Rocketeria Remote Access Server

System Administration Guide

[Scope](#_5vx1d2xvespv)

[Basic System & Network Information](#_hq0e7dj4ig14)

[Updating/Patching](#_m2qxlxtx7i2d)

[Operating System Management](#_35ybz6pbv8am)

[Linux User Management](#_kdbatvq6v1sy)

[Allow user root access via sudo](#_raao7tkhz3du)

[Allow user to manage VPN accounts](#_ueafejsgptva)

[OpenVPN Management](#_qf4cw91jqzgk)

[VPN User Management](#_g928ctkxmx1r)

[Add a User](#_386gsqqvt845)

[Providing Client Secrets to Users](#_xmats1tg3gb9)

[Delete a User](#_eah7hdy9xgee)

# Scope

This document provides basic operational information about the remote access server and provides instructions for routine tasks such as updating and managing users. It does not cover the initial configuration process.

# Basic System & Network Information

|  |  |
| --- | --- |
| Hardware: | Raspberry Pi Model B Rev. 2.0 (BCM2708)  ARMv6  512 MB RAM |
| OS: | Raspbian Linux |
| Hostname: | gr3nglar |
| eth0 IPv4: | 192.168.1.6/28 |
| eth0 IPv6: | N/A (v6 disabled) |
| OpenSSH Port: | 22022 |
| OpenVPN Port: | 51194 (UDP) |

# Updating/Patching

Follow the instructions below to install updates. This should be done monthly at a minimum.

1. Log in via console or SSH as a user that is a [member of the sudo group](#_raao7tkhz3du)
2. Issue the following commands:

|  |
| --- |
| sudo apt-get update  sudo apt-get install --only-upgrade -y  reboot |

1. When the system comes back up, log back in
2. Issue the following commands:

|  |
| --- |
| sudo service openvpn status |

1. If the output reads, “[ ok ] VPN 'server' is running.”, updating is complete. If the openvpn service is not running, investigate.

# Operating System Management

## Linux User Management

### Allow user root access via sudo

To grant an existing Linux user full root privileges via sudo, issue the following commands, replacing *user* with the username that should be given privileges:

|  |
| --- |
| sudo usermod -a *user* -G sudo |

### Allow user to manage VPN accounts

To grant an existing Linux user the ability to manage VPN user accounts without granting full root privileges, enter the following commands, replacing *user* with the username that should be given privileges:

|  |
| --- |
| sudo usermod -a *user* -G vpnadmins |

Note that this will not give the user the ability to modify the VPN server configuration or start/stop the VPN process.

# OpenVPN Management

**Important Files**

|  |  |
| --- | --- |
| Configuration: | /etc/openvpn/server.conf |
| PKI: | /etc/openvpn/easy-rsa/ |
| Service Log: | /var/log/openvpn.log |
| Status Monitor: | /etc/openvpn/openvpn-status.log |
| Client IP Mapping: | /etc/openvpn/ipp.txt |

## Routing

The following routes are pushed to clients:

* 192.168.1.0/28

Note that 192.168.1.0/24 is a very common private address range. If a client connects from a 192.168.1.0/*X* network, **they will be unable to access any devices on their local network with addresses between 192.168.1.2 and 192.168.1.15.** This traffic will instead be routed over the VPN and reach devices on the Rocketeria network.

### Client Addressing

VPN clients’ TUN adapters receive addresses in the 10.8.0.0/24 range. The rocketeria network must be configured to use 192.168.1.6 (The VPN server) as the gateway to 10.8.0.0/24 or else return traffic will fail to reach clients.

## VPN User Management

### Add a User

The instructions below detail the process of allowing a new user to log in to the VPN.

1. Log in via console or SSH as a user that is a [member of the vpnadmins group](#_ueafejsgptva)
2. Issue the following commands, replacing *newuser* with the desired VPN username:

|  |
| --- |
| cd /etc/openvpn/easy-rsa/  source vars  ./build-key-pass *newuser* |

1. When prompted for a PEM passphrase, enter a strong password. This password will need to be provided to the new user.
2. When prompted:
   1. Press Enter to accept the default values for Country Name, State or Province Name, Locality Name, Organization Name, Organizational Unit Name, and Common Name.
   2. **When prompted for a Name, do not accept the default value.** Enter the new username.
   3. **When prompted for an Email Address, do not accept the default value.** Enter an email address for the new user.
   4. **When prompted for a challenge password, press Enter to leave the field blank.**
   5. **When prompted for a Company Name, press Enter to leave the field blank.**
   6. **Enter ‘y’ to sign the certificate**
   7. **Enter ‘y’ to commit the request**
3. Enter the following commands, replacing *newuser* with the username created above:

|  |
| --- |
| cd keys  openssl rsa -in *newuser*.key -des3 -out *newuser*.3des.key |

1. When prompted, enter the passphrase created earlier. There will the three prompts for this password.
2. Enter the following commands:

|  |
| --- |
| ./make\_new\_client.sh |

1. When prompted, enter the username created previously

The user has been created and can now log in. The user’s .ovpn file and PEM passphrase must be provided via a secure channel. See the section [Providing Client Secrets to Users](#_g5f345vtkeon).

### Providing Client Secrets to Users

After a VPN user account is created or re-keyed, the client secret key must be securely copied from the server and provided (along with the initial PEM pass phrase) to the user. There are many acceptable ways to do this, but the following method is one of the easier ones.

1. While logged in to the server as a VPN admin user, issue the following commands, replacing *user* with the username:

|  |
| --- |
| cat /etc/openvpn/easy-rsa/keys/*user*.ovpn |

1. The contents of the ovpn file will be printed to the terminal. Locate the beginning of the file (the first line will read “client”, and the last line will read “</tls-auth>”) and copy the contents to the clipboard.
2. Browse to <http://www.fourmilab.ch/javascrypt/javascrypt.html>
3. Paste the contents of the ovpn file in the green text field
4. Type a secure pass phrase in the yellow text field. This should **not** be the same as the PEM passphrase.
5. Do not change any other settings on the page. Click the Encrypt button under the green text field.
6. Copy the encrypted text from the red text field. This can be sent through insecure channels - e.g., paste it in the body of an email to the user.
7. Provide the following decryption instructions to the user:

|  |
| --- |
| 1. Browse to <http://www.fourmilab.ch/javascrypt/javascrypt.html> 2. Paste the encrypted message in the red text field. Be sure to include the first and last lines that begin with “#####” 3. Enter the key that I gave you in the yellow text field 4. Click the Decrypt button under the red text field 5. Copy the contents of the green text field to a plain text document, e.g. Notepad or TextEdit 6. Save the file as <yourname>.ovpn, e.g., kyle.ovpn   Treat this file like a secret document ! |

1. Provide the passphrase through some other channel, e.g. verbally or via text message

### Delete a User

The instructions below revoke a VPN user’s access.

1. Log in via console or SSH as a user that is a [member of the vpnadmins group](#_ueafejsgptva)
2. Issue the following commands, replacing *user* with the VPN username to remove:

|  |
| --- |
| cd /etc/openvpn/easy-rsa/  source vars  ./revoke-full *user* |