**Připojení NB/PC k firemní síti pomocí Cisco ANY CONNECT klienta s ověřením MFA (MS AUTHENTICATOR)**

**Změna od ledna 2021**

S ohledem na potřebu zabezpečení přístupu k firemní síti je od **6.1.2021** zaveden přístup do firemní sítě z prostředí internetu pomocí VPN klienta (CISCO ANY CONNECT) pouze s dvou faktorovou autorizací (dále jen MFA) pomocí MS AUTHENTICATORU na mobilním zařízení. Jiná forma MFA není podporována a funkční.

S tím souvisí změna chování a změna používání CISCO ANY CONNECT klienta viz níže

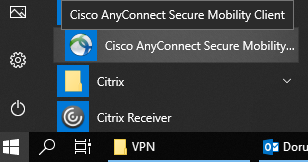
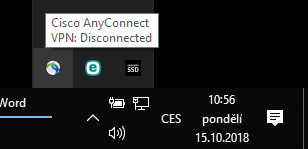
Od zmíněného data již nebude funkční původní připojení s profilem nevyžadujícím MFA (v Cisco ANY CONNECT klientovi je profil s názvem AC-INT-VPN) a je nahrazen novým profilem **AC VPN + MFA.** Tento profil je možné získat zde: [\\scfs\Install\AC CISCO ANY CONNECT](file:///\\scfs\Install\AC%20CISCO%20ANY%20CONNECT), kde je připraven jak samotný profil, tak i upravená instalace, která provede samotné nakopírování profilu do správné složky na vašem počítači.

**Certifikáty potřebné k provozu VPN klienta na PC/NB**

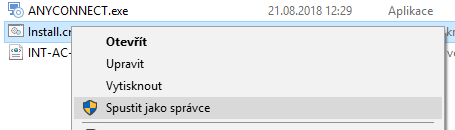
* Certifikát ověření klienta - **Portal Access** nebo **AutoCont WiFi**. Tento certifikát je možno získat dle [postupu na AC portále](https://portal.autocont.cz/css/Stranky/Postupy-a-navody.aspx?RootFolder=%2Fcss%2FIS%2FPostupy%20a%20N%C3%A1vody%2FCertifikaty%20a%20bezpe%C4%8Dnost&FolderCTID=0x0120002AF30C13ACFC47499AC92DDC70534D23&View=%7bB41102AE-E661-4879-9D0A-F2682F07628C%7d) (dokument Žádost o certifikát 2020.docx)
* Kořenový certifikát Autocont CA2, Certifikát nové Certifikační Autority (Root certifikát). Tento certifikát je na Vaše zařízení instalován pomocí GPO. Pokud se tak nestalo, je možné nainstalovat certifikát na stránce <https://crl.autocont.cz>

**Instalace klienta Cisco AnyConnect**

V případě, že jste obdrželi NB připravený oddělením interního IT máte pravděpodobně již instalovánu. Ověřit její přítomnost můžete v nabídce start, případně v oznamovací oblasti systému Windows.

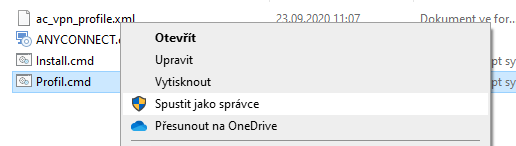
Pokud aplikaci nemáte instalovánu, můžete si jí instalovat z centrálního uložiště instalací : [\\scfs\Install\AC CISCO ANY CONNECT](file://scfs/Install/AC%20CISCO%20ANY%20CONNECT) nebo z prostředí mimo ac síť LAN/WAN : <http://www.autocont.cz/iit>. Instalační zdroj je nutné kompletně nakopírovat na lokální disk a instalaci spustíte kliknutím pravým tlačítkem myši a vybráním v kontextovém menu položka **Spustit jako správce** na souboru **Install.cmd** v případě stažení aplikace z [www.autocont.cz/iit](http://www.autocont.cz/iit) je nutné ji nejprve rozbalit na disk počítače.



Následně se spustí instalace CiscoAnyConnect clienta, u které je třeba projít průvodce instalací. Není nutné nic měnit, stačí pouze odklikat. Instalace je dokončena kopírováním profilu do příslušných složek systému. Ihned po instalaci je možné použít klienta z nabídky start, po restartu OS se objeví v oznamovací oblasti systému Windows.

**Kopírování profilu**

Pokud máte klienta nainstalovaného a požadujete pouze nakopírování nového profilu, tak zvolte z instalačního zdroje dávku **Profil.cmd** a spusťte jí jako správce. Dojde k nakopírování do správných složek systému Windows a při následném spuštění klienta již bude v seznamu pro výběr

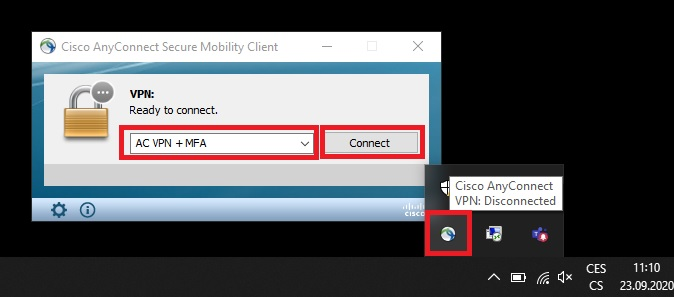


**Používání klienta**

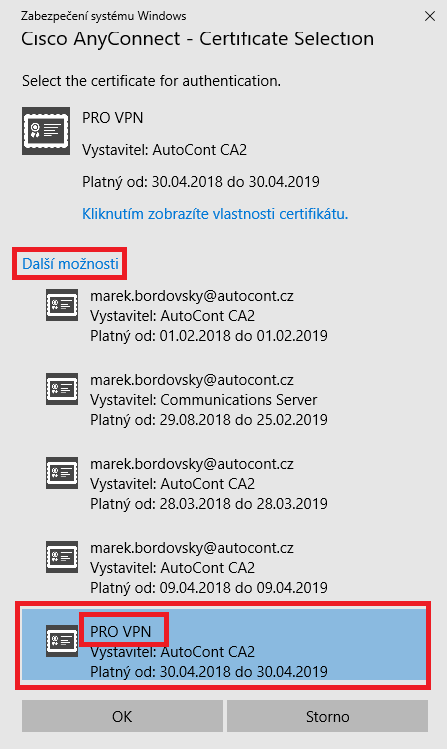
**Připojení do AC VPN,** provedete tak, že kliknete na ikonu v oznamovací oblasti a zvolíte profil **AC VPN + MFA** a kliknete na tlačítko **Connect**. Následně budete vyzvání k výběru certifikátu pro ověření identity **Portal Access**, nebo **AutoCont WiFi**. (zde doporučujeme upravit popisný název certifikátu, tak aby byla jednodušší orientace v seznamu certifikátů). Certifikát bude pravděpodobně nutné vybrat pomocí tlačítka **Další možnosti** a výběrem certifikátu. Po úspěšné autentizaci certifikátem budete vyzvání k zadání jména a hesla a následně schválení přístupu na mobilním zařízení v aplikaci **MS AUTHENTICATOR**. (Návod, jak nastavit [ZDE](https://portal.autocont.cz/css/Stranky/Postupy-a-navody.aspx?RootFolder=%2Fcss%2FIS%2FPostupy%20a%20N%C3%A1vody%2FO365&FolderCTID=0x0120002AF30C13ACFC47499AC92DDC70534D23&View=%7bB41102AE-E661-4879-9D0A-F2682F07628C%7d))

O úspěšném připojení do VPN budete informováni notifikací.

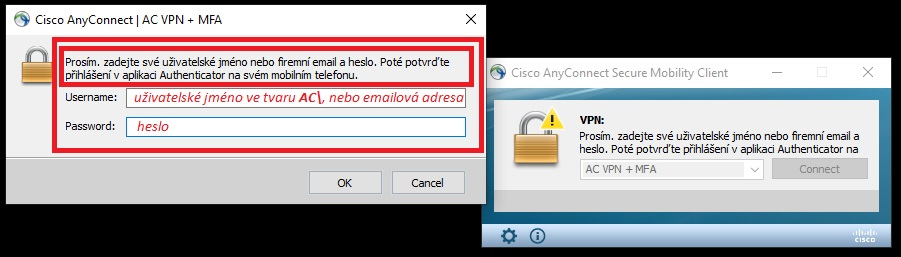
Pozn. Při prvním přihlášení pomocí Cisco ANY CONNECT klienta není uživatel o nutnosti potvrzení MFA nijak upozorněn a je třeba si tento krok uvědomit. Při dalším přihlášení je již v okně pro zadání hesla poznámka o nutnosti potvrdit MFA autentizaci. Je nastaven časový limit, po kterém proces přihlášení vyprší a je třeba celý proces přihlášení opakovat (60s)



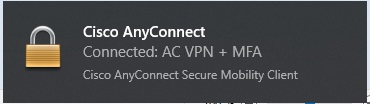
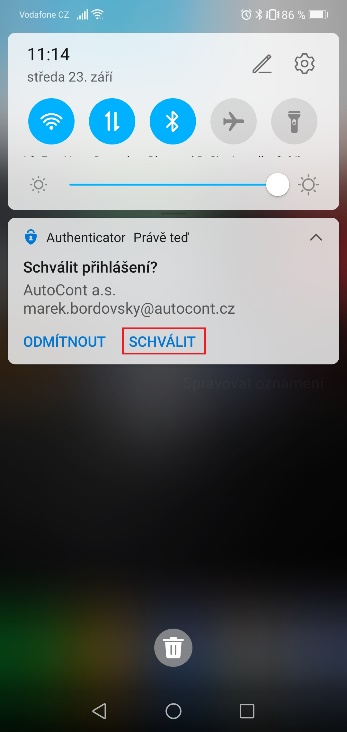
Spuštění klienta Cisco ANY CONNECT



Výběr certifikátu pro ověření

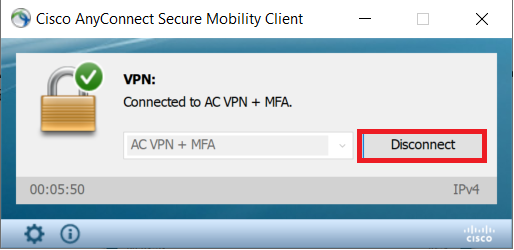


Přihlášení pomocí uživatelského jména a hesla - jméno lze zadat ve formátu AC\uzivatelske jmeno nebo ve formátu emailové adresy



Schválení na mobilním zařízení a potvrzení připojení k VPN

**Odpojení z AC VPN,** provedete po kliknutí na ikonu Cisco AnyConnect v oznamovací oblasti Windows a kliknutím na tlačítko Disconnect.



**Možné problémy s používáním Cisco AnyConnect**

* **Uspaný NB z práce**. Nejčastějším problémem je pouze uspaný a probuzený NB z práce. V takovém případě dochází k použití předem načtených informací jmen serverů z LAN AC místo prostředí internetu. Dochází tak často k problémům jak se samotným připojením, ale také následným spojením s prostředky v síti LAN/WAN AC připojených pomocí VPN. Doporučujeme před samotným používáním VPN provést restart Systému.
* **Prošlý, nebo neplatný certifikát**. V takovém případě je nutné si požádat o nový a to v rámci sítě AC
* **Neplatné heslo**. Kontaktujte správu sítě