

Reviewer's Guide

HMA VPN Version 5

HMA

- 1 – The privacy nuts are at it again: introducing HMA VPN version 5
- 2 – Where to get HMA VPN and how to install it
- 3 – How to use the new, fully redesigned HMA VPN
- 4 – Features: Privacy & Security
- 5 – Features: Location, location, location
- 6 – Features: Performance
- 7 – FAQs & Cheatsheets
- 8 – Contact

1 – The privacy nuts are at it again: introducing HMA VPN version 5



The Web used to be a wild frontier that transcended geographical and political boundaries, and gave people anonymity and freedom. Anyone could go online to share ideas and access anything from anywhere. Now, the Web has become dangerously fragmented along country lines. Everything people do online is tracked, packaged, and sold, or used to control what they can see and do — with consequences that are becoming all too clear every day.

HMA brings back online privacy so people can once again experience freedom on the Web. We've been around for a long time: We were one of the founders of this whole consumer VPN game. And while we're proud of what we've done with Version 5, it isn't just our most ambitious update, yet: it's also the on-ramp for a really aggressive set of improvements we're going to be making to our VPN, and to the industry as a whole. Here's how HMA VPN V5 takes the next steps in online privacy and freedom.

A brief history of our VPN

In 2005, at the age of 16, Jack Cator sought to get around his school's firewall and wrote the very first HMA proxy client himself. Realizing he's not the only one in need for such a product, he began growing his privacy empire with one mission: making sure people can access what they want, from wherever they are, and stay private doing so. And so, HMA VPN was born.

A decade later, HMA had grown into one of the most well known VPNs on the market, which led to it being acquired twice: First in 2015 by AVG, and then again when AVG was acquired in 2016 by Avast, the world leader in consumer security. And we'll admit it: that was a rough ride. Don't let anyone tell you otherwise: Being acquired is never an easy thing. But after a couple of years of dormancy, HMA's dusting itself off and picking up its mission where it left off: providing online privacy and freedom on every major platform PC, Mac, iOS, Android, Linux, and even routers. This reviewer's guide dives deep into HMA VPN V5, its features, and what's changed since the last release.

4 reasons everyone needs a VPN...

1. **Online privacy:** IP addresses are used by ISPs, advertisers, and others to track, store, or sell the data collected from people's online activities. A VPN lets you mask your IP address, so you can hide your activities.
2. **Online security:** Hotspots are everywhere these days, just begging us to connect and save on our data plans. But you never know who else is on that network or who's running the access point. A VPN protects you by encrypting your connection to the web, making sure no one can eavesdrop on — or steal — your data.
3. **Get around censorship:** Some governments and institutions, like workplaces or schools, only want people to access "approved" information and media. A VPN gives people back their freedom.
4. **Access content from around the world:** The web isn't created equal anymore, and some services just aren't available outside certain countries. A VPN helps users get around these restrictions.

...and 5 reasons why people need HMA VPN 5

We're secure: All of our clients are set to run the highest available encryption (256-bit AES) by default, all of our servers use full-disk encryption to protect them from hacks, thefts, or seizures, and all requests we field go through our own secure DNS servers.

We're everywhere: We've got 1000+ servers in over 290 locations across 190 countries. With so many places to choose from, you're never far from a fast, stable connection.

We're easy: We've gone beyond just flipping a switch to let people browse privately from anywhere in the world — we've made it so you're automatically protected if you connect to an unknown network. So go on: just set and forget.

We're on everything: HMA runs not just on the most popular platforms like Windows, macOS, iOS, Android, and Linux, but can be installed on compatible routers to protect entire networks of devices.

Our 24/7 support team has fans: Our support team are the heart of HMA. Always have been. Unlike many VPNs out there, that's one pace we don't skimp on.



This is HMA VPN V5 – 8 new key features at a glance

NEW Completely redesigned by user feedback

This is the biggest update in HMA history, and radically changes many of the core ways our client applications work. It still packs a punch, but we've kept things simple while making those more advanced features accessible to everyday users.

[Read more about the new design](#)

NEW IP Refresh

Facing a block? IP Refresh gets you a new IP address in the same location your working from with just a tap from the main dashboard.

[Read more about IP Refresh](#)

NEW Kill Switch

Whenever the connection to a VPN server drops for any reason, there's the potential your real location and online activities will leak and be picked up. To avoid this, HMA's Kill Switch stops all network communications entirely until secure connection to our servers is reestablished. Available on Mac, Windows, and Android.

[Read more about Kill Switch](#)

NEW Smarter App Kill Switch

We pushed our application-level kill switch a little further this time around. Now, when you

launch an application from the list, HMA will immediately turn on and open up a tunnel – even if it is off.

[Read more about Smarter App Kill Switch](#)

NEW Split-Tunneling

Total, all-encompassing encryption is great, but sometimes you just want one app to securely operate from one location, while the rest of your system stays local, or vice versa. Well, now you can do just that. On Android only.

[Read more about Split-Tunneling](#)

NEW Speed Test

We're bringing back one of the classic HMA features most requested by our users: Speed Tests. Now, you can check to see what speeds you'll get on any one of our servers right from within the app. This feature is now on Mac clients, and will be rolling it out to Windows versions soon.

[Read more about Speed Test](#)

NEW Faster Servers

We are deploying new 20Gbps servers across our infrastructure. Our core data centers already use them, giving a quarter of all HMA VPN sessions 200% increases in peak performance.

[Read more about Faster Servers](#)

NEW Less Logging

We're always taking steps to improve your priva-

cy. Effective 2019, our servers no longer collect your originating IP address, and we delete all logs we have on a 30 day rolling basis.

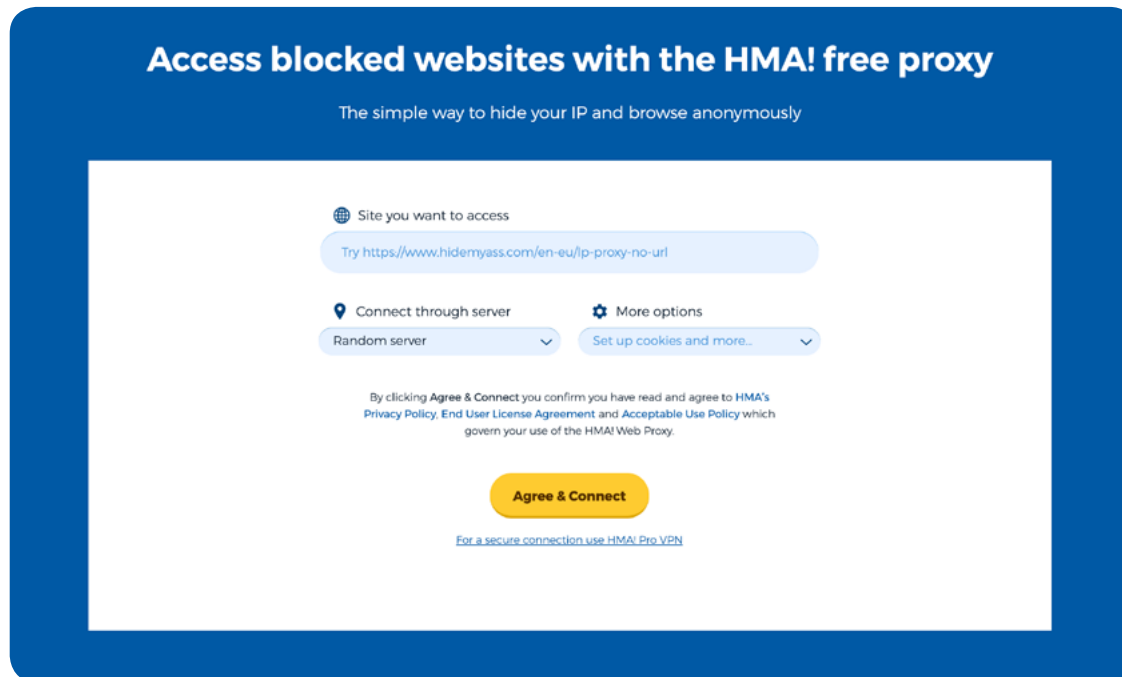
[Read more about reduced logging](#)

Other HMA Products

Blast from the past: the free HMA web proxy

By popular request, we've brought back the original, free HMA proxy on our website. No need for any 3rd party application or client: just fire up your browser, head to www.hidemyass.com/proxy, and you can connect to servers in the US, Germany, the Netherlands, the UK and the Czech Republic.

But we didn't just revive it, we brought it back with a few tweaks to improve your privacy: it now encrypts the URLs that get stored in your history (in case you forgot to use incognito mode), turns off cookies, and even removes scripts.



The screenshot shows the HMA! free proxy interface. At the top, a blue header contains the text "Access blocked websites with the HMA! free proxy" and "The simple way to hide your IP and browse anonymously". Below this is a white form area. The first section is "Site you want to access" with a text input field containing "Try https://www.hidemyass.com/en-eu/ip-proxy-no-url". The second section is "Connect through server" with a dropdown menu showing "Random server". To the right of this is a "More options" section with a dropdown menu showing "Set up cookies and more...". Below these sections is a small text block stating: "By clicking **Agree & Connect** you confirm you have read and agree to HMA's Privacy Policy, End User License Agreement and Acceptable Use Policy which govern your use of the HMA! Web Proxy." Below this text is a large yellow button labeled "Agree & Connect". At the bottom of the form, there is a link that says "For a secure connection use HMA! Pro VPN".

2 – Where to get HMA VPN and how to install it



How to install on Windows, Mac, iOS and Android

Anyone can head out to our main download pages on www.hidemypass.com/downloads to sign up for a free trial or purchase HMA VPN for the various different platforms we support. And of course, all mobile clients can be found in their respective app stores.

Reviewers can get the [latest build online](#) and request license keys from their local HMA PR contact.

How to install on Linux

For our Linux users out there, we're providing instructions for setting up a variety of [clientless configurations](#) on your favorite distributions. You can also run our [OpenVPN configuration scripts to speed things up](#).

How to install HMA on routers

HMA can also be setup to run on routers. This is a great way to cover all of the devices running on your network.

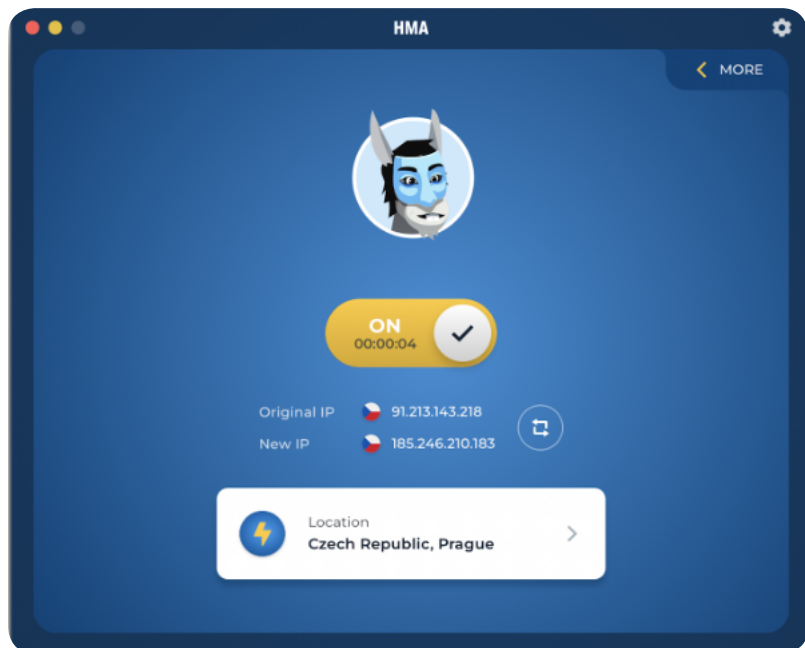
Configurations are different depending on the make and model, [but you can find updated instructions here](#).

3 – How to use the new, fully redesigned HMA VPN



We've sent thousands of surveys, and spent hundreds of hours doing research with longtime HMA users, users of competitor products, and people who'd never heard of a VPN to figure out what the core of the product should be.

Here are some of the biggest changes you'll see:

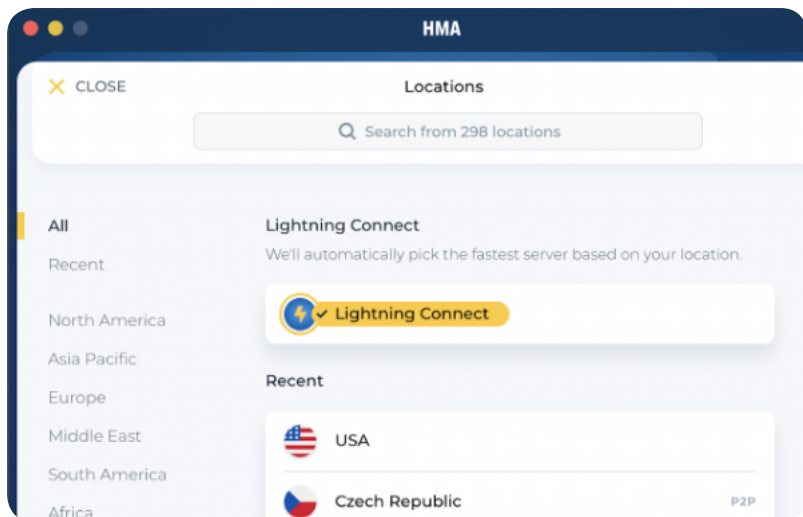


No more modes – just a switch

How you turn on HMA is now simpler than ever. While we were big fans of the three modes, and they did meet the needs of some of you perfectly, many more of you were just confused and thought they did the same thing. Now, there's just a single switch to get your privacy going.

How to use it

Just click or tap on the switch in the center of the dashboard on any HMA VPN client.



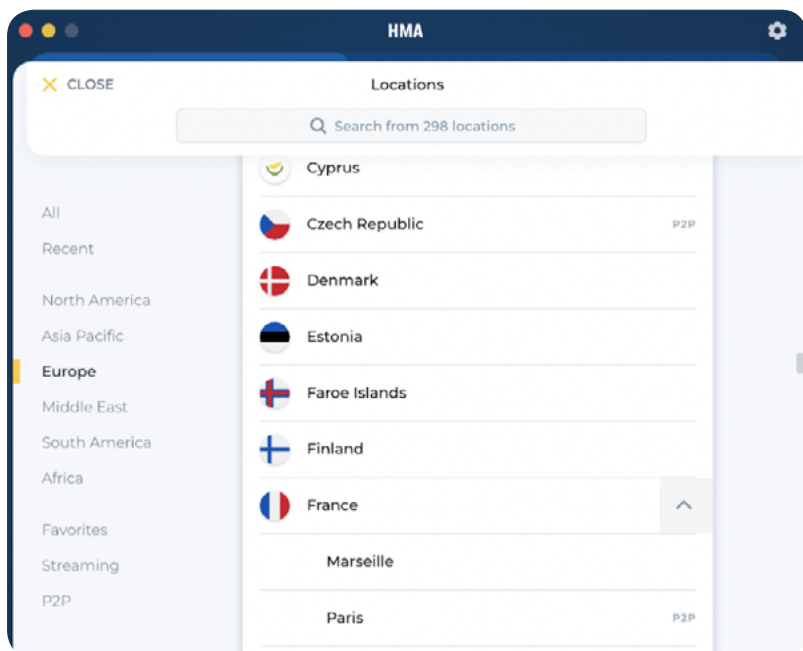
Instant Mode is now Lightning Connect

The modes did have useful functions, and the most useful was “Instant Mode”, which took the guesswork out of finding the faster server for you. We’ve re-branded it Lightning Connect, and you’ll find it at the top of your location list.

How to use

If you haven’t yet changed locations yet, simply turning on the VPN will automatically put you on Lightning Connect.

If you have already changed locations, you can just open the location list, and pick it from the top as if you were picking any other regular location.



A brand new Location List

Speaking of location list: our long time fans know that we have a stupid amount of locations for you to choose from. It’s always been a part of what makes HMA more than just a cool excuse to make donkey puns. But listing that out alphabetically really wasn’t the most efficient way to help you sort through such a massive choice.

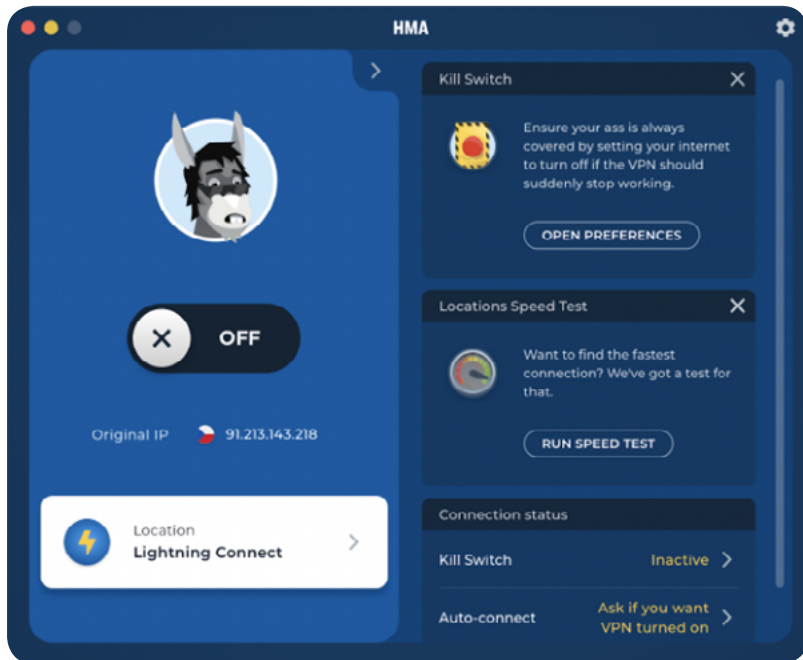
Our new design brings a lot of usability benefits:

- All countries are organized by continents.
- Picking a country now gives you the fastest location within that country, without forcing you to hunt those down.
- City-level locations are now roped in dropdowns under their respective countries.
- All specialty streaming and P2P servers and locations you’ve marked favorite are now easily accessible on the side navigation.

How to use:

To open the location list, tap on the big white button at the bottom of the main dashboard.

You can use the side index of regions and server types to make your way faster.



Making things easier

Finally, all HMA VPN v5 clients now come with a side-panel that will highlight, explain, and give quick access to the more advanced settings like Kill Switch, Split-Tunneling, Auto-connect rules, and more. We'll also highlight privacy tips and insights just when you need them.

How to use

On Windows and Mac: simply click on the **More** button on the top right of the dashboard to open the side-panel.

On iOS or Android, simply tap on **Advanced** on the bottom navigation. You can then engage with the different cards, or dismiss them in the case of messages.

4 – Features: Privacy & Security

Mission priority number one for any VPN is to allow users to surf privately and securely. Period. While we'll be focusing on some great new additions on that front, we'll also be shining a light on some of our older features and the things we do in the background to ensure your security and privacy.

NEW – Less logging

It's been a long time coming, but we're making 2 big changes in how our servers log information.

1. HMA no longer collects your exact IP address

We anonymize the last octet of any IP address connecting to our servers (i.e. 92.145.233.343 becomes 92.145.233.000), so it is effectively no longer possible for your IP to be tied back to you.

But you may be wondering why we didn't we just opt to drop the entire IP address from the logs?

Collecting the subnet gives us a rough indication of the demand we're seeing from different regions, and helps us plan the deployment of additional servers or upgrades. This is invaluable information in helping us improve our service. Many VPNs will claim to not log any detail of IP address at all while still collecting subnets for the same reasons — but we've always been transparent about what we do and why, and we will continue to do so.

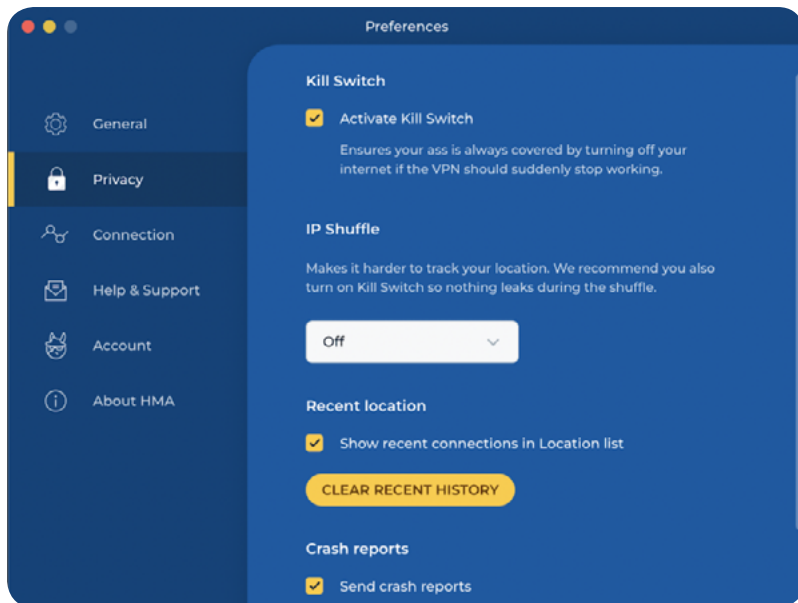
2. All connection logs gets deleted for 30 days, on a rolling basis

Any data created from a unique VPN session on Jan 3rd gets deleted on Feb 2nd. The type of data that gets logged:

Service Data	What we use it for
Timestamps of your connections	To manage the number of concurrent active connections, and handle abuse. Example: We use them to stop brute force password cracking attempts on user accounts.
The subnet of your originating IP address. E.g. We anonymize the last octet to protect your privacy: 92.143.234.000 We don't collect exact IP addresses that could ID you.	To plan for increased network demand and capacity. Example: Help us decide to add servers in a region if we see a rise in demand there, or help troubleshoot issues with a specific ISP.
IP address of the HMA server you're using.	IP address of the HMA server you're using. To troubleshoot our service and plan for new network capacity. Example: Identify when an IP address suddenly doesn't work for accessing certain services, and act to resolve the issue.
Amount of data transmitted E.G. 5GB up or down	To plan for new network capacity and server improvements. Example: We may deploy more capacity to meet demand and make sure speeds stay up for all users.

To be clear: Our VPNs have never collected any data about the applications you use, the services you use, the websites you connect to — basically anything you do online.

We've always stood by our word and been transparent about our logging practices, and have updated our privacy policy to be comprehensive, explicit, and extremely simple to read to continue to earn that trust. [Go read it here.](#)



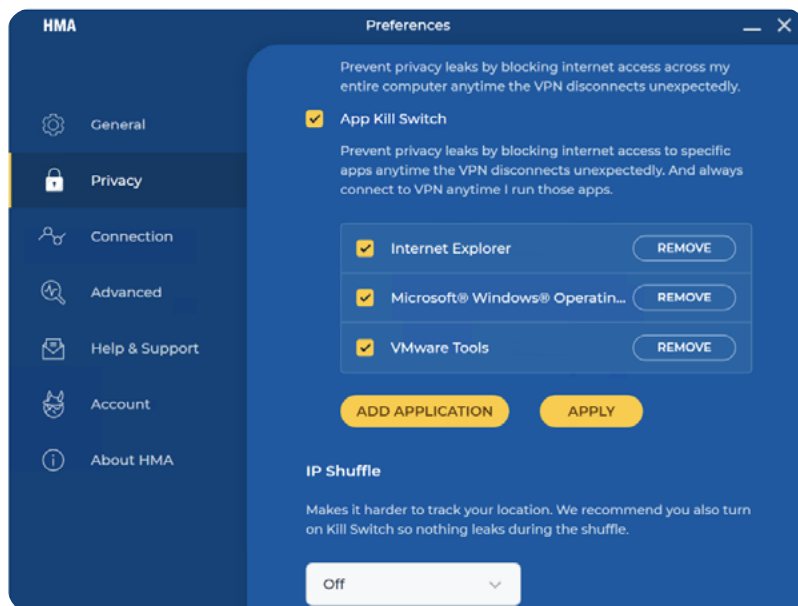
NEW – IP Refresh

Coming across a blocked website used to mean a tedious game of trying other servers until one worked. This is one of the most common frustrations expressed by our users, and we're taking that out by the back shed and OldYeller-ing it for good.

You now have an easily accessible Refresh IP option right on the main screen. One tap, and you'll get a new IP address from the same location you are working with, and can cycle through our available ones until you've got a winner.

How to use it

Once you are connected, you will see the option to refresh your assigned IP address appear on the main dashboard. Simply tap it to get a new one.



NEW – Kill Switch

Nothing's perfect. Sometimes, the connection to our secure servers may drop, whether that's due to a firewall setting, server outage, limited bandwidth, a freak act of God... You get the idea.

But when that happens, your devices are designed to fall back on their feet and reconnect immediately – outside the protection of your VPN. This can suddenly expose your real location and whatever you're up to.

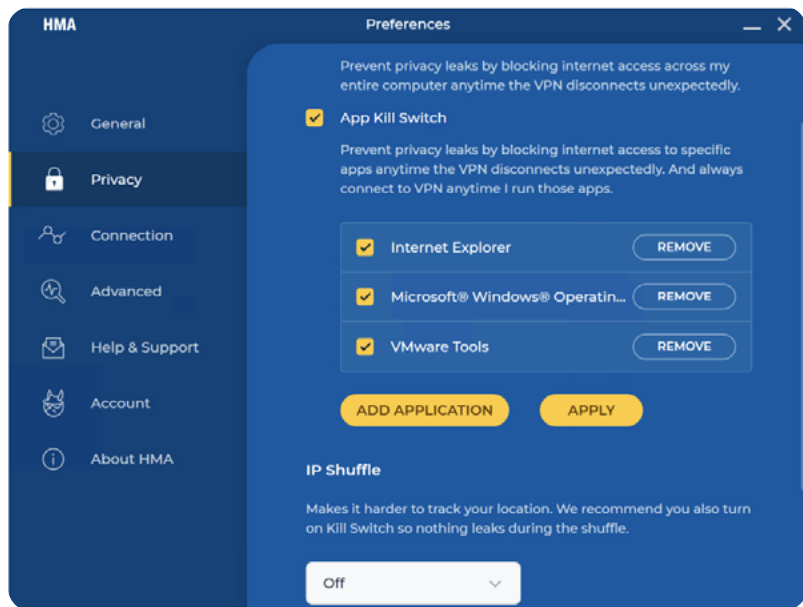
When those drops happen, **HMA's Kill Switch** automatically cuts the internet connection entirely, so not a peep of data gets out. It's the mother of all fail-safes.

How to turn it on

On **PC, Mac or Android**, you'll find the Kill Switch in the side-panel. Simply click **More** on desktop clients, and **Advanced** on the bottom navigation.

Alternatively, you can also look for it in the settings. On PC, Mac, look for the Kill Switch in Settings > Privacy. On Android, you can find it in the Menu > Settings.

Once there, just tick the box and you're set.



NEW – Smarter App Kill Switch

If you know precisely which apps represent a privacy risk, the App Kill Switch on Windows gives you surgical precision in terms of what shouldn't be allowed to keep communicating with the Internet when your connection drops.

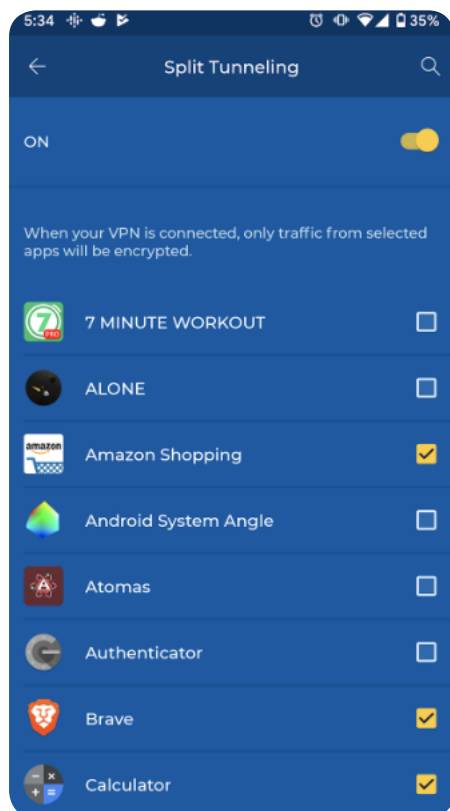
Our research has shown that people tend to use the same applications over and over with their VPN, and launching them without the VPN on can expose their personal data. So our new Smarter App Kill Switch won't just kill them when a connection drops: It will also start a VPN tunnel when they're launched, to make sure they can never connect outside the protection of HMA. And in the case of a dropped connection, it will seek to automatically reestablish the tunnel before letting the apps reconnect.

How to use

On **Windows**, you'll find a quick access to the **App Kill Switch** in the side-panel. Just open it up by clicking on **More** in the top right of the main dashboard. Alternatively, you can also find it by going into **Settings > Privacy**.

Once there:

1. Tick the box to activate the App Kill Switch.
2. Click **Add Application** and pick the executable file you would like to protect.
3. Click **Apply**. If you've picked any application that is currently running, the VPN will turn on automatically if it is off.
4. At any time, you can tick the box next to each application to disable the **App Kill Switch** for it, or you can permanently remove it by clicking **Remove**.



New – Split-Tunneling

Split-tunneling lets you decide which apps go through the HMA VPN tunnel, and which don't, giving you more flexibility in how and when you change locations or add protection. So you're now free to multitask your brain to mush across different geographies: stream some brain-damaging show from one region while browsing the equivalent of BuzzFeed from another.

How to use

On Android:

1. You can find Split-Tunneling under **Menu > Settings**. Or to make things easier, simply pick **Advanced** in the bottom navigation, and you'll find a quick access to Split-Tunneling there.
2. Flick the switch to turn it on.
3. Select the applications you want to keep within the encrypted tunnel. Any application that doesn't have a check will access the internet normally.
4. You can find an **All Apps** selector at the top to toggle all the apps on or off at once.

IP Shuffle

Encrypting your traffic, masking your IP address, and picking a virtual location that is different from yours are all ways of protecting your privacy from prying eyes. But HMA VPN goes one step further: **IP Shuffle** randomly changes IP addresses in order to make it even harder for third parties to track your online activities.

You can choose shuffle at predetermined intervals, or set a custom one. And don't worry about your location: you'll only cycle through IP addresses in the same location you had selected, so that services you want to access in that region still work.

While you're shuffling, your device switches between assigned IP addresses, so you'll be prompted to make sure the Kill Switch is active to prevent any data leaks.



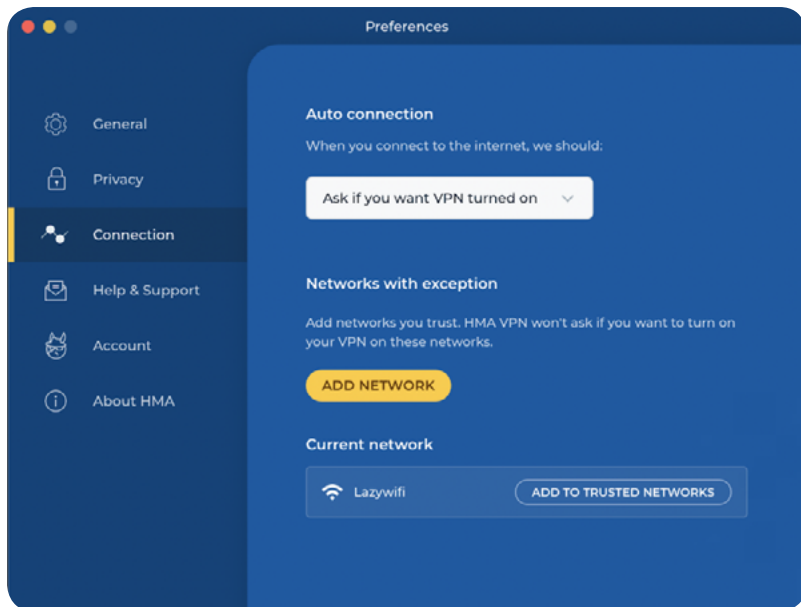
How to turn it on

On PC, Mac, look for **IP Shuffle** under **Settings > Privacy**.

On Android, look for it under **Menu > Settings**.

Once there, turn it on, and you'll be able to set the time interval you want to use. In addition, the countdown to the next shuffle will appear in the side-panel.

iOS devices don't have a setting: iOS switches IP addresses every time your screen is turned off by default.



Auto-Connection Rules

We're more mobile than ever, replacing desktops with laptops, and laptops with smartphones or tablets. And the temptation to get a piece of that sweet free WiFi and save on your mobile plan is just too good to pass up. But that also means we're connecting to more and more hotspots run by people we don't know, with security measures we can't assess.

That's why we baked-in **Auto-Connection Rules** into HMA. You can set your protection to turn on automatically whenever you connect to a WiFi Network, or to ask you if you'd like to turn it on.

So go ahead: connect anywhere you want and save on your mobile data plan. HMA's got you covered.

How to turn it on

The status of your **Connection Rules** will always be visible in the side-panel on each client.

Alternatively, you can find them under **Settings > Connection** on Windows and Mac, and under **Menu > Settings** on Android. iOS's rules can be found in the **Settings**.

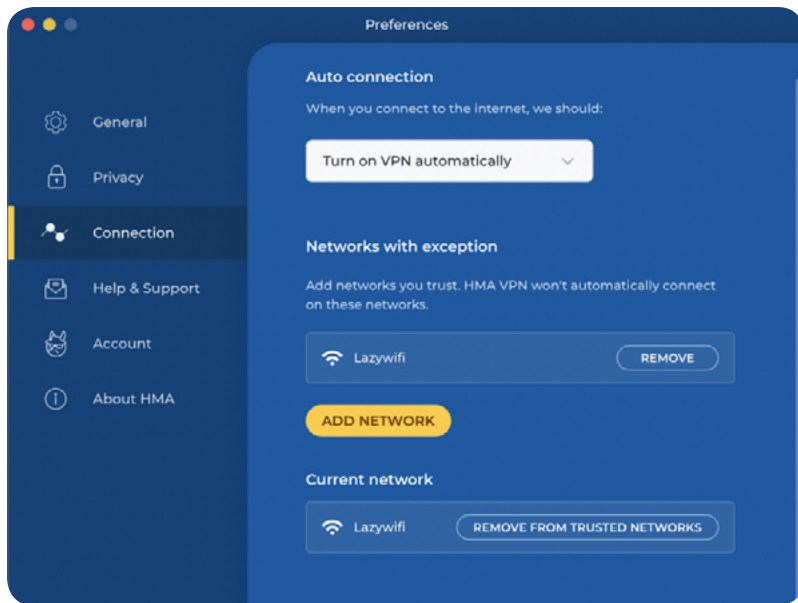
Once there, you'll be offered to choose how you want the rules to operate:

On Mac and Windows

- Do Nothing
- Turn on the VPN automatically
- Ask if you want the VPN to turn on

On Android and iOS

- Never. Don't be so presumptuous
- You connect to unsecured WiFi
- You connect to any WiFi
- You connect to WiFi or cellular data



Trusted Networks

The flipside of the coin: if you actually know a network and trust it's safe, then there's no need for HMA to cover your back, right? No problem. Just tell it you trust the network, and it will exclude that network from triggering the auto-connection.

HMA will always detect the current networks you're connected to so you can easily add them.

How to turn it on

You'll find the Trusted Networks under in the **Settings > Connection** on your PC and Mac, and under settings on your Android and iOS clients.

On Mac, Android and iOS: You'll be able to add the network you are currently connected to, and see the list of all of your trusted networks.

On Windows, you'll be able to piggy back on how the operating system defines what is a private and public network, and the autoconnection rules will work from there. You can always define that on your own as well.

The other privacy and security measures we take behind the scenes



Single Shared IP – Lost in the crowd

Whenever you connect to one of our servers, you're sharing the IP address we assign you with everyone else that's using that server – making it that much harder for anyone to pin down who's doing what.

HMA Private DNS – A safe address book to the internet

Domain Name Systems servers translate your URL requests into IP addresses that machines can understand. And if you're not using a secure one, you could be exposing every little thing you do online even if you do have a VPN – or worse, you could be redirected to a phishing site. HMA doesn't rely on third party DNS servers, but our own encrypted ones to make sure your activities stay private and safe.

Full-Disk Encryption on Servers – Every box is a Fort Knox

What good is a securely encrypted tunnel if your server base isn't protected? We don't horse around with your security and privacy here at HMA (in fact, we take offense at any horse-related activities), so that's why we've rolled out Full-Disk Encryption on all of our servers around the world. Whether it's hackers, thieves, or just good ol

Johnny Law seizing our servers – all they're getting is fuzz.

Leak Protection – Not a peep

We also make sure your IP address doesn't leak out of the encryption tunnel on IPv4, IPv6, or WebRTC, and that your DNS requests stay private.

DDOS Protection

Our servers offer robust protection against DDOS attacks. Combined with our great speeds and low pings, gamers using HMA can feel confident that they won't be sabotaged in the middle of their big moment...

How we lock it down – HMA Protocols

We use several different protocols depending on the platform:

OpenVPN on Windows and Android

OpenVPN is a tried and true protocol that is painstakingly updated on a regular basis. Our implementation uses the 256-bit Advanced Encryption Standard with the Galois/Counter Mode (**AES-256-GCM**) for symmetric encryption between clients and servers. Our handshakes use OpenSSL with **RSA 4096**-bit keys authenticated with **SHA256**.

IKEv2/IPSec on Mac and iOS

While there are many benefits to using OpenVPN, tight integration offers its own strengths. That's why on Apple's operating systems, we've opted to build our client on Apple's own stack of IKEv2/IPSec while applying the same 256-bit Advanced Encryption Standards.

This gives our Apple clients better connection and reconnection speeds and overall better tunnel stability.



5 – Features:

Location, location, location

We're no slouches when it comes to giving people access. In fact, there's barely a spot we don't cover. We're the world leaders in terms of supported countries. Let's walk you through why we're leading the pack.

More supported countries than the official count?

We've got 1000+ servers in 290+ locations across 190 countries! However, in some past communication, you may have seen us claim 220 countries. No, we did not lose countries.

"But wait a minute... There are only 195 official countries," you may be thinking. "These HMA people are trying to pull a fast one on me!"

Well, no so fast. You see, we didn't always use the "official" country count (whatever that means). We were using the current ISO 3166 list of country codes as a reference, and there are 249 countries listed there.

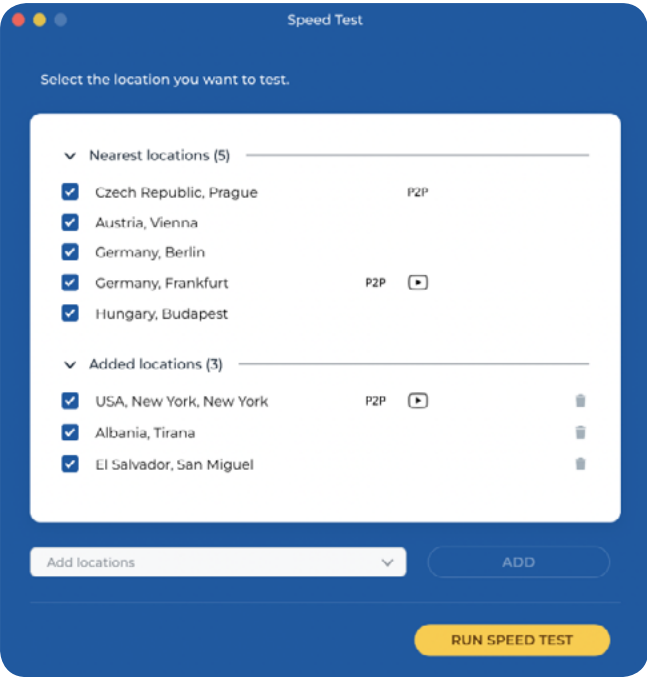
Why do we do that? Simple: If you're in the British Virgin islands, your fastest local server isn't the UK mainland, is it? But by focusing on country codes, we get to map out the world in a way that's a lot more reflective of people's reality.

And this way, we can give as much importance to the Vatican as we do to the Svalbard islands. (It's part of Norway. Look it up).

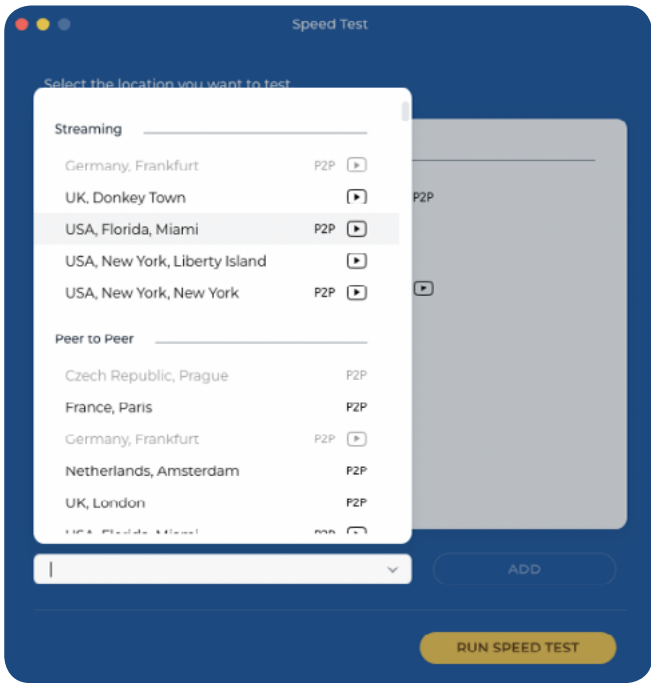


NEW Speed Test

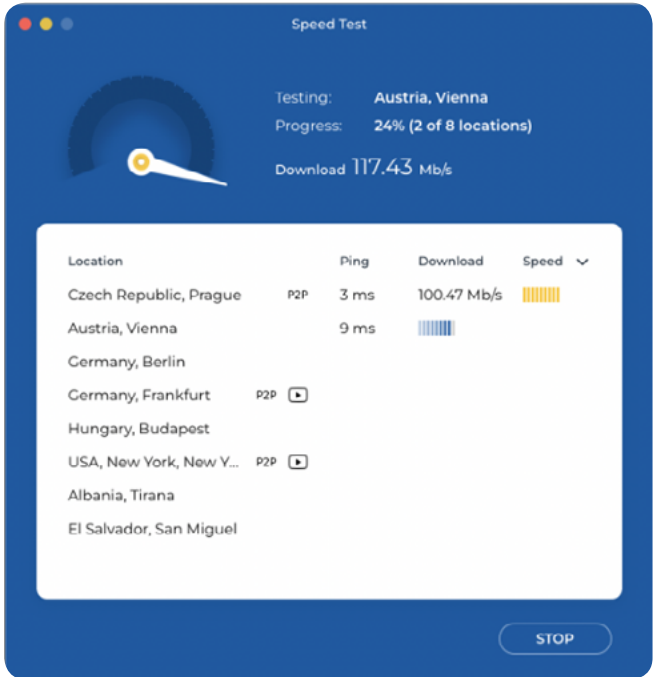
With so many locations, picking the best one for you can be difficult. Our Instant Mode and Location Mode can help make that pick for you, but some of you like doing it yourself. We heard you, and are bringing back the in-app Speed Test.



When you launch the test, it will load the 5 nearest servers to you. You can add any server you want from our list.



As the test runs, you'll see the results for both server Ping (time it takes for a data packet to do a roundtrip from your computer to the server) and Download speeds. Note that the maximums you will see will depend on your own network's speed: the best we can do is max out your speed – and that will usually be on the server closest to you. (If you suddenly find that your speeds improve more than what you usually get without a VPN, it may mean that your ISP is throttling your speed.)



We'll organize the results with from fastest to slowest based on a combination of download and ping times, with the fastest option shown at the top. But if you prefer a different kind of server, just click it to reveal connection options. Here you can see we've opted to go with the streaming and P2P optimized

Frankfurt location, despite it not being the fastest.

How to run the test

On Windows and Mac: You can find the **Speed Test** by clicking on the HMA icon in the System Tray on Windows, or in the **Menu Bar** on Mac.



6 – Features: Performance

Streaming, browsing, sharing anonymously is worth very little when the VPN server offers 56k-era bandwidth. Our hundreds of servers offer high-performance and low latency. Here's how.

NEW Upgrading to 20Gbps servers

By default, HMA automatically switches you to the fastest available server in a selected country, so you don't have to go hunting for servers.

We're also constantly improving our facilities, moving them to networks with better connectivity or adding more servers in multiple countries, with new ones being added on a regular basis. For example, we recently upgraded servers in our core data centers to 20 Gbps, and many of our fringe ones run on 10 Gbps servers.

This means lower latency and better throughput across the board.

Performance Tests

But enough bragging. Let's put our money where our mouth is and run some tests.

The closer a VPN's download and upload is to the performance of the user's regular internet connection is key. If you see massive gains, your ISP may be throttling your connection.

With our extensive array of servers, and the fact that we built our service to pick the fastest servers in any location, you should always get the best possible results, and the VPN should be a non-issue while streaming.

Methodology:

Tests were conducted on Speedtest.net, Fast.com to see if we could handle 4K Streaming with Netflix, and on the gaming latency experienced on Rocket League.

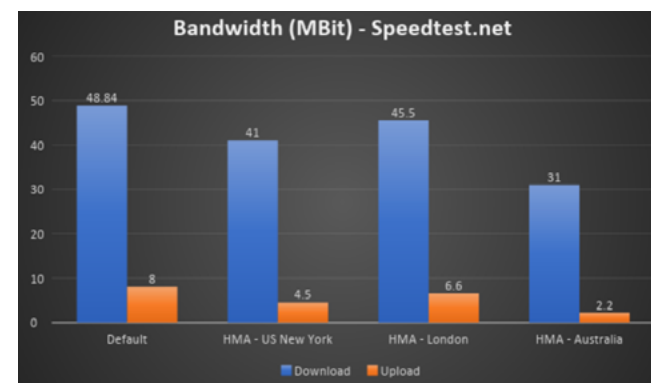
The tests were performed three times per week (weekend and weekdays) during multiple times of the day from a home network in Germany and averaged to provide the most accurate results.

Speedtest.net

Speedtest.net is a service offered by Ookla that tests the ping, download and upload speeds of your internet connection.

Results: In our first test, Speedtest.net showed that bandwidth was kept at high levels despite switching to servers around the globe. The original 48,84 Mbit download speed was not impacted noticeably when connecting from a Germany-based client to HMA's servers in New York or London, with **both operating well above 80%** of the original speed.

Although upload speeds suffered a bit across the board, this is rarely noticeable in common web usage. Even the far-flung servers of Australia were fast enough for 4K streaming, let alone regular online activity.

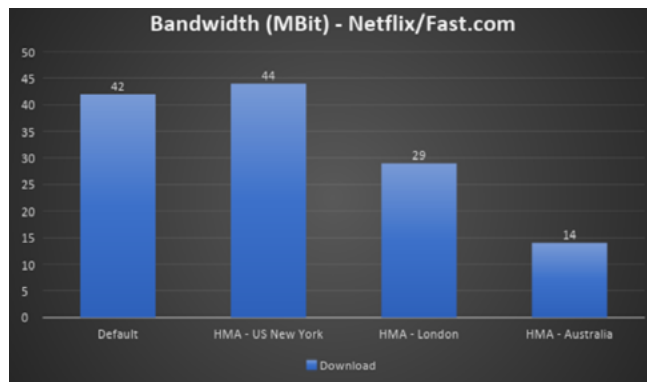


Fast.com

Fast.com tests internet connections using Netflix's streaming servers, making it an easy way to determine if the bandwidth is high enough for Full HD or even 4K streaming.

Results: Again, even when connecting to Australia, speeds never dropped below 14 Mbit which is roughly 3x the speed required for 1080p streaming.

The connection to London was more than enough to stream 4K HDR video material at 29 Mbit and the New York server offered even slightly higher bandwidth than the local connection to a German server. All in all: Streaming with HMA VPN was a flawless experience across the board.

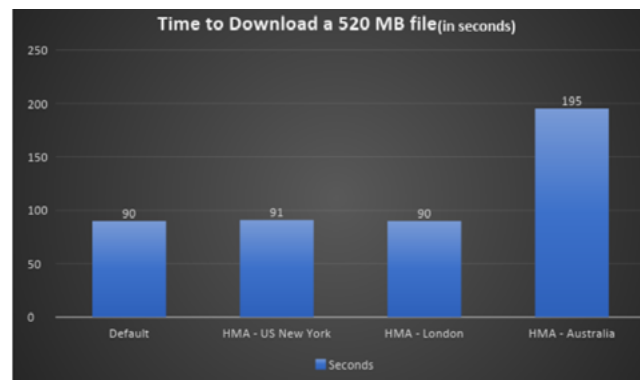


Real download test from NVidia.com

Temporary download speeds are great, but we wanted to see what happens how long it would take to download a real file: a 520Mb driver from NVidia.com.

Results: The download took roughly 90 seconds to complete, both without HMA active and when connecting to New York and London, giving us a constant download rate of 5.7-5.9 MB/sec.

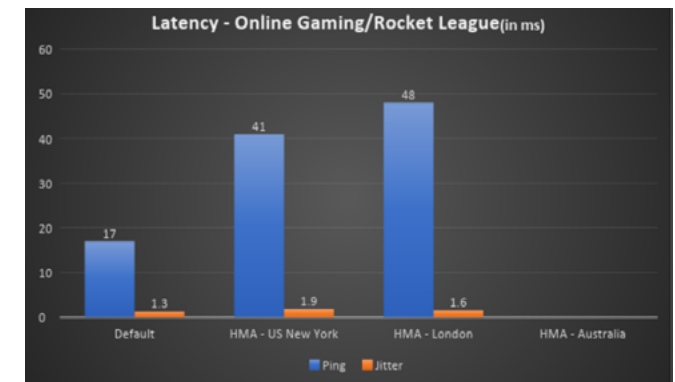
Even when connecting to the Australian server we still had the download completed in a manageable time at about 2.5-3 MB/sec.



Latency in gaming Rocket League

Rocket League is taking over esports by storm. And in a game of motorized football, your team-work lives and dies with your latency.

Results: Ping times went up from 17ms to 41 and 48 respectively, all of which are in line with a normal response rate and should not impact gaming in a perceivable way. Pings upwards of 200-500 are generally felt quite significantly. (Our Rocket League teams weren't available to play during Australian hours, unfortunately).



7 – FAQs & Cheatsheets

What platforms is HMA VPN available on?

- Windows 7 SP1 or later
- macOS 10.10 or later
- Android 5 or later
- iOS 9 or later
- Linux
- Routers that support VPNs or flashed with Tomato, OpenWrt, DD-Wrt, or other custom firmware.

How many devices can I install HMA VPN on?

You can install HMA on as many devices as you'd like, but only 5 can be connected to our servers simultaneously.

If something goes awry, such as random connection drops, how can I figure out what's going on?

HMA VPN comes with free 24/7 customer support.

On Windows and Mac, you'll find a Troubleshooting tool under Settings > Help & Support. This tool will run a series of diagnostic tests to see what's wrong. Any issues it detects will be issued a code that will speed up your experience with our support team.

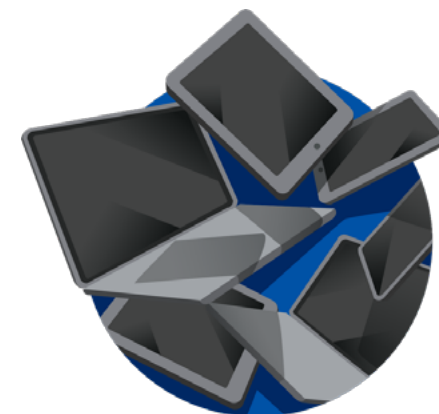
Is there a way I can protect not just my clients, but my entire network?

Yes! You can use HMA VPN with a variety of routers. More information on how to set it up [can be found here.](#)

You're based in the UK. Don't you have to obey the Snooper's Charter and retain data for a year?

No. The Snooper's Charter applies to electronic communications service under "telco" law, and doesn't apply to VPNs. Historically, we have never retained any VPN data for longer than 3 months, and our current retention period of any such data is 1 month.

As proof of that, you can [check our current Privacy Policy](#) and the [archives of its past iterations.](#)



VPN Basics Cheat Sheet

Client software	Windows, macOS, Android, iPhone
Manual 3rd party connections	Linux and supported routers
Max. devices connected at once	5 simultaneous connections
Number of servers	1000+
Number of countries	190+ (220+ under ISO country codes)
Number of locations	290+
Supported protocols	OpenVPN, IKEv2/IPsec
Data encryption type	AES-256-GCM
Handshake encryption	RSA-4096
Data authentication	SHA-256
Kill Switch	Windows, Mac, and Android
'Split-Tunneling	Android
Other key features	IP Shuffling, IP Refresh
DNS leak protection	'IPv4, IPv6 and WebRTC covered.
DNS Requests	'Encrypted with 1st party servers
'Single Shared IPs	Yes
Server protection	256-bit AES full-disk encryption
'Max Individual Server throughput	20 Gbps
Support	24/7 customer support via Live Chat or phone.
Guarantees	30-day Money back. No conditions.

8 – Contact

Provided in case you are working with particular individuals or agencies on this review.

If you have any questions about HMA VPN, please contact: Michael Healy at michael.healy@avast.com