QST-VPN

Supporting documentation

Table of Contents

Introduction

Scope

This document is intended to provide a general view of the QST-VPN product. It contains detailed instructions on every usability aspect of the clients and the servers with some technical details to allow for thorough testing.

OpenVPN

The OpenVPN protocol is at the core of this application, the Client and Server manipulating this protocol to provide a connection between the two. As the application, to some degree, is a wrap around this protocol, the interaction with it is done through the Client and Server interfaces through the options provided there. For further documentation regarding the open protocol please consult the following file: https://github.com/OpenVPN/openvpn/blob/master/src/openvpn/ssl.h

Testing

Testing this product can prove difficult, especially when it comes to error logging and debugging. When testing please ensure the LogLevel variable is set to 7. The location of this variable depends on the specific client or server, details being provided below.

Clients

Shortcuts

Windows

- Control + H Opens the Help file
- Control + E Opens the Settings menu
- Control + Q Closes the application

Mac

- Command ⌘ + H Opens the Help file
- Command ⌘ + , Opens the Settings menu
- Command ⌘ + Q Closes the application

Linux

- Control + H Opens the Help file
- Control + E Opens the Settings menu
- Control + Q Closes the application

Features

Reconnect automatically on disconnect

This feature is located in the client app under the “Settings” tab. It retires to connect to the server using the same credentials as given before if there was a connection issue. The number of seconds between attempts can be set below the feature.

Open QSTVPN on startup

This feature is located in the client app under the “Advanced settings” tab. Enabling this feature will start the QSTVPN application when the machine starts, after the OS is booted.

Connect to server on startup

This feature is located in the client app under the “Advanced settings” tab. Enabling this feature will automatically begin the authentication process with the previously saved credentials and connect the client to the server when the application launches.

Connection mode

This feature is located in the client app under the “Advanced settings” tab and it allows the user to select between UDP and TCP as the protocols used to communicate with the server. Please note that the client application must use the same protocol the server expects.

Two-Factor authentication

This feature is located in the client app under the “Advanced settings” tab. Enabling this will display the OTP, or token text box on the main window of the application and the client will consider two-factor authentication when checking user credentials. Please note that the client application must use the same two-factor authentication settings as the server.

Dark mode

This feature is located in the client app under the “Advanced settings” tab and it refers to the darker selection of colour scheme used by default. Disabling this will change the application client colour scheme to “Light mode”, a ligher colour scheme. Please note that this feature is only available in as part of the Windows client. Linux and Mac clients will default to the general system theme settings.

LDAP authentication

This feature is located in the client app under the “Advanced settings” tab. Enabling this feature will allow users to authenticate against an LDAP server. Please note that the client application must use the same LDAP settings as the server

DNS server change

is located in the client app under the “Advanced settings” tab. Enabling this feature will allow the user to specify a preferred DNS server.

Usage modes

Basic mode

This mode connects the client to the server network by adding an extra route to the client’s routing table. The default route is not changed, therefore the client will still use the same default route as before the connection, without pushing any internet traffic through the server.

Forced mode

This mode connects the client to the server network by adding an extra route to the client’s routing table, but as opposed to Basic mode, it also changes the default route. As such, Internet traffic is now pushed to the server, although, there is still a chance for some traffic to escape.

Lockdown mode

This mode connects the client to the server in the same way as Forced mode does, with one major difference. While running the client in this mode, the default route is removed completely until a successful connection to the server is made. As such, no internet traffic leaves the client until it is pushed through the server through a valid connection.

Windows

Installation

1. Run the QST-VPN installation executable
2. Wait for the installer to unpack
3. Press Next
4. Review the End-User License Agreement for QST-VPN
5. If you agree, tick the “I accept the terms of the License Agreement” box and press Next
6. Review the End-User License Agreement for OpenVPN
7. If you agree, tick the “I accept the terms of the License Agreement” box and press Next
8. Review the components to be installed and Advanced features and click Next
9. Choose a Destination Folder where to install and press Install afterwards.
10. After the installation click Finish

Running

1. Double click the executable or the shortcut created
    a. Alternatively, use the search function to search for the application

Uninstallation

1. Go to Settings > Apps or type in the Start bar search “Add or remove programs” and open it.
2. Search for “QST-VPN” in the list of installed applications
3. Select QST-VPN and click Uninstall
4. Click Uninstall again in the newly opened window
5. After the Uninstall process has finished, click Next and then Finish

Useful information

- Settings location
    - Windows Registry
- Client logs
    - C:\Users\INSTALL_USER\AppData\Roaming\com.qstvpn\QST-VPN.log
    - QST-VPN.log is the current session log, while QST-VPN.log.1 is the previous sessions log
- Daemon logs
    - C:\Users\Public\qstvpn.clientd.log

Mac

Installation

1. Open the .dmg file
2. Drag and drop in the Applications folder the QSTVPN application

Running

Currently, QSTVPN is not a verified Apple developer and so MacOS will try to protect the user from running potentially malicious applications.

1. Double click the application
    a. At this point it will prompt a message which needs to be closed
2. Right click the application
3. Click the Open button shown in the error message

Uninstallation

1. Run the Uninstall tool found in the .dmg file

a. Type “Yes” and press the Enter key – Please ensure that you type “Yes” or “No”, not “y”, “n” or any other common variations

Useful information

- Settings location
  - ~/Library/Preferences/com.qstvnp.client.plist
  - “LogLevel: 7” needs to be added to the plist for debugging level log
- Client logs
  - ~/Library/Logs/com.qstvpn/QST-VPN.log
  - QST-VPN.log is the current session log, while QST-VPN.log.1 is the previous sessions log
- Daemon logs
  - /var/log/qstvpn.clientd.log

Linux

There are several Linux distributions each with its own particularities and as such, these instructions will be as distribution agnostic as possible.

Installation and uninstallation

Please use the built in package manager. If this is not available, please use the relevant command line utility, such as apt, dpkg, yum etc.

Example

Ubuntu18 – Running GNOME Desktop Environment

Option 1 – Using Ubuntu Software

Installation

1. Double click the package
2. Click Install
3. Close Ubuntu Software

Running

1. Click the Applications menu button in the lower left corner of the screen
   a. This instruction is based on Ubuntu 18 using GNOME as the desktop environment.
   b. Other desktop environments will have other options for this instruction.
2. Switch to the “All” tab
   a. Alternatively the search bar can be used to find the application
3. Click the Application

Uninstallation

1. Open Ubuntu Software
2. Switch to the Installed tab and look for “qstvpn”
3. Click Remove
4. Confirm Remove

Option 2 – Command line interface

Installation

1. Open a Terminal window
2. Go to the location of the package (using the “cd” command)
   a. Alternatively you can specify the full path to the package in the next step
3. Use the “apt” tool to install the package

   a. Sudo apt install -f ./"QSTVPN FULL PACKAGE NAME HERE"
4. Confirm the use of additional disk space
   a. Type "y" and press the Enter key

Running

1. Open a Terminal window
2. Type "qstvpn" and press the Enter key

Uninstallation

1. Open a Terminal window
2. Use the "apt" tool to uninstall
   a. Sudo apt remove qstvpn
3. Confirm freed space
   a. Type "y" and press the Enter key

Useful information

- Settings location
  - ~/.config/com.qstvpn.client/QST-VPN.json
  - "LogLevel: 7" needs to be added to the plist for debugging level log
- Client logs
  - ~/.config/com.qstvpn/QST-VPN.log
  - QST-VPN.log is the current session log, while QST-VPN.log.1 is the previous sessions log
- Daemon logs
  - /var/log/qstvpn.clientd.log

Setup

General setup

1. Run QST-VPN
2. Click Settings
3. Configure Settings
4. Configure Advanced Settings
5. Click Save

Settings configuration

1. Click Settings
2. Input the Server address
3. Input the Port (default is 1194)
4. Input your username
5. Input your password
6. Tick the Reconnect automatically on disconnect box, if applicable
7. Input the number of seconds between reconnection attempts, if applicable
8. Import the certificates received by email

Advanced Settings configuration

1. Click Settings and switch to Advanced Settings tab
2. Tick the Open on startup option if you wish the application to open on startup
3. Tick the Connect on startup option if you wish a connection with your saved settings to be made on start-up
4. Tick the Forced mode option if you wish the connection made to be in Forced mode

5. Tick the Forced mode option and the Lockdown option if you wish the connection made to be in Lockdown mode
6. Choose between UDP and TCP as the protocol on which the connection should be made
7. Tick the Use two factor authentication option if you choose to do so
8. Tick the Dark mode option if you prefer to use the application in Dark mode
9. Tick the Server uses LDAP option if it is applicable
10. Tick the Change DNS server on connection option if you choose to do so. If this is the case, then after ticking the box, please enter the address of the DNS server you would like to use.

Connecting to the server

1. With the Settings and Advanced settings configured, click the sphere present on the application user interface
    a. If 2FA is enabled, access your preferred 2FA application and input the relevant code shown in the textbox above the sphere

Servers

Server features

Basic authentication

- Basic authentication is a simple authentication method that separates the server settings from the outside. The username and password are set when the server si first accessed.
- There is no functionality for resetting these credentials. If lost, the server settings can be reset by turning off the server, deleting the settings json file and running the server again.

Home page

- Information box with QST-VPN version, OpenVPN version, Server status and Connected clients
- Connected users graph, showing the number of users connected to the server over time
- Data transferred graph, showing the total sum of data send and received over time

Clients page

- Searchable and sortable table with all the connections made and relevant information for each
- Kill connection button that will kill the connection for that specific client

Users page

- Searchable and sortable table containing user information
- User reset password functionality which will send a password reset link to the user email
- User reset OTP functionality which will send an OTP reset link to the user email
- Edit user functionality for each user
- Delete user functionality for each user

Settings page

- Server port setting
    - Do not set this port to reserved ports
- Server protocol choice between UDP and TCP
    - TCP is able to establish a connection with the server making it more reliable while UDP, although connectionless, is generally faster.
- Max server log size in Mebibytes
- Public facing server address

    - Default HTTP port is 5000 while default HTTPS port is 5001
    - HTTPS needs to be enabled on the hosting server
    - Default value is https://localhost:5001
    - If the server is intended to be accessible from outside of its network, then the address should be replaced with the public address of the server
- Check for use of emails for user management.
    - If this box is not checked, all user management must be performed by the admin. Links are generated by the server and are made available to copy on request by the admin to send to the end users. Certificates can be downloaded by the end users when setting or resetting their passwords, or can be downloaded by the admin and sent using other means.
    - If it is checked the following information must be submitted and either SendGrid must be activated and set up, or an SMTP server must be ready for use.
- User activation email template
    - The content of this textbox will be sent to the user and it represents the activation email
    - ${ACTIVATION_URL} is the variable name that will be substituted for the activation link
    - Ensure the variable is copied exactly, otherwise it will not be recognised and will not be substituted for the link
- User activation email subject
    - Default is “QST-VPN Server User Activation”
- Activation link expiration time
    - Default is 30 min
- User password reset email template
    - The content of this textbox will be sent to the user and it represents the password reset email
    - {RESET_PASSWORD_URL} is the variable name that will be substituted for the password reset link
    - Ensure the variable is copied exactly, otherwise it will not be recognised and will not be substituted for the link
- User password reset email subject
    - Default is QST-VPN Server Password Reset
- Password reset link expiration time
    - Default is 30 min
- User certificates email template
    - The content of this textbox will be sent to the user and it represents the email sent containing the user certificates
- Two factor authentication
    - Tick the box to enable Two factor authentication
    - This will not be valid for existing users
- Sendgid email service
    - Tick the box to enable Sendgrid emailing service
    - Input the Sendgrid key in the textbox below
- SMTP Email server
    - General SMTP settings
- TLS ciphers

- The TLS ciphers listed are available to use
- Click the one you would like to use

- New hope mode
  - Select the new hope mode from the dropdown list
- New hope named parameter
  - Select the new hope named paratemer from the dropdown list
- TLS pre-shared key
  - Tick to use TLS pre-shared key
- LDAP server for client authentication
  - Tick the box to enable LDAP authentication
  - Provide the LDAP server address
  - Provide the LDAP server port (default is 389)
  - Provide the LDAP admin distinguished name (this will be an LDAP admin user)
  - Provide the password for the admin user
  - Provide the LDAP user id prefix (generally “CN”)
  - Provide the LDAP distinguished name (generally CN=Users,DC=*Domain name*,DC=COM)
  - Provide LDAP password attribute (default is userPassword, which is set when the field is blank)

Windows

Installation

1. Run the server installation executable
2. Press Next
3. Review the End-User License Agreement for QST-VPN Server
4. If you agree, tick the “I accept the terms of the License Agreement” box and press Next
5. Review the End-User License Agreement for OpenVPN
6. If you agree, tick the “I accept the terms of the License Agreement” box and press Next
7. Review the components to be installed and Advanced features and click Next
8. Choose a Destination Folder where to install and press Install afterwards.
9. After the installation completed click Next.
10. Click Finish.

Uninstallation

1. Press the Start button and search for “add remove” and press the Enter key
   a. Alternatively, the Apps & features section can be found in System settings
2. Search for QSTVPN in the searchbar and click on the application
3. Click Uninstall and follow the process

At this point the server is no longer installed, but there are leftover files and data. To complete remove the QSTVPN server continue with the following steps:

4. Open Explorer
   a. Press the Start button + E
5. Delete the following:
   a. C:\easyrsa
   b. C:\Windows\System32\config\systemprofile\AppData\Roaming\com.qstvpn.server
   c. C:\Users\Public\qstvpn_auth_plugin.log

Start server

- Initially, the server starts automatically after it has been installed

1. Press the Start key and type “Services”
2. Press the Enter key
3. Search in the list for “QST-VPN Server” and select it
4. Press “Start”

Stop server

1. Press the Start key and type “Services”
2. Press the Enter key
3. Search in the list for “QST-VPN Server” and select it
4. Press “Stop”

Useful information

- Settings location
    - C:\Windows\System32\config\systemprofile\AppData\Roaming\com.qstvpn.server\com.qstvpn.server.json
- Logs
    - C:\Windows\System32\config\systemprofile\AppData\Roaming\com.qstvpn.server\qstvpn-server.log
    - C:\Users\Public\qstvpn_auth_plugin.log
- Restart Service after making changes to the server Settings

Linux

The below example is for installing on Ubuntu Server 18.

Option 1 – Using Ubuntu Software

Installation

1. Double click the package
2. Click Install
3. Close Ubuntu Software
4. Reboot
5. Start server

Uninstallation

1. Stop the server
2. Open Ubuntu Software
3. Switch to the Installed tab and look for “qstvpn-server”
4. Click Remove
5. Confirm Remove
6. Reboot

Option 2 – Command line interface

Installation

1. Open a Terminal window
2. Go to the location of the package (using the “cd” command)
    a. Alternatively you can specify the full path to the package in the next step
3. Use the “apt” tool to install the package
    a. Sudo apt install -f ./”QSTVPN FULL PACKAGE NAME HERE”

4. Confirm the use of additional disk space
    a. Type “y” and press the Enter key
5. Reboot
    a. Sudo reboot now
6. Start server

Uninstallation

1. Stop the server
2. Open a Terminal window
3. Use the “apt” tool to uninstall
    a. Sudo apt remove qstvpn-server
4. Confirm freed space
    a. Type “y” and press the Enter key
5. Reboot
    a. Sudo reboot now

Start server

1. Open a Terminal window
2. Start the service
    a. Sudo systemctl start qstvpn-server.service
    b. If the above command returns the error “Unit qstvpn-server.service could not be found.”, please run the the following command “sudo systemctl daemon-reload” and then try to start the service again

Stop server

1. Open a Terminal window
2. Stop the service
    a. Sudo systemctl stop --now qstvpn-server.service

Useful information

- Settings location
    - /etc/com.qstvpn.server.json
- Logs
    - /var/log/com.qstvpn.server/qstvpn-server.log
    - /var/log/qstvpn_auth_plugin.log
- Restart Service after making changes to the server Settings
    - Sudo systemctl restart qstvpn-server.service

Server setup

1. Open a browser and go to http://server:5000
    a. If the server only has a command line interface, please access the public ip of the server on port 5000 from a different machine
    b. If HTTPS is enabled, port 5001 can be used
2. A Basic authentication window will appear. Press Enter (if on AWS please enter “admin” for the username and the ec2 instance name for the password).
3. Choose an Admin username
4. Choose a Password for the Admin account
5. Confirm the Admin Password
6. Press Save

7. Enter the newly established Admin credentials to authenticate
8. Choose the Server port (Default is 1194)
9. Choose the Server protocol (Default is UDP – if on AWS – TCP is automatically permissible, additional setup is required for UDP to work on AWS)
10. Choose the Max server log size in mebibytes (Default is 10 MiB)
11. Choose a Public Facing server address. This should be the public address of the server.
12. Decide whether to use emails for user communication. If yes:
    a. Customise the User activation email
    b. Set the User activation email subject
    c. Customise the User password reset email
    d. Set the User password reset email subject
    e. Choose the sender email address (Default is qstvpn@qstvpn.com)
13. Set the time in which the activation link should expire, in minutes (Default is 30 min)
14. Set the time in which the User password reset link should expire, in minutes (Default is 30 min)
15. Choose if the server should use two factor authentication.
16. Choose if the server should send emails using SendGrid. If yes, input the SendGrid API key and jump to step 17. If no:
    a. Enter the SMTP Server Address
    b. Choose if the SMTP Server uses SSL
    c. Enter the SMTP Server port
    d. Enter the SMTP Server Username
    e. Set the SMTP Server Password
17. Choose the New Hope mode (Default is Fast)
18. Choose the New Hope named parameter (Default is Leia)
19. Choose if the server should use a TLS pre-shared key
20. Choose if the server should use an LDAP Server for client authentication. If not, click Save. If it should, continue below.
21. Enter the LDAP server address
22. Enter the LDAP server port
23. Enter the LDAP admin distinguished name
24. Enter the LDAP password
25. Enter the LDAP user id prefix
26. Enter the LDAP distinguished name
27. Enter the LDAP password attribute or leave empty to choose the default “userPassword”.
28. Click Save

User account creation

1. Go to the Users page
2. Click Create New
3. Enter a Username (between 8 and 256 characters)
    a. If LDAP is enabled, the username must me the LDAP username
4. Enter the User email address (one that was not used before)
5. Click Create
6. At this point, if emails are being used, an email with the account activation link will be sent to the email address provided before and the User account creation will continue on the client-side. If they are not, the admin must go to the users page and click the “Activate” button. The

link should be added to the paste buffer automatically, but may require manual copying. This link should be sent to the end-user.

7. The user needs to access the specified email and click the Account Activation Link
8. Enter a password and confirm password
    a. If LDAP is enabled, the password needs to be the same as the LDAP user password
    b. If 2FA is enabled, the QR code needs to be scanned with a 2FA app such as Google Authenticator
    c. If emails are not being used, the link to download the certificates will be available on this page. They should be downloaded. If not, the administrator can download them and send them to the end user.
9. At this point an email will be sent with the user certificates for the newly created user if emails are being used. Please safely store these certificates as they are part of the user authentication process.