Vzdálený přístup VPN

Vzdálené připojení přes virtuální privátní síť (VPN) umožňuje zaměstnancům Univerzity Karlovy **bezpečně se připojit k univerzitní síti i mimo pracoviště** - například z domova nebo při služební cestě.
Díky připojení přes VPN můžete využívat stejné služby, jako byste byli přímo v síti univerzity - například **pracovat se síťovými disky**, **tisknout** na vzdálených tiskárnách nebo se **vzdáleně připojit ke kancelářskému počítači**.

S čím potřebujete poradit?

Kdo může VPN používat?
VPN je určena **pouze pro zaměstnance Univerzity Karlovy**. Studenti tuto službu využívat nemohou.
Jak se připojit?
K připojení budete potřebovat svůj univerzitní účet CAS .
Stačí si nainstalovat **VPN klienta** (program pro připojení k VPN) **podle pokynů vaší fakulty nebo součásti**.

Způsob připojení, používaný VPN klient i nastavení se mohou lišit podle jednotlivých fakult a součástí a mohou se v čase měnit.
Aktuální návody a potřebné informace proto **vždy hledejte na webu své fakulty nebo u její IT podpory.**

Po úspěšném připojení máte přístup ke všem interním systémům stejně, jako kdybyste pracovali přímo z univerzitní sítě.
Jaký program VPN klienta si mám nainstalovat?
Používaný VPN klient závisí na tom, **ke které fakultě nebo součásti Univerzity Karlovy patříte** a **ke kterým interním systémům se potřebujete připojit**.

- Aktuálně nejčastěji používaným VPN klientem na Univerzitě Karlově je **Palo Alto GlobalProtect**, který v současnosti využívá např. **Rektorát UK, Jinonice, Katolická teologická fakulta** a řada fakult na toto řešení postupně přechází. **Návody** na instalaci a **Jak se připojit** najdete zde .
- Zároveň platí, že **některé fakulty mohou používat jiný VPN klient** (např. Cisco AnyConnect nebo jiné řešení) a používané technologie se mohou v čase měnit.

Pokud si nejste jistí, **který VPN klient je pro vás správný**, vždy se řiďte pokyny své fakulty nebo se obraťte na její IT podporu.
Často kladené dotazy (FAQ)
Jaké údaje potřebuji k přihlášení?

- K přihlášení použijte své přihlašovací údaje do **Centrální autentizační služby** (CAS).

Je vzdálené připojení VPN bezpečné?

- Ano, VPN připojení je bezpečné a chrání data uživatelů i organizace před kybernetickými hrozbami.

Kde najdu instalační soubory a návody?

- Každá fakulta nebo součást UK spravuje **vlastní VPN přístup**. Návody a odkazy naleznete na stránkách své fakulty v sekci IT služby nebo Helpdesk.

Proč nevidím všechny služby přes VPN?

- Rozsah dostupných služeb se může lišit podle nastavení vašeho pracoviště nebo fakulty.

Lze aplikaci nainstalovat také do počítače se starším operačním systémem?

- Počítače s operačními systémemy Windows2000, WindowsXP, Windows 7 **není možné využít pro vzdálený přístup**.
- Upozorňujeme, že používání těchto zastaralých operačních systémů (bez pravidelné aktualizace bezpečnostních chyb operačního systému) je rizikové.

Kam se obrátit, pokud se nemohu připojit k VPN?

- V případě potíží s připojením k VPN se obraťte na **IT podporu své fakulty nebo součásti** univerzity, která VPN provozuje.
  Používaný VPN klient, nastavení i přístupové údaje se mohou mezi fakultami lišit a centrální podpora nemá k těmto konfiguracím vždy aktuální informace.

Podpora, Helpdesk
Pokud se vám nedaří připojit nebo došlo k chybě při instalaci, obraťte se na IT podporu své fakulty nebo na centrální ServiceDesk UK.
Důležité odkazy

Níže uvádíme vybrané příklady návodů. Přehled není úplný – vždy se řiďte informacemi na webu své fakulty nebo součásti.

- Centrální autentizační služba (CAS)
- Návod pro připojení do VPN Palo Alto Global Protect