Virtual office

A virtual office provides companies with a physical presence without a physical office. Coro's virtual office includes an encrypted VPN, site-to-site tunnels, and firewall exceptions. Secure Web Gateway (SWG) with domain name system (DNS) filtering can optionally be added as well.

From the **Virtual Office** screen, admin users can select the virtual private network (VPN) policy for company devices. VPNs establish a secure and encrypted connection over the internet between devices and a remote server. This connection makes it difficult for hackers or third parties to intercept or access the data being transmitted.

By default, end users can't disconnect their devices from the VPN. Admin users can allow specific devices to be manually disconnected from the VPN.

Admin users can select the VPN encryption strength. For more information, see **Change the encryption strength**.

Different VPN policies can be set for each of your devices. The VPN policy options include:

1. **Default settings**: traffic from protected devices doesn't go through the VPN
2. **Inclusive VPN**: Devices with this policy use the VPN to access and encrypt your virtual office, as well as any external resources which have been added to the include list
3. **Exclusive VPN**: Devices with this policy use the VPN to access and encrypt all networking except for any external resources which have been added to the exclude list