Kerio VPN Client

Příručka uživatele

Kerio Technologies

Tento manuál popisuje program *Kerio VPN Client* ve verzi *7.3* pro *Windows*. Změny vyhrazeny.

Obsah

Kapitola 1

Úvod

Kerio VPN Client je aplikace pro přístup z jednoho počítače (klienta) do vzdálené privátní sítě přes Internet zabezpečeným šifrovaným kanálem. Klient získá přístup do této privátní sítě, jako by byl k ní přímo připojen.

Kerio VPN Client se připojuje k VPN serveru v produktu *Kerio Control*. Pro ověření identity klienta se používají uživatelské účty v *Kerio Control*.

Použití aplikace *Kerio VPN Client* je velmi snadné. Uživatel potřebuje znát pouze jméno nebo IP adresu serveru, ke kterému se připojuje, a uživatelské jméno a heslo. Vše ostatní (nastavení směrovacích informací, DNS atd.) provede *Kerio VPN Client* automaticky.

Kerio VPN Client podporuje uživatelské profily. Každý uživatel počítače, na kterém je *Kerio VPN Client* nainstalován, může definovat a používat vlastní VPN připojení.

Uživatelé s administrátorskými právy mohou rovněž navázat tzv. perzistentní (trvalé) spojení. Takové spojení je automaticky obnovováno i po restartu počítače.

1.1 Systémové požadavky

Hardwarové požadavky a podporované operační systémy

Aktuální systémové požadavky naleznete na stránce:

http://www.kerio.cz/cz/control/technical-specifications

Konfliktní software

Kerio VPN Client nelze provozovat na počítači, na kterém je nainstalován *Kerio Control*. Při pokusu o spuštění *Kerio VPN Client* zároveň s *Kerio Control* je hlášena kolize a *Kerio VPN Client* se nespustí.

1.2 Instalace

Instalaci provedeme spuštěním instalačního archivu pro příslušnou platformu (např. `kerio-control-vpnclient-1.2.3-4567-win32.exe`). Při instalaci lze zvolit cílovou složku.

Výchozí složkou je `C:\Program Files\Kerio` (je-li na počítači již nainstalován některý produkt firmy *Kerio Technologies*, pak je automaticky detekována a nabídnuta složka, ve které je tento produkt nainstalován).

Při instalaci je v systému *Windows* vytvořen virtuální síťový adaptér *Kerio Virtual Network Adapter* a speciální síťové rozhraní *Kerio Virtual Network*. Dále je nainstalována systémová služba *Kerio VPN Client Service*, která je ihned spuštěna (a automaticky spouštěna při každém startu systému).

Za normálních okolností není třeba po instalaci počítač restartovat (restart může být vyžadován, pokud instalační program přepisuje sdílené soubory, které jsou právě používány).

1.3 Licence

Kerio VPN Client je poskytován jako doplněk aplikace *Kerio Control*. Samotný program *Kerio VPN Client* nevyžaduje speciální licenci.

Připojení VPN klienti se však započítávají do celkového počtu uživatelů (chráněných počítačů) při kontrole licence v aplikaci *Kerio Control*. Z toho vyplývá, že minimální počet uživatelů, pro který musí být *Kerio Control* na příslušném serveru licencován, je dán součtem počtu počítačů v lokální síti a počtu VPN klientů současně se připojujících k tomuto serveru.

Poznámka: Podrobné informace o licencích produktu *Kerio Control* naleznete v manuálu *Kerio Control — Příručka administrátora*.

1.4 Jak Kerio VPN Client funguje?

Kerio VPN Client zajišťuje přístup z počítače klienta do vzdálené privátní sítě zabezpečeným šifrovaným komunikačním kanálem (tento kanál je v operačním systému reprezentován virtuálním síťovým rozhraním *Kerio Virtual Network*). Tomuto rozhraní VPN server v *Kerio Control* automaticky přidělí IP adresu, která logicky patří do příslušné privátní sítě.

Operační systém klienta musí znát cesty do jednotlivých subsítí vzdálené sítě. Za tímto účelem *Kerio VPN Client* automaticky aktualizuje systémovou směrovací tabulku klienta (přidává cesty do vzdálených subsítí).

Při aktualizaci směrovací tabulky se předávají cesty do všech vzdálených subsítí (případně cesty do dalších sítí nastavené v konfiguraci VPN serveru), pokud se jejich IP adresy nepřekrývají s IP adresami lokální sítě, ke které je počítač klienta připojen. *Kerio VPN Client* nikdy nemění výchozí cestu (tj. nastavení výchozí brány). Zabezpečený komunikační kanál slouží pouze pro přístup do vzdálené privátní sítě. Pro přístup do Internetu používá klient své stávající internetové připojení.

VPN server rovněž klientovi přiděluje adresu primárního, případně i sekundárního DNS serveru, příponu domény DNS a adresu primárního, případně i sekundárního WINS serveru. Tyto služby umožňují zadávat počítače ve vzdálené síti jejich jmény a procházet okolní počítače v síti *Microsoft Windows*.

Poznámka: Kerio VPN Client neumožňuje navázat více než jedno VPN připojení současně. Je však možné se střídavě připojovat k libovolnému počtu serverů.

Kapitola 2

Použití aplikace Kerio VPN Client

Kerio VPN Client může být používán ve dvou režimech:

Uživatelský režim

V tomto režimu navazuje a ukončuje VPN připojení sám uživatel, který právě s počítačem pracuje. V okně aplikace *Kerio VPN Client* zadá přihlašovací údaje nebo vybere některé z uložených připojení a připojí se. Připojení ukončuje opět sám uživatel, nebo je ukončeno automaticky při ukončení aplikace *Kerio VPN Client*, odhlášení uživatele nebo vypnutí/restartu počítače.

K navázání VPN připojení v tomto režimu nejsou vyžadována speciální uživatelská práva na klientském počítači — aplikaci *Kerio VPN Client* může využít kterýkoliv uživatel daného počítače.

Režim trvalého připojení

V tomto režimu uživatel naváže VPN připojení, které je pak trvale udržováno v připojeném stavu. Systémová služba *Kerio VPN Client Service* zajišťuje, že připojení zůstane navázané i po ukončení aplikace *Kerio VPN Client* a/nebo odhlášení uživatele a bude automaticky obnoveno po výpadku a/nebo restartu počítače. Po startu počítače je VPN připojení navázáno (obnoveno) ještě před přihlášením uživatele. Díky tomu je možné např. přihlášení uživatele do domény ve vzdálené privátní síti.

Pro navázání a ukončení trvalého VPN připojení musí mít uživatel na klientském počítači administrátorská práva (uživatelský účet typu *správce počítače*). Uživatelé bez administrátorských práv mohou využít pouze přístup do vzdálené privátní sítě, pokud je VPN připojení navázáno.

2.1 Spuštění aplikace

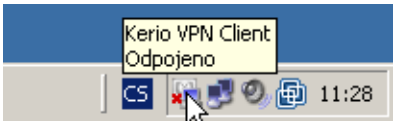
Aplikace *Kerio VPN Client* se spouští automaticky po přihlášení uživatele a zobrazuje se jako ikona v oznamovací oblasti nástrojové lišty (viz kapitola 2.2).

Pokud není ikona zobrazena (typicky v případě ručního ukončení aplikace), pak lze aplikaci znovu spustit ze systémové nabídky *Start* volbou *Start* → *Programy* → *Kerio* → *VPN Client* → *Kerio VPN Client*. Při spuštění z nabídky *Start* se také ihned zobrazí hlavní okno aplikace, které slouží pro definici VPN připojení (viz kapitola 2.3).

2.2 Ikona na nástrojové liště

Je-li *Kerio VPN Client* spuštěn, pak je v oznamovací oblasti nástrojové lišty zobrazena ikona informující o jeho stavu. Při umístění kurzoru myši na ikonu se zobrazí podrobnější informace formou nápovědného textu.

- Neaktivní stav (VPN připojení není navázáno) je znázorněn červeným křížkem a šedým logem *Kerio Control*.



Obrázek 2.1 Ikona aplikace Kerio VPN Client v odpojeném stavu

- Aktivní VPN připojení je znázorněno plně barevnou ikonou.

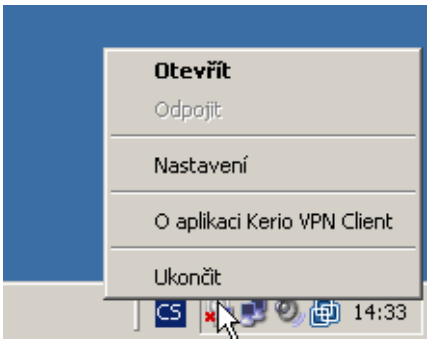
Obrázek 2.2 Ikona aplikace Kerio VPN Client v připojeném stavu

- Trvalé připojení je odlišeno pouze nápovědným textem.

Obrázek 2.3 Ikona aplikace Kerio VPN Client v připojeném stavu

Funkce přístupné přes ikonu na nástrojové liště

Po kliknutí na ikonu pravým tlačítkem myši se zobrazí kontextové menu s těmito funkcemi:



Obrázek 2.4 Kontextové menu ikony na nástrojové liště

- *Otevřít* — zobrazení hlavního okna programu *Kerio VPN Client*.
- *Odpojit* — možnost ukončení navázaného VPN připojení.
- *Nastavení* — konfigurace některých parametrů programu *Kerio VPN Client* (viz kapitola 2.4).
- *O aplikaci* — informace o verzi jednotlivých komponent aplikace *Kerio VPN Client* (programu, systémové služby a nízkoúrovňového ovladače).
- *Ukončit* — ukončení programu *Kerio VPN Client*. Tato volba rovněž odpojí aktivní VPN připojení, pokud je navázané jako dočasné (viz kapitola 2.3).

  Volba *Ukončit* nezastavuje systémovou službu *Kerio VPN Client Service* ani neodpojuje trvalé VPN připojení.

2.3 Hlavní okno — definice VPN připojení

Hlavní okno aplikace *Kerio VPN Client* slouží k zadání údajů o VPN připojení. Toto okno lze zobrazit dvojitým kliknutím na ikonu aplikace na nástrojové liště, volbou *Otevřít* z kontextového menu ikony na nástrojové liště (viz kapitola 2.2), případně ze systémové nabídky *Start* volbou *Start* → *Programy* → *Kerio* → *VPN Client* → *Kerio VPN Client*.

Obrázek 2.5 Hlavní okno aplikace Kerio VPN Client

Do položky *Server* je potřeba uvést jméno nebo veřejnou IP adresu počítače, na kterém je nainstalován *Kerio Control* a který funguje jako internetová brána v příslušné síti. Dále je nutné zadat uživatelské jméno a heslo pro ověření uživatele. V závislosti na konfiguraci firewallu je v některých případech nutné uvést uživatelské jméno včetně domény (např. `jnovak@firma.local`). Pokud si nejste jisti, kontaktujte správce příslušného firewallu.

Připojení může být navázáno jako dočasné nebo jako trvalé (viz kapitola 2). Pro navázání nebo ukončení trvalého připojení musí mít uživatel na klientském počítači administrátorská práva (*správce počítače*). V systémech *Windows Vista* a *Windows Server 2008* může být aktivní funkce *řízení uživatelských účtů* (*UAC — User Account Control*). V takovém případě je potřeba akci připojení nebo odpojení ještě potvrdit, případně zadat jméno a heslo uživatele s administrátorskými právy.

Kerio VPN Client si zapamatovává zadané VPN servery, odpovídající uživatelská jména a volbu trvalého připojení. Uživatel může zvolit, zda má být uloženo také zadané heslo.

Pro definici jiného VPN připojení jednoduše přepíšeme aktuální jméno serveru a přihlašovací údaje. Při dalším připojení již stačí vybrat požadovaný VPN server (a případně zadat heslo, pokud nebylo uloženo).

Upozornění:
Neukládejte heslo k VPN připojení, pokud mohou stejný uživatelský účet na klientském počítači používat další osoby. Mohlo by dojít ke zneužití přístupu do vzdálené privátní sítě.

Stavové informace a chybová hlášení

V horní části hlavního okna se zobrazuje aktuální stavová informace (připojeno/odpojeno, připojuje se/odpojuje se...) nebo chybové hlášení (připojení se nezdařilo, chyba ověření uživatele...).

Stavové informace a chybová hlášení se také zobrazují formou bublinových zpráv u ikony aplikace *Kerio VPN Client* na nástrojové liště, pokud jsou tyto zprávy povoleny (viz kapitola 2.4).

2.4 Nastavení programu

Volba *Nastavení* v kontextovém menu otevírá menu pro výběr jazyka uživatelského rozhraní programu *Kerio VPN Client* a nastavení bublinových zpráv.

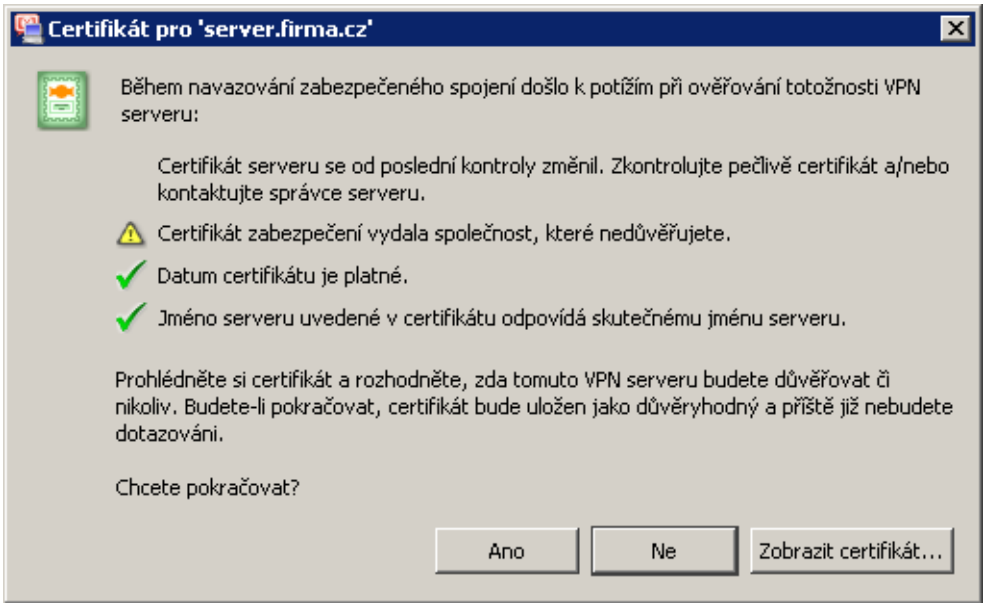
V menu se zobrazují všechny lokalizace (jazyky), které jsou momentálně k dispozici. Současná verze aplikace *Kerio VPN Client* je lokalizována do 16 jazyků.

Po výběru některého jazyka se uživatelské rozhraní programu ihned přepne do tohoto jazyka. Výchozí volba *Automaticky* nastavuje jazyk podle národního prostředí operačního systému (*Ovládací panely / Místní a jazyková nastavení*).

Volba *Povolit bublinové zprávy* zapíná/vypíná zobrazování informativních zpráv u ikony aplikace *Kerio VPN Client* v oznamovací oblasti nástrojové lišty. Nastavení těchto zpráv závisí pouze na osobních preferencích uživatele (informace o stavu připojení lze získat kdykoliv v hlavním okně aplikace).

2.5 Kontrola SSL certifikátu VPN serveru

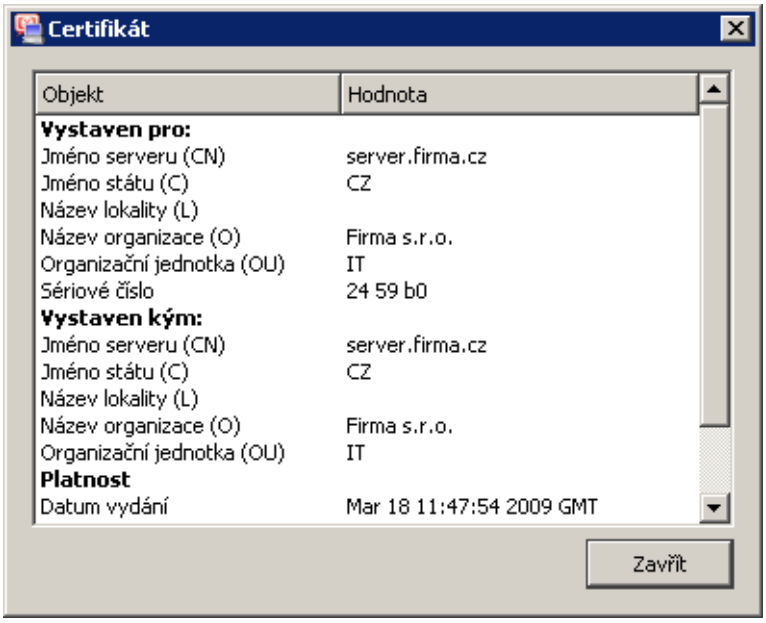
Kerio VPN Client provádí při každém připojování kontrolu SSL certifikátu příslušného VPN serveru (stejně jako WWW prohlížeč při použití protokolu *HTTPS*). Při zjištění problémů s certifikátem je zobrazeno varovné hlášení s dotazem, zda uživatel považuje příslušný VPN server za důvěryhodný a povolí připojení na tento server.



Obrázek 2.6 Informace o problémech s certifikátem VPN serveru

Tlačítkem *Zobrazit certifikát* lze získat podrobné informace o certifikátu VPN serveru (kým byl vydán, pro jaký server byl vystaven, datum skončení jeho platnosti atd.). Na základě těchto informací se uživatel může rozhodnout, zda bude příslušný server považovat za důvěryhodný, a připojení povolit nebo zamítnout.

Po stisknutí tlačítka *Ano Kerio VPN Client* předpokládá, že uživatel považuje daný VPN server za důvěryhodný. Certifikát uloží a při příštím připojení k tomuto serveru již nezobrazí žádné varování.



Obrázek 2.7 Zobrazení certifikátu VPN serveru

Nejčastější problémy s certifikáty a jejich řešení

Problémy s certifikáty mají zpravidla některé z následujících příčin:

Certifikát byl vystaven nedůvěryhodnou společností

Kerio VPN Client kontroluje, zda byl certifikát vystaven organizací, která je uvedena v seznamu důvěryhodných vydavatelů v operačním systému (*Ovládací panely / Možnosti Internetu*, záložka *Obsah*, sekce *Certifikáty*). Po importu certifikátu určité společnosti do seznamu důvěryhodných vydavatelů budou automaticky akceptovány všechny certifikáty vydané touto společností (nebudou-li zjištěny jiné problémy).

Jméno serveru neodpovídá

Jméno serveru uvedené v certifikátu se liší od jména serveru, na který se *Kerio VPN Client* připojuje. Tato situace může nastat, pokud server používá nesprávný certifikát nebo pokud se jméno serveru změnilo, může však také signalizovat pokus o útok (klientovi je podvržen falešný DNS záznam s jinou IP adresou).

Poznámka: Certifikát může být vystaven pouze na DNS jméno serveru, nikoliv na IP adresu.

Datum certifikátu není platné

SSL certifikáty mají z bezpečnostních důvodů časově omezenou platnost. Je-li hlášeno neplatné datum, znamená to, že platnost certifikátu příslušného serveru již vypršela a je potřeba jej obnovit. Kontaktujte správce příslušného VPN serveru.

Certifikát se od poslední kontroly změnil

Pokud uživatel akceptuje připojení k určitému VPN serveru, *Kerio VPN Client* uloží certifikát tohoto serveru jako důvěryhodný. Při každém dalším připojení pak kontroluje, zda se certifikát serveru shoduje s uloženým certifikátem. Neshoda certifikátů může

být způsobena výměnou certifikátu na serveru (např. z důvodu vypršení platnosti původního certifikátu), může však také signalizovat pokus o útok (jiný server s falešným certifikátem).

Upozornění:
V případě nejasností či pochyb o identitě VPN serveru neprodleně kontaktujte správce příslušného firewallu.

2.6 Záznamy

Kerio VPN Client vytváří záznamy o své činnosti a zjištěných chybách. Systémová služba a uživatelské rozhraní aplikace pracují nezávisle, a proto každá z těchto komponent vytváří své vlastní záznamy. Soubory záznamů lze využít při řešení případných problémů ve spolupráci s technickou podporou společnosti *Kerio Technologies* (důležité jsou zejména záznamy systémové služby).

Záznamy systémové služby

Záznamy systémové služby *Kerio VPN Client Service* jsou uloženy v podsložce `logs` složky, ve které je aplikace *Kerio VPN Client* nainstalována, typicky:

```
C:\Program Files\Kerio\VPN Client\logs
```

K dispozici jsou dva soubory záznamů:

- `error.log` — závažné chyby, např.: službu *Kerio VPN Client Service* nelze spustit, VPN server není dostupný, nezdařilo se ověření uživatele apod.
- `debug.log` — podrobné informace o činnosti systémové služby a zjištěných chybách.

Záznamy uživatelského rozhraní

Záznamy uživatelského rozhraní jsou uloženy v příslušné složce uživatelského profilu uživatele, který s aplikací *Kerio VPN Client* pracuje, typicky:

```
Data aplikací\Kerio\VPNClient\logs
```

resp.

```
Application Data\Kerio\VPNClient\logs
```

Stejně jako v případě systémové služby jsou k dispozici dva soubory záznamů:

- `error.log` — závažné chyby, např.: nelze navázat komunikaci se službou *Kerio VPN Client Service*.
- `debug.log` — podrobné informace o činnosti aplikace a zjištěných chybách.

Příloha A

Právní doložka

Microsoft®, *Windows*® a *Windows Vista*™ jsou registrované ochranné známky nebo ochranné známky společnosti *Microsoft Corporation*.

Ostatní uvedené názvy skutečných společností a produktů mohou být registrovanými ochrannými známkami nebo ochrannými známkami jejich vlastníků.