

Kerio Administration Console

Nápověda

© Kerio Technologies. Všechna práva vyhrazena.

Tato nápověda je určena k programu *Kerio Administration Console* ve verzi 2.3.5. Změny vyhrazeny.

Obsah

1	Co je Kerio Administration Console?	4
2	Instalace, umístění souborů a spuštění	5
2.1	Operační systém Windows	5
2.2	Operační systém Linux	6
2.3	Operační systém Mac OS X	7
3	Ovládání programu	9
3.1	Hlavní okno	9
3.2	Připojení k serveru a vytvoření záložky	9
3.3	Kontrola identity serveru	12
3.4	Ochrana záložek heslem	17
3.5	Chyby při připojování	19
3.6	Nastavení jazyka a úvodní obrazovky	21
3.7	Nápověda (Windows)	23
3.8	Import starých záložek	24
4	Síťová komunikace Administration Console	26

Kapitola 1

Co je Kerio Administration Console?

Aplikace *Kerio Administration Console* (dále jen *Administration Console*) slouží ke správě serverových produktů firmy *Kerio Technologies* (tj. *Kerio WinRoute Firewall* a *Kerio MailServer*).

Jedná se o zcela nezávislou aplikaci, která komunikuje se serverovou aplikací (službou) speciálním síťovým protokolem. Tento způsob komunikace umožňuje použít *Administration Console* jak pro lokální správu (tj. přímo z počítače, na kterém služba běží), tak pro vzdálenou správu po síti (z libovolného jiného počítače). Veškerá síťová komunikace mezi *Administration Console* a serverovou aplikací je šifrována — tím je zabráněno odposlechu a zneužití přenášených dat.

Administration Console umožňuje jednorázové připojení k serveru (přihlašovací informace se neukládají) nebo vytvoření tzv. záložky — uložení přihlašovacích informací pro určité servery k opakovanému použití. Uložené záložky mohou být chráněny heslem proti zneužití.

Administration Console je koncipována jako modulární aplikace. Jejím základem je jednoduchý program (dále nazývaný *hlavní okno*), který umožňuje nastavení základních parametrů (např. jazyk administračního rozhraní) a specifikaci přihlašovacích údajů. Podle typu a verze konkrétní serverové aplikace je pak spuštěn odpovídající administrační modul, ve kterém lze konfigurovat její parametry a sledovat její stav. Díky této modularitě poskytuje *Administration Console* kompaktní prostředí pro správu různých verzí serverových aplikací na různých serverech.

Instalace, umístění souborů a spuštění

Tato kapitola obsahuje podrobné informace o instalaci, umístění souborů a spuštění *Administration Console* v operačních systémech — *Windows*, *Linux* a *Mac OS X*. Informace o systémových požadavcích a podporovaných verzích (příp. variantách) jednotlivých operačních systémů jsou uvedeny v manuálech ke konkrétním serverovým aplikacím.

Poznámky:

1. Aplikace *Kerio WinRoute Firewall* je určena pouze pro operační systém *Windows*. Příslušný administrační modul je rovněž k dispozici pouze pro tento systém.
2. Znalost umístění souborů není pro běžné použití *Administration Console* nutná. Umístění souborů je třeba znát při přidávání nových lokalizací (viz kapitola 3.6), nových souborů nápovědy (pouze systém *Windows* — viz kapitola 3.7) nebo při přenášení vytvořených záložek na jiný počítač.

2.1 Operační systém Windows

Administration Console je instalována společně s produktem *Kerio WinRoute Firewall* a/nebo *Kerio MailServer* (ve volitelné instalaci se jedná o komponentu *Administration Console*). Na serveru není nutné instalovat *Administration Console* ze samostatného instalačního balíku.

Administration Console lze spustit z menu *Start* → *Programy* → *Kerio* → *Kerio Administration Console*, případně z kontextového menu programu *WinRoute Engine Monitor* nebo *Kerio MailServer Monitor* (viz manuály k příslušným produktům).

Umístění souborů

Instalačním adresářem *Administration Console* je podadresář *Admin* adresáře, kde jsou nainstalovány produkty *Kerio Technologies* (typicky `C:\Program Files\Kerio\Admin`).

V tomto adresáři se nachází spustitelný soubor *Administration Console* (`kadmin.exe`), jednotlivé administrační moduly (`wradmin*.exe` a `mailadmin*.exe`) a potřebné dynamické knihovny (`*.dll`).

V podadresáři `translations` jsou uloženy lokalizační soubory (`*.qm`) a v podadresáři `help` soubory s nápovědou ve formátu *HTML Help* (`*.chm`).

Záložky (tj. uložené přihlašovací informace pro jednotlivé servery) se ukládají do uživatelského profilu (každý uživatel má vlastní sadu záložek). Každá záložka je uložena v samostatném souboru v adresáři

`C:\Documents and Settings\uzivatel\Application Data\Kerio\Admin`.

(v systémech *Windows 2000/XP/2003*), resp.

C:\Users\uzivatel\Application Data\Kerio\Admin

(v systému *Windows Vista*).

Přípona souboru závisí na aplikaci, pro kterou je záložka určena (.bkwf pro *Kerio WinRoute Firewall* a .bkms pro *Kerio MailServer*).

Instalace Administration Console pro vzdálenou správu

Chceme-li provádět správu serverové aplikace z jiného počítače, nainstalujeme na tento počítač pouze *Administration Console*. K tomuto účelu slouží samostatný instalační balík *Administration Console* pro příslušný produkt (název souboru začíná *kerio-kwf-admin*, resp. *kerio-kms-admin*).

— **Tip** —

Instalační balík *Administration Console* pro *Kerio MailServer* lze stáhnout prostřednictvím odkazu na stránce *Integrace* ([http\(s\)://jmeno_serveru/integration/](http(s)://jmeno_serveru/integration/)). Tímto způsobem vždy získáte *Administration Console* ve verzi odpovídající verzi příslušného serveru.

Instalaci provedeme jednoduše spuštěním příslušného instalačního balíku. Pokud je na počítači již nainstalována starší verze *Administration Console* nebo *Administration Console* pro jiný produkt, nedoporučujeme měnit výchozí instalační adresář!

Po úspěšné instalaci lze *Administration Console* spustit z menu *Start* → *Programy* → *Kerio* → *Kerio Administration Console*.

2.2 Operační systém Linux

Pro operační systém *Linux* je *Administration Console* distribuována pouze v samostatném RPM balíku (název balíku začíná *kerio-kms-admin*). Tento balík je třeba nainstalovat jak na serveru (pro lokální správu), tak na počítačích, ze kterých má být prováděna vzdálená správa.

Administration Console nainstalujeme příkazem:

```
rpm -i <název_instalačního_souboru>
```

tedy např.: `rpm -i kerio-mailserver-6.1.2build573-linux.i386.rpm`

Je-li již *Administration Console* nainstalována, můžeme provést upgrade na novější verzi příkazem:

```
rpm -U <název_instalačního_souboru>
```

Administration Console můžeme odinstalovat příkazem:

```
rpm -e kerio-mailserver-admin
```

Spuštění Administration Console

Ke spuštění *Administration Console* slouží skript `kerioadmin`. Tento skript je umístěn v adresáři `/usr/bin`, do kterého je v systému standardně nastavena cesta.

Upozornění: *Administration Console* by měla být vždy spuštěna uvedeným skriptem. Při přímém spuštění souboru `kadmin` může dojít k načtení nesprávné verze knihovny *Qt* (případně tato knihovna nebude nalezena vůbec) a *Administration Console* nebude fungovat správně.

Umístění souborů

Administration Console se instaluje do adresáře `/opt/kerio/admin`. V tomto adresáři se nachází spustitelný soubor *Administration Console* (`kadmin`), jednotlivé administrační moduly (`mailadmin*`) a potřebné dynamické knihovny (`lib*`).

Lokalizační soubory (`*.qm`) jsou uloženy v podadresáři `translations`. Návoděda není v systému *Linux* k dispozici.

Záložky (tj. uložené přihlašovací informace pro jednotlivé servery) se ukládají do podadresáře `.kerio/admin` domovského adresáře aktuálního uživatele (každý uživatel má vlastní sadu záložek). Každá záložka je uložena v samostatném souboru. Přípona souboru závisí na aplikaci, pro kterou je záložka určena (v současné době pouze `.bkms` pro *Kerio MailServer*).

Instalace Administration Console pro vzdálenou správu

Administration Console pro vzdálenou správu nainstalujeme stejným způsobem jako pro lokální správu na serveru (viz výše).

Tip

Instalační balík *Administration Console* pro *Kerio MailServer* lze stáhnout prostřednictvím odkazu na stránce *Integrace* ([http\(s\)://jmeno_serveru/integration/](http(s)://jmeno_serveru/integration/)). Tímto způsobem vždy získáte *Administration Console* ve verzi odpovídající verzi příslušného serveru.

2.3 Operační systém Mac OS X

Administration Console je instalována společně s produktem *Kerio MailServer*. Na serveru není nutné instalovat *Administration Console* ze samostatného instalačního balíku.

Administration Console lze spustit ze *System Preferences* → *Other* → *KMS Monitor* → *Administration Console*.

Umístění souborů

Administration Console se instaluje do adresáře `/Applications/Kerio MailServer`. V tomto adresáři se nachází programový balík *Administration Console.app*. V podadresáři `Contents/MacOS` je uložen hlavní spustitelný soubor *Administration Console* a v podadresáři `Contents/Resources` jednotlivé administrační moduly (`mailadmin*`).

Lokalizační soubory (*.qm) jsou uloženy v podadresáři Contents/Resources/translations. Nápověda není v systému *Mac OS X* k dispozici, v adresáři /Applications/Kerio MailServer je však uložen manuál k produktu *Kerio MailServer* ve formátu *PDF*.

Záložky (tj. uložené přihlašovací informace pro jednotlivé servery) se ukládají do podadresáře .kerio/admin domovského adresáře aktuálního uživatele (každý uživatel má vlastní sadu záložek). Každá záložka je uložena v samostatném souboru. Přípona souboru závisí na aplikaci, pro kterou je záložka určena (v současné době pouze .bkms pro *Kerio MailServer*).

Instalace Administration Console pro vzdálenou správu

Chceme-li provádět správu *Kerio MailServeru* z jiného počítače, nainstalujeme na tento počítač pouze *Administration Console*. K tomuto účelu slouží samostatný instalační balík (obraz disku) *Administration Console* (název souboru začíná kerio-kms-admin).

Tip

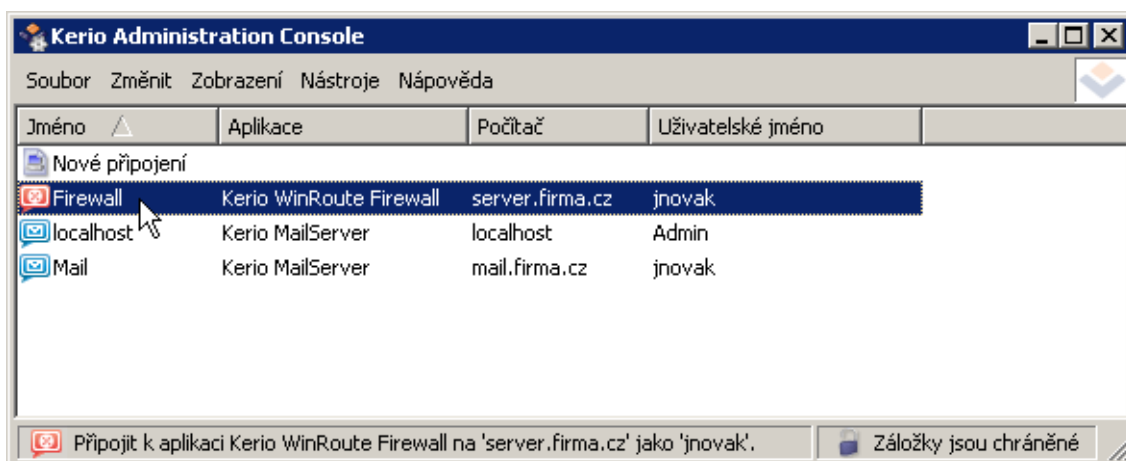
Instalační balík *Administration Console* pro *Kerio MailServer* lze stáhnout prostřednictvím odkazu na stránce *Integrace* ([http\(s\)://jmeno_serveru/integration/](http(s)://jmeno_serveru/integration/)). Tímto způsobem vždy získáte *Administration Console* ve verzi odpovídající verzi příslušného serveru.

Administration Console nainstalujeme jednoduše pomocí průvodce, který se spustí při otevření příslušného obrazu disku. *Administration Console* lze spustit ze *System Preferences* → *Other* → *KMS Monitor* → *Administration Console*.

Ovládání programu

3.1 Hlavní okno

Po spuštění programu *Administration Console* se zobrazí hlavní okno, které obsahuje vytvořené záložky a ikonu *Nové připojení* pro jednorázové připojení k serveru, případně vytvoření nové záložky.



Obrázek 3.1 Hlavní okno Administration Console

Při umístění kurzoru myši na některou záložku se ve stavovém řádku v dolní části okna zobrazí podrobné informace o této záložce (název serverové aplikace, jméno nebo IP adresa serveru a uživatelské jméno). Dvojitým kliknutím na záložku (resp. stisknutím klávesy *Enter* na vybrané záložce nebo volbou *Soubor / Připojit* z hlavního menu) dojde k připojení k příslušnému serveru. Pokud není v záložce uloženo heslo (viz kapitola 3.2), budeme po připojení vyzváni k jeho zadání.

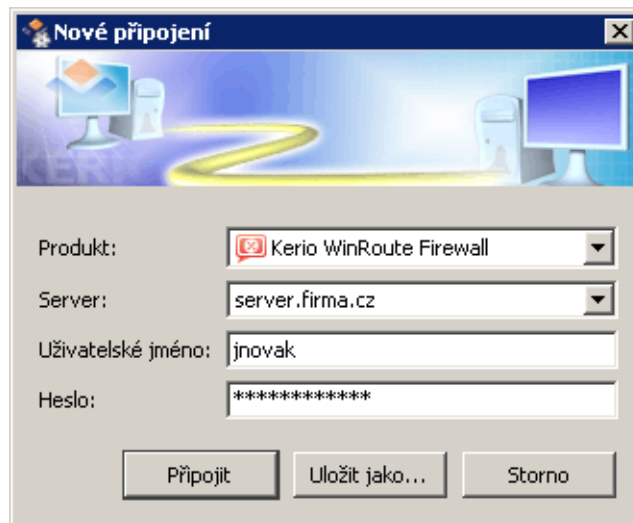
3.2 Připojení k serveru a vytvoření záložky

Dvojitým kliknutím na ikonu *Nové připojení* nebo volbou *Soubor / Nové připojení...* z hlavního menu otevřeme dialog *Nové připojení*.

Produkt

Výběr serverové aplikace, ke které se chceme připojit.

Administration Console při svém spuštění zjistí, jaké administrační moduly jsou k dispozici a nastaví odpovídající aplikace do této položky. Není-li administrační program pro určitou aplikaci k dispozici, nelze se pokusit o připojení ani vytvořit záložku.



Obrázek 3.2 Dialog pro připojení k serverové aplikaci

Server

DNS jméno nebo IP adresa počítače, na kterém je nainstalována příslušná serverová aplikace.

Chceme-li se k serverové aplikaci přihlásit přímo z počítače, na kterém je nainstalována, zadáme jméno serveru `localhost` (tj. lokální zpětnovazební rozhraní — loopback).

Nedoporučujeme používat IP adresy síťových rozhraní tohoto počítače (resp. odpovídající DNS jména). Podle IP adresy, na kterou se *Administration Console* připojuje, serverová aplikace rozpoznává, zda se jedná o lokální nebo vzdálenou správu. Není-li povolena vzdálená správa, pak aplikace akceptuje pouze připojení na `localhost`.

Dialog *Nové připojení* si pamatuje několik naposledy použitých serverů. Při opakovaném připojování tak stačí pouze vybrat jméno nebo adresu serveru ze seznamu (pro tyto případy však doporučujeme vytvořit si záložku — připojení k serveru pak bude mnohem rychlejší a jednodušší).

Uživatelské jméno, Heslo

Jméno uživatele a heslo pro přihlášení ke správě serverové aplikace. Tento uživatel musí mít právo *Přístup pro čtení i zápis* (pro administraci), případně *Přístup pouze pro čtení* (pro prohlížení konfigurace).

Přihlašovací dialog si rovněž pamatuje naposledy zadané uživatelské jméno.

Stisknutím tlačítka *Připojit* dojde k pokusu o připojení k serverové aplikaci. Je-li připojení i ověření uživatele úspěšné, zobrazí se příslušný administrační modul a hlavní okno *Administration Console* se zavře.

Poznámky:

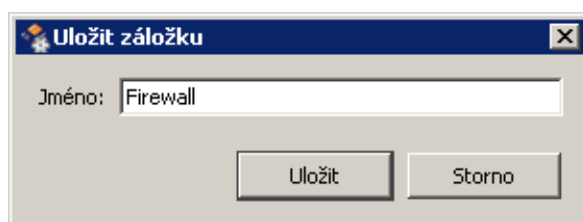
1. Síťový protokol použitý při komunikaci mezi *Administration Console* a serverem je nezávislý na operačním systému. Z toho vyplývá, že např. *Kerio MailServer* na serveru s operačním systémem *Mac OS X* lze vzdáleně spravovat z pracovní stanice se systémem *Windows*

apod.

2. Pro zajištění maximální bezpečnosti provádí *Administration Console* při každém připojení kontrolu důvěryhodnosti certifikátu serveru. Podrobnosti viz kapitola [3.3](#).

Vytvoření záložky

Chceme-li přihlašovací údaje pro určitý server uchovat pro opakované připojení, pak před stisknutím tlačítka *Připojit* stiskneme nejprve tlačítko *Uložit jako*. Toto tlačítko otevírá dialog pro uložení záložky.



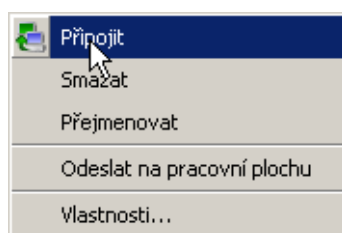
Obrázek 3.3 Dialog pro uložení záložky

Do položky *Jméno* je třeba zadat název, pod kterým bude záložka zobrazována v hlavním okně *Administration Console*. Tento název bude také použit jako jméno souboru, do kterého bude záložka uložena (viz kapitola [2](#)).

Upozornění: Je-li v okamžiku ukládání záložky vyplněno heslo, pak bude toto heslo také uloženo. Záložky v *Administration Console* lze ochránit proti zneužití zadáním hesla pro přístup k záložkám (podrobnosti viz kapitola [3.4](#)).

Kontextové menu pro záložky

Při kliknutí pravým tlačítkem myši na vybranou záložku se zobrazí kontextové menu s těmito funkcemi:



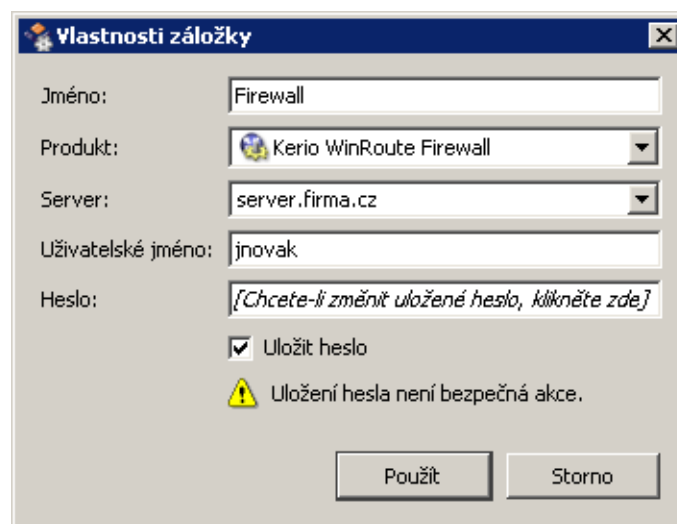
Obrázek 3.4 Kontextové menu pro záložku

- *Připojit* — přihlášení k příslušné serverové aplikaci (připojit se lze rovněž dvojitým kliknutím myši nebo stisknutím klávesy *Enter* na této záložce).
- *Smazat* — odstranění vybrané záložky. Smazání záložky znamená fyzické odstranění příslušného souboru na disku (viz kapitola [2](#)). Smazanou záložku již nelze obnovit (nemáme-li k dispozici zálohu příslušného souboru).

- *Přejmenovat* — změna názvu záložky. Záložku lze rovněž přejmenovat jednoduchým kliknutím levým tlačítkem myši na její název (podobně jako ikonu na pracovní ploše *Windows*) nebo stisknutím klávesy *F2*.
- *Odeslat na pracovní plochu* — vytvoření odkazu na záložku (tj. zástupce příslušného souboru) na pracovní ploše. Soubory záložek jsou asociovány s *Administration Console* — dvojitým kliknutím na záložku na pracovní ploše dojde ke spuštění odpovídajícího administračního modulu a připojení na příslušný server.

Poznámka: Tato funkce je dostupná pouze v operačních systémech *Windows*.

- *Vlastnosti* — tato volba otevírá dialog pro změnu parametrů vybrané záložky. Dialog *Vlastnosti záložky* je spojením výše popsaných dialogů *Nové připojení* a *Uložit záložku*.



Obrázek 3.5 Úprava parametrů záložky

3.3 Kontrola identity serveru

Při připojování ke správě serverové aplikace (*Kerio WinRoute Firewall* nebo *Kerio MailServer* — dále jen *server*) kontroluje *Administration Console* (dále jen *klient*) identitu příslušného serveru. Toto je ochrana proti útoku typu „man-in-the-middle“ (útočník se vydává za cílový server, od klienta získá přihlašovací údaje a ty pak použije pro přihlášení na skutečný server).

Server svou identitu prokazuje SSL certifikátem. Klient pak porovnává tzv. otisk certifikátu s otiskem, který má uložený ve svém konfiguračním souboru. Pokud otisky certifikátu souhlasí, připojení je automaticky povoleno. V opačném případě je nutný zásah uživatele.

Poznámky:

1. Kontrola certifikátu se neprovádí při připojování přímo z počítače, na kterém je nainstalována příslušná serverová aplikace (připojení k `localhost`). V tomto případě totiž útok

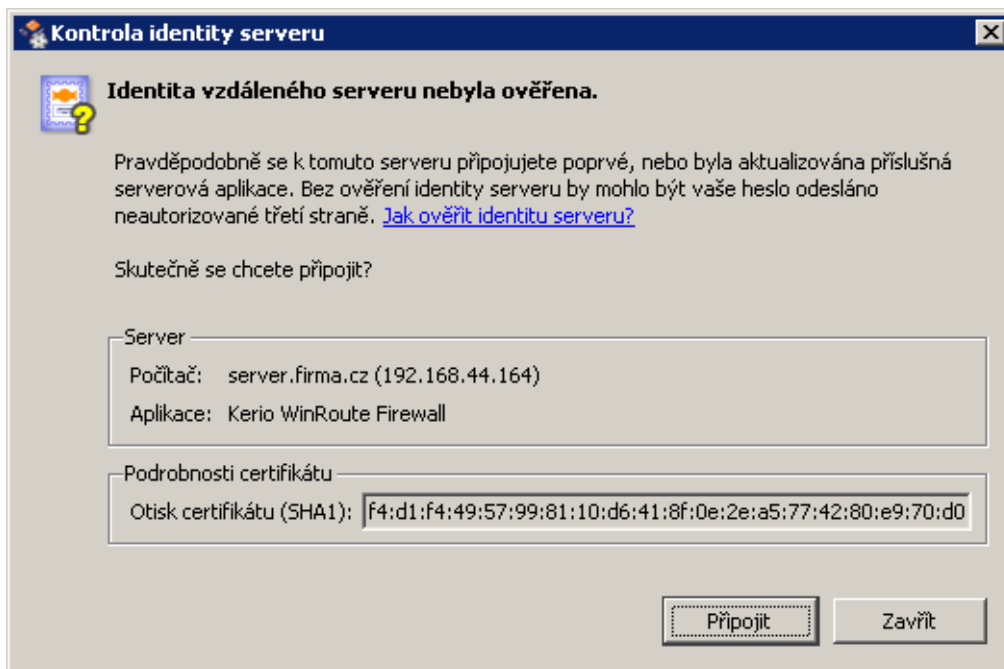
„man-in-the-middle“ nemá smysl (pokud by útočník pronikl přímo na server, mohl by získat požadované informace jednodušším způsobem).

2. Pro účely připojení programem *Administration Console* se nepoužívá SSL certifikát, který je v serverové aplikaci nastaven pro „klientské“ služby (webová rozhraní apod.), ale speciální automaticky generovaný certifikát.

První připojení k serveru

Předpokládejme, že jsme na server `server.firma.cz` nainstalovali aplikaci *Kerio WinRoute Firewall*¹ a nyní se chceme k tomuto serveru poprvé připojit programem *Administration Console* z jiného počítače.

Vyplníme přihlašovací dialog (případně vytvoříme záložku — podrobnosti viz kapitola 3.2). Po stisknutí tlačítka *Připojit* se zobrazí informace, že identitu serveru nebylo možné ověřit — viz obrázek 3.6.



Obrázek 3.6 Kontrola identity serveru — připojení k novému serveru

Nyní musíme zkontrolovat, zda se *Administration Console* skutečně připojuje k požadovanému serveru:

- V poli *Server* zkontrolujeme typ serverové aplikace a IP adresu cílového serveru. Pokud byl server zadán jménem a jeho IP adresa nesouhlasí, je třeba zkontrolovat DNS záznam pro příslušné jméno počítače, případně zadat server přímo IP adresou. Nesprávná IP adresa může signalizovat pokus o útok (podvržení DNS záznamu).

¹ Pro *Kerio MailServer* je postup připojení a ověření identity stejný.

Poznámka: Pokud byl server zadán IP adresou, pak je kontrola DNS záznamů bezpředmětná.

Nesouhlasí-li typ serverové aplikace, pak je vhodné prověřit spuštěné serverové aplikace přímo na příslušném serveru a zkusit se k nim připojit lokálně.

- Porovnáme otisk certifikátu v poli *Podrobnosti certifikátu* s otiskem certifikátu příslušného serveru.

Pokud otisky certifikátů nesouhlasí, jedná se o podvržený certifikát.

TIP: Otisk certifikátu lze označit myší, zkopírovat do schránky a vložit do souboru, e-mailové zprávy apod.

Souhlasí-li IP adresa, typ aplikace i otisk certifikátu, můžeme se k serveru bez obav připojit. V opačném případě připojení zamítneme (tlačítkem *Zavřít*) a pokusíme se najít příčiny zjištěných problémů.

Pokud se při příštím připojení nezmění IP adresa ani certifikát serveru, bude *Administration Console* považovat tento server za důvěryhodný a popsany dialog pro ověření identity se již nezobrazí.

Jak zjistit otisk certifikátu serveru?

Pro zabezpečení komunikace mezi serverovou aplikací a programem *Administration Console* se používá speciální automaticky generovaný SSL certifikát. Tento certifikát se vytvoří při prvním startu serverové aplikace po instalaci, resp. při každém startu, kdy není certifikát nalezen (pokud byl smazán, poškozen apod.). Certifikát je uložen v souboru `server.crt` v podadresáři `dbSSL` instalačního adresáře serverové aplikace (konkrétní umístění závisí na typu aplikace a operačním systému).

Způsob zjištění otisku certifikátu závisí na operačním systému serveru:

Windows

Certifikát serveru je standardně ukládán do adresáře

`C:\Program Files\Kerio\WinRoute Firewall\dbSSL`

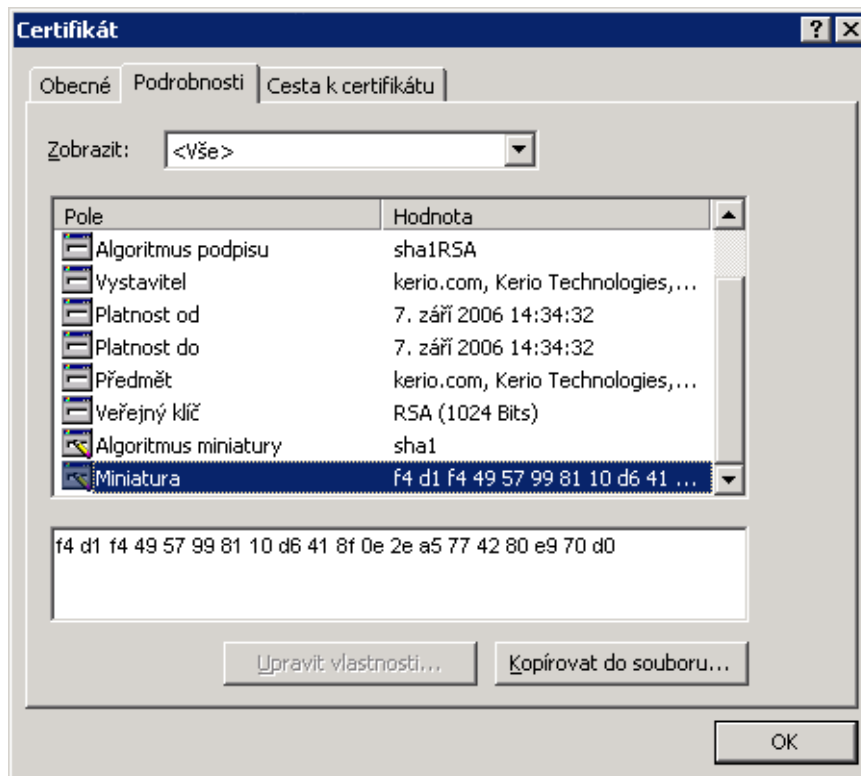
resp.

`C:\Program Files\Kerio\MailServer\dbSSL`

Při otevření souboru s certifikátem (dvojitým kliknutím myší nebo klávesou *Enter*) se zobrazí dialog s informacemi o certifikátu.

V záložce *Podrobnosti* vyhledáme pole *Miniatura*². Toto pole obsahuje otisk certifikátu, který můžeme označit myší, zkopírovat do schránky a vložit do souboru, e-mailové zprávy apod.

² Proprietární název otisku certifikátu.



Obrázek 3.7 Zobrazení otisku certifikátu serveru v systému Windows

Linux a Mac OS X (pouze Kerio MailServer)

Certifikát serveru je standardně ukládán do adresáře

/opt/kerio/mailserver/dbSSL (Linux),

resp.

/usr/local/kerio/mailserver/dbSSL (Mac OS X).

Pro zjištění otisku certifikátu využijeme program `openssl` (v systému musí být nainstalován balík *OpenSSL*).

V konzoli (terminálu) se přepneme do adresáře se souborem `server.crt` a zadáme následující příkaz:

```
openssl x509 -in server.crt -noout -text -fingerprint -sha1
```

Tento příkaz zobrazí informace o certifikátu, přičemž na posledním řádku výpisu bude uveden otisk certifikátu:

```
SHA1 Fingerprint=F4:D1:F4:49:57:99:81:10:D6:41:8F:0E:2E:A5:
77:42:80:E9:70:D0
```

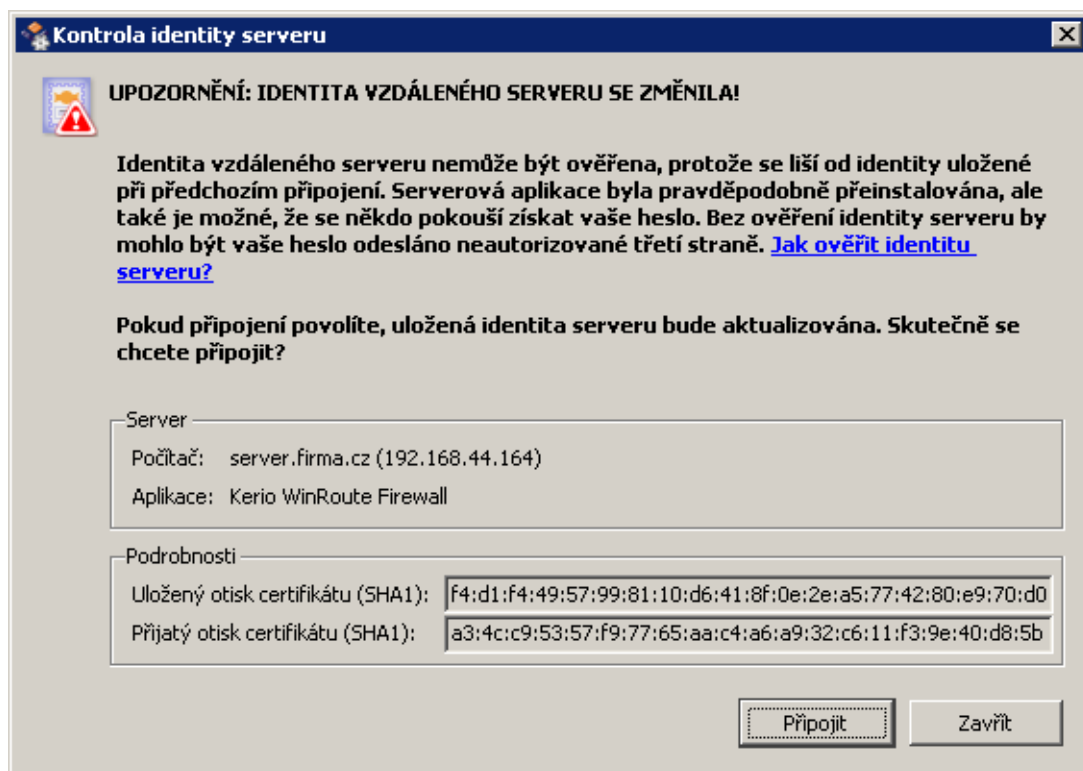
Upozornění: Uvedené informace platí pro produkty *Kerio WinRoute Firewall* verze 6.3.0 a vyšší a *Kerio MailServer* verze 6.4.0 a vyšší. *Administration Console* zároveň zachovává kompatibilitu se staršími verzemi těchto aplikací. Pokud je nainstalován příslušný administrační modul (viz kapitola 2), pak je možné se připojit např. ke správě aplikace *Kerio WinRoute Firewall* 6.2.0. Při prvním připojení (resp. po změně IP adresy atd.) se rovněž zobrazí varování, že

identita serveru nebyla ověřena. U starších verzí serverových aplikací však není možné zjistit otisk SSL certifikátu, který se používá pro připojení ke správě. V tomto případě musíme připojení akceptovat bez kontroly otisku certifikátu, pokud se k danému serveru skutečně chceme připojit.

Opakované připojení k témuž serveru

Pokud nedojde ke změně otisku certifikátu nebo IP adresy serveru, pak při dalších připojeních *Administration Console* ověřuje pouze uživatelské jméno a heslo. Kontrola certifikátu a IP adresy serveru zůstává uživateli skryta.

Dojde-li ke změně otisku certifikátu, zobrazí se varování — viz obrázek 3.8.



Obrázek 3.8 Kontrola identity serveru — detekce změny certifikátu

Tato situace může nastat, pokud byl server přeinstalován, nebo pokud byl jeho certifikát z nějakého důvodu poškozen či smazán. V takovém případě serverová aplikace při svém startu vytvořila nový certifikát, jehož otisk se samozřejmě liší od otisku, který má *Administration Console* uložený. Pokud víme, že na serveru k takové změně došlo, provedeme kontrolu otisku certifikátu stejně jako v případě prvního připojení (viz výše). Pokud nový (přijatý) otisk certifikátu souhlasí s otiskem certifikátu serveru, můžeme připojení povolit. V tomto případě se uložený otisk certifikátu přepíše otiskem nového certifikátu a při dalším připojení již opět nebude zobrazováno žádné varování.

Jestliže k žádné změně certifikátu na serveru nedošlo, pak se s nejvyšší pravděpodobností jedná o útok (podvržení certifikátu). V takovém případě připojení zamítneme (tlačítkem *Zavřít*) a pokusíme se najít příčiny zjištěných problémů.

Poznámka: Při prosté aktualizaci (upgrade) serverové aplikace zůstává certifikát zachován. Přeinstalováním je v tomto případě míněna kompletně nová instalace — např. při výměně pevného disku apod.

Za určitých okolností může také dojít ke změně IP adresy serveru (např. pokud byl server přepojen do jiné subsítě). Při změně IP adresy se (zpravidla) provádí také aktualizace příslušných DNS záznamů. Z toho vyplývá, že při dalším pokusu o vzdálené připojení programem *Administration Console* k příslušné serverové aplikaci sice použijeme stejné DNS jméno, ale IP adresa bude odlišná. Na změnu IP adresy serveru může *Administration Console* reagovat dvěma způsoby:

- Pokud pro novou IP adresu (a port příslušné serverové aplikace) dosud neexistuje záznam, *Administration Console* zobrazí varování jako v případě prvního připojení k novému serveru (viz obrázek [3.6](#)).
- Existuje-li pro novou IP adresu a příslušný port záznam (tzn. *Administration Console* se v minulosti již připojovala k dané serverové aplikaci na dané IP adrese), pak je tato situace vyhodnocena jako změna identity serveru (viz obrázek [3.8](#)).

V obou případech platí, že pokud se jedná o záměrnou (vědomou) změnu IP adresy, pak ve varovném dialogu zkontrolujeme IP adresu a otisk (nového) certifikátu a je-li vše v pořádku, můžeme připojení akceptovat. Pokud k žádné změně IP adresy serveru nedošlo, pak připojení zamítneme a pokusíme se zjistit příčinu tohoto problému.

3.4 Ochrana záložek heslem

Záložky v *Administration Console* slouží k rychlému připojení ke konkrétnímu serveru, a proto obsahují kompletní přihlašovací informace, zpravidla včetně hesla. Pokud k počítači s *Administration Console* získá přístup neoprávněná osoba, mohlo by dojít ke zneužití některé záložky a provedení nežádoucích konfiguračních změn na příslušném serveru.

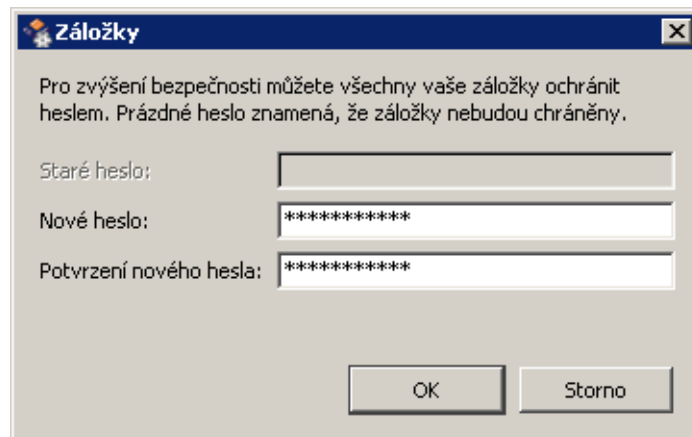
Na ochranu proti zneužití záložek umožňuje *Administration Console* ochránit přístup k záložkám heslem.

Nastavení ochrany záložek

Volbou z hlavního menu *Nástroje / Chránit záložky heslem* se zobrazí dialog pro nastavení hesla.

Ve výchozím stavu (po instalaci *Administration Console*) nejsou záložky chráněny. V dialogu je potřeba zadat zvolené heslo a pro potvrzení jej zopakovat (vyloučení překlepů apod.).

Pokud jsou záložky již chráněny, pak menu *Nástroje* obsahuje položku *Změnit heslo pro ochranu záložek*. Pro změnu hesla je nutné se ověřit zadáním stávajícího hesla do položky



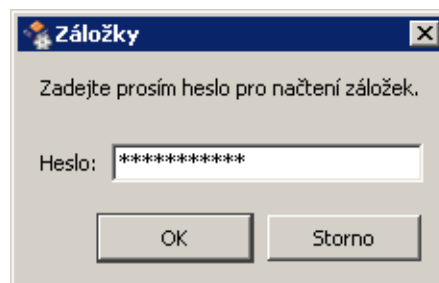
Obrázek 3.9 Nastavení hesla pro ochranu záložek

Staré heslo. Nastavením prázdného hesla (tzn. položky *Nové heslo* a *Potvrzení nového hesla* zůstanou nevyplněné) bude ochrana záložek zrušena.

Upozornění: Záložky doporučujeme chránit heslem vždy, pokud existuje nebezpečí přístupu neoprávněných osob k počítači s *Administration Console*!

Použití chráněných záložek

Jsou-li záložky chráněny heslem, pak se bezprostředně po spuštění *Administration Console* zobrazí dialog pro zadání hesla.



Obrázek 3.10 Zadání hesla pro přístup k záložkám

Po zadání správného hesla bude možné pracovat se záložkami běžným způsobem (viz kapitola 3.2). Pokud bude tento dialog stornován (např. při neznalosti hesla), pak bude možné použít pouze volbu *Nové připojení* pro připojení k serveru bez možnosti vytvoření záložky.

Dialog pro zadání hesla lze znovu vyvolat volbou z hlavního menu *Nástroje / Načíst záložky* (heslo je rovněž vyžadováno při pokusu o použití některé záložky).

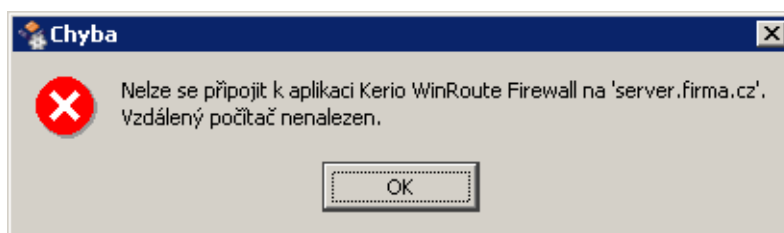
3.5 Chyby při připojování

V této kapitole jsou popsána nejčastější chybová hlášení, která se zobrazují v případě neúspěšného připojení k serverové aplikaci.

Poznámka: Je-li hlášena chyba, která zde není uvedena, doporučujeme kontaktovat technickou podporu firmy *Kerio Technologies* (kontakty naleznete na WWW stránkách <http://www.kerio.cz/>).

Vzdálený počítač nenalezen

Tato chyba je hlášena, pokud je zadaný cílový počítač (server) nedosažitelný.



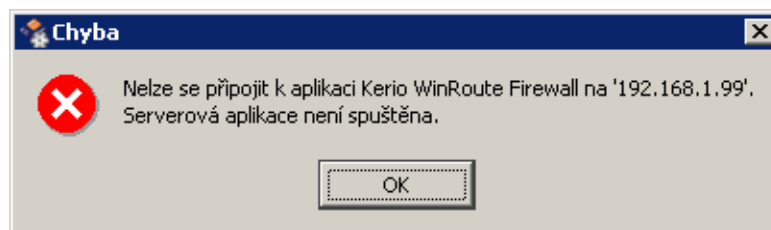
Obrázek 3.11 Chyba při připojování: server nenalezen

Možné příčiny této chyby:

- Chybná IP adresa nebo DNS jméno serveru.
Ujistěte se, že zadáváte správnou IP adresu, případně pro DNS jméno ověřte, zda je platné (např. systémovým nástrojem `nslookup`).
- Cílový počítač není dostupný (např. došlo k síťové chybě nebo je komunikace blokována firewallem).
Vyzkoušejte dostupnost cílového počítače příkazem `ping`, případně proveďte potřebné změny v nastavení firewallu.

Serverová aplikace není spuštěna

Pokud se *Administration Console* nepodaří navázat síťové spojení se serverovou aplikací na daném počítači, pak je hlášena chyba *Serverová aplikace není spuštěna*



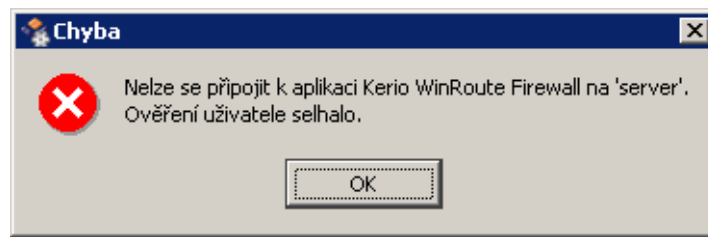
Obrázek 3.12 Chyba při připojování: serverová aplikace není spuštěna

Možné příčiny této chyby:

- Serverová aplikace není spuštěna.
Zkontrolujte, zda na počítači, kam se připojujete, běží služba *Kerio WinRoute Firewall*, resp. *Kerio MailServer*.
- Nelze navázat spojení na port příslušné aplikace (komunikace je blokována firewallem).
Zkuste navázat spojení příkazem `Telnet` na konkrétní port (viz kapitola 4), případně proveďte potřebné změny v nastavení firewallu.

Ověření uživatele selhalo

Pokud *Administration Console* naváže spojení se serverem, ale nastane problém s přihlášením uživatele, zobrazí se hlášení *Ověření uživatele selhalo*.



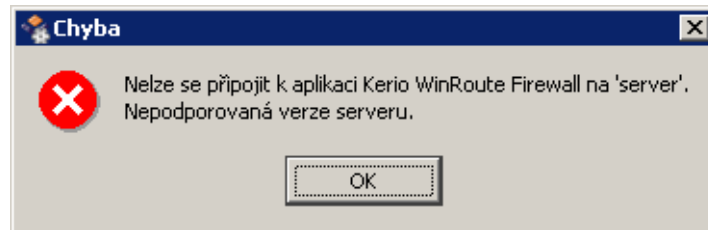
Obrázek 3.13 Chyba při připojování: ověření uživatele selhalo

Možné příčiny této chyby:

- Neplatné uživatelské jméno nebo heslo.
Zkontrolujte, že jsou přihlašovací údaje zadány správně. Pokud tato chyba nastává při připojování pomocí záložky, zkuste se připojit pomocí funkce *Nové připojení* a zadat všechny přihlašovací údaje (např. mohlo dojít ke změně hesla uživatele a záložka stále obsahuje staré heslo).
- Vzdálená správa serverové aplikace není povolena nebo je povolena pouze z určité skupiny IP adres (do které není zařazen váš počítač). Podrobnosti naleznete v manuálu k příslušné serverové aplikaci.
- Uživatel nemá potřebná přístupová práva.
Uživatelský účet, pod kterým se chcete přihlásit, musí mít právo *Přístup pro čtení i zápis* (pro administraci), případně *Přístup pouze pro čtení* (pro prohlížení konfigurace).
- Problém s ověřením uživatele na serveru.
Na serveru se vyskytla chyba, kvůli které nelze uživatele ověřit příslušnou ověřovací metodou (např. v *Active Directory*). Pro účely přihlášení ke správě doporučujeme vytvořit speciální uživatelský účet v interní databázi uživatelů (podrobnosti viz manuál k příslušné serverové aplikaci).

Nepodporovaná verze serveru

Tato chyba je hlášena, pokud *Administration Console* nenalezne administrační modul odpovídající verzi serverové aplikace, ke které se připojujeme (např. na serveru je nainstalován *Kerio WinRoute Firewall 6.1.x*, zatímco administrační modul je k dispozici pouze pro verzi 6.0.x).



Obrázek 3.14 Chyba při připojování: nepodporovaná verze serveru

Je-li při připojování hlášena tato chyba, je třeba nainstalovat (případně zkopírovat do adresáře Admin) příslušný administrační modul. Doporučujeme použít stejný instalační balík, ze kterého byla nainstalována příslušná serverová aplikace.

3.6 Nastavení jazyka a úvodní obrazovky

Volba *Nástroje / Volby* v hlavním menu otevírá dialog pro výběr jazyka *Administration Console* včetně všech spouštěných administračních modulů.



Obrázek 3.15 Nastavení jazyka a předvolby

Volba *Zobrazovat úvodní obrazovku* v dolní části dialogu zapíná/vypíná zobrazování úvodní obrazovky (*splash screen*) administračního modulu při připojování k serverové aplikaci.

Volba *Okno se záložkami nechávat vždy zobrazené* způsobuje, že po připojení k vybrané serverové aplikaci zůstane zobrazeno také hlavní okno *Administration Console* se seznamem záložek. Tuto funkci lze využít zejména v případech, kdy se postupně (střídavě) připojujeme k několika různým serverům.

Poznámka: Ve výchozí konfiguraci *Administration Console* jsou obě výše uvedené volby zapnuté.

Možnosti nastavení jazyka

V sekci *Preferovaný jazyk* lze vybrat jazyk, ve kterém bude zobrazována *Administration Console* a všechny spouštěné administrační moduly.

Položka *Primární* slouží k výběru jazyka, který bude za normálních okolností používán. V případě, že nebude možné načíst definiční soubor zvoleného primárního jazyka (např. chybějící nebo poškozený soubor), pokusí se *Administration Console* načíst jazyk nastavený jako *Alternativní*. Nepodaří-li se načíst ani ten, přepne se *Administration Console* do výchozího jazyka, kterým je angličtina.

Volba *Automaticky* znamená, že se *Administration Console* pokusí automaticky nastavit jazyk podle národního prostředí operačního systému.

Definiční soubory jazyků

Program *Administration Console* (a příslušné administrační moduly) obsahuje pouze anglickou verzi uživatelského rozhraní. Ostatní jazyky musejí být uloženy v tzv. definičních souborech.

Umístění definičních souborů pro jednotlivé operační systémy je podrobně popsáno v kapitole 2. Pro každý podporovaný jazyk jsou potřeba tyto soubory:

kadmin.<jazyk>.qm — pro hlavní okno *Administration Console*

mailadmin<XY>.<jazyk>.qm — pro administrační modul aplikace *Kerio MailServer*

wradmin<VW>.<jazyk>.qm — pro administrační modul aplikace *Kerio WinRoute Firewall* (pouze v systému *Windows*)

kde:

- <XY> je hlavní (jednomístné) a vedlejší (dvojmístné) číslo verze administračního modulu pro *Kerio MailServer*
- <VW> je hlavní a vedlejší číslo verze administračního modulu pro *Kerio WinRoute Firewall*
- <jazyk> je standardní dvoupísmenná zkratka jazyka (např. cs pro češtinu, sk pro slovenštinu, de pro němčinu atd.)

Poznámka: Pokud nainstalujeme administrační modul pouze pro jednu aplikaci, pak budou nainstalovány pouze definiční soubory jazyků pro *Administration Console* a pro tento modul.

Příklad: Nainstalujeme produkty *Kerio MailServer 6.0.5* a *Kerio WinRoute Firewall 6.1.5*. Pro češtinu budou nainstalovány definiční soubory kadmin.cs.qm, mailadmin600.cs.qm a wradmin601.cs.qm.

3.7 Nápověda (Windows)

V operačním systému *Windows* umožňuje *Administration Console* otevřít nápovědu ve formátu *HTML Help* (*.chm), a to jak pro hlavní okno *Administration Console* (volba *Nápověda / Obsah* v hlavním menu), tak pro jednotlivé administrační moduly (volba *Nápověda / Příručka administrátora* v hlavním menu).

Instalační balíky obsahují pouze nápovědu v anglickém jazyce; soubory s nápovědou v dalších jazycích lze stáhnout z WWW stránek <http://www.kerio.cz/>.

Umístění souborů s nápovědou je podrobně popsáno v kapitole 2. Soubory jsou pojmenovány podle tohoto schématu:

kadmin.<jazyk>.chm — nápověda pro hlavní okno *Administration Console*

mailadmin<XY>.<jazyk>.chm — příručka administrátora pro aplikaci *Kerio MailServer*

wradmin<VW>.<jazyk>.chm — příručka administrátora pro aplikaci *Kerio WinRoute Firewall*

kde:

- <XY> je hlavní (jednomístné) a vedlejší (dvojmístné) číslo verze administračního modulu pro *Kerio MailServer*
- <VW> je hlavní a vedlejší číslo verze administračního modulu pro *Kerio WinRoute Firewall*
- <jazyk> je dvoupísmenná zkratka jazyka (např. cs pro češtinu, sk pro slovenštinu, de pro němčinu atd.)

Administration Console (resp. administrační modul) vždy hledá nejprve soubor s nápovědou ve zvoleném jazyce uživatelského rozhraní (viz kapitola 3.6). Pokud jej nenalezne, pokusí se najít odpovídající nápovědu v angličtině. Nenažde-li ani anglickou verzi, pak nebude dostupná položka hlavního menu *Nápověda / Obsah* (v hlavním okně), resp. *Nápověda / Příručka administrátora* (v okně administračního modulu).

Poznámka: V operačních systémech *Linux* a *Mac OS X* není v současné době nápověda k dispozici. Hlavní menu *Administration Console*, resp. administračního okna, v těchto systémech neobsahuje výše uvedené položky. Jako nápovědu můžeme použít manuál ve formátu *HTML* nebo *PDF* — obsah manuálu/nápovědy je ve všech formátech shodný.

Přidání souboru s nápovědou

Příklad: Do *Administration Console* chceme přidat českou nápovědu a českou příručku administrátora pro aplikaci *Kerio WinRoute Firewall 6.1.x* (aktuální verzi zjistíme na úvodní obrazovce po přihlášení). Z WWW stránek

<http://www.kerio.cz/> stáhneme odpovídající manuály ve formátu *HTML Help* a uložíme je do podadresáře *help* (viz výše):

- nápovědu pro *Administration Console* pod názvem *kadmin.cs.chm*
- příručku administrátora pro *Kerio WinRoute Firewall* pod názvem *wadmin601.cs.chm*

Přidáváme-li novou nápovědu v době, kdy je *Administration Console* (případně některý administrační modul) spuštěna, platí následující pravidla:

- Nápověda pro *Administration Console* bude dostupná po příštím spuštění *Administration Console*, případně po změně jazyka (tj. přepnutí z jiného jazyka na jazyk, pro který byla nápověda přidána).
- Příručka administrátora pro konkrétní aplikaci bude dostupná po příštím přihlášení k této aplikaci (tj. po dalším spuštění příslušného administračního modulu).

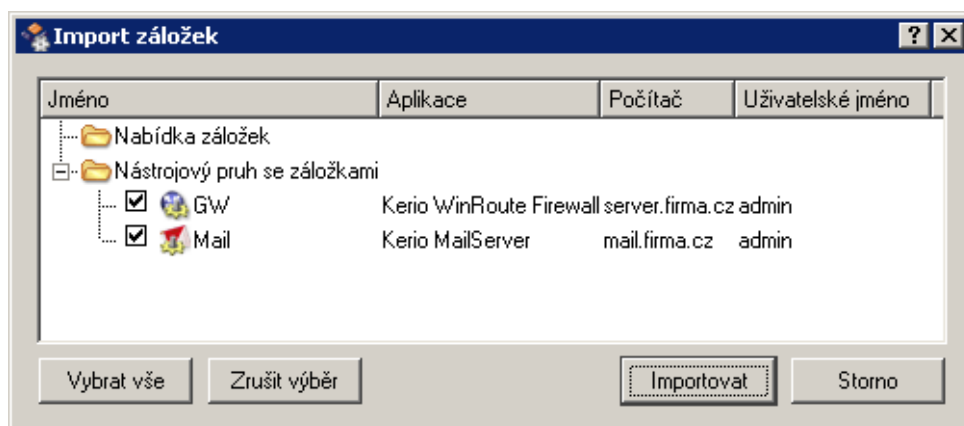
3.8 Import starých záložek

Starší verze *Kerio Administration Console* (1.x, dodávané se serverovými produkty řady 5.x) používaly jiný způsob uložení záložek. Současná verze *Administration Console* (2.x) nedokáže s těmito záložkami pracovat přímo, umožňuje však načtení odpovídajících přihlašovacích údajů a vytvoření nových záložek.

Načtení a konverzi záložek z předchozí verze lze provést volbou *Nástroje / Importovat staré záložky* z hlavního menu *Administration Console*.

Administration Console se nejprve pokusí nalézt soubor se starými záložkami (*_admin.bkm*) v domovském adresáři aktuálního uživatele. Je-li soubor nalezen, zkontroluje se, zda je šifrovan a chráněn heslem. Pokud ano, uživatel je vyzván k zadání tohoto hesla.

Po úspěšném načtení souboru se zobrazí dialog pro import záložek.



Obrázek 3.16 Import starých záložek

Seznam obsahuje všechny záložky, které byly ve starší verzi *Administration Console* definovány — jak v nabídce záložek, tak v nástrojovém pruhu. Označíme záložky, které chceme převést do nové verze, a stiskneme tlačítko *Importovat*. Je-li import záložek úspěšný, budou importované záložky přidány do seznamu v hlavním okně *Administration Console*.

Poznámka: K serveru definovanému importovanou záložkou se můžeme připojit pouze tehdy, pokud příslušná serverová aplikace byla aktualizována na verzi 6.x. Připojení ke starším verzím (5.x) není možné.

Kapitola 4

Síťová komunikace Administration Console

V této kapitole uvádíme stručný popis síťové komunikace mezi *Administration Console* a serverovou aplikací. Tyto informace jsou důležité zejména v případě, chceme-li provádět vzdálenou správu a v cestě je firewall, na kterém musíme povolit příslušnou komunikaci.

Při komunikaci se používá protokol TCP (přenos konfiguračních dat) a UDP (přenos asynchronních zpráv ze serveru do *Administration Console*). Každá serverová aplikace má přiřazeno jedno číslo portu pro připojení k administraci (dále jen „port aplikace“). Na tomto portu server čeká na příchozí TCP spojení a synchronizační UDP zprávu (viz dále).

Produkty firmy *Kerio Technologies* používají tyto porty:

- 44333 — *Kerio WinRoute Firewall*
- 44337 — *Kerio MailServer*

Průběh komunikace

Komunikace mezi *Administration Console* (dále jen „klient“) a serverovou aplikací (dále jen „server“) probíhá následovně:

1. Klient naváže TCP spojení (šifrovaný kanál) na server na příslušný port aplikace. Po úspěšném ověření získá od serveru tzv. identifikátor spojení.
2. Klient pošle serveru UDP zprávu s identifikátorem spojení na příslušný port aplikace.
3. Server si zapamatuje port, ze kterého klient zprávu s identifikátorem spojení odeslal. Na tento port bude pak klientovi zasílat asynchronní zprávy (např. nové položky do oken záznamů).
4. Po ukončení TCP spojení (odhlášením, ukončením klienta nebo serveru, z důvodu síťové chyby atd.) server i klient zruší příslušný identifikátor spojení. Případné další UDP zprávy s tímto portem klienta budou ignorovány.

Nastavení firewallu

Z výše uvedeného popisu komunikace vyplývá nastavení firewallu pro komunikaci mezi *Administration Console* a serverovou aplikací v těchto situacích:

1. Server za firewallem (tj. v chráněné lokální síti nebo přímo na počítači s firewallem), klient v Internetu

Na firewallu je třeba otevřít (mapovat) port příslušné aplikace (tj. 44333 nebo 44337) pro protokoly TCP a UDP.

2. Klient za firewallem, server v Internetu

Firewall musí být nastaven tak, aby povolil odchozí TCP spojení a UDP komunikaci na port příslušné aplikace.