Global Protect VPN

Washington State University offers VPN access for those departments and users that require secure remote user access to specific, restricted university services and data. The VPN service provides authenticated and encrypted access to resources such as the administration of departmental servers, administrative systems and applications, and/or systems that house sensitive information.

ITS VPN portals utilize OKTA Multifactor Authentication (MFA). This is the same MFA used by other WSU systems such as Workday, myWSU, and email.

VPN Portal	Username Used to Access	Typical People to Use Portal
vpn.wsu.edu	WSU NID*	All WSU Staff and Students
vpn.everett.wsu.edu	WSU NID*	Everett Staff and Students
sslvpn.spokane.wsu.edu	WSU NID*	Spokane Staff and Students
vpn.vancouver.wsu.edu	WSU NID*	Vancouver Staff and Students
vpn.tricity.wsu.edu	WSU NID*	Tricities Staff and Students

*Note: WSU NID is same logon as myWSU

Who should use the WSU GlobalProtect VPN service?

Students, staff, faculty, and sponsored affiliates should use the WSU GlobalProtect VPN Service for accessing WSU systems, including, but not limited to, connecting to on-campus computers via remote desktop (RDP).

When should the WSU GlobalProtect VPN service not be used?

The WSU GlobalProtect should not be used for personal activities such as YouTube, Netflix, Facebook, email, etc. which is not associated with a University academic or business activity.

What operating systems are currently supported?

WSU is currently running the 6.1.x version of the GlobalProtect client. Current support for operating systems can be found on the PaloAlto website at https://docs.paloaltonetworks.com/compatibility-matrix/globalprotect/where-can-i-install-the-globalprotect-app.

Related Information

WSU Electronic Device Security Tips for International Travel

Downloading Global Protect