

Kerio Connect

Krok za krokem

Kerio Technologies

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

Tento manuál popisuje produkt: *Kerio Connect* ve verzi 7.4. Změny vyhrazeny.

Aktuální verzi produktu a manuálů naleznete na WWW stránkách

<http://www.kerio.cz/cz/connect/download/>.

Informace o registrovaných ochranných známkách a ochranných známkách jsou uvedeny v příloze [A](#).

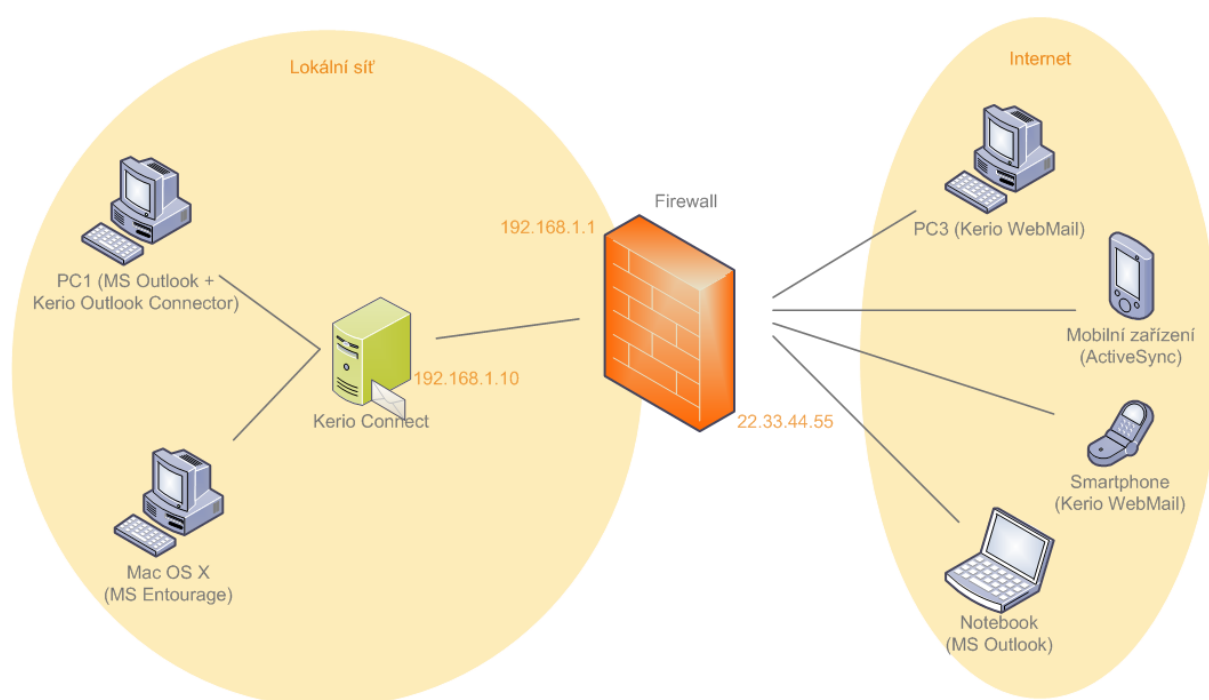
Obsah

1	Úvod	4
1.1	Dříve než začneme	5
2	Instalace	7
2.1	Windows	7
2.2	Mac OS X	7
2.3	Linux	8
2.4	Průvodce počáteční konfigurací	8
3	Nastavení serveru	10
3.1	Spuštění Kerio Connect	10
3.2	Rozhraní pro administraci	10
3.3	Nastavení domény a uživatelských účtů	11
3.4	Nastavení internetového připojení a SMTP serveru	12
3.5	Antispamová kontrola SMTP serveru	13
3.6	Antivirová kontrola zpráv	13
3.7	Zálohování pošty	14
3.8	Založení a správa zdrojů	15
3.9	Nastavení veřejných složek	15
4	Nastavení klientských aplikací a připojení ke Kerio WebMailu	18
4.1	Přihlášení ke Kerio WebMailu	18
4.2	Nastavení MS Outlooku	18
4.3	Nastavení MS Entourage	20
4.4	Nastavení synchronizace mobilních zařízení	20
A	Právní doložka	22

Kapitola 1

Úvod

Tato příručka slouží jako průvodce základní konfigurací aplikace *Kerio Connect* včetně instalace a spuštění v síti. Aby byl průvodce co nesrozumitelnější, vytvoříme modelové nasazení *Kerio Connect* (vizte obrázek [1.1](#)):



Obrázek 1.1 Schéma modelového nasazení Kerio Connect

1. *Kerio Connect* nainstalujeme na samostatný server (nebude provozovat žádné další služby) a spustíme jej v lokální síti chráněné firewallem.
2. *Kerio Connect* bude k Internetu připojen pomocí pevné linky. Poštu bude přijímat i doručovat přes protokol SMTP. Z tohoto důvodu bude nezbytné nastavit antivirovou a antispamovou kontrolu.
3. *Kerio Connect* bude obsluhovat jednu doménu nazvanou *firma.cz*. Server bude nainstalován a spuštěn v lokální síti na počítači s IP adresou 192.168.1.10 a DNS jménem *mail.firma.cz*.
4. V interní databázi uživatelů bude založen pouze jeden lokální účet určený pro správu *Kerio Connect*. Ostatní uživatelské účty budou mapovány z adresářové služby *Microsoft Active Directory* (analogicky lze postupovat i v případě *Apple Open Directory*).

Název *Active Directory* domény bude shodný s názvem poštovní domény a názvem Kerberos realm.

5. Server bude přístupný jak z lokální sítě, tak z Internetu. Spojení z Internetu ovšem bude z bezpečnostních důvodů umožněno pouze u služeb chráněných SSL/TLS šifrováním.
6. Veškerá nedoručitelná pošta (pošta, s nesprávně nastavenou částí e-mailové adresy umístěnou před znakem @) bude doručena na adresu `admin@firma.cz`.
7. Nastavíme duální antivirovou ochranu *Kerio Connect*. Použijeme integrovaný antivirus Sophos (je třeba mít k dispozici licenci *Kerio Connect* s *Sophos*) a externí antivirus *Clam AntiVirus*, který bude nainstalován na stejném počítači jako *Kerio Connect*.
8. Veškerá pošta bude jednou týdně zálohována, a také archivována do lokální archivační složky.
9. Do systému zadáme zdroje sdílené společností (firemní automobily, zasedací místnosti, promítačky a další), aby si je uživatelé mohli rezervovat.
10. Nastavíme veřejnou složku typu kalendář, kam budou zadávány celofiremní akce a důležitá data, která by měli znát všichni zaměstnanci společnosti. Práva pro přidávání nových událostí budou přidělena recepční společnosti. Dále nastavíme veřejnou složku typu kontakty, které budou moci využívat pouze členové obchodního oddělení a budou do této složky přidávat kontakty zákazníků společnosti.
11. Uživatelé budou pro přístup ke své poště používat *Kerio WebMail*, *Kerio Outlook Connector (Offline Edition)*, *MS Entourage* a pro přímý přístup ke schránce z mobilních zařízení budou používat některou z aplikací založených na protokolu ActiveSync.

Uvedenou modelovou konfiguraci lze snadno přizpůsobit konkrétním podmínkám a požadavkům. Podrobné informace o nastavení jednotlivých funkcí aplikace *Kerio Connect* lze najít v manuálu *Kerio Connect 7, Příručka administrátora* v kapitole [Příklady nastavení](#). Celý manuál si můžete stáhnout na stránkách společnosti *Kerio Technologies* (<http://www.kerio.cz/cz/connect/manual>).

1.1 Dříve než začneme

Než začneme s instalací a konfigurací, připravíme si následujícím způsobem prostředí:

Nastavení DNS MX záznamů

Kerio Connect je umístěn v privátní síti, ovšem přijímat a doručovat poštu bude i z/k Internetu. To znamená, že je třeba nastavit příslušný záznam ve veřejné DNS na veřejnou IP adresu přidělenou poskytovatelem (v tomto příkladu to bude adresa 215.75.128.33). V privátní síti jménu `mail.firma.cz` přiřadíme lokální IP adresu 192.168.1.10. Privátní adresu nastavíme na lokálním DNS serveru.

Záznam pro veřejný server může vypadat například takto:

firma.cz	MX	10	mail.firma.cz
mail.firma.cz	A		215.75.128.33

Máte-li k dispozici také záložní poštovní server, přidejte záznam i pro něj.

Nastavení firewallu

Kerio Connect je nainstalován v lokální síti chráněné firewallem. Kromě vlastní konfigurace poštovního serveru tedy musíme provést doplňující nastavení firewallu.

Má-li být poštovní server přístupný z Internetu, je třeba ve firewallu otevřít (tzv. mapovat) některé porty. Každý mapovaný port znamená potenciální problém se zabezpečením. Namapujeme tedy porty jen pro služby, které chceme zpřístupnit z Internetu.

V případě naší modelové sítě bude nezbytně nutné namapovat port 25, což je standardní port pro službu SMTP. Toto nastavení je potřebné vždy, když je na server nasměrován MX záznam pro danou doménu. Na port SMTP serveru se může legálně připojit libovolný SMTP server v Internetu, chce-li odeslat e-mail do některé z jeho domén. Z tohoto důvodu nesmí být na mapovaný port 25 omezen přístup dle IP adres.

Dále bude třeba namapovat porty, na které se budou připojovat uživatelé mimo lokální síť. Protože se zde zvyšuje bezpečnostní riziko, budeme mapovat pouze služby zabezpečené SSL/TLS šifrováním. Nastavení znázorňuje tabulka [1.1](#).

Služba (standardní port)	Odchozí spojení	Příchozí spojení
SMTP (25)	povolit	povolit
SMTPS (465)	povolit	povolit
POP3 (110)	povolit	zakázat
POP3S (995)	povolit	povolit
IMAP (143)	povolit	zakázat
IMAPS (993)	povolit	povolit
NNTP (119)	povolit	zakázat
NNTPS (563)	povolit	povolit
LDAP (389)	povolit	zakázat
LDAPS (636)	povolit	povolit
HTTP (80)	povolit	zakázat
HTTPS (443)	povolit	povolit

Tabulka 1.1 Služby, které je třeba povolit na firewallu

Kapitola 2

Instalace

Kerio Connect lze nainstalovat a provozovat na třech typech operačních systémů. Vybrat si můžeme ze systémů Windows, Mac OS X nebo Linux.

Seznam verzí (případně distribucí) těchto operačních systémů, na které je možné *Kerio Connect* nainstalovat, najdeme na stránkách společnosti [Kerio Technologies](#).

Na každý operační systém je třeba nainstalovat speciální instalační balík (v případě Linuxu jsou to balíky dva). Všechny typy instalačních balíků lze získat na stránce (<http://www.kerio.cz/cz/connect/download>).

Máme-li stažený správný instalační balík, můžeme začít s instalací. Instalace se liší podle typu operačního systému:

2.1 Windows

Po stažení balíku instalaci spustíme pod uživatelem, který má nastavena administrační práva k systému.

Instalace proběhne pomocí standardního instalačního průvodce. *Kerio Connect* se typicky nainstaluje do následujícího adresáře:

```
C:\Program Files\Kerio\Mailserver
```

Po instalaci se automaticky otevře průvodce počáteční konfigurací (vizte sekci [2.4](#)).

2.2 Mac OS X

Po stažení balíku instalaci spustíme pod uživatelem, který má nastavena administrační práva k systému (instalační program bude vyžadovat ověření). Instalační balík se otevře v aplikaci *Finder* jako disk a nabídne spustitelný instalační soubor.

Instalace probíhá pomocí standardního instalačního průvodce, kde vybereme volbu *Easy Install*, která provede kompletní instalaci produktu do adresáře `/usr/local/kerio/mailserver`.

Po instalaci se automaticky otevře průvodce počáteční konfigurací (vizte sekci [2.4](#)).

2.3 Linux

Instalaci je třeba provádět s právy superuživatele (root). *Kerio Connect Engine* se instaluje do adresáře `/opt/kerio/mailserver`.

Instalaci RPM balíčku provedeme příkazem:

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

U novějších verzí distribucí se při instalaci mohou vyskytnout problémy se závislostmi balíčku. V tomto případě nainstalujte balíček `compat-libstdc++`

Instalaci DEB balíčku provedeme příkazem:

```
# dpkg -i <název_instalačního_souboru.deb>
```

Bezprostředně po instalaci doporučujeme důkladně pročíst LINUX-README soubor, který najdete v adresáři:

```
/opt/kerio/mailserver/doc
```

2.4 Průvodce počáteční konfigurací

Průvodce počáteční konfigurací je shodný na všech třech operačních systémech, proto si průběh popíšeme pro všechny platformy společně.

Konfigurační průvodce se na platformách Windows a Mac OS X otevře automaticky po instalaci aplikace *Kerio Connect*. Pouze na Linuxu je třeba jej explicitně spustit pomocí příkazu:

```
./cfgwizard pro RPM
```

```
dpkg-reconfigure kerio-connect pro DEB
```

Příkaz spusťte z adresáře, kam byl *Kerio Connect* nainstalován (typicky `/opt/kerio/mailserver`).

Upozornění: Po dobu, kdy je spuštěn konfigurační průvodce, nesmí být spuštěn *Kerio Connect Engine*.

V konfiguračním průvodci nastavíme následující parametry:

1. V prvním dialogu založíme poštovní doménu (jednoznačný identifikátor, podle kterého lze poznat, na jaký server má být pošta doručena. U e-mailových adres se doménová část vyskytuje vždy za znakem @) a doplníme internetové jméno serveru. Internetové jméno serveru je DNS název počítače, na který jste *Kerio Connect* nainstalovali. Jméno serveru se používá pro identifikaci serveru při navazování SMTP komunikace.

Upozornění: Je-li *Kerio Connect* umístěn za NAT, je nutné jako internetové jméno serveru doplnit jméno, které je možné zpětně převést na IP adresu odesílajícího serveru, tj. internetové jméno firewallu.

2. V dalším kroku průvodce vytvoříme administrátorský účet. Jméno *Admin* ponecháme a doplníme heslo. Jméno a heslo zadané do tohoto dialogu později použijeme pro přihlášení

k administračnímu rozhraní aplikace *Kerio Connect*, proto je třeba si přihlašovací údaje dobře zapamatovat.

3. Další krok průvodce umožňuje nastavení umístění datového adresáře. V tomto adresáři budou umístěny všechny uživatelské schránky a záznamy (logy) serveru.
4. V posledním kroku průvodce následuje pouze oznámení o právě nastavených parametrech. Po jeho ukončení se zobrazí oznámení o úspěšnosti instalace.

Kapitola 3

Nastavení serveru

3.1 Spuštění Kerio Connect

Kerio Connect se po instalaci spustí automaticky na systémech Windows a Mac OS X. Na Linuxu je třeba spustit server ručně.

Spouštění/zastavování se liší podle operačního systému, kde je *Kerio Connect* nainstalován:

Windows

Kerio Connect spustíme nebo zastavíme pomocí ikonky, která se po instalaci objevila v oznamovací oblasti v nástrojové liště.

Pokud na ikonku klikneme pravým tlačítkem, otevře se kontextové menu. Volbou *Start/Stop Kerio Connect* můžeme server zastavit nebo spustit.

Linux

Kerio Connect lze zastavit, spustit nebo restartovat pomocí následujících příkazů:

```
sudo /etc/init.d/kerio-connect start
```

```
sudo /etc/init.d/kerio-connect stop
```

```
sudo /etc/init.d/kerio-connect restart
```

Mac OS X

Na systémech Mac OS X můžeme *Kerio Connect* zastavit nebo spustit pomocí *Kerio Connect Monitoru* (jeho ikonu pro spuštění najdeme v *System Preferences* v sekci *Other*). Pro zastavení nebo spuštění služby je nutné zadat uživatelské jméno (musí být součástí skupiny Admins) a heslo. Poté stačí použít tlačítko *Stop* (pro zastavení služby) nebo *Start* (pro spuštění služby).

3.2 Rozhraní pro administraci

Ke konfiguraci *Kerio Connect* slouží webové rozhraní *Kerio Connect Administration*. *Kerio Connect Administration* používá pouze zabezpečený protokol HTTPS a běží na portu 4040.

Pro přístup k tomuto rozhraní stačí zadat do prohlížeče URL ve tvaru `http://DNS.nazev.serveru/admin` (`http://IP.adresa/admin`, není-li jméno ještě zaneseno v DNS) a *Kerio Connect* se automaticky přesměruje na `https://DNS.nazev.serveru:4040/admin` (`https://IP.adresa:4040/admin`).

URL tedy může vypadat například takto:

```
https://mail.firma.cz:4040/admin nebo https://192.168.1.1:4040/admin).
```

Je-li URL zadáno správně, zobrazí se v prohlížeči přihlašovací stránka, kde je třeba doplnit jméno a heslo primárního administrátora, které jste doplnili do konfiguračního průvodce.

Při prvním přihlášení se nejprve zobrazí dialog pro registraci produktu. Registrovat lze nejen plnou verzi produktu, ale také trial verzi — registrací trial verze vzniká nárok na bezplatnou technickou podporu. Tento nárok trvá po celou dobu platnosti trial verze.

3.3 Nastavení domény a uživatelských účtů

Nastavení poštovních domén se provádí v sekci *Konfigurace* → *Domény*. Sekce již obsahuje doménu, kterou jsme založili v konfiguračním průvodci.

Mapování uživatelských účtů a skupin z adresářové služby

1. Na doménový server nainstalujeme aplikaci *Kerio Active Directory Extension*, která je volně k dispozici na stránkách společnosti *Kerio Technologies*. Tato aplikace slouží k rozšíření adresářové služby o některé položky *Kerio Connect*.
2. V administračním rozhraní *Kerio Connect* otevřeme sekci *Konfigurace* → *Domény*. Doménu, kterou jsme založili při instalaci, otevřeme tlačítkem *Změnit*.
3. Přepneme se do záložky *Adresářová služba* a doplníme údaje doménového serveru. Mapování aktivujeme volbou *Mapovat uživatelské účty a skupiny z adresářové služby do této domény*. Jako typ adresářové služby zvolíme *Active Directory*. Do položky *Jméno počítače* doplníme DNS název nebo IP adresu doménového serveru. Do položky *Uživatelské jméno* je třeba zadat takové uživatelské jméno, které má nastavena práva pro čtení a zápis do LDAP databáze v *Active Directory*.
Tlačítkem *Test připojení* vyzkoušíme, zda jsme všechny parametry nastavili správně tak, aby se *Kerio Connect* mohl připojit k doménovému řadiči *Active Directory*.
4. Přepneme se do záložky *Upřesnění*. V této záložce musí být v položce *Kerberos 5* doplněn *Kerberos realm*. Název se automaticky zapíše velkými písmeny.

Po nastavení mapování se přepneme do sekce *Účty* → *Uživatelé*. Seznam uživatelů bude zobrazovat všechny namapované uživatele a jeden lokální účet pro administraci *Kerio Connect*.

Podobně jako uživatelé se namapují také uživatelské skupiny. Ty se zobrazí v sekci *Účty* → *Skupiny*.

Nastavení aliasu pro nedoručitelnou poštu

Definici aliasu provedeme v sekci *Účty* → *Alias*:

1. Klikneme na tlačítko *Přidat*.
2. Otevře se dialog pro přidání nového aliasu. Do položky *Alias* doplníme znak ***. Do položky *E-mailová adresa* napíšeme adresu uživatelské schránky, do které má být veškerá nedoručitelná pošta směrována (v našem případě je to *admin@firma.cz*).
3. Po uložení aliasu můžeme také vyzkoušet jeho funkci tlačítkem *Zkontrolovat adresu* umístěným v sekci *Alias* vpravo dole pod seznamem aliasů.

Alias pro nedoručitelnou poštu (nebo také hvězdičkový alias) se použije tehdy, pokud část e-mailové adresy umístěné před znakem @ nenalezne shodu s žádným uživatelským jménem ani aliasem v dané doméně.

3.4 Nastavení internetového připojení a SMTP serveru

Na SMTP server se může připojit kdokoliv, aby poslal zprávu do některé z lokálních domén. Odesílání zpráv do jiných domén omezíme pouze na uživatele v lokální síti. Pro uživatele připojené z Internetu nastavíme povinnost ověřit se na SMTP serveru uživatelským jménem a heslem. K tomuto nastavení slouží záložka *Řízení přístupu* v sekci *Konfigurace* → *SMTP server*:

1. V záložce zaškrtneme možnost *Odesílat poštu mimo lokální domény smějí pouze*:

Upozornění: Důrazně doporučujeme nepřepínat SMTP server do režimu Open Relay, pokud je *Kerio Connect* dostupný z Internetu (tzn. má veřejnou IP adresu a port 25 není blokován firewallem). Pokud režim Open Relay nastavíte, bude *Kerio Connect* pravděpodobně zneužit spammery k rozesílání nevyžádané pošty, čímž zahltí vaši internetovou linku. Může se také dostat do veřejných blacklistů SMTP serverů.

2. Zaškrtneme položku *Uživatelé z této skupiny IP adres* a vybereme skupinu *Local Clients*, do které jsou zahrnuty všechny privátní rozsahy IP adres.
3. Zaškrtneme položku *Uživatelé ověření na SMTP serveru*, aby mohli poštu odesílat i uživatelé připojení z Internetu.

Poznámka:

Ověřování na SMTP serveru je třeba nastavit v poštovním klientovi. Nastavení některých běžných klientů popisuje sekce [4.2](#).

Dále pro SMTP server nastavíme některá bezpečnostní omezení v záložce *Bezpečnostní volby*:

1. *Max. počet zpráv za hodinu z jedné IP adresy* nastavte na 100 zpráv.
2. *Max. počet současných připojení k SMTP serveru z jedné IP adresy* nastavte na 20.
3. *Max. počet neznámých příjemců* nastavte na 10.
4. V položce *Tato omezení neplatí pro tuto skupinu IP adres* nastavte skupinu IP adres s lokálními uživateli aplikace *Kerio Connect*, aby se na ně výše nastavená pravidla nevztahovala. Pokud ve vaší vnitřní síti používáte privátní IP adresy, stačí vybrat výchozí skupinu *Local Clients*, která je definována všemi rozsahy privátních IP adres.

Podrobnosti nastavení bezpečnosti SMTP serveru najdeme v kapitole [SMTP server](#) v manuálu *Kerio Connect 7, Příručka administrátora*.

3.5 Antispamová kontrola SMTP serveru

SMTP server je přístupný z Internetu, a proto je nezbytně nutné nakonfigurovat antispamovou kontrolu SMTP serveru. Antispamové filtry lze nastavit v sekci *Konfigurace* → *Filtrování obsahu* → *Filtr spamu*:

1. Ke spuštění a nastavení hodnocení antispamovými filtry slouží záložka *Hodnocení spamu*. Nastavení této záložky můžeme nechat ve výchozím stavu.
2. V záložce *Zakázání odesílatelů* doporučujeme zapnout kontrolu pomocí internetových databází spammerů a nastavit každé databázi spamové skóre +2 body.
3. Přepneme se do záložky *SpamAssassin* a zaškrtneme volbu *Kontrolovat každou příchozí zprávu v databázi Spam URI Realtime Blocklist (SURBL)*.
4. V záložkách *Caller ID* a *SPF* nastavíme kontrolu e-mail policy záznamů odesílajícího SMTP serveru a nastavíme spamové skóre na +2 body. Tato kontrola umožňuje odfiltrování zpráv s podvrženou adresou odesílatele.
5. V záložce *Odrásování spammerů* zapneme zpoždění při navazování SMTP komunikace (ponecháme přednastavených 25 vteřin). Tento filtr velmi účinně odmítá spam již na úrovni SMTP komunikace a server tudíž není tolik zatěžován prováděním dalších spamových testů.

Antispamové filtry SMTP serveru podrobně popisuje manuál *Kerio Connect 7, Příručka administrátora* v kapitole [Antispamová kontrola SMTP serveru](#).

3.6 Antivirová kontrola zpráv

Dalším nezbytným nastavením aplikace *Kerio Connect* je spuštění antivirové kontroly a filtrování příloh, které můžeme provést v následujících sekcích:

Antivirus

Kerio Connect umožňuje zvolit různé konfigurace antivirové ochrany. *Kerio Connect* lze zakoupit s integrovaným antivirem *Sophos* nebo bez něho. Mimo to *Kerio Connect* podporuje řadu dalších externích antivirů (aktuální podporované antiviry jsou uvedeny na stránkách společnosti [Kerio Technologies](#)). Takže můžeme využívat buď integrovaný *Sophos* antivirus, nebo některý z podporovaných externích antivirů. Nejbezpečnější variantou je duálně zkombinovat ochranu pomocí *Sophos* a externího antiviru. Jak bylo řečeno v úvodní kapitole [1](#), popíšeme si zde variantu aplikace *Kerio Connect* s integrovaným antivirem *Sophos* a přidaným externím antivirem *Clam AntiVirus*.

Nastavení serveru

Ke spuštění antivirové kontroly slouží sekce *Konfigurace* → *Filtrování obsahu* → *Antivirus*:

1. Zkontrolujeme, zda je spuštěna volba *Použít integrovaný antivirový modul Sophos*.
2. Na počítač s aplikací *Kerio Connect* nainstalujeme externí antivirus *Clam AntiVirus*.
3. V sekci *Konfigurace* → *Filtrování obsahu* → *Antivirus* zaškrtneme volbu *Použít externí antivirový program* a v menu vybereme *Clam AntiVirus*.

Filtrování příloh

Filtrování příloh nastavíme v sekci *Konfigurace* → *Filtrování obsahu* → *Filtrování příloh*, kde zaškrtneme volbu *Povolit filtrování příloh*.

V seznamu typů příloh můžeme navíc vybrat/odebrat další přílohy, které chceme odfiltrovat, nebo pomocí tlačítka *Přidat* doplnit typy příloh, které seznam neobsahuje.

3.7 Zálohování pošty

Zálohování pošty a archivaci zpráv nastavíme v sekci *Konfigurace* → *Zálohování*.

Archivace všech zpráv

Archivaci zpráv nastavíme v záložce *Archivace*:

1. Archivaci aktivujeme volbou *Povolit archivaci pošty*.
2. Cestu k adresáři pro archivaci ponecháme ve výchozím nastavení.
3. Zaškrtneme volbu *Archivovat do lokální složky*.
4. Interval vytváření složek nastavíme na jeden týden.

Archivační složky budou zobrazeny jako součást poštovní schránky Administrátora *Kerio Connect*. Zobrazit je bude možné například v rozhraní *Kerio WebMail*.

Zálohování datového adresáře a konfiguračních souborů

Zálohování nastavíme v záložce *Zálohování*:

1. Zálohování aktivujeme volbou *Povolit zálohování datového adresáře a konfigurační serveru*.
2. V tabulce *Plán zálohování* nastavíme jednu plnou zálohu na nedělní půlnoc, aby provádění zálohy nezatěžovalo server v pracovní době.

3. Do pole *Adresář pro zálohu* nastavíme cestu k adresáři, do kterého se budou zálohy ukládat. Cestu je třeba zadat v takovém tvaru, aby vyhovoval konvenci operačního systému, na kterém je *Kerio Connect* spuštěn.
4. Do pole *E-mailová adresa* doplníme svou adresu. *Kerio Connect* bude automaticky generovat výsledek každé zálohy a odešle je na zadanou adresu.

3.8 Založení a správa zdrojů

Kerio Connect umožňuje rezervaci zdrojů (automobilů, místností a dalšího zařízení). Aby byla rezervace možná, musí mít každý zdroj vlastní kalendář. Z toho důvodu je nutné všechny zdroje zadat do *Kerio Connect* v administračním rozhraní v sekci *Účty* → *Zdroje*:

1. Klikneme na tlačítko *Přidat*.
2. Do dialogu v záložce *Obecné* doplníme název zdroje. Název bude sloužit jako část e-mailové adresy před zavináčem. Z toho důvodu není dovoleno, aby název obsahoval diakritiku, mezery a speciální znaky.
3. V položce *Typ* vybereme, zda jde o místnost či zařízení.
4. Přepneme se do záložky *Oprávnění* a přidáme ke zdroji všechny uživatele, kteří mají nárok jej rezervovat.
5. Nastavíme správce rezervací. Správcem rezervací zdrojů je uživatel, kterému je umožněno zasahovat do kalendáře zdrojů. Rezervace může v případě potřeby mazat nebo přesouvat na jinou dobu.

Po založení zdroje zkontrolujeme v poštovním klientovi nebo *Kerio WebMailu* zdali:

- se při plánování schůzky zobrazí jeho free/busy kalendář,
- si kalendář zdroje můžeme přihlásit standardním sdílením,
- se ve veřejných složkách zobrazila složka *Zdroje*, která obsahuje kontakty všech založených zdrojů, aby je uživatelé mohli snadno zadávat při plánování schůzek.

Rezervaci zdrojů podrobně popisují manuály [Kerio Connect 7, Příručka administrátora](#) i [Kerio Connect 7, Příručka uživatele](#)

3.9 Nastavení veřejných složek

Kerio Connect podporuje veřejné složky. Této možnosti využijeme a vytvoříme veřejný firemní kalendář nazvaný *Akce* a veřejnou složku *Zákazníci* s kontakty firemních zákazníků, kterou však uvidí a bude ji moci editovat pouze obchodní oddělení vaší společnosti.

Poznámky:

- Veřejná složka je speciální složka, která se po svém vytvoření zobrazí ve schránkách všem uživatelům z domény s právy pro čtení (přístupová práva lze samozřejmě upravit).
- Veřejné složky může vytvářet a spravovat pouze uživatel se speciálními přístupovými právy. Po instalaci *Kerio Connect* je má přidělena pouze primární administrátor.

Veřejný kalendář

1. Přihlaste se do rozhraní *Kerio WebMail* jako primární administrátor aplikace *Kerio Connect* (použijte jméno a heslo zadané v konfiguračním průvodci při instalaci serveru).
2. Ve stromu složek klikněte pravým tlačítkem myši na uzel *Veřejné složky*.
3. V kontextovém menu klikněte na *Nová podsložka* a zadejte jméno kalendáře *Akce* a typ nové veřejné složky *Kalendář*.
4. Klikněte na nově vytvořenou složku pravým tlačítkem myši a v kontextovém menu zvolte *Přístupová práva*.
5. Standardně mají všichni uživatelé z domény práva pro čtení. Toto nastavení ponechte a klikněte na tlačítko *Přidat*.
6. V menu *Typ sdílení* ponechte volbu *Uživatel* a do pole *Uživatelské jméno* přidejte e-mailovou adresu správce kalendáře (v našem případě adresu recepční). Klikněte na tlačítko *OK*.
7. V tabulce práv vybranému uživateli přidejte typ oprávnění *Správa*.

Adresář zákazníků

1. V administračním rozhraní *Kerio Connect* se přepněte do složky *Účty* → *Skupiny* a založte skupinu OBCHOD, jejímiž členy budou všichni z obchodního oddělení vaší společnosti.
2. Přihlaste se do rozhraní *Kerio WebMail* jako primární administrátor *Kerio Connect* (použijte jméno a heslo zadané v konfiguračním průvodci při instalaci serveru).
3. Ve stromu složek klikněte pravým tlačítkem myši na uzel *Veřejné složky*.
4. V kontextovém menu klikněte na *Nová podsložka* a zadejte jméno kalendáře *Zákazníci* a typ nové veřejné složky *Kontakty*.
5. Klikněte na nově vytvořenou složku pravým tlačítkem myši a v kontextovém menu zvolte *Přístupová práva*.

6. Standardně mají všichni uživatelé z domény práva pro čtení. Toto nastavení zrušte a klikněte na tlačítko *Přidat*.
7. V menu *Typ sdílení* vyberte volbu *Skupina* a do pole *Jméno skupiny* přidejte e-mailovou adresu skupiny OBCHOD. Klikněte na tlačítko *OK*.
8. V tabulce práv skupině přidejte typ oprávnění *Úpravy* (členové skupiny budou moci kontakty do složky přidávat, mazat i upravovat).

Nastavení klientských aplikací a připojení ke Kerio WebMailu

Uživatelé se k serveru budou připojovat buď přes rozhraní *Kerio WebMail*, nebo využijí některý z podporovaných klientů *MS Outlook* (na systémech Windows) nebo *MS Entourage* (na systémech Mac OS X). Následující sekce obsahují návody, jak se přihlásit ke *Kerio WebMailu*, a jak optimálně nastavit poštovní klienty.

4.1 Přihlášení ke Kerio WebMailu

Pro přístup ke službě HTTP je třeba do WWW prohlížeče jako URL zadat adresu počítače, na němž je *Kerio Connect* spuštěn, nebo jeho jméno, je-li zaneseno v DNS. V URL musí být rovněž specifikován protokol, a to buď HTTP pro nezabezpečený přístup, nebo HTTPS pro přístup zabezpečený SSL. URL tedy bude mít tvar `http://mail.firma.cz` nebo `https://mail.firma.cz`.

Při přístupu odjinud než z lokální sítě je doporučeno používat bezpečný protokol HTTPS (při použití protokolu HTTP lze velmi snadno odposlechnout a zneužít přihlašovací údaje uživatele). Při výchozím nastavení jsou spuštěny služby *HTTP* a *HTTPS* na standardních portech (80 a 443). Budou-li tyto porty změněny, je třeba při přístupu k dané službě uvést v URL také port, tedy `http://mail.firma.cz:8000` nebo `https://mail.firma.cz:8080`.

Poznámka:

Pro přístup k poště přes PDA zařízení platí předchozí popis. Pokud se PDA zařízení nemůže ke *Kerio Connect* připojit, pravděpodobně neumí rozpoznat, že se musí spustit verze *Kerio WebMail Mini* (zkouší se připojit k plné verzi). V tomto případě stačí zadat URL v následujícím tvaru: `https://mail.firma.cz/pda`.

Je-li URL zadáno správně, zobrazí se v prohlížeči přihlašovací stránka, kde je třeba doplnit uživatelské jméno a heslo. Ke schránce se připojíme tlačítkem *Přihlásit*.

4.2 Nastavení MS Outlooku

Kerio (MAPI) účet — Kerio Outlook Connector (Offline Edition)

Instalaci a konfiguraci účtu provedeme následovně:

1. Na klientskou stanici nainstalujeme *MS Outlook* (aktuálně podporované verze najdete na stránkách společnosti [Kerio Technologies](#)).
2. Na tutéž stanici nainstalujeme *Kerio Outlook Connector (Offline Edition)*.

3. Přihlásíme se do *Kerio WebMailu* (vizte sekci [4.1](#)) a v menu *Nastavení* vybereme položku *Integrace s Windows*.
4. Na stránce použijte odkaz *Klikněte zde pro automatickou konfiguraci doplňku Kerio Outlook Connector*.
5. Podle typu prohlížeče, který jste použili, se nástroj stáhne a automaticky spustí, nebo pouze stáhne a spustíte ji poklikáním na ikonu nástroje.
6. Skript spustí *MS Outlook*, vytvoří nový profil a přednastaví váš Kerio účet.
7. Do účtu je třeba z bezpečnostních důvodů doplnit pouze heslo k vaší uživatelské schránce. Po doplnění hesla je konfigurace *MS Outlooku* dokončena.

POP3 a IMAP účet

Nastavení IMAP nebo POP3 účtu v *MS Outlooku* vypadá takto:

1. V průběhu vytváření profilu v *MS Outlooku* nastavíme příslušný POP3 nebo IMAP účet.
2. V průvodci nastavením nového účtu vybereme buď možnost POP3 nebo IMAP podle typu účtu, který chceme nastavit.
3. Pečlivě vyplníme krok průvodce *Nastavení e-mailu síť Internet*. Do položky *Jméno* zadáme jméno a příjmení uživatele a do položky *E-mailová adresa* doplníme adresu uživatele. Do položky *Uživatelské jméno* zadáme uživatelské jméno. V případě, že uživatel nemá účet založen v primární doméně, potom je třeba uživatelské jméno zapsat včetně domény, tedy ve tvaru `uzivatelske_jmeno@firma.cz`. Do položky *Heslo* zadáme heslo pro přihlášení ke *Kerio Connect*. Nakonec do položek *Server příchozí pošty* a *Server pro odchozí poštu* doplníme DNS jméno nebo IP adresu serveru, kde je spuštěn *Kerio Connect*.
4. Pokud se uživatel připojuje z Internetu, je třeba vzhledem k nastavení SMTP serveru (vizte sekci [3.4](#)) nastavit ověřování. Klikneme na tlačítko *Další nastavení*. Otevře se dialog s několika záložkami, kde lze nastavit další parametry účtu. Přepneme se do záložky *Server pro odchozí poštu*, zaškrtneme volbu *Server pro odchozí poštu (SMTP) požaduje ověření* a zvolíme *Použít stejná nastavení jako pro server příchozí pošty*.
5. Spustíme *MS Outlook* v novém profilu.

Poznámka:

Tento návod lze využít i pro nastavení libovolného jiného poštovního klienta, který podporuje protokoly IMAP a POP3.

4.3 Nastavení MS Entourage

Kerio Connect využívá rozhraní pro *MS Exchange* v *MS Entourage* a díky tomu umožňuje práci s groupwarovými daty (pošta, kalendář, kontakty a veřejné poštovní složky), využívání *Free/Busy* serveru, připojení různých LDAP databází pro vyhledávání kontaktů, atd. Nastavení účtu je následující:

1. Nainstalujeme *MS Entourage* a spustíme ho.

Poznámka:

Aktuálně podporované verze *MS Entourage* najdeme na stránkách společnosti [Kerio Technologies](#).

2. Přihlásíme se do *Kerio WebMailu* (vizte sekci [4.1](#)) a v menu *Nastavení* vybereme položku *Integrace s Mac OS X*.
3. Klikneme na odkaz *Nastavit Entourage automaticky*.
4. Nástroj se stáhne na stanici a automaticky se spustí.
5. Během instalace je třeba zadat uživatelské jméno a heslo účtu, který má nastaven práva k administraci našeho počítače.
6. Po dokončení instalace se otevře se dialog *MS Entourage* pro zadání hesla k naší poštovní schránce. Zadáme jej a potvrdíme.
7. Po dokončení průvodce je konfigurace *MS Entourage* kompletní.

4.4 Nastavení synchronizace mobilních zařízení

Kerio Connect umožňuje přímou synchronizaci dat s mobilními zařízeními přes protokol ActiveSync (aktuálně podporovaná zařízení najdete na stránkách společnosti [Kerio Technologies](#)). Pomocí tohoto protokolu lze synchronizovat poštu, události, kontakty a úkoly. Implementace ActiveSync aplikací v jednotlivých mobilních zařízeních se může lišit, avšak každé zařízení obsahuje nastavení ActiveSync účtu, kam je třeba zadat v různém pořadí následující údaje, aby bylo možné se k poštovním serveru připojit:

1. Je třeba zadat internetové jméno serveru (DNS) nebo IP adresu, kde je poštovní server spuštěn.
2. Uživatel musí znát své uživatelské jméno a heslo k poštovní schránce v *Kerio Connect* serveru.
3. Nastavení účtu vyžaduje zadání poštovní domény, ve které je uživatel na serveru založen.
4. Pokud vaše bezpečnostní politika vyžaduje SSL komunikaci, je třeba do zařízení importovat SSL certifikát ověřený buď důvěryhodnou certifikační autoritou nebo alespoň

certifikát podepsaný sám sebou, který lze vytvořit přímo v *Kerio Connect*. Certifikát do zařízení nainstalujete snadno takto:

- a. Do prohlížeče v mobilním zařízení zadejte adresu, kde je spuštěn *Kerio Connect* (tamtáž adresa, kterou používáme pro připojení k rozhraní *Kerio WebMail* — sekce [4.1](#)).
- b. Na přihlašovací stránce *Kerio WebMailu* najdete přímo pod přihlašovacím dialogem odkaz *Nainstalovat SSL certifikát*.

Nelze tímto způsobem certifikát nainstalovat, pokuste se instalaci provést pomocí návodu v manuálu [Kerio Connect 7, Příručka administrátora](#)

Příloha A

Právní doložka

Microsoft[®], Windows[®], Windows NT[®], Windows Vista[®], Internet Explorer[®], Active Directory[®], Outlook[®], ActiveSync[®] a Windows Mobile[®] jsou registrované ochranné známky společnosti Microsoft Corporation.

Apple[®], Mac OS[®], Tiger[™], Panther[®], Leopard[®] a Snow Leopard[®] jsou registrované ochranné známky nebo ochranné známky společnosti Apple Inc.

Linux[®] je ochranná registrovaná známka Linuse Torvaldse.

Kerberos[™] je ochranná známka Massachusetts Institute of Technology (MIT).