

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.

When asked to enter the serial number, you'll find it on the label on the top of the device.

Serial number

Step 8: Open *groov*

You can open *groov* using just your web browser. Or, if you have a Windows computer, you can use *groov* Find (see below). If your network does not have DNS, use *groov* Find.

Using your web browser:

a. On your computer, open Firefox or Chrome, or Internet Explorer 10 or newer.

b. Enter https:// and your *groov* Box's hostname as the URL. The hostname is printed on top of the *groov* Box.

For example, if the hostname is opto-01-ab-c2, you type

`https://opto-01-ab-c2`

Default hostname

Make sure you type http**s**. The **s** indicates it is a secure connection.

NOTE: If you've assigned a static IP address to the groov Box, use the IP address instead of the hostname to open groov.

c. Accept the security warning. Your *groov* data is protected by the Secure Socket Layer 256-bit encryption, so you can safely accept the warning.

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: Click "Continue to this website (not recommended)."

For Safari: Click Continue.

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

Using *groov* Find:

If you are using a Windows computer, you can use *groov* Find to locate the *groov* Boxes on your network. If your network does not have DNS, you must use *groov* Find.

a. Insert the *groov* CD in your CD-ROM drive, then click the link to copy the Find application file to your computer.

b. Open the Find application file.

This product is obsolete.

A message might 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 top of the *groov* Box.

Serial number

d. Locate the matching serial number in Find.
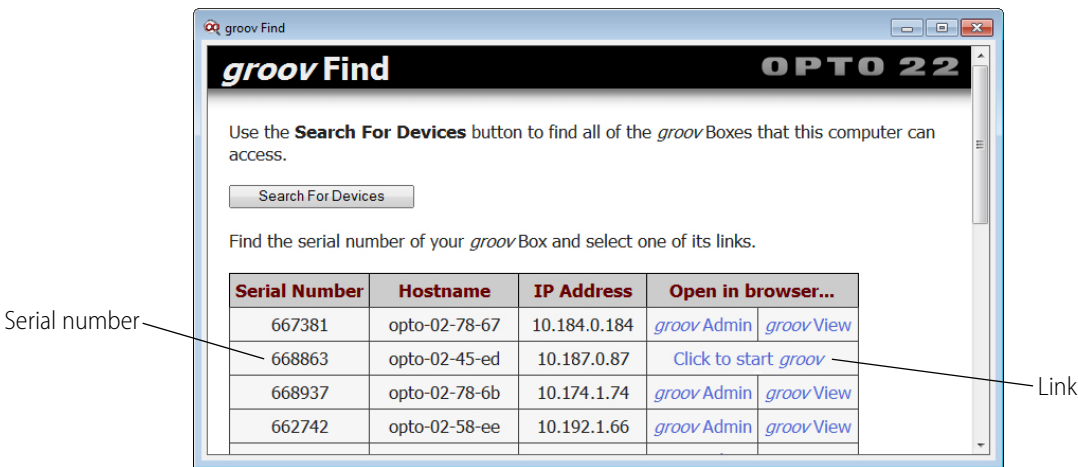
Serial number

Link

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

e. Click the link "Click to start *groov*."

When your browser connects to *groov* for the first time, the browser will display a security warning.

f. Accept the security warning. Your *groov* data is protected by the Secure Socket Layer 256-bit encryption, so you can safely accept the warning.

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)."
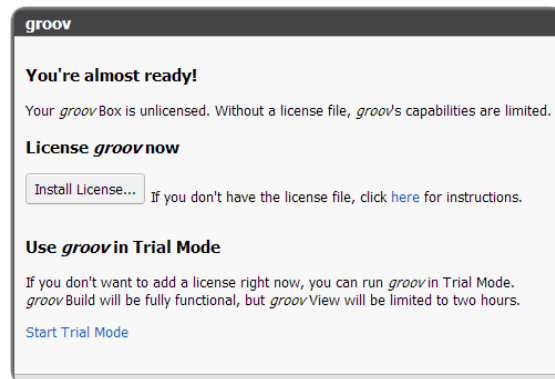
For Safari: Click Continue.

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

Step 9: 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.

groov

You're almost ready!

Your *groov* Box is unlicensed. Without a license file, *groov*'s capabilities are limited.

License *groov* now

Install License... If you don't have the license file, click here for instructions.

Use *groov* in Trial Mode

If you don't want to add a license right now, you can run *groov* in Trial Mode. *groov* Build will be fully functional, but *groov* View will be limited to two hours.

Start Trial Mode

b. Browse to the license file, then click Open.

Step 10: Create New Usernames and Passwords

Follow the on-screen instructions to create usernames and passwords for *groov* Admin and for *groov* Build. If the security warning appears once more, accept the warning again.

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.*

After you have completed the instructions in **welcome to *groov***, *groov* Build opens in your web browser. For information on using *groov* Build, see form 2027, the *groov User's Guide*.

This product is obsolete.
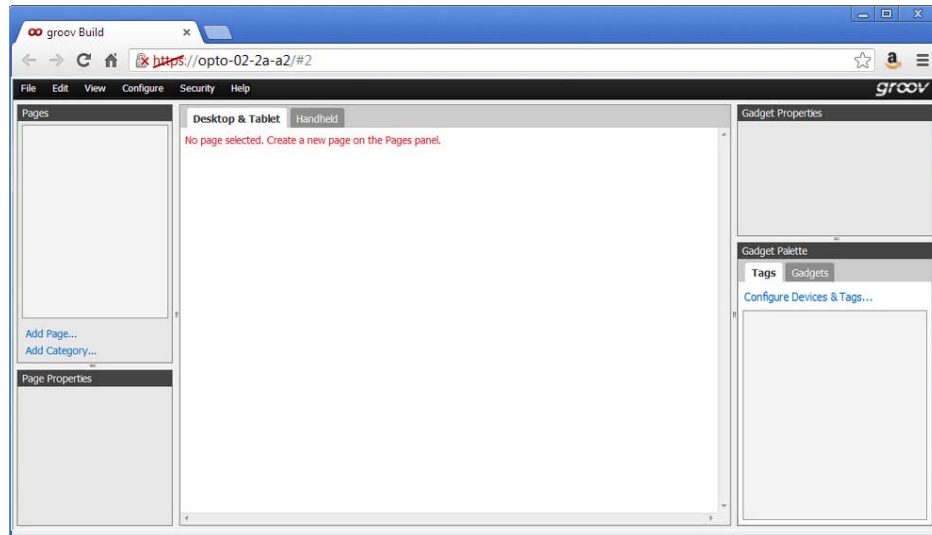
3: Using *groov* Admin

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 *groov* Admin

You can open *groov* Admin in three ways:

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

Open *groov* Admin from *groov* Build

In *groov* Build, choose Configure > *groov* Admin. To log in, see .

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

Hostname

2. When groov Admin opens, log in (see).

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 25.) 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.

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

Serial number

3. Locate the matching serial number in Find.

Serial number
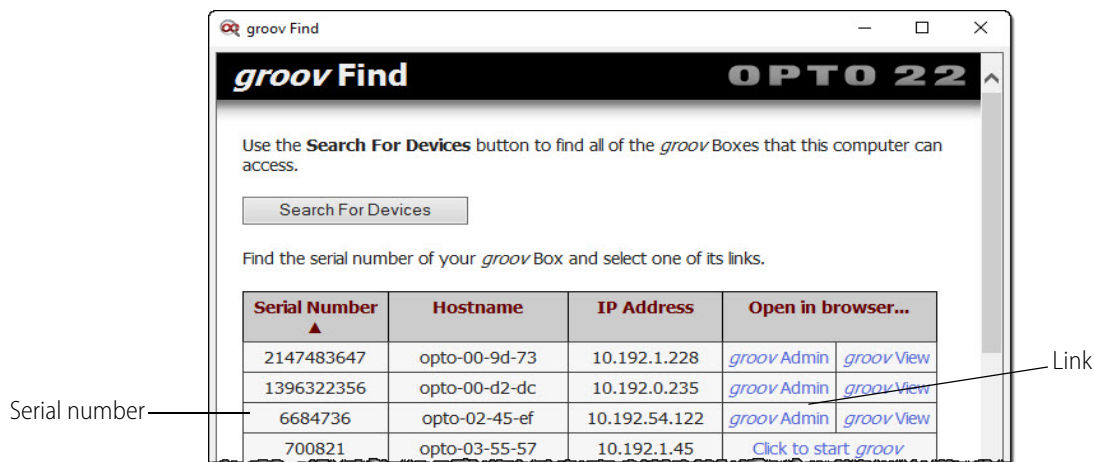
Link

4. 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 22).

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 48.

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 54.

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.*

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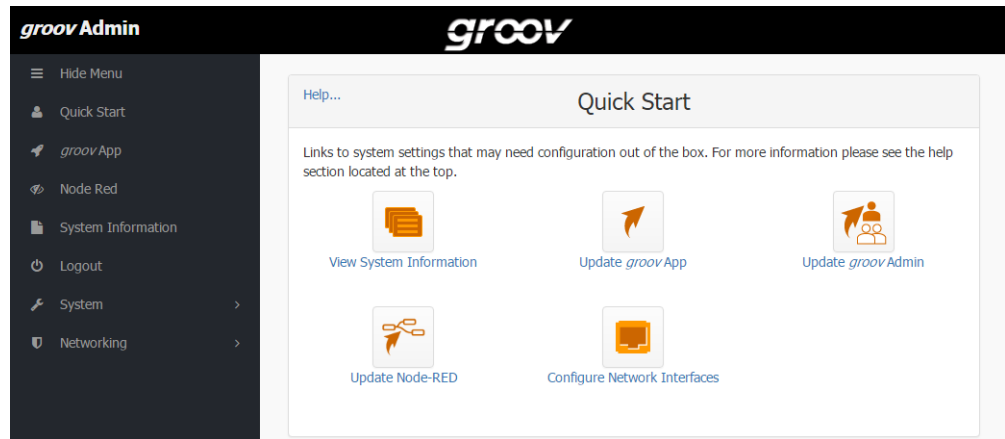
The quick start buttons take you directly to some of the more common actions in *groov* Admin.

View System Information
Check system information and see usage statistics. "Checking System Information" on page 41.

Update *groov* App
Update *groov* Build and View. See "Updating groov App (Build and View)" on page 31.

Update *groov* Admin
Update *groov* Admin itself with the latest version. See "Updating groov Admin" on page 36.

Update Node-RED
Update Node-RED software running on the groov Box. See "Updating Node-RED" on page 37.

Configure Network Interfaces
Configure IP settings for the wired and optional wireless Ethernet interfaces: ETH0, ETH1, and WLAN0. See "Configuring Network Connections" on page 24.

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

This product is obsolete.

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

To go to *groov* View or *groov* Build, in the left navigation bar, click *groov* App.
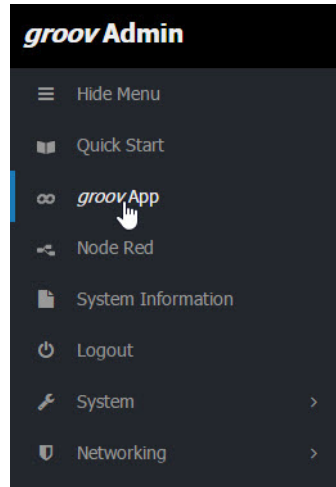
Your *groov* project opens in *groov* View. To get to *groov* Build, in View click the gear icon in the upper right and choose Switch to *groov* Build.

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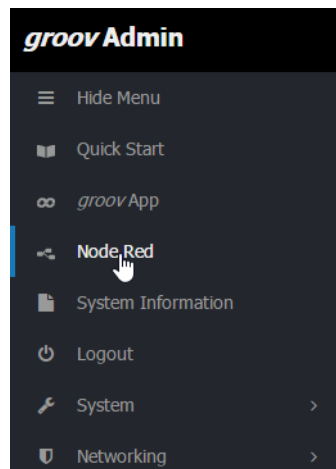
Node-RED Admin opens. You'll need to log in; use your groov Admin username and password.

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:

-
-
-
-

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.
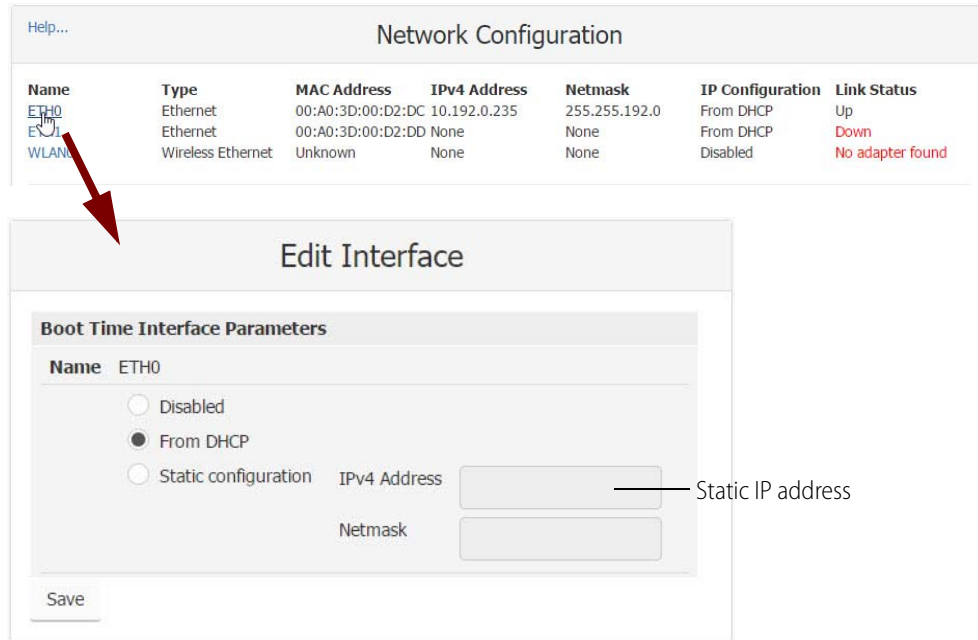

OR:

Configure Network Interfaces
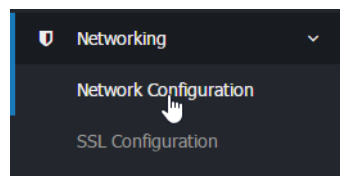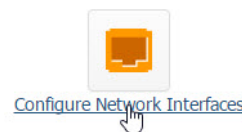
2. Click the wired Ethernet connection you want to configure.

   NOTE: Use ETH0 as the main network connection. Only use ETH1 if you have segmented networks.
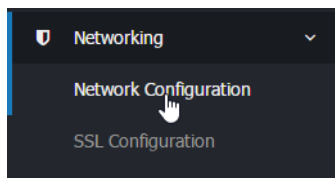
3. Select Static configuration. Enter the static IP Address and Netmask.

4. Click Save.

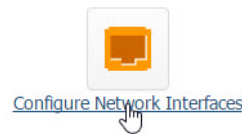## Changing the Hostname, DNS Servers, or IPv4 Gateway

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.

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

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

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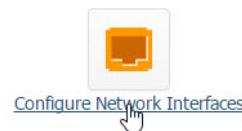
3. Click Save.

Configuring ETH1 for the Control Network

If your computer is on a different network than the control network, you need to configure ETH1 by assigning it an IP address and subnet appropriate for the control network.
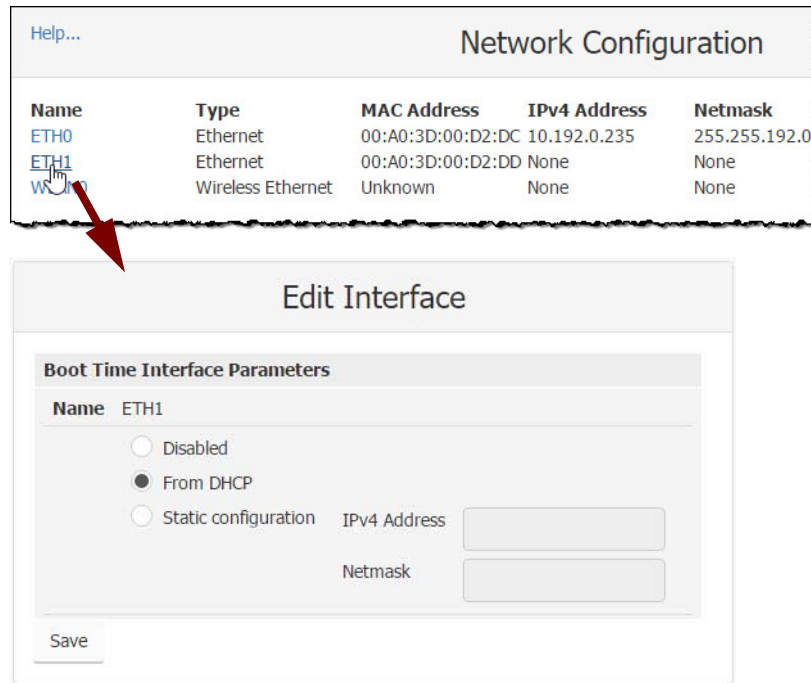
1. In the left navigation bar choose Networking > Network Configuration, or click the Configure Network Interfaces button in Quick Start.

OR:
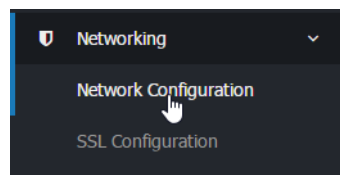
2. Click ETH1.

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

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

4. Click Save.

Configuring Wireless Communications

You can configure the *groov* Box to connect to a wireless network through an access point using the 802.11b, 802.11g, and 802.11n protocols.
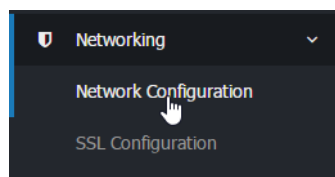
Before you begin, get the following information from your IT Department:

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

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

Password—To access the wireless network

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

OR:

2. Click WLAN0.

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.

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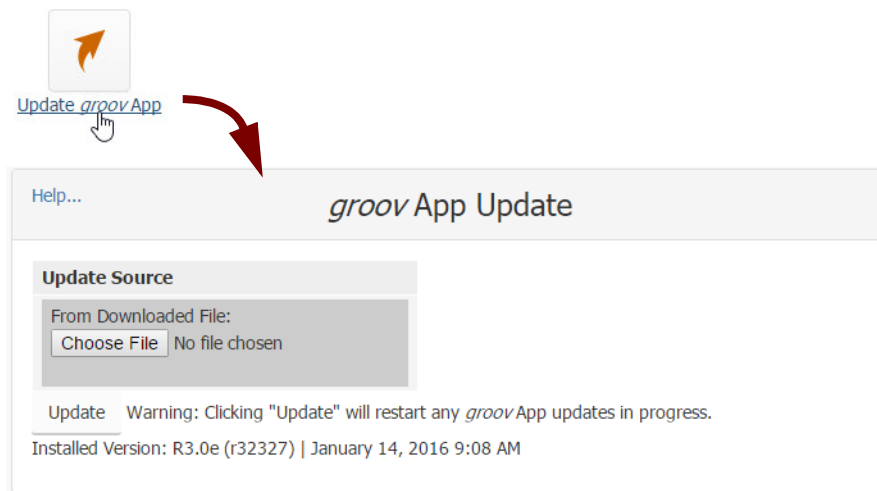
a. In the Network Configuration page, click ETH0.

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).

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

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 32).

2. Make sure the *groov* Box is activated. See "Step 7: Activate the groov Box and Get the License File" on page 14.

3. Go to manage.groov.com and follow directions to download the latest groovApp update file and save it to your computer.

4. Open *groov* Admin.

5. Click Quick Start and then the Update *groov* App button.

Update *groov* App

groov App Update

Update Source

From Downloaded File:
Choose File | No file chosen

Update   Warning: Clicking "Update" will restart any *groov* App updates in progress.
Installed Version: R3.0e (r32327) | January 14, 2016 9:08 AM

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.

Module Index   *groov* App Update

Executing Update...

✓ Update from version R3.0e (r32327) | January 14, 2016
9:08 AM to version R3.1a (r33692) | March 09, 2016 5:37
PM successful.

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.

USB connectors for backing up and restoring using a flash drive

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 34.

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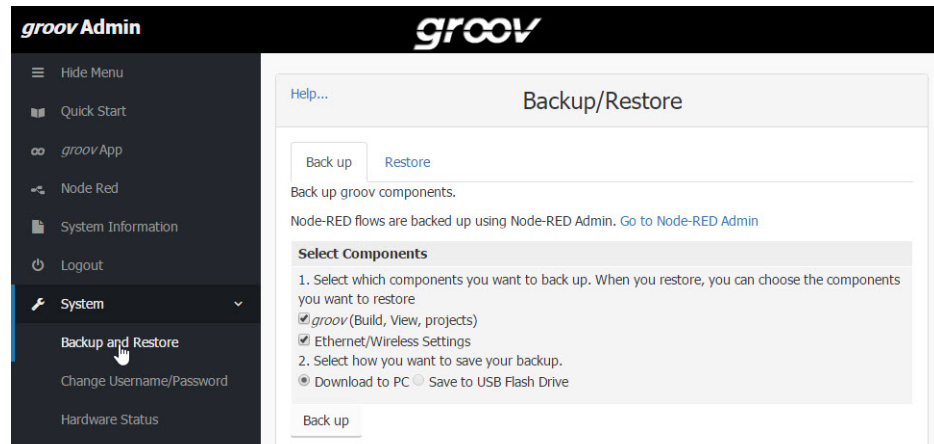
Also, be aware that if you send project files to Opto 22, our personnel will have access to the information listed above.

Follow these steps to back up groov:

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

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.
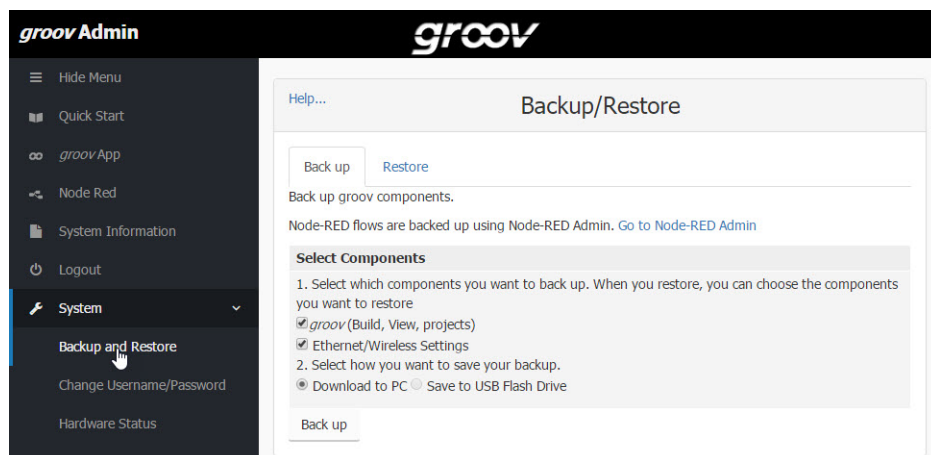

USB connectors for backing up and restoring

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.
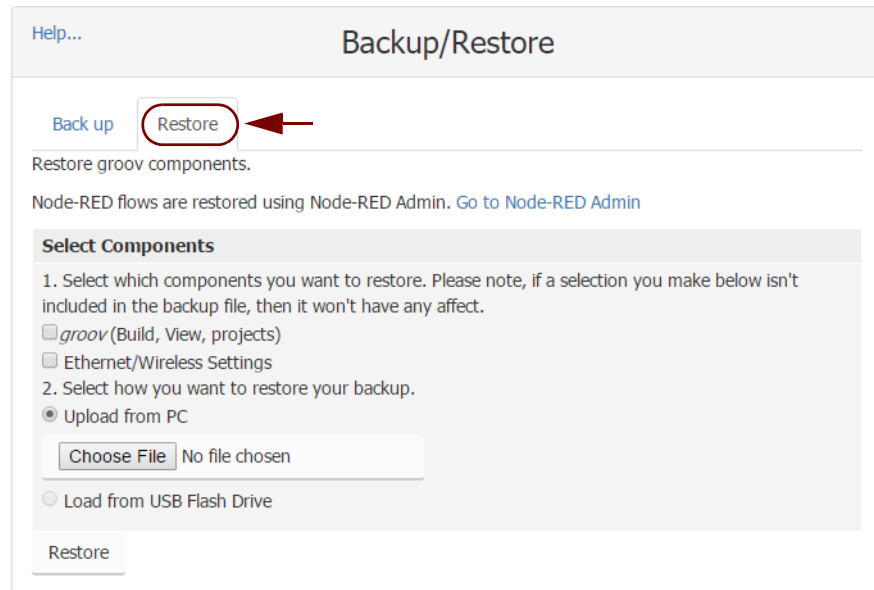
Restoring *groov*

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 32).

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,

This product is obsolete.

refresh the page.) Click Load from USB Flash Drive, then click the browse button and select your backup file.

USB connectors for backing up and restoring

**5.** 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.

1. Go to manage.groov.com and follow directions to download and save the latest *groov* Admin update file to your computer.

IMPORTANT: If you have a GROOV-AT1 or GROOV-AT1-SNAP groov Box running groov Admin R1.570.40 or lower, first download and install groov Admin version R1.570.41. After you install 41, you can download and install the most recent version.

2. If the Quick Start menu is not open, in the left navigation bar, click Quick Start.
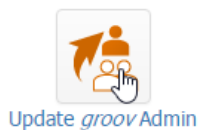
Update *groov* Admin

3. Click Update *groov* Admin.
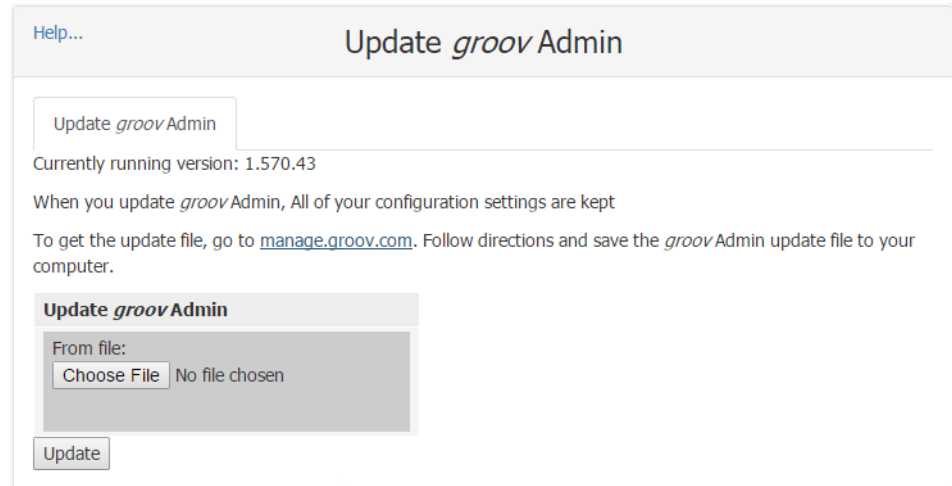
4. Click Choose File and locate the update file you downloaded. Highlight the file, and click Open.

5. 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:

   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.

6. 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

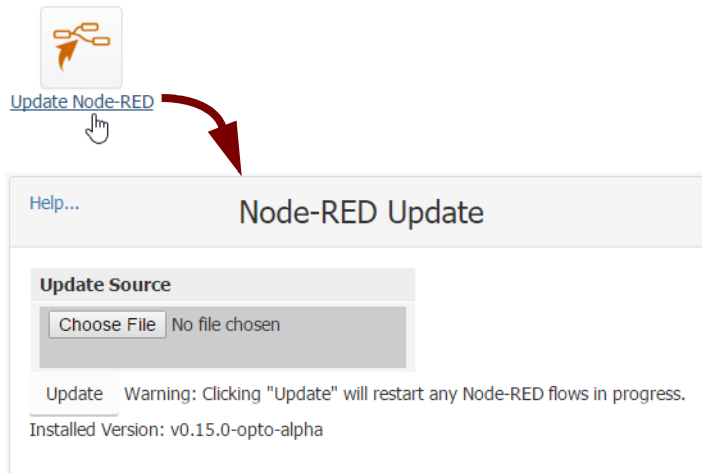1. Before updating, back up your Node-RED project using Node-RED Admin (see "Backing up and restoring your Node-RED project" on page 61).

2. Log into manage.groov.com and follow directions to download and save the latest Node-RED update file to your computer.

3. Open *groov* Admin.

4. Click Quick Start and then the Update Node-RED button.

5. 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.

6. 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."

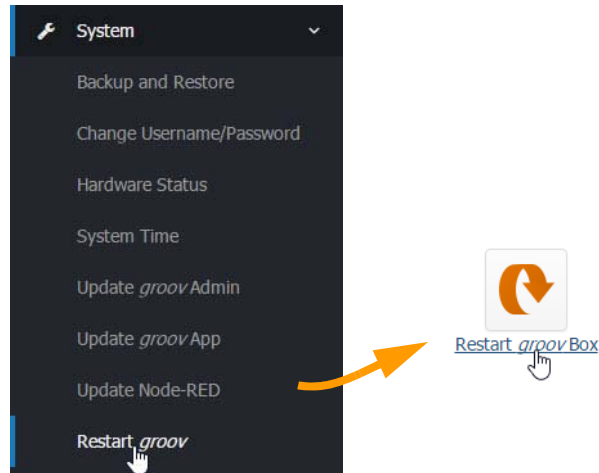- **In the left navigation bar**, choose System > Restart *groov* and then click the Restart *groov* Box button.

- **If you've updated but not restarted** the Box, click System Information, and then click "Click here to restart now."
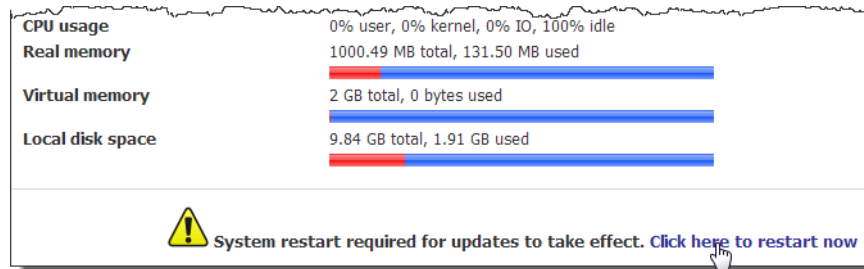
- **Hardware restart:** Press the On/Off button briefly and wait for the *groov* Box to turn off. Then briefly press the On/Off button again to power it back up.

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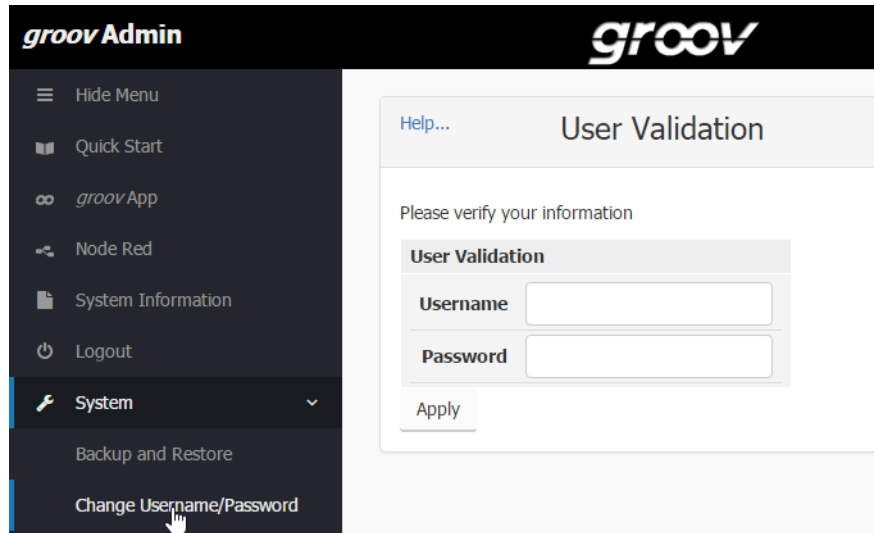
2. Enter your current username and password to verify your identity, and click Apply.

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.

☰ Hide Menu	
📖 Quick Start	
∞ *groov* App	OR
⚡ Node Red	
📄 System Information	View System Information
⏻ Logout	
🔧 System ›	
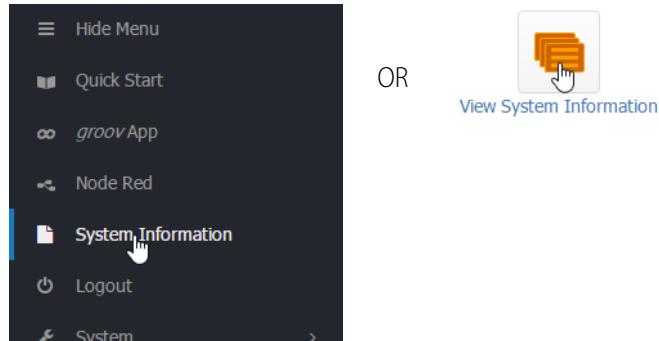
The following information is provided.

System Information

System Hostname	opto-02-80-b2.opto22.com
Activation key	VMM9KGWR7B3Q
groov **Serial Number**	668880
groov **Part Number**	GROOV-AT1
groov **Image Version**	45
groov **Admin Version**	1.570.43
groov **App Version**	R2.1c (r19913)	March 17, 2014 4:12 PM
Hardware Date	September 1, 2011
Time on System	Wed Mar 30 16:31:12 2016
System Uptime	0 hours, 10 minutes
CPU Load Averages	0.02 (1 min) 0.17 (5 mins) 0.16 (15 mins)
CPU Usage	0% user, 0% kernel, 0% IO, 100% idle
Real Memory	997.29 MB total, 84.04 MB used
Local Disk Space	19.69 GB total, 3.84 GB used

OPTO 22
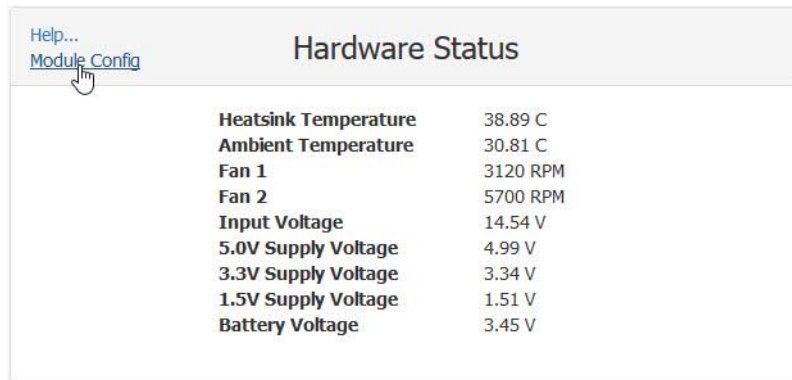
Checking Hardware Status

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

🔧 System ⌄
Backup and Restore
Change Username/Password
Hardware Status
System Time
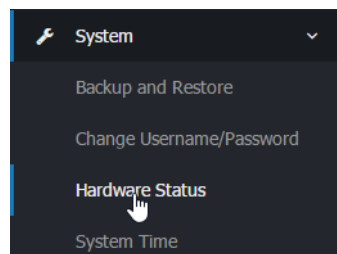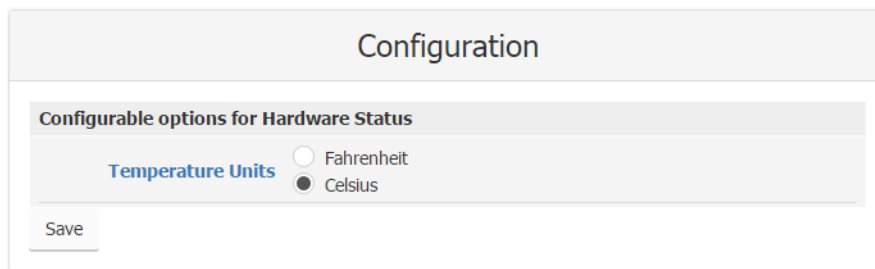
The following information is provided:

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

3. Select either Fahrenheit or Celsius.

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.

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.

This product is obsolete.

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 *groovs* 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 *groovs*, or the set of browsers that will access *groovs* 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 *groov* administrator has demonstrated the validity of the certificate (e.g. by providing the certificate thumbprints).	Trusted by those who trust the *groov* 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 32 for instructions. Certificates can be tricky, and you want to make sure you can recover if needed.*

After you've backed up your groov 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.
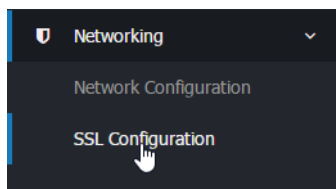
2. Click the Create certificate tab.

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 26.) 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 26.) 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-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDRPRqlSuifghET
BeRA0sykgyXxjqK5qGXT4qmNL5npsZhSyM6nlxCyf+wZuiJi2Ct4h+dC+g4lRLKu
Qt9ESDm+3Sn9qCSDGIdKf+OVRUU6eCT2whAqwSx258Uox66ZkbZsykxkMXpftq9m
V5+jAumrEW3irEV3pGb0mUgbhsdH+C94fdKv5qiYQ3YII073VgzLOTowOwPHcYy+
j9XF2k7Uhxul1kwEjXWZ0NRdBYZdvybAOgsu/0Fwmi+Fwtpy4Non00WJxXAuci8b

JUp8gxyeHuRgxeuIT766QJhVKX9eNJFYg2eeBGG2y7odHVBR3K/TfNvaOSqJR8T2
mDeAuCsnlSoYhb6NF6Yy8hmNPwuEokJv1XCcTYd0OQKEgFgJrwSLNWbgPgYLlndL
SH3ldhVAG014MiuZEIMM6yYly0v1Syiywnf3SY2u8M4PK/IL7UtSJ37PZdg0SLeV
IN+EEMBclnVLR4CcC+Z0QI7XnTsUCqY3ddKLuHvoE3GkbyP7Wss5KVeLqb1vE7iX
ehoT2RtfQ7OiOmri9Kwh38XE
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIEBTCCAu2gAwIBAgIJAKrj5zQwh5MFMA0GCSqGSIb3DQEBCwUAMIGYMQswCQYD
VQQGEwJVUzELMAkGA1UECAwCQ0ExETAPBgNVBAcMCFR1bWVjdWxhMSEwHwYDVQQK
DBhPUFRPIDIyIG9uIG9wdG8tMDAtZDItZGMxDDAKBgNVBAsMA0VuZ2ENMBQGA1UE
Aww9NT1yLjE2OC4wLjEwNDEgMB4GCSqGSIb3DQEJARYRZHRjYXJyQG9wdHA=Mi5j

AQsFAAOCAQEAEs7qtKZsgKLD1zqYq2kNfpA/slg6QWeKUuelnK+75R1mCYyo+YKV
MgIvvaykfOCQaz8S9s+hsrvW8jCNj6cvPn0EWIWSy4+Z0HvhmE/LFwJZNR8//G/B
Zd5XF/FoTx0ee6AHTNOi6AoRSsZRN+9vUTIsaFwAO4av9baGgsk28SDOKd1Gal6x
LPBwVVXZlHkHDsKOTaxTKPuQ/S2IFgs4yyXkFtrxuLKvXm+5QP5vXnvOsrIJzsgA
hQKg47WA69nxUXUrT6MhFeTSmruIFmw7ee2mbmGyQrpVr8Ee8x+TP+mZC18tS1rP
Isb/crB07uollldreDBQhU/ES5NNo3HpCA==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE REQUEST-----
MIIC8jCCAcYCAQAwgZgxCzAJBgNVBAYTA1VTMQswCQYDVQQIDAJDQTERMA8GA1UE
BwwIVGVtZWN1bGExITAfBgNVBAoMGE9QVE8gMjIgb24gb3B0by0wMC1kMi1kYzEM
MAoGA1UECwwDRW5nMRYwFAYDVQQDDA0xOTIuMTY4LjAuMTA0MSAwHgYJKoZIhvcN
AQkBFhFkc2NhcnJAb3B0cDIyLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBANPdqdUvH6INYTXPMPEEDSsKSDJfGQornoZdPixY0vmenNnFLIsseXELJ/

y30gL/yscMvaKFBAc4iR5bUA1j/pu6UCAwEAAaAAMA0GCSqGSIb3DQEBCwUAA4IB
AQA8nrjK1hnqwlsqY9rj3J3XuP66PtQ8JNJ3gNd2iJHjuo9OQr3nVqxT4/WzUgNys
KmnNGHWrdx/pQmW1jhWRYTwpOWqRcH/vrfi76UpNC58EVF/ZRD7a5avP/kynY0ZR
0wdIFhwwSMJtojKDdj8mHMskBsrjft4SspWGo8rsWTv1n6PJEllWgKSvgtPUE0Rsi
eNVd9LsPsFdFSkT02/GOW17RSTCTIPaD6cP2J+bt/Tra9EUPoV9+Z3X/2mBs+ndO
Jgo38F3ksaI8sNlxHsHP8dXQt0hlRAkvxJY+ZbFjYgEqLsfalLLrNCHXmGTVaogc
NIKBQzXjqVirfIDMdSHjKjLd
-----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 54.

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 49

This product is obsolete.

Finish the Self-Signed Certificate

When you created the private key ("Step 2: Create a Private Key" on page 46), 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.
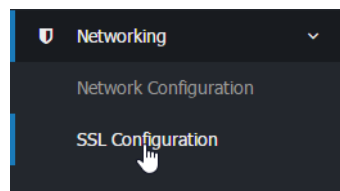
    For Internet Explorer 10: Click "Continue to this website (not recommended)."

    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
VQQGEwJVUzELMAkGA1UECAwCQ0ExETAPBgNVBAcMCFRlbWVjdWxhMSEwHwYDVQQK
DBhPUFRPIDIyIG9uIG9wdG8tMDAtZDItZGMxDDAKBgNVBAsMA0VuZzEWMBQGA1UE
AwwNMTkyLjE2OC4wLjEwNDEgMB4GCSqGSIb3DQEJARYRZHNjYXJyQG9wdHAyMi5j
b20wHhcNMTUwMjEwMjEzNTU3WhcNNDUwMjEwMjEzNTU3WjCBmDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgMAkNBMREwDwYDVQQHDAhUZW1lY3VsYTEhMB8GA1UECgwYT1BU
TyAyMiBvbiBvcHRvLTAwLWQyLWRjMQwwCgYDVQQLDANFbmcxFjAUBgNVBAMMDTE5
Mi4xNjguMC4xMDQxIDAeBgkqhkiG9w0BCQEWERzY2FyckBvcHRwMjIuY29tMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApGMvd+ATfSBegut+qy0C20QP
HJsphbae+OP1mKl8LRSXGmOkC1+Ul2qMf7vVpokFD2lXmg/ytBOCfcjPuxriGCh5
3RF7mdF4RBaZOTnF7Y3cqdBtQO87UPUfAsv6BXyLXA3qlFMnnsp1+Jrh8l/dNwN/
twIS0rgrDf1j3ugGdV0e4wzZ+SGqoYiIVkASUzV5a3+2SCfojRYxmvvSnfew9Lg4
GWUJMTHW0qmpCwXgBOIasXzyvxxwIO4zqZEygbVhnltjCgSxhnm/86O7s6lRh7Fd
ZtllvEj8X/T/oDceFp7Na48fKUggjo7ubcYEWiAnWpLbA/8LdfW4mDoSok2bhQID
AQABo1AwTjAdBgNVHQ4EFgQUb+2Tvx3Rpg3b9ZB1hwrZiIitutswHwYDVR0jBBgw
FoAUb+2Tvx3Rpg3b9ZB1hwrZiIitutswDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0B
AQsFAAOCAQEAA7lG7qjadOdWHldBwA0VMu85uHzi+NUDLQDVoyJQ2+TVEOgC4m+x
p2wuf/c4+RAvTOeNzxYGvt2iVCmH1vyZWW0VJ3OIXSfgdgkLjN7xioYW5Sjttq0G
g4xGAsN1opxG4Nut9ubjYLSjibF7liGZu4d5/PLhQDHqAUIWHk+sHyQDiWASgeh0
Spft39SKnNgBLBASwRCnmasqylTYwh1D9AHWXAZVI3h0xCv1qxhKhjRKRWA5bqrG
c5fm0eXf3cGe/XYaDn9iWdt/7fHnJZ7ACncXQVXxjTdF8lZ2Ca9ge2y4E/+ox0Yj
Cg8O1mjL70Bjs96jP9YbWJO+BOGbkhOTjw==
-----END CERTIFICATE-----
```

If you have multiple certificates and have any doubt about whether this is the right one, open up the certificate in Windows. When the certificate wizard/exlporer 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 46..)

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 51**

"**OS X" on page 52**

Windows

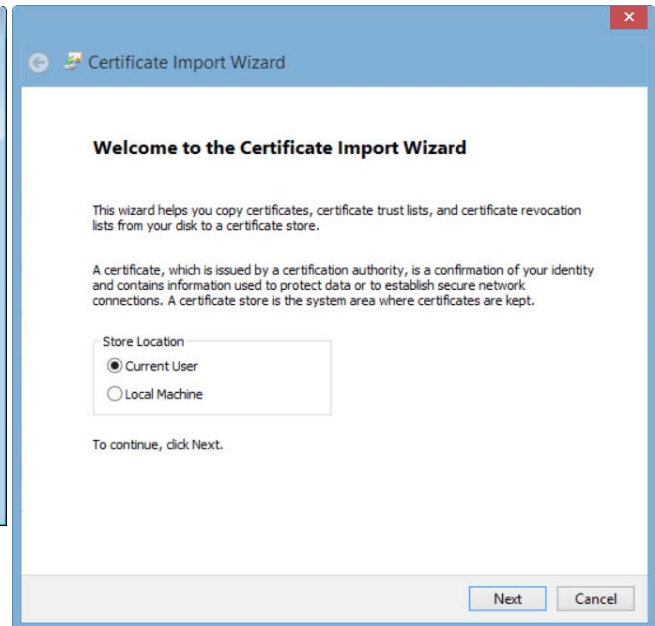*Internet Explorer & Chrome*

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.

<div style="display:flex">

Windows 7

Windows 8

</div>

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

This product is obsolete.

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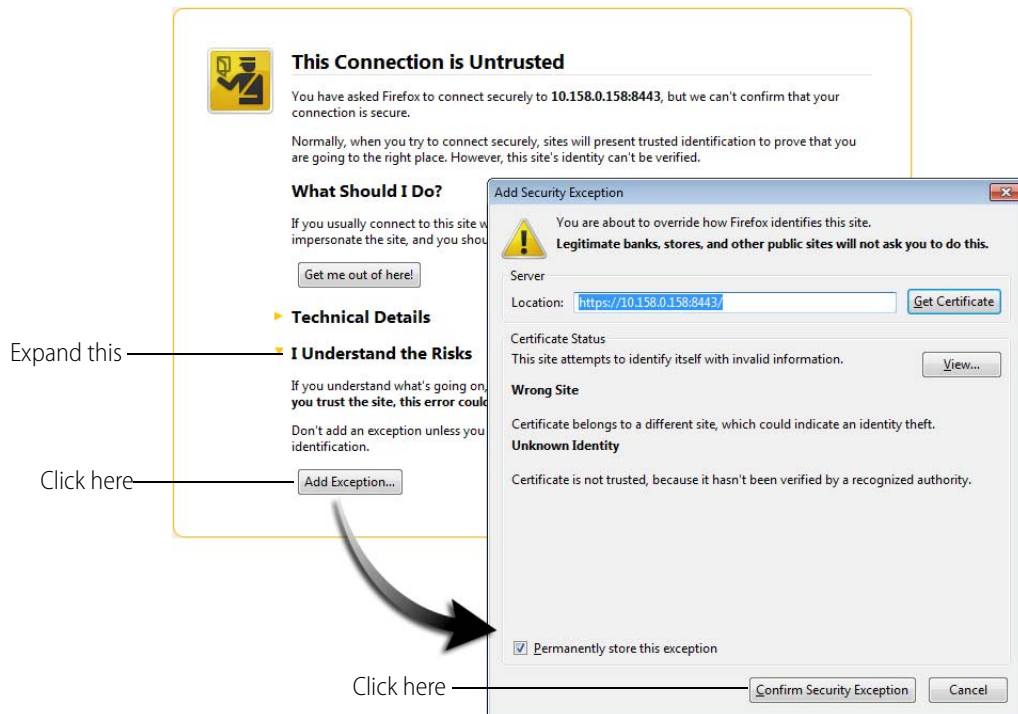
6. To verify the certificate was installed correctly, open Firefox and enter the hostname specified on the certificate. If the browser does not generate an untrusted site warning, the certificate was installed correctly.

OS X

Safari and Chrome

1. Open Safari and enter https://<server name> to open this dialog box:
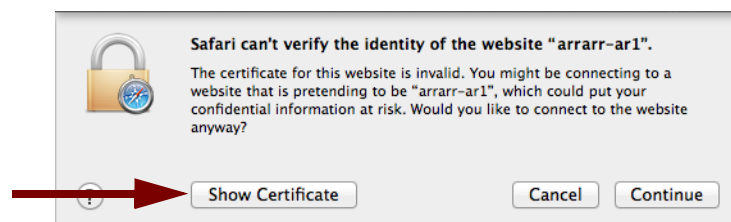
2. Click Show Certificate to reveal the full details:
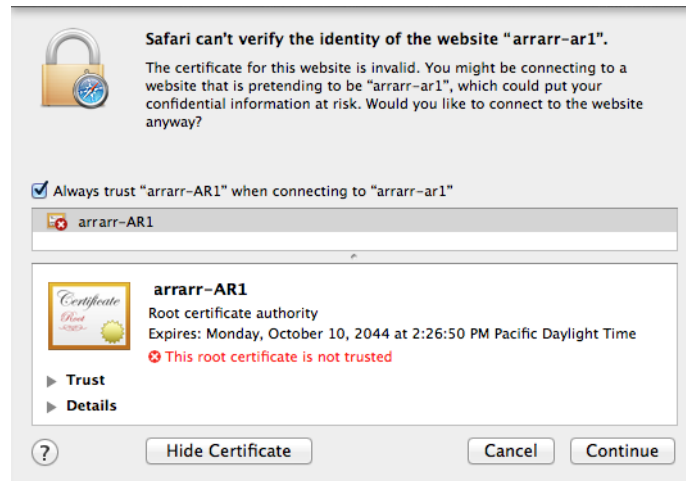
3. If the certificate looks good to you, check the "Always trust *<server name>* when connecting to *<server name>*" and click Continue. You will be asked to provide your password to authorize the addition of this certificate to your keychain, after which the browser and the Hosted Projects window will 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 53**
- "**Android Devices" on page 54**

iOS Devices

1. Email the *<server name>.cer* file you created previously (see "Step 2: Create a Private Key" on page 46) 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 46) 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 54)

"Obtain a CA-Signed Certificate" (see page 55)

"Install the CA-Signed Certificate on groov Box" (see page 56)

Finish the CSR

When you created the private key ("Step 2: Create a Private Key" on page 46), you also created a certifcate 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.

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 46.)

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
b3B0by0wMi0yYS1hNjEWMBQGA1UEAwwNb3B0by0wMi0yYS1hNjCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAPnEPMiUKONk5YKpt4jwtl83qShIKHpPOIbE
c3D4IpSa0e1iPjbyIxsesY68DmqcXEvPXzSxyjeFVHKgDdOgrQIVhrAtUWn4aLCU
sNI9GbcCOft1dLRxxceyIlDeVQD5KI6DR2xCGnqvMwpc8tzbJksYWroPjCRFwVi7
V5oG405YGsqxBQAVKiQBRyjTJUkKDu/HGb5WtVYUoieoguLlnhnttpH71Kk2iZ+K
ZgXss8W017v9/I4nsc9sFTq8Iclg9G9tSfSjX+S46UfVmeu2ExYzbz3dvTJF6mzC
z9mL5Q5Sy6RZT56ksJGMZGVaQo9sfHcgjdYJIbAEpM9nYXfDgq8CAwEAAaAAMA0G
CSqGSIb3DQEBBQUAA4IBAQCvRm0AQVeMyj6LC7YBLCP5iGnlFM++PH3rZjwrJi2b
rOdgStAeYLMewo+XU/8G5pMojnwhfvBnBbukovA7gi77my0JBvQPLJBQ8u9GQlEU
GY7r19gcn9uncW6FzkH0WNkvCC6Ps5lqPUgcBQE9+/aI10MRWNdwVLVZn21HKYMH
+H/SdPFtbSUzoHvHBJNZG5WPaJwrdrnOSvdLtOuPl/TBuOKIDTmqjYoUANtyjQnc
U745b/kU8RQuNsyvk6aFmNP7oWgIou7CgWQ09ZfFcEGATn3+QDXHl5tlpYOGLjMM
7UD2Y6uE9s5sxv2ME6V2BAP6Vk8DcSWDq78NhQcwkj/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.
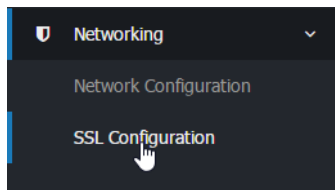
2. Click the Upload certificate tab on the SSL Encryption page.

3. 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 46.

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

4. Under "Certificate text" click "Entered below," then click Browse and specify the file containing the signed certificate that was obtained from the CA.

5. 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*.

a. 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.

5: Maintenance and Troubleshooting

Maintenance

Turning the *groov* Box On and Off

STOR LED   SYS LED   PWR LED

On/Off button

Turning the Box on

1. Check to make sure the PWR LED is on. This means that the *groov* Box is receiving power.
2. Briefly press the On/Off button. Wait until the SYS LED has stopped blinking and is solid green.

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

Turning the Box off

With the *groov* Box on, briefly press the On/Off button. The SYS LED will blink orange and then turn off. The PWR button will remain on as long as there is power from the power supply. Always allow the *groov* Box to turn off completely before removing power.

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

Resetting the *groov* Box to factory defaults

Restoring the *groov* Box restores the default network settings and erases all user data, including your project. When the process is complete, the Box will send out a DHCP request on ETH0, and you will be able to connect using the default hostname.

CAUTION: *When the groov Box is restored to factory default settings, your project will be erased.*

1. Check to see that the *groov* Box is turned off, but the PWR LED is on.
2. Press and hold the On/Off button for at least four seconds and until the STOR LED is blinking orange. Then release the button.

    Both the SYS LED and STOR LED will be blinking orange at this point. When both the SYS LED and STOR LED stop blinking orange, the procedure is finished.

3. Briefly press the On/Off button to turn off the *groov* Box, then briefly press it again to turn the *groov* Box back on so that you can log in.

Maintaining the fan filters

Be sure you check and clean the fan filters periodically and replace them when necessary. How often you do this will depend on the installation environment. If the fan filters on the *groov* Box become clogged, they can be re-used. A pair of extra filters is also provided.

1. Pry off the outer cover using a small utensil around the outer edge.
2. Remove the old filter.
3. Rinse and pat dry the old filter, or replace it with a new one.
4. Using your fingers, snap the outer cover back into place.
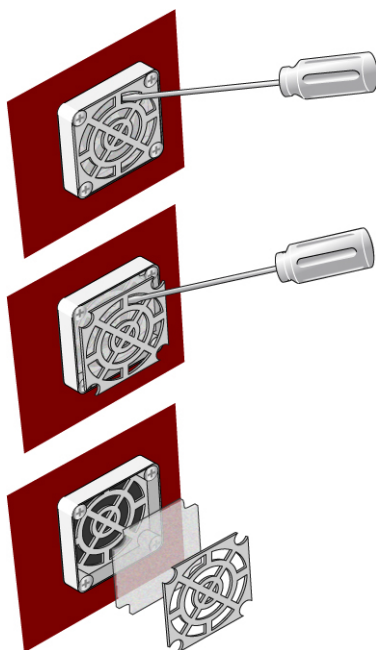
Troubleshooting

The *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 65.
- Check that the power supply is securely attached to the *groov* Box and the power supply is receiving power.

The *groov* Box is connected to the Ethernet network but not working

- Make sure the *groov* Box has been turned on, the PWR LED is lit and not blinking, and the LNK ACT LED for the connected Ethernet interfaces are lit. (See "LEDs" on page 68.)
- 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 top of the *groov* Box, where the hostname should be written.

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

See the next questions for more answers.

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 25.

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 20*.

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://192.168.1.54

Computer with more than one NIC

A: 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.

Controller, Modbus device, or OPC UA server 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 controller:

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 27 to configure the ETH1 connection.
3. Now try configuring your controller or tag server again. This time *groov* should be able to find it.

Cannot log into the *groov* Box using the 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 SYS LED does not stop blinking after reset

If you have restored the *groov* Box to factory defaults, but the SYS LED continues to blink for more than an hour, the Box is unable to start the *groov* software. Try this:

1. Log into manage.groov.com. Download and save to your computer the most recent version of the *groov* App for your Box.
2. In your browser, open *groov* Admin by using the Admin URL: https://*hostname*:10000 (For example, `https://opto-00-d2-dc:10000`)
3. Once you are logged into *groov* Admin, update the *groov* app using the file you downloaded.

If these steps do not solve the problem, contact Opto 22 Product Support.

Considerations for locating the *groov* Box

The *groov* Box is an industrial appliance made to operate in tough environments, so it doesn't have to be pampered. Make sure you check the specs for temperature and humidity, and then place it where you can connect it to both your company computer network and your control network. (You will use separate connectors on the *groov* Box for these two networks to keep them physically separated—better for security.)

If you're using the wireless LAN, choose a location where the signal is constant and strong. Wireless networks can be unreliable unless carefully designed and periodically checked.

The Box can be DIN-rail mounted (DIN clips are built into the back) or mounted on a wall or equipment using the four exterior mounting tabs. Make sure there's space on both sides of the box so air can flow freely through the fans.

If you're a machine builder or OEM and including *groov* in your machine, the same basic ideas apply: check specs, check security, and mount where there's room for the Box to breathe. Also, make sure you have network access to the Box for updates.

Using external Wi-Fi antennas

If you want, you can use external wireless antennas instead of the two that are provided. The connector is a reverse SMA.

This product is obsolete.

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
Security (wireless)	WEP (64-bit and 128-bit) WPA PSK (also known as WPA Personal) WPA2 PSK (also known as WPA2 Personal)
Antenna Connector	Reverse polarity SMA (RP-SMA or RSMA)
Power Consumption	14-36 VDC, 24 VDC @ 1 amp (Power supply included; input 100-240 VAC. Use international adapter if needed.)
Enclosure	Sturdy metal case
USB	USB 2.0 (two)
Indicators	Ethernet interfaces (2): Link/Activity and Speed System: STOR, WLAN, USER, BATT, TEMP, FAN, SYS, & PWR
Operating Temperature	0 to 50 °C (32 to 122° F)
Storage Temperature	-20 to 60 °C (-4 to 140° F)
Operating Humidity	10% to 90% relative humidity, non-condensing
Storage Humidity	5% to 95% relative humidity, non-condensing
Agency Approvals	CE, RoHS, DFARS Wireless: U.S., FCC Part 15 Subpart C; Canada, IC RSS-210
Warranty	30 months

Dimensions
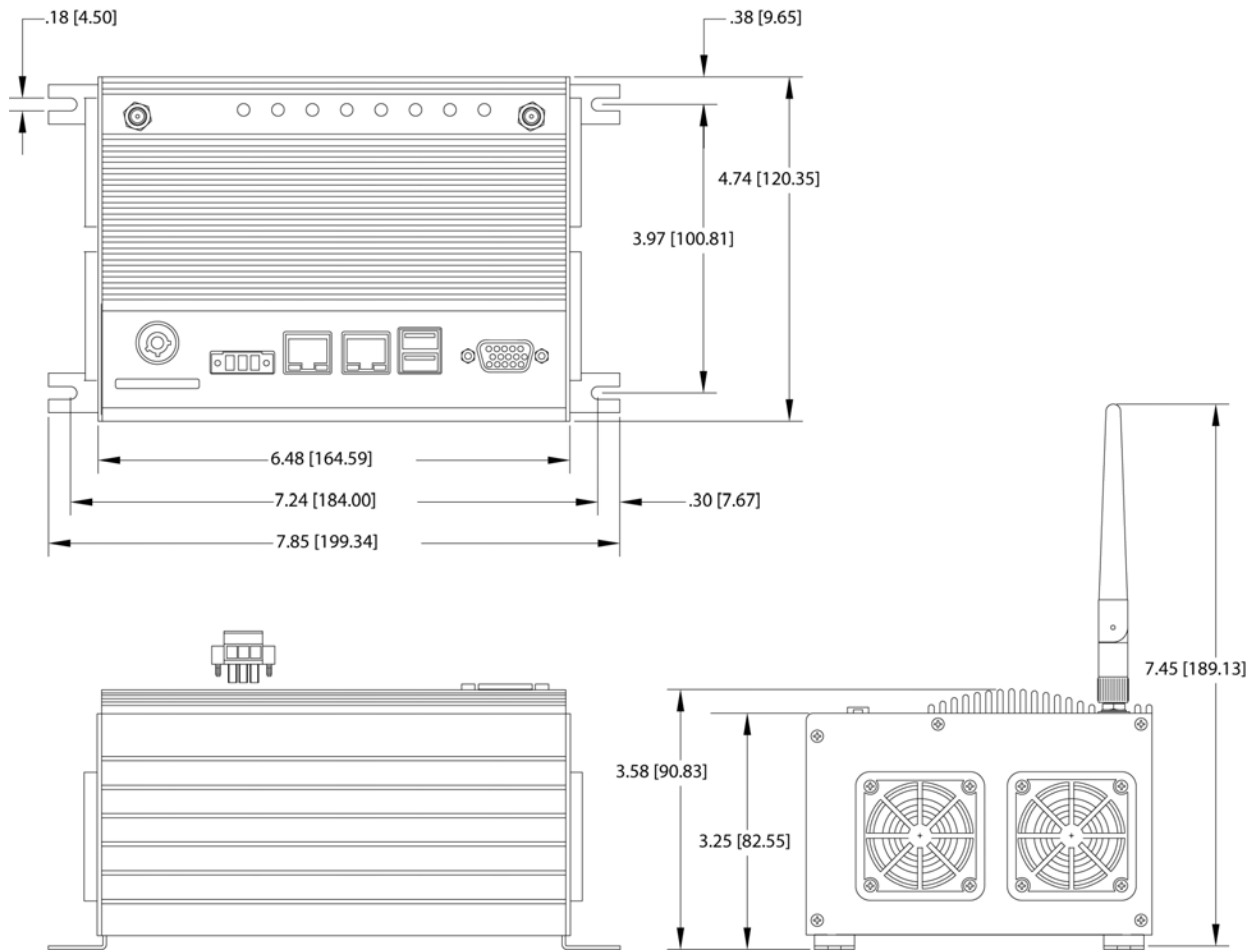
B: Connectors, Indicators, and LEDs

Connectors and Indicators

Status and activity LEDs

Ethernet LEDs

On/Off button

USB connectors for backing up and restoring

Power connector

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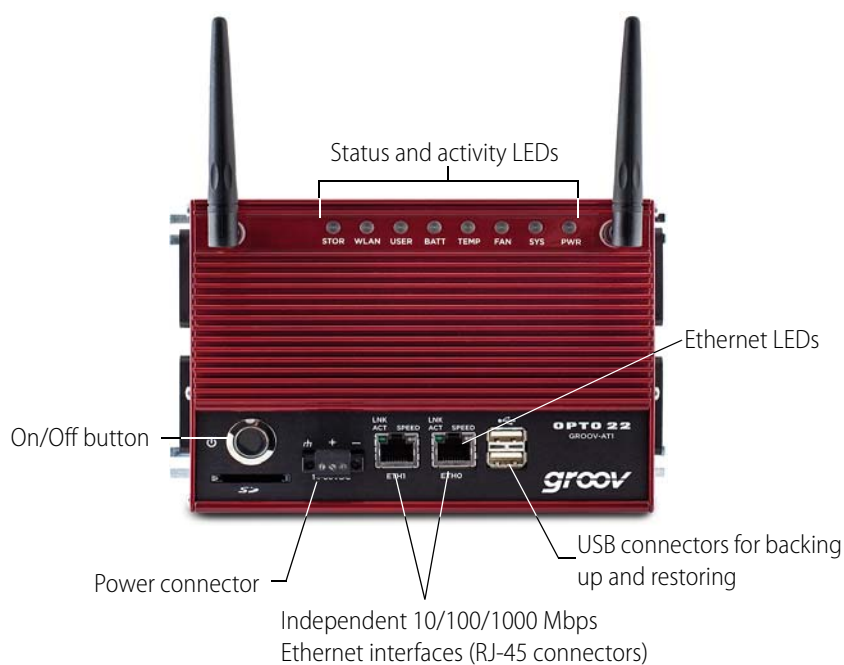
LEDs

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

LED	What it shows	Color	What it means
STOR	Hard drive activity	Blinking green	Activity on hard drive
		Blinking orange	Hard drive is being restored to factory defaults
WLAN	Wireless network connection status and network activity	Off	*groov* Box is disconnected from the wireless LAN.
		Green	*groov* Box is connected to the wireless network
		Blinking green	Wireless LAN activity
USER	Not used	n/a	n/a
BATT	Battery status	Green	Battery 90% Charged
		Blinking green	Battery charging
		Red	Outside voltage range. BIOS may be corrupted. Contact Product Support.
TEMP	Temperature status	Green	Temperature OK
		Red	Temperature outside operating range
FAN	Fan status	Green	Fans are operating properly
		Red	One or both fans have failed
SYS	*groov* Box status	Off	*groov* Box is turned off
		Green	*groov* Box is turned on
		Blinking green	*groov* Box is booting up
		Blinking orange	*groov* Box is shutting down
PWR	Power to Box	Off	No input power
		Green	Good input power
		Red	Input power outside normal range
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

Index

This product is obsolete.

This product is obsolete.