

***GROOV* SERVER FOR WINDOWS USER'S GUIDE**

groov SERVER FOR WINDOWS USER'S GUIDE

Form 2078-150512—May 2015

OPTO 22
Automation made simple.

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

Product Support Services

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

groov Server for Windows User's Guide
Form 2078-150512—May 2015

Copyright © 2013–2015 Opto 22.

All rights reserved.

Printed in the United States of America.

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

Opto 22 warrants all of its products to be free from defects in material or workmanship for 30 months from the manufacturing date code. This warranty is limited to the original cost of the unit only and does not cover installation, labor, or any other contingent costs. Opto 22 I/O modules and solid-state relays with date codes of 1/96 or newer are guaranteed for life. This lifetime warranty excludes reed relay, SNAP serial communication modules, SNAP PID modules, and modules that contain mechanical contacts or switches. Opto 22 does not warrant any product, components, or parts not manufactured by Opto 22; for these items, the warranty from the original manufacturer applies. These products include, but are not limited to, OptoTerminal-G70, OptoTerminal-G75, and Sony Ericsson GT-48; see the product data sheet for specific warranty information. Refer to Opto 22 form number 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, 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. Unicenter is a registered trademark of Computer Associates International, Inc. 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. Nokia, Nokia M2M Platform, Nokia M2M Gateway Software, and Nokia 31 GSM Connectivity Terminal are trademarks or registered trademarks of Nokia Corporation. Sony is a trademark of Sony Corporation. Ericsson is a trademark of Telefonaktiebolaget LM Ericsson. CompactLogix, MicroLogix, SLC, and RSLogix are trademarks of Rockwell Automation. Allen-Bradley and ControlLogix are registered trademarks of Rockwell Automation. CIP and EtherNet/IP are trademarks of ODVA.

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

OPTO 22

Chapter 1: Getting Started	1
Welcome	1
Try Before You Buy	1
For Help	2
What You Will Need	2
Setting Up groov Server	2
Step 1. Activate groov	3
Step 2. Download Software	3
Step 3. Install Software	4
Step 4. Start groov and Install the License File	4
Working with groov	5
Create a New Username and Password	5
Add a Tag Database	6
Build an Operator Interface	8
Create Layouts	10
Chapter 2: Using an SSL Certificate	15
Using a Self-Signed Certificate	16
Step 1: Create a Self-Signed Certificate and Private Key	16
Step 2: Add the Self-Signed Certificate to the Browser Trust Store on Client Computers	18
Windows	18
OS X	20
Step 3: Install a SSL Certificate on Mobile Devices	21
iOS Devices	21
Android Devices	22
Using a CA-Signed Certificate	22
Step 1: Create a CSR	23
Step 2: Obtain a CA-Signed Certificate	24
Step 3: Install the CA-Signed Certificate on the Computer	25
Chapter 3: Maintenance and Troubleshooting	27
Starting and Stopping groov Server	27
Changing and Opening the groov SSL Port	29
Changing the groov Port	29

Manually Opening Ports	30
Getting groov Updates	30
Erasing Your groov Project	31
Backing Up and Restoring Your Project	31
Troubleshooting	33
groov Server doesn't start	33
Cannot read or write to a Modbus/TCP device OR the data doesn't make sense	33
Problems with groov Build or groov View	33
For Help	33

1: Getting Started

Welcome

groov Server for Windows (p/n GROOV-SVR-WIN) runs on a PC instead of a *groov* Box appliance. *groov* Server for Windows includes *groov* Build for building operator interfaces and *groov* View for using them. Although this software is stored and served on a Windows PC, any computer with a modern web browser can be used to build interfaces. These operator interfaces can then be viewed on almost any computer or mobile device regardless of its manufacturer or operating system, including PCs, tablets, smartphones, and even smart high-definition televisions.

Once installed, *groov* Server runs as a service on the server computer. This means that it starts when Windows does, and it continues to run in the background as long as Windows is running. In order to build or use *groov* interfaces on any device, this PC must be on and *groov* Server must be running. For more information on building and using interfaces, see [form 2027](#), the *groov* User's Guide.

Try Before You Buy

A fully functional version of the software-based *groov* Server for Windows is available to download and try so you can see your own system's data on a smartphone, tablet, or other mobile device. It includes *groov*'s built-in Data Simulator, so while you're evaluating *groov* it doesn't have to be connected to a live machine or system.

Just download and install *groov* Server for Windows (groov.com). Simple instructions walk you through software setup, connecting to one or more systems, and building simple interfaces so you can quickly see realtime system data on a mobile device. *groov* Server operates for two hours without a license key.

NOTE: You must log on as an administrator to install groov Server for Windows.

If you need an OPC UA server to connect to a third-party controller, Kepware Technologies' KEPServerEX 5 communication platform is also available for download and trial (www.kepware.com). It also operates for two hours without a license key.

For Help

If you have questions about using *groov* Server and you cannot find the answer you need in this document or in the [groov User's Guide](#), please contact Opto 22 Product Support.

Phone: 800-TEK-OPTO (835-6786)
951-695-3080
Monday through Friday, 7 a.m. to 5 p.m. Pacific Time

Fax: 951-695-3017

E-mail: support@opto22.com

Website: www.opto22.com

What You Will Need

To install and run *groov* Server for Windows you'll need:

- A PC on the same network as your control device, with one of the following Microsoft® operating systems. This can be the same computer where the tag server is installed, or a separate computer.
 - Windows® 7 Professional (32-bit and 64-bit)
 - Windows 8 Professional (32-bit and 64-bit)
 - Windows Server 2008 R2
 - Windows Server 2012

NOTE: .NET Framework 3.5 or greater is required for all operating systems. Use the "Add roles and features" option for Windows Server 2012.

- A minimum of 250 MB available disk space to install *groov* Server for Windows. Additional disk space is required to create projects. (Projects may be created on this PC or on another computer.)

Setting Up *groov* Server

Setting up *groov* Server for Windows is a four-step process: activate *groov*, download software, install software, and download and apply your License File. *All steps except installing software require Internet access.*

If the PC where you plan to install *groov* Server has Internet access, do all steps on that PC. Start with "[Step 1. Activate *groov*](#)" on page 3.

If the PC where you will install *groov* Server does not have Internet access, you can use another PC to activate and download files. However, to download the License File, you need to know a MAC address on the PC where *groov* Server will be installed. To get it, go to the server PC and open a Command Prompt. Type `ipconfig /all` and look for "Physical Address." It will be a hex value with 12 digits separated by hyphens into groups of two. Write it down, go to the PC with Internet access, and follow the procedures starting with "[Step 1. Activate *groov*](#)" on page 3.

Multiple *groov* Server installations. If you plan to install *groov* Server on multiple PCs, here are some important things to know:

- Each *groov* must be individually activated using its Activation Key, because each purchase of *groov* is a separate installation.
- The software download file is the same for all *groov* Servers for Windows, so if you are downloading from one PC and then installing on multiple other PCs, you only need to download the software once.
- Each *groov* requires its own License File, which is tied to a MAC address for the PC on which it's installed. If you download multiple License Files, you can tell them apart by the MAC address in the filename. Make sure the correct License File goes on each server PC.

Step 1. Activate *groov*

*NOTE: If you already have the *groov* Server Installation File, skip to "Step 3. Install Software" on page 4.*

1. Open a web browser (Firefox or Chrome recommended). Go to activate.groov.com.

The screenshot shows the 'Activate groov' page. At the top right, there is a phone number '800-321-OPTO (6786)'. Below the header, there are social media icons for Twitter and Facebook. The main text says: 'Activate your *groov* to get free updates and be notified when updates are available. You need a free My.Opto22 account to activate.' There is a text input field for 'Enter your email address:' followed by a red 'Go' button. To the right of the input field is the large red 'groov' logo.

2. Log in using your email address and your My.Opto22 password.

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

The screenshot shows the 'Activate groov' page with the activation key step. It features the same header and social media icons. The main text says: 'Enter your *groov* activation key:'. There is a text input field for the activation key followed by a red 'Go' button. Below the input field, it says: 'Your Activation Key is in the certificate you received by mail or email when you purchased *groov*.'

3. Enter the Activation Key you received via mail or email when you purchased *groov* Server. Click Go.
Your *groov* is activated.

Step 2. Download Software


Click Download *groov* Software and save the file to your computer. (Or click Show next to your *groov* in the list, and download the *groov* Server Installation File.)

(Optional) If you already know the MAC address of the PC where you're installing *groov* Server, you can also get your License File now. To do so, enter it in the MAC address field, click Go, click Get License File, and save the file to your PC.

Step 3. Install Software

NOTE: You must log on as an administrator to install groov Server for Windows.

1. On the PC where you want to install *groov* Server, double-click the *groov* Server installation file and follow the onscreen instructions.
2. When asked whether to open port 443 (needed to access *groov*), check the box to open it unless you need to use a different port or want to open it manually. (See [page 29](#) for instructions.)

groov Server begins running as soon as it is installed. You can tell it's running by the *groov* Monitor icon  in the system tray. The little green arrow means it's running.

Step 4. Start *groov* and Install the License File

1. If you haven't already started *groov* App, in your web browser type: `https://localhost`. Make sure you include the `s` in `https` as the `s` indicates a secure connection. If you're not on the PC that's running *groov* Server for Windows, type `https://` plus the hostname or IP address of the *groov* Server computer.
2. When your browser connects to *groov* for the first time, accept the *security warning*. This is normal behavior for *groov*. 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:

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

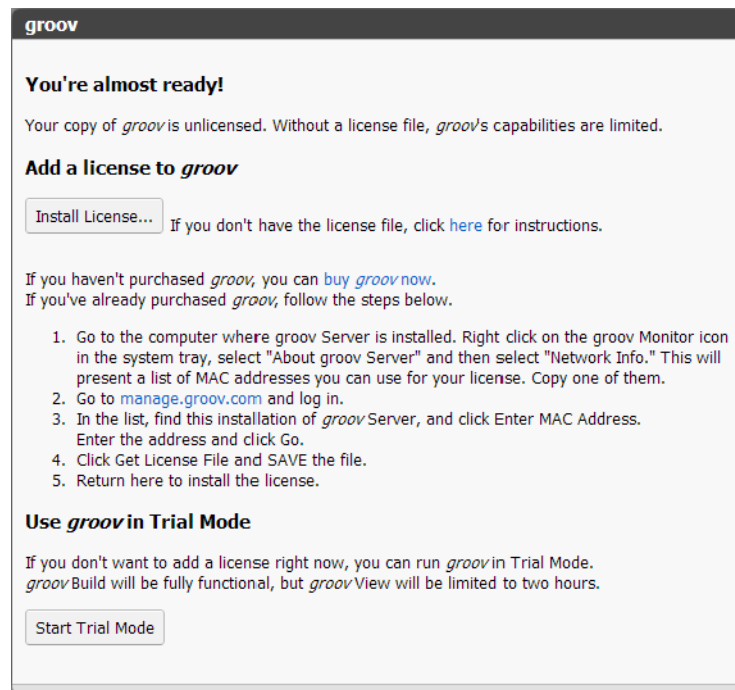



For Safari: Click Continue.



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

- When prompted to add a license file to *groov*, click the word “here” and follow the onscreen instructions.



- After you have saved the license file on your PC, come back to the Licensing dialog box and click Install License.
- Browse to the license file, then click Open.
If you have any trouble opening *groov*, check the *groov* Monitor icon  in the system tray (lower right corner of the screen) to make sure *groov* Server is running. If you don't see it, click the Show Hidden Icons arrow. For more about *groov* Monitor, see [Chapter 3: Maintenance and Troubleshooting](#). If *groov* Server does not start, see [Chapter 3: Maintenance and Troubleshooting](#).
If *groov* Server is running but *groov* Build does not open, see Troubleshooting in [form 2027](#), the *groov* User's Guide.
- Continue with “[Create a New Username and Password](#)” on page 5.

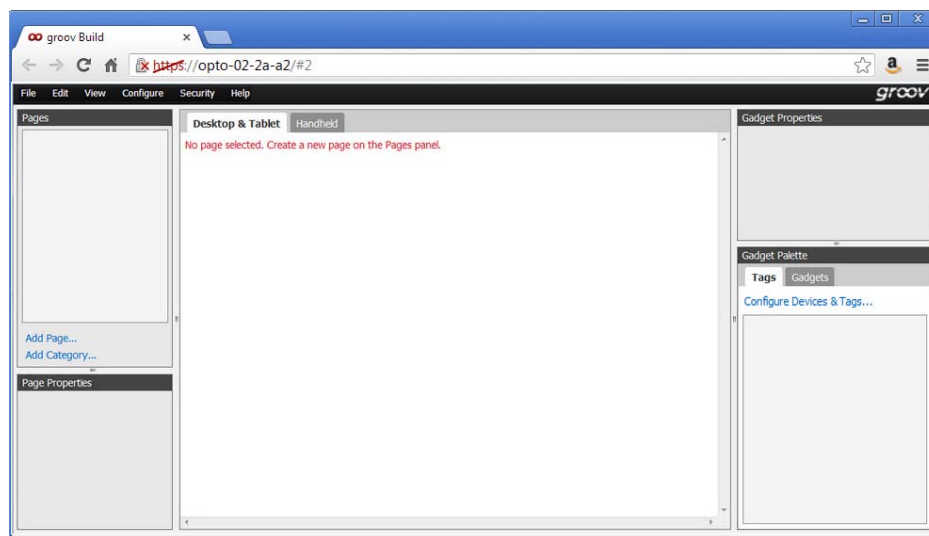
Working with *groov*

Create a New Username and Password

Follow the on-screen instructions to create an administrator username and password for *groov* Build. If the security warning appears again, accept the warning again. Write down your Username and Password, and keep it in a safe place. You will need this information each time you log in.

CAUTION: If you lose your login information, you will not be able open your project. There is no password recovery option! To log in to groov again you'll need to erase your project and start over. See "Erasing Your groov Project" on page 31.

After you have completed the instructions in **Welcome to groov**, groov Build opens in your web browser.

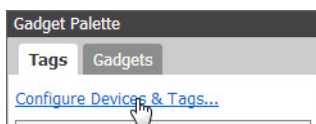


Add a Tag Database

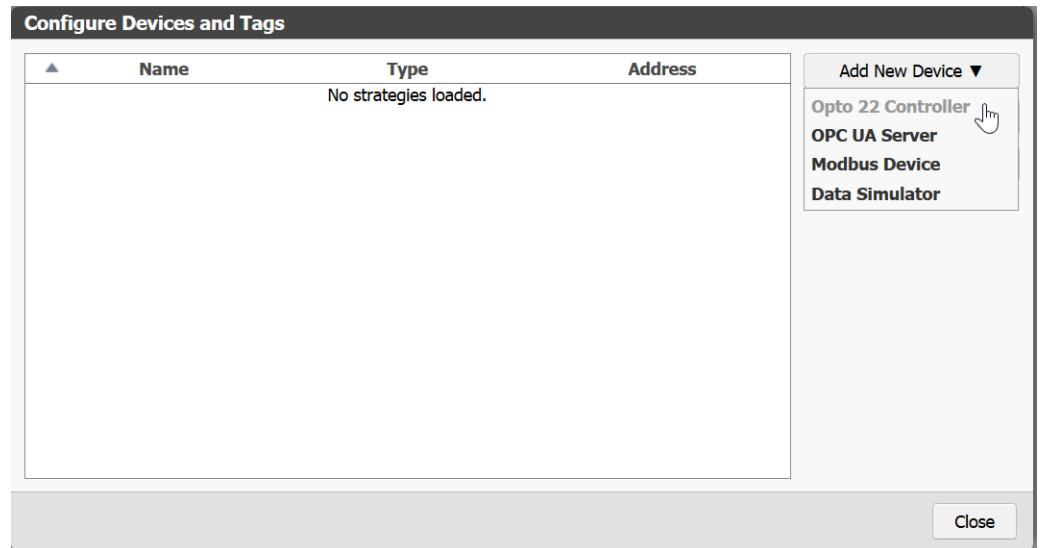
You can import a tag database from an Opto 22, an OPC UA-compatible tag server, or a Modbus/TCP slave device. This section describes briefly how to import tags from an Opto 22 controller. For more information about this or about how to use tags from another manufacturer's system, see [form 2027](#), the *groov User's Guide*.

Follow these steps to add an Opto 22 controller that the operator interface will communicate with. When you add a controller and the .idb.txt file associated with the strategy that runs on the controller, the strategy's tags become available in *groov* for you to use. Repeat the steps to add additional Opto 22 controllers and tags.

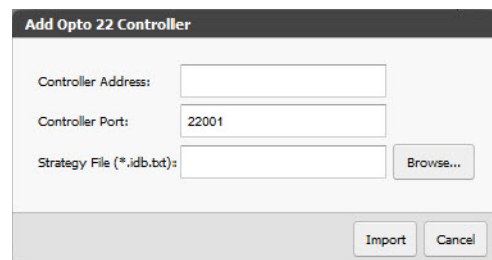
1. Under Gadget Palette on the right side, click **Configure Devices & Tags**, or select **Configure > Devices and Tags**.



- Click Add New Device and then select Opto 22 Controller.



- Enter the hostname or IP address of the controller running the strategy you want to use.



For a SoftPAC controller, use the full name of the computer running SoftPAC as in this example:
 JAlvarez-w7.ACME.com

- Click Browse to locate the .idb.txt file you want to use.

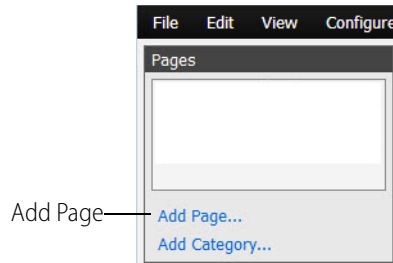
NOTE: When PAC Control compiles a strategy it automatically generates an .idb.txt file and places it in the same directory as the strategy. If you are setting up groov on a computer other than the one used to develop the PAC Control strategy, copy the .idb.txt file into a directory that is accessible to the computer you are using to set up groov.

- Click Import.

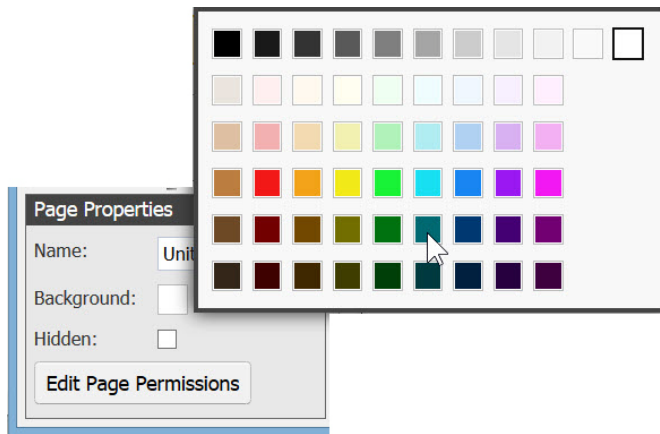
Build imports the .idb.txt file. The tag database is now available in groov.

Build an Operator Interface

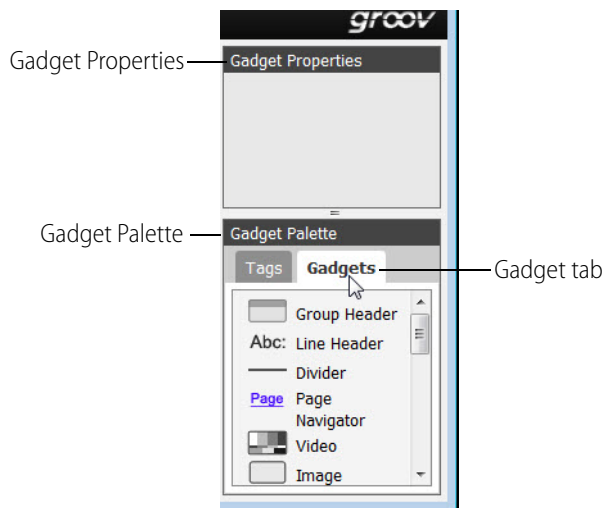
1. Click Add Page on the left side under Pages.



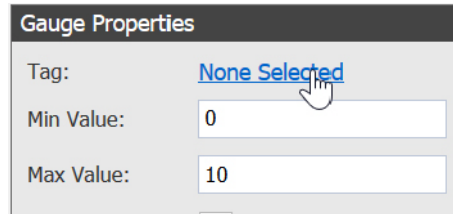
2. Type a new name for the page, then click OK.
3. Under Page Properties, click the box next to Background and select a background color.



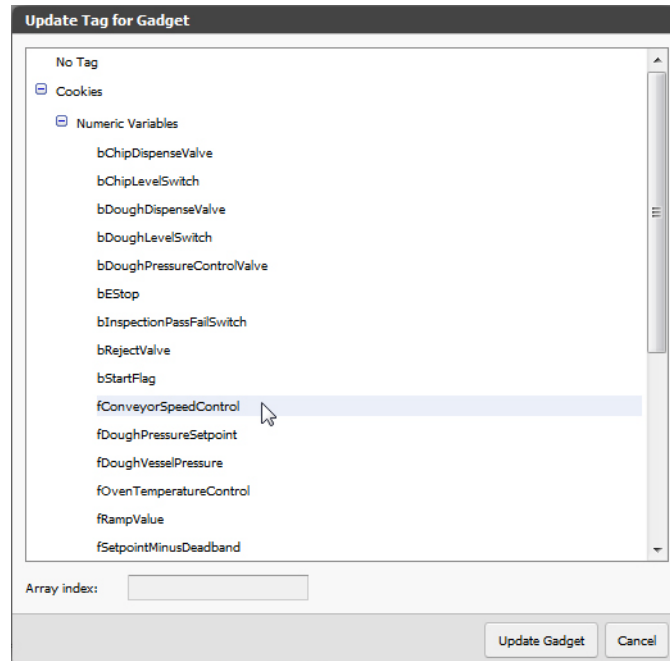
4. Select the Gadget tab in the Gadget Palette.



5. Select a gadget such as a Round Gauge and drag it into the work area.
6. Click None Selected in Gadget Properties (in the upper-right corner).

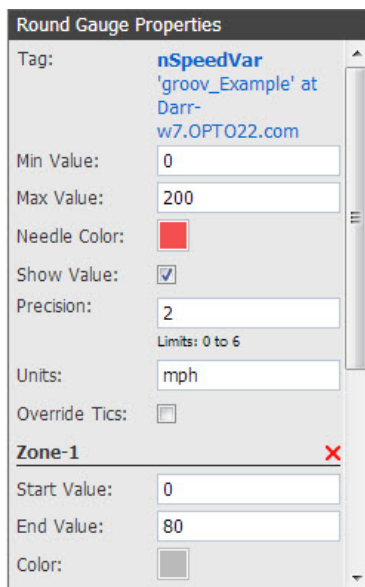


7. In the Update Tag for Gadget dialog box, browse to a tag and select it.



8. Click Update Gadget
9. Configure the gadget's properties.

For example, the Round Gauge allows you to add zones with different colors for each zone. To add a zone, simply click the Add Zone button, then choose the Min Value, Max Value, and Units that make sense for your variable.



10. Select File > Save All and Switch to *groov* View.

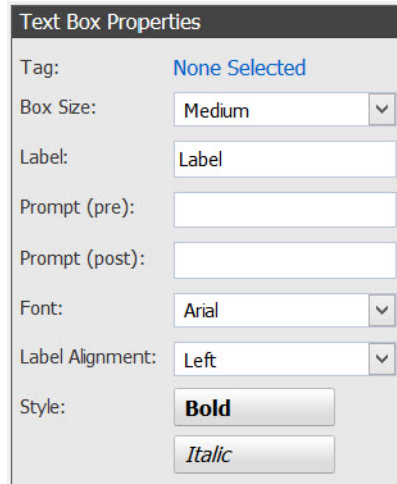
You should now see your gadget running in View. The round gauge's needle shows the tag's current value. Note that the live value is shown in blue text.



Create Layouts

1. Click the gear symbol in the upper-right corner of View, and select "Switch to *groov* Build."
2. Add several more tags and gadgets to your project, and arrange them in the Desktop & Tablet view. For help, see [form 2027](#), the *groov User's Guide*.

- For a Graph gadget, use a variable that will change over time and generate a curve, such as temperature.
- For a Text Box gadget, use a variable that can be changed with text input.



Text Box Properties

Tag: **None Selected**

Box Size: **Medium** ▼

Label: **Label**

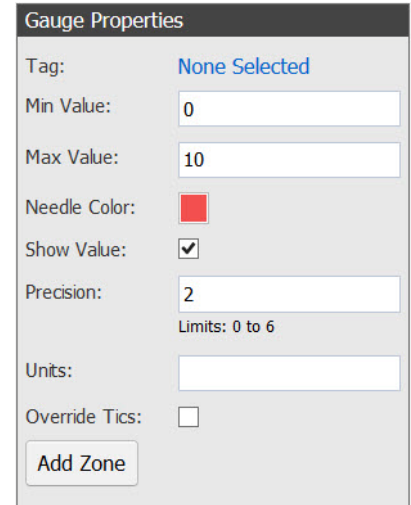
Prompt (pre):

Prompt (post):

Font: **Arial** ▼

Label Alignment: **Left** ▼

Style: **Bold**
Italic



Gauge Properties

Tag: **None Selected**

Min Value: **0**

Max Value: **10**

Needle Color: ■

Show Value:

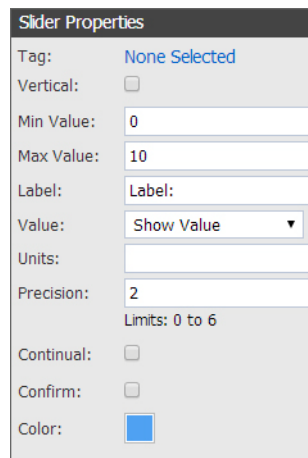
Precision: **2**
Limits: 0 to 6

Units:

Override Tics:

Add Zone

- For a Slider, use a variable that can be changed within a given range.



Slider Properties

Tag: **None Selected**

Vertical:

Min Value: **0**

Max Value: **10**

Label: **Label:**

Value: **Show Value** ▼

Units:

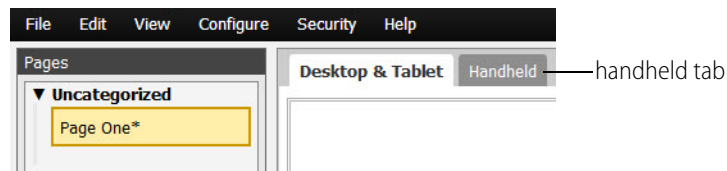
Precision: **2**
Limits: 0 to 6

Continual:

Confirm:

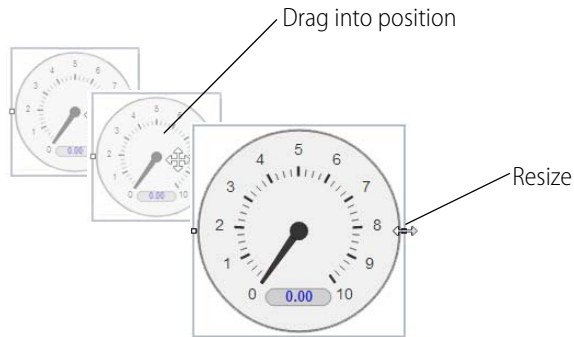
Color: ■

3. Click the Handheld tab at the top of the work area.



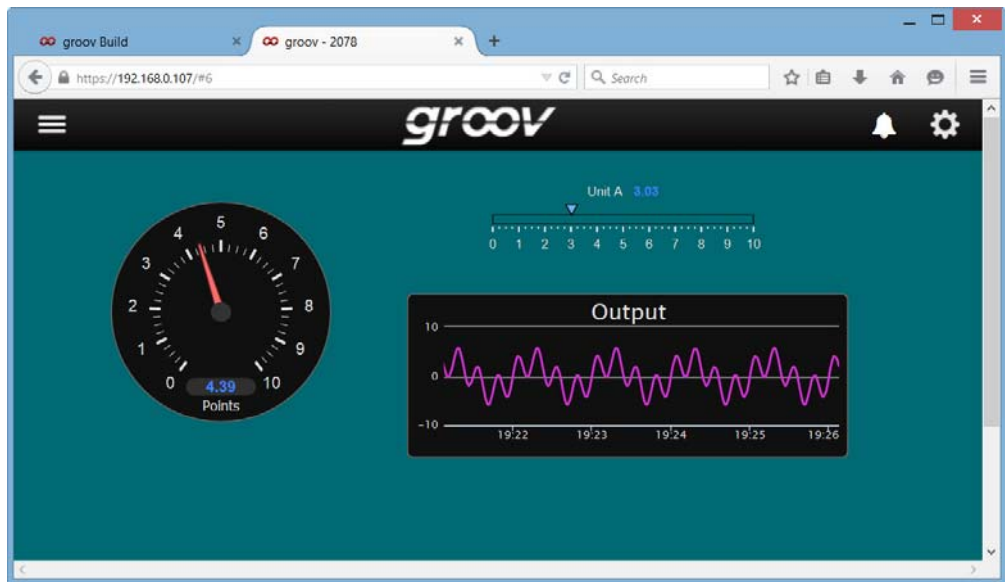
You'll notice that the gadgets are arranged differently in the Handheld view, but both views contain exactly the same gadgets, tags, and properties.

4. Drag each gadget into position, and resize it as necessary for the Handheld view.

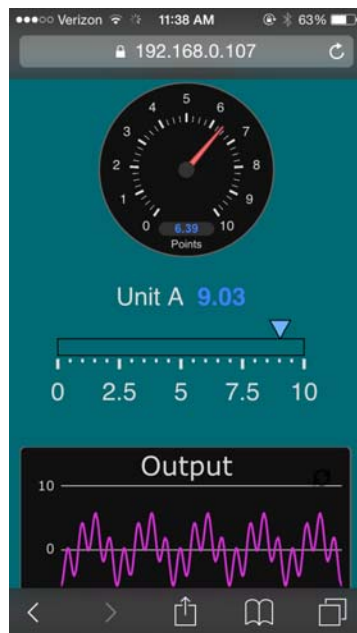


5. Switch to the Desktop & Tablet layout. You'll notice that arranging the gadgets in the Handheld layout does not affect the Desktop & Tablet layout.
6. Select File > Save All Changes and Switch to *groov* View.

Your completed operator interface might look something like this:



After you have arranged the Handheld layout, the same project viewed on a handheld device might look like this:



2: Using an SSL Certificate

groov uses an SSL certificate to encrypt communications and prove *groov*'s identity to client browsers. An SSL 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 is always encrypted.

Here's a comparison of the certificate types:

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

If you are using a **self-signed certificate**, see ["Using a Self-Signed Certificate"](#) on page 16.

If you are using a **CA-signed certificate**, see ["Using a CA-Signed Certificate"](#) on page 22.

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 create and install a self-signed certificate:

[“Step 1: Create a Self-Signed Certificate and Private Key” on page 16](#)

[“Step 2: Add the Self-Signed Certificate to the Browser Trust Store on Client Computers” on page 18](#)

[“Step 3: Install a SSL Certificate on Mobile Devices” on page 21](#)

Step 1: Create a Self-Signed Certificate and Private Key

Follow the steps below to generate the following components required to configure self-signed certificate SSL communication.

- **Private Key:** This must be kept secret and never shared. Keep a copy of it in a safe and secure place.
- **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* Server.

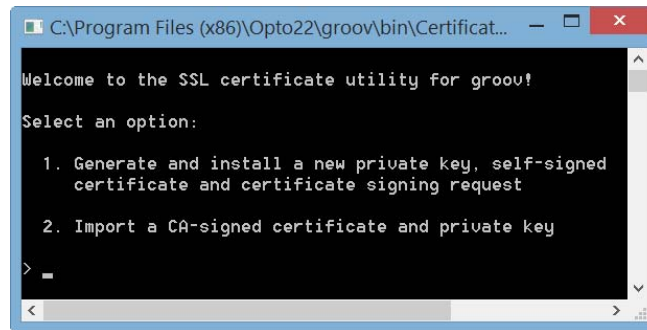
Creating a self-signed certificate also generates in the *groov* folder a certificate-signing request (.csr) file that you can use to get an SSL certificate from a Certificate Authority. See [“Using a CA-Signed Certificate” on page 22](#).

NOTE: You must have administrator privileges to use the SSL Certificate utility.

To generate a private key and self-signed certificate:

1. On the computer where *groov* Server is installed, do one of the following:
 - For Windows 7 and Windows Server 2008, choose Start > All Programs > Opto 22 > groov > groov SSL Certificate.
 - For Windows 8, click the *groov* SSL Certificate utility metro tile.
 - For Windows Server 12, navigate to the directory where *groov* was installed (C:\Program Files (x86)\Opto22\groov, by default). The SSL Certificate Utility is in the “bin” folder. Start the utility.

The utility opens in a DOS window.



2. Enter 1 and press RETURN.
3. Enter the information requested by the onscreen instructions, including the following.

Server Name—Enter the fully qualified hostname of this *groov* Server that client browsers will use to access *groov* (i.e. the hostname and domain name, such as *mobilehmi.mydomain.com*.) The server name may contain letters a–z (case insensitive), digits 0–9, or a hyphen (-). No other characters are allowed. The server name must not start with a hyphen.

Example:

If the URL you will use to access *groov* in client browsers is

<https://process1.acme.com>

enter `process1.acme.com`

Example:

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

<https://mobilehmi.mydomain.com>

enter `mobilehmi.mydomain.com`

Department: Use this field to differentiate between divisions within an organization. For example, “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. The listed organization must be the legal registrant of the domain name in the certificate request. If you are enrolling as a small business or sole proprietor, please enter the certificate requester’s name in this field, and the DBA (doing business as) name in the Organizational Unit field.

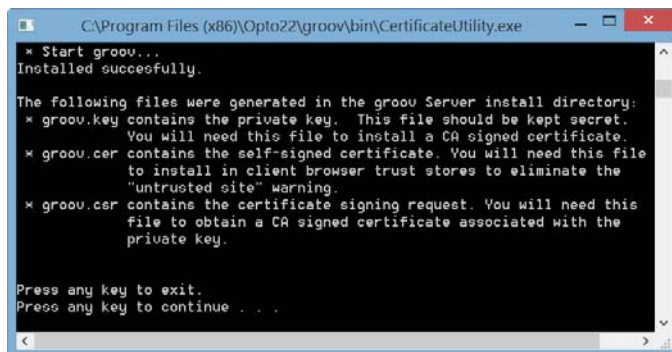
City or Location: Name of the city or locality where your organization is located. Please spell out the name of the city or locality. Do not abbreviate.

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

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

Days until expiration: Enter the number of days before the certificate is expired and has to be replaced. We recommend 3560 (10 years).

The utility will stop *groov* Server, install the new private key and certificate, and then restart *groov* Server. When successful, the following message appears.



```

C:\Program Files (x86)\Opto22\groov\bin\CertificateUtility.exe
* Start groov...
Installed successfully.

The following files were generated in the groov Server install directory:
* groov.key contains the private key. This file should be kept secret.
  You will need this file to install a CA signed certificate.
* groov.cer contains the self-signed certificate. You will need this file
  to install in client browser trust stores to eliminate the
  "untrusted site" warning.
* groov.csr contains the certificate signing request. You will need this
  file to obtain a CA signed certificate associated with the
  private key.

Press any key to exit.
Press any key to continue . . .

```

The following files are created and placed in the directory where *groov* was installed (C:\Program Files (x86)\Opto22\groov, by default).

- **groov.key** (private key)
- **groov.cer** (self-signed certificate)
- **groov.csr** (certificate signing request)

4. Press any key to exit.

Step 2: Add the Self-Signed Certificate to the Browser Trust Store on Client Computers

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 step describes how to add the self-signed certificate on a computer. See the section below for the client computer's operating system.

["Windows" on page 18](#)

["OS X" on page 20](#)

If you want to add a self-signed certificate on a mobile device, see [Step 3](#).

Windows

Internet Explorer & Chrome

1. In Windows file explorer, browse to the *groov.cer* file you created previously. See ["Step 1: Create a Self-Signed Certificate and Private Key" on page 16](#)).

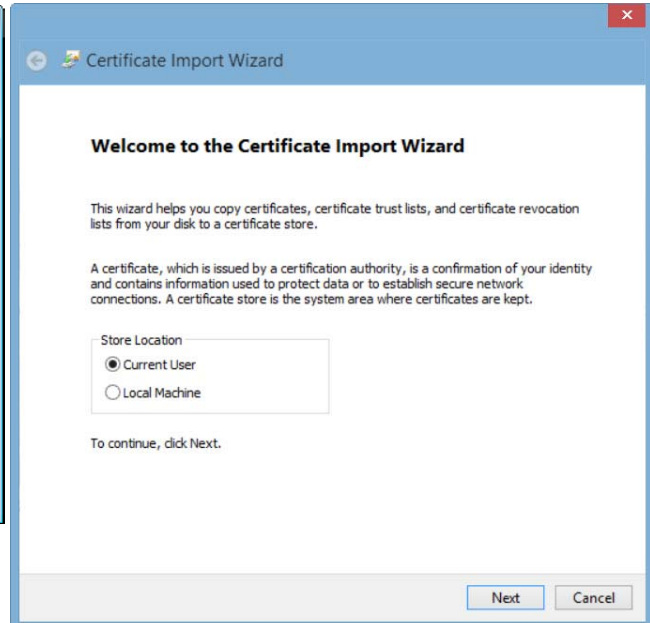
This file is available in the directory where *groov* was installed (C:\Program Files (x86)\Opto22\groov, by default).

2. Right-click on the certificate file *groov.cer* and choose Install Certificate to open the Certificate Import Wizard.

Windows 7



Windows 8



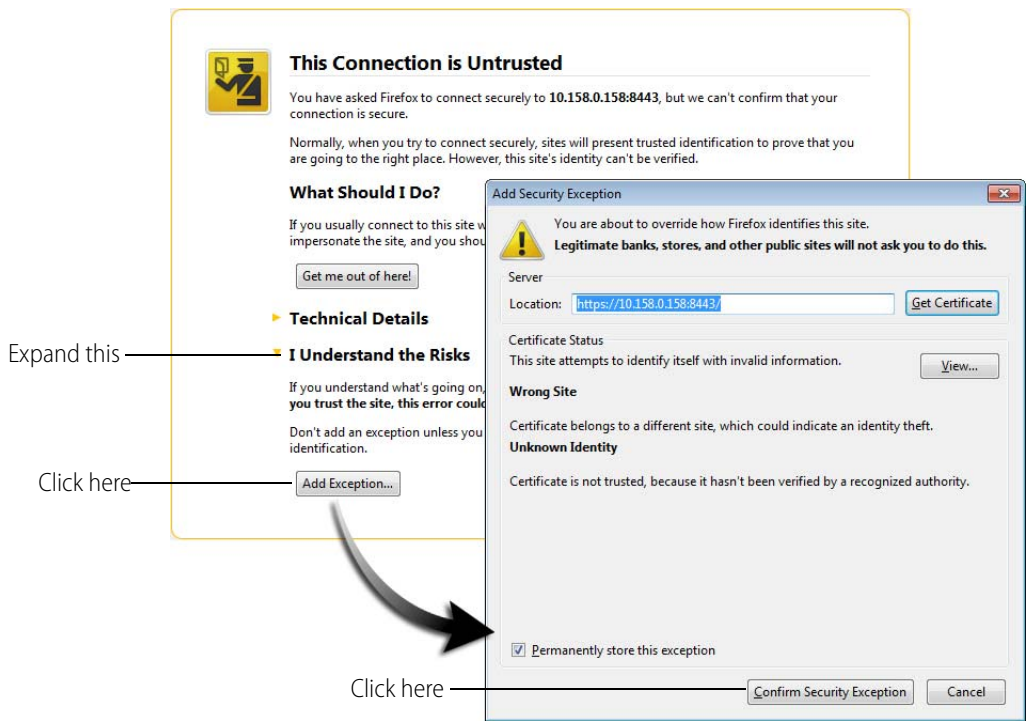
3. (*Windows 8 only*) If you are administrator of local machine, choose the Local Machine certificate store so this certificate will be trusted by all user accounts. Otherwise it will only be trusted by the current user account.
4. Click Next.
5. Select "Place all certificates in the following store."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

Firefox

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

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

5. Click Confirm Security Exception.

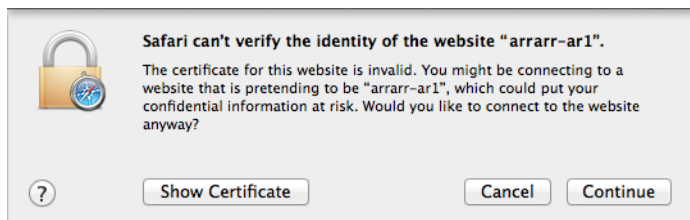


6. To verify the certificate was installed correctly, open Firefox and enter the hostname specified on the certificate. If the browser does not generate an untrusted site warning, the certificate was installed correctly.

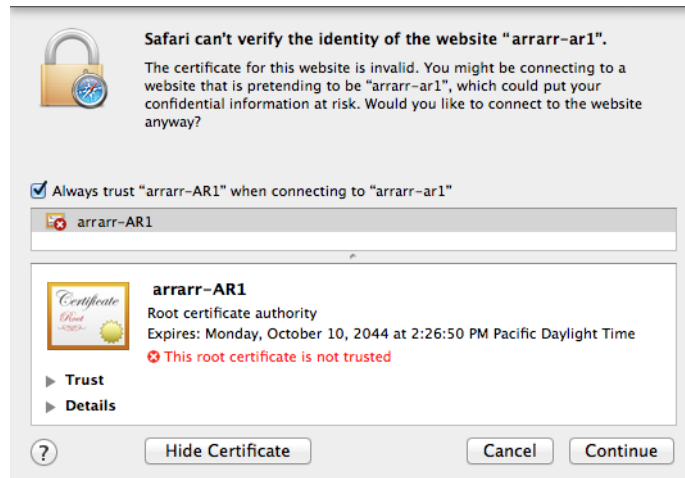
OS X

Safari and Chrome

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



2. Click Show Certificate to reveal the full details:



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

Step 3: Install a 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 or third-party SSL certificate. See the section below for the device’s operating system.

- “iOS Devices” on page 21
- “Android Devices” on page 22

iOS Devices

1. Email the *groov.cer* file you created previously (see “Step 1: Create a Self-Signed Certificate and Private Key” on page 16) to an email account accessible from iOS.
This file is available in the directory where *groov* was installed (C:\Program Files (x86)\Opto22\groov, by default).
2. On the iOS device, open the email message containing *groov.cer*.
3. Tap on *groov.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 *groov.cer* file you created previously (see [“Step 1: Create a Self-Signed Certificate and Private Key” on page 16](#)) to an email account accessible from Android.

This file is available in the directory where *groov* was installed (C:\Program Files (x86)\Opto22\groov, by default).

2. On the Android device, open the email and click the *groov.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

If *groov* is installed on a network that is exposed to the Internet, Opto 22 strongly recommends obtaining an SSL certificate from a third-party vendor called a certificate authority. When installed on *groov* and the devices that access *groov*, the certificate validates the connection between the user and *groov* Server, and it alerts users if they are re-directed to another *groov* Server on a different network.

So long as you stay connected directly to *groov* on a secure connection (using https) you are protected from a man-in-the-middle attack.

The cost of a certificate from a certificate authority ranges from free to \$300 or more, depending on the features and company you buy them from. Please work with your IT department if you choose this option.

Creating a self-signed certificate generates in the *groov* folder a certificate-signing request (.csr) file that you can use to get an SSL certificate from a Certificate Authority.

NOTE: You must have administrator privileges to use the SSL Certificate utility.

Follow these steps to create a certificate signing request (CSR) and install a CA-signed certificate:

[“Step 1: Create a CSR”](#) (see [page 23](#))

[“Step 2: Obtain a CA-Signed Certificate”](#) (see [page 24](#))

[“Step 3: Install the CA-Signed Certificate on the Computer”](#) (see [page 25](#))

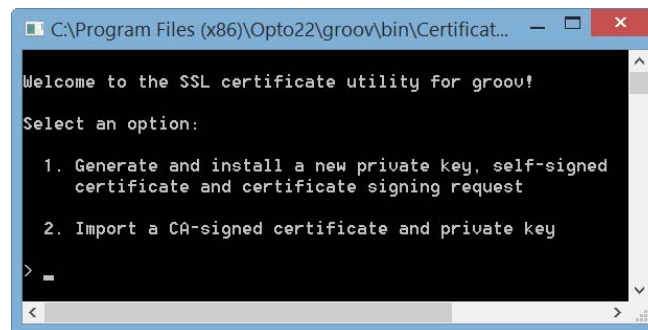
Step 1: Create a CSR

IMPORTANT: This procedure will create and install a new private key on the groov Server.

You will send the 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.

To create a certificate signing request (CSR), you'll use the SSL certificate utility to generate a self-signed certificate. This will also generate the CSR.

1. On the computer where *groov* Server is installed, do one of the following:
 - For Windows 7 and Windows Server 2008, choose Start > All Programs > Opto 22 > groov > groov SSL Certificate.
 - For Windows 8, click the *groov* SSL Certificate utility metro tile.
 - For Windows Server 12, navigate to the directory where *groov* was installed (C:\Program Files (x86)\Opto22\groov, by default). The SSL Certificate Utility is in the “bin” folder. Start the utility. The utility opens in a DOS window.



2. Enter 1 and press RETURN.
3. Enter the information requested by the onscreen instructions, including the following.

Server Name—Enter the fully qualified hostname of this *groov* Server that client browsers will use to access *groov* (i.e. the hostname and domain name, such as *mobilehmi.mydomain.com*.) The server name may contain letters a–z (case insensitive), digits 0–9, or a hyphen (-). No other characters are allowed. The server name must not start with a hyphen.

Example:

If the URL you will use to access *groov* in client browsers is

<https://process1.acme.com>

enter process1.acme.com

Example:

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

<https://mobilehmi.mydomain.com>

enter mobilehmi.mydomain.com

Department: Use this field to differentiate between divisions within an organization. For example, “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. The listed organization must be the legal registrant of the domain name in the certificate request. If you are enrolling as a small business or sole proprietor, please enter the certificate requester's name in this field, and the DBA (doing business as) name in the Organizational Unit field.

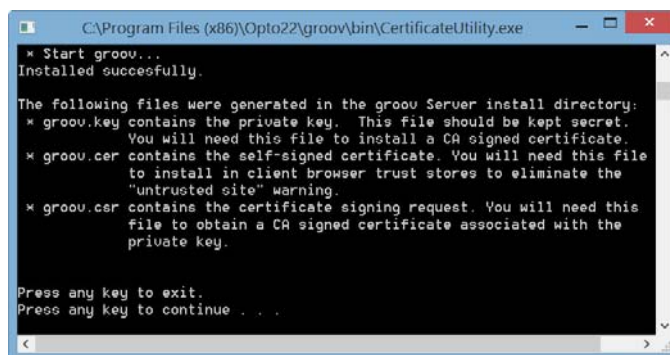
City or Location: Name of the city or locality where your organization is located. Please spell out the name of the city or locality. Do not abbreviate.

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

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

Days until expiration: Enter the number of days before the certificate is expired and has to be replaced. We recommend 3560 (10 years).

The utility will stop *groov* Server, install the new private key and certificate, and then restart *groov* Server. When successful, the following message appears.



```

C:\Program Files (x86)\Opto22\groov\bin\CertificateUtility.exe
* Start groov...
Installed successfully.

The following files were generated in the groov Server install directory:
* groov.key contains the private key. This file should be kept secret.
  You will need this file to install a CA signed certificate.
* groov.cer contains the self-signed certificate. You will need this file
  to install in client browser trust stores to eliminate the
  "untrusted site" warning.
* groov.csr contains the certificate signing request. You will need this
  file to obtain a CA signed certificate associated with the
  private key.

Press any key to exit.
Press any key to continue . . .

```

The following files are created and placed in the directory where *groov* was installed (C:\Program Files (x86)\Opto22\groov, by default).

- **groov.key** (private key)
- **groov.cer** (self-signed certificate)
- **groov.csr** (certificate signing request)

4. Press any key to exit.

Step 2: Obtain a CA-Signed Certificate

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 computer where *groov* Server for Windows is installed.

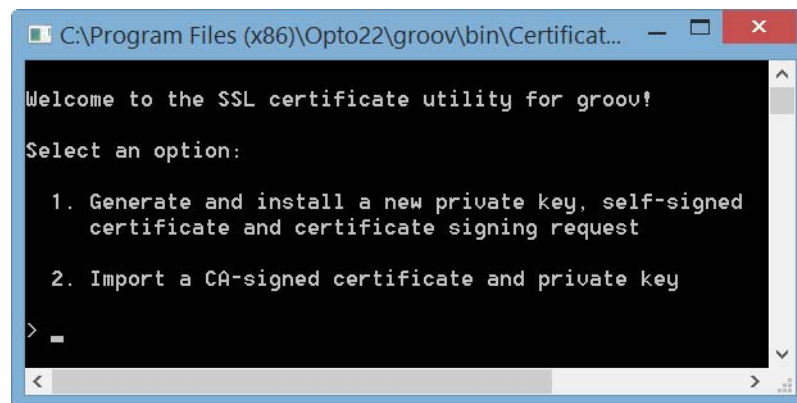
When you apply for an SSL certificate from a certificate authority, you will need to send them a Certificate Signing Request (CSR). If you have not yet created a CSR file, see “[Step 1: Create a CSR](#)” on [page 23](#).

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. Provide the text to the certificate authority in whatever form they require, whether it’s a text file or just text pasted into a text field.
2. Finish the transaction with the certificate authority and receive your new SSL certificate.

Step 3: Install the CA-Signed Certificate on the Computer

1. On the computer where *groov* Server is installed, do one of the following:
 - For Windows 7 and Windows Server 2008, choose Start > All Programs > Opto 22 > groov > groov SSL Certificate.
 - For Windows 8, click the *groov* SSL Certificate utility metro tile.
 - For Windows Server 12, navigate to the directory where *groov* was installed (C:\Program Files (x86)\Opto22\groov, by default). The SSL Certificate Utility is in the “bin” folder. Start the utility. The *groov* SSL Certificate utility opens in a DOS window.



2. Enter 2 and press RETURN.
The following message appears.

```
Sometimes the CA signed certificate is signed with an intermediate
certificate instead of a root certificate. In this case all
intermediate certificates in the chain of trust between your
certificate and the root certificate should be gathered into
one chain file and installed on groov Server.
Install a chain file? [y/n]: _
```

3. If you are unsure, enter *n*.
A prompt says, “Provide the path and file name of the private key file.”
4. Enter the path and file name of the *groov.key* file if it’s the currently installed key.
A prompt says, “Provide the path and file name of the certificate file.”

5. Enter the path to the CA-signed certificate file.

For example, `C:\Certificates\sub.class1.server.ca.pem`

When the operation has finished, a message says "Installed successfully."

3: Maintenance and Troubleshooting


Starting and Stopping *groov* Server

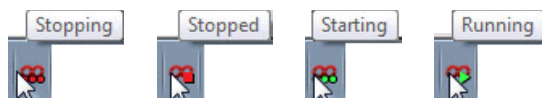
groov Server must be running on the Windows computer where it's installed in order for anyone on any device to use *groov* for building or viewing operator interfaces.

If you need to stop *groov* Server or start it again, you can use the Windows control panel or *groov* Monitor. *groov* Monitor is a utility that starts with *groov* Server but runs independently from the service and lets you see information about it.

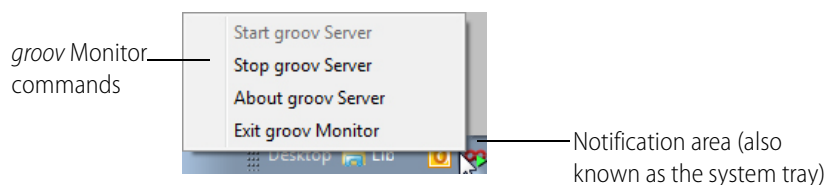
NOTE: You must have administrator privileges to use groov Monitor.

To use *groov* Monitor:

1. In the Windows notification area of the taskbar, find the *groov* Monitor icon . (If you don't see it, click the Show Hidden Icons arrow.)
2. To check whether *groov* Server is running or stopped, look at the icon or hover over it.



3. For other options, right-click the icon. Use the commands as follows:



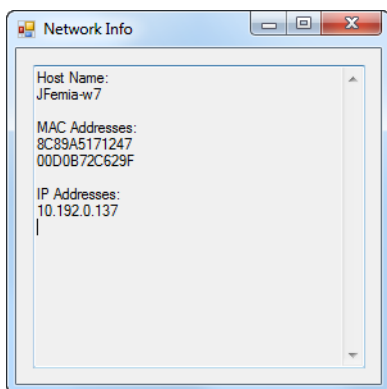
Start groov Server starts the *groov* Server service.

Stop groov Server stops the *groov* Server service.

About groov Server shows *groov* Server's version number and other information.



Click **Network Info** to see hostname, MAC addresses, and other information helpful for using *groov*:



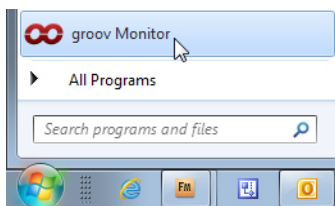
Host Name—Typically part of the URL when you access *groov* from another computer or from a tablet or smartphone. You open a web browser and type `https://` plus this hostname.

MAC Address—Use one of these to get your *groov* Server License File, which is required to use *groov*. See steps on [page 2](#).

IP Address—If your network does not use hostnames, you may access *groov* from another computer/tablet/smartphone by opening a web browser and typing `https://` plus the IP address.

Exit groov Monitor closes *groov* Server Monitor and the icon disappears. Exiting *groov* Server Monitor does *not* affect the *groov* Server service. If the service is running, it will continue to run after you exit Monitor.

To start *groov* Server Monitor again, click “groov Monitor” in the Windows Start menu.

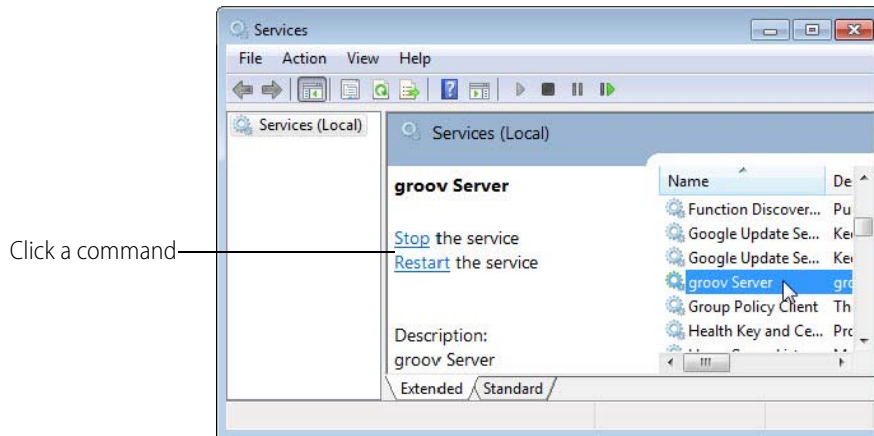


If *groov* Server is stopped, starting the monitor will *not* start the service. To start the service again, use *groov* Monitor’s Start command.

You can also stop, start, or restart *groov* Server in the Windows control panel:

1. Open the Windows Control Panel and click Administrative Tools.
In Windows 7, if the control panel is viewed by category, Administrative Tools is in the System and Security group.
2. Double-click Services.
3. Select *groov* Server.

4. Click the command you want to use.



Changing and Opening the *groov* SSL Port

By default *groov* communicates on port 443. If 443 is not available, 8443 is used.

Changing the *groov* Port

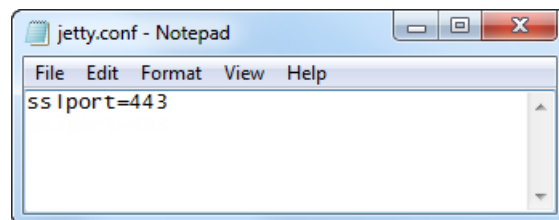
If you want to change the SSL port number, first consult with your IT manager. If you change the port, you will need to use the following format when connecting to *groov* Server:

`https://localhost:port`

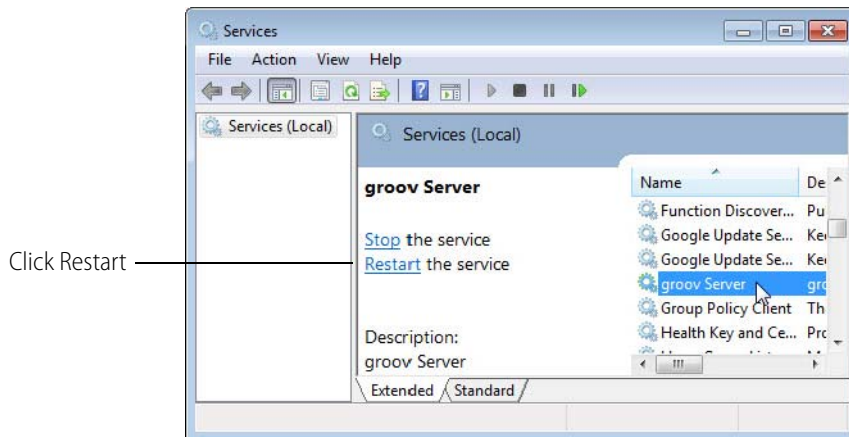
where *port* is the new port number. For example if the new port number is 888, you enter `https://localhost:888`

To change the SSL port, do the following steps:

1. In Notepad or a similar program, open the `jetty.conf` file installed on the *groov* Server computer. Find the file in the directory where *groov* was installed (C:\Program Files (x86)\Opto22\groov\jetty, by default).



2. Change only the port number.
3. Save and close the file.
4. Restart *groov* Server:
 - a. Open the Windows Control Panel and click Administrative Services.
 - b. Select *groov* Server.
 - c. Click Restart.



Manually Opening Ports

When you install *groov* Server, you're given the option to have the *groov* SSL port 443 opened automatically. If you didn't choose this option, you'll need to open the port manually. Steps may vary depending on your version of Windows.

1. On the computer where *groov* Server is installed, choose Start > Control Panel > Windows Firewall.
2. Click Advanced Settings.
3. Create an Inbound Rule for the Program *groov*. (By default, *groov* is installed in C:\Program Files (x86)\Opto22\groov).
4. Restart *groov* Server (see "[Starting and Stopping groov Server](#)" on page 27).

Getting *groov* Updates

Because you have activated *groov*, you are eligible to receive updates. Updates add new capabilities and fix issues that may arise.

Each *groov* installation is treated independently, so you must activate each one; updates are valid for a specific *groov* installation only.

To install an update, download the update file and then run the installation.

If updates are available, an updates icon appears next to the *groov* logo in the upper-right corner of *groov* Build. Click the updates icon (or select Help > Check for Updates).



The Check for Updates dialog box tells you what kind of updates are available. Follow the onscreen instructions to download an update file or view a list of updates on the latest *groov* readme.

Another way to check for updates is to go directly to manage.groov.com. If there is an update available for your *groov*, download the file. To install an update for *groov* Server for Windows, double-click the downloaded update file and run the installation.

Before updating the application, make sure to save any changes in your project so that they will still be there after the update takes effect.

Erasing Your *groov* Project

If you've forgotten your password and can't login, or if you just want to start your project over again from scratch, you can delete the project as follows. Also see the next section, "[Backing Up and Restoring Your Project](#)."

1. Stop *groov* Server for Windows.
For help, see "[Starting and Stopping groov Server](#)" on page 27.
2. Navigate to the *groov* installation directory.
Usually this is C:\Program Files (x86)\Opto22\groov.
3. Find the project file named *project.grv*.
4. *If you are sure you don't want to keep the project*, delete the project file. Otherwise you should archive the project by moving or renaming the project file.
5. Restart *groov* Server.

Backing Up and Restoring Your Project

You should back up *groov* frequently because there is no automatic backup. During backup, your project is saved to a file on your computer.

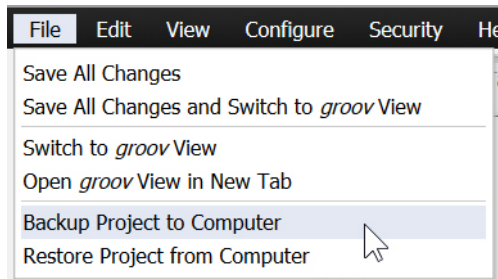
IMPORTANT: Your groov project files are not encrypted or obfuscated in any way. This means that most of the project information (except for groov User passwords) in them can be read, including the following:

- *SMTP account info (including password)*
- *User email accounts (does not include the groov User passwords, which are securely hashed 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.

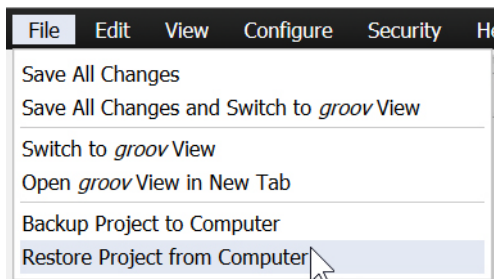
To back up your project, select File > Backup Project to Computer. A backup file is saved to your computer.



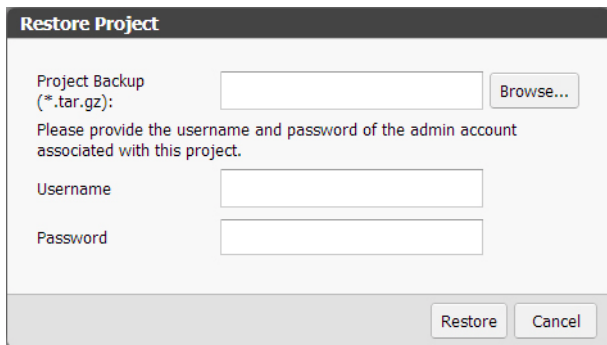
To restore your project from a backup file:

CAUTION: Only restore your project if you have to. You will lose all work done since the last backup, and all users will be logged out.

1. Select File > Restore Project from Computer.

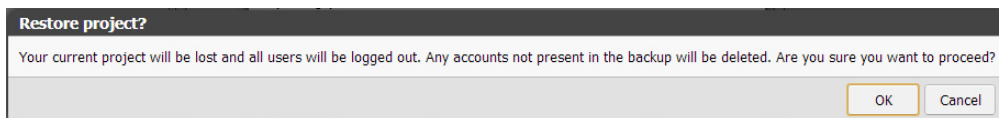


2. In the Restore Project dialog box, browse to the Windows Download directory to locate the tar.gz backup file.



3. Enter the username and password for the Admin account.
4. Click Restore.

The following warning appears.




5. If you are sure you want to proceed, click OK.

When the restoration process is complete, the restored project opens in *groov* View.

Troubleshooting

groov Server doesn't start

groov Server normally starts as soon as it is installed, even though no window opens. Check to see if the *groov* Monitor icon  is in the system tray. (If you don't see it, click the Show Hidden Icons arrow.) Hover over the icon with your mouse to see *groov* Server status.

If status shows "Stopped," right-click the icon and choose Start *groov* Server from the popup menu. If the status shows "Running," try stopping *groov* and then starting it again.

If you can't find the icon, from the Start menu choose "groov Monitor." See ["Starting and Stopping groov Server" on page 27](#) for more information.

If *groov* Server fails to start, there might be a conflict with another service running on your computer. In this case, you might need to change the SSL port *groov* Server uses to run. To change the port number, first consult with your IT manager, and then follow steps in ["Changing the groov Port" on page 29](#).

The following command can be run at a command prompt to see what application (if any) is listening on port 443:

```
netstat -a -n -p tcp -b
```

Cannot read or write to a Modbus/TCP device OR the data doesn't make sense

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

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

Problems with *groov* Build or *groov* View

See the Troubleshooting chapter in the [groov Build and View User's Guide](#). To open the user's guide in *groov* Build, choose it from the Help menu.

For Help

Product support for *groov* Server is free. See ["For Help" on page 2](#) for contact information.

