Getting the most from your **nbn**™ Sky Muster™ satellite service when using a Virtual Private Network (VPN).

This guide is designed to help you optimise your internet experience when using a Virtual Private Network (VPN).^

What is the **nbn**™ Sky Muster™ satellite service?

- The **nbn**™ Sky Muster™ satellites sit 36,000km in a geo-stationary orbit above the equator and connects Australians across the country and surrounding islands to the internet.

- When the internet is in use, the data travels a round trip of 72,000km from your **nbn**™ satellite dish, up to the Sky Muster™ satellites and back down to the **nbn**™ satellite ground station in order to transmit the signal.

- This distance causes a delay in the transmission called latency.

^ Your experience, including the speeds actually achieved over the **nbn**™ network, depends on the **nbn**™ network technology and configuration over which services are delivered to your premises, whether you are using the internet during the busy period, and some factors outside **nbn**'s control (like your equipment quality, software, broadband plan, signal reception and how your service provider designs its network).

What is a Virtual Private Network (VPN)?

• A VPN is a private network that accesses the internet over a secure connection. Only authorised parties have access to this network.

• A VPN encrypts the traffic and the information being accessed on the network so it can't be seen by unauthorised parties.

• Using a VPN can cause limitations on your device when using the internet, which means it can slow down the connection.

• Internet traffic via VPN is metered* when using the **nbn**™ Sky Muster™ satellite network.

Why is the nbn™ Sky Muster™ satellite service slower when using a VPN connection?

• Internet activity such as browsing the web, sending emails and downloading documents uses a system which acknowledges when data has been received before sending more.

• On the **nbn**™ satellite network, this acknowledgement is delayed due to latency.

• To combat this, (when not using a VPN), **nbn** uses acceleration to acknowledge the data received mid-way through the network, rather than at the end. This helps ensure the data can be sent with as little delay as possible.

• When data is encrypted by a VPN, the acceleration is not possible. This reintroduces latency into the network, resulting in slower download and upload speeds; or network responsiveness.

What can I do to help optimise my internet connection?

Firstly, check and compare your service's speed with and without a VPN over the **nbn**™ network.^ This helps identify whether your slower speeds are due to the VPN connection, or if another factor is at play. To do this, perform a speed test using the following steps:

1. Connect your device to your **nbn**™ connection box using an Ethernet cable rather than connecting with Wi-Fi. Refer to your **nbn**™ user guide for help with connecting to the **nbn**™ connection box.

2. Turn off the VPN and perform a speed test without being connected to the VPN. You can check your speed through your internet provider or by using a publicly available speed test service as a guide. **nbn** recommends **nbn**™ Sky Muster™ Plus customers use **plustest.com.au**, which makes results available to your provider for troubleshooting. Make note of your download and upload speed results from the test.

3. Turn on the VPN and perform another speed test whilst being connected to the VPN. Use the same speed test service used in Step 2. Make note of your download and upload speed results from this test.

4. Compare the download and upload speeds on both tests. If you notice a poor result without being connected to the VPN, contact your service provider for assistance.

> Some speed tests will also give you the 'ping' value. This indicates the latency on your connection as described above. The latency should be larger when you're connected to the VPN.

Now that you've checked your service, here are some tips to help you, and possibly your employer, to troubleshoot issues and further optimise your experience.

Tips for using a VPN:

- Only use a VPN when required. In general, not every work application requires a VPN. Check with your IT department for applications that don't require a VPN connection. Here are some examples of work applications that might not need a VPN connection:

    - Websites that begin with https:// (or show the padlock symbol) indicate secure browsing.

    - Email services such as Microsoft Outlook and Gmail use Secure Mail Transfer Protocol (SMTP).

    - Cloud based services are inherently secured. This includes Office 365 applications (OneNote, OneDrive, SharePoint etc.), Google Suite applications (Google Docs, Sheets, Drive etc.), Salesforce, Oracle, Slack, WhatsApp and more.

- Avoid using a VPN for video conferencing if you can. Video conferencing services such as MS Teams, Signal and Google Meet etc. should not require a VPN as they are typically secure. On a plan via the **nbn**™ Sky Muster™ Plus service, video conferencing is an unmetered application and won't count towards your data usage if you are not using a VPN, whereas all VPN traffic is metered.*

- Whilst using a VPN, connect directly to your **nbn**™ connection box with an Ethernet cable rather than using Wi-Fi. This can usually provide a stronger connection.

- Keep personal devices such as laptops, computers and phones up to date by performing software updates regularly. This can help applications run smoothly and protect your devices from malicious cyber-attacks.

Tips for employers/IT departments:

- Assess all applications used on the corporate network and determine which ones require VPN access and which ones don't. Compile and share a list of VPN applications with employees so they can turn off the VPN when it's not required and can avoid using it unnecessarily.

- Check the type of VPN being used. If your VPN is a 'split tunnel' VPN, it can be configured so that only the necessary applications tunnel through the VPN. Other applications will not tunnel through the VPN even whilst connected.

- Check the encryption type being used by the VPN – encrypted headers vs. encrypted payload. TLS/SSL based VPNs only encrypt the payload (secure) but do not encrypt the header, so satellite acceleration processes can help speed up the connection. IPSec based VPNs encrypt both the payload and the headers which prevents this acceleration.

Please note, **nbn**™ Sky Muster satellite service eligibility criteria may apply to some medium and large business premises. Speak to your preferred phone and internet provider for more information.

For more information on **nbn**™ Sky Muster™ satellite services, visit **nbn.com.au/SkyMuster** or contact your phone and internet provider