

Kerio VPN Client

Příručka uživatele

Kerio Technologies

© 2012 Kerio Technologies s.r.o. Všechna práva vyhrazena.

Tento manuál popisuje program *Kerio VPN Client* ve verzi 7.3 pro *Mac OS X*. Změny vyhrazeny.

Obsah

1	Úvod	4
1.1	Systémové požadavky	4
1.2	Instalace	4
1.3	Licence	5
1.4	Jak Kerio VPN Client funguje?	5
2	Použití aplikace Kerio VPN Client	6
2.1	Panel systémových předvoleb — definice VPN připojení	6
2.2	Stavová ikona na liště hlavní nabídky	7
2.3	Kontrola SSL certifikátu VPN serveru	9
2.4	Záznamy	12
A	Právní doložka	13

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.

Konfigurační údaje se ukládají do domovské složky uživatele, který s aplikací *Kerio VPN Client* pracuje. 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 nevykazuje konflikty s jinými aplikacemi.

1.2 Instalace

Kerio VPN Client nainstalujeme z příslušného balíku s příponou `.dmg` (např. `kerio-control-vpnclient-1.2.3-4567-mac.dmg`), který se připojí jako disk. Z připojeného disku spustíme instalační program *Kerio VPN Client Installer*. Instalace probíhá formou standardního instalačního průvodce.

Kerio VPN Client se instaluje jako panel systémových předvoleb (*System Preferences*). Při instalaci je v systému vytvořen virtuální síťový adaptér `kvnet0` a systémová služba *Kerio VPN*

Client Service (*kvpncsvc*), která je ihned spuštěna a automaticky spouštěna při každém startu systému.

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 *kvnet0*). 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 a příponu domény DNS. Díky tomu je možné zadávat počítače ve vzdálené síti jejich jmény.

Změna konfigurace DNS způsobí, že všechny DNS požadavky z počítače klienta budou odesílány na DNS server ve vzdálené privátní síti. Uživatel však ve většině případů žádnou změnu nezaznamená. Po ukončení VPN připojení je obnovena původní konfigurace DNS.

V systému *Mac OS X 10.5 Leopard* může VPN server přidělovat klientovi také adresu primárního, případně i sekundárního WINS serveru. Služba WINS umožňuje procházet okolní počítače v síti *Microsoft Windows*. Stejně jako v případě DNS je po ukončení VPN připojení obnovena původní konfigurace WINS.

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

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 panelu systémových předvoleb *Kerio VPN Client* uživatel zadá přihlašovací údaje 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.

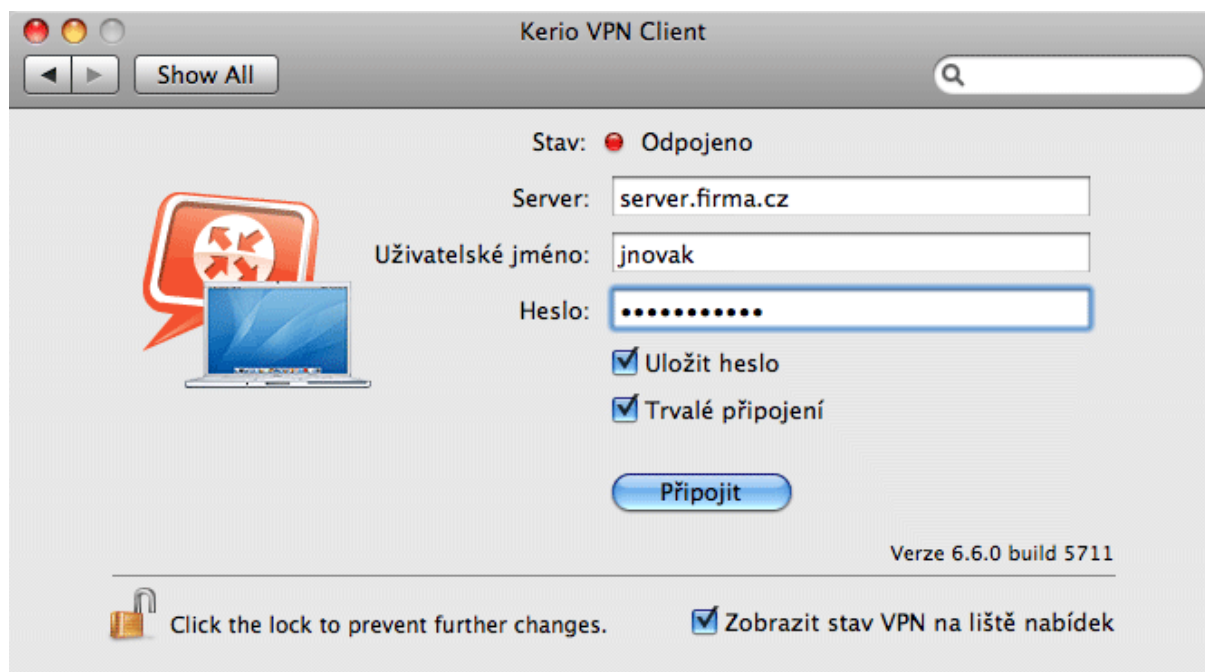
Pro navázání a ukončení trvalého VPN připojení musí mít uživatel na klientském počítači administrátorská práva (uživatelský účet typu *správce počítače*). Uživatelé bez administrátorských práv mohou využít pouze přístup do vzdálené privátní sítě, pokud je VPN připojení navázáno.

2.1 Panel systémových předvoleb — definice VPN připojení

Panel *Kerio VPN Client* je umístěn v systémových předvolbách (*System Preferences*) v sekci *Ostatní (Others)*. Tento panel lze také snadno otevřít klepnutím na stavovou ikonu v pravé části lišty hlavní nabídky (viz kapitola [2.2](#)).

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](#)). Trvalé připojení může navazovat a ukončovat pouze administrátor počítače. Pro navázání trvalého připojení je nutné panel systémových předvoleb nejprve „odemknout“. Je-li trvalé VPN připojení právě



Obrázek 2.1 Hlavní okno aplikace Kerio VPN Client

navázáno, pak je při otevírání panelu systémových předvoleb vyžadováno zadání jména a hesla uživatele s administrátorskými právy.

Kerio VPN Client si zapamatovává zadaný VPN server, odpovídající uživatelské jméno a volbu trvalého připojení. Uživatel může zvolit, zda má být uloženo také zadané heslo.

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 panelu se zobrazuje aktuální stavová informace (připojeno/odpojeno, připojuje se/odpojuje se...) nebo chybové hlášení (připojení se nezdařilo, chyba ověření uživatele...).

Základní informaci o stavu VPN připojení (odpojeno, připojuje se, připojeno) poskytuje rovněž ikona aplikace *Kerio VPN Client* v pravé části lišty hlavní nabídky. Tuto ikonu lze povolit nebo zakázat volbou *Zobrazit stav VPN na liště nabídek*. Podrobnosti viz kapitola [2.2](#).

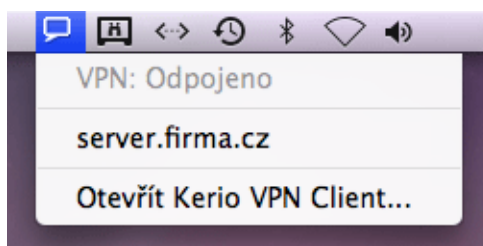
2.2 Stavová ikona na liště hlavní nabídky

Součástí aplikace *Kerio VPN Client* je stavová ikona, která se zobrazuje v pravé části lišty hlavní nabídky. Klepnutím na tuto ikonu se zobrazí kontextové menu se stavovou informací a dalšími volbami.

Použití aplikace Kerio VPN Client

Poznámka: Zobrazení ikony na liště hlavní nabídky lze zakázat v panelu systémových předvoleb *Kerio VPN Client* (viz kapitola [2.1](#)).

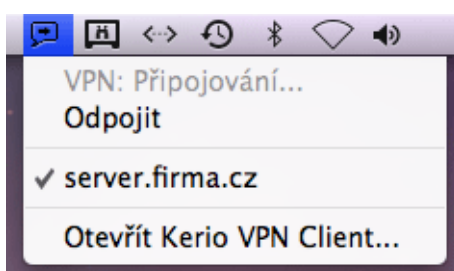
- Neaktivní stav (VPN připojení není navázáno) je znázorněn prázdnou ikonou ve tvaru bubliny — logo aplikací *Kerio Technologies*.



Obrázek 2.2 Ikona aplikace Kerio VPN Client v odpojeném stavu

Název serveru v menu představuje uložené přihlašovací údaje k příslušnému VPN serveru. Klepnutím na tento název *Kerio VPN Client* zahájí navazování VPN spojení. Pokud je připojení definováno jako trvalé, je nutné nejprve zadat uživatelské jméno a heslo uživatele s administrátorskými právy na klientském počítači.

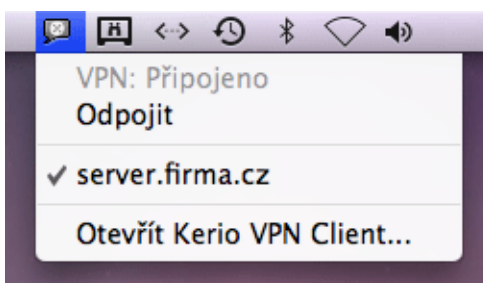
- Probíhající navazování VPN spojení je znázorněno ikonou se šipkou.



Obrázek 2.3 Ikona aplikace Kerio VPN Client ve stavu navazování spojení

Volbou *Odpojit* lze navazování spojení přerušit.

- Aktivní VPN připojení je znázorněno ikonou s logem *Kerio Control*.



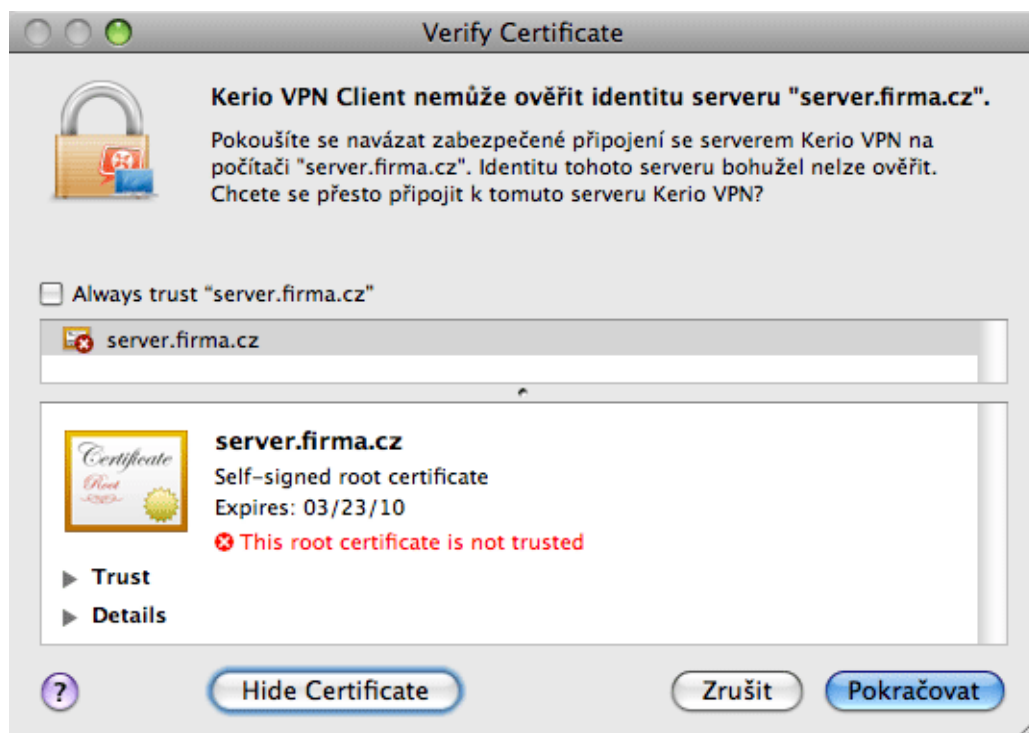
Obrázek 2.4 Ikona aplikace Kerio VPN Client v připojeném stavu

Volbou *Odpojit* lze ukončit navázané připojení. Pokud se jedná o trvalé připojení, je nutné nejprve zadat uživatelské jméno a heslo uživatele s administrátorskými právy na klientském počítači.

Název serveru má v tomto případě pouze informativní charakter.

2.3 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 2.5 Informace o problémech s certifikátem VPN serveru

Volbou *Podrobnosti (Details)* 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 uživatel může zvolit jednu z možností:

- Zrušit připojení — v případě jakýchkoliv pochybností o důvěryhodnosti VPN serveru. Zároveň je doporučeno neprodleně kontaktovat správce příslušného serveru a informovat jej o zjištěných problémech.
- Pokračovat v připojování — typicky v případě, pokud je server důvěryhodný a problémy s certifikátem mají pouze dočasný charakter. *Kerio VPN Client* povolí

připojení k danému serveru pouze jednorázově a příštím pokusu o připojení bude opět zobrazeno varování (nebude-li problém s certifikátem do té doby vyřešen).

- Pokračovat a prohlásit certifikát za důvěryhodný (volbou *Always trust* — *Vždy důvěřovat*). Certifikát bude uložen do systémové klíčenky (*Keychain*) a při dalším připojování již nebude zobrazeno žádné varování. Toto je vhodné provést v případě, že server používá certifikát, který je podepsán sám sebou.

Poznámka: V systému *Mac OS X 10.4 Tiger* nelze automaticky nastavit jako důvěryhodný certifikát, který je podepsán sám sebou. Zde je potřeba certifikát ručně vložit do klíčenky — viz níže.

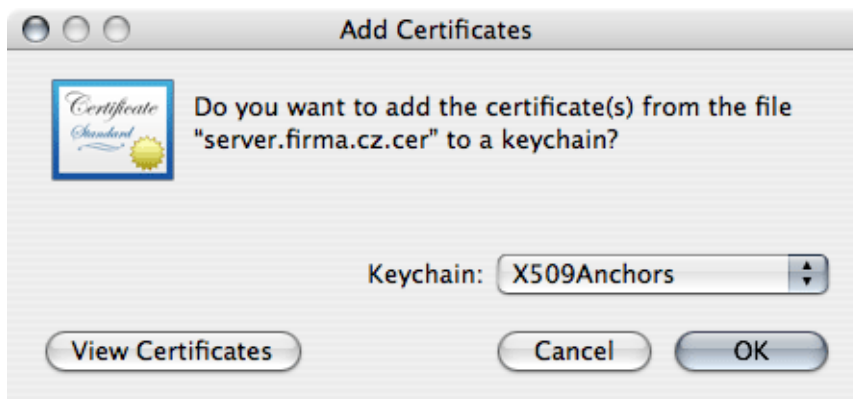
Upozornění:

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

Nastavení důvěryhodného certifikátu v systému Mac OS X 10.4 Tiger

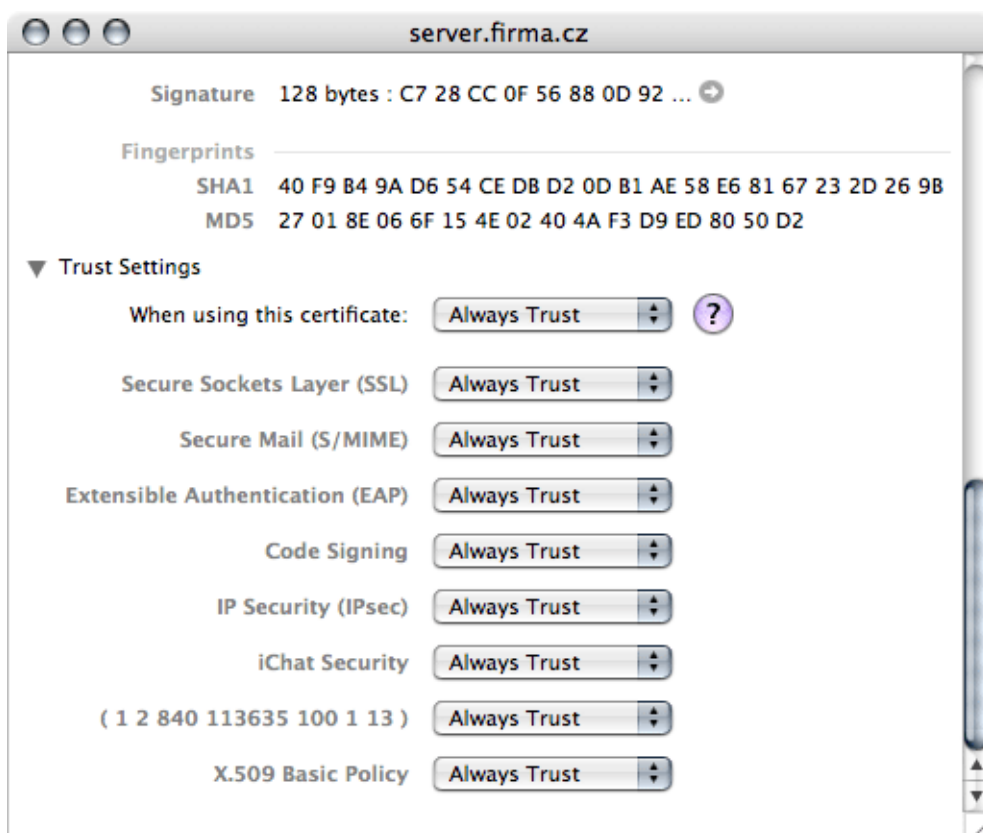
V systému *Mac OS X 10.4 Tiger* nelze automaticky označit jako důvěryhodný certifikát, který je podepsán sám sebou (systém dovolí uložit do klíčenky pouze certifikát vystavený důvěryhodnou certifikační autoritou). V případě takového certifikátu je potřeba provést následující kroky:

1. V okně s varováním o nedůvěryhodném certifikátu (viz obr. 2.5) klepneme na obrázek certifikátu a přetáhneme jej na pracovní plochu. Tím bude na ploše vytvořen soubor certifikátu (např.: `server.firma.cz.cer`).
2. *Důležité:* Nyní nesmí být spuštěna aplikace *Keychain Access*. Je-li právě otevřena, zavřeme ji.
3. Klepnutím na soubor certifikátu na ploše se spustí aplikace *Keychain Access* a zobrazí se dotaz, do které klíčenky má být certifikát uložen.



Obrázek 2.6 Uložení certifikátu do klíčenky

4. Zvolíme klíčenku *X509Anchors*. Do této klíčenky se ukládají certifikáty, které mohou podepisovat jiné certifikáty (typicky certifikáty certifikačních autorit).
Pro přidání certifikátu bude vyžadováno ověření uživatele s administrátorskými právy.
5. V aplikaci *Keychain Access* zvolíme klíčenku *X509Anchors*, vyhledáme přidáný certifikát (např.: *server.firma.cz*) a klepnutím jej otevřeme.
6. V okně se zobrazeným certifikátem odrolujeme na konec, rozbalíme sekci *Trust Settings* (nastavení důvěryhodnosti) a v položce *When using this certificate* (při použití tohoto certifikátu) zvolíme *Always Trust* (vždy důvěřovat).



Obrázek 2.7 Vlastnosti certifikátu — nastavení důvěryhodnosti

7. Ukončíme spuštěné aplikace a odhlásíme se ze systému.
8. Po novém přihlášení zkusíme navázat VPN připojení k příslušnému serveru. Nyní by již nemělo být zobrazeno žádné varování v souvislosti s certifikátem.

2.4 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, tj. `/usr/local/kerio/vpnclient`

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 ve skryté podsložce domovské složky uživatele, který s aplikací *Kerio VPN Client* pracuje:

`~/.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

Mac OS® a *Safari™* jsou registrované ochranné známky nebo ochranné známky společnosti *Apple Inc.*

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