Kerio VPNClient

Příručka uživatele

Kerio Technologies

Tento manuál popisuje program *Kerio VPN Client* ve verzi *6.5.0*. Změny vyhrazeny.

Tento produkt obsahuje software vyvinutý sdružením *OpenSSL Project* pro použití v *OpenSSL Toolkit* (http://www.openssl.org/). *OpenSSL Toolkit* je implementace protokolů *Secure Sockets Layer* (SSL v2/v3) a *Transport Layer Security* (TLS v1) volně šiřitelná ve formě zdrojových kódů (open-source).

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 do ní přímo připojen.

Kerio VPN Client se připojuje k VPN serveru v produktu *Kerio WinRoute Firewall* (dále jen *WinRoute*). Pro ověření identity klienta se používají uživatelské účty ve *WinRoute*.

Kerio VPN Client podporuje tzv. perzistentní (trvalá) spojení — spojení je automaticky obnovováno po výpadku i po odhlášení a dalším přihlášení uživatele.

Použití aplikace *Kerio VPN Client* je velmi snadné (lze jej přirovnat např. k připojení do Internetu pomocí *Telefonického připojení* ve Windows). Uživatel potřebuje znát pouze DNS jméno nebo IP adresu serveru, ke kterému se připojuje, a uživatelské jméno a heslo. Vše ostatní (nastavení směrovacích informací 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.

1.1 Instalace

Hardwarové požadavky

Kerio VPN Client nemá žádné zvláštní hardwarové nároky. Konfigurace počítače by měla vyhovovat požadavkům pro příslušný operační systém.

Podporované operační systémy

Kerio VPN Client je distribuován ve dvou edicích: pro 32-bitové platformy a pro 64-bitové platformy.

32-bitovou edici (instalační balík označený „*win32*“) lze nainstalovat na tyto operační systémy:

- Windows 2000
- Windows XP (32 bit)
- Windows Server 2003 (32 bit)
- Windows Vista (32 bit)
- Windows Server 2008 (32 bit)

64-bitovou edici (instalační balík označený „*win64*“) lze nainstalovat na tyto operační systémy:

- Windows XP (64 bit)
- Windows Server 2003 (64 bit)
- Windows Vista (64 bit)
- Windows Server 2008 (64 bit)

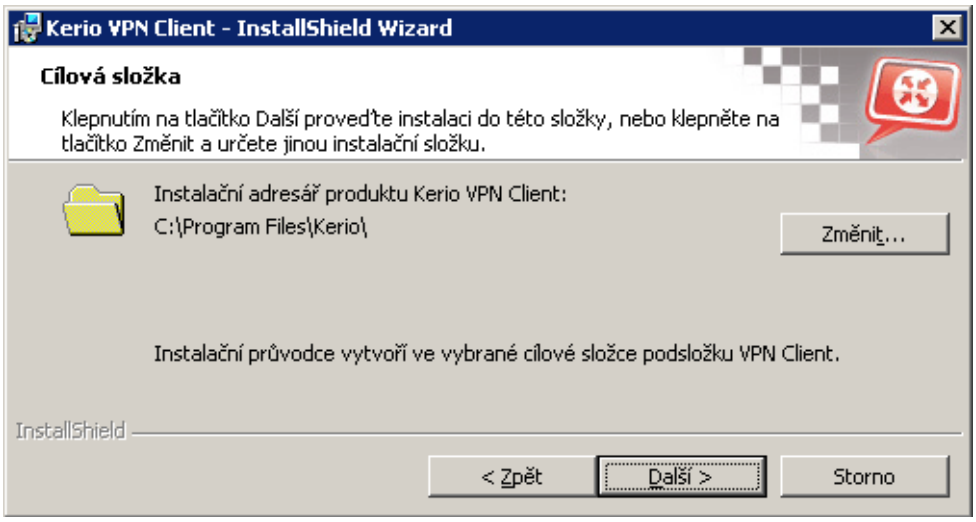
Starší verze operačních systémů Windows nejsou podporovány.

Konfliktní software

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

Postup instalace

Instalaci provedeme spuštěním instalačního archivu pro příslušnou platformu (např. `kerio-kvc-6.5.0-4794-win32.exe`). Při instalaci lze zvolit cílový adresář.



Obrázek 1.1 Instalace — výběr cílového adresáře

Výchozím adresářem je `C:\Program Files\Kerio` (je-li na počítači již nainstalován některý produkt firmy *Kerio Technologies*, pak je automaticky detekován a nabízen adresář, ve kterém je tento produkt nainstalován).

Při instalaci bude zaveden nízkoúrovňový ovladač *Kerio VPN* (`kvpndrv.sys`) a vytvořeno speciální síťové rozhraní *Kerio VPN*.

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

Umístění souborů

Spustitelné soubory aplikace se nainstalují do adresáře zvoleného při instalaci. Sdílené soubory a nízkoúrovňový ovladač se instalují do příslušných systémových adresářů (typicky `C:\WINNT\system32` a `C:\WINNT\system32\drivers`, resp. `C:\WINDOWS\system32` a `C:\WINDOWS\system32\drivers`).

Datový soubor (tj. soubor obsahující údaje o definovaných připojeních a další konfigurační informace) se ukládá do uživatelského profilu uživatele, pod kterým je *Kerio VPN Client* spuštěn, do podadresáře `Data aplikací\Kerio\VPNClient` (v české verzi systému Windows), resp. `Application Data\Kerio\VPNClient` (v anglické verzi systému Windows).

1.2 Licence

Kerio VPN Client je dodáván jako doplněk aplikace *Kerio WinRoute Firewall*. 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 WinRoute Firewall*. Z toho vyplývá, že minimální počet uživatelů, pro který musí být *Kerio WinRoute Firewall* 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 WinRoute Firewall* naleznete v manuálu *Kerio WinRoute Firewall — Příručka administrátora*.

1.3 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 VPN Adapter*).

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

- při každé změně síťové konfigurace na straně serveru,
- periodicky v intervalu 1 minuta (od poslední změny konfigurace).

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, do 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.

Kapitola 2

Použití aplikace Kerio VPN Client

Kerio VPN Client spustíme z programové nabídky *Start* → *Programy* → *Kerio* → *VPN Client*. *Kerio VPN Client* může být používán ve dvou režimech:

Základní režim
: Tento režim je vhodné použít, pokud se programem *Kerio VPN Client* připojujeme pouze k jednomu VPN serveru (tzn. pokud vzdáleně přistupujeme pouze do jedné privátní sítě) a nezajímají nás podrobné informace o průběhu spojení.

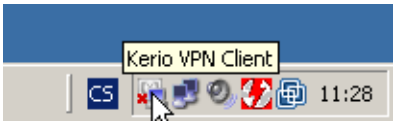
Rozšířený režim
: V rozšířeném režimu je možné uložit přihlašovací údaje pro více serverů a na tyto servery se připojovat (*Kerio VPN Client* může být připojen k více VPN serverům současně). Tento režim je vhodný, pokud potřebujeme vzdáleně přistupovat do více různých privátních sítí.
V rozšířeném režimu je také k dispozici detailní záznam činnosti programu *Kerio VPN Client*.

Po prvním spuštění po instalaci je *Kerio VPN Client* nastaven do základního režimu. Při dalším spuštění bude *Kerio VPN Client* vždy nastaven do naposledy použitého režimu.

2.1 Ikona na nástrojové liště

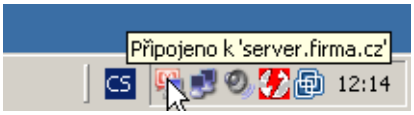
Je-li *Kerio VPN Client* spuštěn, pak je v oznamovací oblasti nástrojové lišty zobrazena ikona informující o jeho stavu.

- Stav, kdy není aktivní žádné VPN připojení, je znázorněn červeným křížkem.



Obrázek 2.1 Ikona aplikace Kerio VPN Client v odpojeném stavu

- Je-li aktivní alespoň jedno VPN připojení, je tento stav znázorněn zelenou šipkou.

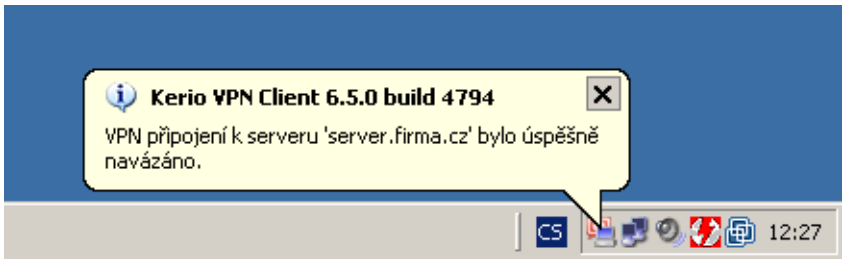


Obrázek 2.2 Ikona aplikace Kerio VPN Client v připojeném stavu

Je-li aktivní jedno připojení, zobrazí se v nápovědném textu (po umístění kurzoru myši na ikonu) jméno příslušného serveru. Jsou-li aktivní dvě a více připojení (v rozšířeném režimu — viz kapitola 2.3), zobrazuje se pouze jejich počet.

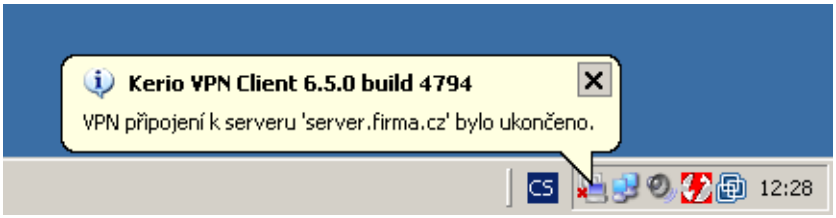
Informace o připojení a ukončení spojení

Bezprostředně po úspěšném připojení se u ikony na nástrojové liště na určitou dobu zobrazí informace, ke kterému serveru bylo připojení navázáno.



Obrázek 2.3 Bublinová zpráva s informací o navázání připojení

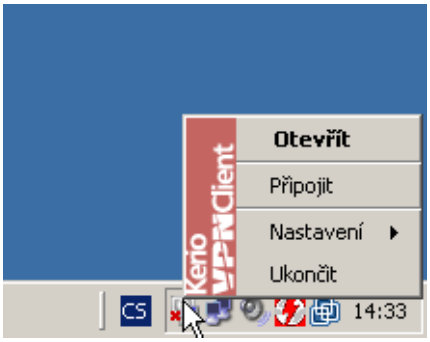
Bezprostředně po odpojení se zobrazí informace, že spojení s příslušným serverem bylo ukončeno.



Obrázek 2.4 Bublinová zpráva s informací o ukončení připojení

Funkce přístupné přes ikonu na nástrojové liště

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

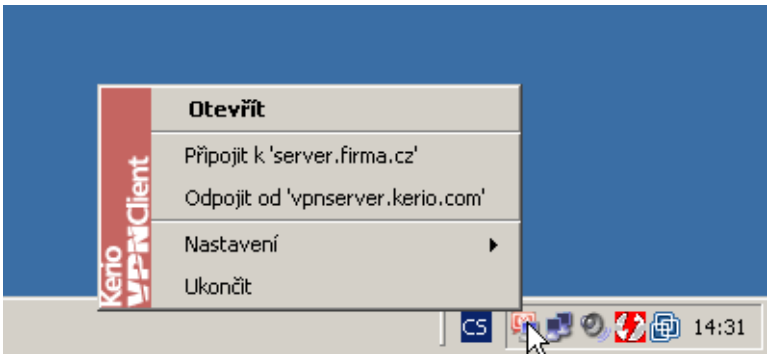


Obrázek 2.5 Kontextové menu (základní režim)

- *Otevřít* — zobrazení hlavního okna programu *Kerio VPN Client* (zobrazuje se vždy okno naposledy nastaveného režimu).

- *Připojit / Odpojit* — připojení k VPN serveru, resp. ukončení aktuálního spojení.

  V rozšířeném režimu (viz kapitola 2.3) může být *Kerio VPN Client* připojen k více serverům současně. V kontextovém menu ikony na nástrojové liště se pak zobrazují volby pro připojení nebo odpojení od jednotlivých serverů.



Obrázek 2.6 Kontextové menu (rozšířený režim)

- *Nastavení* — konfigurace některých parametrů programu *Kerio VPN Client* (viz níže).

- *Ukončit* — ukončení programu *Kerio VPN Client*.

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 angličtiny, češtiny, slovenštiny, španělštiny a ruštiny.

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*).

Základním (vestavěným) jazykem je angličtina. Pro ostatní lokalizace musí být k dispozici příslušné definiční soubory (soubory s příponou `.qm` v podadresáři `Translations` instalačního adresáře aplikace *Kerio VPN Client*).

Volba *Povolit bublinové zprávy* zapíná/vypíná zobrazování informativních zpráv po úspěšném navázání VPN připojení a po jeho odpojení. Nastavení těchto zpráv závisí pouze na osobních preferencích uživatele (informace o stavu připojení lze získat kdykoliv z hlavního okna aplikace *Kerio VPN Client*).

2.2 Kerio VPN Client v základním režimu

V základním režimu obsahuje hlavní okno programu *Kerio VPN Client* pouze dialog pro připojení k serveru.

Obrázek 2.7 Hlavní okno v základním režimu

Do položek *Server*, *Uživatelské jméno* a *Heslo* je třeba zadat jméno (příp. IP adresu) VPN serveru, uživatelské jméno a heslo.

Po zapnutí volby *Uložit heslo* si *Kerio VPN Client* zapamatuje zadané heslo — při dalším připojování nebude třeba zadávat heslo znovu (heslo se ukládá do uživatelského profilu uživatele, pod kterým byl *Kerio VPN Client* spuštěn). Ukládat heslo doporučujeme pouze v případě, kdy je zajištěno, že připojení do vzdálené sítě nemůže být zneužito neoprávněnou osobou.

Volba *Trvalé připojení* zapíná režim trvalého (perzistentního) spojení. Pokud bude spojení z nějakého důvodu přerušeno (např. výpadek internetového připojení), *Kerio VPN Client* se jej automaticky pokusí obnovit. Bude-li rovněž zapnuta volba *Připojovat automaticky*, bude perzistentní spojení automaticky obnoveno také po novém přihlášení uživatele (po odhlášení, restartu nebo vypnutí počítače).

Pro automatické obnovení spojení musí *Kerio VPN Client* znát příslušné uživatelské heslo — proto je tato volba dostupná pouze v případě, pokud je zapnuta volba *Uložit heslo*.

Stisknutím tlačítka *Připojit* dojde k navázání spojení — zabezpečeného šifrovaného komunikačního kanálu mezi klientem a vzdálenou privátní sítí (tlačítko je aktivní, pouze pokud není spojení navázáno). Při navazování spojení provádí *Kerio VPN Client* kontrolu SSL certifikátu příslušného WWW serveru (podrobnosti viz kapitola 2.4).

Po úspěšném připojení bude dialogové okno skryto. O stavu VPN spojení bude uživatel informován prostřednictvím ikony na nástrojové liště (viz kapitola 2.1).

Tlačítkem *Odpojit* lze ukončit spojení s VPN serverem. Po ukončení spojení se dialog dostane zpět do výchozího stavu, tzn. budou dostupné všechny výše popsané volby a aktivní tlačítko *Připojit*.

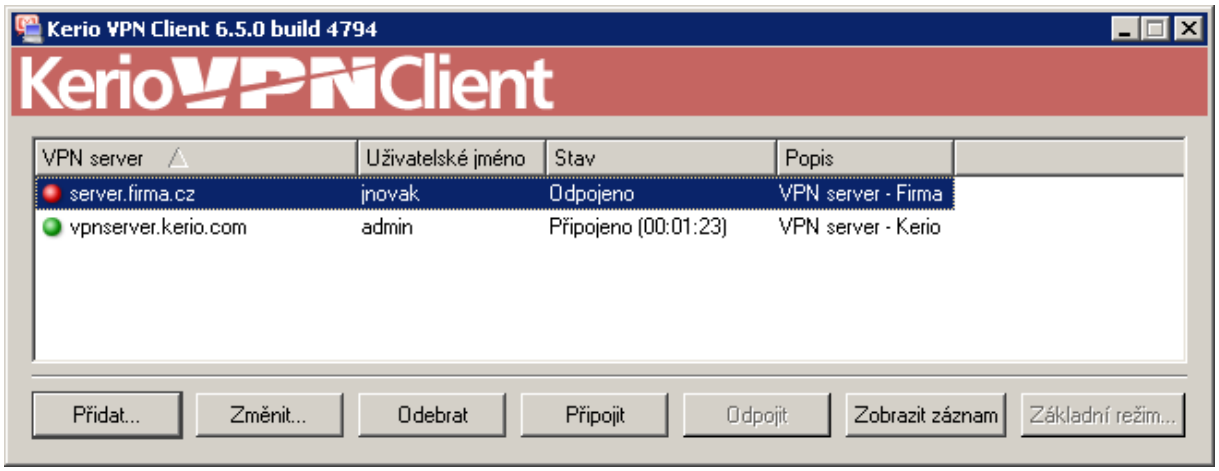
Tlačítko *Rozšířený režim* přepíná aplikaci *Kerio VPN Client* do režimu, kdy lze vytvořit více VPN připojení současně a jsou k dispozici některé další funkce. Přepnutí je možné pouze v odpojeném stavu. Podrobnosti o rozšířeném režimu naleznete v kapitole 2.3.

Poznámky:

1. Při přepnutí do rozšířeného režimu se nepřenášejí žádné přihlašovací údaje.
2. Uzavřením hlavního okna nedojde k ukončení programu *Kerio VPN Client*! *Kerio VPN Client* lze ukončit volbou *Exit* z kontextového menu ikony na nástrojové liště (viz kapitola 2.1).

2.3 Kerio VPN Client v rozšířeném režimu

V rozšířeném režimu obsahuje horní část hlavního okna programu *Kerio VPN Client* seznam uložených připojení (tj. položek s přihlašovacími informacemi pro jednotlivé servery). V dolní části okna lze volitelně zobrazit záznam o činnosti programu.

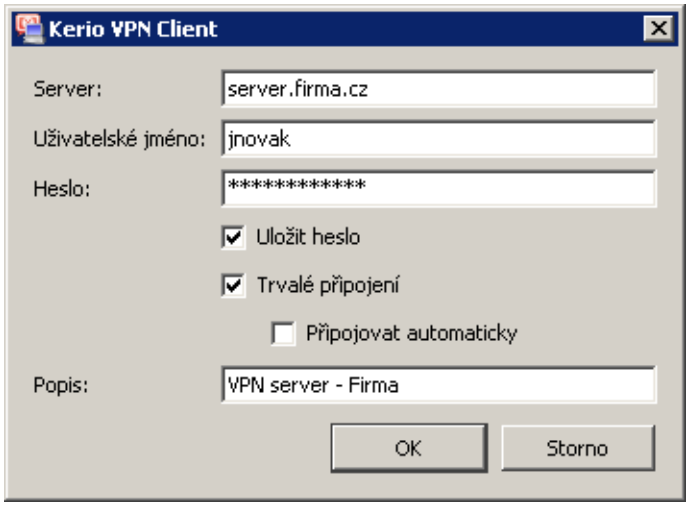


Obrázek 2.8 Hlavní okno v rozšířeném režimu

Ve sloupci *Stav* se zobrazují následující stavy:

- *Odpojeno* — připojení je neaktivní,
- *Připojování...* — probíhá připojování (navazování spojení, kontrola certifikátu serveru atd.),
- *Připojeno (hh:mm:ss)* — připojení je aktivní (v závorce je uvedena doba připojení),
- *Chyba (nnn): Text* — při navazování spojení došlo k chybě. V závorce je uvedeno číslo chyby, za dvojtečkou pak podrobný popis chyby.

Tlačítko *Přidat...* otevírá dialog pro definici nového VPN připojení.



Obrázek 2.9 Rozšířený režim — definice připojení

- *Server* — DNS jméno nebo IP adresa VPN serveru, ke kterému se *Kerio VPN Client* připojuje.
- *Uživatelské jméno* — uživatelské jméno pro ověření na VPN serveru.
- *Heslo* — heslo pro ověření na VPN serveru.
- *Uložit heslo* — volba pro uložení hesla uživatelského profilu.

  Heslo doporučujeme ukládat pouze v případě, kdy je zajištěno, že přístup do vzdálené privátní sítě nemůže být zneužit neoprávněnou osobou.
- *Trvalé připojení* — zapnutím této volby bude připojení označeno jako trvalé. Tato připojení *Kerio VPN Client* automaticky udržuje v připojeném stavu (po výpadku spojení bude toto připojení automaticky obnoveno).
- *Připojovat automaticky* — trvalé připojení bude automaticky obnoveno také po dalším přihlášení uživatele (po odhlášení, restartu nebo vypnutí počítače).

Tlačítko *Změnit...* otevírá dialog pro změnu parametrů vybraného připojení (shodný s dialogem pro vytvoření nového připojení). Tlačítkem *Odebrat* lze vybrané připojení odstranit. Tato dvě tlačítka jsou aktivní pouze v případě, že je vybrané připojení v odpojeném stavu.

Tlačítka *Připojit*, resp. *Odpojit* slouží k připojení, resp. odpojení vybrané položky (v závislosti na stavu vybrané položky je aktivní vždy jedno z těchto tlačítek).

Tlačítko *Základní režim* přepíná aplikaci *Kerio VPN Client* do základního režimu (viz kapitola 2.2). Přepnutí režimů je možné, pouze pokud jsou všechna definovaná připojení v odpojeném stavu. V opačném případě se zobrazí chybové hlášení.

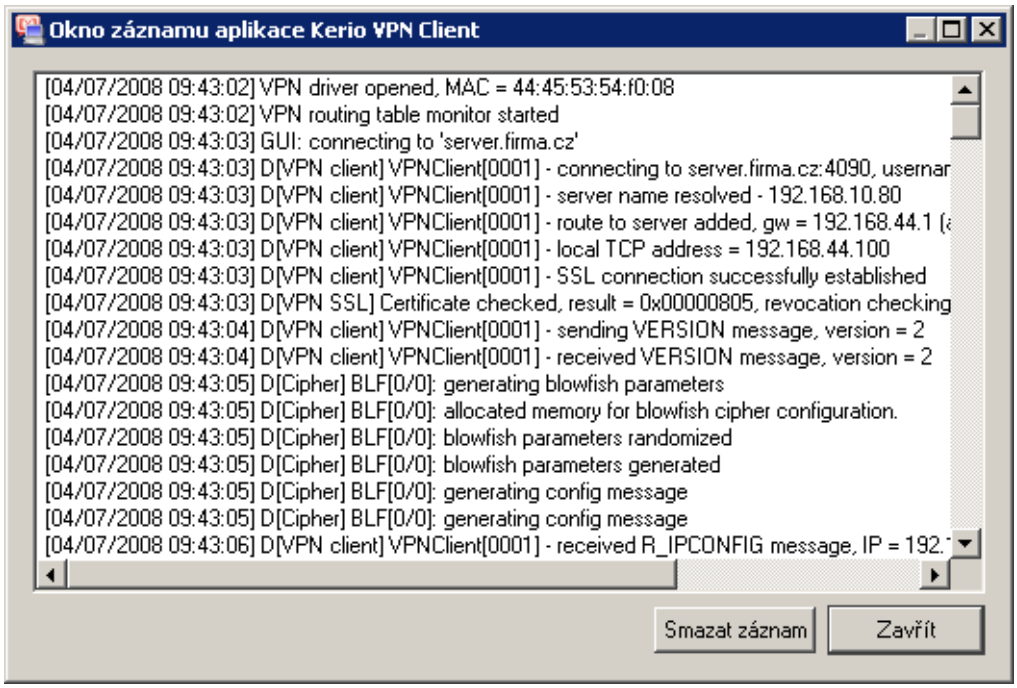
Poznámky:

1. Při přepnutí do základního režimu se nepřenášejí žádné přihlašovací údaje.

2. Uzavřením hlavního okna nedojde k ukončení programu *Kerio VPN Client*! *Kerio VPN Client* lze ukončit volbou *Exit* z kontextového menu ikony na nástrojové liště (viz kapitola 2.1).

Záznam o činnosti programu Kerio VPN Client

Tlačítkem *Zobrazit záznam* lze zobrazit samostatné okno s podrobným záznamem o činnosti programu *Kerio VPN Client*.



Obrázek 2.10 Záznam aplikace Kerio VPN Client

Do záznamu se zapisují informace o inicializaci aplikace *Kerio VPN Client*, navazování spojení, ověřování, výměně směrovacích informací, detekovaných chybách atd. Na každém řádku záznamu jsou uvedeny informace o jedné události. Řádek vždy začíná časovou značkou (datum a čas, kdy událost nastala). Za časovou značkou následuje popis příslušné události.

Záznam je udržován pouze v operační paměti, neukládá se do souboru. Po stisknutí tlačítka *Smazat záznam* nebo při ukončení aplikace *Kerio VPN Client* budou všechny informace ze záznamu nenávratně smazány.

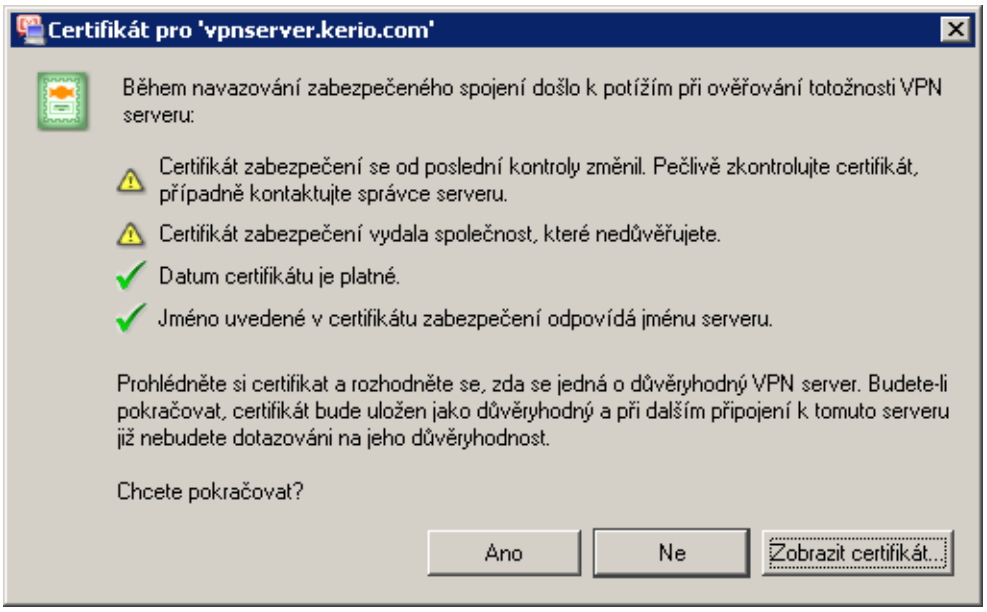
Informace ze záznamu lze využít při testování a hledání chyb, případně konzultaci problémů s technickou podporou firmy Kerio Technologies.

TIP: V záznamu lze myší označit část textu a volbou z kontextového menu (po kliknutí pravým tlačítkem myši v okně záznamu) jej zkopírovat do schránky. Kontextové menu nabízí rovněž

volbu pro označení celého záznamu. Pro kopírování textu do schránky a označení celého záznamu lze také použít standardní klávesové zkratky *Ctrl-C* a *Ctrl-A*.

2.4 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.

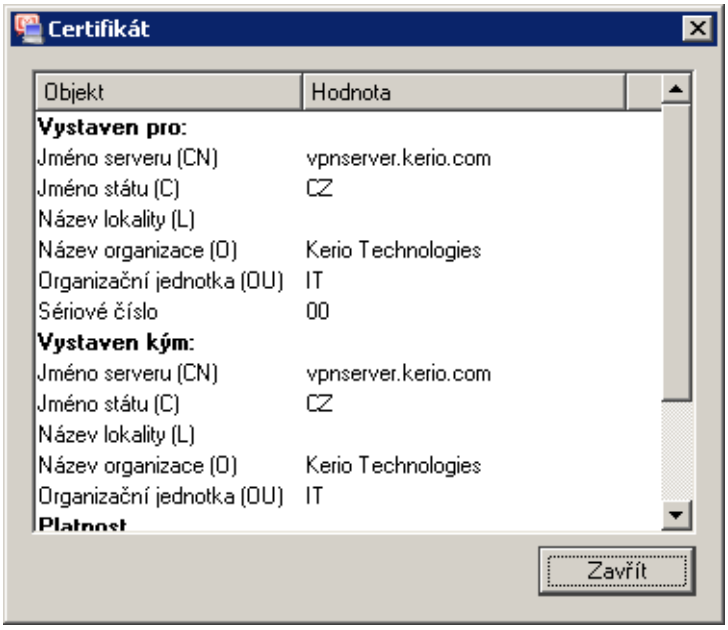


Obrázek 2.11 Informace o problémech s certifikátem VPN serveru

Tlačítko *Zobrazit certifikát* otevírá nové okno s podrobnými informacemi 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.

Poznámka: Další informace o certifikátech VPN serverů naleznete v manuálu *Kerio WinRoute Firewall — Příručka administrátora*.



Obrázek 2.12 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).

Poznámka: Při použití funkce *Vytvořit certifikát* dojde k vytvoření certifikátu, který je podepsán sám sebou (*self-signed* — vydavatel certifikátu je shodný s jeho subjektem). Tento typ certifikátu nezajišťuje plnou bezpečnost a na straně klienta jej nelze automaticky akceptovat. Pro zajištění plné bezpečnosti je třeba použít certifikát vydaný důvěryhodnou certifikační autoritou. Podrobnosti viz zmíněný manuál k produktu *Kerio WinRoute Firewall*.

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). Doporučujeme konzultovat tento problém se správcem příslušného VPN serveru.

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). Kontaktujte správce příslušného VPN serveru.

2.5 Výběr režimu a trvalá připojení

Po přihlášení do operačního systému Windows se *Kerio VPN Client* pokouší obnovit trvalá připojení:

- Pokud byl *Kerio VPN Client* ukončen v základním režimu, pokusí se obnovit připojení definované v dialogu základního režimu (jsou-li zapnuty volby *Trvalé připojení* a *Připojovat automaticky* — viz kapitola 2.2).

- Byl-li *Kerio VPN Client* ukončen v rozšířeném režimu, pak se pokusí obnovit všechna VPN spojení definovaná v dialogu rozšířeného režimu a označená jako trvalá s automatickým připojováním (viz kapitola 2.3).

Není-li v příslušném režimu definováno (žádné) automaticky připojované trvalé připojení, *Kerio VPN Client* se ukončí (uživatel jej může kdykoliv později spustit ručně).

Z výše uvedeného vyplývá, že je velmi důležité, ve kterém režimu byl *Kerio VPN Client* ukončen. Proto doporučujeme zvolit jeden režim a používat jej (tzn. nepřepínat se „chaoticky“ mezi oběma režimy).