groov EPIC SECURITY DESIGN AND BEST PRACTICES

Opto 22's *groov* EPIC® system was designed from the ground up to help you build a secure system for gathering, processing, and sharing useful data from industrial equipment. In fact, no other industrial real-time controller currently on the market offers the same level of cyber security features and options.

For all digital systems, security is a complex issue with different implications depending on your organization and your system. Security requirements constantly change as your system evolves, and building security into your system design is key. As Bruce Schneier wrote in 2000, "Security is a process, not a product."

To address security's complex, changing nature, you need to understand security risks, understand your environment, and understand the security tools you have to work with. Security experts recognize several elements of system security, including physical security, policies and procedures, and network security. We designed *groov* EPIC to address network security requirements as a primary goal.

Our objective was to give you the tools and methods necessary to make this system as secure as possible from a network access standpoint, while maintaining the flexibility you need for a variety of implementations. The ultimate security of your system depends on you.

> **"Security is a process, not a product."**
>
> **- Bruce Schneier**

This technical note describes the security features built into *groov* EPIC and lists best practices for setting up a secure *groov* EPIC system.

For Help

As always, if you are using *groov* EPIC and cannot find the help you need in this technical note or in the *groov EPIC User's Guide* (form 2267), contact Opto 22 Product Support. Product support is free.

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.

groov EPIC SYSTEM DESIGN AND DEFAULT CONFIGURATION

Let's look at *groov* EPIC's security design and defaults in the following areas:

- Operating system
- Network interfaces
- Networking tools
- Firewalls
- Accounts

- Security certificate management
- Data communication options
- Additional security design for developers

Operating system

Unlike the traditional controllers and computers typically used in automation or industrial internet of things (IIoT) applications, *groov* EPIC processors have an open-source Linux® operating system. Contrary to what you might think, an open-source OS is in many ways more secure than a closed one (especially a well-known and often-attacked OS such as Microsoft® Windows®).

First, *groov* EPIC includes only the operating system components necessary for its purpose, which reduces attack vectors. Contrast this limited vulnerability with Windows, for example, which includes components for all kinds of purposes. "The easiest vulnerability to address is the one you don't include," noted Ryan Ware, Security Architect at Intel®, in 2017.

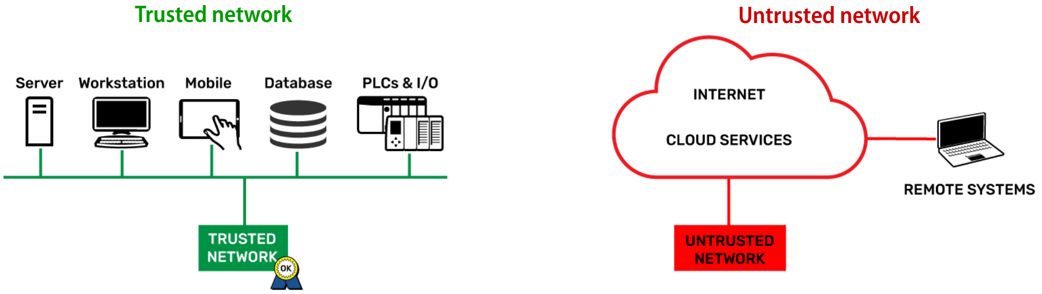
Second, open source means crowd sourced. Because of the number of developers working on Linux, vulnerabilities tend to be addressed very quickly—far more quickly than they can be at an individual software company with a limited number of developers.

Third, and most important, the Opto 22 Yocto build of EPIC Linux is **cryptographically signed** with the Opto 22 Private Key. That means that any firmware or software package a hacker might try to upload to the EPIC processor will not be accepted; only firmware and packages that are Opto 22 cryptographically signed can be loaded.

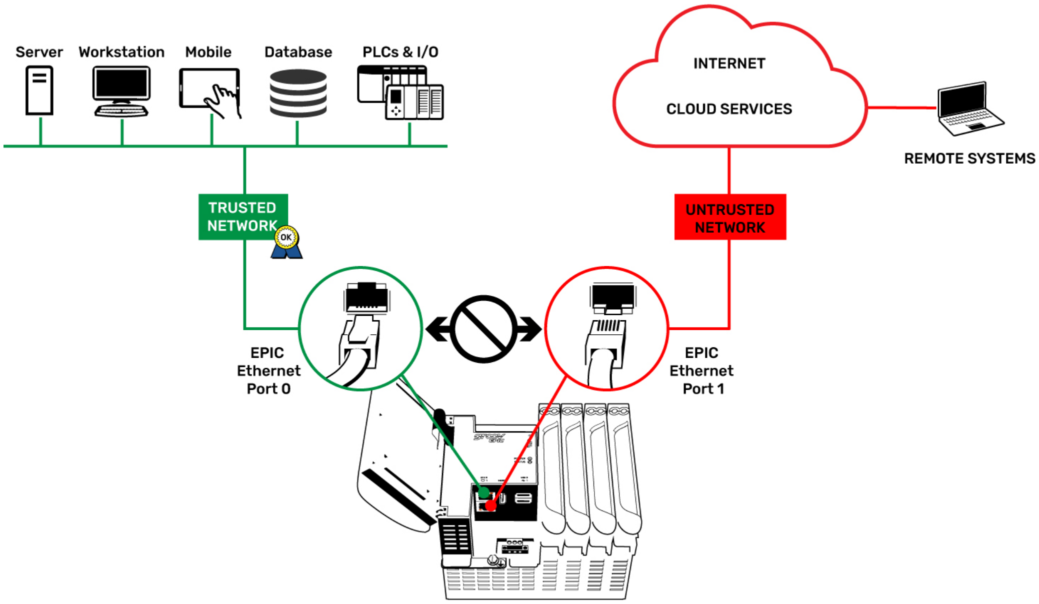
Network interfaces

groov EPIC includes two independent Ethernet interfaces that segment trusted networks (ETH0) from untrusted networks (ETH1).

- A **trusted network** is any network where you know exactly who has access to it, for example, an IT-managed corporate network.
- An **untrusted network** is any network where you don't know who has access to it, like the internet.



groov EPIC is not a router, which functions to join two networks together. Instead, *groov* EPIC keeps your trusted network isolated from your untrusted network by **not routing** network traffic **between** its network interfaces.

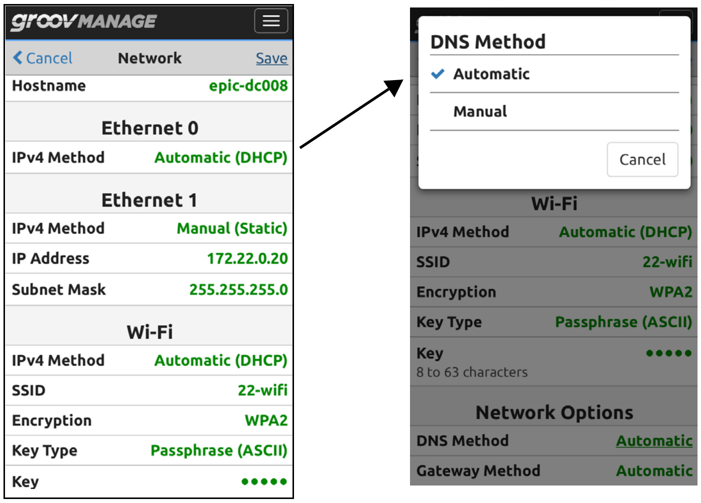


In addition, you can add a WiFi network (a WLAN) to *groov* EPIC using an approved USB WiFi adapter connected to the EPIC processor's USB port. (For more information on approved adapters, see the *groov EPIC User's Guide*.) The wireless network interface is independent from both Eth0 and Eth1, and again, EPIC does not route network traffic between any of its network interfaces.

Networking tools

On all network interfaces, *groov* EPIC uses standard network services like DHCP. It can be configured to use optional static IP configurations, if necessary, but the default is DHCP and DNS.

For name resolving and outbound, device-originating access to other networks, you can use *groov* Manage to choose standard DNS and Gateway addresses and automatic or manual configuration.



Network

Hostname	epic-dc008

Ethernet 0

IPv4 Method	Automatic (DHCP)

Ethernet 1

IPv4 Method	Manual (Static)
IP Address	172.22.0.20
Subnet Mask	255.255.255.0

Wi-Fi

IPv4 Method	Automatic (DHCP)
SSID	22-wifi
Encryption	WPA2
Key Type	Passphrase (ASCII)
Key	●●●●●

DNS Method

✓ Automatic

Manual

Wi-Fi

IPv4 Method	Automatic (DHCP)
SSID	22-wifi
Encryption	WPA2
Key Type	Passphrase (ASCII)
Key 8 to 63 characters	●●●●●

Network Options

DNS Method	Automatic
Gateway Method	Automatic

Firewalls

Firewalls are critical in securing data communications. The *groov* EPIC processor has its own configurable firewall, which is critical in addressing security for the system.

Generally speaking, firewalls help provide security by stopping unsolicited traffic from accessing your network or device/host. Typically the only traffic they allow through is responses to traffic that originated from the inside. Device-originated connections are considered trustworthy because their origin is known.

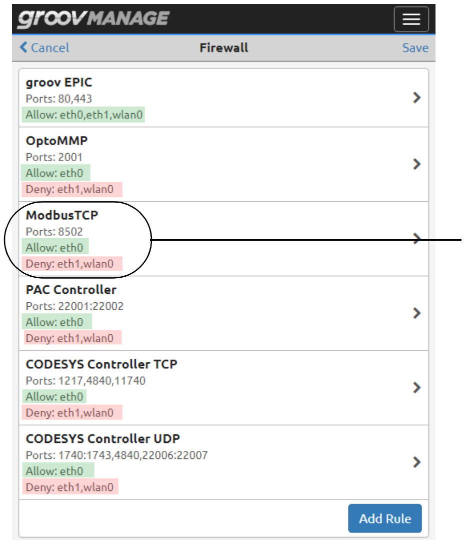
Most firewalls—including corporate firewalls (*network* firewalls) and the firewall in *groov* EPIC (a *device* or *host* firewall)—permit devices or services behind the firewall to originate communications outbound to external servers or services. At the same time, these firewalls generally block all inbound connection attempts originating from devices and services outside the firewall. However, a firewall may allow inbound connections when a specific port has been configured *open* to allow them.

EPIC default firewall configuration

The EPIC processor's **internal firewall** default configuration assumes that you are using the two wired network interfaces as designed to segment trusted and untrusted networks:

- On the Ethernet **trusted** network interface (**ETH0**), *groov* EPIC allows network communications through necessary but unsecure industrial protocol ports that are configured *open*. These ports allow communication with software and protocols in the EPIC processor, for example:
  - PAC Control™ and CODESYS® (development tools)
  - OptoMMP (protocol used by the EPIC's I/O)
  - Modbus®/TCP and Ignition Edge® Designer (for communication with PLCs and other devices)
- On the Ethernet **untrusted** network interface (**ETH1**), *groov* EPIC opens secure port 443 and permits only authenticated access over secure, encrypted connections. This network interface provides authenticated, encrypted access to *groov* Manage, *groov* View, and RESTful APIs.
- All other inbound connection ports on the ETH1 Ethernet network interface are **blocked by default**.

In *groov* Manage the configuration for each network interface is shown by application, so you can clearly see which applications are allowed access and which are denied:



groov EPIC
Ports: 80,443
Allow: eth0,eth1,wlan0

OptoMMP
Ports: 2001
Allow: eth0
Deny: eth1,wlan0

ModbusTCP
Ports: 8502
Allow: eth0
Deny: eth1,wlan0

PAC Controller
Ports: 22001:22002
Allow: eth0
Deny: eth1,wlan0

CODESYS Controller TCP
Ports: 1217,4840,11740
Allow: eth0
Deny: eth1,wlan0

CODESYS Controller UDP
Ports: 1740:1743,4840,22006:22007
Allow: eth0
Deny: eth1,wlan0

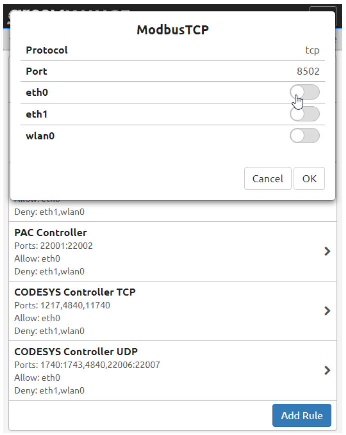
Default configuration by application for trusted Eth0 and untrusted Eth1 network interfaces

Note: Port 80 is open, but all traffic is automatically redirected to secure port 443.

For example, Modbus/TCP is allowed by default on trusted Eth0 but denied on untrusted interfaces.

Remember that the default configuration assumes that ETH0 is on a trusted network. Make sure that network actually is trusted.

You can configure the EPIC's firewall for each network interface to suit your application. For example, you can change the default configuration to close ports for any services that won't be used. In the example below, if you are not using Modbus/TCP, you can close port 8502 so it will not allow any traffic, even on the trusted network interface:



ModbusTCP

Protocol	tcp
Port	8502
eth0	○
eth1	○
wlan0	○

Deny: eth1,wlan0

PAC Controller
Ports: 22001:22002
Allow: eth0
Deny: eth1,wlan0

CODESYS Controller TCP
Ports: 1217,4840,11740
Allow: eth0
Deny: eth1,wlan0

CODESYS Controller UDP
Ports: 1740:1743,4840,22006:22007
Allow: eth0
Deny: eth1,wlan0

You can (and should) close unused ports for greater security.

Clients and servers

Note that *groov* EPIC can act as both a client (a device that originates connections) and a server (a device that listens for requests to connect). Firewall configuration varies based on how the EPIC acts. For example:

- MQTT and Node-RED running on EPIC are clients that originate communications. MQTT originates communications to MQTT brokers, and Node-RED originates communications to SQL servers, cloud-based services, and so on. No firewall configurations are needed for MQTT or Node-RED. Their communications are outbound and by default are allowed by the EPIC's firewall. (See more about MQTT on page 7.)
- *groov* View running on EPIC is a server that listens for connection requests from PCs or mobile devices running browsers. By default, the EPIC's firewall is configured to open the secure port used for *groov* View to allow incoming connections. These connections are encrypted and must be authenticated by users.

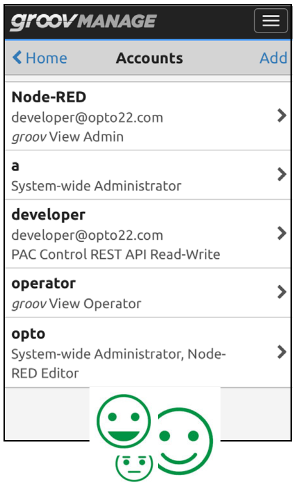
Whether EPIC acts as a client or a server, once communications are established, data can flow in both directions as long as the connection is active.

Accounts

When you first start *groov* EPIC, you must create an administrator account with your own username and password before you can do anything else. The EPIC processor does not have a default username or password that someone might be able to guess. The administrator account credentials you create are *not recoverable*.

groov EPIC provides **user account management** through *groov* Manage. You can create administrator, developer, operator, REST API, and other accounts, and then assign those user rights to authorized people or software services. Authentication (over an encrypted connection) is by either username/password or API token.

All users can create long, complex passwords consisting of numbers, capitalization, punctuation, spaces, phrases and words in any language, and even emoticons.



Node-RED
developer@opto22.com
groov View Admin

a
System-wide Administrator

developer
developer@opto22.com
PAC Control REST API Read-Write

operator
groov View Operator

opto
System-wide Administrator, Node-RED Editor

LDAP (lightweight directory access protocol)

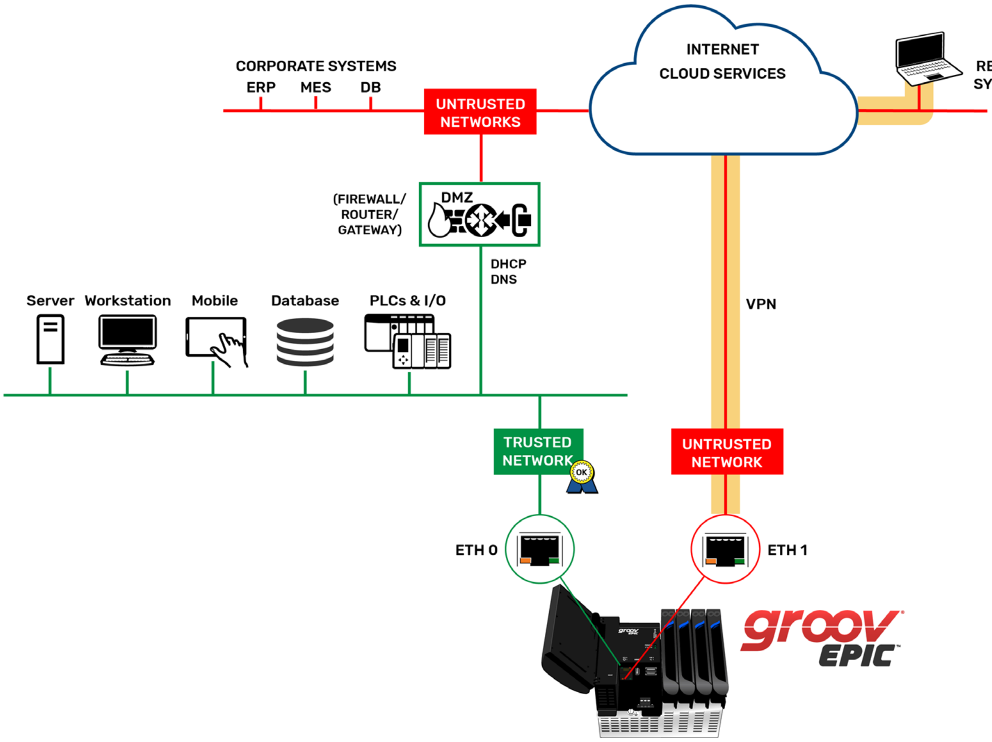
If your site manages user IDs through an LDAP service, you can work with your IT department to configure your *groov* EPIC in *groov* Manage to **connect to the LDAP server**, authenticate a user, and help determine which services a user can access. For simple setups you can use the LDAP server to authenticate users and give them default local permissions. For systems with a larger number of users or more complex user management, you can use *groov* Manage to map an LDAP group to a specific set of permissions.

NOTE: Your original administrator account for groov EPIC gives you direct, local access to your EPIC and is ***not*** *managed by your LDAP service.*

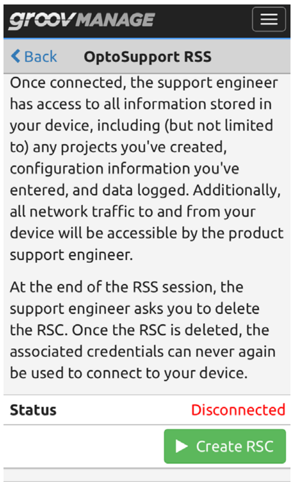
Details on how permissions work and how to assign them are in Chapter 6 of the *groov EPIC User's Guide*.

VPN (virtual private network)

For users who are off site, you can use *groov* Manage to create **secure VPN tunnels** from *groov* EPIC to externally configured OpenVPN servers. An OpenVPN client is included in *groov* EPIC.



You can also create a secure VPN tunnel to Opto 22 Product Support. Suppose you are having concerns about your *groov* EPIC system and contact Product Support for assistance. If you think it would be helpful, you can use *groov* Manage to open a VPN tunnel so that the Product Support Engineer can temporarily access your device and help resolve the issue.



Once connected, the support engineer has access to all information stored in your device, including (but not limited to) any projects you've created, configuration information you've entered, and data logged. Additionally, all network traffic to and from your device will be accessible by the product support engineer.

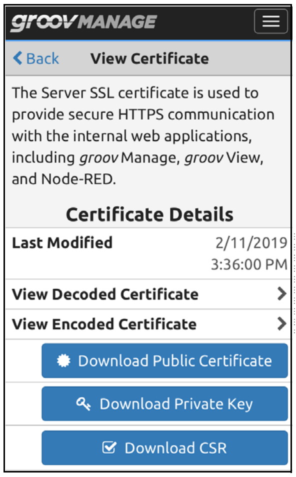
At the end of the RSS session, the support engineer asks you to delete the RSC. Once the RSC is deleted, the associated credentials can never again be used to connect to your device.

Status Disconnected

Security certificate management

groov EPIC provides built-in **certificate management** in *groov* Manage. Certificates are a way that machines can identify themselves to other machines, so that when one machine tries to connect to another, it can be assured it's communicating with the correct machine and not an impostor.

The EPIC system supports X.509 PKI standard certified connections to servers and from clients using SSL certificates, which can be device generated, self-signed, or registered publicly through a Certificate Authority (CA).



The Server SSL certificate is used to provide secure HTTPS communication with the internal web applications, including *groov* Manage, *groov* View, and Node-RED.

Certificate Details

Last Modified 2/11/2019 3:36:00 PM

Data communication options

As we saw in the Firewalls section, a device is inherently more secure and requires less security configuration when it **initiates data communication** on a port, rather than having to open a port to receive connection requests.

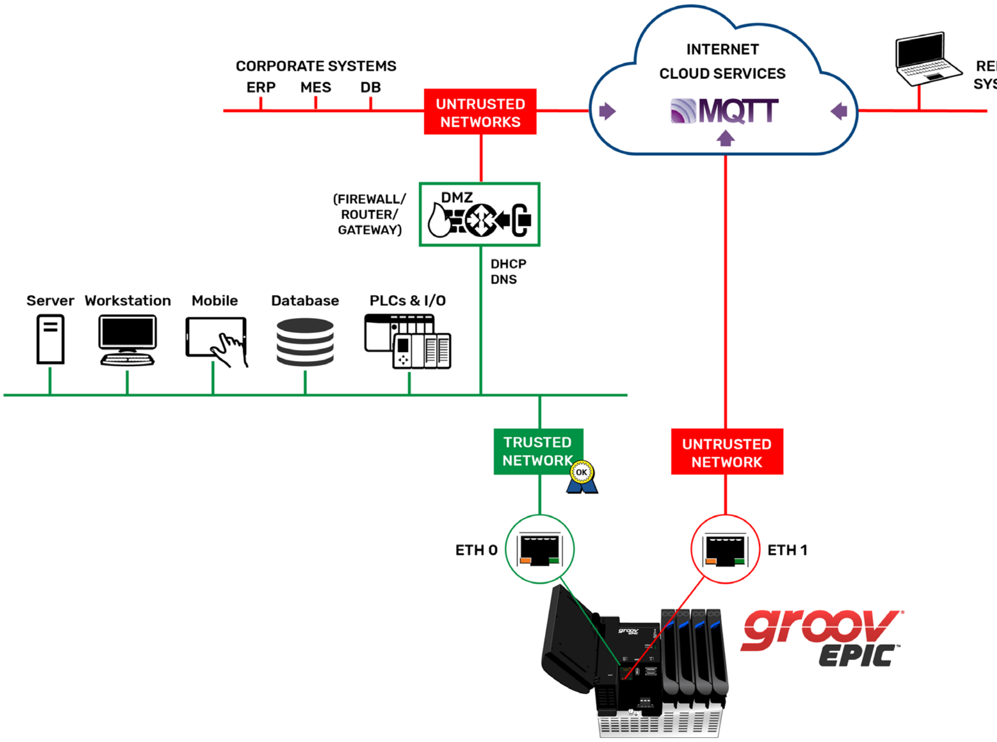
Publish/subscribe (pub/sub) is a communication method that takes advantage of this greater security by using device-originated communications only. *groov* EPIC can use MQTT, a pub/sub protocol, to report status (authenticated and encrypted) to a central broker. Once connected to the broker, the connection persists, so the EPIC can also subscribe to any new commands for it or to status messages from other devices.

Because MQTT data flow is device originating, the firewall allows the data out, keeps track of the session status, and allows any packets coming back from the broker to pass through.

With MQTT, this persistent connection is the critical mechanism for the MQTT broker to determine the state of client connections at all times. In a pub/sub model for SCADA (supervisory control and data acquisition) or industrial communications, you always want to be sure that clients are still connected. If a data publisher's persistent connection is broken, the broker notifies all subscribers about the disconnect so that the state of the system is known to all.

In contrast, in request/response communication, connections do not persist unless the client maintains them. For example, if Node-RED (a client) connects to a SQL server, once data is sent from the client to the server and the server responds, the connection is closed. Subsequent data transfers must be initiated by the client each time. In the example of *groov* View, the client (your browser) keeps the connection open to the server (*groov* View) only as long as the client software is active.

Device-originated communication may be referred to as using an outbound port; when the device must open a port to receive communications originated from outside, it may be called an inbound port. Through outbound, device-originating data communications such as MQTT, *groov* EPIC offers a secure option that requires far less configuration.



Additional security design for developers

The *groov* EPIC system's design gives developers optional **Secure Shell access** (SSH) for developing custom applications, while maintaining security. Again, you have tools in *groov* EPIC to help you design a secure system.

A license is required to activate Secure Shell access (Opto 22 part number GROOV-LIC-SHELL). Once you have the license, you can:

- Manage SSH access and restrict it to the trusted network only.

- Configure specific network interface ports on the *groov* EPIC firewall as required for your custom applications.
- Install cryptographically signed packages from Opto 22's git repository.
- Compile applications, monitor server log files, start and stop applications or services, and facilitate file transfers.

groov EPIC BEST PRACTICES FOR SECURITY

Every situation is different, and as a practitioner, you know best what access your application will need and what network architecture you'll use. However, as mentioned throughout this technical note, *groov* EPIC was designed to help you create a secure system. Based on its design, we strongly recommend the following best practices. Keep these practices in mind as you develop your applications and deploy your projects.

Networks

- Configure your *groov* EPIC to use the ETH0 Ethernet network interface for your trusted network.
- Use ETH1 for any untrusted network. Configure exceptions in the system's firewall only if required for your application.
- Configure the system's firewall in *groov* Manage to close all unneeded network ports on all network interfaces.

Accounts

- Have all your users create long and difficult passwords, and don't write them down anywhere. Consider using a password manager where appropriate.
- If your site uses an LDAP service to manage user IDs, work with your IT department to include *groov* EPIC.
- Use a VPN if you require remote unencrypted network connections over untrusted networks.
- To prevent unauthorized access to the *groov* EPIC processor, always log out of any account that has administrator privileges.
- If you are running your *groov* View HMI on an external monitor, always put it in Kiosk mode so that only *groov* View is accessible.

Other best practices

- If you need a completely closed system (for example, if you are an OEM using *groov* EPIC in your machine), after you have finished development, disable all ports in the firewall and unplug any Ethernet cables.

  If someone attempts to connect an Ethernet cable to the EPIC to try to access the system from their computer, the ports will be closed and network access will be denied. Only an authorized user with administrator privileges can access *groov* Manage through the built-in display to reopen needed ports and gain network access.
- Whenever possible, use authenticated and encrypted outbound, device-originated data connection methods. For example, use MQTT to publish data to an MQTT broker. Device-originated data communication methods help you:
  - Reduce open inbound network ports
  - Eliminate man-in-the-middle exploits
  - Prevent exposing sensitive credentials over the network

Additional best practices for developers

- If you use secure shell, configure SSH access with a unique and difficult username and password, different from *groov* Manage, *groov* View, or any other software running on *groov* EPIC.
- Enable shell access only to configure and program the unit. Once the system is commissioned, disable shell access in *groov* Manage so that no one else can get in. Never leave SSH access enabled once the system is in production.