



Česká agentura pro standardizaci, státní příspěvková organizace, IČO: 06578705

se sídlem Biskupský dvůr 1148/5, Praha 1, PSČ 110 00

Přístup do Interního atestačního prostředí prostřednictvím VPN

Verze: 1.0

Datum vydání: 5. 11. 2024

Datum účinnosti: 5. 11. 2024

Počet stran: 5

Nahrazovaný dokument: není

1 Úvod

Dokument popisuje zřízení přístupu do Interního atestačního prostředí prostřednictvím VPN.

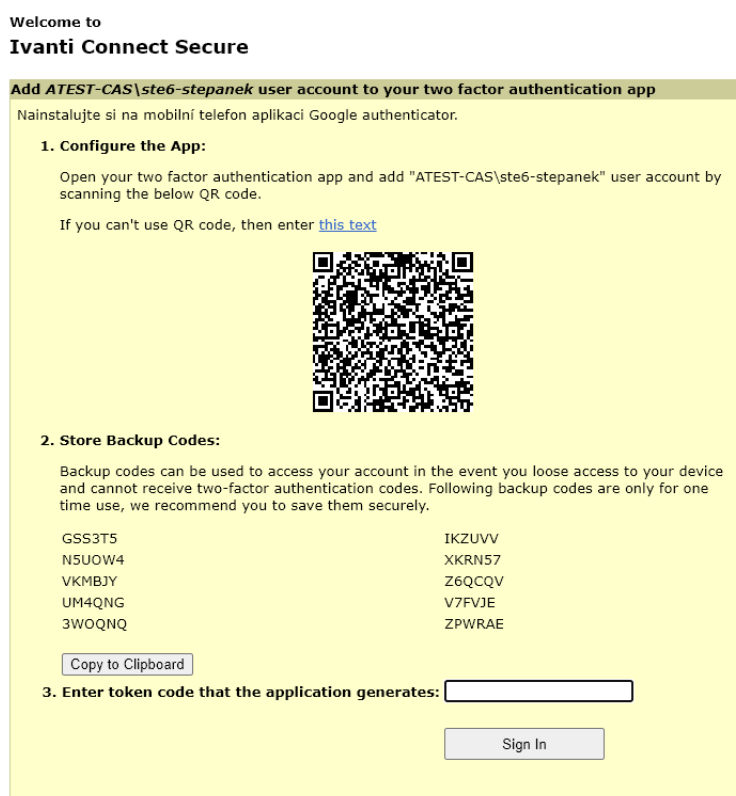
2 Zřízení přístupu do Interního atestačního prostředí prostřednictvím VPN

Vzdálený přístup do Interního atestačního prostředí je umožněn prostřednictvím VPN realizované aplikací *Ivanti Secure Access Client*.

Instalace *Ivanti Secure Access Client* spočívá jednak v instalaci vlastního software a jednak ve vytvoření druhého autentizačního faktoru prostřednictvím aplikace Google Authenticator.

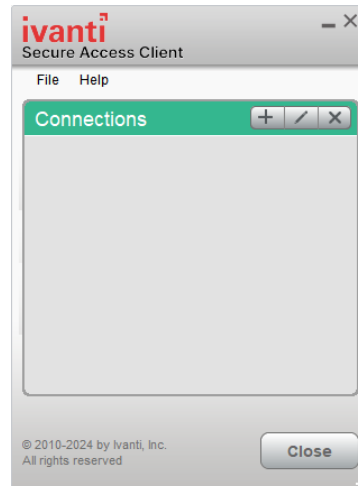
Postup:

1. Zjistěte své počáteční přihlašovací údaje pro VPN; tyto údaje naleznete v aplikaci Vaultwarden v kolekci „Technický zástupce Objednatele“.
2. Na stránce <https://vpn.agentura-cas.cz/eSSL> zadejte přihlašovací údaje.
Pozn.: uživatelské jméno je možno zadat včetně domény (tedy např. „*atest-cas\ste6-stepanek*“), ale i bez ní (tedy např. „*ste6-stepanek*“).
3. Protože zatím nemáte vytvořen druhý autentizační faktor, bude zobrazena výzva pro jeho vytvoření:



4. Na mobilním zařízení z „AppStore“ (pro iOS) nebo „Obchod play“ (pro Android) nainstalujte aplikaci Google Authenticator.
5. Na mobilním zařízení v aplikaci Google Authenticator přidejte další položku (ikona „+“) a naskenujte zobrazený QR kód.
6. Uchovejte vygenerované záložní kódy – použijete je v případě výměny telefonu, případně pro přístup k VPN bez telefonu s OTP. Alternativně můžete použít zálohování kódů prostřednictvím automatického zálohování Google účtu.

7. Na počítači do políčka „Enter token code that the application generates:“ zadejte číslo zobrazené Google Authenticatorem a potvrďte formulář klávesou ENTER.
8. Na počítači prostřednictvím aplikace Vaultwarden z kolekce „VPN Instalátor“ získáte instalační soubor VPN klienta pro váš operační systém (je uložen jako příloha jediné položky této kolekce).
9. Stažený instalační soubor spusťte a následujte pokyny pro instalaci VPN klienta pro váš operační systém. Proveďte a dokončete instalaci.
10. Po spuštění nainstalované aplikace VPN klienta se zobrazí následující okno:




11. Klikněte na ikonku „+“; program zobrazí následující požadavek na zadání údajů. Následující obrázek níže je uveden včetně příkladu vyplnění; v závislosti na operačním systému je možné, že část údajů již bude předvyplněna:

- Do pole „Name:“ zadejte vlastní pojmenování spojení. Doporučujeme, aby toto pojmenování obsahovalo APN aktuálního Atestačního prostředí. Důvod je ten, že pokud byste požádali o další atestaci, dostanete přístup do nového samostatného Atestačního prostředí s jiným APN. VPN se bude připojovat do jiné vnitřní virtuální sítě. Budete tedy mít definovány dvě VPN připojení a je nezbytné mít v pojmenování VPN pořádek.
- Do pole „Server URL:“ zadejte „<https://vpn.agentura-cas.cz/essl>“

12. Klikněte na tlačítko „Add“

Tím je zadávání údajů pro VPN dokončeno.

3 Připojení do VPN

Pro připojení do VPN v operačním systému MS Windows lze využít faktu, že software *Ivanti Secure Access Client* je dostupný též v „oznamovací oblasti (košíčku)“ na hlavním panelu, ikona . Po kliknutí na tuto ikonu se zobrazí seznam nastavených VPN připojení. Pro připojení budete potřebovat zařízení s druhým faktorem (*Google Authenticator*).

Klikněte na tlačítko „Connect“, zadejte přihlašovací údaje uvedené v aplikaci Vaultwarden - je třeba zadat stejné uživatelské jméno a heslo jako v kroku 2 tohoto postupu.

Při výzvě k zadání *Secondary Tokenu* opište číslo OTP z *Google Authenticatoru*.

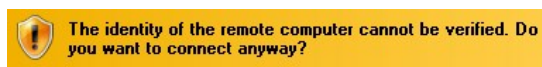
Pozn.: OTP kód je nutno zadávat po 6 hodinách připojení znovu (bezpečnostní nastavení).

4 Přístup na virtualizované stroje Interního atestačního prostředí

Přístup na servery nebo Stanici pro klientské operace v Interním atestačním prostředí je možný pouze poté, co bylo navázáno VPN spojení.

Přístup je umožněn prostřednictvím aplikace Remote Desktop (RDP). Všichni Zástupci na každém virtualizovaném stroji sdílí jeden účet s administrátorskými právy. IP adresy virtualizovaný strojů a přístupová jména a hesla jsou uvedena v aplikaci třídy Password Manager v kolekci „*Technický zástupce Objednatele*“, v samostatné položce pro každý virtualizovaný stroj.

Při pokusu o připojení prostřednictvím RDP budete informováni o tom, že RDP nemůže ověřit identitu cílového počítače:



Důvodem je použití self-signed certifikátů. Bezpečnost není kompromitována, neboť prostřednictvím VPN se připojujete do virtuální sítě vytvořené výhradně pro váš Atestační případ. Virtuální sítě různých Atestačních prostředí jsou izolovány.

5 Zvláštní případy

5.1 Nenásledování výše popsaného procesu

Pokud nenásledujete výše popsaný proces a zadáte VPN do nástroje *Ivanti Secure Access Client* přímo, bude zobrazeno:



V takovém případě postupujte podle kapitoly 2 a nejprve vytvořte druhý faktor. Poté teprve použijte *Ivanti Secure Access Client*.