
UH VPN

Release 2.0.0

Ultra Horizon Ltd

Apr 25, 2021

CONTENTS

1	Setup Guides	3
1.1	Ubuntu Setup Guide	3
2	VPN Management	9
2.1	Groups	9
2.2	Servers	11
2.3	People	15
2.4	Devices	16
3	Server Software	19
3.1	Installation	19
3.2	Adding VPN Servers	20
3.3	Removing VPN Servers	21
3.4	Upgrading	22
3.5	Logging	22
4	Client Apps	23
4.1	Android	23
4.2	iOS	25
4.3	macOS	26
4.4	Windows	29
4.5	Linux	30
5	Security	33
5.1	Website	33
5.2	API	33
5.3	VPN Tunnel	33
6	Support	35
6.1	Questions/Bugs/Features	35
6.2	Sales	35
6.3	Terms and Privacy	35

The documentation, [maintained with the help of the community](#), offers instructions on how to install, configure, and use UH VPN software. Whether you are new to UH VPN, or a seasoned veteran, our docs offer something for everyone.

Our documentation is available here in HTML format or as a [PDF](#) or [Epub](#) which can be downloaded for offline use.

SETUP GUIDES

This chapter of the documentation site contains step by step instructions on how to set up UH VPN on a particular platform. The guides featured here are designed for cloud platforms and on-premise hardware and can be adapted to suit any particular need.

If more information about a particular feature is required whilst reading the setup guides, the extensive documentation on this site details all aspects of UH VPN to cater for more advanced use cases.

1.1 Ubuntu Setup Guide

This guide is a walkthrough tutorial on setting up UH VPN for a machine running Ubuntu. This machine can be either virtual or physical, but must satisfy the following requirements:

- **OS:** Ubuntu 18.04, 19.10, 20.04 or 20.10
- **RAM:** minimum 100MB (1GB preferable)
- **Network:** Machine accessible either by public IP address, hostname or dynamic DNS.

This particular guide can be adapted to suit any cloud providers offering Ubuntu instances as well as on-premise machines configured with Ubuntu.

If you wish to explore UH VPN advanced options or modify the sample deployments consult the extensive documentation on this site.

- *Step 1: Satisfying prerequisites*
- *Step 2: Create a Server on the UH VPN Website*
- *Step 3: Configuring the Ubuntu Server*
- *Step 4: Installing Client Apps*

1.1.1 Step 1: Satisfying prerequisites

1. Note down the public IPv4 address of the Ubuntu machine. This IP address needs to point directly at the Ubuntu machine and not at a router or intermediate gateway.
2. Ensure that the ports UDP 443 and TCP 2802 are open on your Ubuntu instance if a firewall is configured. This guide will set up UH VPN clients to connect over UDP 443 so this port must be open. Server configuration updates are pushed over TCP 2802 by the UH VPN API so this port must also be open.
3. Ensure that either an SSH connection or console access to the machine is available.

1.1.2 Step 2: Create a Server on the UH VPN Website

The UH VPN [website](#) is the command and control centre for the VPN deployment. All VPN settings are managed through this interface. The first step (if you haven't done so already) is to purchase UH VPN. Once this is done, simply login and click on the group name that has been created for you and the following page will be presented:

Personal

Management / Personal
⚙️ 🗑️

Servers

Number of associated servers: 0 About Servers

Search for a server...

Name	URN	Expiry Time	Actions
Create New Server			

People

Number of associated people: 0 About People

Search for a person...

Name	Email	Actions
------	-------	---------

The first step is to create a UH VPN server, click the “Create New Server” button and the following page will be presented:

Create a new VPN Server

Management / Personal / New Server

Plan: **Free** Upgrade

Upgrading to Premium enables custom cryptography and enhanced routing options for servers. Billed at £1 +VAT per device in use.

Name

Enter a name

Domain/IP Address

Enter a domain or IP address

☒ **UDP**

UDP is the fastest mode of operation and is strongly recommended, if disabled TCP will be used instead.

IPv4 Tunnel Network

172.31.255.0/24

This is the subnet from which VPN clients will be allocated addresses via DHCP.

Appearance Order

Enter a number

Servers appear within applications in this order. Lowest at the top, highest at the bottom.

Port

Enter a port number

IPv6 Tunnel Network

fe80::/64

The IPv6 tunnel network (leave as fe80::/64 if you don't have a public subnet).


Enter the following parameters:

- **Name** : UDP

- **Appearance Order** : 0
- **Domain/IP Address** : IPv4 Address noted from the Ubuntu machine earlier
- **Port** : 443
- **UDP** : Enabled
- **IPv4 Tunnel Network** : 172.31.255.0/24
- **IPv6 Tunnel Network** : fe80::/64
- **DNS Servers** : 1.1.1.1, 1.0.0.1
- **Add Forwarding Rule** : Enabled
- **Add NAT Rule** : Enabled

Press submit and the server will then be created.

Note: A full description of all parameters can be found on the [server creation docs page](#).

Once created, press the  icon to obtain a UH VPN API token for the server. Copy and paste this to somewhere safe as it'll be used later.

1.1.3 Step 3: Configuring the Ubuntu Server

Now it's time to SSH into the Ubuntu Server.

The first step is to install the required dependencies:

```
sudo apt-get update
sudo apt-get install software-properties-common
```

Then it's time to add Ultra Horizon's package archive to the system sources:

```
sudo add-apt-repository ppa:ultrahorizon/ppa
```

```
root@UH-VPN:~# sudo add-apt-repository ppa:ultrahorizon/ppa
PPA for all software packages designed, built and produced by Ultra Horizon Ltd.
More info: https://launchpad.net/~ultrahorizon/+archive/ubuntu/ppa
Press [ENTER] to continue or Ctrl-c to cancel adding it.
```

A prompt will then display information about the repository, accept this, then download the package information from this newly added archive:

```
sudo apt-get update
```

Once this is done, UH VPN Server software can now be downloaded through the apt package manager.

```
sudo apt-get install uh-vpn-server
```

Once installed check that the UH VPN Service is running:

```
sudo service uh-vpn-server status
```

The output should say **active (running)** as depicted below:

```
ubuntu@ip-10-0-87-238:~$ sudo service uh-vpn-server status
● uh-vpn-server.service - UH VPN Server
   Loaded: loaded (/lib/systemd/system/uh-vpn-server.service; disabled; vendor preset: enabled)
   Active: active (running) since Thu 2020-04-23 12:27:06 UTC; 2 days ago
```

Then to ensure UH VPN Server starts at boot, issue the following command:

```
sudo systemctl enable uh-vpn-server
```

Next it's time to add the UH VPN Server API token we obtained earlier. This will enable the UH VPN Server software to set up the VPN server on our Droplet.

```
sudo nano /etc/uh-vpn-server/tokens
```

This will bring up an editor prompt like so:

```
GNU nano 2.9.3

# UH VPN Server Token Store
# Paste all tokens here and separate multiple tokens by a newline

0123456789abcdef0123456789abcdef0123456789abcdef
```

In this example, the token (0123456...) has been appended to the file. Once this is done, save the file and exit the editor (Ctrl-X in nano).

Now the server simply needs to be restarted in order to detect the new token:

```
sudo service uh-vpn-server restart
```

The server is now configured and ready to accept incoming VPN connections!

Note: For advanced configurations of the server software follow the [server documentation](#).

1.1.4 Step 4: Installing Client Apps

This is the final step in the set up process. First login to the UH VPN [website](#) and navigate to the group you created earlier. Now it's time to make a new person who's authorised to access the VPN server you just created. Click the "Create New Person" button and the following page will be presented:

Create a new Person

[Management](#) / [Personal](#) / New Person

Name

Email

Submit

Enter your name and email address, then press submit and the person will then be created.

Next it's time to associate a device to the person that's just been created. To do so, click the name of the person and then press the "Add new device" button and the following page will be presented:

Add Device

[Management](#) / [Personal](#) / [James Webb](#) / Add Device

Name

Enter a name that describes the physical device. For example, "iPhone".

Expiry Date

Device profiles expire on the specified date. To never expire, leave blank.

Expiry Time

The device profile will expire at the time specified GMT. Time must be in 24hr format.

Submit

Enter the following parameters:

- **Name** : A name for the device. E.g. Android
- **Expiry Date** : Leave unfilled unless you wish to specify a date for device revocation
- **Expiry Time** : Leave unfilled unless you wish to specify a time for device revocation

Note: A full description of all parameters can be found on the [device creation docs](#) page.

Press submit and the device will then be created. You will then receive an email with a one-time passcode (OTP). Download the UH VPN app for your platform and enter the OTP code to download the profile. Then you can **connect and enjoy a fast, secure and private VPN connection!**

Tip: Instructions for client apps can be found on the [clients docs page](#).

VPN MANAGEMENT

The UH VPN [website](#) acts as the command and control centre for all UH VPN deployments. UH VPN clients and servers rely on the availability of this site to provide functionality such as network authentication, configuration updates and much more. Every time a change is made on the website, this change is securely pushed to all relevant UH VPN clients and servers. This removes the need for administrators to ship new VPN profiles to clients and install new cryptographic keys for servers, instead this can all be done securely, quickly and easily through the simple to use web interface without any extra intervention required from end-users of the service.

The overarching structure of the management interface within the website is based around the following concept:

Groups of people own devices which authenticate onto **servers**.

This is the simplest explanation for the inspiration behind the interface structure and further explanations for each of these terms is detailed below.

2.1 Groups


Groups represent the top level structure for VPN deployments. They should be named to reflect the scenario in which a VPN deployment is being utilised. For example, if one is creating a VPN system for a company, one may wish to name the UH VPN group after that company.

Fundamentally, groups are containers for servers, people and devices. They also hold custom branding attributes and billing information. Multiple groups are independent from one another even if administered through the same user account.

2.1.1 Creating Groups

Groups can be created by contacting Ultra Horizon's [engineering department](#). This is necessary in order to purchase a UH VPN enterprise licence for use within your company.

2.1.2 Editing Groups

Groups can be edited at any point by clicking the  icon next to the appropriate group in the [management page](#). After clicking, one is presented with a page similar to that of group creation, except fields are pre-filled.

Edit the fields (described in [group creation](#)) and then press the submit button to save.

2.1.3 Deleting Groups


Groups can only be deleted by contacting Ultra Horizon. Simply email our [engineering department](#) and your request will be actioned.

Deleting a group removes all servers, people and devices. It is a destructive action that cannot be undone.

Any subscriptions tied to a deleted group will immediately cancel and a final bill will be taken at the end of the billing period.

2.1.4 Group Administrators


UH VPN groups can have more than one administrator. This enables multiple user accounts to control all aspects of the group. This setup is particularly suited to environments where more than one person is responsible for VPN operations. For example, IT engineers within a company.

To associate or remove an administrator one must first click the  icon next to the appropriate group in the [management page](#). After clicking, one is presented with a page displaying group administrators and billing information.

Associating a new admin

To associate a new administrator to the group one must first click the “Associate New Admin” button at the base of the list of admins. One is then prompted for a user ID of the admin one wishes to associate. This can be found on their [profile page](#). Once entered, click submit and the new administrator will have access to the group in their management page.


Deleting an admin

It is also possible to remove administrators from a group. To do so, one needs only to click on the  icon next to the admin they wish to remove.

Note: It is not possible to remove oneself from the list of admins, as doing so could potentially leave the group with zero administrators.

2.1.5 Group Billing

Billing for UH VPN is handled at a group level and not at a user level. As such administrators of groups can easily control how each group is financed. UH VPN holds card details for core licenced groups through its payment partner, Stripe. All card details are held securely by Stripe, and billing occurs monthly at a rate of £4 +VAT per device used in a monthly period. For example, if a group contains 3 people each with 2 devices, the bill would be £24 +VAT.

Group billing is handled in the group settings page which can be accessed by clicking the  icon next to the associated group in the [management page](#). Here, one is able to view their billing period, card details (shown dynamically in the card image), utilisation rate and pending charges.

Updating Card Details

If card details need to be updated. For example, card currently used has expired. This can be accomplished by clicking the “Update Card Details” button at the base of the group settings page. One will then be presented with a card collection modal. Once card details have been entered and verified, the new card will overwrite the old card and billing will continue as normal.

Cancelling Subscription

If one wishes to cancel their UH VPN subscription, this can be accomplished by clicking the “Cancel Subscription” button at the base of the group settings page. Once cancelled, the group will remain on the core licence until the end of the billing cycle; at which point a final bill will be taken and the group will transition into a frozen state where VPN operation will cease to function.

2.2 Servers

UH VPN servers are managed through the [website](#) and are contained within UH VPN groups. Every server defined within a group permits access from all persons within that group. This facilitates a simple authentication structure.

All VPN configuration options such as transport protocol, port, IP routing, cryptography and so on is specified through the management interface and this information is dynamically pushed every minute to UH VPN Server software to allow for dynamic configuration updates and reduced complexity in server configuration.

2.2.1 Creating Servers

Servers can be created by using the “Create New Server” button at the base of the list of servers on the relevant group page. One will then be presented with a list of fields to fill in as follows:

- **Name** : Generic name for the server in question. E.g. Office UDP.
- **Appearance Order** : The order in which the server will appear in the list on client applications. 0 = highest, ∞ = lowest.
- **Domain/IP Address** : The public IP address or hostname for the server.
- **Port** : IP port number for the server.
- **IPv4 Tunnel Network** : This is the IPv4 network that will be used for DHCP address assignment to UH VPN clients. This should be chosen such that it does not conflict with any subnets already defined on one’s network.
- **IPv6 Tunnel Network** : This is the IPv6 network that will be used for DHCP address assignment to UH VPN clients. If you do not have an IPv6 public subnet, use fe80::/64, fe80:1::/64, fe80:2::/64 or similar to prevent IPv6 traffic from bypassing the VPN.
- **DNS Servers** : CSV list of DNS servers for UH VPN clients to use.
- **Add Forwarding Rule** : This will dynamically update Ubuntu’s iptables to allow forwarding UH VPN traffic onto one’s WAN interface. Only disable this when manually adding filter rules.
- **Add NAT Rule** : This will automatically insert a NAT rule in Ubuntu’s iptables to allow UH VPN clients to access the IPv4 Internet from one’s machine. Only disable this when manually adding NAT rules.


Note: By default all UH VPN servers will push the routes 0.0.0.0/0 and ::/0 to redirect all IPv4 and IPv6 traffic over the VPN interface.

Enterprise Server Options

- **Redirect IPv4 Traffic** : This controls whether the 0.0.0.0/0 route is pushed to clients.
- **Custom IPv4 Routes** : When the above redirect button is disabled, one has the ability to insert custom IPv4 routes in CSV format. E.g. 192.168.0.0/24, 192.168.1.0/24.
- **Redirect IPv6 Traffic** : This controls whether the ::/0 route is pushed to clients.
- **Custom IPv6 Routes** : When the above redirect button is disabled, one has the ability to insert custom IPv6 routes in CSV format. E.g. fc00::/64, fc00:1::/64.
- **Custom Cryptography** : When selected, one is able to specify their own cryptographic parameters for use within UH VPN. Note this is only recommended if you are experienced in generating cryptographic keys and certificates. **Rolling your own crypto is dangerous!**


Upon server submission, the above fields will be validated and submitted.

2.2.2 Editing Servers

Servers can be edited at any point by clicking the  icon next to the appropriate server in the list of servers on the relevant group page. After clicking, one is presented with a page similar to that of server creation, except fields are pre-filled.


Edit the fields (described in [server creation](#)) and then press the submit button to save.

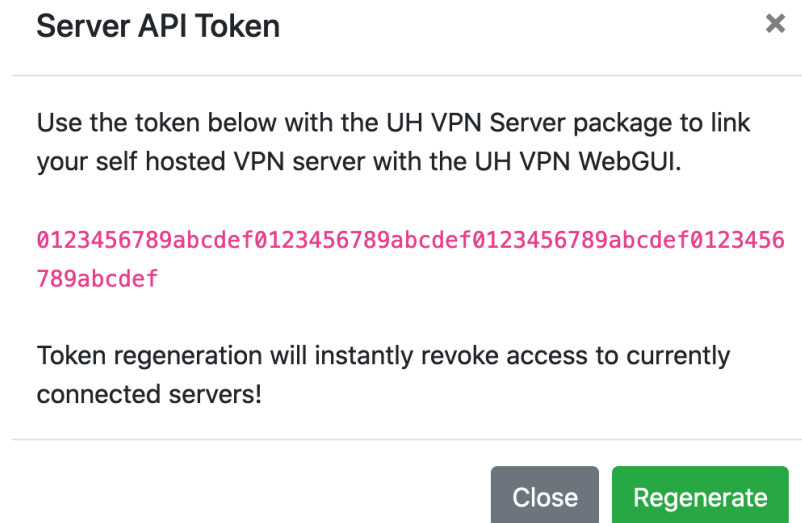
2.2.3 Deleting Servers

Servers can be deleted at any point by clicking the  icon next to the appropriate server in the list of servers on the relevant group page. After clicking and confirming the modal prompt, the page will refresh and the server will be removed from the list.

Deleting a server is a destructive action that cannot be undone.

2.2.4 Obtaining API Tokens

To use a server defined on the [website](#) with UH VPN Server software it is necessary to obtain an API token for the server in question. To do this one needs to click the  icon next to the appropriate server in the list of servers on the relevant group page. After clicking, one will be presented with a modal as shown below:



One simply needs to copy the token (shown in pink) and either follow:

- [UH VPN Setup Script](#) available if using our [Digital Ocean Image](#).
- [Adding servers](#) instructions in order to link the server software with the UH VPN API if using a vanilla Ubuntu installation.

If a token has been compromised, the “Regenerate” button can be used to create a new token for the server in question. **This will instantly revoke the old API token**

2.2.5 Advanced server tutorials

Dualstack Routing

UH VPN is capable of handling both IPv4 and IPv6 traffic and has built in support for dualstack VPN tunneling.

In order to enable dualstack operation it is imperative that the following prerequisites are met:

- **IPv6 Public Subnet Issued:** You must have an IPv6 public subnet issued to you by a relevant Internet registry applicable to your geographical area. E.g. RIPE, ARIN and so on. From this subnet you must choose a /64 subnet as the IPv6 tunnel network.
- **IPv6 Routing:** The entire IPv6 /64 subnet used as the IPv6 tunnel network must be routed to your VPN server. For example, if your VPN server has the public facing IPv6 address of 2000::1/32 and you plan to use the subnet of 2000:0000:0000:0001::/64 as your tunnel network, you must have a route marking 2000::1/32 as the next hop address for the subnet 2000:0000:0000:0001::/64 at your upstream router to avoid NDP failures. Without this routing rule in place, IPv6 traffic will not reach connecting clients.

Once these two prerequisites are met, it's simple to enable dualstack support on a UH VPN server.

First head over to the [website](#) and within the appropriate group, edit the relevant server and include your public IPv6 subnet in the “IPv6 Tunnel Network” field as indicated below:

IPv6 Tunnel Network

2000:0000:0000:0001::/64

An IPv6 subnet can optionally be specified if dualstack operation is required.

Once entered, save the server configuration. Future connecting clients will then be issued an IPv6 address from the /64 network specified above and enjoy dualstack connectivity to the Internet.

Reject inter-client communication

In certain scenarios, it may be desirable to prevent VPN clients communicating with one another. For example, when running a public VPN service through UH VPN.

This can be achieved by disabling the “Add Forwarding Rules” button on the UH VPN server settings page and instead inserting your own rules into `iptables` on your server as follows:

```
iptables --append FORWARD -s 172.31.255.0/24 -d 172.31.255.0/24 -j DROP
iptables --append FORWARD -s 172.31.255.0/24 -j ACCEPT
```

Modify the above example to suit your tunnel network (replace `172.31.255.0/24` as appropriate). These rules will drop inter-client communication, but allow all other communication.

Tip: Use the `iptables-save` package to persist `iptables` rules between reboots.

Custom Cryptography (Enterprise Feature)

Warning: Rolling your own crypto is dangerous. If you are at all unsure about what you are doing, use the cryptographic parameters provided to you automatically by UH VPN. Attempt this at your own risk!

There are certain circumstances where one may elect not to use the RSA keys and certificates issued by the UH VPN certificate authority. For example, corporations often have their own PKI infrastructure already in place and as such will elect to use their own cryptographic parameters.

In order to use custom cryptography, the following prerequisite objects must be obtained:

- **CA Certificate:** A public CA certificate under PEM encoding.
- **Server Certificate:** This is the public server certificate under PEM encoding which has been signed by the CA. This certificate must have “Digital Signing” and “Key Encipherment” privileges. It must also have “Server Authentication” defined as an extended key usage option.
- **Server Key:** This is the private key corresponding to the server certificate above. It must be PEM encoded and in PKCS #1 formatting.
- **Static TLS Key:** This is 256 random bytes of hex encapsulated by a header and trailer. It must have exactly 16 bytes per line (32 hex characters) and must include the standard OpenVPN static key header and trailer.

Once the parameters have been obtained, simply edit the relevant server within the appropriate group, switch on the “Custom Cryptography” option and paste in the parameters into the corresponding fields. Once saved, connecting clients and servers will communicate using your own custom defined cryptography options.

Split Routing (Enterprise Feature)

Split routing is often used where it is not desirable to route your entire Internet connection over the VPN tunnel. For example, you may wish to utilise your standard Internet connection for general browsing whilst having UH VPN to facilitate access to an office network.

In the example below we will configure UH VPN to only route traffic destined for 192.168.0.0/24 over the VPN.

First head over to the [website](#) and within the appropriate group, edit the relevant server and switch off “Redirect all IPv4 traffic” and “Redirect all IPv6 traffic” as shown below:

☐ Redirect all IPv4 Traffic ☐ Redirect all IPv6 Traffic

Custom IPv4 Routes

0.0.0.0/0

Use comma separated CIDR notation. E.g. 192.168.1.0/24, 192.168.4.0/24

Custom IPv6 Routes

::/0

Use comma separated CIDR notation. E.g. fe80::/10, fc00::/7

This will display the custom route fields for both IPv4 and IPv6. Update the fields to the following:

- **Custom IPv4 Routes** : 192.168.0.0/24
- **Custom IPv6 Routes** : Leave blank

This will ensure connecting clients are pushed only a route for the 192.168.0.0/24 subnet. Update the subnet values to match your particular configuration.

Tip: The same procedure can be adapted to IPv6 networks by specifying a custom IPv6 subnet in the “Custom IPv6 Routes” field.

2.3 People

People are managed through the [website](#) and are contained within UH VPN groups. Within UH VPN, people are used as a container for devices. This aims to replicate the real world structure of people owning devices. This allows for reduced complexity when managing the authentication structure of a VPN deployment. Administrators can easily view all devices associated to a person and can perform “one touch” revocation for a person and all their associated devices.


2.3.1 Creating People

People can be created by using the “Create New Person” button at the base of the list of people on the relevant group page. One will then be presented with a list of fields to fill in as follows:

- **Name** : Name of the person one wishes to create.
- **Email** : Email address for the person in question. This is where OTP codes will be sent to allow for VPN profiles to be installed on devices.


Upon person submission, the above fields will be validated and submitted.

2.3.2 Editing People

People can be edited at any point by clicking the  icon next to the appropriate person in the list of people on the relevant group page. After clicking, one is presented with a page similar to that of person creation, except fields are pre-filled.

Edit the fields (described in [person creation](#)) and then press the submit button to save.

2.3.3 Deleting People

People can be deleted at any point by clicking the  icon next to the appropriate person in the list of people on the relevant group page. After clicking and confirming the modal prompt, the page will refresh and the person will be removed from the list.

Deleting a person is a destructive action that cannot be undone. All associated devices for that person will be deleted and revoked.

2.4 Devices

As the name suggests, UH VPN Devices represent devices that people own. This could be a mobile phone, laptop, tablet and so on. Devices authenticate directly onto UH VPN servers and a VPN connection is then established between a device (UH VPN client application) and a server (UH VPN Server software).

Devices are managed through the [website](#) and are contained within people to facilitate easy association between people and their hardware.




Devices are immutable objects (cannot be modified once instantiated). This improves security by ensuring that there is a one-to-one mapping between UH VPN devices and physical devices a person owns. The OTP field on the person's device page indicates whether the OTP code has been redeemed by a client application.

2.4.1 Adding Devices

Adding devices within UH VPN can be done by clicking the “Add New Device” button at the bottom of a person's page within a UH VPN group. After clicking, one will then be presented with a list of fields to fill in as follows:


- **Name** : Name for the device in question, e.g. macOS, iOS, Android or Windows.
- **Expiry Date** : If device expiry is desired, one can specify an expiry date here. If a date is not specified, the device will never expire until manual revocation occurs via deletion.
- **Expiry Time** : If an expiry date is specified, the time can also be specified to provide an increased granularity with respect to expiry. All times should be entered in 24 hour format and will be taken as GMT.

Upon device submission, the above fields will be validated and submitted. If submission succeeds, the person in question will be sent an email containing a one-time-passcode (OTP) for entry into a UH VPN client application. Once this code is entered, all relevant configurations such as server information, cryptography and app branding information is securely sent to the device. Secure dynamic updates will occur automatically for UH VPN clients allowing administrators to change server settings, group parameters and more without any impact to end clients, thus simplifying VPN deployments hugely.

Once a user has redeemed their OTP code, the OTP field for the device in question on the person's page will change from  to . If redemption fails to occur within the time period set by the group's “device registration timeout”, the OTP icon will change to  and the device will need to be deleted and a new one created.


Note: If using custom branding on enterprise groups, UH VPN device enrollment emails are custom branded to your specification.

2.4.2 Revoking Devices

UH VPN supports instant device revocation to aid situations where devices need to be revoked prior to their expiry date. To do so, administrators simply need to click the  icon next to the device in question. Once a device is deleted it cannot be undone and all authentications for the device in question will immediately fail. Moreover, dynamic configuration updates for the device profile will also fail and the end user will be informed of revocation by their UH VPN client application.

2.4.3 Static Profile Export

UH VPN has the ability to export UH VPN device profiles in an OpenVPN compatible format to allow administrators to cater for users running more exotic operating systems where UH VPN client applications don't exist.

To export an OpenVPN profile click the  icon next to the device in question. One will then be presented with a modal prompt with two fields:

- **Server** : The server to link the static VPN profile to. Static profiles can't utilise multi-server selection and thus have to be bound to a single server. Select the appropriate one from the list.
- **Auto Add Credentials** : Certain OpenVPN applications permit credentials being auto-filled by the configuration profile, select this option if the client application supports this.

When the download button is pressed, a compressed zip file will be downloaded. Once extracted the file structure is as follows:

- **README.txt** : Details instructions on how to import the VPN profile.
- **OpenVPN Profile** : OpenVPN config file to be utilised by an OpenVPN application. It is named to indicate the group, server, person and device in question.
- **credentials.txt** : File containing the username (first line) and password (second line) to use when prompted by OpenVPN for credentials.

Warning: Only use this feature if absolutely necessary! Clients using these profiles will not benefit from dynamic secure updates, custom branding or enhanced performance. Use this feature at your own risk!

SERVER SOFTWARE

UH VPN Server software runs on machines hosted by the end-user. This could be in a cloud or on-premise environment. This software is responsible for the VPN link which encrypts and authenticates data between client applications and the hosted machine running UH VPN Server software.

Configuration for UH VPN Servers is done via the [website](#) and each server created is assigned an API token, these tokens are used by the server software to dynamically pull all configuration options from the UH VPN API. This facilitates centralised administration for VPN servers and greatly reduces the complexity involved in VPN deployment.

3.1 Installation

UH VPN Server software demands the following prerequisites:

- **OS:** Ubuntu 18.04, 19.10, 20.04 or 20.10
- **RAM:** 100MB (1GB preferable)
- **Network:** Machine accessible either by public IP address, hostname or dynamic DNS.

The first step is to install the required dependencies:

```
sudo apt-get update
sudo apt-get install software-properties-common
```

Then it's time to add Ultra Horizon's package archive to the system sources:

```
sudo add-apt-repository ppa:ultrahorizon/ppa
```

```
root@UH-VPN:~# sudo add-apt-repository ppa:ultrahorizon/ppa
PPA for all software packages designed, built and produced by Ultra Horizon Ltd.
More info: https://launchpad.net/~ultrahorizon/+archive/ubuntu/ppa
Press [ENTER] to continue or Ctrl-c to cancel adding it.
```

A prompt will then display information about the repository, accept this, then download the package information from this newly added archive:

```
sudo apt-get update
```

Once this is done, UH VPN Server software can now be downloaded through the apt package manager.

```
sudo apt-get install uh-vpn-server
```

Once installed check that the UH VPN Service is running:

```
sudo service uh-vpn-server status
```

The output should say **active (running)** as depicted below:

```
ubuntu@ip-10-0-87-238:~$ sudo service uh-vpn-server status
● uh-vpn-server.service - UH VPN Server
   Loaded: loaded (/lib/systemd/system/uh-vpn-server.service; disabled; vendor preset: enabled)
   Active: active (running) since Thu 2020-04-23 12:27:06 UTC; 2 days ago
```

If one desires UH VPN Server to start at boot, issue the following command:

```
sudo systemctl enable uh-vpn-server
```

3.2 Adding VPN Servers

It is possible to add servers whilst the uh-vpn-server service is running. To do so, one must update the token store in `/etc/uh-vpn-server`.

First, an API token for the relevant server must be obtained from the [website](#) by following the instructions for [obtaining API tokens](#). Once this is done, it is necessary to append this token to the token store by following the steps outlined below:

```
sudo nano /etc/uh-vpn-server/tokens
```

This will bring up an editor prompt like so:

```
GNU nano 2.9.3

# UH VPN Server Token Store
# Paste all tokens here and separate multiple tokens by a newline

0123456789abcdef0123456789abcdef0123456789abcdef
```

In this example, the token (0123456 . . .) has been appended to the file. Once this is done, save the file and exit the editor (Ctrl-X in nano).

Note: It is possible to add as many tokens as you wish to this store in order to run multiple VPN servers at once. However, one must ensure that servers don't share the same socket (port + protocol) or the same tunnel network if running on the same machine.

Now the server simply needs to be restarted in order to detect the new token:

```
sudo service uh-vpn-server restart
```

It is possible to confirm the acceptance of a new token by viewing the last few lines of output from the uh-vpn-server service daemon:

```
tail /var/log/uh-vpn-server/daemon.log
```

The last few lines of this output should acknowledge the new token and confirm that the associated configuration has been downloaded and installed:


```
ubuntu@ip-10-0-87-238:~$ tail /var/log/uh-vpn-server/daemon.log
2020-04-26 16:16:47,792 - uh-vpn-server - INFO - Starting UH VPN Server daemon
2020-04-26 16:16:47,792 - uh-vpn-server - INFO - Enabling Dualstack IP Forwarding
2020-04-26 16:16:48,063 - uh-vpn-server - INFO - Found new VPN server token: 0123456789abcdef0123456789abcdef0123456789abcdef
2020-04-26 16:16:48,249 - uh-vpn-server - INFO - Retrieved and installed new config for server: UDP
```

3.3 Removing VPN Servers

Removing servers cannot be done whilst the uh-vpn-server service is running. The service needs to be stopped, then the associated token removed from the token store in `/etc/uh-vpn-server/tokens` and then the service needs to be restarted.

This operation has the side effect of halting all VPN servers configured on the host machine.

```
sudo service uh-vpn-server stop
```

Now, the associated token needs to be removed from the token store:

```
sudo nano /etc/uh-vpn-server/tokens
```

This will bring up an editor prompt like so:

```
GNU nano 2.9.3

# UH VPN Server Token Store
# Paste all tokens here and separate multiple tokens by a newline

0123456789abcdef0123456789abcdef0123456789abcdef
```

Remove the token and save the file (Ctrl-X in nano). The service can then be restarted by issuing the command:

```
sudo service uh-vpn-server start
```

One should then check that the service is up and running:

```
sudo service uh-vpn-server status
```

The output should say **active (running)** as depicted below:

```
ubuntu@ip-10-0-87-238:~$ sudo service uh-vpn-server status
● uh-vpn-server.service - UH VPN Server
   Loaded: loaded (/lib/systemd/system/uh-vpn-server.service; disabled; vendor preset: enabled)
   Active: active (running) since Thu 2020-04-23 12:27:06 UTC; 2 days ago
```

3.4 Upgrading

Upgrading UH VPN Server software is simple and is done via the apt package manager on Ubuntu. It is worth noting that this operation will restart all VPN servers in operation on the machine, having the effect of disconnecting all connected clients which will then subsequently reconnect after a period of around one minute.

The first step is to update the package archives:

```
sudo apt-get update
```

To upgrade just UH VPN Server software issue the command:

```
sudo apt-get install uh-vpn-server
```

This will install any updates for the uh-vpn-server service or alert you if you are already on the latest version.

Alternatively, UH VPN Server software is also upgradeable via the command:

```
sudo apt-get upgrade
```

However, doing so upgrades other packages already installed on the system.

3.5 Logging

UH VPN Server software is built with various logging to aid users in diagnostic activities and to provide telemetry data. All log files are stored in `/var/log/uh-vpn-server/`.

Within the aforementioned directory there exists two file types:

1. **Daemon Log** : This provides information about the uh-vpn-server service. More specifically, information pertaining to tokens and configuration updates.
2. **VPN Log** : This provides information about specific VPN servers running on the host machine.

The daemon log file can be accessed at `/var/log/uh-vpn-server/daemon.log` and is limited to 4MB in size. However, the file adopts a rotational backup policy such that when the file reaches 4MB in size, the contents of this file is moved to `/var/log/uh-vpn-server/daemon.log.1` and the `/var/log/uh-vpn-server/daemon.log` is wiped to allow for fresh data to be recorded. This process occurs twice meaning that a total of 12MB of log storage is permitted and three files are created, namely `daemon.log`, `daemon.log.1` and `daemon.log.2` with `daemon.log` containing the most up to date logging information.

VPN log files adopt the naming policy of `<token>.log` where `<token>` is the associated API token for the server in question. These log files are written directly from the underlying VPN core and are useful in assisting with specific server problems.

Tip: When reading these files it is recommended to use the commands `less +G` or `tail` to avoid polluting your terminal with endless log data!

CLIENT APPS

UH VPN client applications are available free of charge for users to download and use with UH VPN deployments. One simply needs to download the appropriate application for their operating system, enter the one-time-passcode sent in an email and they're all set. Once the OTP code has been entered, secure dynamic updates will occur to the UH VPN client application, meaning administrators never need to issue manual updates to their end users. Furthermore, this method of deployment removes all risks associated with manual VPN profile distribution as all exchanges are handled securely and automatically via the UH VPN API.

This chapter of our documentation is designed specifically to support end users and provide simple instructions on how to operate their application and connect to a chosen VPN server to establish a secure connection.

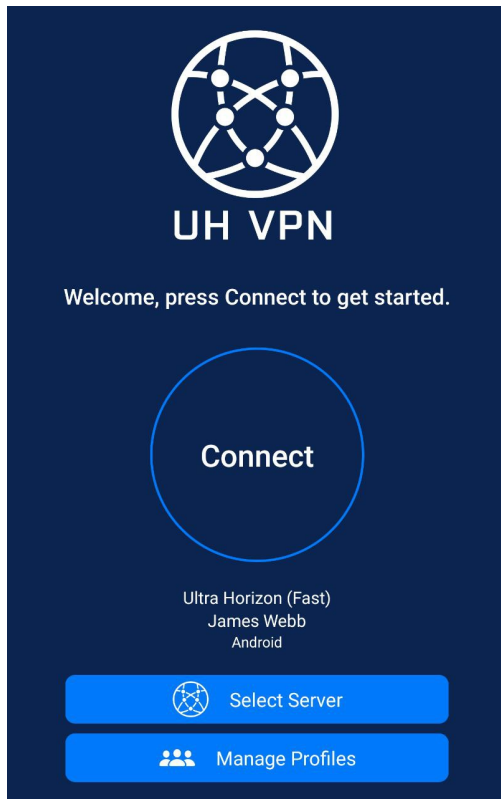
4.1 Android



The UH VPN android application can be downloaded by clicking the Play Store badge at the top of the page. The sections below detail specific instructions on how to use the Android application.

4.1.1 Connecting and Disconnecting

Connecting and disconnecting to/from VPN networks is a very simple procedure. The app is centred around a single connect/disconnect button to ensure this.



To connect, one simply needs to select a group by visiting the “Manage Profiles” page, then select an appropriate server from the list presented by the “Select Server” button. Then press “Connect”. The connection is complete and established when the text: **Secure connection established** is shown.

To disconnect, one simply needs to press the “Disconnect” button in the centre of the application screen.

4.1.2 Adding Profiles

Adding VPN profiles within the Android application is simple. One simply needs to click the “Manage Profiles” button on the app, then press the “+” icon in the top right of the modal alert. The user will then be prompted for a six digit code which will have been received in an email. Once this is entered, the UH VPN profile will then be securely downloaded to the device ready for use.

4.1.3 Deleting Profiles

Deleting VPN profiles within the Android application is simple. One simply needs to click the “Manage Profiles” button on the app, then swipe left on the profile to delete. This is demonstrated by the screenshots below:

Profile to delete:



Swiping left to delete:

ULTRA HORIZON

Delete 

Note: Deleting profiles cannot be undone and access to any UH VPN Servers associated with the group in question will be lost. New profiles must be issued from the UH VPN [website](#).

4.2 iOS



The UH VPN iOS application can be downloaded by clicking the AppStore badge at the top of the page. The sections below detail specific instructions on how to use the iOS application.

4.2.1 Connecting and Disconnecting

Connecting and disconnecting to/from VPN networks is a very simple procedure. The app is centred around a single connect/disconnect button to ensure this.

To connect, one simply needs to select a group by visiting the “Manage Profiles” page, then select an appropriate server from the list presented by the “Select Server” button. Then press “Connect”. The connection is complete and established when the text: **Secure connection established** is shown.

To disconnect, one simply needs to press the “Disconnect” button in the centre of the application screen.

4.2.2 Adding Profiles

Adding VPN profiles within the iOS application is simple. One simply needs to click the “Manage Profiles” button on the app, then press the “+” icon in the top right of the modal alert. The user will then be prompted for a six digit code which will have been received in an email. Once this is entered, the UH VPN profile will then be securely downloaded to the device ready for use.

4.2.3 Deleting Profiles

Deleting VPN profiles within the iOS application is simple. One simply needs to click the “Manage Profiles” button on the app, then swipe left on the profile to delete.

4.3 macOS



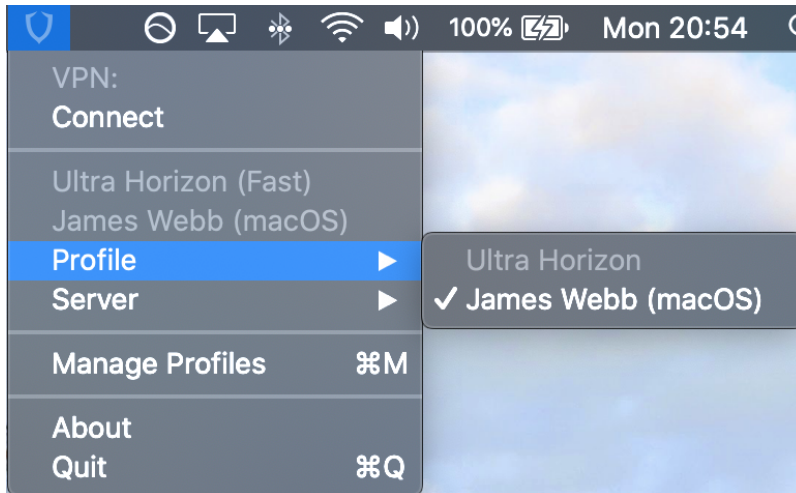
The UH VPN macOS application can be downloaded by clicking the AppStore badge at the top of the page. The sections below detail specific instructions on how to use the macOS application.

4.3.1 Connecting and Disconnecting

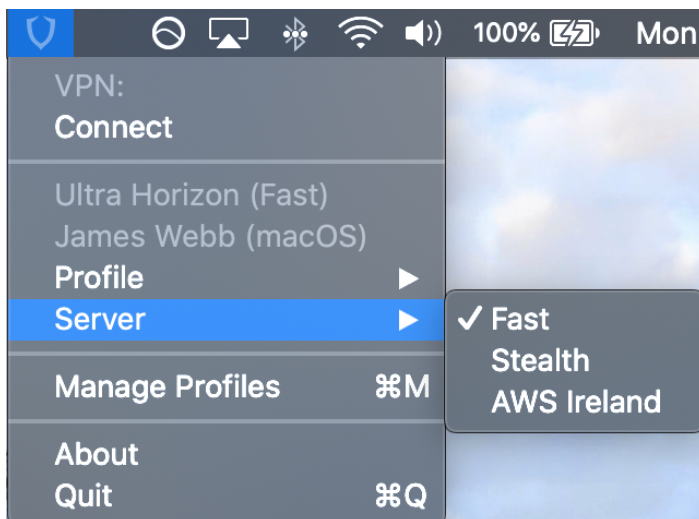
Connecting and disconnecting to/from VPN networks is a very simple procedure and is done solely from the menu bar.

Connecting

To choose a base VPN profile to connect with select one from the Profile list:



Then choose a server to connect to that's associated with the group in question:



Once this is done, one simply needs to press the connect button at the top of the menu bar to connect to their chosen server and group.

Note: If this is the first time a connection is made, a pop up will appear asking permission to install VPN profiles, one must accept this in order for UH VPN to function correctly.

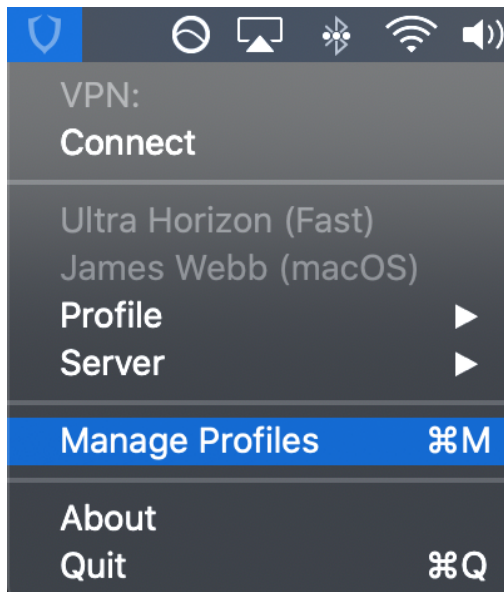
Disconnecting

Once connected to a VPN server, one needs to simply press the disconnect button at the top of the menu bar to completely disconnect from the VPN server in question.

Tip: If one wishes to switch VPN profiles or servers quickly, it is possible to select a different profile or server whilst connected and UH VPN will dynamically reconnect to a chosen selection in real-time.

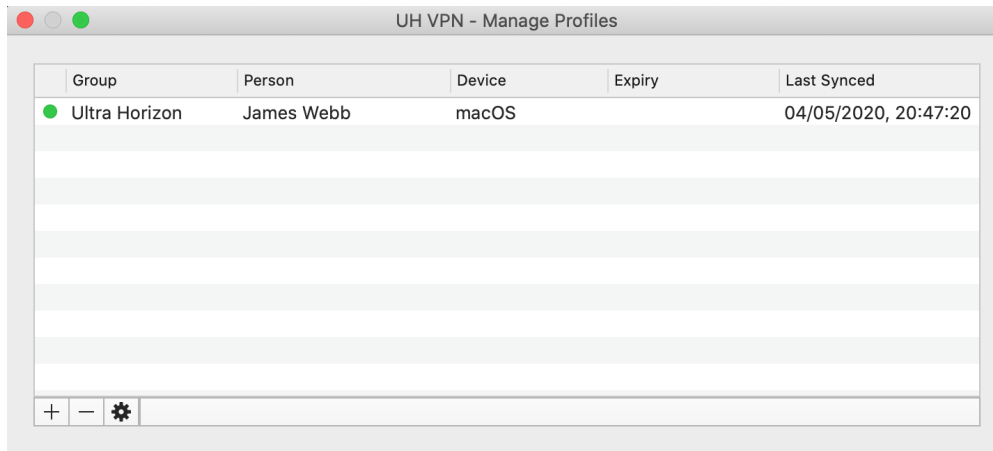
4.3.2 Adding Profiles

Adding VPN profiles within the macOS application is simple. First, one simply needs to click the “Manage Profiles” button within the menu bar list:

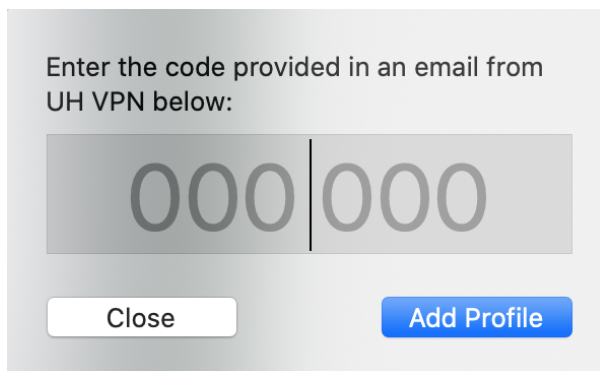


Note: If this is the first time a profile has been added, you will be asked to accept Ultra Horizon’s [Terms of Service](#) and [Privacy Policy](#).

The manage profiles window will then appear:



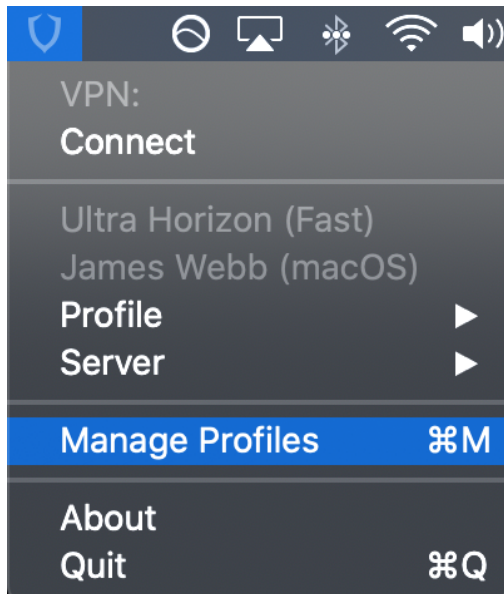
Simply press the “+” button in the bottom left of the window to bring up an OTP prompt:



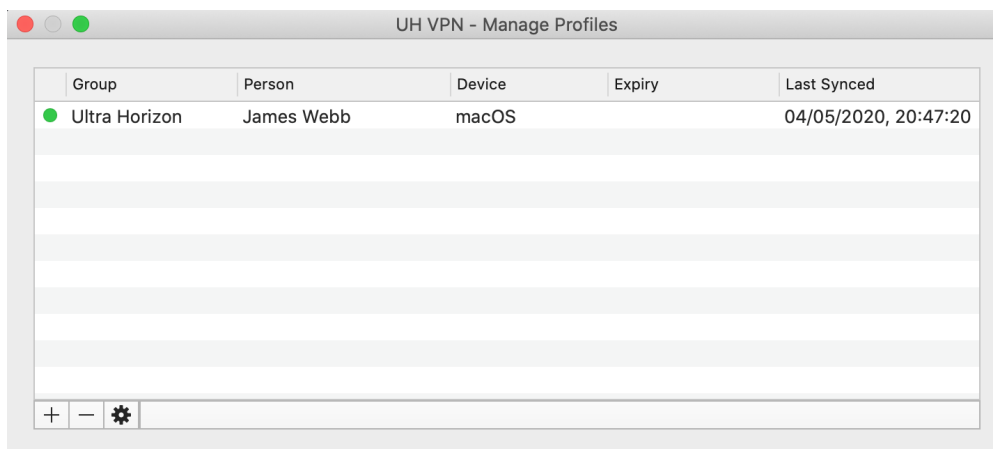
Enter the six digit code which will have been received in an email. Once this is entered, the UH VPN profile will then be securely downloaded to the device ready for use and will appear in the Manage Profiles window.

4.3.3 Deleting Profiles

Deleting VPN profiles within the macOS application is simple. First, one simply needs to click the “Manage Profiles” button within the menu bar list:



The manage profiles window will then appear:



Simply click on the profile you'd like to remove so that it highlights blue and then press the “-” button in the bottom left of the window to remove the profile.

Note: Deleting profiles cannot be undone and access to any UH VPN Servers associated with the group in question will be lost. New profiles must be issued from the UH VPN [website](#).

4.4 Windows



The UH VPN Windows application can be downloaded by clicking the badge at the top of the page. The sections below detail specific instructions on how to use the Windows application.

4.4.1 Installation

Upon downloading the MSI Installer, double click on it to install UH VPN.

You may receive a “Windows protected your PC” SmartScreen warning when launching the installer. Click on “More Info” and then a “Run anyway” button will appear allowing you to continue with the installation.

Verifying the Installer File (Advanced Users Only)

To verify the installer you can check the SHA256 hash with PowerShell. Either navigate to the file in PowerShell, or navigate to the file in Windows Explorer and hold Shift and Right Click, and select “Open PowerShell window here”.

Once in PowerShell and in the same folder as the MSI installer, run the following command:

```
Get-FileHash .\uh-vpn-installer_1.0.4.msi
```

The output should be as follows, pay close attention that the Hash is exactly the same.

```
Algorithm      Hash
-----
SHA256         DCA433813F041B0F2E84D41CF1392DF548E8705549606CD52E93006EA34064F9
→ uh-vpn-installer_1.0.4.msi
... Older versions (for reference):
SHA256         92D7BCE435987EFF7F266BC54A751E5443593FF036575931F5E69229432CBD08
→ uh-vpn-installer_1.0.3.msi
SHA256         C85C9140B9598009D8B6DBC684247263BB8559B5A4079F476FC3B8E40BCDD648
→ uh-vpn-installer_1.0.2.msi
SHA256         1FE952AE389CDEF4F430980C07C6FF29CA7CCD38CD80EF32E19717F2646AAE44
→ uh-vpn-installer_1.0.1.msi
SHA256         32361FCCF91C9D491AD790011CBC529DEC39A0F33EF10B0862BF939A7C4C089A
→ uh-vpn-installer_1.0.0.msi
```

Alternatively, one can right click on the MSI in Windows File Explorer and select “Properties”. In the properties dialog, select the “Digital Signatures” tab, then “Details” for the signature, then “View Certificate”.

In the Certificate dialog go to the “Details” tab, and find the “Thumbprint”. It should match:

```
ccaef34bfe6f8c8d180b240392487f4de45ed887
```

If you have any further questions feel free to raise an issue on our [issue tracker](#).

4.5 Linux

At present, UH VPN does not provide a Linux application, but will be releasing one by the end of 2020 targeted at Ubuntu. In order to provide connectivity to Linux clients, a static profile must be [exported](#).

Before the profile can be used, one must install OpenVPN using their appropriate package manager. For example, on Ubuntu the following commands would be executed:

```
sudo apt-get update
sudo apt-get install openvpn
```

Once OpenVPN has been installed and the UH VPN profile has been exported and is present on your local filesystem, it can be utilised via executing the following command:

```
sudo openvpn --config <profile>.ovpn
```

where `<profile>` is substituted for the filename of UH VPN profile. Note that the credentials must then be supplied from the `credentials.txt` file supplied with the static profile.

Note: One may wish to append the `.ovpn` profile with the `up/down` directives in order to execute commands upon connection or disconnection from the UH VPN server.

SECURITY

UH VPN utilises the latest standards in networking and cryptography and aims to be fully transparent with respect to the protocols used. To that end, the list below itemises all the cryptographic mechanisms used for each piece of infrastructure.

5.1 Website

- The website mandates HTTPS connections for all pages of the site and requires that TLS 1.2 be used.

5.2 API

- The API mandates HTTPS connections for all routes and requires that TLS 1.2 be used.
- Where infrastructure authentication is required (e.g. uh-vpn-server instances), a secret API token is used to provide access to a resource.
- Device profile synchronisation is handled by a proprietary one-time-code mechanism. A temporal nine digit code is exchanged for a JSON Web Token (JWT) which is signed by the UH VPN API. This JWT is stored within the device's secure enclave. Subsequent profile synchronisations utilise this JWT to gain access to a specific device profile.

5.3 VPN Tunnel

The underlying protocol used within UH VPN is OpenVPN. The following security parameters are chosen:

- Each server is generated a unique 4096 bit RSA key signed by the UH VPN CA.
- AES-256-GCM is used as the data encryption algorithm.
- ECDHE is used for symmetric key exchange and uses curve secp384r1.
- TLS version 1.2 is mandated.
- Symmetric data encryption keys are exchanged and replaced every 30 minutes.
- Client authentication is handled by the UH VPN API and is performed over HTTPS.

SUPPORT

6.1 Questions/Bugs/Features

For support with UH VPN please submit a question to our [GitHub issue platform](#). We aim to respond within two working days.

6.2 Sales

If you'd like to get in touch regarding enterprise deployments or custom built VPN technology please contact our sales team on +44 (0) 117 200 1107 or email us at sales@ultra-horizon.com.

6.3 Terms and Privacy

Our Terms of Service and Privacy Policy governing the operation of UH VPN can be found below:

6.3.1 UH VPN Privacy Policy

Ultra Horizon is committed to protecting your privacy. We want you to understand what information we collect, what we don't collect, and how we collect, use, and store information.

We do not collect logs relating to an organisation or user's activity, including no logging of browsing history, traffic destination, data content, or DNS queries. We also never store connection logs, meaning no logs of your IP address, your outgoing UH VPN IP address, connection timestamp, or session duration. This is fundamentally because the servers operating behind UH VPN are owned and controlled by user or organisation paying for the service.

Our guiding principle towards data collection is to only collect the minimal data required to operate a world-class secure network authorisation service at scale. We designed our systems to not have sensitive data about our customers; even when compelled we cannot provide data that we do not possess.

This privacy policy will help you understand how Ultra Horizon Ltd. collects, uses, and stores information.

Parties

In this privacy policy (up to and past this section), Ultra Horizon Ltd. will be referred to as “**Ultra Horizon**”, or the English first person plural: “**we**”, “**us**”, “**our**”, “**ours**”, or “**ourselves**”

UH VPN is a service that is provided to third party entities, which will be referred to as the “**entity**”, “**organisation**”, “**enterprise**”, or (unless otherwise specified) English third person plural: “**they**”, “**them**”, “**their**”, “**theirs**”, or “**themselves**”.

The service provided by UH VPN to the organisation is for use by whoever they wish be it clients, employees or other relations. These users will be referred to as the **users**, or (unless otherwise specified) English second person plural: “**you**”, “**your**”, “**yours**”, or “**yourselves**”.

Table of contents

- *Information stored about the Organisation*
- *Information stored about the users*
- *Aggregate information stored*
- *Information Related to Email Support*
- *VPN Tunnel Monitoring*
- *Jurisdiction and Applicable Law*
- *Security Measures*
- *Third-party Websites*
- *Consent and Age Restrictions*
- *Changes to the Privacy Policy*
- *Contacting Ultra Horizon*

Information stored about the organisation

This section is only applicable to the organisation and administrators making use of the management interface at <https://uh-vpn.com>. In this section, the second person plural (“**you**”, “**your**”, “**yours**”, or “**yourselves**”) refers to the individual account holders on management interface.

Information is collected for the purpose of administering the UH VPN subscription owned by the entity, and includes your email address which you submit when you sign up for our Services. This information is stored by our third party authentication provider, Auth0. All interactions with Auth0 are done over encrypted connections.

Information stored about the entity is for the purpose of maintaining the core UH VPN service, and includes the name, logo, one-time password expiry time and colour choices of the organisation.

Billing information collected when utilising groups with a core licence is held securely by our payment partner Stripe, please see [Stripe’s privacy policy](#) for more information. UH VPN securely sends stripe the number of devices in use, billing address, cardholder name and tokenized card details in order to facilitate future payments. Ultra Horizon Ltd is a VAT registered UK based company and so billing address details are required in order to determine VAT status on customer invoices.

In addition to the above, critical information to facilitate VPN connections to servers hosted by the entity are stored, including a server name, domain/IP address, port number, CA certificate, server certificate, server key, static TLS Key, routing information and transport protocol.

Finally, information pertaining to abstract persons and devices are kept by us. Information related to the person includes a string that represents a name for the person, along with an email address to deliver one-time passwords to. Information related to the device includes a string that represents the name of the device, along with an optional expiry time for the device. After generation of a device and until consumption, a one-time password that is associated with a group, person and device is also stored.

Information stored about the users

This section is only applicable to the users of the UH VPN native applications, be it on any mobile or desktop platform, and marks the return of the second person plural (“**you**”, “**your**”, “**yours**”, or “**yourselves**”) referring to the users.

The users are provided with a one-time password to their email address by the organisation when assigned a device profile. The organisation will have specified an identifier for them which may or may not be their name, along with an identifier for the device that the one-time password is entered on. Once consumed, this one-time password is removed from the server and the profile is synced by use of a cryptographically signed token (JWT) stored only on the users device.

No information is collected by Ultra Horizon about the app users.

After a profile is synced, the secure token is used to request from Ultra Horizon any updates pertaining to the device profile, including revocation and server configuration changes. All other interactions are then solely through the VPN connection directly to the organisation’s servers.

Aggregate information stored

Ultra Horizon collects minimal information about usage in order to maintain excellent customer support and quality of service. The section below describes in detail what specific information we collect. These statistics never include anything about what the user has done with the secure network connection: no data about the contents or destinations of traffic, no DNS queries, and no IP addresses.

For users of our VPN applications, we collect practically no metadata on usage. Similarly, for management users we only store a name and email address to allow unique identification of a UH VPN subscription.

We’ve engineered our systems to categorically eliminate storage of sensitive data. We stand by our firm commitment to our customers’ privacy by not possessing any data related to a user’s online activities.

App Data Collection

We do not add any of our own telemetry or tracking to any UH VPN web or native apps. Telemetry information including but not limited to installation/reviews/crash reports may be collected out of our control by third party app distribution platforms or operating systems.

In the rare event that you experience a problem with a native UH VPN app, you may be asked if you wish to submit a bug report automatically which will send you to a pre-populated report on our [issue tracker](<https://github.com/ultrahorizon/UH-VPN-Docs/issues/>), provided by GitHub. Pre-populated reports contain information about the platform that the app is on, the time of the crash, along with minimal critical debugging information that will allow us to identify the issue quickly. No reports are ever sent automatically, and you can preview all information before it is sent.

Connection Statistics

We ensure that we never log browsing history, traffic destination, data content, IP addresses, or DNS queries. Therefore:

- We do not know whether a user ever accessed a particular website or service.
- We do not know which user was connected to the secure network at a specific time or which UH VPN server IP addresses they used.
- We do not know the set of original IP addresses of a user's computer.

Should anyone try to compel Ultra Horizon to release retrospective user information based on any of the above, **we cannot supply this information because the data doesn't exist.**

Information Related to Email Support

In this section, the second person plural (“**you**”, “**your**”, “**yours**”, or “**yourselves**”) refers to the individual account holders on management interface.

Ultra Horizon keeps records of any correspondence, questions, complaints, or compliments you submit to us through our Site or Services, along with our response. Depending on how you contact Ultra Horizon, we may collect any information that is listed on your account and any subsequent information you provide to us. Having full correspondence records enables our staff to provide the best possible customer support experience.

We use one third-party platform for support correspondence: GitHub (for the remainder of this section referred to as the English third person plural: “**they**”, “**them**”, “**their**”, “**theirs**”, or “**themselves**”). When you correspond with us using this platform, your correspondence records, including your username are placed on our repository issue records. The platform utilises modern security practices and connections to this site are secured via HTTPS.

VPN Tunnel Monitoring

Ultra Horizon does not monitor or log any traffic being sent over the VPN tunnel. The only time Ultra Horizon has knowledge of information regarding a connection is to authenticate users logging into a server operated by an organisation. These authentications are logged and submitted to the UH VPN management interface.

Once connected, the secure VPN tunnel is direct from the organisation's server to the user. We do not have any access to the connections, nor can offer any guarantee about what happens to data upon arriving at the organisation. Users should be familiar with an organisation and their operating procedures/privacy policy and associated terms of service where applicable.

Jurisdiction and Applicable Law

Ultra Horizon's core mission is to keep your information private. We are a registered company in the United Kingdom.

Should we receive a valid legal order from the United Kingdom High Court to release information pertaining to a user, it is important to note that **Ultra Horizon does not collect any IP addresses, browsing history, encryption keys, traffic data, or DNS queries that could be used to identify any specific user.**

Security Measures

Ultra Horizon uses best-in-class physical, procedural, and technical security with respect to our offices and information storage facilities so as to prevent any loss, misuse, unauthorised access, disclosure, or modification of information. Access to user information is restricted to staff who require such access to perform their job functions.

Any servers provided by Ultra Horizon for use as endpoints by organisations are designed to these same standards, but may not be managed by Ultra Horizon.

Any profiles stored on a user's device are also encrypted and stored in the best means possible for the respective platform.

While we believe these systems are robust, it is important to understand that no data security measures in the world can offer 100% protection.

Even if a government were to physically seize a server, UH VPN endpoint, or user's device from us, the organisation or a user, there would be no logs or information that would tie any individual user to a particular event, website, or behaviour.

Third-party Websites

The websites operated by Ultra Horizon may contain links to external websites that do not fall under Ultra Horizon's domain. Ultra Horizon is not responsible for the privacy practices or content of such external websites.

Consent and Age Restrictions

By using the Website, Content, Apps, Software, or Services, you agree to have your information handled as described in our [Terms of Service](/terms) and this Privacy Policy.

The Services are intended for adults aged 18 and above. If you believe your child has provided information to us, please let us know immediately.

Changes to the Privacy Policy

We may change our Privacy Policy from time to time, without prior notice to you, consistent with applicable privacy laws and principles. Your continued use of the Website or Services constitutes your acceptance of our Privacy Policy.

Contacting Ultra Horizon

If you have any questions regarding our Privacy Policy and how we handle your information, please feel free to contact Ultra Horizon on the [contact page](#) of the website or get in touch via enquiries@ultra-horizon.com.

6.3.2 UH VPN Terms of Service

This Terms of Service document (the “**Terms**”) outlines the terms and conditions of use of the secure network services (the “**Services**” or “**Service**”) provided by Ultra Horizon Ltd (“**Ultra Horizon**”). These Terms also govern the use of and access to Ultra Horizon’s content (the “**Content**”), which includes the Ultra Horizon/UH VPN website (the “**Site**”), applications (the “**Apps**”), and any software provided by Ultra Horizon (the “**Software**”).

By agreeing to these Terms, you are also agreeing to the [Privacy Policy](#) (“**Privacy Policy**”).

Table of Contents

- *Acceptance*
- *Modification*
- *Privacy Policy*
- *Acceptable Use Policy*
- *Licence*
- *Language and Translation of Content*
- *Third-party Websites*
- *Disclaimers*
- *Limitations of Liability*
- *Indemnification*
- *Choice of Law*

Acceptance

By accessing the Content or Services, you are agreeing on behalf of yourself or those you represent (“**you**”) to comply with and be legally bound by these Terms in their entirety. These Terms constitute a legally binding agreement (the “**Agreement**”) between you and Ultra Horizon. If you do not agree with any part of the Terms, you may not use our Services.

By creating an account for using our Services, you represent that you are at least eighteen (18) years of age or that you are a valid legal entity, and that the registration information you have provided is accurate and complete.

Modification

Ultra Horizon may update the Terms from time to time without notice. If you continue to use Ultra Horizon’s Services, Content, Site, Apps, or Software after these changes take effect, then you agree to the revised Terms. You understand and agree that it is your obligation to review these Terms from time to time in order to stay informed on current rules and obligations. Your use of the Content or Services following the changes to these Terms constitutes your acceptance of the changed Terms.

Privacy Policy

Ultra Horizon is committed to your privacy and does not collect browsing history, traffic destination, data content, or DNS queries from users connected to UH VPN. During your registration, we may collect some personal information, such as your name and email address. We only collect information that is necessary for the proper delivery of the Site and Services.

For the sake of clarity and transparency, we have placed all information related to data collection in a separate document known as the [Privacy Policy](#), which is available on the UH VPN documentation hub. Please review the Privacy Policy in its entirety to get a clear understanding of how we handle your data.

Acceptable Use Policy

Ultra Horizon Services may be accessed from all around the world, so it is your responsibility to assess whether using the Site, Apps, Software, or Services is in compliance with local laws and regulations. Whenever you use the Site, Apps, Software, or Services, you should comply with these Terms and applicable laws, regulations, and policies.

You understand that it is your responsibility to keep your Ultra Horizon account information confidential. You are responsible for all activity under your account. If you ever discover or suspect that someone has accessed your account without your authorisation, you are advised to inform us immediately so that we may revoke your account credentials and issue new ones.

Ultra Horizon aims to provide the best service possible to all of our users. In that sense, we require that you do not misuse our Content or Services. A misuse refers to any use, access, or interference with the Content or Services contrary to the Terms or applicable laws and regulations.

In order to protect the Services from being misused or used to harm someone, Ultra Horizon reserves the right to take appropriate measures when our Services are being used contrary to these Terms and applicable laws. You agree that Ultra Horizon may terminate your account, without providing a refund for Services already paid, if you misuse the Service.

In using our Services, you agree not to:

- Send or transmit unsolicited advertisements or content (i.e., “spam”) over the Service.
- Send, post, or transmit over the Service any content which is illegal, hateful, threatening, insulting, or defamatory; infringes on intellectual property rights; invades privacy; or incites violence.
- Upload, download, post, reproduce, or distribute any content protected by copyright or any other proprietary right without first having obtained permission from the owner of the proprietary content.
- Upload, download, post, reproduce, or distribute any content that includes sexual or explicit depictions of minors.
- Engage in any conduct that restricts or inhibits any other user from using or enjoying the Service.
- Attempt to access, probe, or connect to computing devices without proper authorisation (i.e., any form of “hacking”).
- Attempt to compile, utilise, or distribute a list of IP addresses operated by Ultra Horizon in conjunction with the Service.
- Use the Service for anything other than lawful purposes.

Licence

Subject to your compliance with these Terms, Ultra Horizon grants to you a non-exclusive and limited license to download and use the Software. Modifying, distributing to unauthorised parties, reverse engineering, or otherwise using the Software in any way not expressly authorised by Ultra Horizon is strictly prohibited.

Usage of any material which is subject to Ultra Horizon's intellectual property rights is prohibited unless you have been provided with explicit written consent by Ultra Horizon.

Language and Translation of Content

All of our Content was originally written in English. Any translation of our Content is done on a best-effort basis. We cannot guarantee the accuracy of translated Content. In the event of any discrepancy between the translated Content and the English Content, the English Content shall prevail.

Payments

If you are a core licence customer you will be billed monthly at the rate of £4 +VAT per device. Device usage calculation is done via the maximum number of devices used within the billing period. Billing is handled via our payment partner, Stripe. Failed payments will freeze all VPN operations for a group until billing information is updated. If you delete a group during a billing cycle, you acknowledge that you will be billed immediately with no proration for the amount of devices used during the current billing month.

Third-party Websites

Ultra Horizon may provide you with content belonging to Third Parties ("Third Parties") or links leading to third-party websites. Ultra Horizon is not responsible for the availability of the content provided by Third Parties as they are not under the control or supervision of Ultra Horizon, and they may have different terms of use and policies. Your access through our Services to any website, service, or content provided by Third Parties does not indicate any relationship between Ultra Horizon and such Third Parties.

Disclaimers

We will strive to prevent interruptions to the Site and Services. However, these are provided on an "as-is" and "as-available" basis, and we do not warrant, either expressly or by implication, the accuracy of any materials or information provided through the Site or Service, or their suitability for any particular purpose. We expressly disclaim all warranties of any kind, whether express or implied, including but not limited to warranties of merchantability or fitness for a particular purpose, or non-infringement. We do not make any warranty that the Services will meet your requirements, or that it will be uninterrupted, timely, secure, or error-free, or that defects, if any, will be corrected. You acknowledge that you access the Site and Services at your sole risk and discretion.

UH VPN service coverage, latency, and overall service quality may vary. Ultra Horizon will attempt to make the Service available at all times. However, the Service may be subject to unavailability for a variety of factors beyond our control, including but not limited to emergencies; third-party-service failures; or transmission, equipment, or network problems or limitations, interference, or signal strength; and may be interrupted, refused, limited, or curtailed. We are not responsible for data, messages, or pages lost, not delivered, delayed, or misdirected because of interruptions or performance issues with the Service, communications services, or networks. We may impose usage or Service limits, suspend Service, terminate UH VPN accounts, or block certain kinds of usage in our sole discretion to protect Subscribers or the Service. The accuracy and timeliness of data received is not guaranteed; delays or omissions may occur.

Ultra Horizon reserves the right to investigate matters we consider to be violations of these Terms. We may, but are not obligated to, in our sole discretion and without notice, remove, block, filter, or restrict by any means any materials or information that we consider to be actual or potential violations of the restrictions set forth in these Terms, and any other activities that may subject Ultra Horizon or our customers to liability. Ultra Horizon disclaims any and all liability for any failure on our part to prevent such materials or information from being transmitted over the Service and/or into your computing device.

Limitations of Liability

Ultra Horizon shall not be liable and shall not have responsibility of any kind to any Subscriber or other individual for any loss or damage that you incur in the event of:

1. Any failure or interruption of the Site or Service;
2. Any act or omission of any Third Party involved in making the Site or Service or the data contained therein available to you;
3. Any other cause relating to your access or use, or inability to access or use, any portion of the Site or its Content;
4. Your interactions on the Site or Service;
5. Your failure to comply with this Agreement;
6. The cost of procurement of substitute goods or services; or
7. Unauthorized access to or alteration of your transmissions or data, whether or not the circumstances giving rise to such cause may have been within the control of Ultra Horizon or of any vendor providing software, services, or support for the Site or Service.

In no event will Ultra Horizon, its partners, affiliates, subsidiaries, members, officers, or employees be liable for any direct, special, indirect, consequential, or incidental damages, or for any other loss or damages of any kind, even if they have been advised of the possibility thereof. The foregoing shall not apply to the extent prohibited by applicable law.

Indemnification

You agree to indemnify, defend, and hold harmless Ultra Horizon, its officers, directors, employees, members, partners, agents, and suppliers, and their respective affiliates, officers, directors, employees, members, shareholders, partners, and agents, from any and all claims and expenses, including attorneys' fees, arising out of your use of the Content and Service, including but not limited to your violation of this Agreement. We may, at our sole discretion, assume the exclusive defence and control of any matter subject to indemnification by you. The assumption of such defence or control by us, however, shall not excuse any of your indemnity obligations.

Choice of Law

This Agreement shall be governed by and construed in accordance with the laws of the United Kingdom, excluding its rules governing conflicts of law.