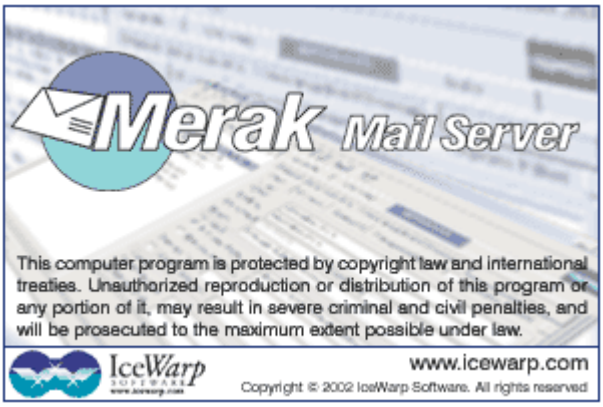


IceWarp Merak Mail Server (CZ)

www.icewarp.cz – poslední aktualizace 5. Dubna 2002

Obsah

Copyright Upozornění

Licenční ujednání

Výrobce produktu zaručuje, že je výhradním majitelem dodaného produktu a všech autorských práv s produktem spojených, a že je ze zákona oprávněn poskytnout licenci bez souhlasu třetí straně.

Předmětem licenčního ujednání je výhradně licence na použití programového díla – programu.

Uživatel se stává majítelem licence nem zakoupění a přestává být majitelem licence v tom případě, že písemnou formou požádá o zrušení licence, nebo v případě vypršení platnosti licence (platí u 30ti denní zkušební verze)

Zakoupením jedné instalace produktu Merak Mail server, či IceWarp webmail získává uživatel právo na jeho instalaci a použití na jednom počítači.

Uživatel je srozumněn se skutečností, že držitelem věškerých autorských práv spojených s produktem Merak Mail server, či IceWarp Webmail je výrobce programu – společnosti IceWarp software.

Uživatel je srozumněn se skutečnosti, že Merak Mail server je během instalace ozačen referenčním klíčem a je podle tohoto klíče jednoznačně identifikovatelný.

Uživatel se zavazuje používat Merak Mail server, či IceWarp webmail tak, aby nedošlo k porušení či ohrožení autorských práv výrobce.

Uživatel smí pořizovat archivní kopie programu popř. instalačních medií pouze pro potřeby archivace a vytvoření záložních kopií.

Uživatel nesmí poskytnout Merak Mail server, či IceWarp webmail třetí straně bezplatně ani za úplatu.

Uživatel nesmí provádět žádné změny v Merak Mail serveru, IceWarp webmailu ani v doprovodných souborech, či programech vyjma takových změn, které jsou prováděny obslužnými programy dodanými s instalací produktu.

Přehled

Merak je plně vybavený, kompletně zabezpečený a standardizovaný e-mailový server pro Windows. Může být použit vedoucími společnostmi stejně, jako malými firmami.

Merak v plném rozsahu podporuje protokoly SMTP/POP3/IMAP4/HTTP (všechny tyto protokoly mohou být zabezpečeny pomocí SSL), může být spravován přes zabezpečené webové spojení, obsahuje funkční obsahové filtry, statické routování, mailing listy, má integrované antivirové jádro, obsahuje ochranu proti spamu a anti relayingové funkce.

Jednoduše řečeno Merak Mail server je kompletní e-mailový systém, který poskytuje všechno, co potřebuje firma ke spravování své e-mailové komunikace a který umožňuje spolupracovat s řadou kompatibilních produktů.

Důležitou funkcí je zabezpečené přenášení informací. Merak automaticky pozná, jestli je server, se kterým komunikuje schopný pracovat se zabezpečným spojením TLS/SSL a pokud ano, automaticky naváže spojení pomocí této technologie.

Merak Mail Server Professional

Merak Mail server Professional je (jak už název napovídá) professionální verze mailového serveru. Nabízí podporu pro více něž milion účtů (e-mailových schránek) a je dodáván současně s produktem IceWarp webmail (IceWarp webmail je plně vybavený interface, umožňující uživatelům Vašeho e-mailového serveru psát a číst poštu odkudkoliv ze světa). Profesionální verze je rychlejší, než standardní a má větší hardwarové nároky. Můžete u ní také nastavit spolupráci s databází pomocí ODBC.

Kontaktujte nás

Pokud byste nečemu nerozuměli, potřebovali jste znát aktuální cenu, či byste měli zájem zakoupit produkt. Můžete nás kontaktovat:

E-Mail info@icewarp.cz
Podpora podpora@icewarp.cz
Website http://www.icewarp.cz/
Tel +420 777 600 351

1. Než začneme

Požadavky

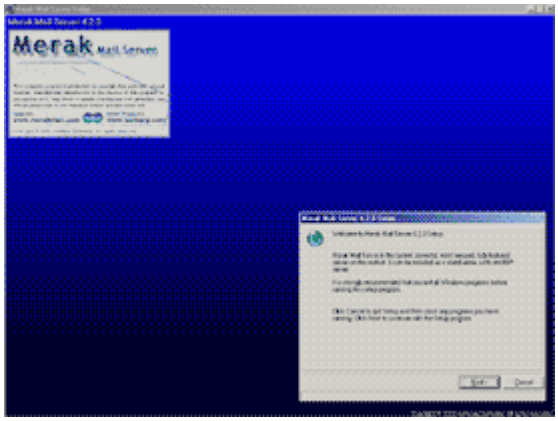
Pokud chcete mít nainstalovaný Merak, musíte mít počítač vyhovující následujícím požadavkům:

- Musíte mít nainstalovaný operační systém Windows 2000, XP, NT, 9x, ME (všechny verze)
- Síť podporující TCP/IP

Instalace

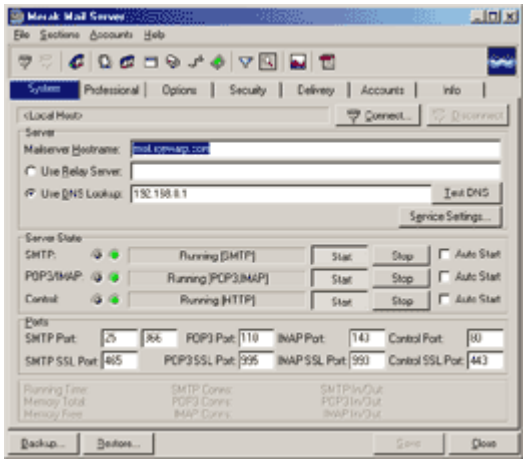
Software je dodáván jako ZIP archiv. Pro rozbalení a následnou instalaci budete potřebovat program Winzip. Ten naleznete například na adrese http://www.winzip.com

Pokud používáte jednu z nedávno vydaných verzí programu Winzip, budete moci použít instalační tlačítko na liště. Pokud ne, rozbalte instalační soubory do nějakého dočasného adresáře (**např. c:\temp\merak**) a z tohoto dočasného adresáře spusťte instalační program.



Prosím přečtěte si licenční ujednání.
Pokud je třeba, změnte instalační adresář.

K instalaci softwaru použijte tlačítko "install". Merak Mail server je hned po instalaci připraven k použití. Dočasný adresář již nebudete déle potřebovat a můžete ho smazat. Pokud používáte automatický instalátor, program WinZip to udělá za vás.



Pro kontrolu výsledku instalace spusťte konfigurační applet Meraka. Ten najdete nainstalovaný v ovládacích panelech Windows.

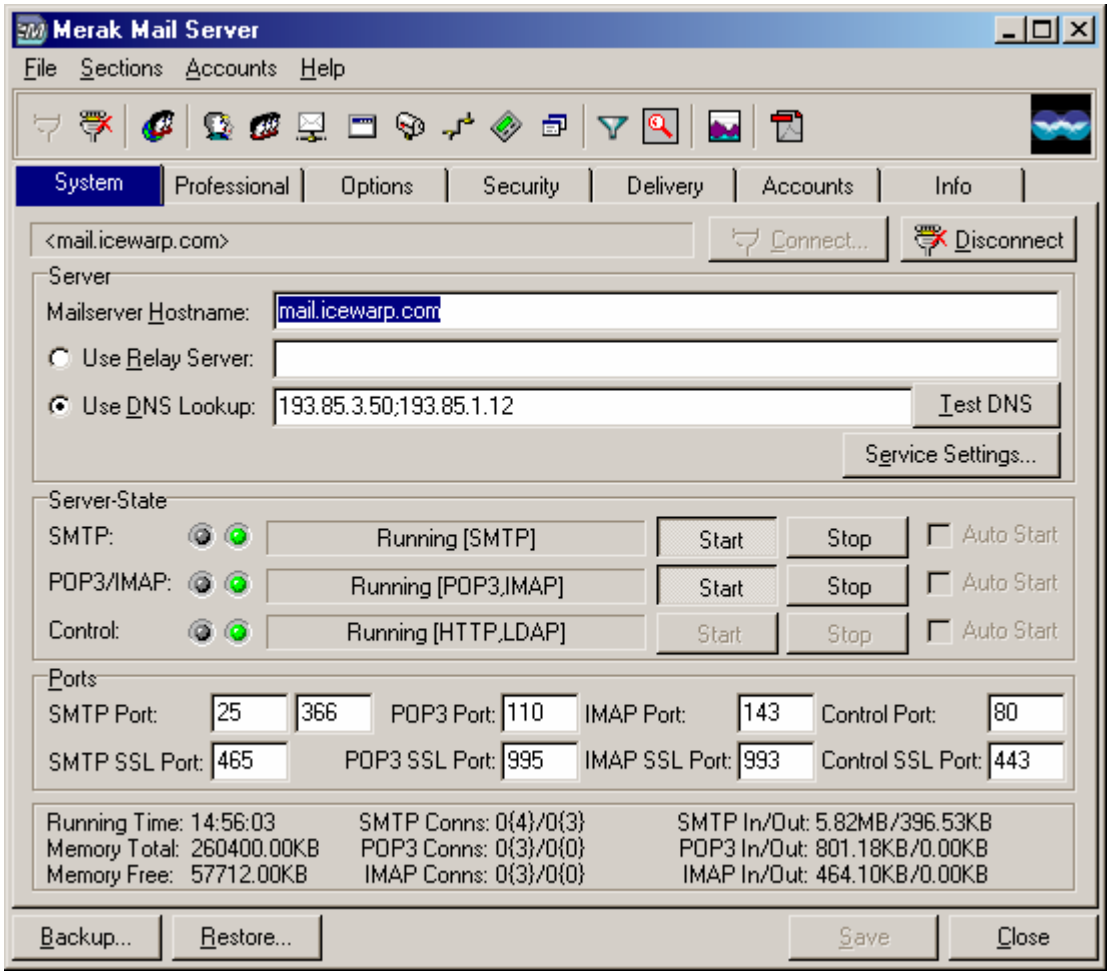
Zkontrolujte, zda jsou v provozu všechny tři služby provozované programem Merak Mail server (SMTP, POP3 a „Control“). Pokud u všech služeb svítí zelená kontrolka, znamená to, že služba je spuštěna . Pokud ne znamená to, že Merak Mail server je pravděpodobně v konfliktu s jinou aplikací, poskytující na vašem serveru v reálném čase stejnou službu, jako Merak. Typickým problémem je spuštěný Microsoft SMTP server - ten je většinou nainstalován spolu s IIS - jeho služby zastavte.

Když všechny kontrolky svítí zeleně, můžete pokračovat.

2. Konfigurace

Základní nastavení

V následujících krocích budete nastavovat základní konfiguraci mail serveru. Většina z následujících nastavení se provádí pouze jednou. Jako první krok tedy spusťte konfigurační applet Meraka.



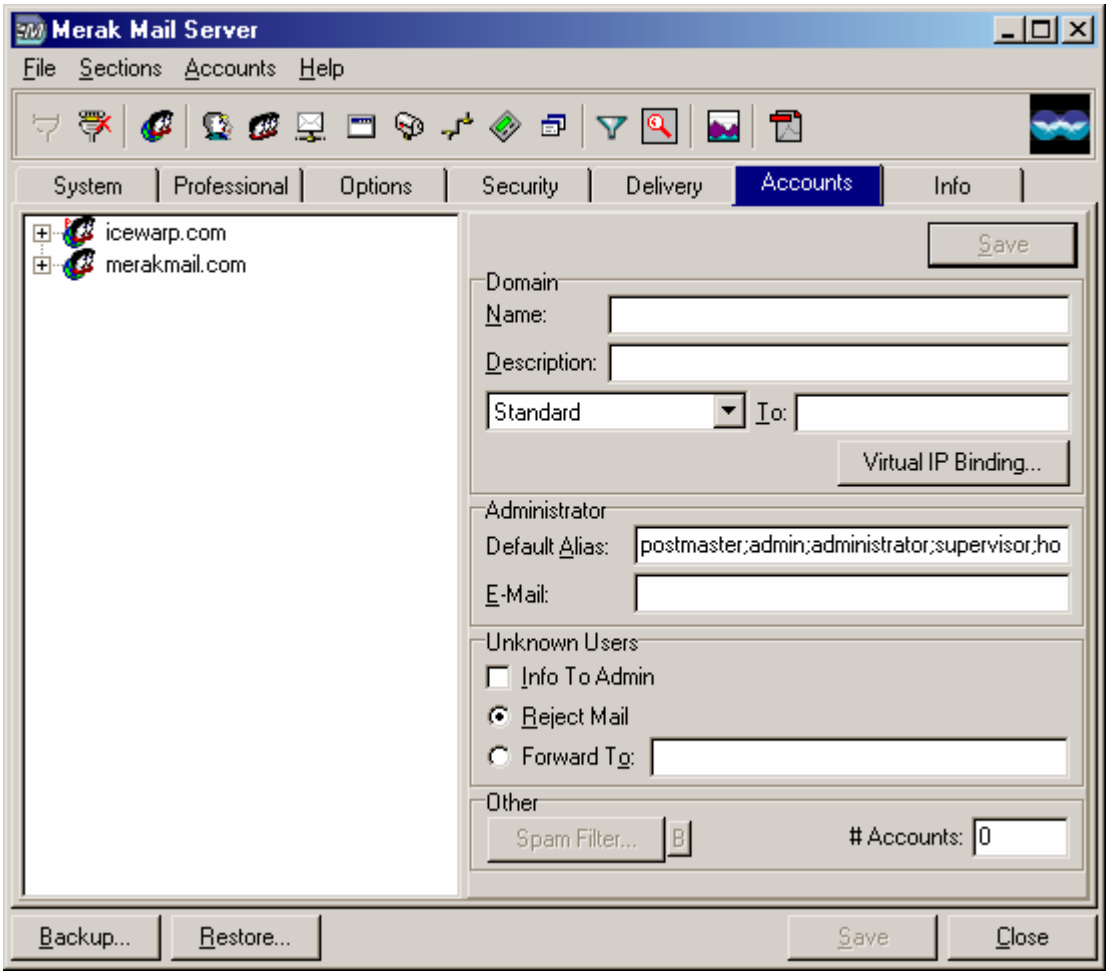
1. Musíte změnit host adresu mail serveru z původního nastavení mail.domain.com na vámi používanou adresu. Zde můžete použít jakékoliv jméno, ale tuto položku nesmíte nechat nevyplněnou. Právě toto je jméno, pod kterým bude server pracovat. Většinou je jméno mail server nastavováno jako mail.vašedoména.cz

2. Použijte funkci pro testování DNS. Jestliže nastavení nefunguje, zadejte do pole „DNS“ host, nebo přímo IP adresu nejméně jednoho z vámi používaných DNS serverů. Ujistěte se, že jste si dobře přečetli dodatek o nastavení DNS v tomto manuálu. Pokud si nebudete jisti nastavením vašich DNS serverů, můžete použít standardní nastavení. Pokud zadáte chybné parametry, nebude mail server správně pracovat.

Dalším krokem je vytvoření uživatelských účtů. V tomto případě budeme předpokládat, že námi nastavovaný mail server je určen pro provoz v doméně icewarp.com. Jako první budeme chtít vytvořit standardní účet pro doménu icewarp.com. Ze všeho nejdříve musíme ale nadefinovat

základní nastavení samotné domény.

K tomu použijeme záložku “accounts”:



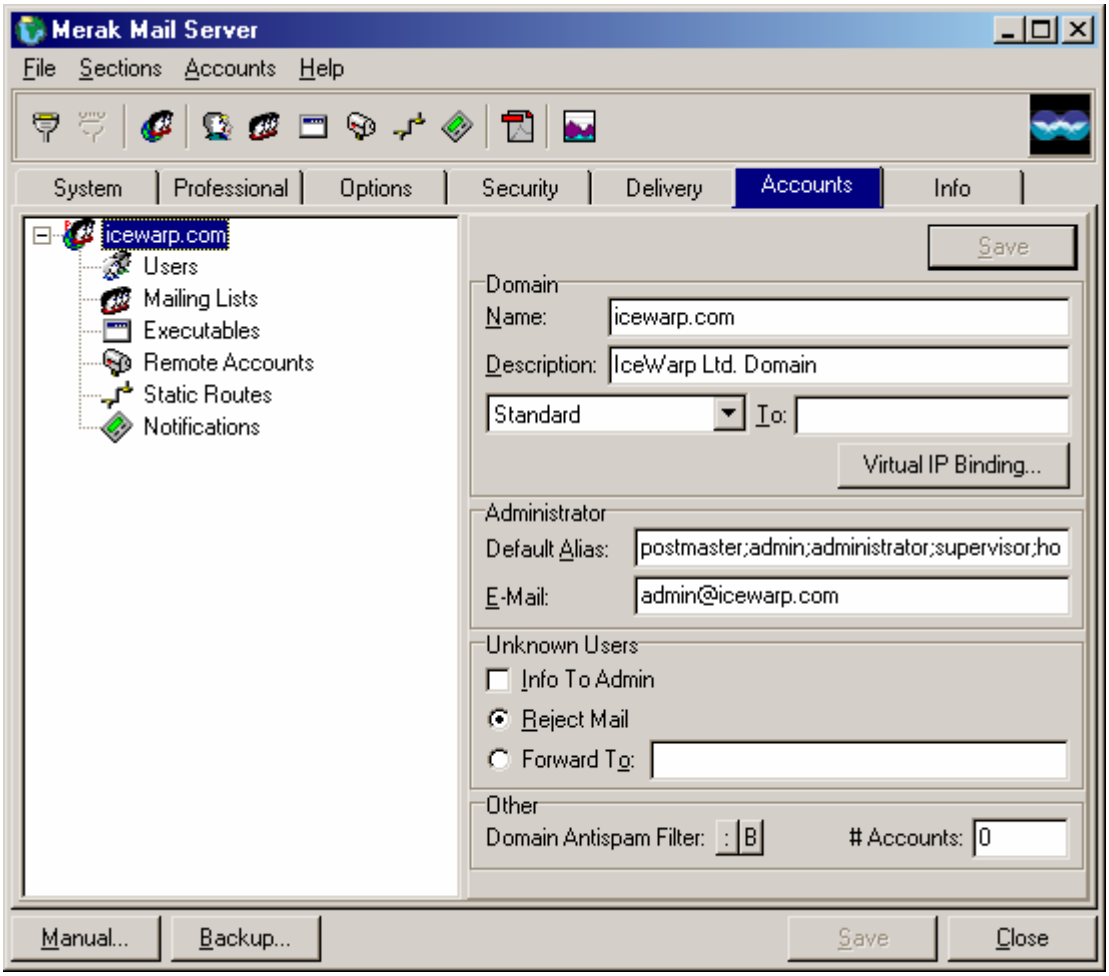
3. Do položky „name“ zadajte jméno samotné domény. V našem případě tedy icewarp.com

4. Do položky „description“ si můžete pro tuto doménu zvolit libovolný popis

5. Do položky „e-mail“ nastavujeme výchozí E-mail pro aliasi postmaster, admin, administrator, supervisor a hostmaster. Doporučený **alias je admin.** Tato emailová adresa může být externí a může být používána jako běžná emailová adresa pro administrátora, který spravuje více domén. Pokud je tomu tak, nezapomeňte tento účet vytvořit.

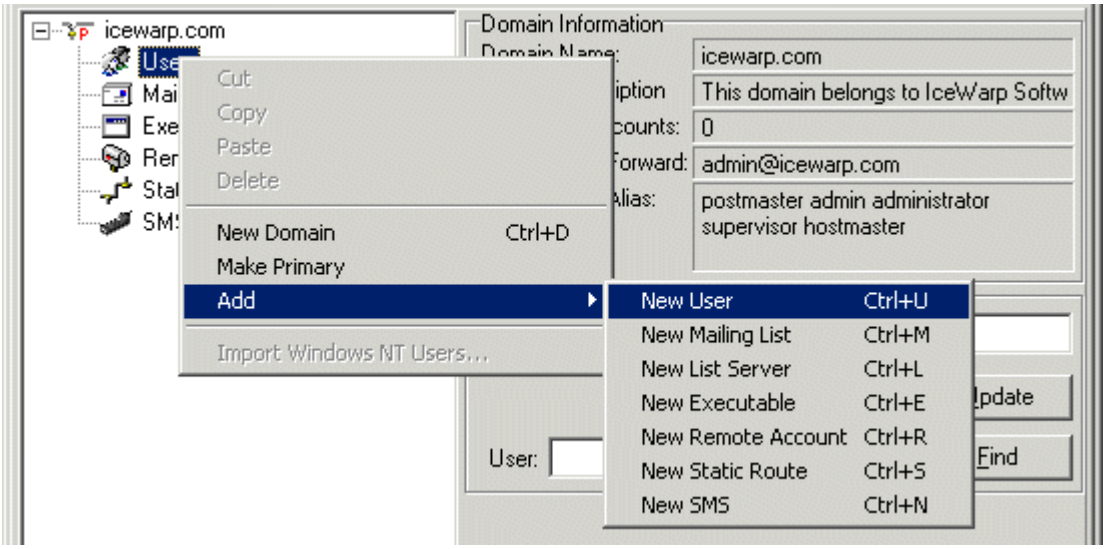
6. Klikněte na tlačítko “Save” (Uložit)

Pokud jste doménu IceWarp.com nastavili správně, bude záložka „Accounts“ nyní vypadat asi takhle:



Nyní potřebujeme do systému přidat uživatele „admin“. Na něho nás bude odkazovat námi před chvílí nastavená E-mailová adresa správce domény. V této fázi můžeme zároveň přidat i ostatní uživatele.

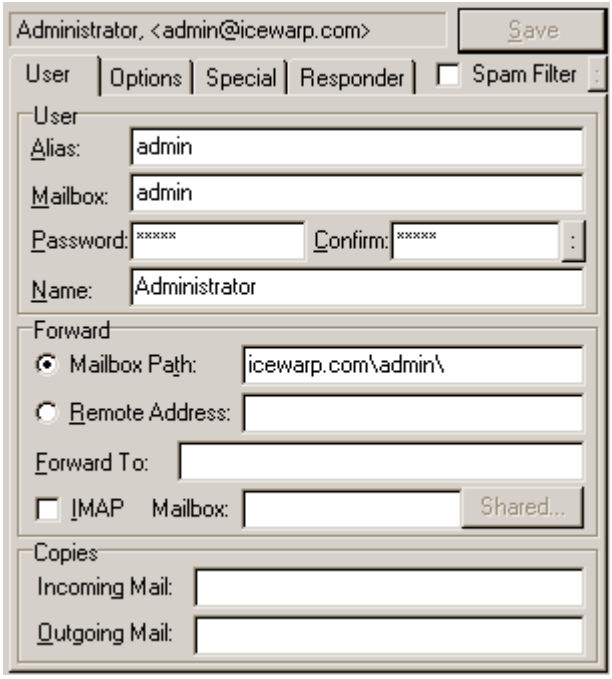
7. Klikněte pravým tlačítkem na větev „Users“, jděte na položku „Add“ a potom na položku „New User“.



8. Do poloožky Alias zadejte admin, čímž se stejnou hodnotou vyplní i pole mailbox.
9. Zadejte heslo a potvrďte jej do pole Confirm.
10. Do položky name si můžete vyplnit libovolný popis účtu.

11. To je dostatek informací, pro uspokojení základních požadavků programu. Nyní klikněte na tlačítko „save“ pro uložení nastavení účtu.

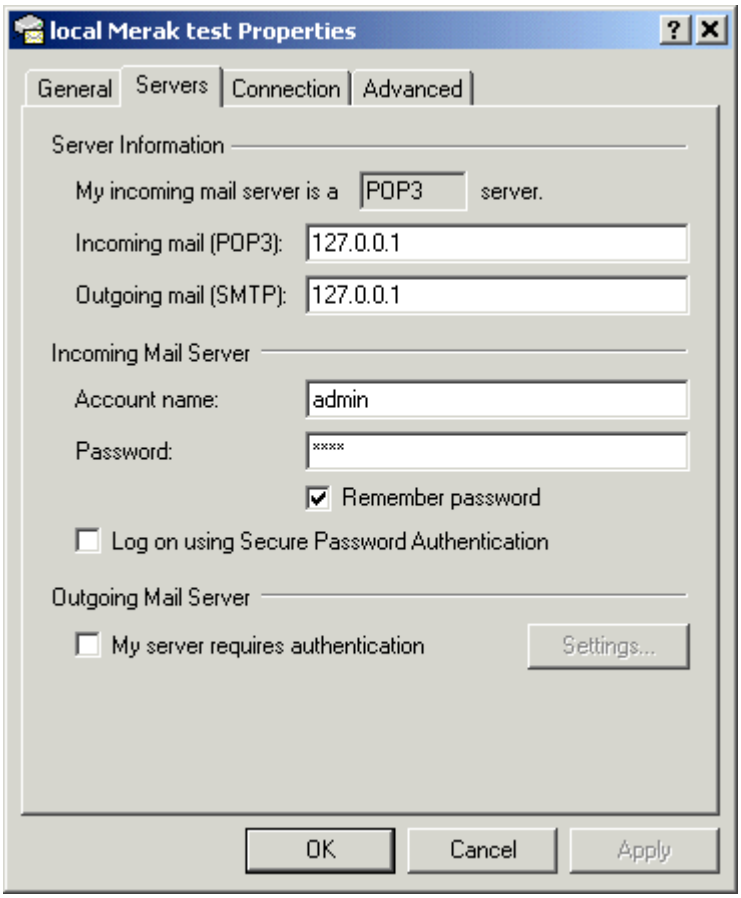
12. Musíte si být jisti, že Váš server není “open relay”. Pokud by totiž byl open relay, může přes něj kdokoliv nepovolaný odesílat zprávy. Otestovat můžete server pomocí stránky http://www.abuse.net/relay.html. Jednoduše zadejte IP adresu serveru.



Na řadě je nyní test, který se provede mimo mail server. Budete potřebovat nastavit nový účet ve vašem emailovém klientu.

Typ účtu je POP3.

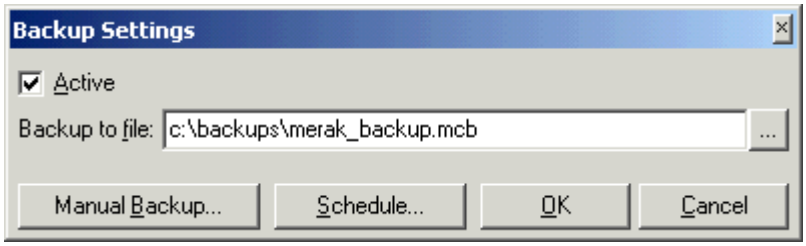
Do příchozího a odchozího mail serveru nastavíme adresu počítače, na kterém běží Merak. IP adresa 127.0.0.1 je vždy používána jako místní IP adresa počítače. Uživatelské jméno a heslo je stejné, jako jsme vyplňovali výše. E-mailový program má nyní dostatek informací potřebných k používání námi vytvořeného E-mailového účtu. Zkuste poslat E-mail na adresu admin@icewarp.com! **(Obrazovka je původní nastavovací dialog programu Outlook 2000 - ostatní emailové programy budou mít nastavování odlyšné)**



3. Hlavní část dokumentace

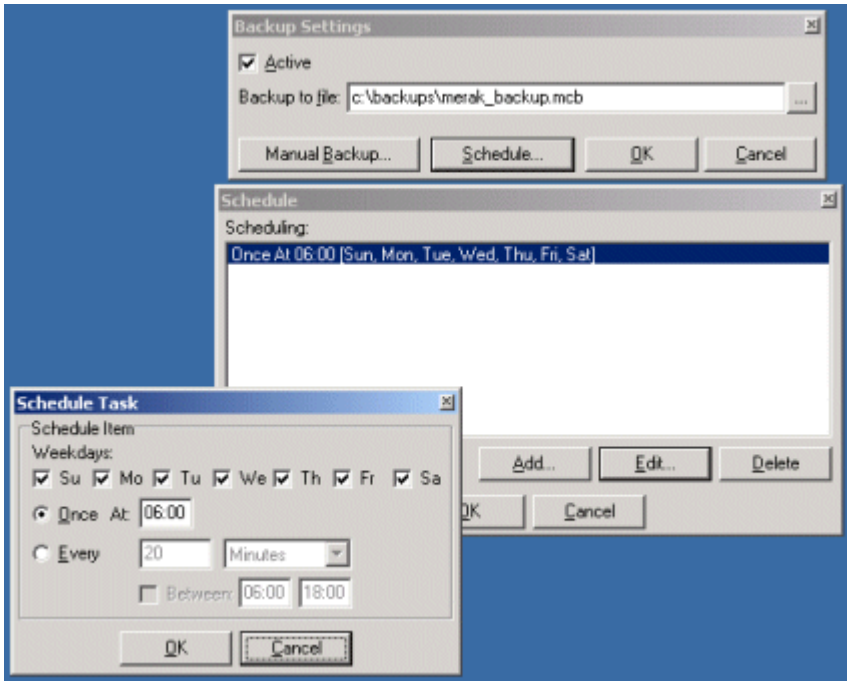
Záloha a obnovení konfigurace

Pod menu “File” umístěným na horní liště je umístěna funkce “back up”, umožnující zálohování vaší konfigurace. Ta konkrétně zahrnuje zálohu nastavení domén, informací o uživatelských účtech, váš licenční klíč a obsah celého konfiguračního adresáře. Doporučujeme provést tuto zálohu až po konečné fázi konfigurace a to včetně vašich licenčních informací.



Po zvolení nabídky Backup Settings se zobrazí toto dialogové okno. Funkce „Active“ a „Backup to file“ budou důležité pouze v případě, že bude nastavené plánované zálohování.

Klikněte na nabídku „Manual Backup“, pak si zvolte jméno souboru, do kterého se uloží veškeré konfigurační informace. Doporučujeme, uložit tento soubor na nějaké bezpečné místo (např. na výměnné médium) a udržovat mimo server.



Raději než na pravidelné zálohování pamatovat, je lepší nastavit plánované zálohování přímo v Meraku. V dialogu „Backup Settings“ zaškrtněte funkci „Active“, zadejte požadované umístění a

jméno souboru, pak použijte tlačítko „Schedule“. Pomocí tlačítka „Add“ přidejte, nebo editujte již existující rozvrh zálohování.

Merak vám nabídne kompletní plánovací záznamník. Zálohy se budou provádět v daný čas, v časových intervalech v dané dny týdne, nebo mezi dvěma zadanými časy

Obnovení konfigurace

Zvolením funkce „Restore“, (ta se nachází pod nabídkou „File“ stejně jako funkce Backup), budete vyzváni k zadání cesty k souboru obsahujícímu zálohované informace. Otevřete jeden vámi zvolený soubor a z něho obnovíte původní zazálohovanou informaci. Při použití této funkce buďte velice opatrní, aby nedošlo k přepsání starší verzí konfigurace.

Můžete tedy server v klidu přestavět, čerstvě nainstalovat všechny programy, ale o vaše konfigurační data nepřijdete. Zálohovaní poskytuje výbornou cestu ke znovu získání veškerých informací o uživatelských účtech, aniž by bylo potřeba je znovu ručně zadávat.

Z vašeho zálohovacícho souboru bude obnoven i licencnční klíč k Meraku. Proto je docela dobrý nápad provést zálohu celého systému, jakmile bude produkt zaregistrován.

Rady ohledně konfigurace

Každý zákazník má na produkt odlyšné požadavky. Jako tvůrci produktu vám naslouchámе a pravidelně náš produkt vylepšujeme. Navštěvujte časteji naše webové stránky a zkontrulte si uvěřejněná vylepšení produktu, nebo navrhněte své vlastní. Výsledkem toho je Merak Mail server jeden z nejvíce konfigurovatelných a nejsilnějších e-mailových řešení na trhu.

Jakkoliv vzroste hladina obtížnosti konfigurace, vzroste také složitost a tím potřebná uživatelská znalost dané problematiky.

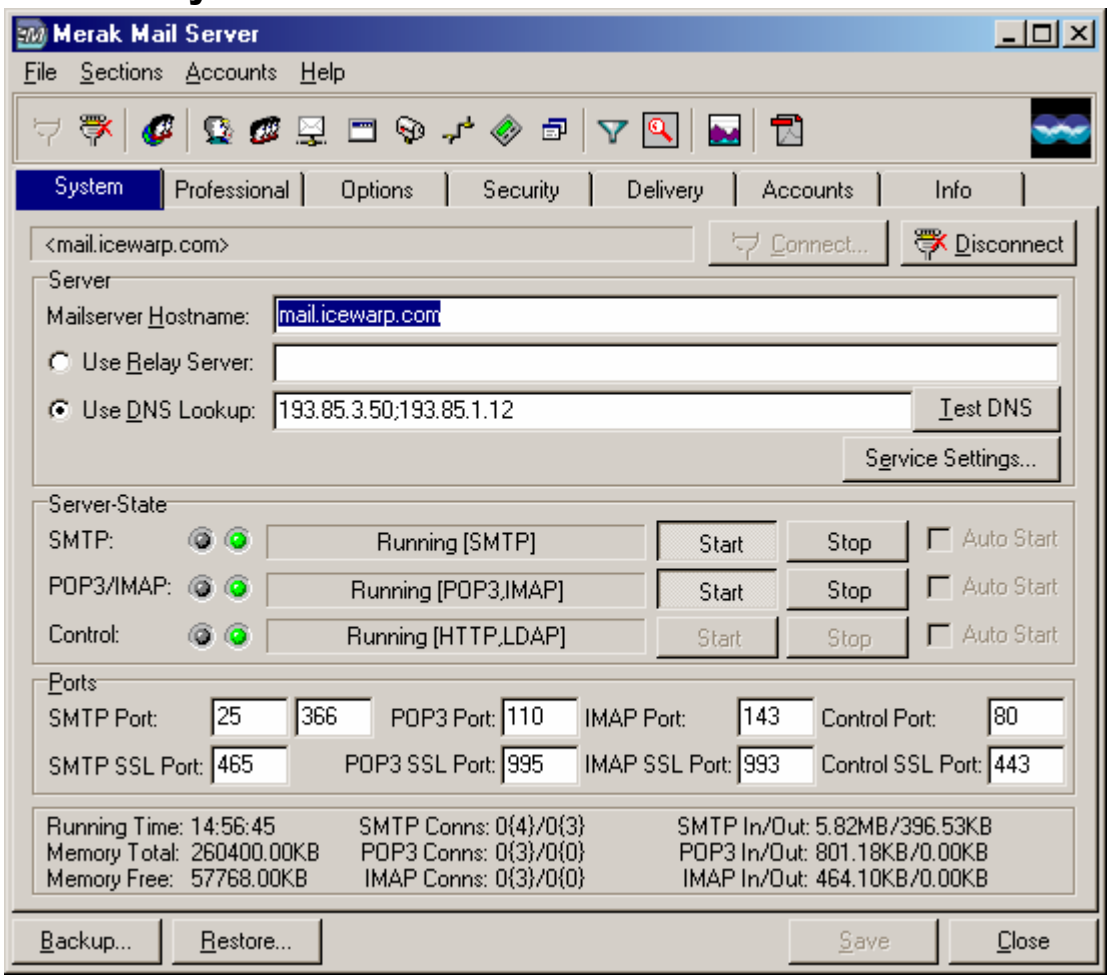
Když se rozhodnete používat Merak, musíte znát své požadavky a musíte vědet, zda právě Merak těmto požadavkům vyhovuje. Nejčastější problém, se kterým jsme se doposud setkali, nastává, když zákazníci zapnou všechny úrovně zabezpečení, udělají nějakou chybu v konfiguraci a v konečném výsledku není mail server schopen odesílat a přijímat e-maily.

Pamatuj!

- Nastavovat pouze to, co je skutečně třeba!
- Je důležité přečíst si dokumentaci a tím porozumět tomu, co nastavuji
- Pravidelně zálohovat konfiguraci
- Změny v konfiguraci dělat jednu po druhé aby bylo možné zjisti přesne to, co jste nastavoval
- Testovat Meraka po každé byť sebemenší změně v konfiguraci. Je nutné si také zamapatovat všechy provedené změny, aby bylo možné vrátit program do původního nastavení.

Řiďte se těmito pravidly a nebudete mít žádné problémy.

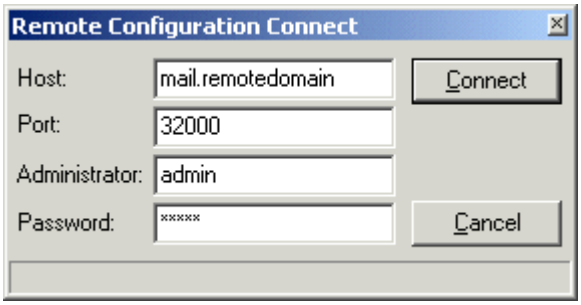
Tabulka System



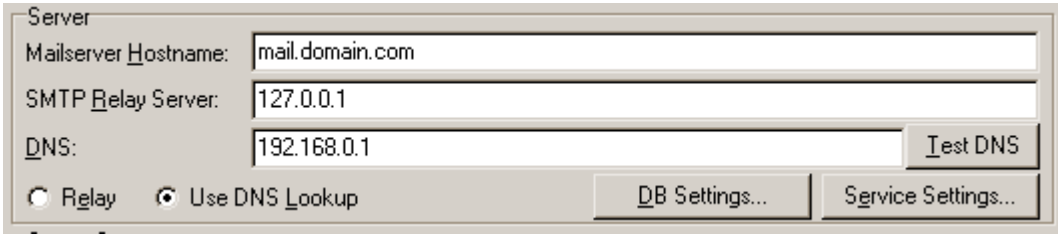
Toto je první tabulka konfiguračního apletu. Ukazuje nám přehled toho, co se v systému děje stějne jako výpis ze základního nastavení.

Panel umístěný v dolní části obrazovky nám ukazuje, co dělá Merak v reálném čase. Právě probíhající připojení a přenesená data do omažiku otevření nabídky.

Standardně se kontrolní panel appletu připojuje na lokální instalaci Meraka. Pokud chcete použít applet pro připojení na vzdálený Merak Mail server, použijte tlačítko connect, pak zadáte host adresu cílového počítače, port na kterém běží administrace samotného Meraka, administrátorské jméno a heslo



Jako administrátorský účet může fungovat jakýkoliv účet, který má administrátorská práva.
Tabulka systém (pole nastavení serveru)



Pole	Popis
Mailserver Hostname	Toto pole specifikuje jméno mail serveru. Tato položka nesmí být prázdná. Mail server pomocí svého jména prokazuje sám sebe ostatním mail serverům. Typickým nastavením host adresy u mail serveru bývá mail.[vašedoména.cz]. Jméno mail serveru by mělo být stejné, jako jméno, které bylo registrované na vašem DNS serveru.
SMTP Relay Server	Jestliže tento server neposílá emaily přímo do internetu (chovají se tak např. emailové servery, které jsou připojené přes DialUp připojení na internet a předávají své emaily Mail serveru svého internetového poskytovatele.), budete potřebovat přenést maily mail serveru, který je bude schopen odesílat. Toto pole specifikuje host, nebo IP adresu cílového přenosového serveru(ů). Více zadání v této položce oddělte středníkem.
DNS	Jestliže mail server odesílá zprávy přímo do internetu, budete potřebovat vyhledávat DNS MX (Mail Exchange) záznamy externích domén. Zadejte host, nebo IP adresu vámi používaného DNS serveru. Více zadání oddělte opět středníkem. Vždy použijte testovací DNS tlačítko. Musíte si být ale jisti, že jste si dobře prostudovali DNS přílohu.
Relay / Use DNS Lookup	Toto pole specifikuje, která se dvou možných metod bude používána při doručování e-mailů..
Server Statistics	Pomocí funkcí “Server Statistics” můžete sledovat statistiku provozu všech služeb Meraka. Ten je pomocí PIPů získává každých 5 sekund.

Konfigurační soubor Config\hosts.dat – Doručování zpráv pomocí statické IP adresy (toto nastavení je určené především pro LAN a intranety).

Pomocí souboru hosts.dat můžete v Meraku nastavit staticky IP adresy pro servery, které jsou umístěny uvnitř Vaší sítě.

Pokud je soubor hosts.dat v konfiguračním podadresáři nalezen, Merak nepoužívá klasickou cestu MX záznamů. Pouze se řídí nastavením v souboru hosts.dat a nedotazuje se DNS serveru. Syntaxe v konfiguračním souboru hosts.dat je následující:

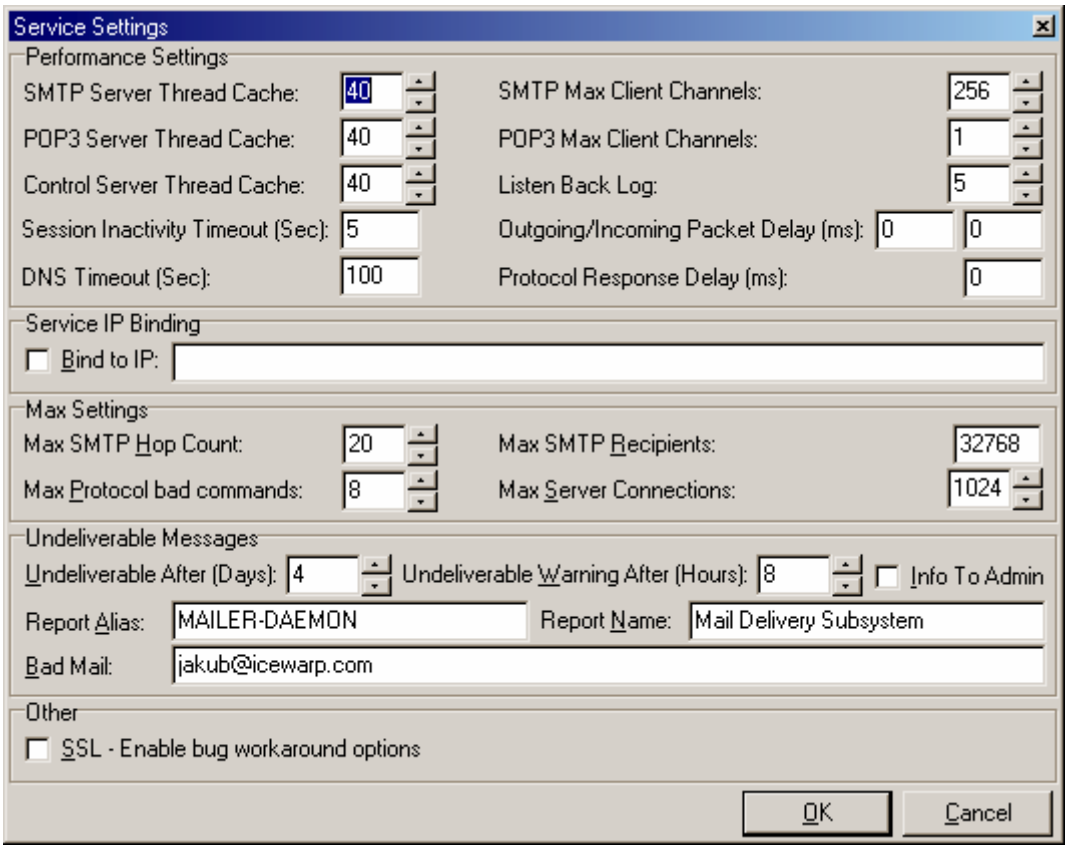
```
<doména>=<hostjméno>
nebo
<doména>=<IP adresa>
```

Příklad:

```
doména1.lokalni=hlavniserver
doména1.lokalni=192.168.0.100
```

Pokud budete chtít obnovit standardní cestu DNS dotazu, stačí smazat soubor hosts.dat

Klikněte na tlačítko “Service settings” (nastavení služeb). Pomocí této nabídky můžete využít pokročilejších nastavení služeb:

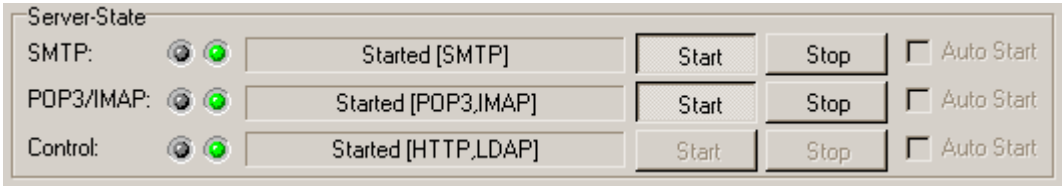


Pole	Popis
SMTP Client Channels	Tato položka specifikuje maximální možný počet současných spojení na jiný SMTP server
POP3 Client Channels	Tato položka specifikuje maximální počet současných spojení na jiný POP3 server ve chvíli, kdy dochází k výběru zpráv přes POP3.
DNS Timeout	Nastaví časovou prodlevu pro DNS lookup. Pokud DNS server neodpovída ve stanoveném čase, začně pokládat Merak DNS server za nefunkční. Standardní hodnota je 20 sekund a může být snížena, pokud si myslíte, že by měl DNS server odpovídat rychleji. To si můžete otestovat pomocí DNS dotazovacího nástroje.
Packet Delay (Outgoing & Incoming)	Pokud je server na velmi rychlém připojení (např. místní LAN) rychlost, kterou Merak pracuje by mohla mít vliv na výkon ostatních služeb. Použijte tuto funkci, pouze pokud jste si jisti, že ji bezpodmínečne potřebujete. Rozhodně ji však nebudete potřebovat u žádné pevné linky o přenosové rychlosti 128k a méně.

Protocol Response Delay	Merak je velmi rychlý e-mailový server, který podporuje internetové protokoly a zcela bezproblémově s nimi dokáže spolupracovat. Stejně tak spolupracuje s Merakam zcela bez problémů většina e-mailových klientů. Je ale na světě pár produktů, které jsou poněkud zmateny rychlostí, kterou je Merak schopen spolupracovat. Mluvíme tady hlavně o programu Outlook 2002/XP. Microsoftu se bohužel podařilo implementovat do tohoto produktu chybu, která někdy může činit problém. Nastavte zde hodnotu 10 v případě, že máte nějaký problém.
Bind to IP	Pomocí tohoto nastavení můžete zvolit IP adresu síťového adaptéru, který má Merak používat (toto nastavení se hodí např. Když potřebujete mít na server nainstalovano více mail serverů). Adresy jsou odděleny středníkem. Tuto funkci nedoporučujeme používat, pokud ji skutečně nepotřebujete.
Report Alias / Report Name	Report alias je alias, který systém přidává k názvu primární domény a vkládá jej do pole „Odesilatel“. Systém tento alias používá při generování automatických hlášení, jako např. hlášení o nedoručitelném emailu, či o místě na disku serveru. .
DNS Timeout	Specifikuje časovou prodlevu při funkci DNS Lookup. Pokud DNS server neodpovídá v daném čase, Merak ho začne brát jako neodpovídající DNS server. Standardní hodnota je 20 sekund a pokud si myslíte, že váš DNS server bude odpovídat rychleji, může být tato hodnota snížena. Vše můžete otestovat pomocí nástroje DNS Query.
Hide IP	Tato funkce skryje IP adresu, která se uvádí v hlavičkách přijmutných emailových zpráv. Pokud tuto funkci zapnete, nikdo nebude schopen zjistit konfiguraci vaší lokání sítě.
SSL – Enable bug workaround options	Jestliže je SSL spojení z jakéhokoliv důvodu neuspěšné, může to být způsobeno mail klientským programem. V tomto případě použijte tuto funkci. Víme o problémech s e-mailovými klienty Eudora a The Bat!.
Bad Mail adress	V tomto nastavení je možné definovat adresu, nebo adresy (oddělené středníkem), které budou použity ve všech případech, kdy není možné doručit odeslaný e-mail zpět odesilateli. Budou zpracovány zprávy s neuvedeným odesilatelem, serverem generované zprávy a případy, kdy má odesilatel plnou e-mailovou schránku. Tato adresa může být umístěna na lokálním i externím serveru.
Info to Admin	Pomocí tohoto pole můžeme zapnout infrormování administrátora v případě, že je nedoručitelná nějaká zpráva a byla vrácena odesilateli.
Undeliverable After	Pomocí tohoto nastavení specifikujeme počet dní, po který se Merak pokouší doručit zprávu. Jestliže správa nemohla být v nastaveném termínu doručena, bude vrácena odesilateli jako nedoručitelná.
Max Server Connections	Nastaví maximální možný počet spojení na server. Pokud je počet spojení překročen, budou zprávy, které nebylo možné doručit, vráceny jako dočasně nedoručitelné.
Protocol Max bad commands	Nastaví maximální možný počet neplatných příkazů, které Merak akceptuje během jednoho spojení.

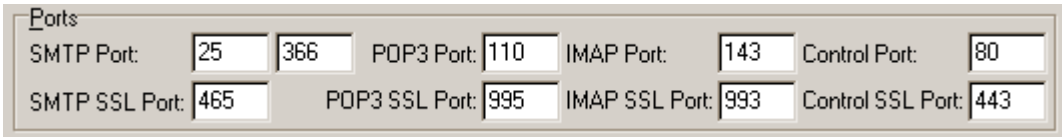
Max Recipients	Nastaví maximální možný počet příjemců v jedné zprávě.
Max Hop Count	V tomto poli specifikujeme maximální počet skoků z emailových serverů. Toto je ochrana proti cyklování zpráv. Definujeme zde maximální počet emailových serverů, přes které může být email doručen. Pokud je zde nastavená hodnota překročena, zpráva je vrácena jako nedoručitelná. Tento problém se může vyskytovat při chybně fungujícím DNS Mail Exchange (MX) záznamu pro doménu, nebo pokud používate předávací (forward) funkci a předávate zprávu Meraku.
Session Inactivity Timeout	Nastaví maximální povolenou dobu (v sekundách), po kterou nemusí být spojení aktivní. Pokud nebude spojení aktivní delší dobu, bude automaticky ukončeno.

Popis stavových polí v tabulce System



Pro každou ze tří služeb jsou podél umístěna kontrolní tlačítka Start / Stop. Na platformách Windows 9X jsou zde „Autostart“ pole. Ta zajistí automatický start služby při nabootování stroje. Tato funkce se standardně používá u Windows NT / 2000 (služby).

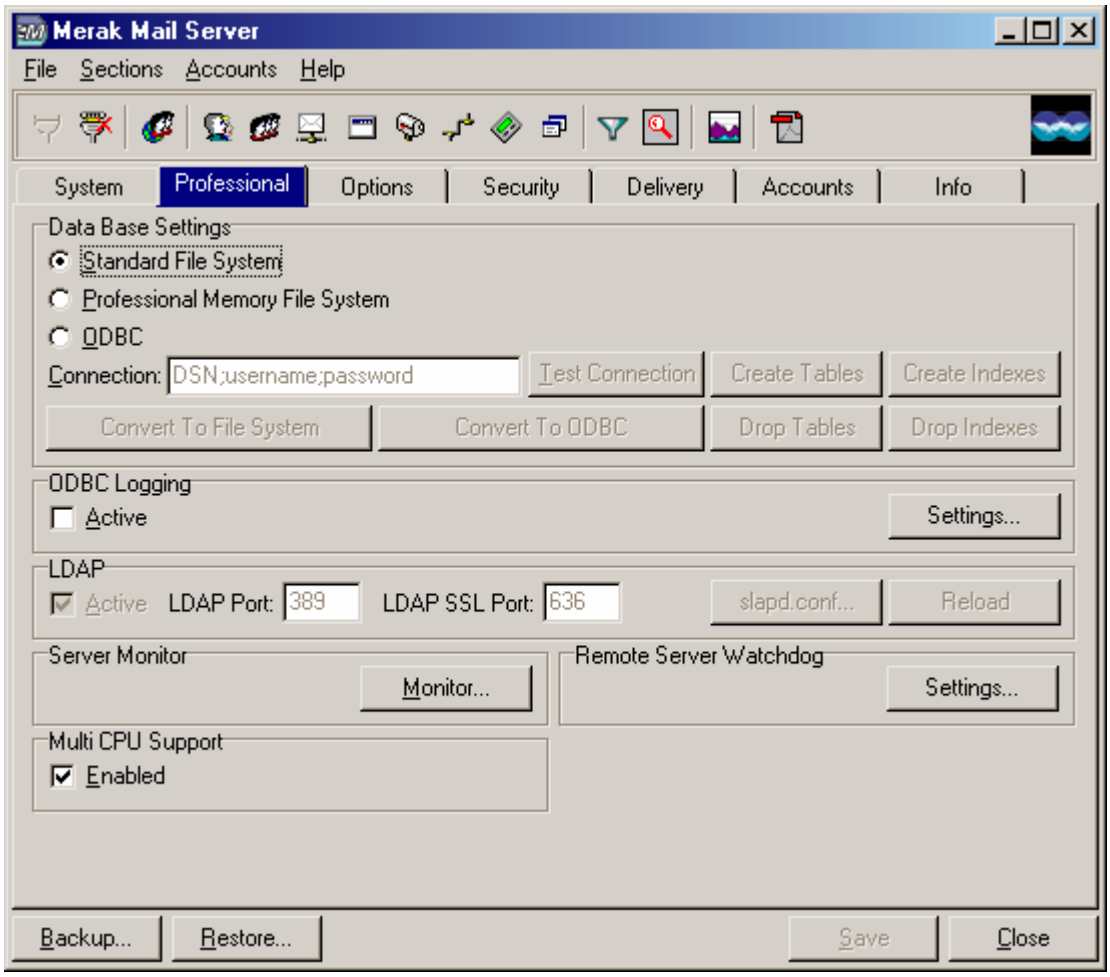
Popis polí nastavení portů v tabulce System



Každá služba je vázána na číslo TCP portu. To může být (pakliže je to zapotřebí) změněno. Nicméně standardní nastavení odpovídají internetovým standardům, který byly požadovány Poskytovateli. Právě oni pracují s nejvíce instalacemi. Toto nastavení neměnte, pokud nerozumíte tomu, co děláte.

SMTP server může poslouchat na dvou portech. Tím se můžete vyhnout problémům v případě, že firewall Vašeho providera blokuje port 25.

Tabulka Professional



Celá tabulka Professional je dostupná pouze v profesionální verzi Meraka.

Pole	Popis
Data Base Settings	Toto nastavení vám zvolí typ databáze, kterou by měl Merak používat pro ukládání dat. Můžete si zvolit te tří rozdílných možností: **Standard File System (Standardní souborový systém)** Typ Standard DB je stejný typ databáze, jakou používají ostatní verze Meraka. **Professional Memory File System (Profesionální paměťový souborový systém)** Pomocí profesionálního paměťového souborového systému můžete uložit všechny účty dočasně do paměti. Rychlost takové konfigurace je velmi působivá. Nicméně celé nastavení vyžaduje větší množství operační paměti. **ODBC** ODBC vám umožní přistupovat a ukládat data všech účtů do jakýchkoliv databází přes ODBC. Systém může potom použít databáze jako MS SQL, MySQL, Oracle, MS Access, InterBase, Postgre, Informix a ostatní.

Řetězec, který použijete pro připojení k databázi obsahuje všechny potřebné informace, které jsou potřeba k připojení k databázi:

```
DSN;uživatelskéjméno;heslo

Např.:
emailovýserver;sa;sapass
```

Po každém nastavení použijte tlačítko pro otestování spojení z databází. Pokud vše proběhne v pořádku, zadaný řetezec byl správný.

Někdy může být potřeba volat pro správnou funkčnost DB ODBC enginu a nepoužívat ODBC Cursors nebo použít Magic Quotes (pro MySQL). Budete muset vytvořit soubor DB.INI v adresáři Meraka. Ten má následující strukturu:

```
MagicQuotes=1
ODBCCursors=0
OracleSyntax=0
```

Poznámka: Uživatelé MySQL databází by měli používat myODBC 3.51

Před použitím serveru potřebujete vytvořit strukturu tabulek v DSN. K tomu použijte tlačitko “Create Tables”.

Nastavení ODBC krok za krokem:

1. Pro připojení k databázi vytvořte systémovou DSN v ODBC Data Sources (zdroje dat ODBC)

2. Vytvořte správný řetězec pro připojení k databázi a zadejte ho do DB settings (nastavení databáze) v konfiguračním appletu Meraka. Spojení otestujte pomocí tlačítka Test Connection.

3. Uložte nastavení

4. Pro vytvoření tabulek klikněte na tlačítko “Create Tables”

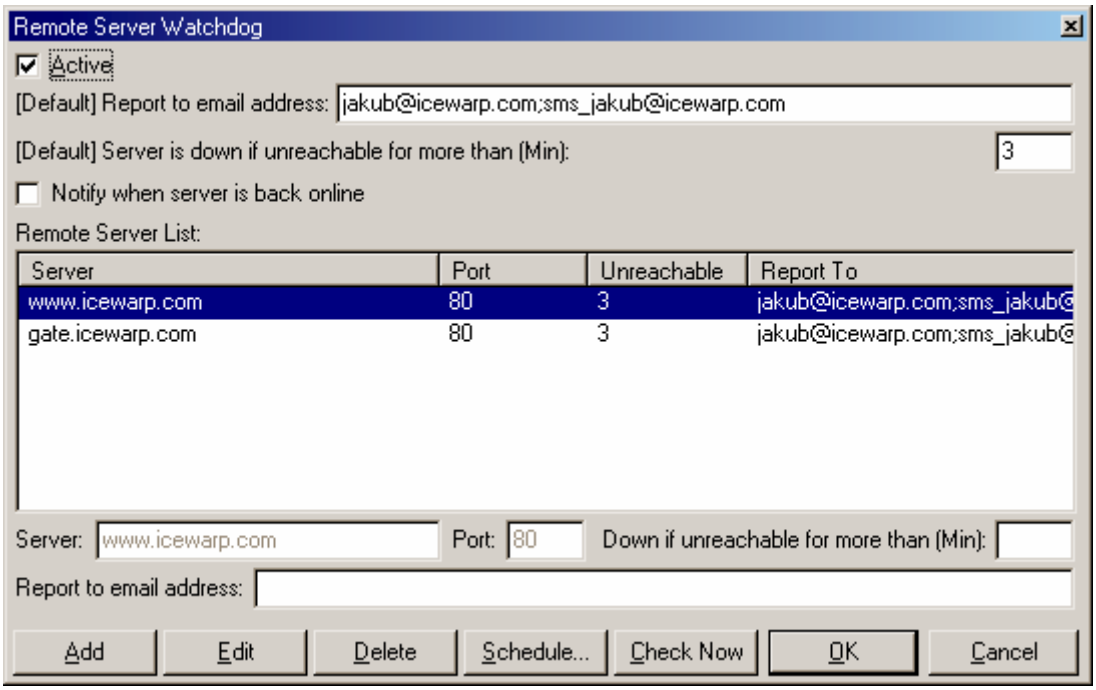
5. Pokud vše proběhlo úspěšně, můžete importovat předchozí nastavení uživatelů Meraka kliknutím na tlačitko “Convert to ODBC” (konvertovat do ODBC).

5. Po zmáčkuní F5 pro znovunačtení by mělo vše fungovat..

Tlačítko pro konverzi dat do databáze použijte jenom jednou. Data musí být importována do prázdné databáze, nebo souborového systému Meraka.

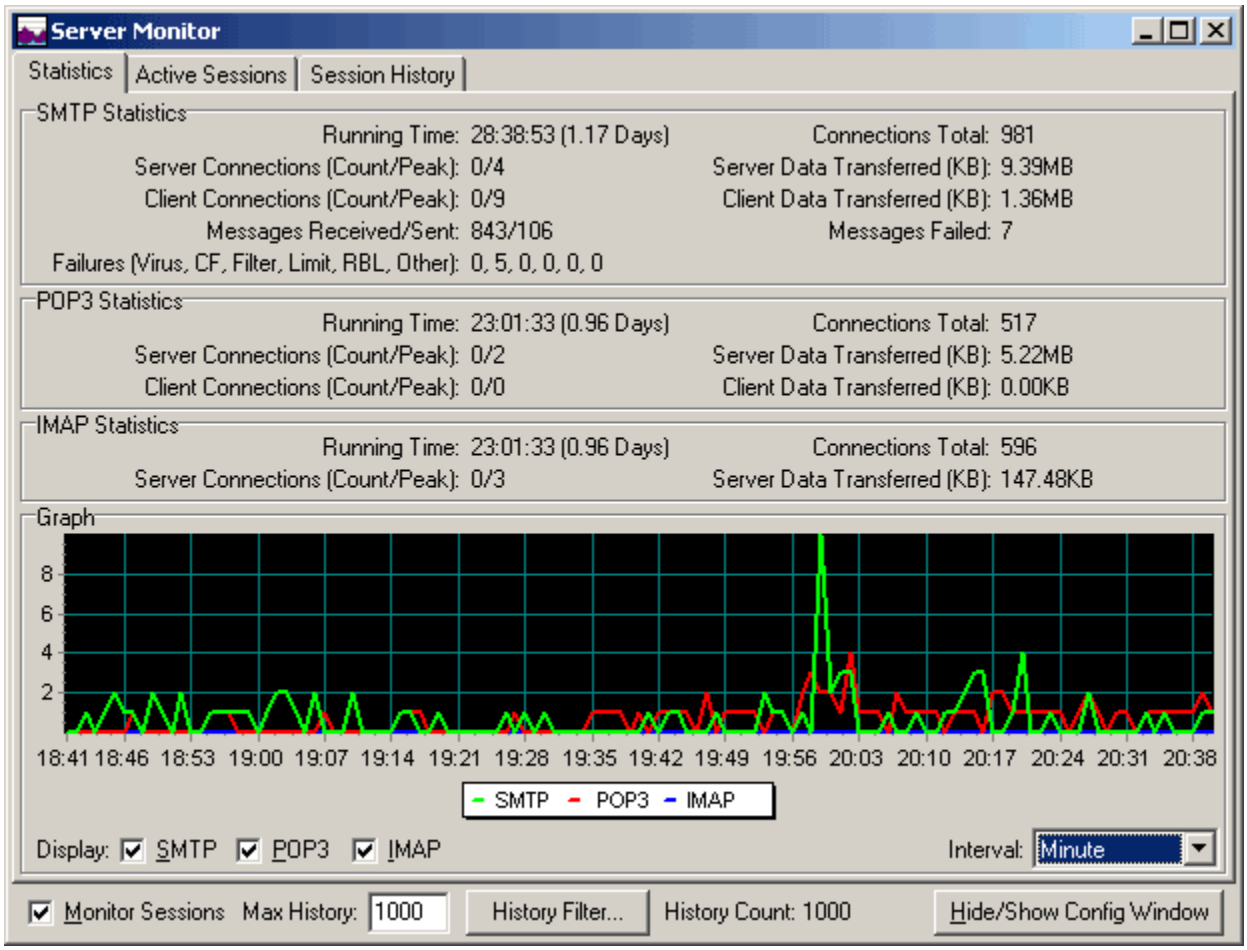
ODBC Logging	Do databáze můžete také ukládat logy (zaznamenané informace při běhu serveru). Stačí nastavit připojovací řetězec a vytvořit tabulky.
LDAP	Prosím prohlédněte si část manuálu o LDAP.
Server Monitor	Pomocí funkce server monitor můžete sledovat provoz serveru v reálném čase a také krátkou historii spojení. Server podává statistiky o zátěži, aktivních spojeních všech služeb. Můžete také sledovat záznamy spojení, pokud je zaznamenávání aktivováno.
Remote Server	Merak Mail server vám umožní monitorovat ostatní vzdálené server a jejich specifické služby. Staší nastavit host adresu, číslo portu a časový interval, ve kterém

Watchdog	má být provaděna kontrola. Pokud je jeden z nastaveným serverů mimo provoz, Merak automaticky vygeneruje a zašle zprávu obsahující jméno serveru a čas výpadku. Pro každý kontrolní záznam může být nastavena odlyšná cílová e-mailová adresa.



Pole	Popis
Active	Specifikuje stav nastavení (aktivní / neaktivní)
Report To Email Address	Všechny generované zprávy ze serveru budou odeslány na tuto e-mailovou adresu, nebo adresy. Toto pole může zůstat prázdné pro jednotlivá kontrolní nastavení. V takovém případě bude použita globálně nastavená e-mailová adresa.
Server is down when unreachable for more	Někdy je server mimo provoz zcela cíleně (např. Kvůli udržbě). V tomto poli nastavujeme počat minut po které musí být server mimo provoz, aby bylo zásláno upozornění. Toto pole může zůstat prázdné pro jednotlivá kontrolní nastavení. V takovém případě bude použit globálně nastavený časový interval.
Notify when server is back online	Pokud je server mimo provoz a Merak zjistí, že byl opět spuštěn, zašle upozornění.

Server Monitor

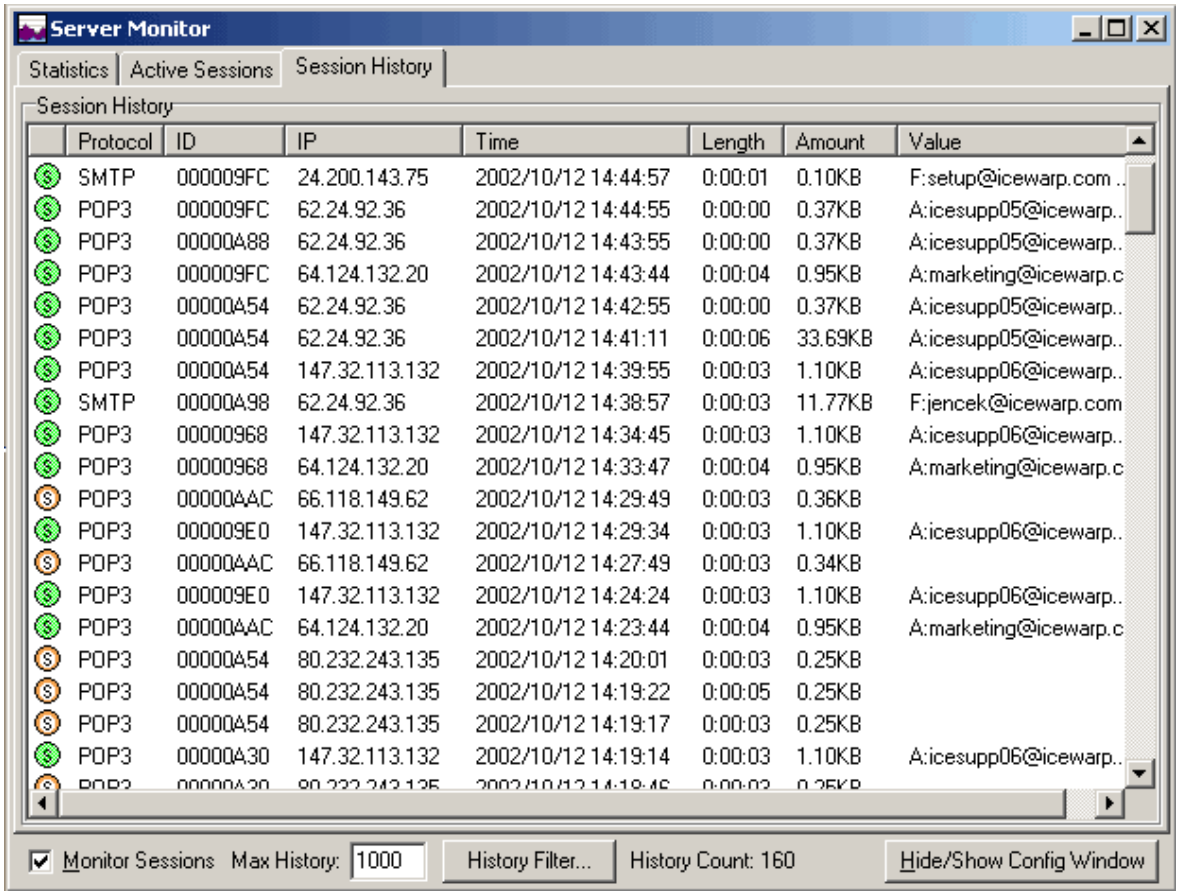


Nástroj server monitor se skládá ze tří tabulek

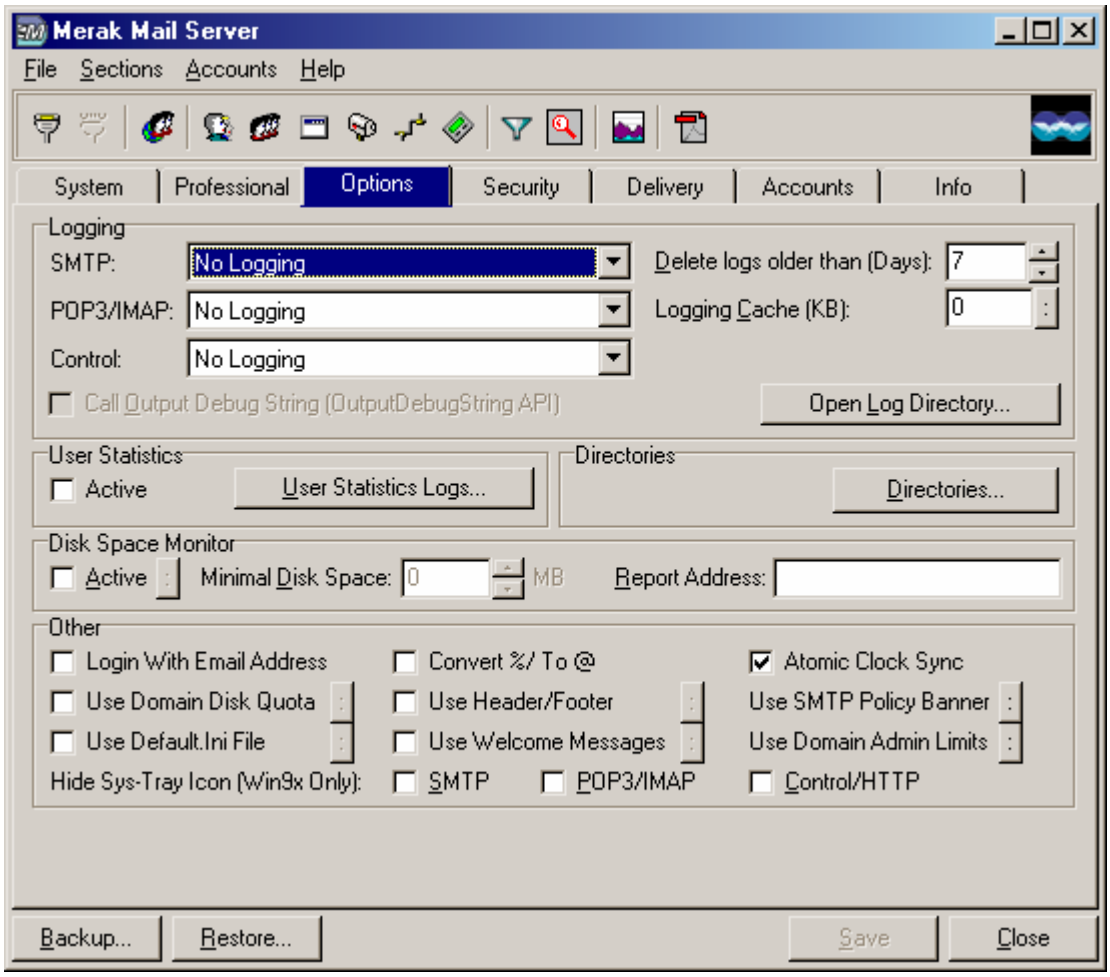
Tabulka “Statistics” ukazuje všechy výkonostní přehledy a statistické informace včetně grafu.

Tabulka “Active Sessions” Vám umožní sledovat aktivní spojení na serveru. Pokud máte zapnuté logování, můžete si celý obsah daného spojení prohlédnout dvojklikem. K aktivací, nebo deaktivaci monitorování jednotlivých spojení použite pole “Monitor Sessions”.

Ikony na levé straně specifikují typ spojení. Znak C specifikuje klientská spojení a znak S serverová spojení. Barva může být buď Zelená, Červená, nebo Hněda. Zelená ikonka znamená, že všechno proběhlo v pořadku a spojení bylo úspěšné, hnědá barva znamená, že během spojení se stalo něco divného a spojení nebylo úspěšné. Červená barva znamená, že spojení bylo z nějakého důvodu odmítnutí (např. Kvůli obsahovým filtrům).


Server Monitor
Statistics
Active Sessions
Session History
Session History
Protocol ID IP Time Length Amount Value
SMTP 000009FC 24.200.143.75 2002/10/12 14:44:57 0:00:01 0.10KB F:setup@icewarp.com ..
POP3 000009FC 62.24.92.36 2002/10/12 14:44:55 0:00:00 0.37KB A:icesupp05@icewarp..
POP3 00000A88 62.24.92.36 2002/10/12 14:43:55 0:00:00 0.37KB A:icesupp05@icewarp..
POP3 000009FC 64.124.132.20 2002/10/12 14:43:44 0:00:04 0.95KB A:marketing@icewarp.c
POP3 00000A54 62.24.92.36 2002/10/12 14:42:55 0:00:00 0.37KB A:icesupp05@icewarp..
POP3 00000A54 62.24.92.36 2002/10/12 14:41:11 0:00:06 33.69KB A:icesupp05@icewarp..
POP3 00000A54 147.32.113.132 2002/10/12 14:39:55 0:00:03 1.10KB A:icesupp06@icewarp..
SMTP 00000A98 62.24.92.36 2002/10/12 14:38:57 0:00:03 11.77KB F:jencek@icewarp.com
POP3 00000968 147.32.113.132 2002/10/12 14:34:45 0:00:03 1.10KB A:icesupp06@icewarp..
POP3 00000968 64.124.132.20 2002/10/12 14:33:47 0:00:04 0.95KB A:marketing@icewarp.c
POP3 00000AAC 66.118.149.62 2002/10/12 14:29:49 0:00:03 0.36KB
POP3 000009E0 147.32.113.132 2002/10/12 14:29:34 0:00:03 1.10KB A:icesupp06@icewarp..
POP3 00000AAC 66.118.149.62 2002/10/12 14:27:49 0:00:03 0.34KB
POP3 000009E0 147.32.113.132 2002/10/12 14:24:24 0:00:03 1.10KB A:icesupp06@icewarp..
POP3 00000AAC 64.124.132.20 2002/10/12 14:23:44 0:00:04 0.95KB A:marketing@icewarp.c
POP3 00000A54 80.232.243.135 2002/10/12 14:20:01 0:00:03 0.25KB
POP3 00000A54 80.232.243.135 2002/10/12 14:19:22 0:00:05 0.25KB
POP3 00000A54 80.232.243.135 2002/10/12 14:19:17 0:00:03 0.25KB
POP3 00000A30 147.32.113.132 2002/10/12 14:19:14 0:00:03 1.10KB A:icesupp06@icewarp..
Monitor Sessions
Max History:
1000
History Filter...
History Count: 160
Hide/Show Config Window

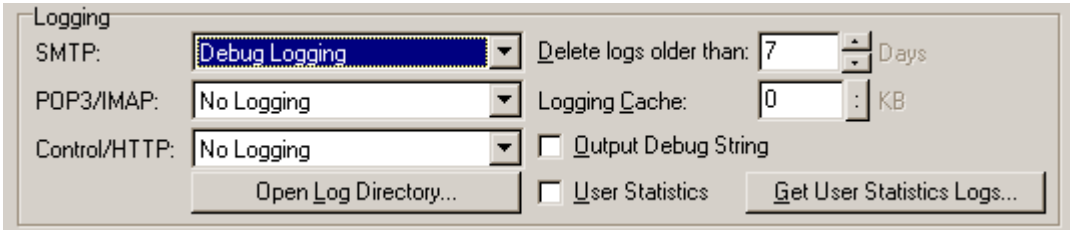
Tabulka Options



Ve druhé tabulce nastavení (Options) je seznam všech funkcní, které jsou důležité pro to, aby mohl Merak fungovat jak má. Adresářová část nám specifikuje, kde Merak vytváří během fungování různé soubory. Adresáře nemusí být vytvořeny předem, Merak si všechny adresáře podle požadavků vytvoří. Pokud je potřeba můžete modifikovat také soubor path.cfg (který je umístěn v adresáři Meraka) – první řádek specifikuje umístění konfiguračního adresáře Meraka, druhý řádek specifikuje umístění HTML adresáře (adresář pro vzdálenou administraci).

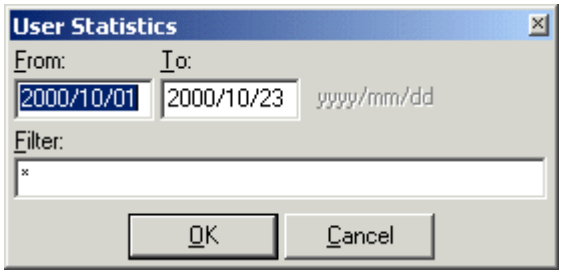
Většina z textových konfiguračních souborů může obsahovat komentáře, které jsou značeny dvěmy „//“ lomítky

Popis polí nastavujích logování v tabulce Options



Pole	Popis
Logging Levels	**V Meraku můžete nastavit různé úrovně logování (zaznamenávání) informací o běhu serveru:**

	No Logging Funkce logování je vypnuta. Nejsou tedy zaznámenávány žádné informace. **Debug Logging** Nejvíce detailní logování celého systému. Ve výsledném výpisu jsou obsaženy informace z celého provozu server. **Summary Logging** Tato funkce zaznamenává nejvíce důležité informace a také sumarizuje celou činnost služby. Jinými slovy: To, co ve funkci Debug Logging zabere několik řádků, zde zabere řádek, ve kterém je obsaženo více informací. **Debug & Summary Logging** Při záznamu provozu serveru budou použity oba módy.
Logging Cache	0 specifikuje žádnou cache. Jinak logovací cache je definována v KB. Logy jsou uchovávány v paměti a uloženy na disk, když je povolená cache přeplněna.
Delete logs older than :	Pokud je logování zapnuté, je potřeba udržet množství logů v nějaké rozumné míře. A přesne k tomu je tato položka. Zde totiž specifikujete po kolika dnech má být log soubor smazán.
Output Debug String	Pokud je funkce „Output debug String“ zapnuta, je po každé změně v logu vyvoláná Windows API funkce „OutputDebugString“, která každou událost zapíše do „event logu“. Tato funkce je použitelná pro online monitorování serveru a může být používána vzdáleně. Tuto funkci můžete mít zapnutou, pokud máte vhodný nástroj určený pro zobrazení těchto vzkazů. Jedním z takových nástrojů je i program DebugView/EE. Ten můžete najít na adrese: http://www.sysinternals.com. Nezapoměnte v tomto programu zapnout položku „CRLF Return“. Pokud tak neučiníte, nebudou se vám vzkazy zobrazovat.
User Statistics	Pokud zapnete funkci **User Statistics**, řeknete tím serveru, aby logoval veškerou uživatelskou aktivitu. U každého uživatele se bude zaznamenávat velikost a počet přijmutných, odeslaných emailů. Zaznamenávat se bude dokonce aktivita neznámých externích uživatelů.



Logy můžete použitím tlačítka Get exportovat Požky From a To specifikuji časovou stupnici, kterou chcete z logu získat. Do položky Filter specifikujete větší množství filtrů, které bude odděleno čárkami. Můžete zde zadat E-mailové adresy, nebo domény.

Např. info@icewarp.com;merakmail.com

Formát samotného logu je následujícíc:

```
Doména,Alias,Přijmuto,Přijmuto_množství,Odesláno,Odesláno_množství,Odesláno
ven,Množství_odesláno_ven,Poslední odesláno,Poslední přijmuto,Poslední přihlášení
```

Množství je uvedeno v bajtech. Tento soubor můžete importovat do nějaké databáze, nebo nástroje určeného k analýze. Poslední řádek obsahuje statistiku externích, neznámých uživatelů a zpráv, které systém vytvořil sám.

K logování jednotlivých služeb stačí zvolit mód logování, který potřebujete. Mód Debug logging je doporučen pro použití s SMTP.

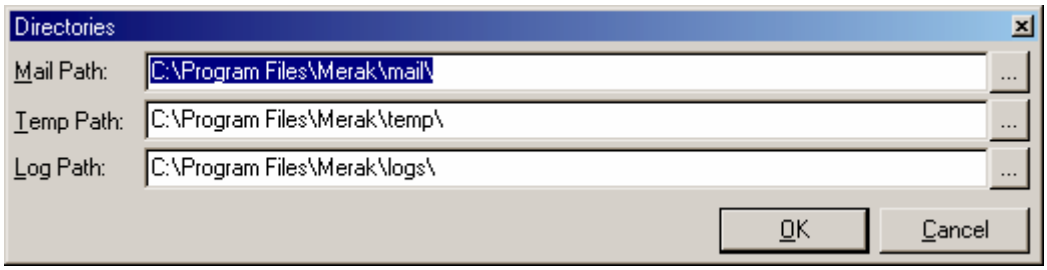
Samotné jméno logu je v následujícím formátu:

SRRRRMMDD.log

S = Typ služby (S)MTP, (P)OP/IMAP or (C)ontrol or (E)rror
RRRR = Rok např. 2000
MM = Měsíc např. 10
DD = Den např. 23

So P20001023 by měl být POP3/IMAP4 záznam pro 23 Října 2000.

Tlačítko pro nastavení adresářů (directories)



Pole	Popis
Temp Path	Dočasná cesta je používána při přijímaní E-mailů a jejich vstupu do systému. Potom, co je E-mail přijmut, Merak jej zkopíruje do správného mailboxu, či mailboxů a poté je z dočasného adresáře E-mail smazán. Při každém spuštění Meraka je tento adresář automaticky smazán.
Mail Path	Zde specifikujeme adresář, pod kterým se budou vytvářet uživatelské emailové schránky. Např. pokud máme uživatele pojmenovaného admin v doméně icewarp.com pak bude standardní adresář pro administrátorský uživatelský mailbox e:\merak\mail\icewarp.com\admin. Tento adresář také obsahuje odchozí frontu složku, která se jmenuje Forward. Tato složka uchovává všechny zprávy, které mají být odeslány. Pokud tato složka není prázdná, není něco v pořádku z vaším internetovým připojením.
Log Path	Položka log path definuje cestu k adresáři, ve kterém se budou vytvářet logové soubory. Budou zde k dispozici SMTP/POP3/IMAP4 a „Control“ logy.Log soubory můžete prohlížet přes webové či kontrolní rozhraní.

Popis polí sledování místa na disku v tabulce Options

Pole	Popis
Monitor Active	Pokud chcete funkci monitorovaní místa na disku zapnout, zaškrtněte tuto položku. Merak může monitorovat volné místo na vašich discích a v případě malého množství místa vás může včas informovat pomocí emailu odeslaného na vaši emailovou schránku.
Minimal Disk Space	Zadejte hodnotu (v MB). Tato hodnota bude považována za práh, po jehož překročení vám bude zaslán email.
Report	Právě sem uvedeme e-mail adresu, na kterou se budou odesílat zprávy

Address	upozorňující na místo na disku. Můžeme zadat více E-Mailových adres, oddělíme je pomocí středníku.

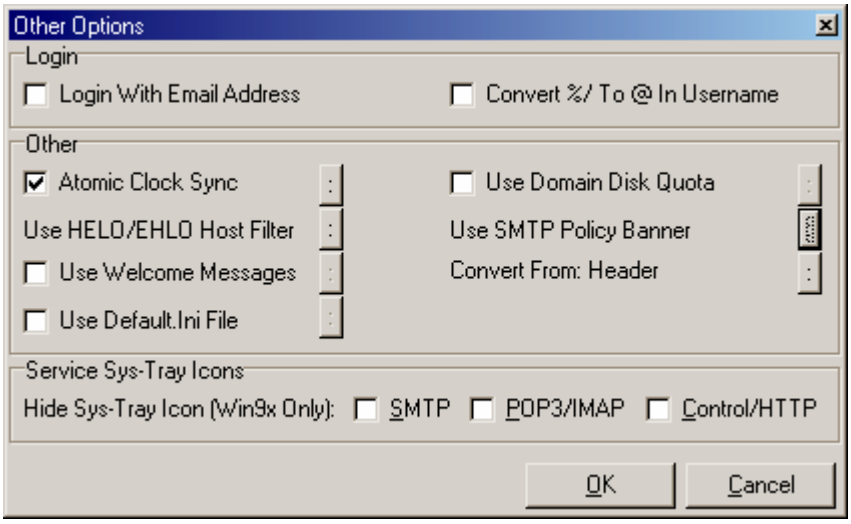
Můžete také použít soubor diskspace.dat pro monitorování více disků:

```
C=400
D=800
```

Jestliže hodnota místa na disku dosáhla vámi nastaveného prahu, bude systémem odeslán email, který vypadá asi takto:

```
From: Mail Delivery Subsystem [MAILER-DAEMON@icewarp.com]
Sent: 23 October 2000 21:31
To: admin@icewarp.com
Subject: Warning: system report

Warning: system report

Disk Space Monitor has detected low disk space on drive D: 410 MBytes
```

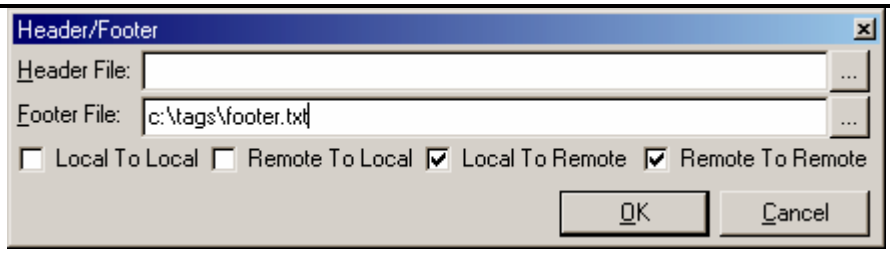
Popis ostatních polí v tabulce Options



Pole	Popis
Login With Email Address	Pokud máte na svém serveru velké množství domén doporučujeme vytvořit formát jejich mailových schránek ve tvaru jejich emailové adresy např. ian@icewarp.com. Pokud zapnete fukci domain mailbox processing, zredukujete autentifikační a přihlašovací čas – Merak je totiž schopen vyhledat uživatelskou doménu rychleji, pokud je specifikována v samotném názvu mailboxu. Pro velké servery to tedy jistá možnost dalšího zvýšení výkonu. Pakliže se ale rozhodnete tuto možnost využít, nebududete moci používat standardní formát pro názvy mailboxů. Všechny názvy mailboxů musí obsahovat doménové jméno. Pokud nebude doménové jméno použito, bude automaticky použita primární doména.
Convert % To @	Tato volba umožnuje administrátorům, kteří používají plnou emailovou adresu jako uživatelské jméno a spolu s tím internetový přohlížeč Netscape a osobní počítač Macintosh a nemohou tedy použít @ ve svém přihlašovacím jménu. Pomocí této volby zapnete možnost konverze znaku @ v přihlašovacím jménu. Uživatelé s Netscapem a Macintoshem budou tedy moci jako přihlašovací jméno

	použít tvar jméno%doména.com a auntentifikační engine Meraka provede automatickou konverzi znaku @ na %
Atomic Clock Sync	Tato volba umožní zvolit automatickou synchronizaci času na serveru podle atomových hodin. Synchronizace probíhá o půlnoci. Nastavení bere v potaz časové zóny.
Use Domain Disk Quota	Tato položka indikuje domény, by měly podléhat diskovým kvotám při přijímaní emailu. Pokud kvóta překročí daný limit, emaily budou odmítany. Jakékoliv domény vyžadující kvótu musí být specifikovány v soboru diskquot.dat (umístěného v konfiguračním adresáři).Tento konfigurační soubor může být otevřen opět použitím tlačítka „:“. Formát souboru je následující: doména=limit Příklad: Main.cz=5192 *=10000 Toto nastavení by určilo, že všechny domény mají diskovou kvótu 10 MB nehledě na doménu main.cz, která má kvótu 5 MB

Pole	Popis
Use HELO/EHLO Host Filter	Tento soubor slouží pro nastavení filtru, který je proveden při HELO/EHLO příkazu během SMTP spojení. Tento filtr umožňuje velmi snadno blokovat servery bez znalosti jejich IP adres.
Use Header / Footer	Toto nastavení umožní vkládat hlavičky a patičky do zpráv automaticky. Můžete nastavit pouze hlavičku a patičku, nebo oboje. Toto nastavení pracuje společně se souborem tags.dat (v konfiguračním podadresáři). Ten můžete ručně editovat, nebo otevřít pomocí tlačítka”:”. Umístění konfiguračního souboru tags.dat v konfiguračním adresáři převyšuje hlavní nastavení serveru. Nastanou tři možné scénáře: 1) Lokální odesilatel, lokální příjemce: obě hodnoty “From:” a “To:” náleží do lokální domény. Potom všechny čtyři řádky v souboru tags.dat budou vloženy do těla zprávy. 2) Lokální odesilatel, vzdálený příjemce: pouze adresa uvedená ve “From:” patří do nějaké z lokálních domén. Pak bude do těla zprávy vložen řádek 1 a 2 ze souboru tags.dat 2) Vzdálený odesilatel, lokální příjemce: pouze adresa v poli “To” náleží do lokální domény. V tomto případě budou do těla zprávy přídány řádky 3 a 4 ze souboru tags.dat. Nastavení probíhá pomocí následujícího dialogu:



Use SMTP Policy Banner

Tento text bude zobrazen vždy, když emailový klient kontaktuje server s požadavkem na odeslání e-mailu. K editaci tohoto textu použijte tlačítko „:“. Po použití tlačítka bude spuštěn textový editor, zadejte vámi požadovaný text, zavřete okno a uložte, nebo smažte vámi modifikované nastavení.

Abyste byli schopni tento text editovat, budete muset možná provést restart služby SMTP. Celý text začíná po zobrazení linkou s hvězdičkou

```
220-mail.domena.cz ESMTP Merak 5.0.1; Sun, 22 Oct 2000 14:32:28 +0100
220-*********************************************************************
220-* Zabezpeceny e-mailovy server
220-*
220-* Vsechna spojeni se zaznamenavaji!
220-* Tento server obsahuje antivirovou a antispamovou technologii
220-*
*********************************************************************
```

Use Default.ini File

Tato funkce specifikuje, že soubor default.ini by měl být použit vždy při přidání nového uživatele. Uživatel bude přidán s nastavením uvedeným v souboru default.ini. Tento soubor je umístěn v hlavním adresáři a může být editován pomocí tlačítka . Toto nastavení je platné pro uživatele vytvořené přes webové rozhraní, nikoli však pro uživatele vytvořené z příkazové řádky.

Use Welcome Messages

Pomocí tohoto nastavení specifikujete zprávu, která bude uložena do schránky novému uživateli hned po jeho založení. Můžete nastavit různé uvítací zprávy pro různé domény, ale ne všechny domény musí mít uvítací zprávu nastavenu.

Uvítací zprávy musí být vytvořeny v oddělených textových souborech. Na tyto textové soubory odkazuje soubor messages.dat (v konfiguračním podadresáři), který může být otevřen použitím editačního tlačítka “.”

Struktura souboru je následující:
Doména=jmeno_souboru

Příklad:
Icewarp.com=c:\merak\welcome.tmp

Pokud nastavíte místo jména domény hvězdičku (pomocí hvězdičkové konvence), bude vámi definovaná uvítací zpráva použita pro zbytek domén. Pamatujte si, že pokud budete chtít využít tuto funkci, musí být parametr s hvezdičkou na posledním řádku konfiguračního soubory, protože pokud by byl výš, byly by všechny nastavení pod ním ignorovány.

Upozornění: Zpráva obsahující uvítací e-mail musí mít stejnou strukturu, jako skutečná e-mailová zpráva. Musí obsahovat pole jako From: (odesilatel), Subject: (předmět) apod. Konec e-mailu musí být ukončen “.” Na konci.
Příklad:

From: Administrator <administrator@icewarp.cz>

To: všem uživatelům
Subject: Vítej nový uživateli

Drahý nový uživateli,
Rádi bsme tě přivítali.....

.

Pole	Popis
Server Title	Při jakémkoliv spojení na SMTP server se Merak na prvním řádku identifikuje. Pokud chcete na tento řádek umístit jiný text, nebo z nějakého důvodu nechcete, aby někdo věděl, jaký e-mailový server používáte, stačí vytvořit konfigurační soubor servertitle.dat (tento soubor je umístěn v konfiguračním adresáři). V něm je možné tento první řádek editovat.
Hide Systray Icons	Pokud používate Meraka ve Windows 9X, můžete tři stavové ikony, které se zobrazují v dolní liště schovat pomocí tohoto nastavení.

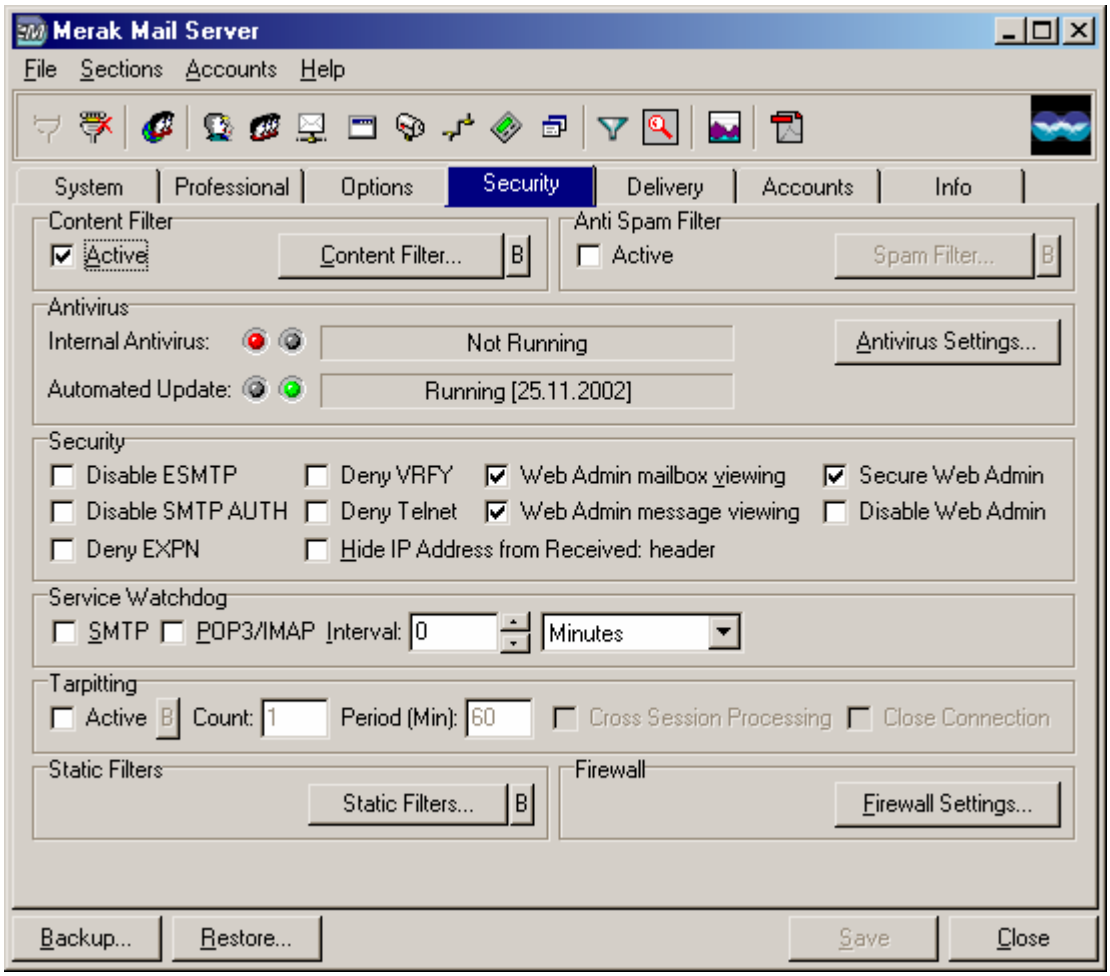
Header Conversion	Merak umožňuje automaticky měnit doménové jméno původce, nebo příjemce. Když Merak odesílá zprávu, může tato funkce automaticky konvertovat doménové jméno na nové, specifikované v souboru config\headerconvert.dat. Struktura tohoto souboru je následující:
	
	`{staradomena}={novadomena}`
	`{staradomena}={novadomena}`
	
	`Např.:`
	`merakmail.com=icewarp.com`
	`usa.net=netaddress.com`

Automatická archivace zpráv

Pole	Popis
Active	Pomocí autoamatické archivace zálohujeme všechny zprávy doručené na server. Jsou brány v potaz jak SMTP,tak IMAP zprávy. Ukládání probíhá podobně, jako do Mail adresáře. Do adresáře nastaveného v auto archivaci jsou vlastně zrcadleny zprávy z mail adresáře. Adreářem můžete velmi jednoduše procházet a v případě potřeby zprávy smazat. Dávejte si pozor, aby velikost archivačního adresáře nepřekročila kapacitu

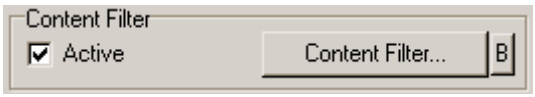
	vašeho pevného disku.
Archive Path	Nastavuje adresář, do kterého bude ukládána pošta.

Tabulka Security

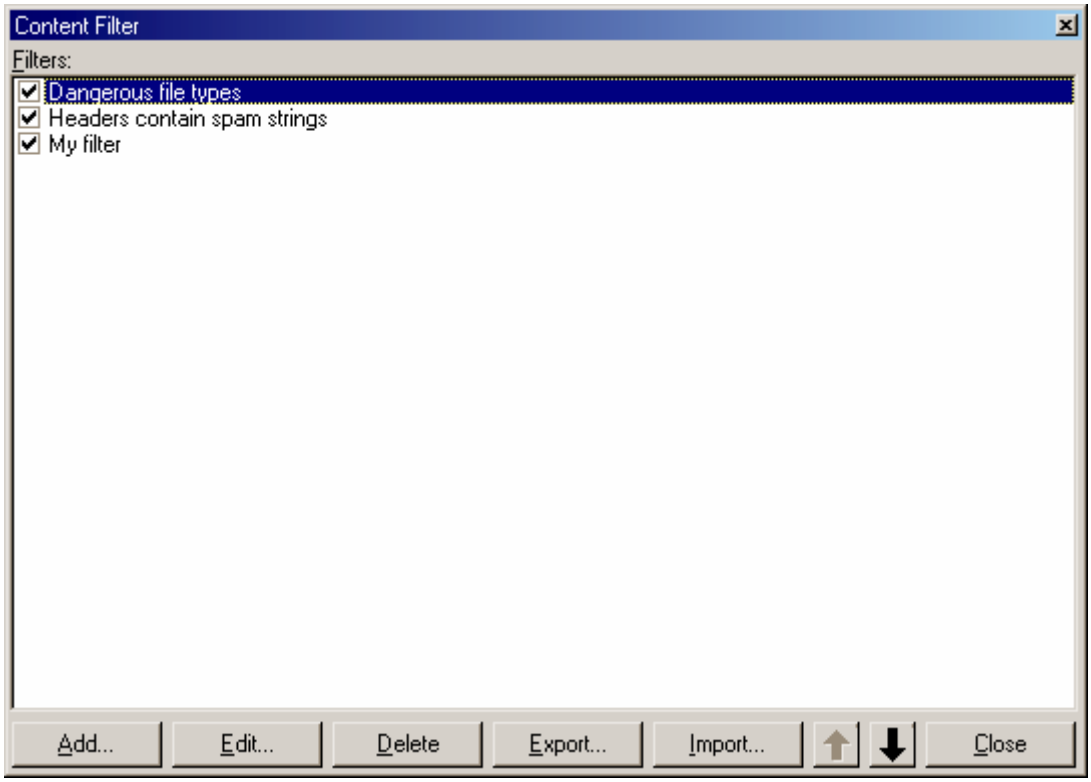


Tato tabulka Vám umožnuje nastavit velmi učinná nastavení ohledně zabezpečení.

Tabulka Security (Nastavení obsahových filtrů – Content Filter)



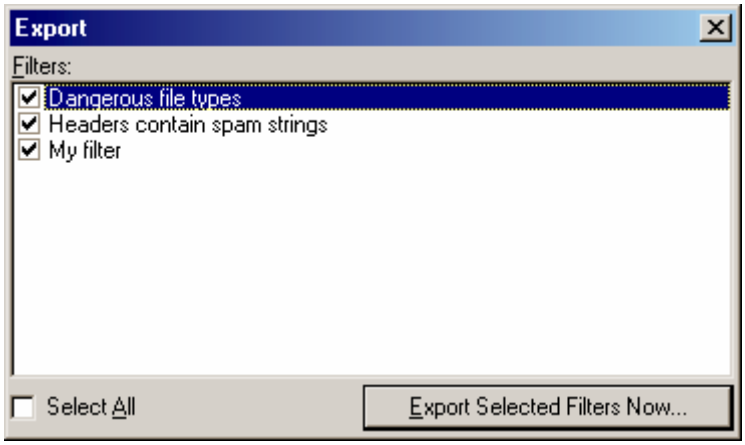
Merak má velmi důmyslný filtr pro kontrolu obsahu, umožnuje kontrolovat a filtrovat příchozí Poštu. Celý filtr je založen na obsahu Emailu. Email může být předán, vymazán, odmítnut, nebo povolen. Na základě tohoto filtru může být také spuštěn buď program, nebo dynamická knihovna. Pomocí i neodborné logiky můžete vytvořit filtr pro emailové přílohy. Filtry jsou platné pro všechny emaily, které projdou přes Meraka (příchozí i odchozí). Aktivujte filtr a pro jeho editaci klikněte na funkci „Content Filter“.



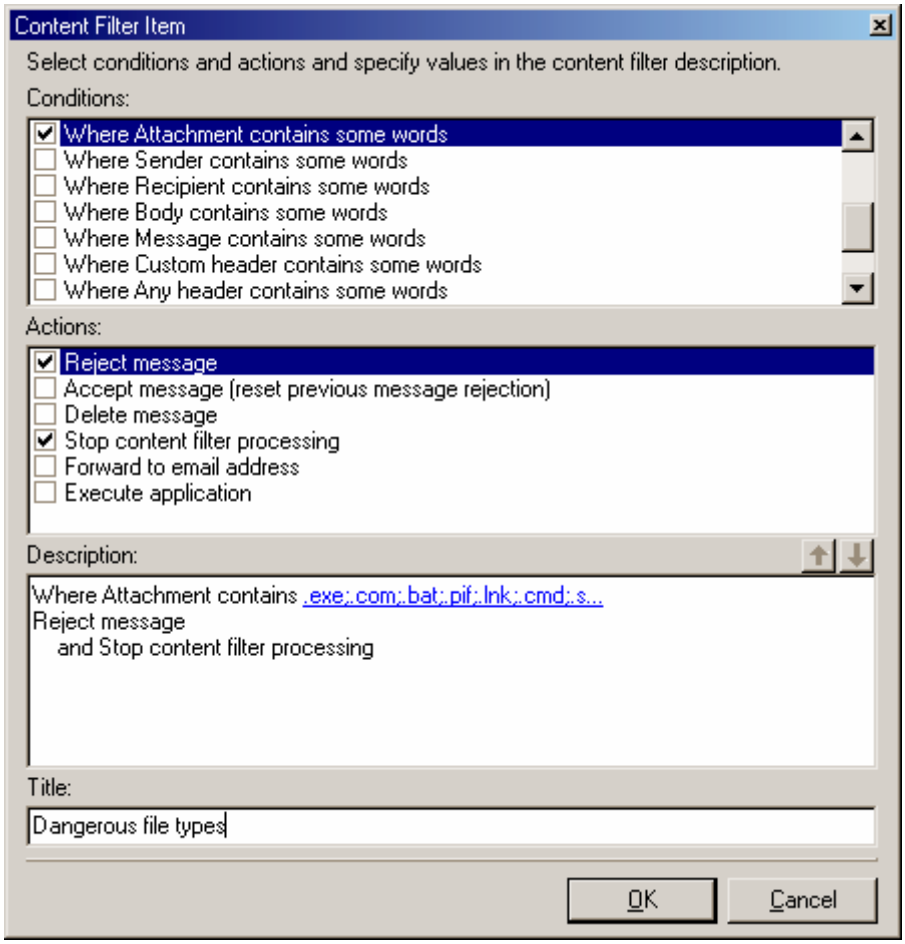
Pole na levé straně umožní aktivovat, nebo deaktivovat daný obsahový filtr. Filtry můžete přidávat/mazat/editovat. Pomocí šipek je také můžete přesouvat nahoru a dolů.

Velkou výhodou filtrů je, že můžou být exportovány, nebo importovány z jiného Meraka.

Importovat soubory můžete z XML souboru, nebo můžete filtry jednoduše do XML souboru exportovat a sdílet s ostatními.



Editace a oddělení obsahových filtrů



Toto okno Vám umožňuje kompletně nastavit celý filtr.

Pole	Popis
Conditions	Pole condition obsahujhe všechny podmínky, který můžete použít k filtrování zpráv. Jednodušek klikněte na zaškrtávácí pole a podmínka bude přidána do Vašeho filtru. Pro přidání více podmínek stejného typu, použijte dvojklik. Po přidání podmínek, je někdy nutné je blíže specifikovat. Pro bližší specifikaci stačí kliknout na odkaz dané podmínky. **Attachment (Příloha)** Nastaví celé jméno přílohy ve zprávě. **Sender & Recipient (Odesilate a příjemce)** Specifikuje skutečné jméno odesilatele a příjemce v SMTP spojení (MAIL FROM a RCPT TO) **Message & Body (Zpráva a tělo)** Nastavení specifikuje celou dekódovanou zprávy, tělo je hlavní část zprávy. **Custom Header (volitelná hlavička)** Umožní vám nastavit Vaší vlastní MIME hlavičku zprávy. Do textového pole ale musíte zadat přesný formát zpráv např. “X-Mailer: Web Mail”. **Any Header (jakákoliv hlavička)**

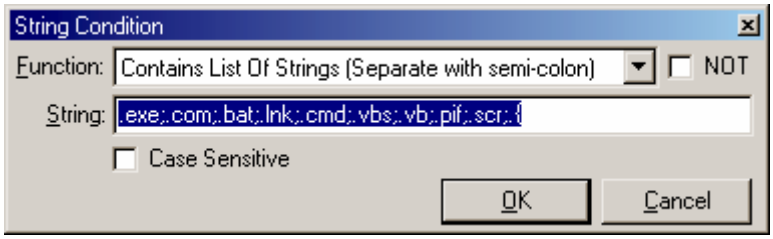
	Umožňuje nastavit celou hlavičku
Actions	Obsahuje seznam všech akcí, které můžete použít pro filtrování zpráv. Pomocí zaškrtávacích polí můžete přidat, nebo odebrat jednotlivé akce z popisu. Některé akce obsahují odkaz pro doplnění nastavení.
Description	Tato oblast je společná pro všechny filtry. Klikáním na odkazy můžete nastavit přesné parametry filtrů. Pomocí šipek v horní části dialogu můžete přesouvat jednotlivé podmínky nahoru a dolů.
Title	Nastaví popis jednotlivých obsahových fitlrů. Tento popis bude také zobrazen během SMTP spojení při odmítnutí zprávy.

Podmínky (Conditions)

Pomocí podmínek můžeme nastavit více funkcí jednotlivých filtrů. Každý filtr souvisí s následujicím a předchozím filtrem pomocí boolean operátora A, Nebo. Můžete tedy použít tolik fitrů, kolik potřebujete.

Pro nastavení akce a jednotlivých podmínek klikněte na odkaz v Description (popisové) části dialogu. Všechny dialogy jsou řešeny velmi intuitivně. Vše co potřebujete je vysvětlení jednotlivých podmínek.

Řetězcové podmínky (String Condition)



Pole	Popis
Function	Nastavuje funkcí provedenou při nalezení shody s obsahovým filtrem. **Contains List (Obsahuje seznam řetězců)** Nastaví seznam jednotlivých řetězců, které se mají ve zprávě vyhledávat. Jednotlivé řetězce jsou odděleny pomocí středníků. **Contains (Obsahuje)** Zkouši vyhledat konkrétní řetezec **RegEx** Používá technologii GNU Regular Expressions. Pomocí této technologie je možné velmi efektivně filtrovat jednotlivé zprávy. Příklad: Nastavení `(!){4,}$` Bude vyhledávat 4 nebo více ! na konci testovaných řetězců.

NOT	Negace pro celou funkci
String	Specifikuje hodnotu řetězce pro porovnání

Statické filtry

Statické filtry jsou vlastně speciální DLL filtry, které jsou nahrané do paměti a pokaždé, když je přijmuta zpráva jsou na ní aplikovány. Formát DLL je stejný, jako Content Filter DLL soubory používající Cdecl paramtery.

Statický filter je uložen v souboru **config\staticfilters.dat** a má následující strukturu:

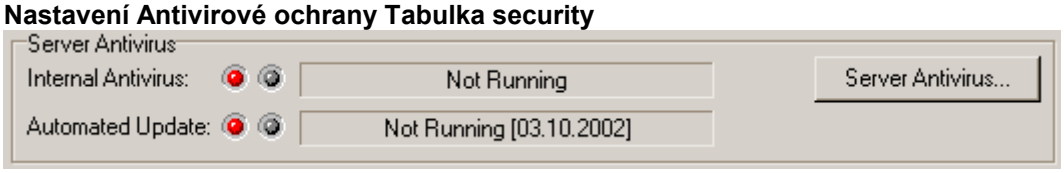
```
Title=<nadpis>
Filter=<plna ceska k dll knihovne>
Message=<zprava, ktera je zobrazena v SMTP spojeni>
SMTPMessage=<zprava, ve ktere je obsazen SMTP navratovy kod>
Enabled=<[0,1] pokud chcete vypnout filter, pouzijte '0'>
```

Více filtrů je odděleno mezerou. Nyní můžete použít RegEx filter, který je programován společností Doug Swallow a nemusíte používtvat Obsahový filtr.

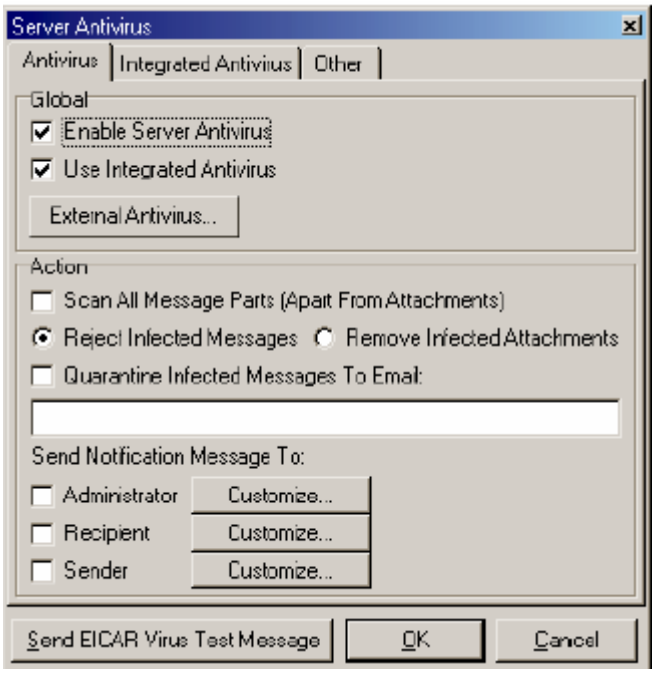
Příklad:

```
Title=Reg Ex Filter
Filter=c:\filters\mregexflt.dll
Message=Reg Ex Filter Rejection
Enabled=1

Title=LF Filter
Filter=c:\filters\lffilter.dll
Message=Contains bare LF
SMTPMessage=551 5.7.1 Message contains bare LFs (violates RFC822)
Enabled=1
```

Nastavení Antivirové ochrany Tabulka security

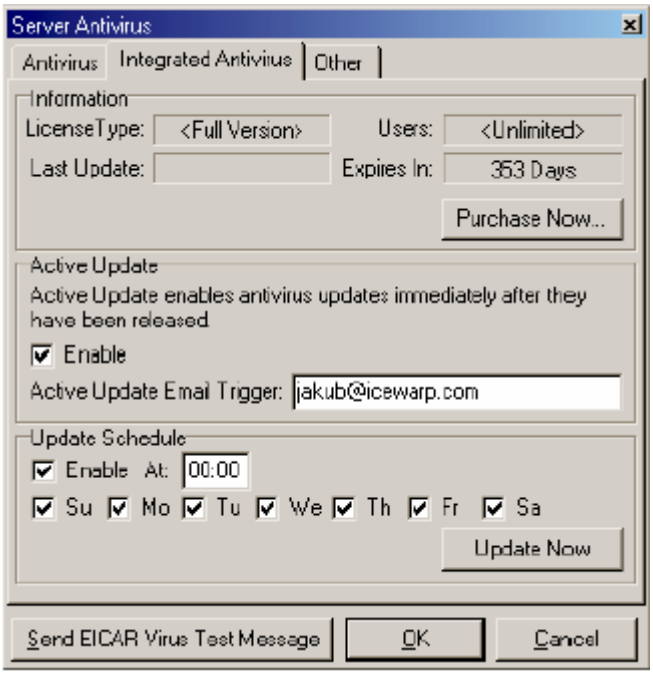


Sekce obsahuje tlačítko Server Antivirus, které je určeno pro konfiguraci antivirového jádra. Pomocí statových indikátorů je možné zjistit, zda je aktivní integrovaný antiviru a zda je zapnutá automatická aktualizace.

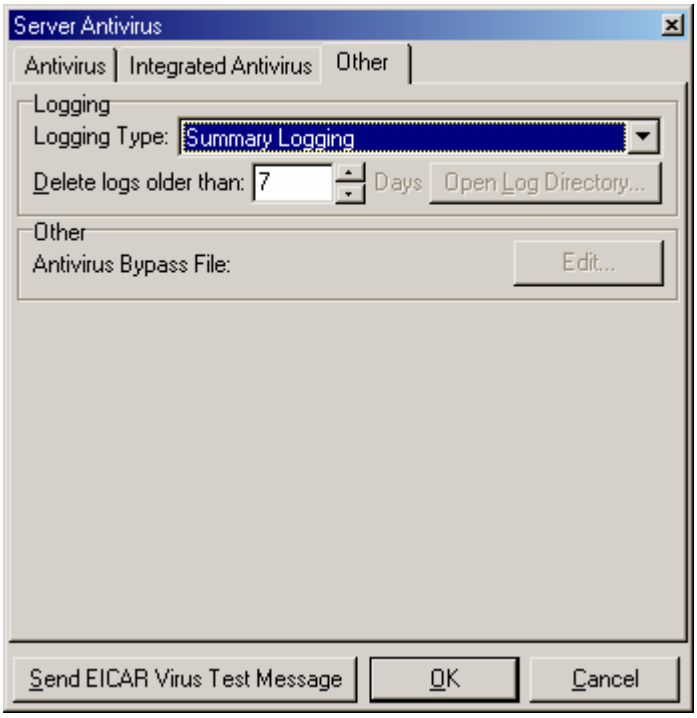


Merak podporuje plnou antivirovou kontrolu a má integrované antivirové jádro Avast. Po provedeni konfigurace antiviru můžete vyzkoušet jeho funkčnost pomocí tlačítka „Send EICAR Virus Test message“.

Pole	Popis
Enable server Antivirus	Od chvíle, kdy aktivujete toto pole, budou procházet všechny zprávy antivirovou kontrolou. Právě toto je pole, které zabezpečí váš server proti virům.
Use Integrated Antivirus	Pomocí tohoto pole aktivujete integrované antivirové jádro. To je velmi rychlé a je schopné prověřovat velké množství souborů najednou.
External Antivirus	Pomocí této funkce můžete nastavit používání externího antivirového programu. Pro více informací prosím prostudujte část o antivirech.
Scan All Messages Parts	Po aktivaci této funkce budou proti virům prověřovány všechny části e-mailových zpráv. Většinou se prověřují pouze přílohy zpráv. Mnohem efektivnější ale je scanovat celou zprávu.
Reject / Remove	Standardně jsou všechny zprávy obsahující virus odmítnuty. Někdy ale nechcete takovou zprávu odmítnout, ale pouze vyjmout virus a zbytek zprávy doručit příjemci. V takovém případě zvolte funkci Remove.
Quarantine Infected Messages	Merak umožňuje nastavit pro infikované zprávy karanténu. Tato funkce funguje tak, že přesměruje infikovanou zprávu na vámi specifikovanou e-mailovou adresu. Adresa může být jak lokální, tak externí. Je možné specifikovat více adres a oddělit je pomocí středníku.
Notification to Administrator / Recipient / Sender	Zde můžete nastavit upozorňování v případě odhalení viru v poště. Upozornění může dostávat administrator serveru, příjemce zprávy a odesilatel. I

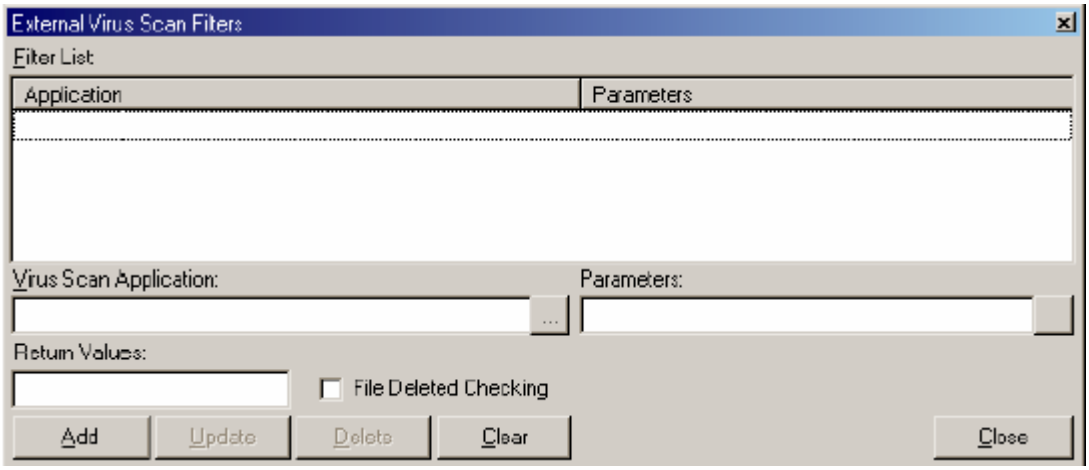


Pole	Popis
Active Update Email Trigger	Systém Active update zajistí update virové báze antiviru hned po jejím vypuštění. K tomu ale potřebujeme uchovat vaši e-mailovou adresu na našich serverech. Ve chvíli vypuštění nové virové báze bude na zde nastavený e-mail odeslána zpráva, která ihned po přijetí serverem spustí automatický aktualizační proces.
Update Schedule	Aktualizaci virové báze je možné plánovat.



Pole	Popis
Bypass Files	Jako u ostatních nastavených filtrů je možné i u antiviru nastavit překlenovací soubory (Bypass Files). Výsledkem správného nastavení překlenovacího souboru bude neprověřování nastavených zpráv antivirovou kontrolou. Nastavení musí obsahovat e-mailovou adresu, IP adresu, nebo ostatní možné nastavení ke specifikaci.
Logging	Logování u antiviru umožňuje sledovat všechny údálosti spojené s antivirem v logách. Antivirové logy jsou uloženy v adresáři Logs\Antivirus. Můžete nastavit automatické mazání logů starších než daný počet dnů. Debug – Loguje všechny události včetně jmen jednotlivých souborů Summary – Loguje pouze infikované souboru, jejich jména a stahování update balíčků

Nastavení externích antivirových řešení



Poznámka: Pro uživatele Windows 9x a antivirů využívajících dosovskou příkazovou řádku, vždy nastavte následující:

- vytvořte odkazovací link (soubor s koncovkou pif) ke spustitelnému souboru
- Nastavte ve vlastnostech linku automatické uzavření okna po dokončení
- Použijte tento link jako spouštěcí soubor

Klikněte na tlačitko „Virus Scan Filters“ . Tím vyvoláte konfigurační panel, kde můžete přímo nakonfigurovat parametry vámi používaného antivirového programu.

- Do pole „**Virus Scan Application**“ zadejte cestu a název spuštěcího souboru.
- Do pole „**Parametrs**“ zadáte parametry příslušného antivirového programu
- Položka „**Return Values**“ může být buď prázdná (v tom případě je interval 1-*), nebo můžete specifikovat vlastní návratový kód. Např. 1,2,4,8-255. Prostudujte si výchozí kódy vámi používané antivirové aplikace. Pro antivirus také můžete nastavit timeout. TIMEOUT=0, nebo TIMEOUT=30. Standardně je timeout nastaven na 30 sekund. Pokud nastavíte 0, timeout zůstává nenastaven.
- Funkce „**File Deleted Checking**“ je pro takové antiviry, které nevrací správně svoje výchozí kódy. V takovém případě mu tato funkce řekne, aby infokované soubory smazal. Merak to rozpozná a bude předpokládat, že soubor je infikovaný. Doporučujeme tuto funkci použít

s programem Norton Antivirus.

Parametry jsou u každého antivirového programu jiné. Pro každý antivirový program je ale dobré používat paramtery pro vypnutí scanování paměti a boot sektoru disku, parametry pro prověřování archivních souborů (.zip a .arj souborů).

- **Enable virus scaning and test** . Jedna z nejtěžších věcí je najít správný virus k testování funkcní Meraka. Naštěstí ale máme k dispozici testovací virus zvaný Eicar (http://www.eicar.org) . Testovací soubor není ve skutečnosti virus, který by vám mohl z nějakých důvodů ublížit. Při testování nemusíte mít strach.

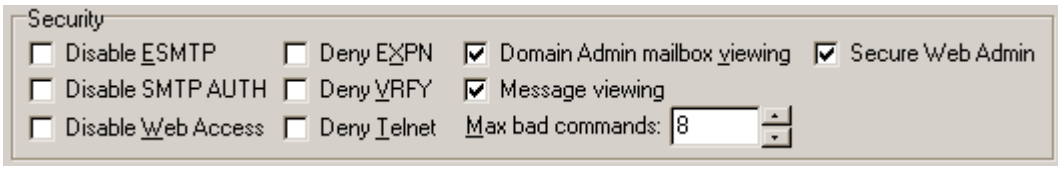
Pomocí kláves CTLR+C a V prosím okopírujte následující řetězec do poznámkového bloku a uložte ho jako eicar.com. Přiložte ho k emailu, který zkuste následně poslat přes Meraka. Vzkaz by měl být odmítnut.

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Pro další příklady nastavení si prosím prohlédněte přílohu o Nastavení antiviru

Můžete si také sami zvolit antivirový e-mail pomocí soubor **Config\virusmsg.txt**

Popis ostatních polí v tabulce Security



Popis	Pole
Deny Telnet	Tato položka zabraňuje komukoliv připojit se na porty používané Merakem přes telnet a možnost zasahovat tak normální klávesnicí. Měli byste tuto položku nechat vypnutou, protože náš tým technické podpory vám nebude v případě nutnosti testování vašeho mail serveru schopen pomoci.
Disable Web Admin	Tato položka zabraňuje komukoliv používat administrační webové rozhraní (to standardně pracuje na portu 32000). Na obrazovku uživatele bude zobrazena hláška „Access Denied“ (přístup odepřen).
Disable SMTP AUTH	Pokud tuto funkci vypnete, server nebude přijímat autentifikovaná SMTP spojení. Vypnutím této funkce umožníte uživatelům zvolit si cestu autentifikace jejich odchozí pošty. Merak podporuje tyto AUTH schémata: LOGIN, PLAIN, CRAM-MD5
Domain Admin mailbox viewing	Pokud je tato funkce zapnuta, bude moci doménový administrátor číst obsah uživatelských emailových schránek.
Web Admin Message	Pokud je tato funkce zapnuta, povolíte doménovým administrátorům a i administrátorům samotným číst obsahy ostatních uživatelských schránek.

Viewing	
Secure Web Admin	Pokud je tato funkce zapnuta, je u všech souborových cest provedena kontrola umístění v adresáři Config. Tato kontrola je prováděna nad webovým rozhraním. To zabrání uživatelům v přístupu k důležitým souborům.
Deny EXPN	Tato položka zabraňuje komukoliv používat funkci EXPN (expanduje a vrací uživatele do mailing listů). Pokud vzdálený server bude chtít použít příkat EXPN Merak bude odpovídat chybovou hláškou „not supported“ (není podporováno). Tuto funkci doporučujeme mít zapnutou.
Deny VRFY	Toto nastavení zabrání každému používat při obsluze příkaz VRFY, tím kontrolujeme, zda na vašem serveru existují konkrétní uživatelský účet, či nikoliv. Pokud vzdálený server bude chtít tento příkaz použít, Merak odpoví chybovým hlašením „not supported“ (není podporováno). Tuto funkci můžete nechat deaktivovanou.
Hide IP From Received Header	Tato funkce umožňuje skrýt IP adresu v hlavičce zprávy. Pokud tuto funkci použijete, nebude nikdo schopen zjistit konfiguraci Vaší lokální sítě.

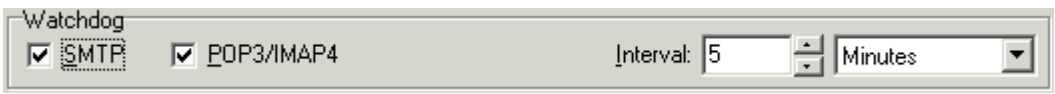
Tarpitting pole tabulka Security

Merak nabízí jednu výbornou funkci, které říkáme tarpitting. Když je Tarpitting aktivní, kontroluje nezdařené pokusy o doručení emailů neznámým uživatelům externími nebo na systému neexistujícími uživateli. Pokud počet pokusů převýší vámi zadanou hodnotu v „Count“ poli, systém si bude pamatovat IP adresu a po čas uvedený v poli „Period“ nebude mít tato IP adresa povolený vstup do systému.

Tato funkce poskytuje v podstatě výbornou ochranu proti pokusům spammerů spamovat účty, existující na vašem mail serveru. Spameři většinou mají většinou slovníky aliasů, kterými se pokouší doručovat na emailové účty zprávy. Jednou překročí počet neznámých aliasů vámi definovaný limit a spameři nebudou schopni vás v daném časovém rozmezí spamovat
Někdy byste možná chtěli umožnit nějakým IP adresám možnost nečekat, dokud vámi definovaná lhůta nevyprší. V tomto případě budete muset mít hexa editor a editovat konfigurační soubor config\tarpid.dat. Vyhledejte si vámi požadovanou IP adresu, a přepište
IP řetězec na nějaký jiný (potřebujete změnit pouze první znak, aby byl změněn celý řetězec). Každý záznam v tomto souboru má délku 64 bajtů. Musíte si být jisti tím, co děláte, abyste nepoškodili soubor.

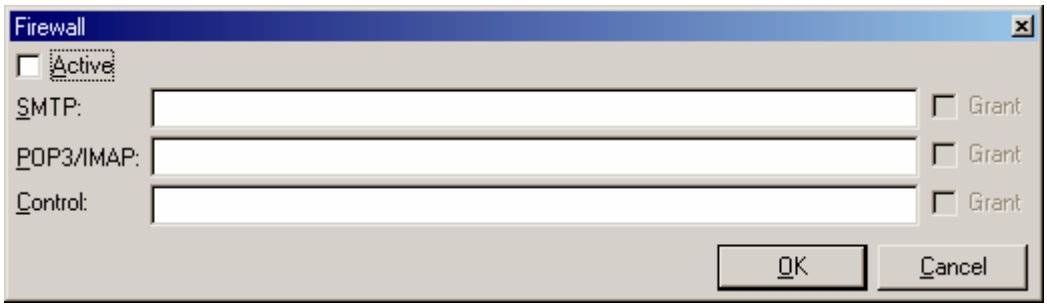
Watchdog funkce tabulka Security

Merak nabízí také funkci Watchdog. Ta sama kontruluje, jestli jsou základní emailové služby Aktivní.



Pro správné fungování funkce Watchdog musí také běžet služba „Controls“. Kontrolní služba bude ověřovat (v nastaveném časovém intervalu), jestli jsou požadované služby stále spuštěné. Pokud nebudou, bude je automaticky restartovat.

Nastavení firewallu

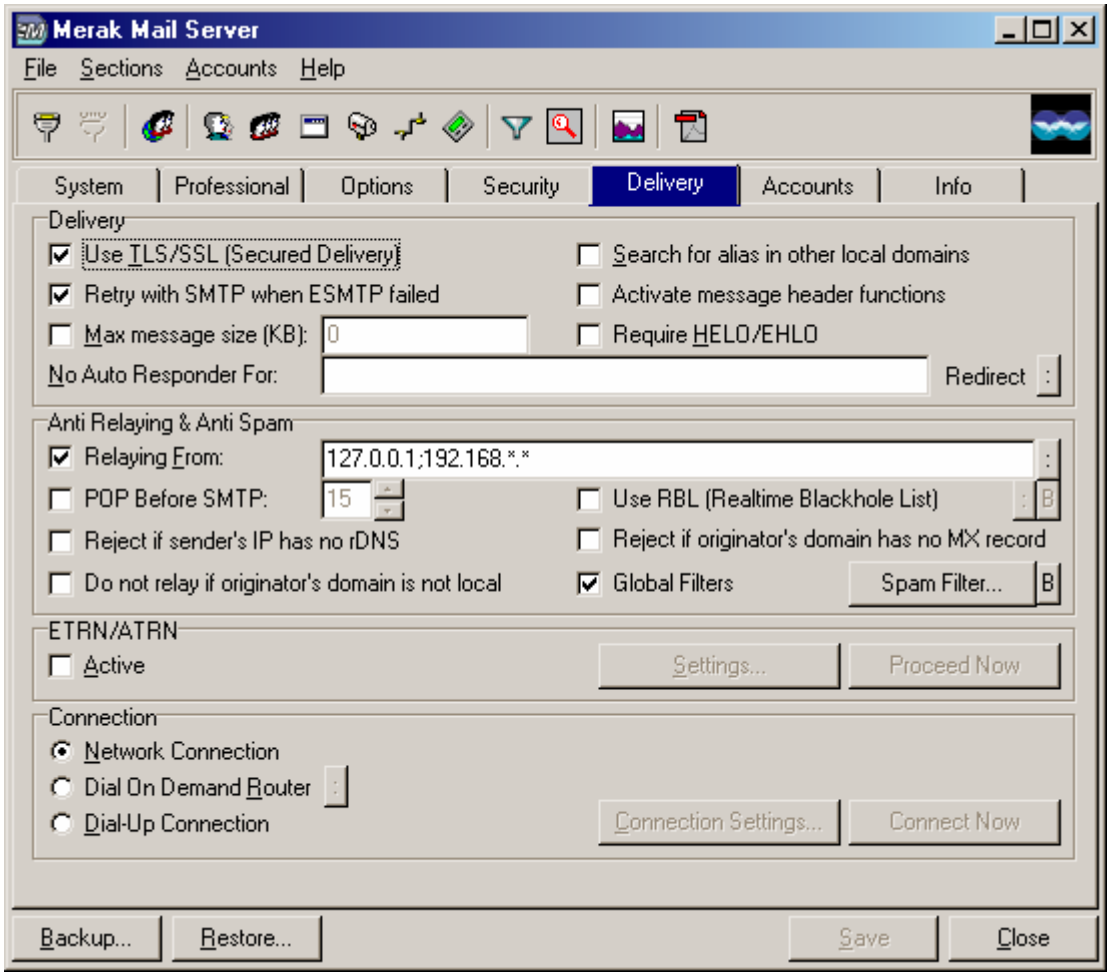


Pole	Popis
Firewall active	Tato volba umožní funkčnost firewallu, který je definován v následujících třech polích. Nejedná se zde o anti relayingové možnosti. Je to firewall, který umožní specifickým IP adresám schopnost připojit (či nepřipojit) se na mail server. Nemluvíme tady o posílání, nebo přijimání emailových zpráv. V nastavení firewallu mluvíme o možnosti vůbec se připojit. Pokud je pole „Grant“ umístěné napravo od hlavního pole nezaškrtlé, nebude se moci seznam IP adres zadaných v poli vůbec na váš emailový server připojit, pokud je pole Grant zaškrtlé, bude se moci naopak připojit pouze seznam IP adres zadaných v poli.
SMTP - POP3/IMAP4 – Control	Tyto pole, jak jsme již uvedli výše jsou použity pro definování konkrétních IP adres, nebo podsítí. Formát zadání může být aaa.bbb.ccc.ddd, *.*.*.*., Nebo rozsah a-b.*.*.* . Hvězdičkami myslíme specifikaci podsítě, mínus definuje rozsah mezi a a b. Zadání oddělujeme středníky.

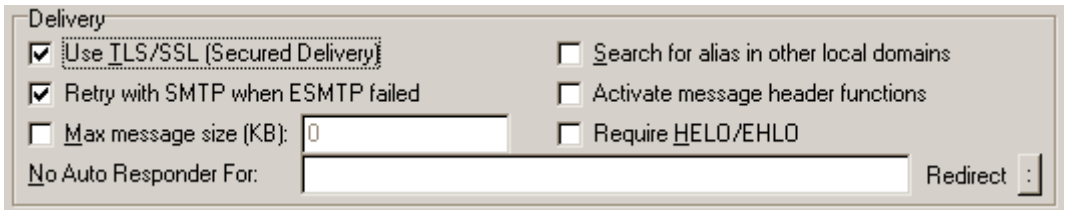
Tabulka Security funkce Auto Archive

Pole	Popis
Active	Funkce Auto archiv umožňuje automatickou archivaci všech zpráv doručených na server pomocí SMTP a IMAP protokolu. Všechny zprávy budou online zrcadleny z adresáře MAIL, do kterého jsou ukládány všechny servery doručené na server. Archviní adresář můžete velmi jednoduše procházat a zprávy v případě potřeby mazat. Dejte si ale pozor, aby nedošlo k přeplnění Vašeho peveného disku.
Archive Path	Nastaví cestu k archivnímu adresáři.

Tabulka Delivery



V pořadí čtvrtá tabulka (Delivery) umožňuje konfiguraci ještě několika bezpečnostních funkcí a klíčových funkcí serveru



Pole	Popis
Use TLS/SSL	Pokud tuto funkci zapneme, budou všechny odchozí zprávy odesílany pomocí STARTTLS ESMTP příkazu. Pokud vzdálený server, na který odesíláme email bude podporovat technologii TSL/SSL, budou zprávy odeslány pomocí zabezpečeného rozraní Secure Socket Layer (SSL). Ten je podobný protokolu https protokolu. Zprávy nejsou odeslány jako prostý text a nikdo tedy nemůže monitorovat TCP/IP protokol. Všechna spojení probíhající mezi Merakem a Merakem jsou kompletně zabezpečeny. Doporučujeme tento parametr používat.

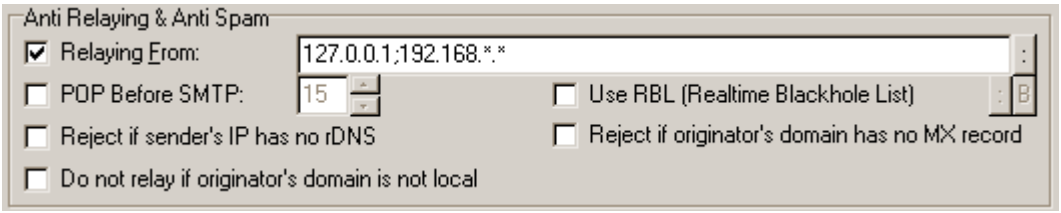
Retry with SMTP when ESMTP failed	Na sítích fungují různé soutery, nebo proxy servery, které nemají úplně správně implementovaný standard RFC821 a nepodporují funkce SMTP EXTENSIONS. V čem je tedy problém. Když Merak odesílá zprávu, snaží se standardně používat tyto funkce. Problém nastane ve např. chvíli, kdy extensions funkce používá i cílový SMTP server, ale neumí je proxy server, který je umístěn mezi nimi. Pokud tuto funkci aktivujete, Merak problém pozná a pokusí se zpracovat zprávy pomocí planého protokolu SMTP, který většina proxy serverů i routerů, které by byly v normálních případech problematické, podporuje.

Pole	Popis
Max message size	Specifikuje maximální velikost zprávy, která může být přes váš server odeslána. Zpráva, která bude větší bude serverem odmítnuta.
Search for alias in other local domains	Pokud je zpráva zaslána na adresu xyz@domain.cz, ale xyz je neznámý alias, bude Merak (pokud zapnete tuto funkci) kontrolovat alias i v jiných doménách. Takže pokud server najde někoho s aliasem xyz@jinádoména.cz zašle email tomuto uživateli namísto uživatele prvního. Používání této funkce může být někdy nebezpečné.
Activate Message Header Functions	Pokud tuto funkci nastavíte jako aktivní, bude Merak sledovat speciální hlavičky (jako např. “Return-Receipt-To” a “Deffered-Delivery”. Pokud bude přijmuta zpráva, která bude obsahovat hlavičku “Return-Receip-To” Merak automaticky sdělí uživateli, že byla jeho zpráva přijmuta. Upozornění: Toto není stejná funkce oznámení o doručení, kterou obsahuje Outlook. Odklad doručení definuje, kdy má být zpráva doručena (pouze u odchozích zpráv).
Require HELO/EHLO	Pokud tuto položku nastavíte, SMTP server bude vždy na začátku spojení vyžadovat od vzdáleného serveru (nebo mailového klienta) jeho představení pomocí příkazu HELO nebo EHLO. V případě, že se server (nebo klient) nepředstaví, Merak od nich nebude přijímat žádné zprávy.

Redirect	Pomocí tohoto nastavení můžeme velmi jednoduše předávat automaticky zprávy z jedné e-mail adresy na druhou. Všechno nastavení je uloženo v souboru **redirect.dat**, který má následující formát:
	`{email}={email}`
	`{domena}={email}`
	`{domena}={domena}`
	
	Příklad:
	`info@icewarp.com=info@business.com`
	`sales@luko.com=info@business.com`
	
	Toto nastavení bude mít za následek, že po přijmutí zprávy na účet info@icewarp.com bude zpráva automaticky předána na info@business.com. Stejně tak, jakmile bude přijata zpráva na sales@luko.com bude předána na info@business.com.

No Auto Responder	Toto nastavení specifikuje domény, ve kterých nebude možné používat funkci automatického odpovídače. E-mail adresy a domény jsou odděleny pomocí středníků.

Popis doručovacích funkcí v tabulce Delivery



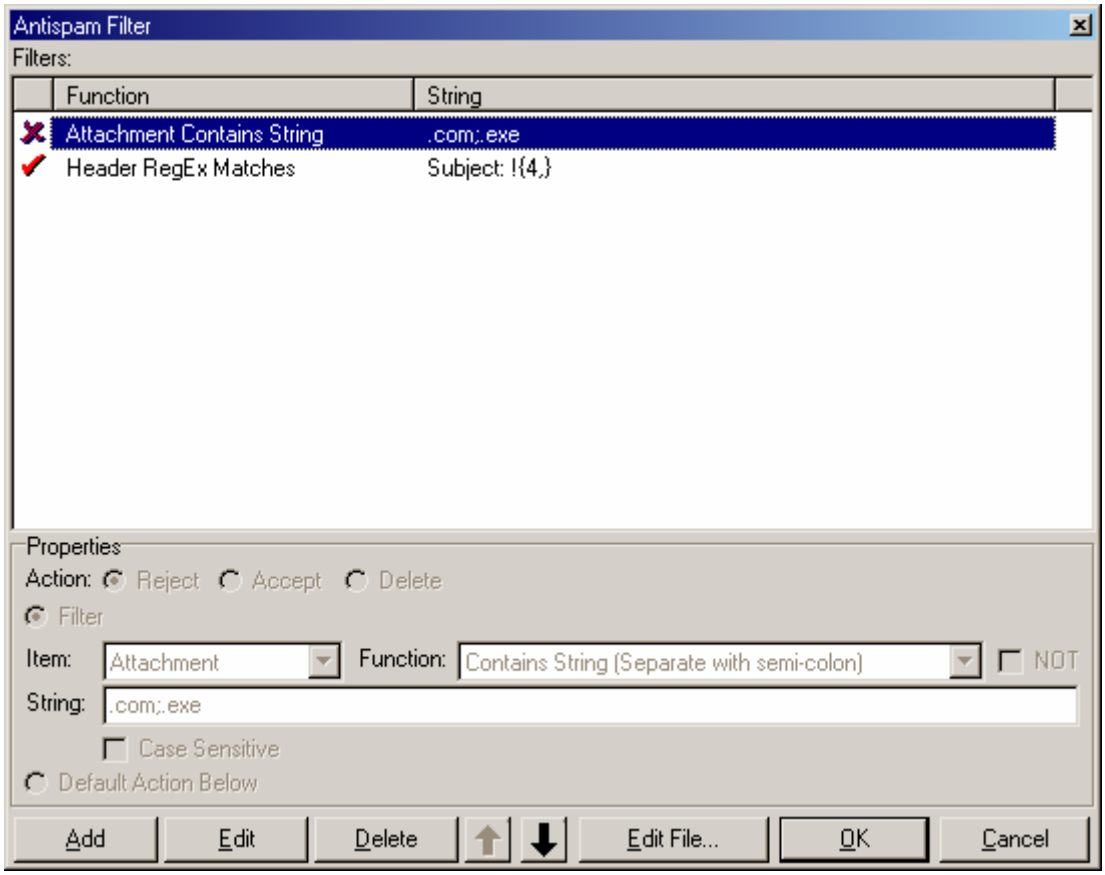
Pole	Popis
Do not relay if originator's domain is not local	Merak bude přeposílat pouze zprávy z domén nastavených na vašem serveru. Nebude možné odesílat zprávy z prázdné e-mailové adresy. Tuto funkci však nedoporučujeme používat.
Relaying from	Pokud je tato funkce nastavená, mají povolené odesílat přes mail server zprávy pouze v tomto poli specifikované IP adresy. Lokální IP stroje (127.0.0.1) by mělo být vždy nastaveno. IP adresy a domény jsou odděleny středníkem Například: 192.168.1.*;127.0.0.1;194.213.224.5-20 Pokud máte větší počet záznamů, bude možná snažší nastavit specifikaci IP adres a domén přímo v konfiguračním souboru relay.dat (umístěném v konfiguračním podadresáři). Formát každého záznamu je v tomto případě na odděleném řádku. Například: 192.168.1.* 127.0.0.1 Toto je nejvíce účinné a bezpečné nastavení k ochraně proti SPAMU. Buďtě si jisti tím, co nastavujete a nevypínejte tuto funkci. Je opravdu potřebná. Prosím přečtěte si přílohu o relayingu (předávání zpráv) a hlášce we do not relay
POP3 before SMTP	Jestliže se klient připojí na službu POP3 nebo IMAP4 (pro kontrolu emailů) a správně se autentifikuje, systém si po dobu určitého časového rozpětí, které je možné specifikovat v tomto nastavení zapamatuje klientem používanou IP adresu. Během tohoto rozpětí má klient povolené používaná SMTP služby. Časové rozpětí je specifikováné v minutách. Toto nastavení nebude mít vliv ze standardním relayingem.
Reject if originator's domain has no MX record	Další bezpečnostní kontrolou je kontrola pravosti e-mailových adres u příchozích emailových zpráv. Jedním ze způsobů, jak ověřit pravost e-mailové adresy je ověřování MX záznamu (Mail Exchange) v DNS serveru. Pokud tuto funkci aktivujete, Merak bude provádět MX Lookup a jestliže nebude pro danou doménu existovat MX záznam, bude zpráva odmítnuta. Pokud ale nebudete mít správně nakonfigurován váš DNS server může vam tato funkce ublížit.
RBL - Realtime Blackhole list	RBL je služba, která poskytuje seznam známých Spammerů. Pokud je odesilatel nalezen na tomto seznamu, budou všechny zprávy od něho odmítnuty všechny zprávy. Poskytovatele RBL seznamu můžete specifikovat v souboru rbl.dat (v

konfiguračním podadresáři), který můžete otevřít použitím tlačítka . .
Každá doména poskytovatele je v tomto konfiguračním souboru na odděleném řádku.
Doporučujeme vám používat server rbl.maps.vix.com. Do souboru můžete zadat i jiné poskytovatele, které naleznete na internetu. Jedním z takových je například blackhost.mail-abuse.org.

Pokud potřebujete vypnout u některých IP adres kontrolu z RBL serveru, můžete je zadat v souboru jménem config\rblbypass.dat. Tento soubor obsahuje IP adresy, které nebdou kontrolovány.
Možné RBL servery:

```
bl.spamcop.net
relays.ordb.org
orbs.dorkslayers.com
dev.null.dk
relays.osirusoft.com
relays.visi.com
blackholes.wirehub.net
dynablock.wirehub.net
proxies.relays.monkeys.com
ipwhois.rfc-ignorant.org
```

Globální a Anti spamové filtry



Toto nastavení určuje, který Global Anti Spam filter (globální antispamový filtr), Domain Anti Spam filter (doménový antispamový filtr) a Greeting fiter (zdravící filtr) by měl být použit. Touto cestou můžeme specifikovat oddělené filtry platné pro celý mailový server stejně tak, jako pro jednotlivé domény. Tyto filtry budou použity všechny společně spolu s uživatelským Anti-Spamovými filtry.

Uživatelský antispamový filter nesouvisí s tímto nastavením. Uživatelské antispam filtry jsou filtry pro oddělené účty. Globalní filtry mají větší prioritu v systému a budou zpracovány jako první. Jako poslední jsou zpracovány právě filtry jednotlivých účtů.

Struktura filter souboru:

Pro nastavení fitrů použijeme dialog. Někdy je ale také potřeba, abysme byli schopni analyzovat souboru, který obsahuje jednotlivé filtry.

Tento file je složen z jednotlivých anti spam filtru. Každý filter je umístěn na vlastním řádku. Obyčejně všechny filtry odmítnou všechny zprávy. Něky ale chcete některé zprávy přijmout. Pro tyto případy můžete použít předponu na začátku jednotlivých řádků:

0: - Odmítnout
1: - Akceptovat
2: - Smazat

Tím způsobíte vyjímku v daném filtru, toto nastavení ale nebude mít vliv na ostatní filtry.

Můžete také nastavit celou oblast filtrů pro příjímání, nebo odmítání zpráv jedním řádkem, který bude obsahovat 1 nebo 0. Který nastaví, že všechny následující filtry budou myšleny jako 0 (odmítnout) nebo 1 (přijmout).

Syntaxe filtrů:

Položky:

H - Hlavička
B - Tělo
A – Příloha
S - Odesilatel
R - Příjemce
I – IP adresa
Y – Jakákoliv hlavička

Funkce:

~ - Obsahuje
^ - RegEx
{ - Začít s
} – Končit s
= - Je
! - Není (Negující funce)
$ - Case sensitive (Citlivé na přesný řetězec)

Příklady fitrů:

```
A~.com;.exe;.bat;.cmd;.scr // Příloha obsahující jakoukoliv přílohoš
                              Nastavenými koncovkami
H~Subject: win;free;!!! // Hlavička obsahující specifikované řetězce
I=205.128.218.193 // IP Adresy
Y$^^Subject: WIN Free!!!$ // Jakýkoliv nastavený řetezec v hlavičce
(RegEx)
H!~Subject: money // Hlavička neobsahuje řetězec
205.*.*.193 // Shoduje se maska IP sítě
domain.com // Shoduje se doména odesilatele
bill*@domain.com // Adresa odesilatele se shoduje s nastavenou maskou
```

Další složitější příklady filtrů:

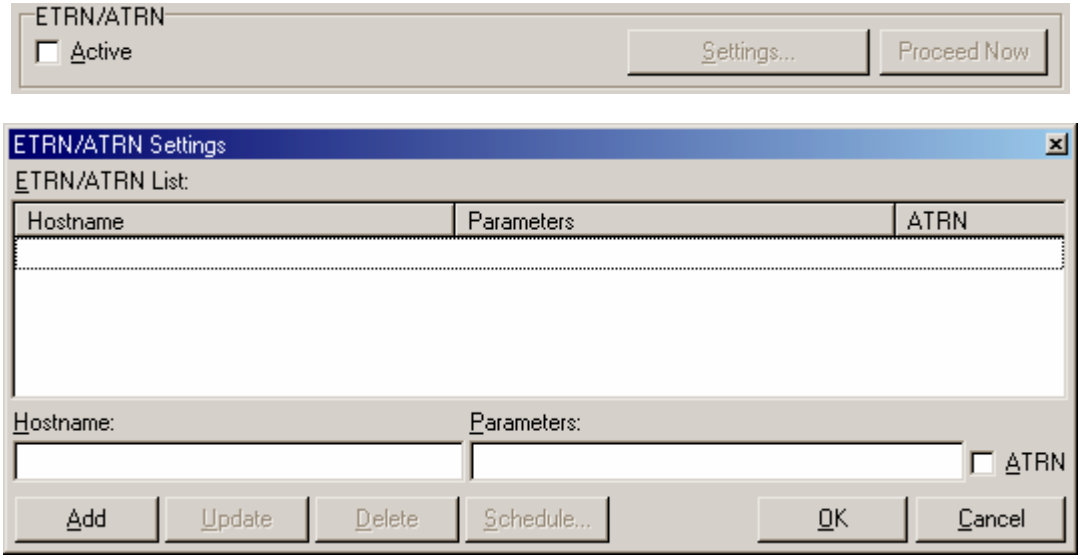
```
1:H~Subject: please help // Přijme zprávu, pokud subject obsahuje řetezec
                          „please help“
A~.com;.exe;.bat;.cmd;.scr // Odmítne všechny přílohy obsahující
1 // Akceptuje následující filtr
IP=192.168.0. // 1 Akceptuje zprávy z IP adresy 192.168.0.1
0 // Odmítne následující filtr
A~.vbs;.bat // Odmítne přílohy obsahující jakýkoliv definovaný řetězec
```

Je zde také greeting filter “zdravící filtr”, který nastavujeme v souboru config\heloehlo.dat. Tento filtr filtruje jména serveru, během HELO/EHLO příkazu v SMTP spojení. Můžete tedy velmi jednoduše blokovat servery, aniž byste znali jejich IP adresu. Tato funkce funguje pouze v případě, že jsou aktivované globální filtry.

Překlenovací soubory (Bypass files)

Merak podporuje vytváření tzn. Překlenovacích souborů (bypass files), pro antispamové filtry, obsahové filtry a pro interní doručování mezi jednotlivými doménamy. V praxi můžete vytvořit soubor s určitým specifickým obsahem, pomocí kterého můžete obejít jednotlivé filtry. Pokud bude příjemce uložen v jednom z překlenovacích souborů, bude daný filtr tuto zprávu ignorovat. Máme pět typů překlenovacích souborů: uabypass.dat, gabypass.dat, dabypass.dat, cbfbypass.dat a idbypass.dat. Jednotlivé soubory jsou určeny pro jednotlivé filtry: UA – uživatelský antispamový, GA – globální antispamový, DA – doménový antispamový, CF – obsahový filtr (content filtr). Překlenovací soubory by měli být umístěny v adresáři Merak\Config. Soubor musí obsahovat e-mailové adresy a domény, každou na novém řádku.

ETRN/ATRN



Pole	Popis
ETRN/ATRN	Pomocí tohoto pole nastavíme, standardní používání ETRN nebo ATRN příkazů pro host adresy specifikované v ETRN seznamu s danými parametry. Po stisknutí tlačítka ETRN se vám zobrazí dialogové okno, ve kterém můžete specifikovat host adresu a parametry pro provedení ETRN příkazu.

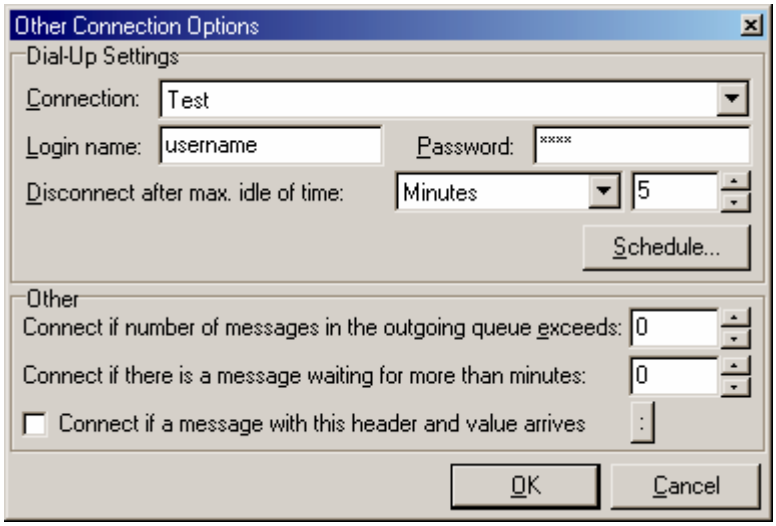
ETRN
Parametrem obyčejně bývá jméno domény. Merak umožnuje používat více, než jeden ETRN příkaz. Tyto funkce se používají, když se na vzdáleném serveru ukládají všechny e-mailové zprávy pro námi konfigurovaný server. Tím, že spustíte tuto proceduru, dáte vzdálenému serveru vědět, že náš server je právě připojen a vzdálený server pošle zpráva do fronty. Toto je klientská procedura. Merak má také implementované vlastnosti serveru pro ETRN frontu.
.

ATRN
Pokud potřebujete u Meraka použít funkce ATRN, zaškrtněte pole ATRN. ATRN používá k autentifikaci na vzdáleném server uživatelské jméno a heslo. Formát parametrů pro ATRN je následující: {domeny};{uzivatel}:{heslo}

Příklad:
icewarp.com;atrnuzivatel:atrnheslo

Pole nastavující spojení v tabulce Delivery

Pole	Popis
Network Connection	Specifikuje, zda je Merak připojen na internet přes síť. Pokud je tomu tak, nejsou žádná další nastavení potřebná. Tento typ připonení je preferován.
Dial on Demand Router	Toto pole je určeno pro uživatele s dial-up připojením k Internetu. Umožní nastavit restrikce pro spojení s Internetem. Merak by se po použití této funkce neměl pokoušet připojovat k Internetu dokud to nebude vyžadovat funkce “Schedule” (plánovač pomocí kterého je možné nastavit přesdnou hodinu, kdy má být spojení uskutečněno), nebo funkce “other connection options”. Dokud tyto funkce nebudou vyžadovat spojení, Merak se nebude připojovat. Možná budete chtít použít konfigurační soubor config\demand.dat ke spuštění nějaké aplikace před uskutečněním samotného spojení. Soubor obsahuje jediný řádek, který specifikuje aplikaci, která má být spuštěna a spouštěcí parametry.
Dial-Up Connection	Pomocí tohoto nastavení specifikujete nastavení dial-up spojení, které bude otevřeno ve chvíli, kdy to bude požadovat jedna z funkcí (Schedule, nebo other options.). Pokud je spojení již navázáno, Merak použije již toto vytvořené spojení (nebude ho přerušovat a vytáčet nové).



Kliknutím na položku “Other” získáte možnost nastavit ještě několik dalších upřesňujících nastavení.

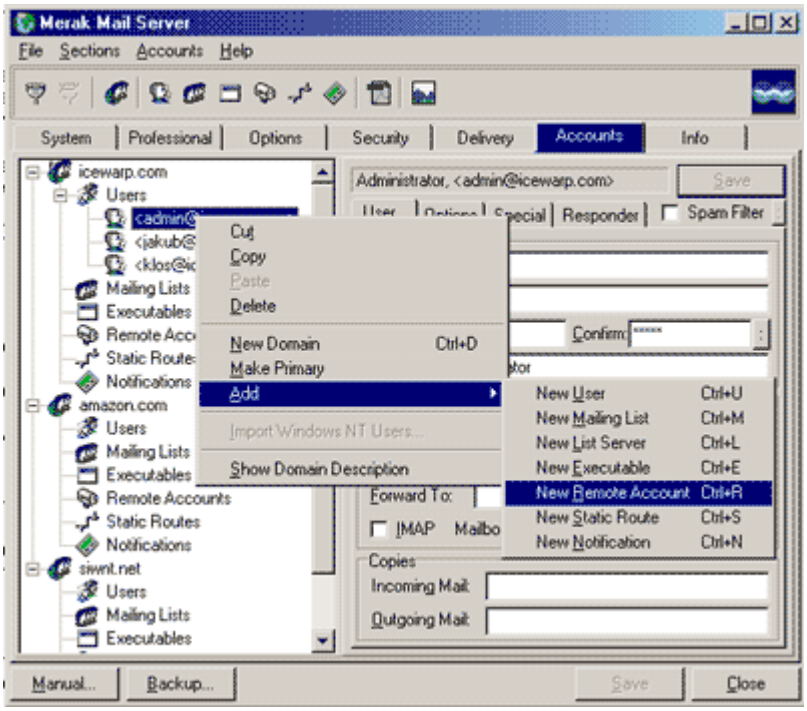
Pole	Popis
Login Name / Password	Nastavení uživatelského jména a hesla, které bude použito při spojení.
Disconnect after max idle time:	Pokud bude po nějakou dobu spojení neaktivní, Merak ho automaticky ukončí. V tomto poli nastavíme dobu, po kterou má být spojení neaktivní.
Schedule	Připojování na Internet může být naplánováno pomocí standardního plánovače. Plánovač, který nastavuje připojování na Internet předčí svoji prioritou plánovače ve vzdálených účetech (Remote Accounts). Je tím zajištěno, že spojení nebude navázáno díky vzdálených účtům.

Merak umožňuje nastavit vytváření spojení pokud počet zpráv v odchozí frontě přesahuje nastavenou hodnotu, pokud zprávy ve frontě čekájí nastavenou dobu, nebo pokud zprávy ve frontě obsahuje danou hodnotu v hlavičce. Díky poslednímu funkcí je možné nastavit automatické vytváření spojení, např. v případě, že někdo potřebuje odeslat zprávy z vysokou prioritou.

Jednotlivá nastavení hlaviček by měli být umístěné každý na nové řádce. Příklad:

```
Priority: High
X-Priority: High
```

Manipulace s účty



K základní správě účtů můžeme použit funkce **Cut, Copy** a **Paste**

Funkce **Delete** smaže účet. Nicméně smaže pouze konfigurační data. Samotný adresáře a data zůstanou uložena na disku. Je to opatření proti možným nehodám při mazání uživatelskcýh účtů.

Funkce **New Domain** vyvolá nabídku pro vytvoření nové domény a umožní přidat více domén.

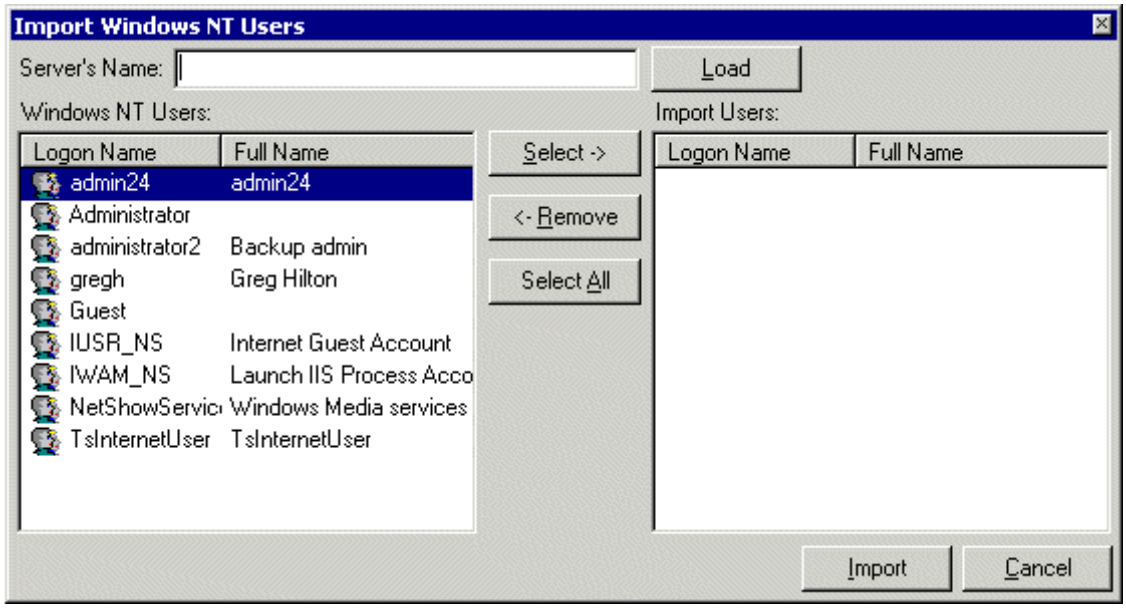
Funkce **Make Primary (vytvořit primární)** zkonvertuje zvolenou doménu na primární (primární je doména, která přijímá systémem generované zprávy).

Funkce **Add (Přidat)** umožňuje vytvořit v systému nový uživatelský účet.

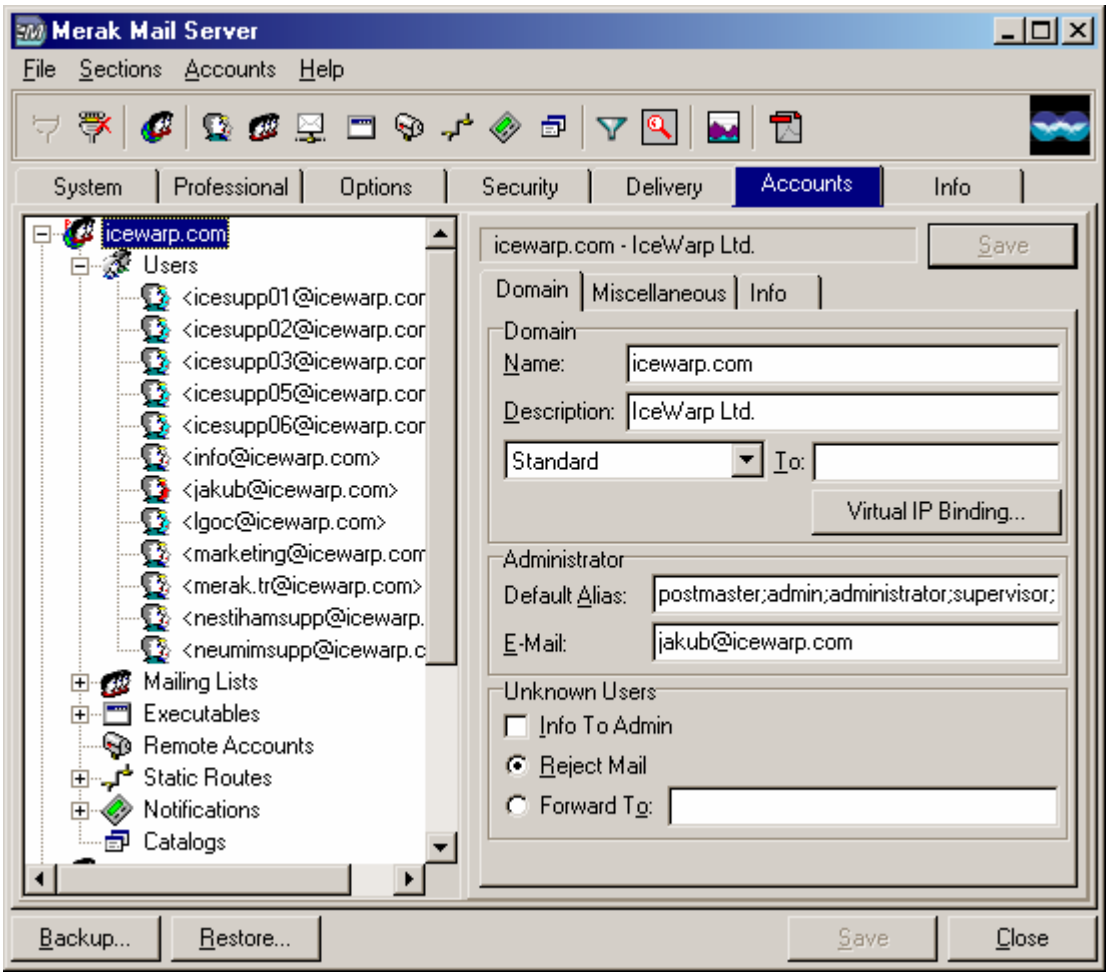
Importování uživatelů ze systému Windows NT

Pokud máte ve svých Windows NT již nastavenou databázi uživatelských účtů. Pro ušetření ručního zadávání účtů, můžete importovat celou databázi přímo do Meraka.

Zvolte uživatele, které chcete importovat a zmáčkněte tlačítko Import. Další uživatelé mohou být zavedení z odlyšných domén/serverů použitím tlačítka Load. Jestliže se zde vyskytnou mailové schránky, nebo aliasy se stejnými hodnotami, budou takoví uživatelé ignorováni a nebudou importováni. Hesla nemůžou být nikdy ze žádných verzí windows získány, systém zanechá položky hesel prázdné a vy je budete muset později editovat. Proto je lepší importovat uživatele před započetím samotné konfigurace.

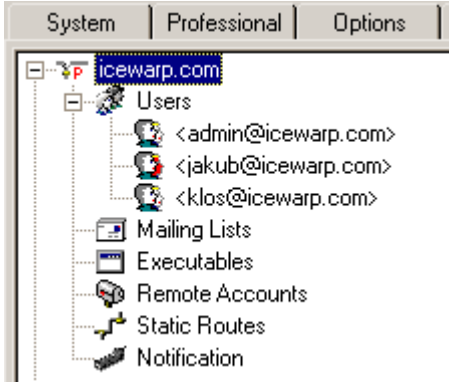

Import Windows NT Users
Server's Name:
Load
Windows NT Users:
Import Users:
Logon Name
Full Name
admin24
admin24
Administrator
administrator2
Backup admin
gregh
Greg Hilton
Guest
IUSR_NS
Internet Guest Account
IWAM_NS
Launch IIS Process Acco
NetShowServic
Windows Media services
TsInternetUser
TsInternetUser
Select ->
<- Remove
Select All
Logon Name
Full Name
Import
Cancel

Účty (nastavení domén)



Do této nabídky většina uživatelů přistupuje nejčastěji. Nastavujeme zde konfiguraci domén a uživatelských účtů.

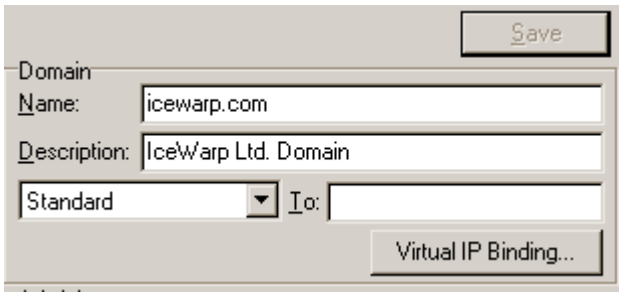
V nastaveních není rozdíl mezi nastavením primární a sekundární domény. Oboje nastavení pracují stejně. Když pracujete s nastavením primární domény, nastavení sekundárních domén musí fungovat také. Je potřeba si také uvědomit, že jméno domény a host adresa není to samé. Pokud se Váš uživatel bude chtít připojit např. na adresu mail.sekundarnidomena.cz, musíte mít na DNS serveru vytvořený specifický MX záznam.



Merak zobrazuje nastavení domén a účtů v hierarchickém formátu. Rozšířením nabídky nastavení domén zobrazíte typy účtů, dalším rozšířením nabídky zobrazíte individuální nastavení jednotlivých účtů.

Poznámka: v této nabídce může být pouze jedna doména označovaná písmenkem červeným P. Právě to je primarní doména, na kterou systém zasílá kritické systémové zprávy. Můžete kliknout pravým tlačítkem na doménu a zvolit funkci „Make Primary“ pomocí které můžete nastavit jinou doménu jako aktivní.

Nastavení domén v tabulce Account



Pole	Popis
Jméno	Do tohoto pole specifikujete jméno domény. Nejedná se o IP adresu, zkratku, nebo alias, ale o plné aktuální jméno domény. Zprávy mohou být doručovány pouze do vytvořené domény. Jestliže doména neexistuje, budou zprávy předávány ven z vašeho serveru. Můžete také vytvořit nějakou IP doménu, pokud chcete a víte proč. V tomto případě si musíte být vytvářením IP domény jisti a jiné domény ve formátu : [IP] budou brány jako doménový alias k IP doméně. To je nezbytné.
Description	Libovolný popis k doméně.
Virtual IP Binding	Doména může být vázána ke specifické IP adrese. (Pokud je primární doména vázána k nějaké IP adrese, je potřeba, ale se IP adresa specifikovala i u ostatních domén). Doména může být vázána na více IP adres, ty můžeme nastavit za sebou a oddělit pomocí středníku. Když se uživatel připojuje, bude k vyhledání autentifikačních údajů vždy použita specifikovaná IP adresa. Není doporučeno používat toto nastavení, když přesně nevíte, co dělate. Pokud provedete špatné nastavení, může být systém nepoužitelný. Buďte si jisti tím, co nastavujete. Nepoužívajte tuto funkcí, pokud nemusíte !!!
Standard	Toto pole specifikuje normální doménu s oddělenými uživatelskými schránkami. To je standardní nastavení.
ETRN/ATRN Queue	Toto je rozšiřující možnost volby. Ta specifikuje, že doména by měla přidržovat l server, který (pokud bude chtít poštu přijmout) bude používat ETRN klientské říkazi Do pole „**To**“ budeme zadávat IP adresu, pokud jí má vzdálený počítač přidělenou staticky, nebo necháme pole nevyplněné v případě, že má klient přidělovanou IP adresu dynamicky. Dynamický host bude obvykle firemní mail server, který raději než formu neustálého připopojení na internet používá připojení na internet pomocí dial up. Pokud vytvoříte nějakou ETRN doménu, musíte vytvořit pouze jeden účet v doméně. Tento účet bude používán k uchování emailů na serveru a měl by mít standardní uživatelskou strukturu a nastavení. Dejte si pozor třeba na heslo. Většina nastavení uživatele je ignorována. Jediné důležité položky jsou: Password (heslo), Alias (přezdívka), Mailbox Path (poštovní schránka) a ETRN. Položku ETRN musíte mít nastavenou na polohu

	zapnuto. Toto je jediný případ, kdy je tato položka potřebná a nařízená – celé nastavení nebude bez této položky pracovat. Pokud nastavíte pro tento účet heslo, vzdálený poštovní server vydávající ETRN klienta musí mít do svého nastavení toto heslo také přidané. Jiný mail server, který se potřebuje vydávat pomocí ETRN příkazu by to měl dělat podle následujících parametrů: **ETRN {doména}** Nebo **ETRN {doména} {heslo}**
Domain Alias	Pomocí této položky můžete docílit toho, že každý e-mail, který bude přijmut do nastavované domény bude předán na jednu specifikovanou e-mailovou adresu. Tu zadáme do pole “To:”. Toto nastavení je použitelné ve chvíli, kdy klient používá více domén a potřebuje, aby byly všechny zprávy přesměrovány do jedné poštovní schránky. Pouze potřebujete vytvořit účty pro primarní doménu, nebo jeden, kam bude předávána pošta.

Backup Domain	Záložní doména (Backup doména) je doména, která je aktivní v případě, kdy je z nějakého důvodu primární doména nedostupná. Tím že nastavíme záložní doménu docílime toho, že všecha pošta, která bude přijmuta do této domény se uloží a bude předána na host adresu specifikovanou v poli “To”. V takové doméně není potřeba vytvářet žádné uživatele, ale zkrátka budete předávat všechny zprávy na jiný e-mailový server (externí, nebo lokální). Toto řešení se používá pro realizaci tzv. Záložních mailových front, nedo doménových košů. Pokud zůstane pole To prázdné, bude pro doručení domény použit standardní MX dotaz. Merak se bude pokoušet doručit zprávy pouze na MX záznamy z nižší prioritou. To je mechanismus, který zabrání cyklení zpráv v Meraku.

Nevyplněná pole nastavení domén v tabulce Accounts

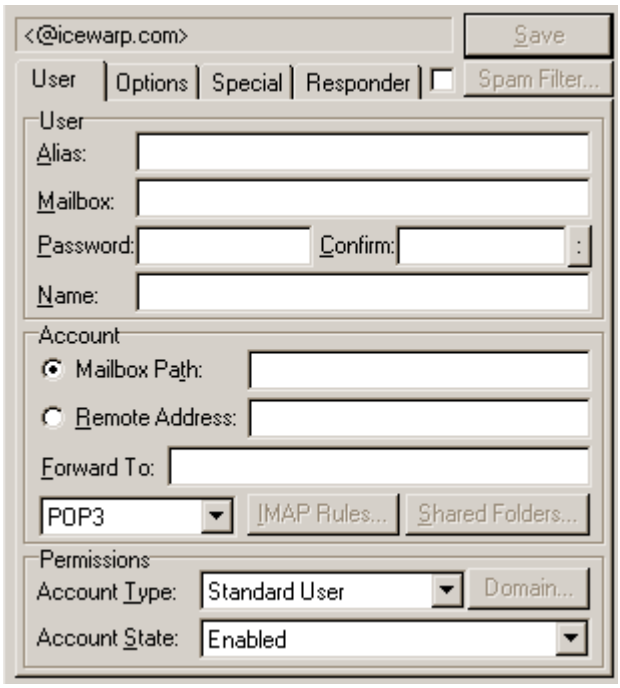
Pole	Popis
Default Alias	Toto pole specifikuje standardní aliasy správce poštovního serveru. Aliasy mohou být odděleny použitím středníku bez mezer. Díky tomuto nepotřebujete vytvářet tyto uživatele jako standardní uživatelské účty.
E-Mail	V tomto poli specifikujeme aktuální E-mailovou adresu správce poštovního serveru. Jako vždy zde pomocí středníku může být uvedeno více účtů, dokonce vzdálené účty pro různé domény. Tato položka nesmí zůstat nevyplněná.

Pole	Popis
Info to admin	Pokud je nějaký email zaslán neznámému uživateli, může být upozorněn aktuální administrátor (poštovní správce) pro tuto doménu, nebo může být zpráva odmítnuta, či předána.
Reject Mail	Pokud je nějaký email zaslán neznámému uživateli, měla by tato položka specifikovat odmítnutí emailu a jeho navrácení odesilateli. Žádná taková zpráva nebude nikdy přenesena.
Forward To	Pokud je nějaký email zaslán neznámému uživateli, bude předán na specifikovaný účet. Toto je docela běžné nastavení „catch all“ (volně přeloženo chytit vše – v našich končinách známo jako doménový koš) účtů, který bude přijímat veškeré neznámé zprávy. Právě pomocí tohoto nastavení nabízejí ISP.

Nevyplněná pole nastavení domén v tabulce Accounts

Popis	Pole
Domain Antispam Filter	Ve filtru můžete nastavit emailové adresy, domény a IP adresy, které mají, nebo nemají povoleno odesílat zprávy na váš server. Celé nastavení je vlastně textový soubor, který definuje pravidla pro přijímaní, nebo odmítání zpráv pro tuto doménu. Aby vše fungovalo, musí být zapnuta Globalní Antispamová nastavení. Pro editaci klikněte na tlačítko : . Kliknutím vyvoláte textové pole určené pro editaci. Přečtěte si více informací o Antispamových filtrech.
# Accounts	Tato položka kontroluje počet účtů, které mohou být vytvořeny v doméně doménovým administrátorem přes webové rozhraní. Tato volba převyšuje Domévový Administrační Limit (Domain Admin Limit).

Tabulka Accounts (nastavení uživatele)



Pole	Popis
Alias	Tato položka specifikuje uživatelovo jméno v doméně. Příklad: K nastavení emailové adresy support@icewarp.com zadejte do pole alias jméno support. Více aliasů pro jeden uživatelský účet můžeme definovat pomocí hodnost oddělených středníkem **Např. support;help;bugs;info**
Mailbox	Toto je jméno poštovní schránky a poštovního účtu. Většinou je automaticky zadáno Merakem při definování aliasu. Zde definované jméno je používano pro autentifikaci a sběr zpráv. Standardně je jméno schránky stejné jako alias ale nemusí být. Jméno poštovní schránky je také použito jako přihlašovací jméno (login) pro webové administrační rozhraní, nebo vzdálenou konfiguraci.
Password	Heslo pro poštovní schránku. Volbu opakujte do potvrzovacího pole.
Name	Reálné jméno uživatele, nebo nějaký identifikátor. Používá se také v automatických odpovídačích. Můžete ke jménu nastavit také komentář. K nastavení komentářů by mělo být používáno oddělení pomocí středníku. Komentář nepoužívá autoresponder, ani není zobrazeno v informacích o účtu. Většinou se používá pouze při vyledávání. Např. "Jan Novák; můj komentář"

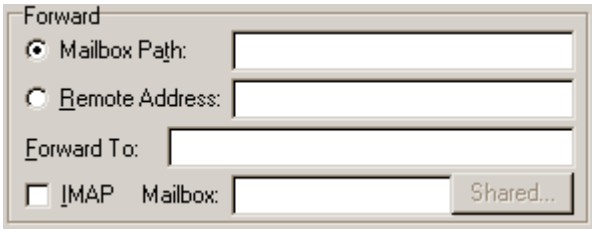
Velmi důležitá informace ohledně duplicity jmen poštovních schránek!!

Velmi častým problémem je vytváření duplicitních jmen poštovních schránek na serveru. Dochází k němu v případě, že vztváříme v jedné doméně schránku jménem prodej@domemaa.cz a prodej@domenab.cz.

Problém ale nastává pouze v případě, že vytváříte stejné jméno poštovní schránky a nastavíte mu stejné heslo, jako u účtu v druhé doméně. Merak porovnává účty podle jména a hesla. Pokud je jméno schránky a heslo stejné, Merak nemůže e-mail správně doručit. Ve chvíli, kdy je definované u každé schránky se stejným jménem jiné heslo, nenastává žádný problém.

Jednou z cest jak tento problém také můžeme řešit je přiradit každé z domén jinou IP adresu. Merak bude v tom případě porovnávat účty podle jména, hesla a IP adresy.

Pole nastavení uživatele v tabulce Account nevyplněné

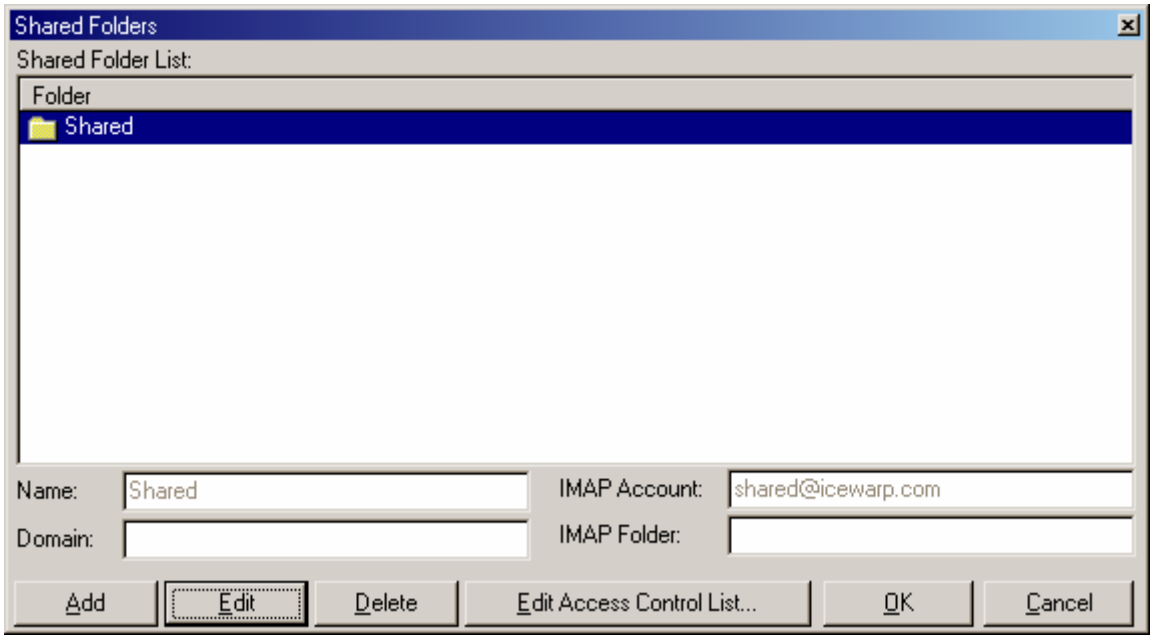


Pole	Popis
Mailbox Path	Pomocí této položky nastavíme, zda se mají přijmuté zprávy ukládat do vámi definované poštovní schránky. Jméno adresáře poštovní schránky je standardně stejné, jako název aliasu, ale může se odlišovat. Toto pole může dokonce obsahovat plnou cestu do úplně jiného adresáře.
Remote Address	Zprávy pro tento účet nemusí být ukládány na serveru, ale můžou být automaticky ukládány na jinou e-mailovou adresu. Adresa uvedena v tomto nastavení by měla být ve formátu **jmeno@domena.cz**
Forward To	Všechny příchozí zprávy budou předány na zde specifikovanou adresu. Toto je separované nastavení nevychází z funkce „mailbox path“ nebo „remote adress“. Tato funkce poskytuje mechanismus pro kopírování zpráv na vzdálené, nebo lokální účty.
Account Type	Nastaví, jaký typ účtu má být použit. **POP3** Obyčejný POP3 účet přístupný pouze přes POP3 **IMAP** IMAP účet přístupný pouze přes IMAP **IMAP & POP3** Kombinovaný účet. Je přístupný přes oba protokoly.

Sdílené složky (Shared Folders)

V Meraku je možné nasdílet specifický IMAP účet ostatním uživatelům. Složky jsou potom jednoduše dostupné v jejich privátním účtu. Je to velmi užitečná funkce.

Pro takové případy Merak také podporuje ACL (Access Control List – přístupový kontrolní seznam) IMAP rozšíření, které umožní specifikovat práva pro každý mailbox a identifikátor (uživatele). Pro všechny uživatele je zde speciální identifikátor nazvaný “anyone” (kdokoliv).



Jednotlivá tlačítka Vám umožní otevřít Folder dialog, kde můžete editovat/mazat a přidat nové sdílené složky.

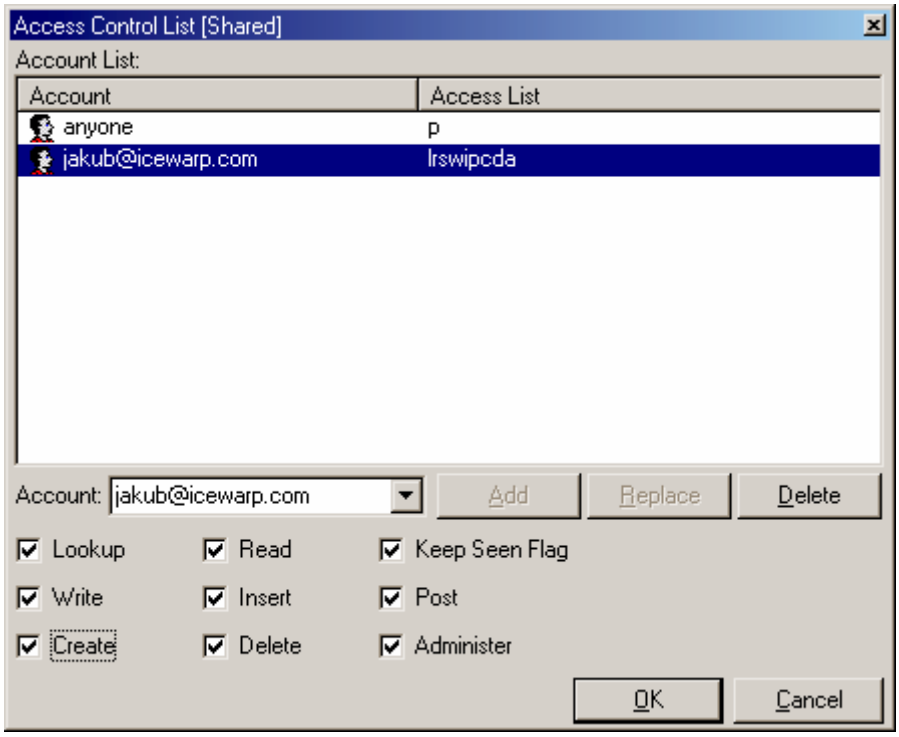
Name (Jméno)
Jmeno složby, která bude zobrazena v IMAP spojení

Domains (Domény)
Standardně může být nevyplněné. Toto pole zůstává prázdné, pokud je nastavení určeno pro všechny domény. Samozřejme zde můžete nastavit přístup z ostatních domén.

IMAP Account (IMAP účet)
Každá sdílená složka je propojena s nějakým IMAP účtem. Toto pole obsahuje e-mailovou adresu IMAP účtu.

IMAP Folder (IMAP složka)
Pokud je nastavení prázdné, bude jako sdílená složka použit INBOX adresář. Můžete zde ale také specifikovat odlyšné adresáře.

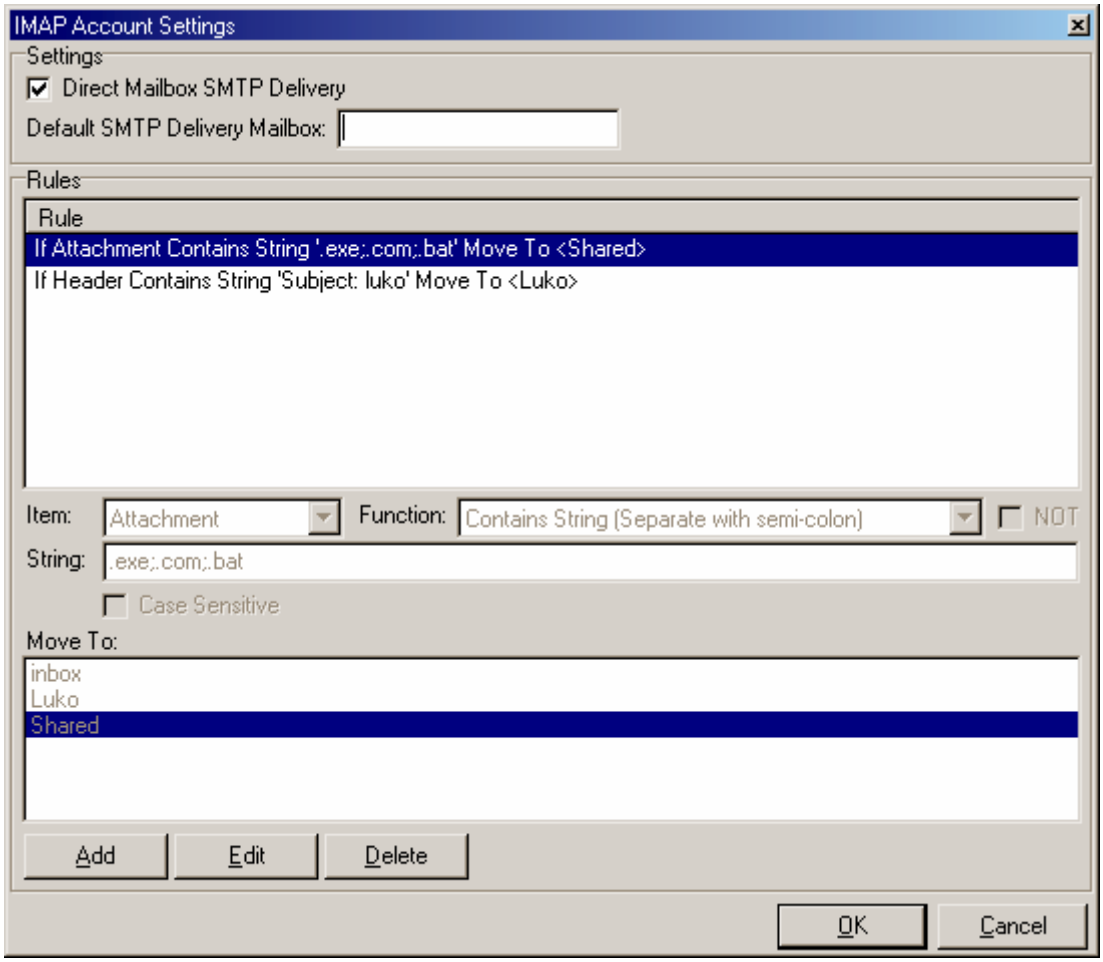
Kontrolní seznam přístupů ke sdíleným složkám



V tomto dialogu nastavujete práva pro jednotlivé emailové účty, které se budou přihlašovat přes IMAP. Můžete také nastavit “anyone” účet, který bude platný pro všechny nedefinované účty.

Seznam přístupových práv:
Lookup (l) – Uživatel uvidí složku ve svém soukromém seznam IMAP složek
Read (r) – Uživatel může otevřít složku a prohlédnout si obsah
Write (w) – Uživatel může měnit stav zpráv v dané složce.
Insert (i) – Uživatel může přidat a kopírovat zprávy do této složky
Create (c) – Uživatel může vytvořit podadresáře uvnitř této složky
Delete (d) - Uživatel může z této složky mazat zprávy
Set Seen Flag (s) – Uživatel může měnit stav zpráv z nepřečtených na přečtené a opačně
Administer (a) – Uživatel může administrovat ACL práva pro tuto složky.
Post (p) – Uživatel může odeslat e-mail přímo do této složky (pokud to dovoluje).

IMAP nastavení



Default SMTP Delivery Mailbox	Standardně můžete nechat toto pole v každém případě nevyplněné. Pokud je IMAP účet aktivní, Merak bude přijímat příchozí zprávy do nastavené IMAP složky. Pro příchozí zprávy je standardně určena složka INBOX. Pokud je toto pole nevyplněné bude INBOX použit.

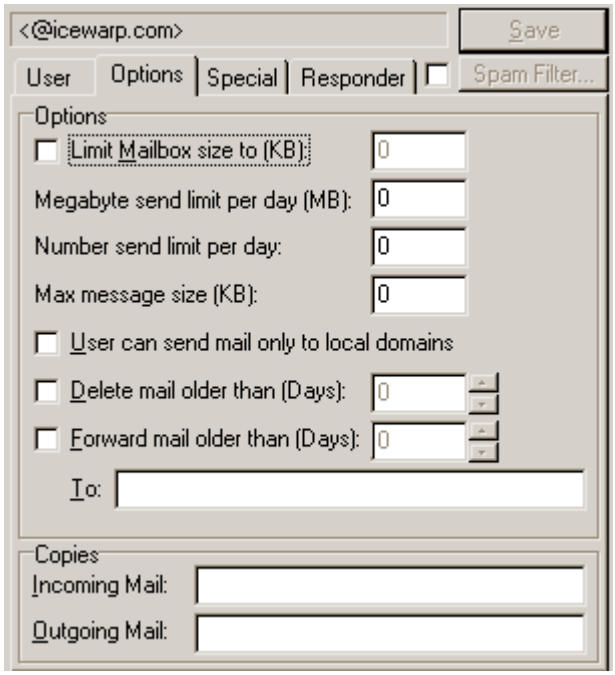
Direct Mailbox SMTP Delivery	Pro odesílání zpráv přímo do dané IMAP složky je nutné zapnout funkci Direct Mailbox SMTP Deliver a nastavit e-mailovou adresu s následující syntaxí:
	`"alias:imapslozka"@domena`
	Příklad:
	`"imap:prijatezpravy"@usa.net`
	Zprávy budou odeslány na účet imap@usa.net a budou doručeny do IMAP složky “Prijate zpravy”. Syntaxe může být použita pro jakoukoliv emailovou adresu.

Rules	Pravidla jsou použita prov všechny zprávy doručené přes SMTP protokol na IMAP pokud byly zprávy poslány přímo na IMAP účet. Můžete specifikovat podmínky stejně jako pro antispam filtry. Nastavení “Move To field” obsahuje všechny IMAP adresáře pro IMAP účty. Ty obsahují soukromé složky a také veřejně sdílené složky.

	Každá zpráva bue kontrolována pravidly. Pokud bude nějaké zprávy vyhovovat pravdilu, bude přesunutá do správné IMAP složky. Pokud ne, bude doručena do standardně nastavené “Default SMTP deliverz mailbox” nebo přímo do INBOXU.

Pole	Popis
Copies Incoming Mail	Cesta pro ukládání poštovní schránky, nebo e-mailová adresa, na kterou je automaticky kopírována příchozí pošta.
Copies Outgoing Mail	Cesta pro ukládání poštovní schránky, nebo e-mailová adresa, na kterou je automaticky kopírována odchozí,

Pole nastavení uživatele v tabulce Account nevyplněné

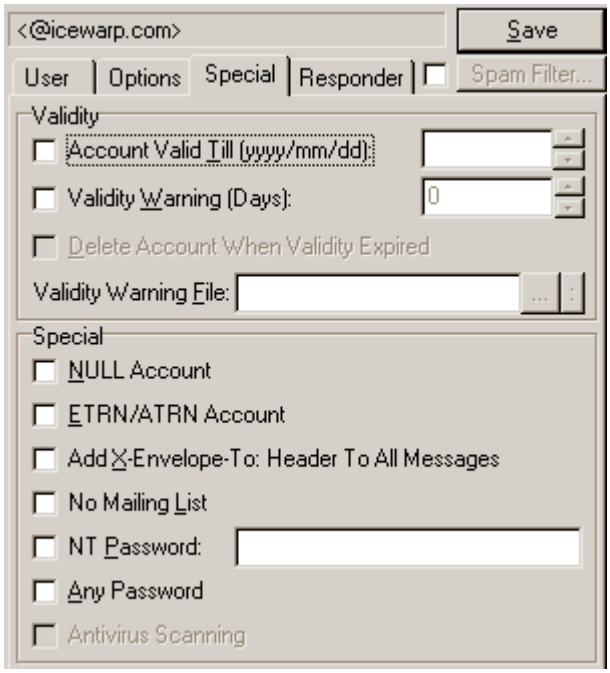


Pole	Popis
Limit mailbox size	Ke každé poštovní schránce může být přiřazena kvóta. Pokud uživatel překročí dovolenou kapacitu, bude zpráva vrácena odesilateli.
Megabyte send limit per day	Nenulová hodnota zde specifikuje množství dat, které může uživate odeslat ven v jednom dni. Navíc, pokud je zpráva odeslána dvoum příjemcům je použití zdvojnásobeno. Pokud uživatel překročí nastavený limit, musí čekat do druhého dne, kdy bude již schopný opět odesílat zprávy.
Number send limit per day	Nenulová hodnota zde, specifikuje maximální počet zpráv, které může uživatel odeslat ven v jednom dni. Logicky je vše ostatní stejné jako u předchozí položky.

Max. message size	Nenulová hodnota zde specifikuje maximální velikost zpráv, kterou může uživatel přijmout do své poštovní schránky.
User can send mail only to local domains	Toto nastavení umožní uživateli odesílat zprávy pouze do lokálně nastavených domén na tomto serveru. Uživatel nebude moci odesílat zprávy externě na jiné servery.

Pole	Popis
Delete mail older than	Merak bude odstraňovat všechny zprávy uložené déle, než ve zde specifikovaném časovém rozsahu. Bude tak činit o půlnoci každého dne.
Forward mail older than to:	Merak bude předávat všechny zprávy, které budou uloženy déle než ve zde specifikovaném časovém rozsahu a to na seznam adres uvedený v poli „To“. Do pole můžeme zadat více adres, které budou odděleny pomocí středníku
User State	Použitím této funkce můžete deaktivovat přihlašování účtu do systému, přihlašování a přijímaní pošty. Přihlašováním myslíme schonost přihlásit se do systému, kontrolovat došlou poštu, či měnit nastavení. Přijímáním myslíme doručování pošty uživateli. Pokud zakážete přijímání nebude moci být uživateli doručena žádná zpráva. Dobrá funkce pro staré a nepoužívané účty je Tarpitting. Některé staré mailing listy odesílají zprávy na staré a neexistující účty. Tyto zprávy budou považovány za spam..
NT Password	Pokud již uživatel na Vašem systému existuje, může Merak pouze “zdědit” jeho heslo přímo ze systému. Mail server ale musí mít v systému nastavena privilegia SE_TCB_NAME. Pokud chcete ověřovat uživatele na jiné, než standardní doméně, zadejte do tohoto pole jméno požadované domény. Pokud pole necháte prázdné, bude Merak ověřovat ve standardně nastavené doméně. Toto nastavení proveďte pouze v případě, že používate síť Windows NT s nastavenými doménami.
Any Password	Tímto nastavením specifikujeme, že bez ohledu na to, jaké heslo je zadáno, bude vždycky přijmuto.

Pole nastavení uživatele v tabulce Account nevyplněné

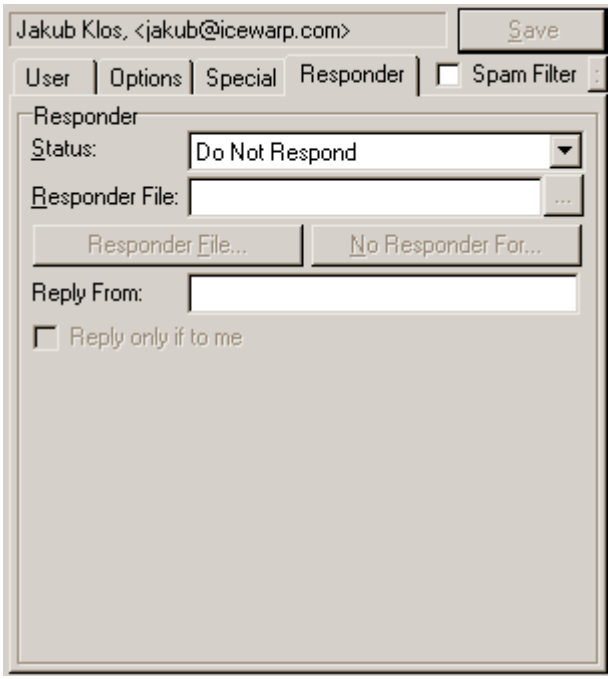


Pole	Popis

User Type	Tyto volby souvisí s webovým administračním rozhraním
	
	Standard User (standardní uživatel):
	Tento účet je nastaven administrátorem jako standardní uživatel a jeho nastavení nebude moci změnit nikdo jiný, než administrátor.
	
	Self Configurable User (uživatel se schopnostmi vlastní konfigurace):
	Nastavení účtu může být modifikováno samotným uživatelem, který bude k tomuto účelu používat webové rozhraní. Hesla, poštovní schránku/předávání zpráv, automatický odpovídač a mazání zpráv po x dnech, to jsou nastavení, které budou moci být změněna. Může také prohlížet svoji poštovní schránku.
	
	Domain Administrator (doménový administrátor):
	Doménový administrátor nemá schopnost měnit globální konfiguraci server, ale má povoleno administrovat účty v jeho doménách. Na pravo je umístěno tlačítko, pro kontrolu práv doménového administrátora. Do této konfigurace zadejte domény (každou na jeden řádek), které bude mít administrátor schopnost spravovat.
	
	Např.
	`icewarp.com`
	`microsoft.com`
	
	Můžete také specifikovat konkrétní práva doménového administrátora:
	Např.
	`RIGHTS=U,M,D`
	
	Znaky, které používáte za "=" umožňují:
	
	U – Spravovat uživatelské účty
	M – Spravovat mailing list účty
	E – Spravovat executables (spustitelné) účty

	N – Spravovat notifikační účty R – Spravovat vzdálené účty (remote accounts) D – Modifikovat doménové nastavení **Administrator (správce)** Pokud má uživatel přidělena práva administrátora, může měnit všechna nastavení, vytvářet účty. A to buď přes webové rozhraní, nebo přes konfigurační applet Meraka.

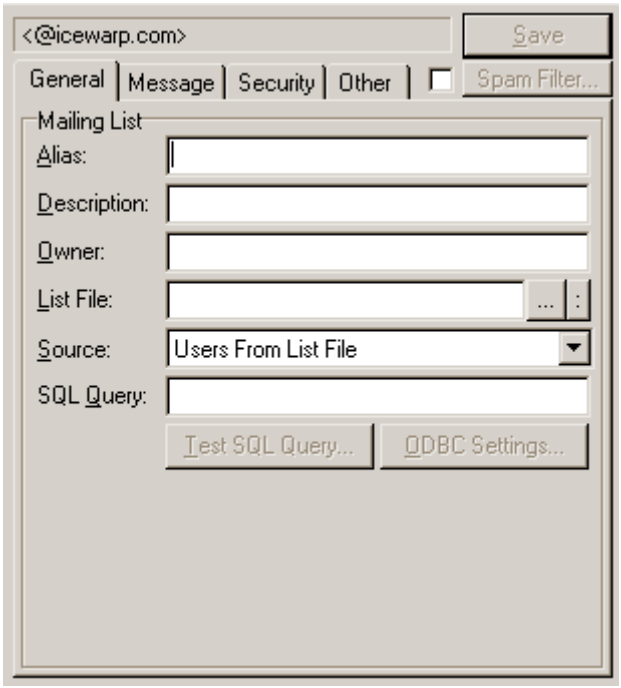
Pole	Popis
Account valid till	Specifikuje, že uživatelský účet je platný pouze do tohoto data. Po tomto datu nebude moci tento účet přijímat žádnou poštu přes POP3/IMAP4 klienta. Výsledek je stejný, jako když je účet deaktivován.
Validity warning	Pokud je aktivována funkce Account Valid till, nastaví v tomto poli jak dlouho před vypršení platnosti účtu má být uživatel informován. Hodnota vyjadřuje počet dní.
Validity Warning File	Toto pole specifikuje cestu k souboru, který bude uživateli zaslán jako zpráva informující ho o jeho brzkém vypršení platností účtu. Pokud nespecifikujete vlastní zprávu, bude automaticky vygenerována systémem.
Delete account when expired	Pokud tuto položku zaškrtneme, bude účet po vypršení platnosti smazán.
NULL	Tato funkce nám umožnuje nastavit účet jako „dummy“ tzn. Zprávy na něho budou moci být stále odesílány, ale nebudou ukládány. Zprávy budou automaticky předávány, či bude fungovat automaticky odpovídač. Takový uživatel se nemůže přihlasit do systému.
No mailing list	Tato položka specifikuje, že tento uživatel bude vyřazený ze všech mailing listů v systému, které mají nastavenou funkci „Send To All“.
ETRN	Touto funkcí nastavíme, že se jedná o účet, ve kterém jsou všechny zprávy uchovávány pro vzdálený poštovní server, který se bude představovat příkazem ETRN. Tento účet musí být definován jako první a jediný v doméně. Bude použit pouze v případě, že doména je typu ETRN.
Add X-Envelope-To	Pomocí této funkce přídáme do každé přimuté zprávy pro tento účet X-Envelope-To hlavičku. Tato funkce se používá pro tzv. “Catch all” účty. Tak vzdálený mail server přesně ví, jaké zprávy přesně byly odeslány.
Anti Spam Filter	Edituje uživatelský antispamový soubor filter.dat. Ten je probrán v sekcí o Anti Spamových Filrech



Pole	Popis
Responder	Pomocí této položky nastavujeme automatický odpovídač aktuální pro daný uživatelský účet. Ten se dá použít ve chvíli, kdy uživatel není po dlouhou dobu schopen vybírat svoji e-mailovou schránku. Například je na dovolené. Zadejte zde cestu k souboru např. c:\autoodpovidac\pryc.txt (nebo použijte tlačítko ... pro vyhledání již existujícího souboru), potom použijte pro editaci souboru tlačítko Můžete také použít některé proměnné: %%From%% %%From_Alias%% %%To_Name%% %%To_Domain%% %%Subject%% %%Size%% %%Time%% %%From_Name%% %%To%% %%To_Alias%% %%IP%% %%Header%% %%Date%% Příklad: Ahoj, Vaše zprávy odeslaná v %%Time%%, %%Date%% měla velikost %%Size%% Kb. **Do Not Respond** Když je tato funkce zapnutá, nebude zasílána žádná automatická odpověď. **Respond Always** Pokud je tato funkce aktivní, bude automatická odpověď zaslána vždy. **Respond Once** Pokud je tato funkce aktivní, bude automatická odpověď zaslána vždy pouze jednou. Merak si totiž udržuje výpis e-mailových, na které už automatickou odpověď poslal.

Responder File	Pomocí tohoto tlačítka můžete editovat soubor s automatickou odpovědí.
No Responder For	Pomocí tohoto tlačítka otevřete soubor, ve kterém je možné specifikovat vyjímky zasílané automatických odpovědí. Můžete tak zabránit zasílání na dané e-mailové adresy a domény. Soubor je nazvaný **norespond.dat** a může obsahovat e-mailové adresy, nebo domény.
Reply From	Do tohoto pole můžete zadat zpáteční adresu, která bude používat pro autoresponder. Pokud necháte pole nevyplněné, bude použita adresa majitele účtu.
Respond only if to me	Pokud zpráva, která byla zaslána na účet, na kterém je právě nastaven automatický odpovídač je určena pro větší množství e-mailových adres, nemusí na ni být zaslána odpověd automatickým odpovídačem.

Účty (Mailing Listy)



Mailing List je nejsnažší cesta, jak po zaslání zprávy na jednu adresu oslovit více lidí. Zpráva, která je přijata na mailing list účet je posléze rozeslána na všechny členy mailing listu (konference). Ta se používa zvláště v případě diskuzních skupin, či při komunikaci uživatelů, vyměňujících si nějaké zajímavé myšlenky.

Merak může jít ještě o jeden krok dál a může být také nakonfigurován jako list server. Ten má svého administátora a uživatele k němu přistupují přes příkazy odesílané ve zprávách.

Nastavování mailing listů je velmi odlyšné od nastavování list serveru. Nastavování list serveru je podrobně popsáno v další části.

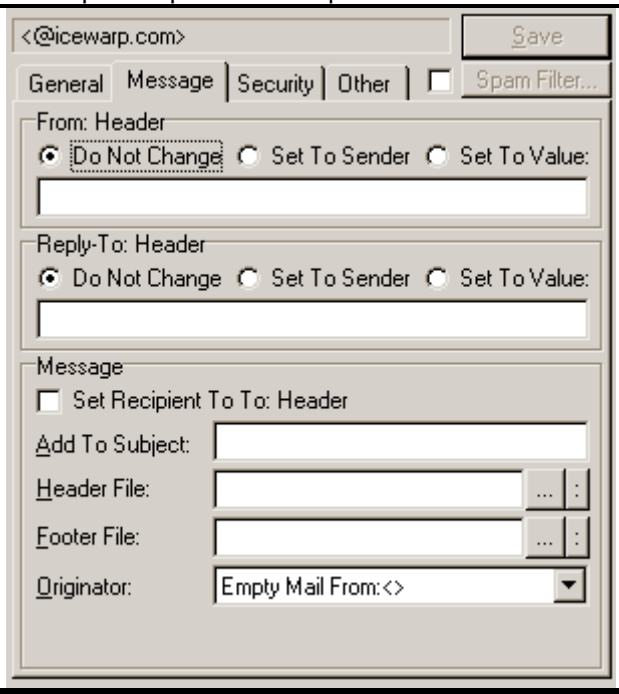
Poznámka: Nastavování Antispamových filtrů probíhá standardním způsobem.

Nastavujeme Mailing list

Pole	Popis
Alias	Zde specifikujeme jméno mailing listu. Jméno mailing listu poté aplikováno do emailové adresy <jméno>@domena.cz
Description	Vámi zvolený popis
Owner	Emailová adresa vlastníka mailing listu. Větší množství adres může být odděleno středníky
List File	Pokud je mailing list využíván k odesílání zpráv různým příjemcům v různých doménách budete muset použít tento seznam. Položka list file specifikuje plnou cestu k textovému souboru obsahujícímu seznam všech členů. Po zadání celé cesty a jména souboru použijte editovací tlačítko  k editování samotného seznamu členů. Umístěte každého člena na nový řádek ve formátu „uživatelské jméno <email>“ jako zde: Jana Kadlecová <iana@rsk.net> Honza Novák <john@msn.com> Můžete také specifikovat seznam emailových adres, které mají povolený vstup do mailing listu ve druhém textovém souboru a připojit ho k prvnímu použitím středníku. Příklad: c:\merak\list.txt;c:\povolene.txt

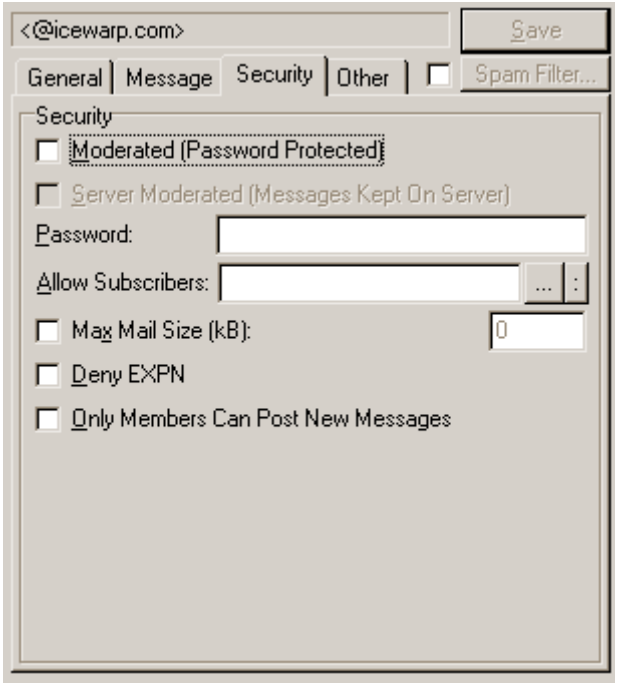
Source	Pomocí této funkce odešleme zprávu všem uživatelům. Získat seznam uživatelů můžeme několika způsoby:
	Users From List File (seznam uživatelů ze souboru)
	Bude použita standardní cesta pro získání seznamu uživatelů z textového souboru.
	
	Users From ODBC (uživatelé z ODBC – uživatelé získaní z databáze)
	Pro získání seznamu můžeme použít ODBC. Připojovací řetězec je zapsán v poli List a musí mít následující strukturu:
	
	`DSN,uzivatelskejmeno,heslo,SQL dotaz`
	Příklad:
	`listusers,user,pass,SELECT Email FROM Users`
	
	SQL dotaz má vrátit pouze jedno pole, které bude obsahovat e-mailové adresy. Pro přehled uživatelů můžete nastavit jakýkoliv ODBC zdroj přídáním znaku "|" a specifikovat jiné DSN pomocí dotazu:
	
	`DSN,uzivatelskejmeno,heslo,SQL dotaz|DSN,uzivatelskejmeno,heslo,SQL dotaz`
	
	Users From Domain
	Tato položka jednoduše předá přijatou zprávu všem uživatelům v doméně.
	
	All Users
	Tato položka předá zprávu všem uživatelům ve všech doménách na serveru.
	
	All Domain Administrators

	Tato položka předá zprávu všem doménovým správcům na serveru. **All Administrators** Tato položka předá zprávu všem správcům serveru



Pole	Popis
From: And Reply-To: Headers	V tomto poli můžete nastavit, co by měla každá hlavička osahovat. To záleží na Vašem přání. Buď budete chtít nastavit pole From na Sender a odpovědět na tuto e-mailovou adresu mailing listu (to způsobí, že všechny odpovědi budou směřovány zpět do mailing listu), nebo chcete nastavit Reply-To pole na Odesilatele a odesílat zprávy z "From" e-mail adresy (to způsobí, že všechny odpovědi budou směřovány zpět na odesilatele zprávy).
Add to subject	V tomto poli specifkujeme řetězec, který chceme přidat do přesmětu zprávy.
Set Recipient To To: Header	Nastaví novéo příjemce v To hlavičce.
Header File	Obsahuje cestu k textovému souboru, který by měl být vložen na začátek všech zpráv procházejících přes mailing list.

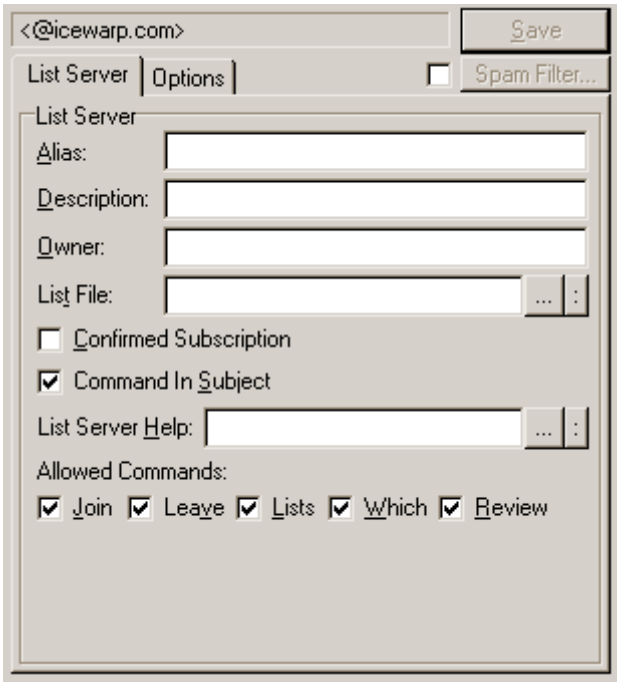
Footer File	Obsahuje cestu k textovému souboru, který by měl být vložen na konec všech zprávy procházejících přes mailing list.



Pole	Popis
Moderated Mailing List	Moderovaný mailing list je takový mailing list, ve kterém jakákoliv zpráva, která má být schválena pro doručení ostatním členům seznamu musí obsahovat heslo. Heslo musí být uvedeno jako první slovo v předmětu zprávy. Pokud není heslo nastaveno, zpráva je zaslána vlastníhovi, který může zprávu odeslat dál členům mailing listu, nebo odeslat zpět původci zprávy. Jakmile je zprávy odeslána mimo mailing list je část předmětu obsahující heslo automaticky odstraněna. Pokud používáte tuto funkci spolu s funkcí Server Moderated, jsou všechny zprávy uloženy na server. Ve chvíli, kdy na tyto zprávy odpovíte, bude zpráva odeslána ven, členům mailing listu. V tom případě slouží jako heslo odpověď. Ke smazání uložených zpráv na serveru a zamezení jejich zasílání ven z mailing listu, stačí přidat '-DELETE' ke schvalovacímu heslu.
Allow Subscribers	Zde můtete nastavit seznam e-mailových adres, které budou mít možnost vstoupit do mailing listu ve druhém textovém souboru. Tento soubor připojíte k prvnímu. Příklad: c:\merak\list.txt;c:\merak\allowed.txt
Deny EXPN	If a client issues an EXPN command the list members will be returned. Checking this option prevents this - "No such mailing list" will be returned.
Max Mail Size	Specifies the maximum message size that can be sent to the mailing list.
Members Only	Specifies that only the members of the mailing list can send messages to the mailing list. If users have some flags set they need the POST flag.

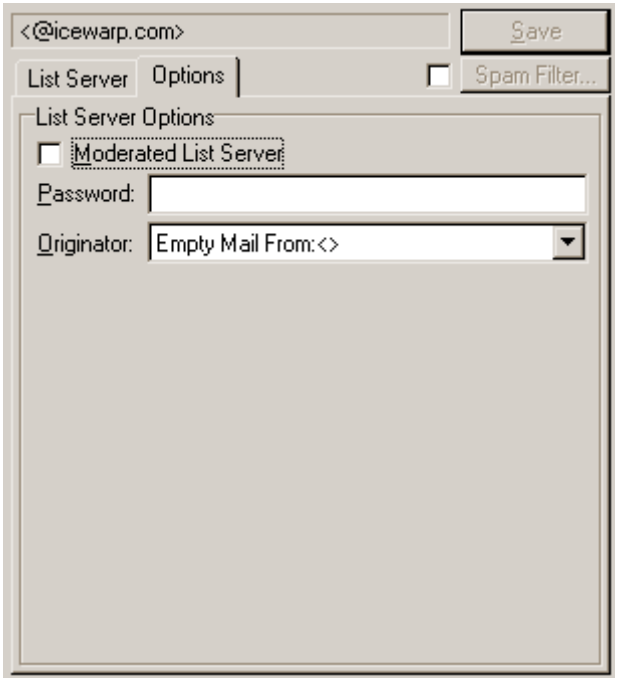
Send to Sender	Pokud není funkce aktivní a uživatel (který je uveden v seznamu) pošle zprávu do mailing listu, sám ji neobdrží. Pokud je funkce aktivní, obdrží kopii jeho vlastní zprávy.
Copy to Owner	Pokud vlastník mailing listu není mezi samotnými členy, umožní mu tato volba příjímat kopie zpráv na emailovou adresu specifikovanou v poli „Owner“ (vlastník). Navrhujeme vám ale, aby vlastníci byly členy vlastního mailing listu a přidali do seznamu členů sami sebe.
Join/Leave File	Pokud používate funkce list serveru, můžete pomocí tohoto nastavení specifikovat cestu k textovému souboru, obsahující informaci, která bude odeslána nově přihlášenému uživateli. Pomocí tohoto souboru může být uživatel informován např. o pravidlech působení v konferenci. Jako vždy můžete k editaci souboru použít editační tlačítko. Cesta k souboru, který má být uživatel doručen po odhlášení z list serveru je oddělena pomocí středníku. Příklad: `c:\list\prihlaseni.txt;c:\odhlaseni.txt`
Digest	Nastaví, že všechny zprávy odeslané do mailing listu budou uloženy a uchovány v baliku, která bude obsahovat seznam všech zpráv a jejich těl. Pak budou všechny zprávy odeslány o půlnoci všem členům mailing listu.
Process Mailing List Variables	V mailing listu můžete použít různé proměnné a to v telé zpráv odeslaných v mailing listu. Proměnné jsou stejné, jako proměnné pro automatický odpovídač. Pokud je tato funkce zapnutá, Merak automaticky nahradí proměnné korektními hodnotami.
Remove Dead Email Addresses	Pokud je funkce zapnutá, bude Merak automaticky ze seznamu členů odstraňovat e-mailové adresy, které budou vykazovat fatální chby během pokusu o doručení zprávy. Adresa je odstraněna během pokusu o odeslání nové zprávy do mailing listu.
Notify Owner	Vlastník mailing listu může být upozorněn při: **Join –** Pokud někdo nový vstoupi do mailing listu **Leave –** Pokud někdo opusti mailing list
Deny EXPN	Pokud klient započne spojení pomocí EXPN příkazu, bude mu vrácen seznam členů mailing listu. Pokud tuto funkci zapnete, zabráníte tím vracení chybové hlášky “No such mailing list”.
Max Mail Size	Nastaví maximální velikost zprávy, která může být poslána do mailing listu.
Members Only	Pomocí této funkce umožníte zasílání příspěvků do mailing listu pouze jeho členům.

Nastavujeme List server



Pole	Popis
Alias	Nastaví alias pro list server. Na adrese, kterou nastavíte v tomto poli bude fungovat list server a právě na tuto adresu budete odesílat příkazy adresa bude ve formátu <jmeno>@domena.cz.
Description	Text, který zvolíte pro popis serveru
Owner	E-mailová adresa vlastníka list serveru. Více adres může být odděleno pomocí středníku. Tato adresa je použita pro odpovědi z list server a pro potvrzující zprávy.
List File	Standardně můžete nechat toto nastavení prázdné a můžete poskytovat služby všem mailing listům. Pokud potřebujete povolit pouze některé mailing listy, obsahuje právě tento soubor seznam povolených malinglistů, které mohou být odtud spravovány. Umístěte adresu každého mailing listu na nový řádek jako v následujícím příkladu: List1@domena1.cz List2@domena2.cz
List Server Help	Pokud uživatel zašle list serveru příkaz z žádostí o pomoc při nastavení, list server pošle uživateli standardní odpověd. Zde můžete specifikovat soubor, jehož obsah bude uživateli odeslán namísto standardní hlášky. Pokud přídáte pomocí středníku jinou cestu k textovému souboru, bude tento soubor použit v potvrzující zprávě, kterou server používá při přihlašování nového účastníka.
Allow Commands	Pomocí zaškrtávacích polí povolte příkazy, které budou moci být použity list server. Přehled příkazů je k dispozici na další stránce.

Moderated Mailing List / List Server	Pokud je účet používán jako list server, jsou všechny příkazy chráněny heslem. Toto heslo je umístěno mezi příkazem a parametrem příkazu.



Paramtery pro list server jsou obvykle umístěny v těle zprávy jako prostý text.

Příkazy list serveru:

JOIN nebo SUBSCRIBE (vstoupit, nebo přihlásit se):

Těmito příkazi se přihlašuje uživatel, když má zájem vstoupit do list serveru. Tyto příkazy budou akceptovány pouze v případě povolení list serverem. Jinak přijme zprávu o uživatelově požadavku vlastník.

Použití:

Join [heslo] {jméno list serveru}, [emailová adresa], [plné jméno], [krátký obsah]
Nebo
Subscribe [heslo] {jméno list serveru}, [emailová adresa], [plné jméno], [krátký obsah]

Hodnoty uvnitř závorek jsou nepovinné. Pokud není zadaná žádná emailová adresa bude použita adresa, ze které byla přihlašovací zpráva odeslána.

LEAVE nebo UNSUBSCRIBE (opuštění, nebo odhlášení se):

Uživatel může automaticky pomocí těchto příkazů list server opustit.

Použití:

Leave [heslo] {jméno list serveru}, [emailová adresa], [krátký obsah]
Nebo
Unsubscribe [heslo] {jméno list serveru}, [emailová adresa], [krátký obsah]

Hodnoty uvnitř závorek jsou nepovinné. Pokud není zadaná žádná emailová adresa bude použita adresa, ze které byla přihlašovací zpráva odeslána.

LIST (seznamy)
Použití tohoto příkazu slouží k získání seznamu všech diskuzních skupin provozovaných na tomto serveru.

Použití:

Lists [heslo]

WHICH (který)
Použitím tohoto příkazu si vyžádáte seznam všech konferencí, do kterých jste již přihlášeni

Použití:

Which [heslo] [email adresa]

Hodnoty uvnitř závorek jsou nepovinné. Pokud není zadaná žádná emailová adresa bude použita adresa, ze které byla přihlašovací zpráva odeslána.

RECIPIENTS nebo REVIEW (příjemcové, nebo přehled)
Použitím tohoto příkazu získate seznam všech příjemců specifikovaného fóra.

Použití:

Recipients [heslo] <list server>
Nebo
Review [heslo] <list server>

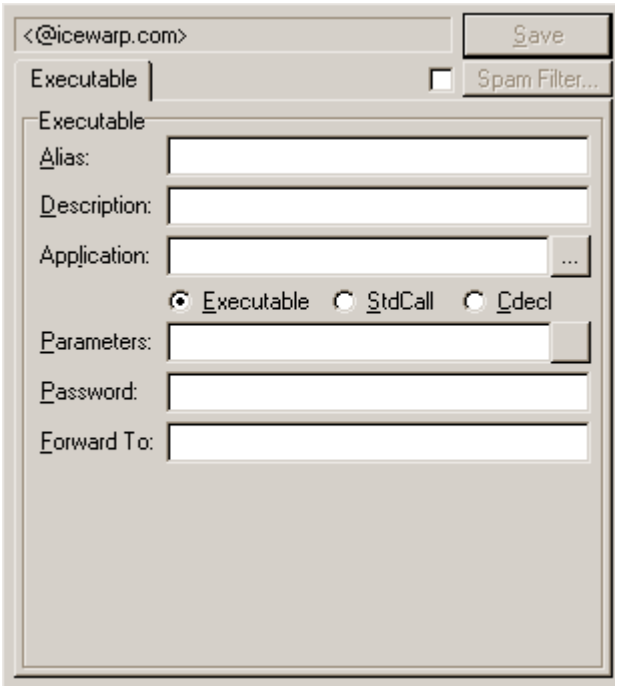
HELP (pomoc)
Použitím této funkce získáte popis všech příkazů (viz. Minulá stránka).

Použití:
Help [heslo]

Accounts (Executables účty – Spustitelné účty)

Spouštěcí účty jsou výborná cesta ke spuštění nějaké úlohy na serveru, aniž byste museli použít nějaký nástroj pro vzdálenou administraci serveru. Jednoduše nastavíte úlohu, kterou je potřeba provést a pouhým zasláním zprávy na tento emailový účet úlohu spustíte. Nezapomeňte, že taková úloha musít být nastavena tak, aby se sama ukončila. Všechny aplikace většinou vyžadují jako vstup zprávy dočasné jméno souboru.

Je velmi dobrý nápad používat u takových účtů antispamové filtry, které umožní zasílání zpráv pouze z vaší emailové adresy.



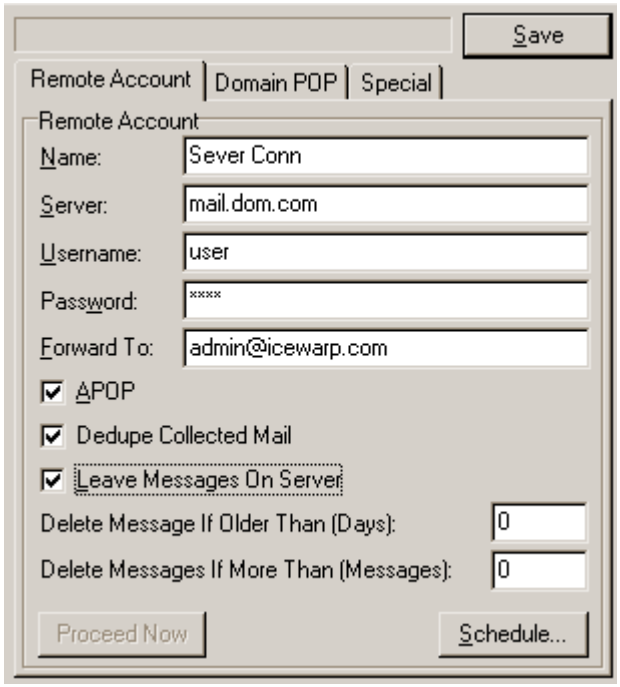
Pole	Popis
Alias	Jako vždy zde specifikujeme jméno účtu, které bude v e-mailu uváděno před jménem domény. Např. vhodná adresa pro spouštění defragmetace disku je defrag@icewarp.cz
Description	Do tohoto pole můžete zadat nějaký popisný text
Forward To	Nastaví adresu, na kterou bude předán obsah zprávy.
Application	Nastaví cestu a jméno souboru aplikace pro spuštění. Může se jednat buď o DOS, Win32 aplikaci, nebo DLL. Nesmí vyžadovat uživatelský vstup. Executable – Standardní spustitelná aplikace StdCall - DLL s WINAPI (StdCall) rozhraním Cdecl - DLL s Cdecl rozhraním
Password	Jakýkoliv spustitelný účet může být chráněn heslem. Heslo se musí zadat vždy do předmětu zprávy. Pokud bude heslo nalezeno, bude z předmětu zprávy

	smazáno a aplikace bude spuštěna. Pokud nebude heslo nalezeno, nebude e-mail vůbec zpracován. d
Parameters	Specifikuje paramtery ke spuštění s aplikací: %%From%% - kdo je původcem zprávy %%To%% - komu byla zpráva odeslána %%Subject%% - předmět zprávy %%Date%% - datum odeslání zprávy %%Message-ID%% - Identifikační hlavičku zprávy %%MessageFile%% - Plnou cestu/jméno souboru zprávy

Accounts (Remote Accounts – vzdálené účty)

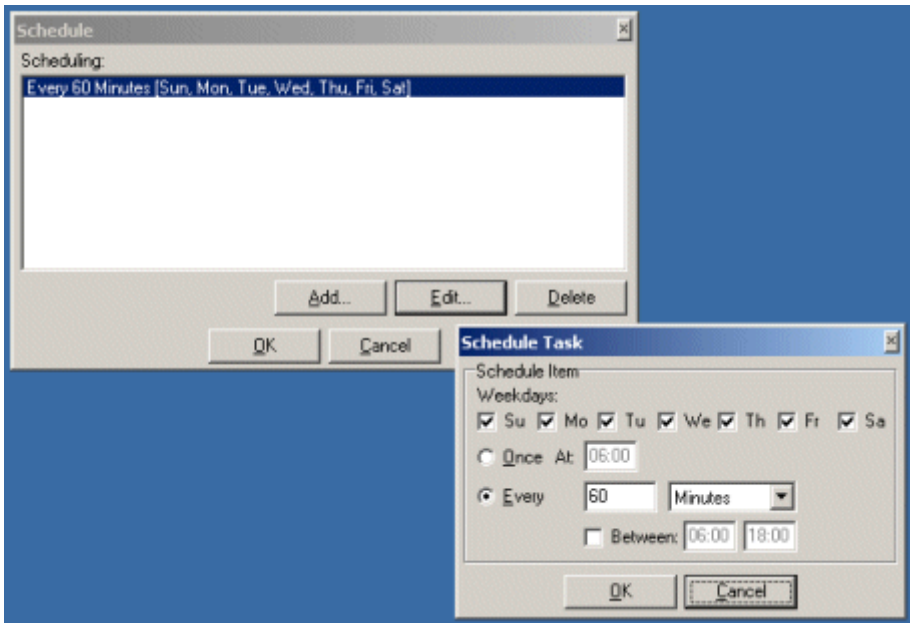
Vzdálené emailové účty (remote accounts) jsou účty, které jsou ve skutečnosti umístěné na vzdálených POP3 serverech. Můžete Meraka nastavit tak, aby kontroloval došlou poštu na vzdálených serverech. Vše může být prováděné pro jeden účet, nebo pro celou doménu využívající doménových POP funkcí.

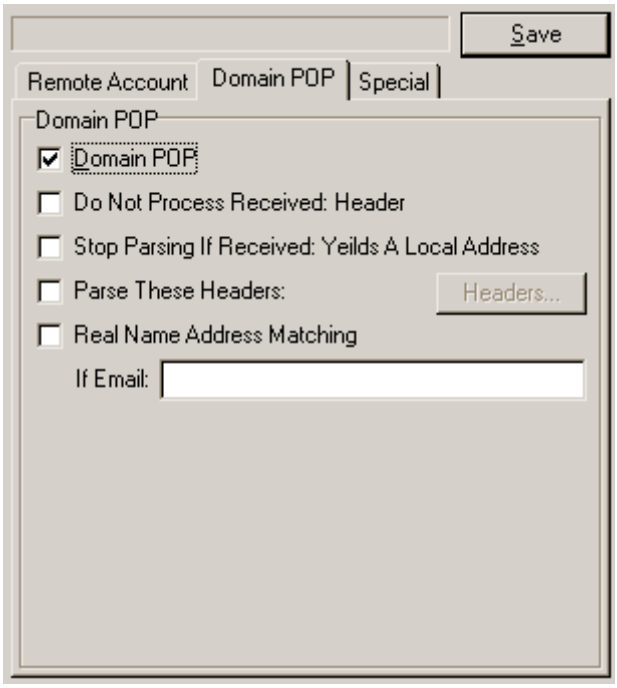
Jestliže domény nepoužívají funkce Domain POP přeposílají nakonfigurované vzdálené účty poštu na adresu nakonfigurovanou v poli „Forward To“..



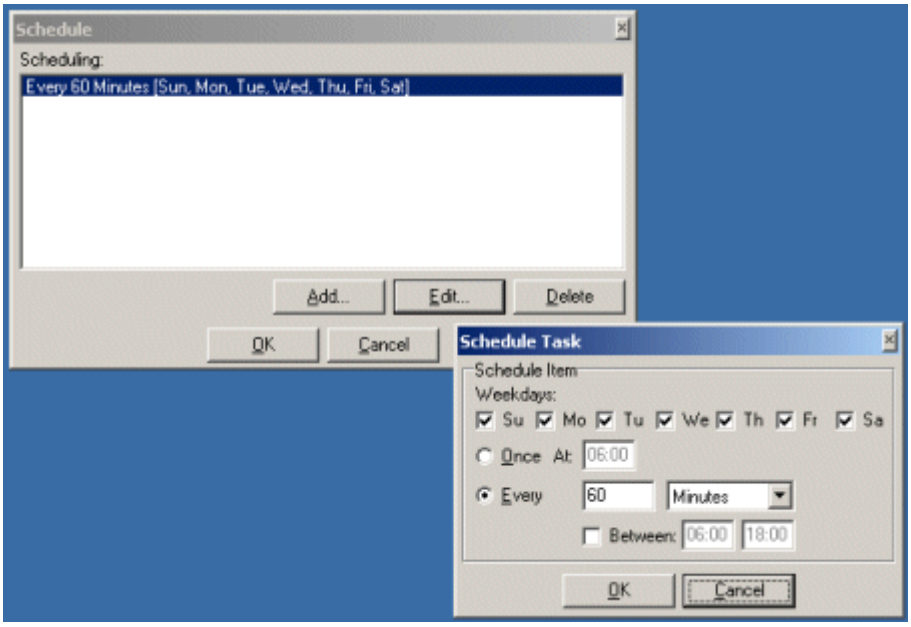
Pole	Popis
Name	Jméno vzdáleného účtu. Je používáné pouze pro informační účely.
POP3	Nastaví host adresu POP3 serveru např. pop3.demon.com
Username	Uživatelské jméno používané na POP3 serveru
Password	Heslo používané na POP3 serveru

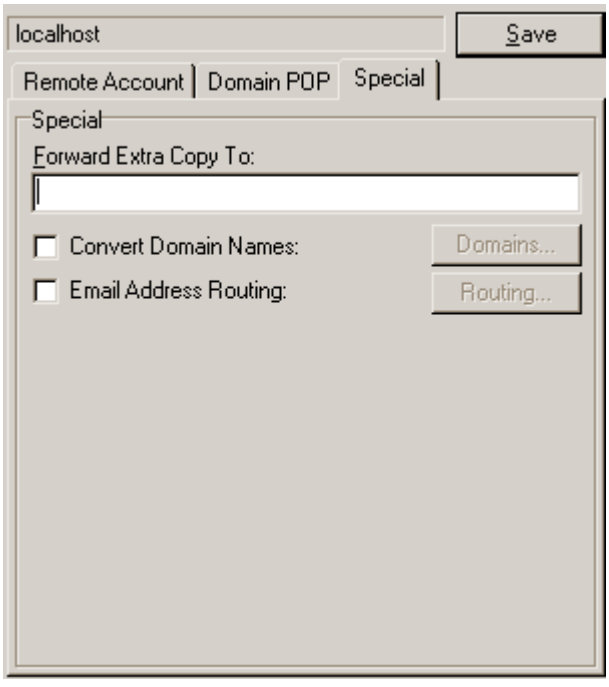
APOP	Pokud se rozhodnete tuto funkci používat, bude Merak při komunikaci se vzdáleným POP3 serverem používat zabezpečené APOP příkazy. Vzdálený server musí tuto funkci podporovat. (APOP je zabezpečené přihlašování používající MD5 šifrování)
Leave messages on server	Merak nechá získané emaily uložené na vzdáleném serveru a nebude je mazat.
Dedupe Collected Mail	Merak bude číst ID zprávy z hlavičky jestliže budou mít některé zprávy stejné ID, bude zpráva zpracována pouze jednou. Nebude tak docházet k duplikaci zpráv.
Delete Message If Older Than	Tato funkce se váže k funkci “Leave messages on server” (zanechávat zprávy na serveru). Pokud je zpráva na severu uložena po určitý počet dní, bude smazána.
Delete Messages If More Than	Tato funkce se váže k funkci “Leave messages on server” (zanechávat zprávy na serveru). Pokud je zde více, než nastavený počet e-mailu, budou zprávy smazány.
Forward to	Nastaví seznam adres (nebo jednu adresu) oddělený středníky, na které budou veškeré získané zprávy přeposílany.
Schedule	Nastavení plánovače pro tento vzdálený účet. Používá se zde standardní plánovací dialog Merak Mail serveru. Nikdy nezapomeňte nastavit plánovač.




Save
Remote Account
Domain POP
Special
Domain POP
Domain POP
Do Not Process Received: Header
Stop Parsing If Received: Yeilds A Local Address
Parse These Headers:
Headers...
Real Name Address Matching
If Email:

Pole	Popis
Domain POP	Pomocí tohoto pole nastavíme, zda vzdálený účet slouží ke sbírání pošty pro celou doménu tzn. Vzdálený POP3 účet obsahuje všechny zprávy pro tuto doménu.Zprávy budou roztříděny pomocí hlaviček „To:“,“Cc:“, nebo pomocí jiných metod. Příklad: Pokud zpráva obsahuje hlavičku „To: John Doe john@doe.cz „ , musí doména due.com existovat v Merakovi a zprávy budou doručeny právě uživateli John Doe v doméně doe.com. Pokud doména nebo uživatel neexistují, bude k přeposlání zprávy použita adresa uvedená v poli „Forward To:“. Jinými slovy, položka “Forward To” obsahuje emailovou adresu sloužící k poslání zpráv, které nejsou doručitelné pomocí funkce Remote Accounts. Někdy jsou všechny zprávy doručeny na účet nastavený v poli “Forward To”. To může být způsobeno několika důvody. V první řadě je nutné zkontrolovat, zda doména uvedená v hlavičce (v poli To – příjemce) je skutečně v Meraku nastavena. Pokud je doména nastavena, ale vy máte stále problémy, zapněte funkci “No received Processing”.
Parse These Haders	Standardně Merak rozebírá daná záhlaví jako To, CC apod. Tato funkce může pak umožňuje nastavit jinou MIME hlavičku pro použití v Meraku. Okno vám umožní nastavit přídavné hlavičky. Každou na jeden řádek.



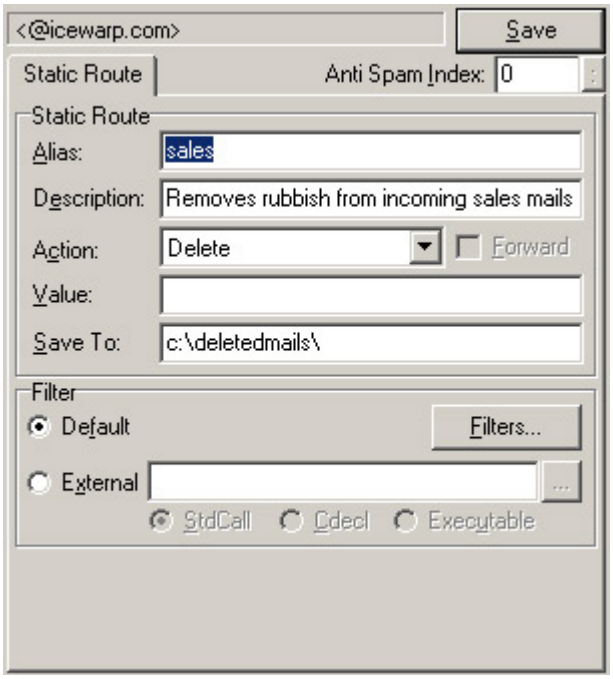


Pole	Popis
Forward Extra Copy To	Všechny zprávy budou kopírovány na nastavený účet.

Convert Domain Names	Merak se spoléhá na domény příjemců definované na server. Pokud bude vaše zpráva doručena vzdáleným účtem nemusí být doménové jméno definované na server a může být vytvořeno konverzí použitím tlačítka “Domains” Příklad: `dummy.com=localdomain.com`
Email Address Routing	Tato funkce umožní specifikovat routování pravidel pro zprávy přijmuté pomocí vzdáleného účtu. Je zde použita stejná syntaxe, jako v automatické redirekci. Můžete zde nastavit e-mailové adresy, domény, prostě cokoliv..

Accounts (Static Routes – Statické routy)

Statické routovací účty jsou jednoduché aliasy, které jsou schopni přijmout zprávy a odeslat je přímo na vzdálený mail server, jsou založené na konfigurovatelném filtrovacím mechanismu.



Pole	Popis
Alias	Specifikuje Alias pro statický routovací účet
Description	Váš vlastní popis účtu
Action	**Forward To Address** Zpráva bude předána na tuto adresu **Forward To Domain** Zpráva bude předána na tuto doménu s příjemcem. **Forward To Host** Zpráva bude předána na tuto host adresu. V tomto poli může být uvedena buď host adresa, nebo IP adresa. **Deliver To This Domain** Zpráva bude doručena do aktuální domény a nebude prováděno žádné další filtrování. To je použiltelná metoda v případě, že chcete kontrolovat všechny zprávy a až potom doručit příjemci. Můžete také k čemukoliv chcete použít externí filtry. **Delete** Zpráva bude smazána

Forward	Toto pole nastaví Meraka tak, že bude předávat poštu přes Internet i v případě, že cílová doména je lokálně uložena na serveru. Tato funkce se používá v případě, že je na DNS serveru více MX záznamů pro jednu doménu a jiný mail server, která má větší prioritu nefunguje. Tento mail server tedy přijme zprávy a pokusí se je doručit jinému primárnímu mail serveru.
Value	Pole pro specifikaci hodnoty (adresy, domény, host adresy atp..).

Tabulka Accounts nastavení statiských rout nevyplěno

Pole	Popis
Save To	Pomocí této položky nastavíme ukládání všech zpráv, které byly prověřeny filtry a byly odfiltrovány. Do tohoto pole uvedeme cestu k adresáři, do kterého bude probíhat ukládání. Měla by zde být uvedena stejná hodnota, která je nastavena pro uživatelské emilové schránky. Tato položka může obsahovat plnou kvalifikovanou cestu.
Default Filter	Tato položka nastaví filtry, které budou na zprávy aplikovány. K editaci filtrů použijte tlačítka Add (přidat), Edit (editovat) a Delete (smazat). Každý filtr se řídí logickými pravidly vycházejícími z BUĎ a NEBO. Jedna logická hodota je pravdivá akce a podle toho je bude také funkce Static Routes zpracovávat.

External Filter	V této položce můžete nastavit externí filtr, který je vložen v samotném Merakovi. Externí filtr musí být DLL knihovna s touto funkcí, nebo nějaká spustitelná aplikace:
	
	TMessageStruct = Packed Record
	szOriginalAddress: Array [$00..$FF] Of Char;
	szRecipientAddress: Array [$00..$FF] Of Char;
	szFilename: Array [$00..$FF] Of Char; // Jméno dočasného souboru se zprávou
	End;
	
	Jsou zde také tři rozdílné možnosti nastavení: StdCall, Cdecl a Executable (spustitelný). První dvě možnosti specifikují typ DLL knihovny.
	
	Function MerakFilterProc(Var MessageStruct: TMessageStruct): Boolean; StdCall;
	
	Pokud funce vrátí pravdivou hodnotu, zpráva bude serverem zpracována. Pokud ne, nebude. Při importování DLL funkcí na to pamatujte. Jméno funkce je citlivé na velikost písma.
	
	Třetí parametr nastaví tento filtr jako spustitelný a tento filtr bude vždy zavolán. První parametr, který projde k samotnému spustitelnému filtru bude jméno zprávy. Pokud filtr vrátí jiný výstupní kód, než 0 bude zpráva zpracována serverem.

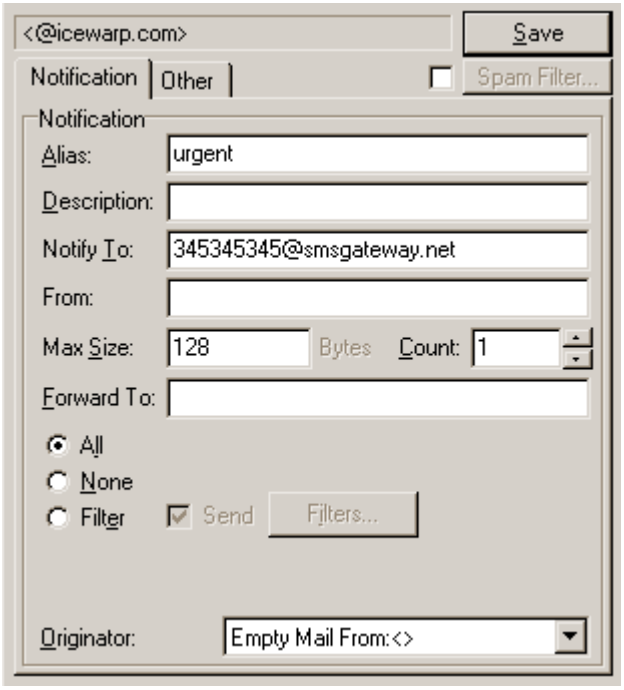
Anti Spam Filter	Jako vždy může být aplikován Antispamový filtr.

Doporučuejeme používat pro funkci statického routování předávání všech zpráv pro domény rozdílným externím mailserverům. Tuto funkci nemůže používat doménový alias dokud je cílová doména externí. Můžete dokonce vytvořit doménovou bránu.

Accounts (Notification - Upozorňovací)

Upozorňovací účet je účet, vytvořený pro konvertování zpráv do vhodného formátu Použitelného pro oznámení o doručení. V podstatě jde o zkrácení zprávy a odstranění příloh. Pro správné fungování tohoto nastavení, potřebujete mít k dipozici funkční emailovou bránu od vašeho poskytovatele, tzn. Zařízení, na které bude odesíláno upozornění o došlé zprávě musít mít vlastní emailovou adresu (mobilní telefon, pager,..).

Pozn. překladu: *V případě České republiky je potřeba mít aktivovanou u Vašeho operátora mobilních služeb e-mailovou adresu mobilního telefonu.*



Pole	Popis
Alias	Specifikujete alias, který se bude používat pro upozorňovací účet.
Description	Nějaký popisný text
Notify To	Specifikujete emailovou adresu cílového zařízení, na kterou má být již upravená zpráva zaslána
Forward To	Specifikujete emailovou adresu, na kterou bude zpráva předána.
From	Toto nastavení se bude uvádět ve zprávě v poli „from“
Max Size	Specifikujete maximální počet písmen, který bude akceptovatelný pro jedno upozornění. Nastavení tohoto pole je specifické pro každého poskytovatele telekomunikačních služeb. ***Pozn. Překladu:*** *obvykle se jedná o 160 znaků*
Count	V tomto poli nastavíte, jak se má Merak chovat, když je zpráva větší, než maximální počet povolených znaků. Jinými slovy, do kolika kusů může zprávu

	Merak rozčlenit. Nastavením hodnoty 1 do tohoto pole a čísla 128 do pole určujícího maximální velikosti docílite odeslání prvních 128 znaků. Nastavením hodnoty 2 do tohoto pole docílíte odeslání prvních 256 znaků rozčleněných do dvou zpráv a předaných na cílovou bránu.
Skip attachments	Pokud je přijmuta zpráva s přílohou, je příloha vyjmuta a zpráva je odeslána jako prostý text.
Into Subject	Text bude umístěn do předmětu předáváného upozornění.

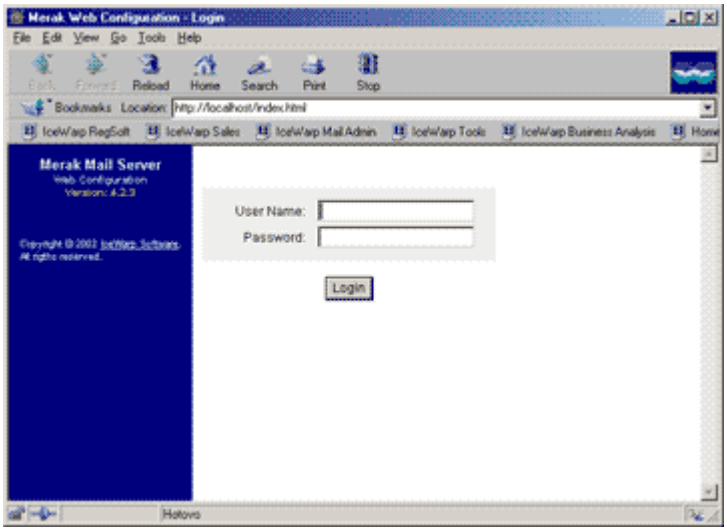
Tabulka upozorňovacích účtů nevyplněno

Pole	Popis
To	Specifikujete hodnotu, která se bude uvádět v poli To (příjemce) odesílaných zpráv
From	Specifikujete hodnotu, která se bude uvádět v poli From (Odesilatele) odesílaných zpráv
Subject	Specifikujete hodnotu, která se bude uvádět v poli Subject (předmětu) odesílaných zpráv
Body	Specifikujete text, který se bude uvádět v tělech odesílaných zpráv
Date / Time	Specifikujete datum a čas, které umisťovat do odesílaných zpráv
All	Budou odeslány všechny zprávy
None	Nebudou odeslány žádné
Filter	Zprávy budou odeslány podle specifikovaných filtrů
Send	Pokud je funkce aktivována, a filtr je platný, bude zpráva odeslána. Jestli že je funkce aktivní a filtr je neplatný zpráva odeslána nebude. Pokud funkce není aktivní a filtr je platný zpráva nebude odeslána. Pokud je tato funkce neaktivní a filtr je neplatný, bude zpráva odeslána.
Originator	U funkce “Originator” se jedná o pokročilé nastavení SMTP protokolu. Ve chvíli, kdy se připojujete na SMTP server, používáte příkaz MAIL from <hodnota>. Obě hodnoty můžou být prázdné, vyplněné s odesilatele nebo vlastníkem mailing listu. Pokud zvolíte variantu “Sender or Owner”, všechny zprávy, které se vrátí zpět, budou odeslány na tuto e-mailovou adresu.
Subject	Každý upozorňovací účet může používat vámi definované téma zprávy. Obsah tématu můžete nastavit pomocí této položky.
Body	Každý upozorňovací účet může používat vámi definované tělo zprávy. Obsah těla můžete nastavit pomocí této položky.
Text File	Každý upozorňovací účet může používat vámi definované tělo zprávy. Obsah těla můžete nastavit pomocí této položky. Do zprávy bude vložen celý obsah textového souboru..

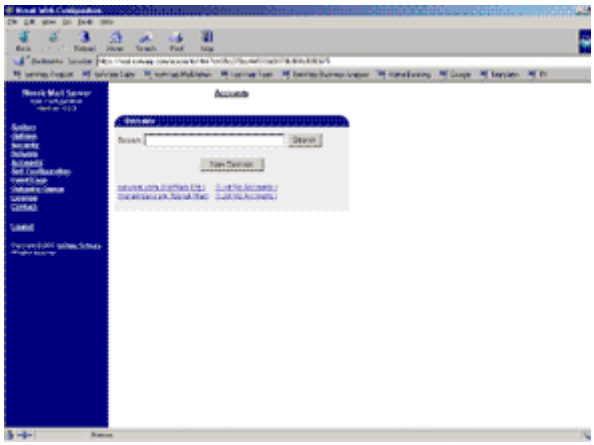
Webové administrační rozhraní

Merak má integrovaný web server, který vám dovoluje vzdálenou administraci přes webový interface. Používání této funkce nemusí být možné pouze pro administrátory jako vždy, mohou i uživatelé (pokud to mají povolené) administrovat své vlastní účty. Jestliže se chcete k tomu rozhraní přihlásit, potřebujete v nastavení účtu Meraka definovat uživatele s možnostmi buď: administrator, self configurable (uživatel, který si bude moci sám konfigurovat základní nastavení, nebo domain administrator (doménový administrátor).

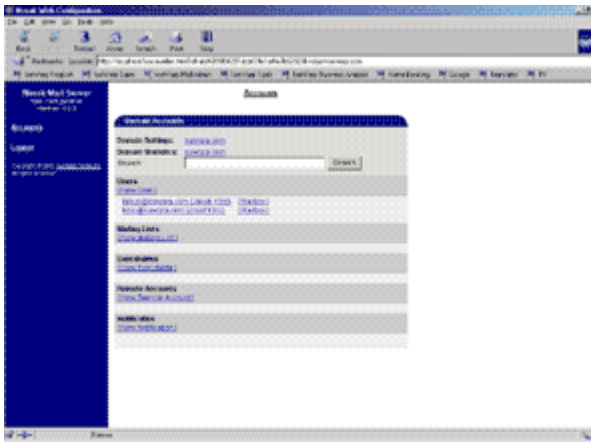
Otevřete si váš internetový prohlížeč a zadejte host, nebo IP adresu serveru, na kterém je Merak spuštěn, webové rozhraní funguje na portu 32000 (např. http://192.168.11.92:32000). (řiďte se prosím podle vašeho nastavení)



Bude po vás vyžadováno uživatelské jméno a heslo. Do tohoto pole můžete zadat jméno nějakého administrátora, doménového administrátora, nebo uživatele, který se má právo konfigurovat. Standardní uživatelé nebudou touto volbou přijmuti.



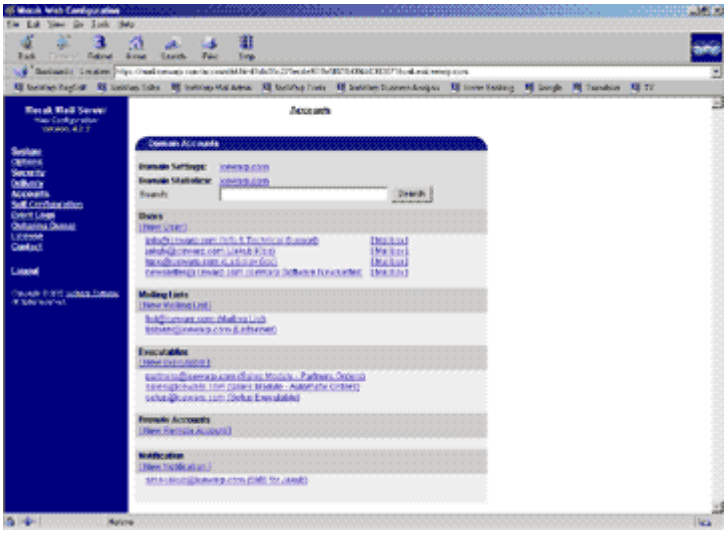
Úvodní obrazovka administrátora



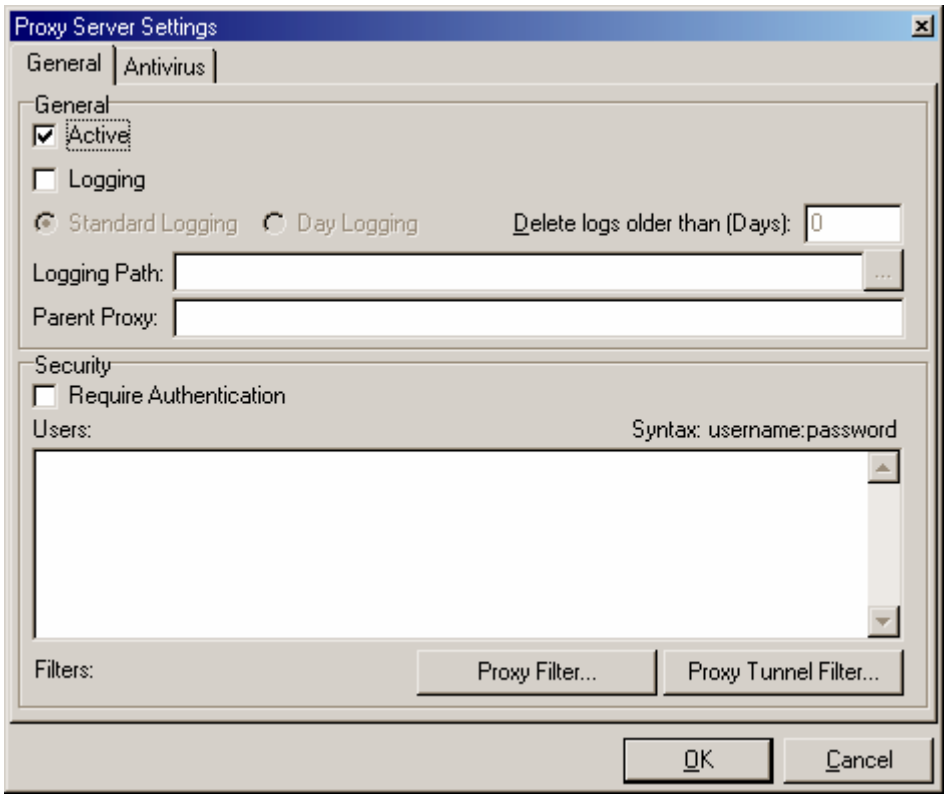
První obrazovka administrátora po příhlášení

Navigace ve webovém rozhraní je stejná jako ve zde popsané odkazové sekci.

Je docela dobrý nápad používat pro vzdálenou administraci přes webové interface zabezpečené SSL rozhraní (čtěte v další části dokumentace).



Proxy server



Merak má v sobě intergrovaný také plně použitelný IceWarp Proxy server. Jediné, co potřebujete je nakonfigurovat váš internetový prohlížeč pro používaní proxy serveru. Host adresa počítače bude stejná s host adresou, kterou používá Merak. Port je stejný, jako port kontrolního serveru (spuštěném standardně na portu 32000). Pokud je Merak jednou nakonfigurován, můžete používat i IceWarp Proxy server.

Autentifikace
Můžete také nastavit speciální uživatele, kterým umožníte použít proxy server až potom, co se autentifikují. Tyto uživatelé ale nejsou skuteční uživatelské účty v Meraku. Všechny uživatele je nutné nastavit je v dolním textovém poli.

Příklad:
user1:pass1
user2:pass2

Pokud nejsou použity žádné filtry a je vyžadována autentifikace, musí být autentifikování všichni uživatelé a to před přístupem na jakoukoliv adresu. Pokud vytvoříte filtry, povolíte potom se nebudou muset vybraní uživatelé autentifikovat.

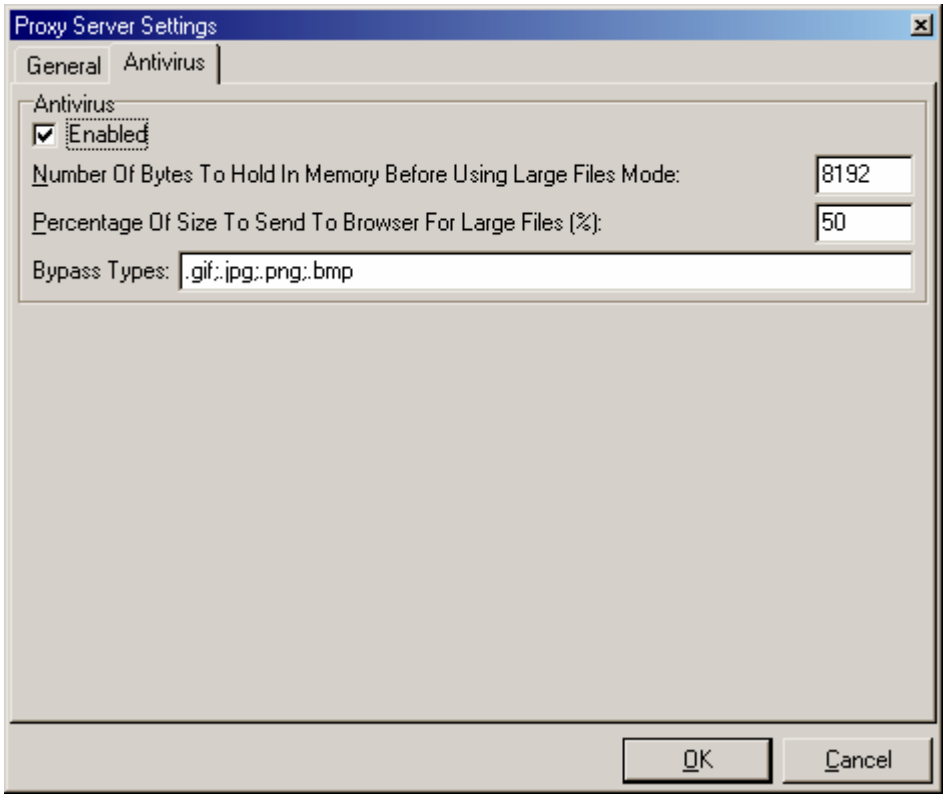
Filtr může obsahovat URL, IP adresu, nebo port. Např:

```
http://www.sexualnihratky.cz
0-191.*.*.*
193-255*.*.*
192.168.0.10
:0-79
:81-65535
```

Na tomto příkladu demonstrujeme nastavení, které má za účinek zákaz přístupu na www.sexualnihratky.cz a povoluje přístup z adres 192.*.*.* vyjímaje 192.168.0.10. Bude pracovat

pouze s 80 portem.

Proxy Server Antivirus



IceWarp proxy server dokáže používat integrovaný antivirus v Meraku. Jakmile je antivirus aktivní, scanuje všechny stažené soubory.

Funkce “Memory scanning” ukládá do paměti všechny soubory až po stanovenou velikost. Tyto soubory jsou poté scanovány a pokud není nalezen virus, jsou poslány webovému prohlížeči. Pokud je virus nalezen je webovému browseru zaslána stránka oznamující nalezení viru.

Větší soubory jsou scanovány procentuálně. To znamená, že prohlížeči je zaslána pouze procentuální část souboru zbytek sobuoru se neodesílá. Jakmile je soubor přijmut proxy serverem, je celý proveřen a poslán dál. Pokud je soubor infikovaný, je zbytek souboru vyplněn nulami. To znamená, že infikované soubory budou automaticky poškozené a nemohou na klientském počítači nijak uškodit.

Můžete nastavit koncovky souborů, které nebudou prověřovány.

Zabezpečená spojení (SSL)

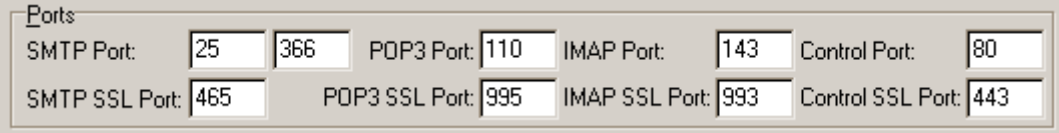
SSL je kryptovací metoda založená na veřejném a privátním klíčy. SSL zajistí, že informace, které budou protékat mezi web serverem a prohlížečem nebude moci kdokoliv prohlížet a tím zajistí vaše soukromí.

Merak používá jeho vlastní integrovaný webserver. Ten plně podporuje standard SSL. Pokud se rozhodnete tuto funkci využívat, budete muset dělat jednu věc jinak. Spojení uskutečnovaná pomocí SSL využívají odlyšné URL:

https://<server>:<port> (parametr https řekne vašemu prohlížeči, že se jedná o chráněnou soketovou vrstvu).

Např.. https://192.168.11.92:32001

Port musí bý standardně nastaven na číslo 32001. Jeho nastavení můžete případně změnit ze Systémových nastavení:



Na této ukázce obrazovky je port standardního administračního rozhraní změnen z portu 32000 na 80 a port SSL administračního rozhraní z portu 32001 na 443.

Porty 80 a 443 jsou průmyslově využívanými standardy pro web a zabezpečený web. To znamená, že nastavením těchto standarních hodnot dosahnéte toho, že za vámi zadávané URL nemusíte psát čísla portů. Např. http://192.168.11.92 bude standarní administrační rozhraní a https://192.168.11.92 bude SSL administrační rozhraní.

Pokud vše funguje, budete pozdravení následujícím varováním:

Co toto varování znamená ?

SSL certifikát vyžaduje 3 podmínky:

1) Musí být vydán od důvěryhodné společnosti
2) Musí být správné datum vydání certifikátu
3) Jméno bezpečnostního certifikátu se musí shodovat se jménem stránky

Ve světě je pouze pár společností, jimiž vydané certifikáty jsou automaticky brány internetovými prohlížeči za hodnověrné (např. Verisign and Thawte). Jestliže je tento certifikát používán spolu se softwarem IceWarp web browser ho nebude brát jako hodnověrný.
K vyřešení tohoto problému, klikněte na tlačítko „View Certificate“ (zobrazit certifikát) a posléze na „Install Certificate“ (instalovat certifikát). Tím řeknete vašemu web browseru, že certifikát lze považovat za hodnověrný.

Bohužel není možné vyřešit problém v bodě 3 (jméno bezpečnostního certifikátu se musí shodovat se jménem stránky).

SSL a certifikáty jsou velmi komplexní řešení. Za certifikáty, ve kterých se vám nezobrazuje varovná hlaška se musí společnostem jako je Verisign nebo Thawte platit. Pokud si přejete obstarat váš vlastní certifikát od důvěryhodné společnosti, kontaktujte IceWarp software (e-mail: podpora@icewarp.cz), myslím, že Vám bude schopni poradit.

Certifikát je uložen v souboru cert.pem. Můžete ho editovat a vytvořit váš vlastní certifikát. Vlastní SSL systém je výborné výhoda, protože je možné mít na jednom systému více SSL certifikátů. Každý certifikát může být využíván odlišnou IP adresou. Soubor cert.pem je používán jako standardní certifikát. Je tam také soubor cert.dat s následující strukturou:

```
[Server]
// [IP]=[certificate file path]
193.179.195.74=c:\certificates\icewarpcert.pem
193.179.195.75=c:\certificates\merakcert.pem
```

Ve varování ohledně certifikátu pokračujte stisknutím tlačítka „Yes“ (ano). Zobrazí se vám obrazovka vzdáleného administračního rozhraní.

Pro uživatelé prohlížeče Internet Explorer, ve spodní části internetového prohlížeče je umístěna lišta indikující stavy jednotlivých služeb. Pokud je zde zobrazen symbol zabezpečení, je vše v pořádku.

Pro uživatele Netscapu, vypadá ikona v dolní části prohlížeče asi takhle:

Toto je pro uživatele potvrzení o bezpečnosti spojení

Důležité upozornění !

Zabezpečena je pouze komunikace mezi prohlížečem internetových stránek a serverem. Nemá to žádný vliv na čtení, nebo odesílnání Emailů.

4. Merak Mail Server Power Pack

Power Pack

Merak Mail server power pack spojuje dva produkty v jeden. Těmito dvěma produkty jsou Merak Mail server a IceWarp Web Mail.

Hlavní výhodou tohoto balíku je, že Icewarp Web Mail je ihned po instalaci automaticky nakonfigurován všemi nastaveními hned potom, co je dokončena instalace. Nemůsíte ručně nastavovat žádné integrační paramtery. Okamžitě po instalaci produktu můžete začít využívat oba produkty bez jakékoliv další separátní konfigurace.

Další výhodou je, že nepotřebujete instalovat žádné další služby které by se musely nainstalovat. IceWarp Web mail. Tenbude spuštěný pod kontrolními službami Meraka. Služby zajištující Merakovu administraci a IceWarp web mail budou používat stejné TCP/IP port. Ten je standardně nastaven na 32000.

IceWarp Web Mail

V používání obou produktů nejsou žádné zásadní rozdíly. Merak jednoduše provozuje pomocí svého integrovaného web serveru IceWarp Web Mail. Je zde ale malá změna v zadávaném URL.

Pro přístup do webmailu musíte zadat URL v následujícím formátu:
http://vasserver:32000/mail/

Objeví se přihlašovací obrazovka IceWarp webmailu

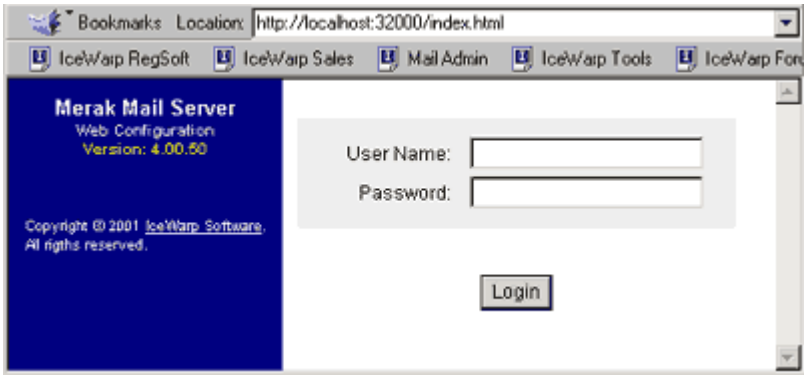
Nastavení a veškerá konfigurace pro IceWarp webmail je umístěna v adresáři **Merak\ WebMail**. Pro webovou administraci webmailu potřebujete využívat URL http://localhost:32000/mail/admin/. Pokud vás zajímají další podrobnosti, prohlédněte si **IceWarp Web mail PDF dokumentaci.**

Pokud potřebujete konfigurovat virtuální hosty a jiná webserverová nastavení, budete potřebovat editovat soubor **Merak\Config\WebServer.cfg**. Platí zde stejná pravidla jako pro web mail.

Web konfigurace Merak Mail server

Samotná administrace Meraka zůstáva stejná. Jednoduše použijete pouze produkt Merak Mail server.

Zadáte do vašeho internetového prohlížeče stejné URL, jako je toto:
http://vasserver:32000
Administrační obrazovka Meraka se vám automaticky objeví:



5. Úvody do nastavení

Mailing List

Tato část manuálu vám skrz na skrz vysvětlí vytváření mailing listů, které budou mít schopnost být vzdáleně administrovány přes email (tuto funkci mají integrovanou list servery).

Pro potřeby tohoto příkladu si představíme následující fiktivní situaci:

Máme zde skupinu lidí, kteří si přejí diskutovat o počítačích a přídružených tématech pomocí svého vlastního mailing listu (konference). Zaregistrovali si vlastní doménu pc-tech.com a přejí si nastavit mailing list pojmenovaný chat@pc-tech.com. Oni sami se rozhodnou, kdo bude vlastník (a tedy i adminstrátor) mailing listu a přidělí mu uživatelský účet admin@pc-tech.com.

Tito lidé se rozhodnou, že hlavní diskuzní skupina bude umožňovat komukoliv volně vstoupit a bude tedy nemoderovaná. Také se rozhodnou, že nový uživatelé by měli být schopni přihlásit do diskuzní skupiny sebe sama.

Posledním přáním, je mít možnost jednoduše identikovat zprávy z jejich skupiny tak, aby všechyn zprávy měli zřetelnou hlavičku a bylo na ně jednodušeji možné aplikovat filtry.

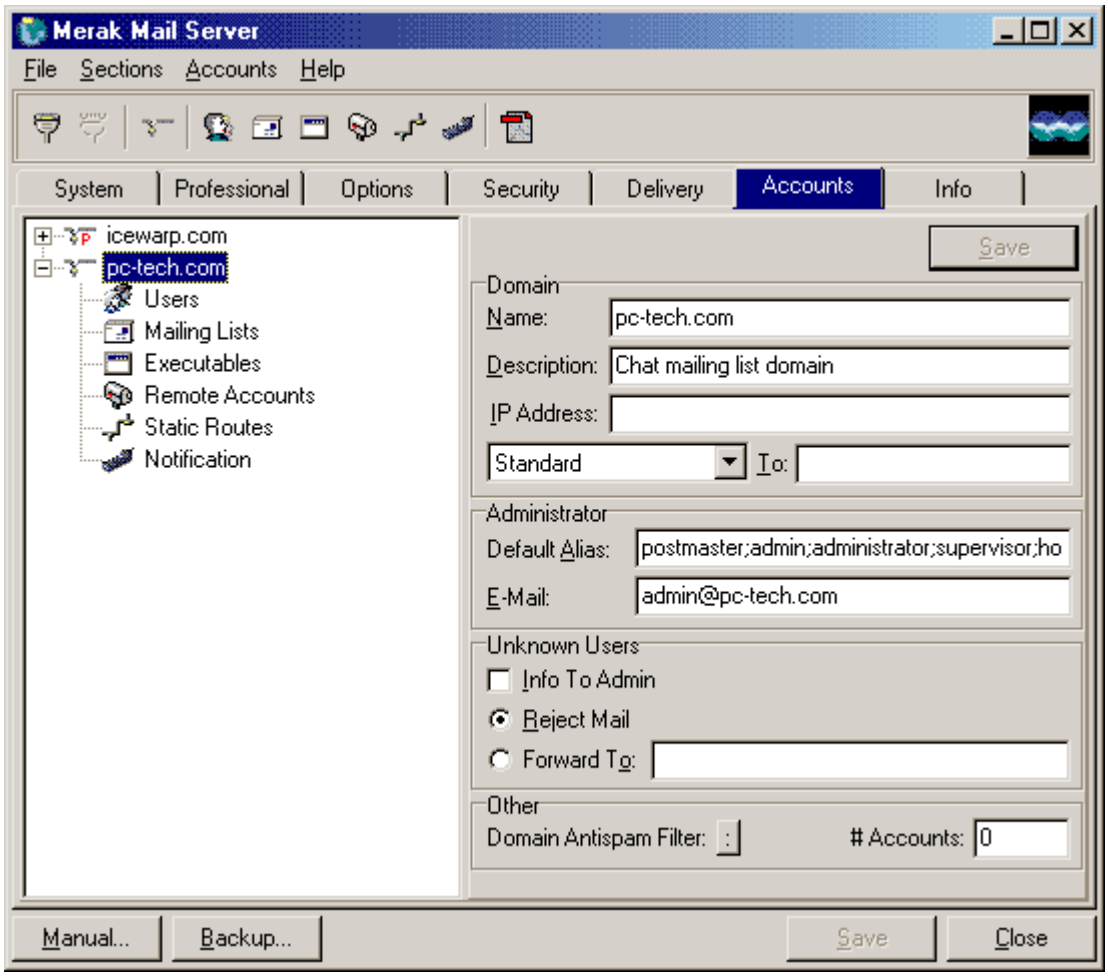
Jednotlivé nastavovací úkony:

- **vytvořit doménu**
- **vytvořir administrační účet**
- **vytvořit mailing list**
- **vytvořit list server**
- **otestovat list server**
- **otestovat mailing list**

a) Vytořit doménu

Otevřete si konfigurační applet Meraka a pod nabídkou Accounts (účty), zvolte nabídku New Domain (nová doména)

Zadejte informace potřebné k vytvoření domény a stistkněte tlačítko save (uložit)

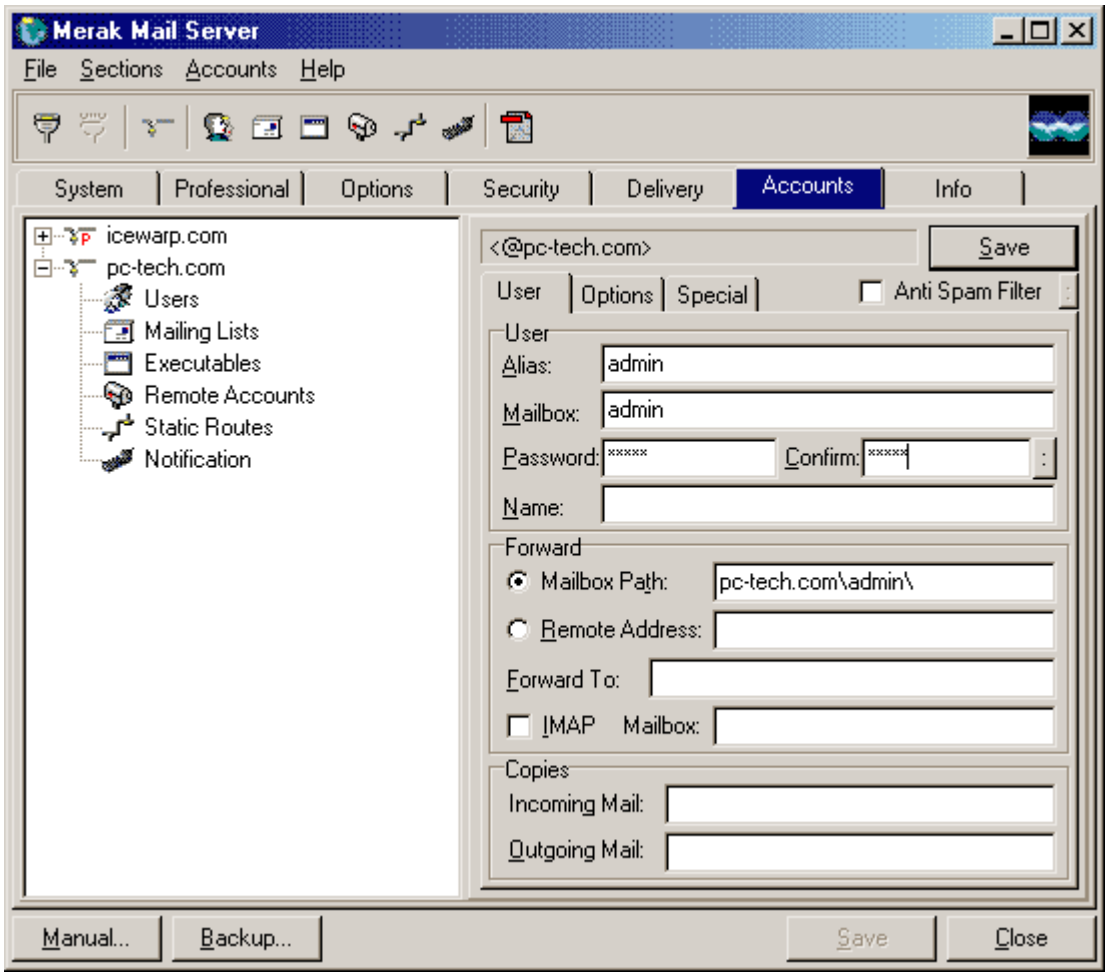


Tady máme vytvořenou doménu pc-tech.com, máme nastavené předávání emailů směřovaných na aliasy správce poštovního serveru na adresu admin@pc-tech.com, máme také nastaveno, že veškeré zprávy odesláné neznámým uživatelům budou odmítnuty a upozornění na tyto zprávy bude zasláno administrátorovi.

b) vyvráření administračního účtu

Zatímco doména pc-tech je stále zvýrazněna, zvolíme z nabídky Accounts (účty) položku Add (přidat) a potom New User (nový uživatel).

Zadáme informace tykající se účtu a stiskneme tlačítko Save (uložit)

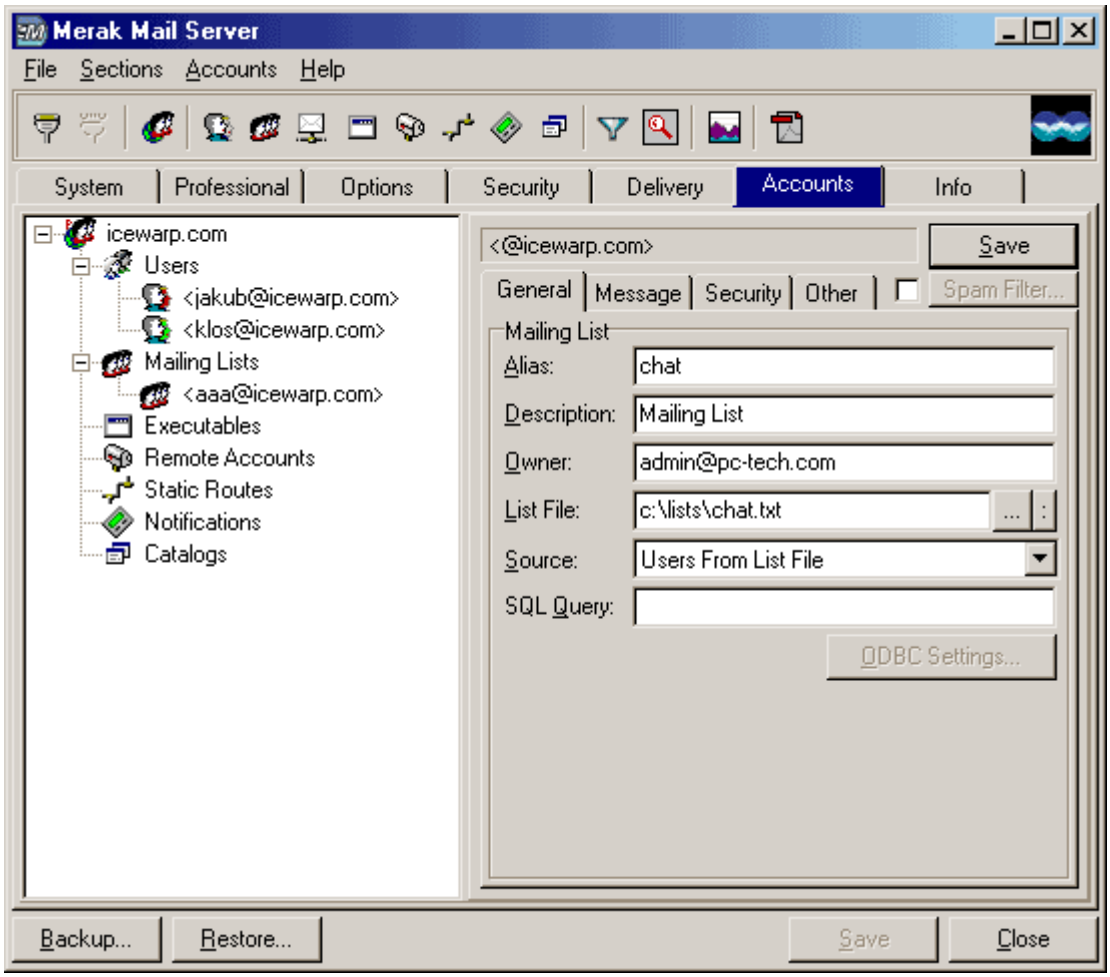


Když máme vytvořený účet admin@pc-tech.com (používající alias admin), vlevo je jméno poštovní schránky stejné, jako alias. Také je nastavené standardní ukládání zpráv do adresáře admin tzn. není nastavené žádné předávání zpráv.

c) Vytvoření mailing listu

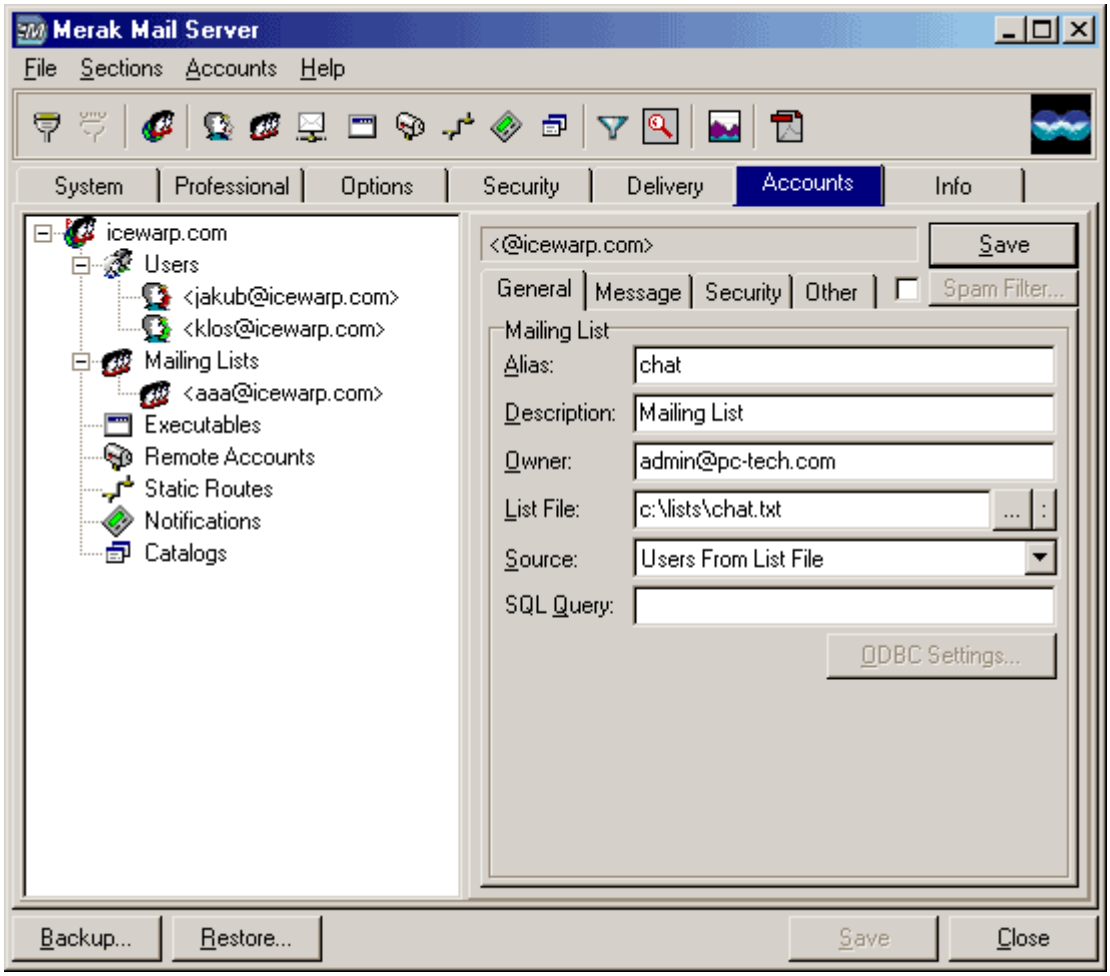
Zatímco doména pc-tech je stále označena, zvolíme z tabulky Accouts položku přidat a zvolíme “New mailing list”

Zadejte detailní nastavení a zmáčkněte Save.



Alias chatu byl nastaven jako chat@pc-tech.com. Vlastníkem byl určen účet admin@pc-tech.com.

Seznam účastníků bude obsluhován list server, nyní ale potřebujeme zvolit soubor, který bude použit pro uložení informací o účastnících. Ten byl nastaven jako c:\list\chat.txt



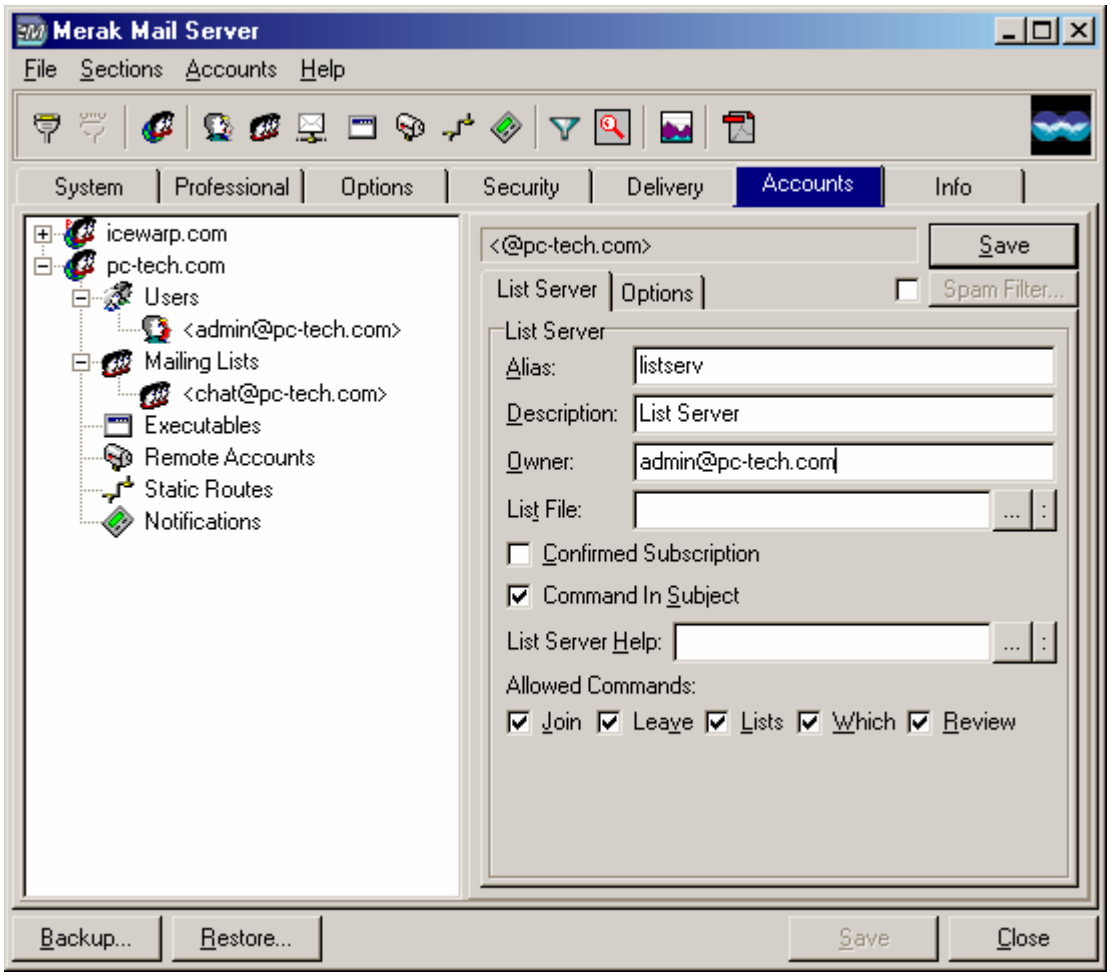
Chceme, aby e-mailové zprávy vypadaly, jako že pocházejí od individuálních uživatelů, nicméně odpovědi musí být posílány zpět na chat. V takovém případě musíme nastavit odlyšné “From:” a “Reply To:”.

V posledním poli nastavujeme požadavek na zřetelnou hlavičku v tématu zprávy. V nastavení je předdefinováno, že každé téma zprávy bude obsahovat ‘[PC-tech] ‘

d) Vytvoření list serveru

Zatímco doména pc-tech je stále zvýrazněna, zvolíme z nabídky Accounts (účty) položku Add (přidat) a potom New List server (nový list server)

Zadejte informace o vytvářeném list serveru a stiskněte Save (uložit)

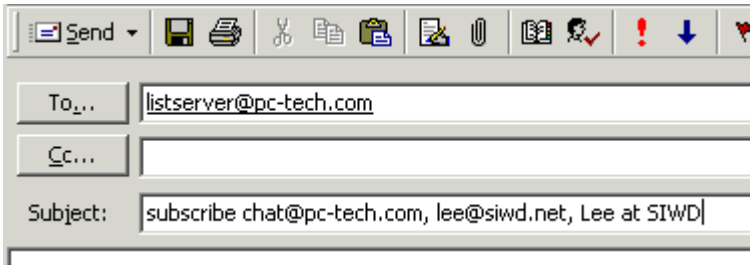


Příkazy pro doplění list serveru budou zasílany na adresu listserv@pc-tech.com, tak je totiž nastaven alias pro list server. Stejně jako u maling listu je jako vlastník nastaven účet admin@pc-tech.com

Pole 'List Server' je automaticky zaškrtnuto, také můžete nastavit používání příkazů v předmětu zprávy. Jsou povoleny všechny příkazy.

e) Testování list serveru

Pro opravdové otestování námi vytvořeného list serveru ho budeme potřebovat požádat o přidání nějakého účtu mezi odběratele.



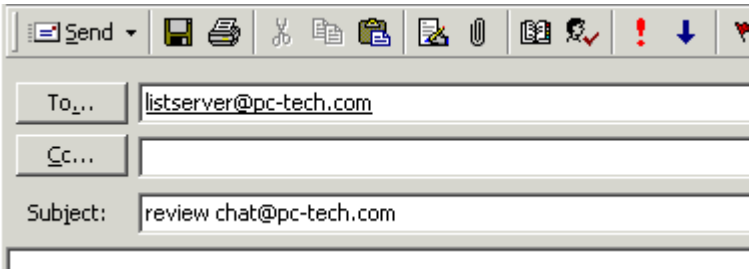
Zasíláme zprávu, žadající o přidání nového uživatele Lee.

Krátce po odeslání našeho požadavku, přijeme následující zprávu:

```
List server report: User Lee at SIWD <lee@siwd.net> has been successfully subscribed
to the mailing list: chat@pc-tech.com

Recipient: Listserver account <listserver@pc-tech.com>
User Lee at SIWD <lee@siwd.net> has been successfully subscribed to the mailing
list: chat@pc-tech.com
```

V rychlosti zkontrolujeme soubor c:\pctechlist.txt, zda byl uživatel skutečne fyzicky přidán.

Zasláním zprávy si můžeme nechat list serverem zaslat seznam všech uživatelů:



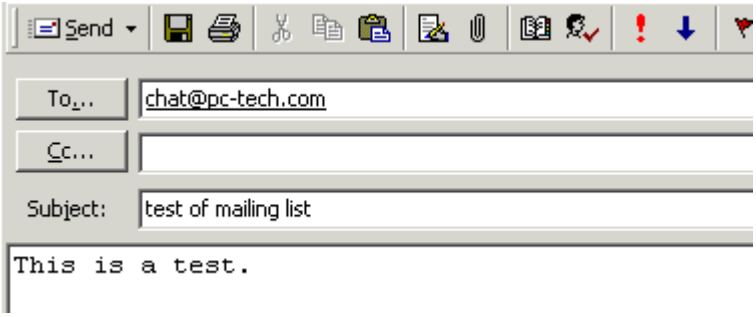
Od list serveru se nám vrátí následující zpráva:

```
List server report: chat@pc-tech.com

Recipient: Listserver account <listserver@pc-tech.com>
All members of the mailing list: chat@pc-tech.com

Lee at SIWD <lee@siwd.net>
```

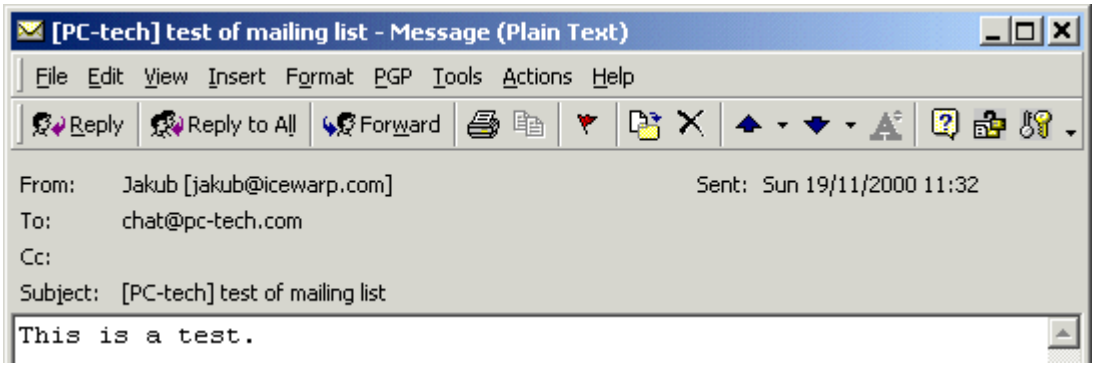
List server funguje perfektně.

e) Testování Mailing listu

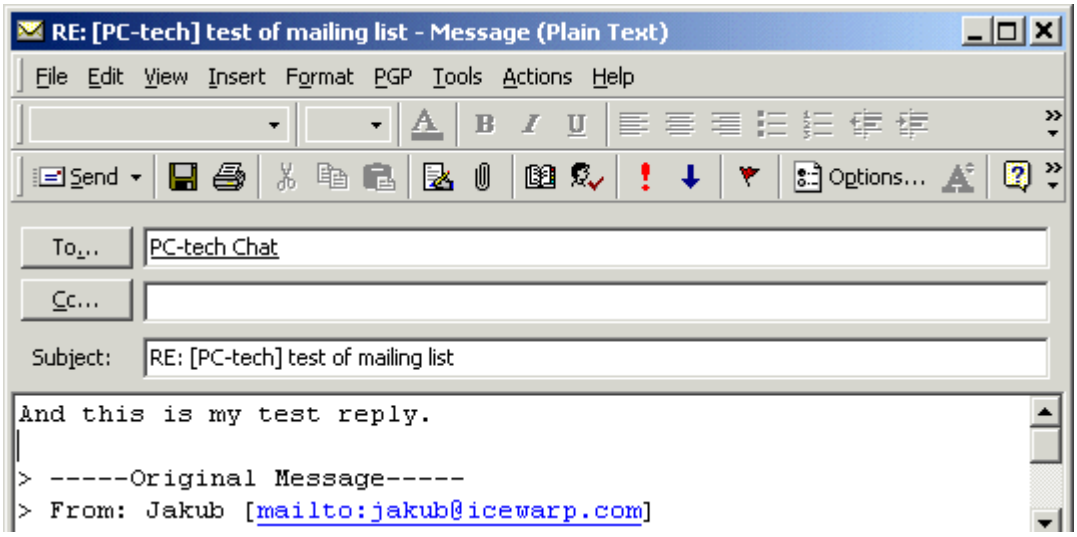
Pokud chceme opravdu otestovat mailing list, zašleme do něho zprávu, kterou by měli později přijmout všichni přihlášení odběratelé. Zkontrolovat by se měla unikátní hodnota v předmětu zprávy, dále adresa uvedená v adresátovi zprávy a odpovědní adresa.



Zasíláme zprávu s velice jednoduchými paramtery. K odeslání zprávy byl použit uživatel, který se jmenuje Jakub a který má emailovou adresu jakub@foo.com. Krátce po našem odeslání zprávy je zpráva přijmuta:



Jak můžeme vidět, odesilatel zprávy byl identifikován a téma zprávy začíná námi nastaveným indentifikátorem. Když na zprávu odpovíme, bude zaslána opět do mailing listu.



Náš mailing list funguje perfektně.

Relaying a hláška "...we do not relay"

Relaying (předávání zpráv mezi mail servery) je docela běžný problém. Celý tento problém spočívá v tom, že mail server dovolí nějakému uživateli poslat zprávy ven. Nicméně vy potřebujete, aby zprávy z vašeho mail serveru mohli odesílat pouze vaši uživatelé. K tomu je nutné využít antirelayingove funkce, které jakýmkoliv něchtěným uživatelůmnedovolí přes váš server posílat spam a předávat zprávy.Chybová hláška "550 5.5.1 <>...we do not relay <>" vám indikuje nesprávné nastavení vaších anti relayingovacích funkcí. Což má zá následek to, že nemůžete ven přes váš server odesílat žádné zprávy.

Nenavrhujeme používání žádných jiných antirelayingových funkcí, než které umožňuje používat Merak. Ten má tři základní funkce zabraňující nechtěnému odesílání zpráv. **Relaying from (relaying z..), POP before SMTP (POP před SMTP) a Separate Relaying (separátní relaying).** Všechny ostatní anti relayiongové funkce, v nastavovací nabídce "Delivery" by neměli být používány. Zapněte námi tři výše uvedené funkce a do pole Relaying From zadejte:

127.0.0.1;192.168.*.*;10.*.*.*;172.16-31.*.*

IP adresy a rozsahy zadané v poli relaying from budou schopny předávat zprávy. Všechny z námi výše uvedených IP adres a rozsahů jsou IP adresy používané LAN síti. V poli je také potřeba uvést samotnou IP adresu serveru. Pomocí tohoto nastavení budete moci zcela bez problému odesílat ven zprávy z vaší lokální sítě.

Někdy můžete potřebovat povolit relaying (předávání) také vašim zákazníkům, kteří se nacházejí mimo váší LAN. To je malý problém, ale může být vyřešen. Většinou je relaying řešen na bázi IP adres. Stejně, jako byla řešena LAN. Např. internetový poskytovatelé znají zákaznické IP adresy a povolí relayingování z těchto adres. To je řešení navrhované pro uživatele zvenku. Můžou použít IP adresu, kterou jim přidělí jejich internetový poskytovatel a pomocí ní odeslat přes mail server poskytovatele poštu. Jistě, vy ale potřebujete používat váš mail server. K vyřešení tohoto problému můžete použít dvě funkce. Buď funkce POP Before SMTP nebo SMTP autentifikaci Používání funkce Relaying from není možné protože IP adresa vašeho externího uživatele není známá, a mění se dymaicky.

Funkce POP Before SMTP

Princip této funkce je velmi jednoduchý. Aby měl uživatel možnost relayingu, musí si před samotným odesláním zprávy zkontrolovat došlou poštu. Server si zapamatuje užiavatelovu IP adresu a v daném časovém intervalu mu dovolí ze zaznamenané IP adresy odesílat zprávy. Tato funkce má ale u některých emailových klientů nepracuje správně. Např. Outlook Express nejdříve zprávy odesílá a až poté kontroluje. Uživatel bude muset pamatovat na to, že si musí provést nejdříve manuální kontrolu poštovní schránky a až poté může odesílat.

SMTP Autentifikace

SMTP Autentifikace je více profesionálním cestou, jakou se dá povolit externím uživatelům relayingovat přes váš server. Uživatel se bude muset během SMTP spojení autentifikovat, aby server věděl, že jedná s legálním uživatelem účtu a dovolil mu relaying zpráv. Uživatel bude muset mít ve svém emailovém klientovi nastaveno, že používá SMTP Autentifikaci a vy budete muset v nastavení Security deaktivovat položku „Disable SMTP Auth“.

Používání všech tří funkcí dohromady není problém.

Bezpečnost (Relaying a Spam)

Právě v této fázi se dostáváme k jednomu z nějvěžších úspěchů Meraka. Merak má velmi dobrý poměr mezi odstraněním spamu a přijetím běžných zpráv. To bývá důležitá otázka u každého mail serveru.

Relaying je v podstatě posílání zpráv ven. A to je důvod, proč tuto službu poskytovat pouze požadovaným uživatelům, zatímco externí uživatelé, nebo vetřelci by tuto možnost mít neměli.

Spam (nebo spamming) je zasílání nevyžádaných zpráv na emailové adresy. Typickým příkladem jsou zprávy nabízející zboží a služby. S těmi by se mělo nakládat velmi uváženě, protože skutečně seriozní společnost nezasílá spamy.

Organizace, která spamuje pomocí svých dlouhých seznamů emailových adres vždycky sleduje, které emailové servery povolují relaying; takovou cestou totiž může spammer chránit svoji identitu. Proto je důležité považovat relayingové a anti spamové funkce Meraka za velmi důležité nastavení.

Máme fakticky tři možné scénáře:

1. Společnost používá Meraka pouze pro svoje interní účely (Interní)

2. Společnost používá Meraka pro svoje interní ale také externí účely a má k dispozici neustálé připojení na internet, nebo používá modemové spoje (Externí)

3. Nějaký Internetové poskytoval používá Meraka pro poskytování emailových služeb svým zákazníkům (ISP)

Každý z těchto tří scénářů vyžaduje nastavení a přístup

Společné nastavení pro všechny scénáře

Nejlepší obranou proti spamu je používání seznamů RBL. Můžete také použít Antispamové filtry ale problém nastavává při jejich časté aktualizaci. RBL seznamy bývají administrovány Internetovými uživateli a jsou regulerně aktualizovány.

Obsah filtrů je další můžete nastavit proti spam a také virům: např. Můžete nastavit obsahový filter, který odmítne všechny zprávy s řetězcem „I Love You“ v hlavičce zprávy.

Interní použití

Při použití na intranetu firmy nehraje bezpečnost moc velkou roli. Není potřeba konfigurovat firewally, nebo různé další bezpečnostní funkce. Není potřeba nastavovat ani antirelayingové funkce. Je velmi málo pravděpodobné, že se nějaký pracovník ve firmě chystá spamovat svoje kolegy. Pro toto řešení je doporučeno mít funkce antirelayingu deaktivované. Nejsou zde žádné externí zprávy, takže si nemusíme dělat starosti s ověřováním původce zprávy.

Všechny zprávy jsou odesílány a přijímány přes lokální domény, jsou zde tedy 2 použitelná nastavení: „Do not forward if the originators domain is not local“ a pod každým účtem „User can send mail only to local domains“.

Externí použití

Ve firmě je malý mail server, který je možné vidět z internetu. Byla by tedy při věci myšlenka aktivovovat firewall pro „Control Service“ (kontrolní službu) tak, aby bylo možné měnit jakékoliv nastavení pouze interně z počítače. Další dobrou myšlenkou je zákaz schopnosti připojovat se na služby pomocí telnetu.

Poslední věcí, kterou firma pro svůj mail server potřebuje je být používána pro odesílání Spamů, nebo další nevyžádáné pošty. To vrhá na společnost špatný dojem a navíc to může mít další důsledky. Je velmi důležité, aby jediní lidé, kteří budou schopni odesílat zprávy přes firemní mail server byly zaměstnanci firmy. Tento scénář je poměrně snadno realizovatelný, protože všichni zaměstnanci jsou fixováni na jednoduše definovatelnou síť.

Například, budeme předpokládat, že společnost má nastavené 3 oddělení a 3 podsítě privátních adresových rozsahů:

192.168.1.X
192.168.2.X
192.168.3.X

Pouze klienti z těchto IP adres budou mít povoleno odesílat zprávy přes firemní mail server. Nastavíme funkci „Relaying from“ a zadáme hodnotu 192.168.* nebo (více bezpečné nastavení), zadáme 192.168.1.*; 192.168.2.*; 192.168.3.*

Dokonce je snadnější místo rozsahu IP adres nastavit doménu(y) společnosti. To povolí pouze uživatelům interní sítě používat server k odesílání zpráv do internetu.

Pamatujte na to, že musíte zadat obě podsítě nebo IP adresy serveru!!

Pokud server přijme zprávy z nějakého externího zdroje, byla by velmi dobrý nápad zkontrolovat zda email adresa pochází ze skužečně existující domény. Aktivujte funkci „Reject mail if the originators domain has no MX record“. Toto nastavení automaticky odmítne zprávu, která nebude odeslána z platné emailové adresy, nebo nebude mít platnou zpáteční cestu.

Poskytovatel internetových služeb

Internetový poskytovatel prožívá zajisté při nastavování nejtežší okamžiky. Nesmí nakonfigurovat až příliš zabezpečený mail server, který zabrání zákazníkům odesílat, nebo přijímat zprávy.

Zajisté, by mělo být nastavené zabezpečené webové administrační rozhraní a zakázaný telnet. Ale aby přístup k administračnímu rozhraní mohl být získán odkudkoliv, je potřeba nastavit firewall.

Je dobrý nápad kontrolovat u příchozích zpráv platnost domény. Zapněte funkce „Reject Mail if the originators domain has no MX record“ tato funkce zajistí, že když zpráva přijde z neplatné adresy, bude serverem odmítnuta.

Nyní se budeme soustředit na anti.-relaying. Máme 2 druhy ISP: první, který kontroluje také uživatelský přístup na internet (z tohoto důvodu budou všichni uživatelé lehce identifikovatelní pomocí IP adres a podsítí), a druhý nezávyslí ISP, kteří budou vyžadovat, aby uživatelé byli schopni využívat server bez ohledu na to, jak jak jsou připojeni na internet.

Pro oba typy ISP je hlavní to, že server nebude používán o k odesílání Spamu.

Pro ISP, kteří mají přehled o tom, které podsítě a IP adresy používají uživatelé k připojování , je jednoduché řešení. Stačí nastavit anti-relayingové funkce zadáním podsítí/IP adres do pole.

Pokud budeme zadávat větší množství položek, bude potřeba (a bude snadnější) vytvořit soubor **relay.dat** (v konfiguračním podadresáři) a specifikovat každou položku na oddělenou linku. Např.

192.168.1.*
127.0.0.1

Pro ISP, jejichž uživatelé se na server připojují z různých IP adres není proveditelné zadávat do relayingových nastavení podsítě a IP. Namísto toho, mohou být zapnuty všechny vyjímaje lokální server a také mohou být nastaveny alternativní metody uživatelské autentifikace jakou jsou POP3 before SMTP a SMTP autorizační příkazy.

Obě funkce (POP3 before SMTP a SMTP autorizace) bude potřeba využít k tomu, aby uživatel, který nemá účet na mail serveru byl schopen odesílat zprávy.

6. LDAP

LDAP

LDA je zkratka pro **Lightweight Directory Access Protocol**.

LDAP vám umožní “lokalizovat organizace, individuální uživatele, nebo ostatní zdroje, jako jsou soubory, zařížení nezávisle na tom, zda jsou na internetu, nebo na firemním intranetu” a to i když neznáte doménové jméno, IP adresu, nebo geografické umístění.

LDAP adresář může být distribuován přes mnoho serverů na sítí, poté pravidelně replikován a synchronizován. LDAP adresář je také známí jako Directory System Agent tzv. DSA.

LDAP bylo vyvinuto na Michiganské univerzitě a je to odlehčená verze DAP, části staršího síťového prokolu X.500.

Implementace LDAP v Meraku je založena na projektu OpenLDAP na adrese http://www.openldap.org, rozšířeného o SSL podporu a je dostupný v Merak Mail serveru Professinal (vlastní verzi i Power Packu). Celý LDAP server je nainstalován a nakonfigurován automaticky během instalace Merak Kail server a je v ní vložená konfigurace pro Netscape Messanger a Outlook Expers (tzv. Schémata).

Na internetu je mnoho zdrojů týkajících se LDAP. Je docela dobrý nápad některé z nich si prostudovat. Prohlédněte si odkazovou sekci v této části dokumentace.

Architektura LDAP

LDAP využívá architekrutu klient - server

LDAP Server je nainstalován společně s Merak Mail server Professional (vlastní verzí, nebo power packem) a je uložen v adresáři Merak\LDAP\

LDAP Klient je obvykle váš e-mailový klient, nebo nějaká jiná aplikace. Hodně dnešních emailových klientů, včetně Microsoft Outlook Expresu, Eudory a Netscape Communicatoru je schopno přistupovat na LDAP server. Pro více informací o konfiguraci si prohlédněte sekci o **Používání LDAP**

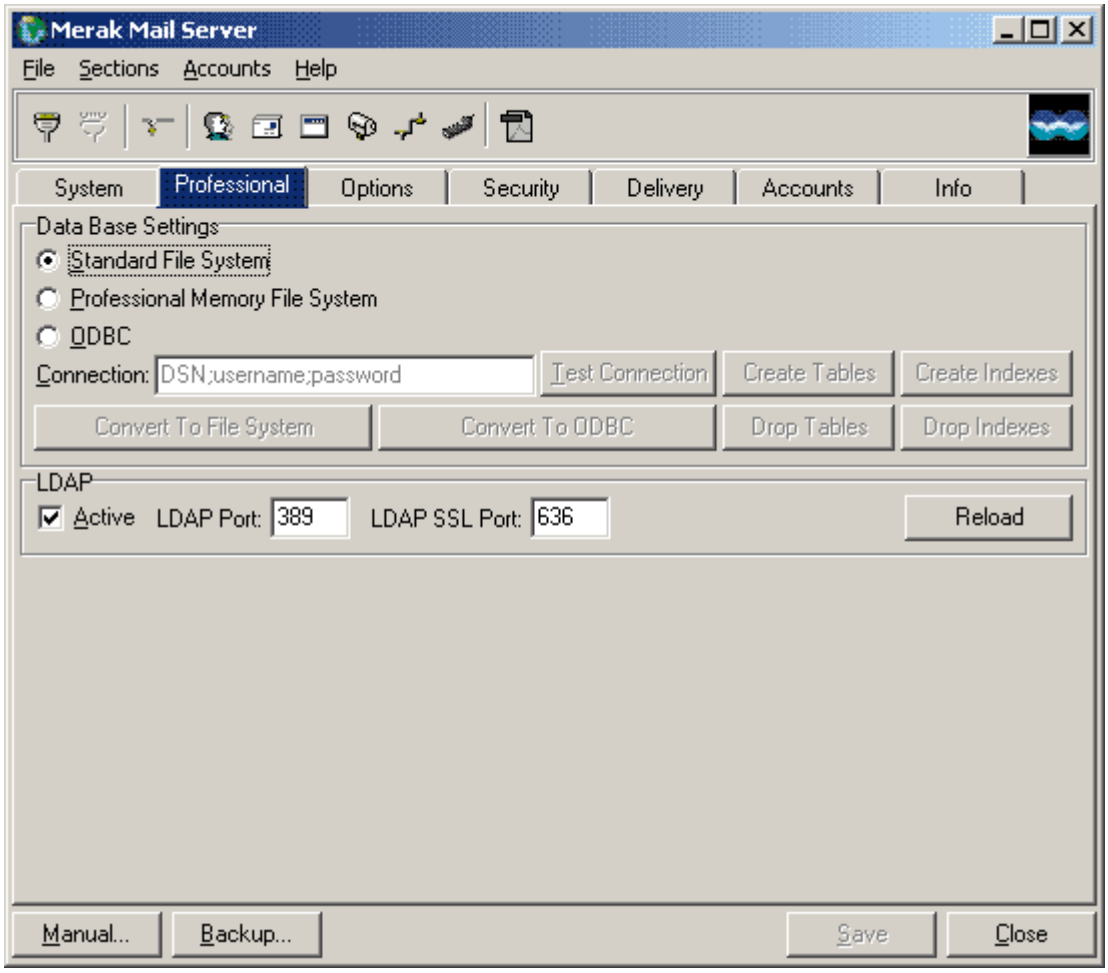
LDAP Server

Merak Mail server ve verzi Professional podporuje LDAP v3 a je založen na projektu Open LDAP http://www.openldap.org/. Jakékoliv další informace můžete nalézt na této stránce. Prohlédněte si také licenční ujednání v souboru LDAP\readme.txt.

Jakmile nainstalujete Meraka, můžete spustit LDAP server a okamžitě ho začít používat. Okamžitě můžete začít vytvářet nové položky.

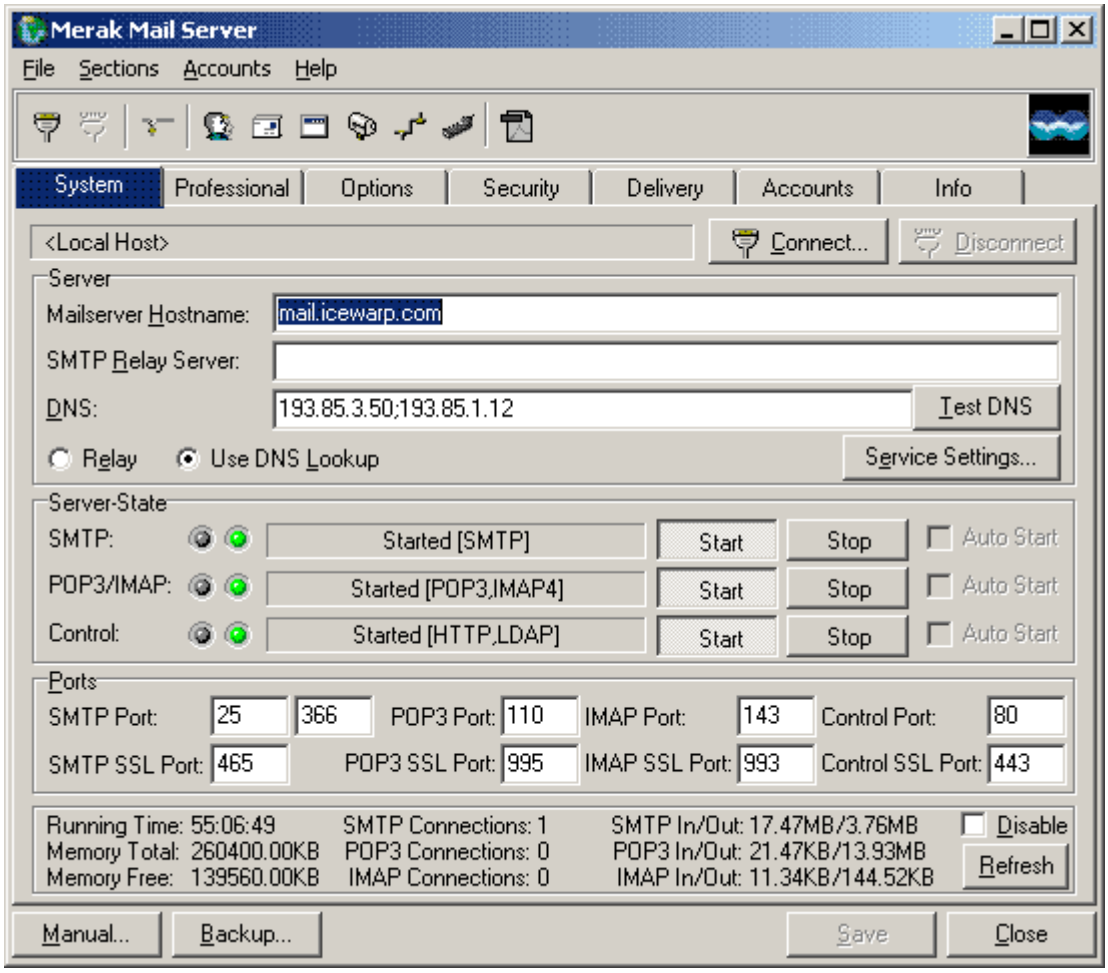
LDAP funguje pod Kontrolní službou Meraka a pracuje pouze na Windows NT a vyšších (NT,2000,XP) platformách. Nepodporuje systému Windows ME,95,98.

Konfigurační soubory LDAP můžete najít v adresáři Merak\LDAP a konfiguraci provádět přesně podle OpenLDAP projektu.



Pro aktiaci LDAP musíte mít nainstalovaný Merak Mail server ve verzi Professional a mít ho spuštěný na platformě Windows NT. Potom stačí kliknout na pole Active a uložit konfiguraci. LDAP server je okamžitě spuštěn.

Jakmile je LDAP nastartováno, můžete zkontrolvoat, zda skutečně běží v tabulce Systém. Zde LDAP funguje pod kontrolní službou Meraka.



Můžete také změnit porty, na kterých LDAP funguje. LDAP v Meraku podporuje SSL a tak můžete spolení na LDAP realizovat přes SSL a používat při tom certifikáty instalované v Meraku. Budou použity stejné certifikýty, jako pro ostatní služby.

Tlačítko Reload provede restart LDAP server a načte znovu konfigurační soubory. To je většinou provést po ruční změně schémat, nebo souboru slapd.conf. Nemusíte tedy restartovat celou kontrolníslužby Merak. Pouze použijtete tlačítko Reload. Vždy zkontrolujte, zda je LDAP skutečně spuštěno. Pokud jste udělali během konfigurace chybu, LDAP server se nenastartuje.

Konfigurace LDAP

Ke správné konfiguraci LDAP je potřeba míž nějaké znalostí o jeho fungování. Více si o LDAP můžete najít na internetu, nebo si projděte odkazy v této sekci dokumentace. LDAP v Meraku vám umožní okamžitě přidat, modifikovat, smazat a najít LDAP záznamy.

Hlavní nastavení se provádí v souboru **LDAP\slapd.conf**. Soubor vypadá asi takto

```
# $OpenLDAP: pkg/ldap/servers/slapd/slapd.conf,v 1.8.8.7 2001/09/27
20:00:31 kurt Exp $
#
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#
include         schema/core.schema
include        schema/inetorgperson.schema

# Define global ACLs to disable default read access.

# Do not enable referrals until AFTER you have a working directory
# service AND an understanding of referrals.
#referral   ldap://root.openldap.org

#pidfile         slapd.pid
#argsfile   slapd.args

# Load dynamic backend modules:
# modulepath      %MODULEDIR%
# moduleload      back_ldap.la
# moduleload      back_ldbm.la
# moduleload      back_passwd.la
# moduleload      back_shell.la

#
# Sample Access Control
#     Allow read access of root DSE
#     Allow self write access
#     Allow authenticated users read access
#     Allow anonymous users to authenticate
#
#access to dn="" by * read
#access to *
#     by self write
#     by users read
#     by anonymous auth
#
# if no access controls are present, the default is:
#     Allow read by all
#
# rootdn can always write!

#######################################################################
# ldbm database definitions
#######################################################################

database    ldbm
suffix          "dc=root"
rootdn          "cn=admin,dc=root"
# Cleartext passwords, especially for the rootdn, should
# be avoid.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw          admin
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd/tools. Mode 700 recommended.
directory   ldbm
# Indices to maintain
index objectClass eq
```

include
V této položce jsou obsaženy definice přídavných schémat. Všechny definice schémat jsou uložený v adresáři LDAP\Schema. Můžete vaši vlastní definici a editovat existující. Během jakékoliv manipulace se říďte pravidly, jinak se LDAP server nespustí. Pokud jste začátečník, vždy použijte již existující definice schémat. Ty již obsahují použíté řádky. Prosím prohlédněte si odstavec věnovaný Schématům.

suffix
Tato položka identifikuje příponu (suffix), kterou budete používat pod LDAP serverem. Všechna klientská spojení budou muset používat daný suffix. Všechny záznamy v databázi jsou vedeny pod tímto suffixem a když ho potřebujete změnit, je potřeba vytvořit nový záznam a znovu pod daným suffixem. Většinou vypadá suffix, jako vaše doména:

```
suffix      "dc=icewarp,dc=com"
```

My jsme ale chtěli, aby jste byli schopni používat LDAP vždy správně. Proto jsme vytvořili suffix:

```
suffix      "dc=root"
```

rootdn
Tato položka identifikuje uživatele s administrátorskými právy, který nemusí existovat v LDAP a je stále schopný provádět různé operace, jako např. přidávání, editování a mazání záznamů. Vždy musí na konci obsahovat suffix. Standardní nastavení je:

```
rootdn      "cn=admin,dc=root"
```

rootpw
Tato položka obsahuje heslo pro rootdn (správcovský účet v LDAP).

Ve zbytku kofiguračního souboru, můžete měnit přídavná nastavení. Pokud budete chtít něco měnit, musíte si být jisti tím, co děláte. Špatné nastavení může vést k nefunkčnosti LDAP serveru. Další podrobné informace můžete najít na: http://www.openldap.org/.

LDAP Nástrole

V adresáři LDAP se nacházejí ještě další nástroje, které mají za úkol pomocí při administraci LDAP databáze. Nástroje mají stejné parametry, jako nástroje z OpenLDAP projektu.

Jedním z hodnotných nástrojů je **slapadd**, který vám umožní přídat záznamy do LDAP databáze. Slappadd používá LDIF format. Příklad jeho použití můžete najít přímo v adresáři LDAP. Jsou tam 2 souboru **create.ldif** a **create.bat** tyto dva dávkové soubory vvytváří suffix v LDAP databázi a to právě pomocí slapadd. Editací souboru creat.ldif můžete vytvořit více LDAP záznamů. Správnou syntaxi LDAP formátu můžete najít na Internetu.

Schémata

LDAP schéma, jako všechna databásová schémata, je definice toho, co je může být uloženo v adresáři. Základní věcí je nějaký **attribute**, jako např. **givenName /křestní jméno/**. Každý atribut je asociován se **syntaxí,** pomocí která určuje co může být uloženo v attributu (prostý text, binární data, zakodováná data různého druhu), a jakým způsobem je informace vyhledávána (citlivě na obsah /case sensitive/ např.) **Objectclass** funkce určuje, jaké by měli být přítomny ostatní attributy.

LDAP v Meraku obsahuje standarní jádro definicí schémeat (objektové třídy, attributy, syntaxe) a vy můžete definovat váše vlastní schéma, přesně podle toho, co potřebujete. Hodně organizací se zabývá právě tím. Nejlepším zdrojem informací na internetu je LDAP schema repository (skladiště LDAP schémat). Kde můžete najít objektové třídy, attributy, syntaxi a schodující pravidla.

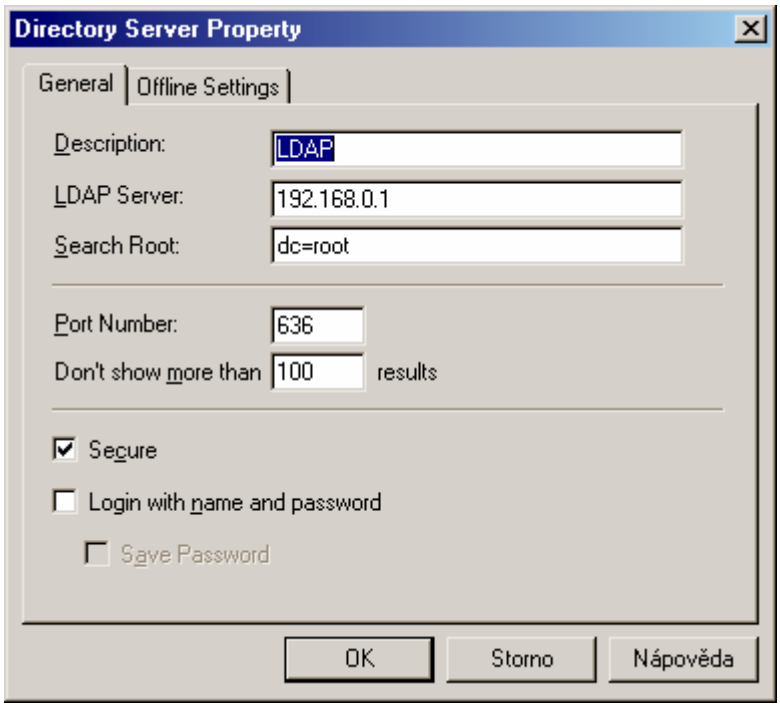
Používání LDAP

Přídávání, modifikace a mazání záznamů na LDAP serveru může být prováděno používáním různých LDAP nástrojů. My doporučujeme používat LDAP administrační nástroj od společnosti Softerra. Jedná se o nástroj distribouvaný pod shareware licencí a je možné ho stáhou z adresy http://www.softerra.com/. Je to velmi zajímavý nástroj, podobný vášemu průzkumníkovi ve Windows.

Všichni poštovní klienti podporují LDAP a umožňují vyhledat záznamy na LDAP serveru. Některé vám budou pomáhat při modifikací záznamů. Některé klientské programy mají lepší implementaci LDAP a vyhledávání probíha hladce, některé nejsou zrovna šikovné a špatně se používají.

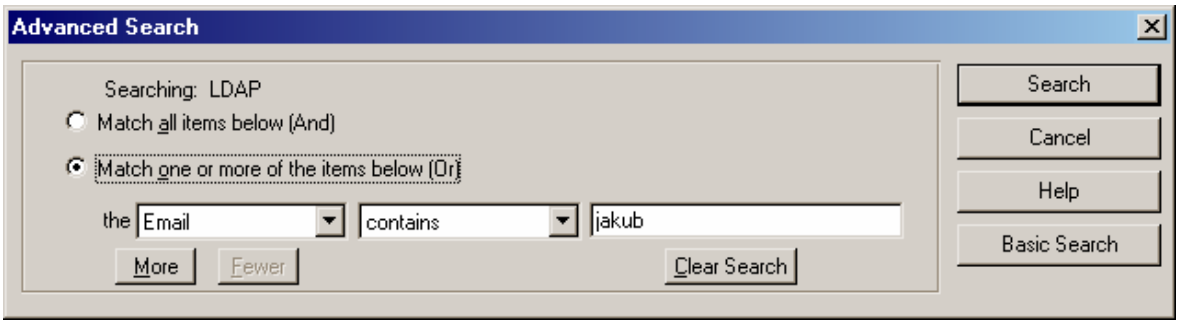
Netscape Messenger

Používání LDAP je v Netcape Messangeru lehce konfigurovatelné. Veškerá konfigurace probíhá v Adress Booku (adresáři). Klikněte na “File” menu a “New Directory”.



Popis (description) si můžete libovolně zvolit. U položky server je ale nutné nastavit IP adresu, nebo host adresu LDAP serveru. V poli Search Root nastavíte požadovaný suffix. Nastavení portů můžete nechat standardně nastaveno. Pokud chcete můžete použít zabezpečené spojení. Po kliknutí na OK je konfigurace dokončena.

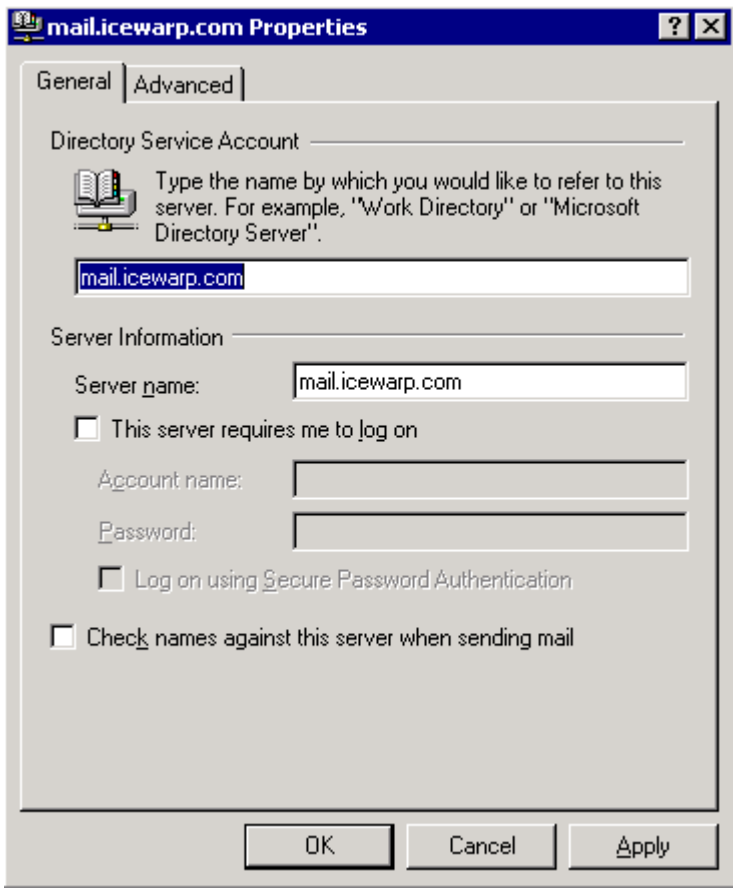
Nyní je nutné přejí do vyhledávacího adresáře. Klikente na adresář a použijte tlačítko Searh (vyhledat). Po kliknutí by se mělo vyvolat následující dialogové okno.

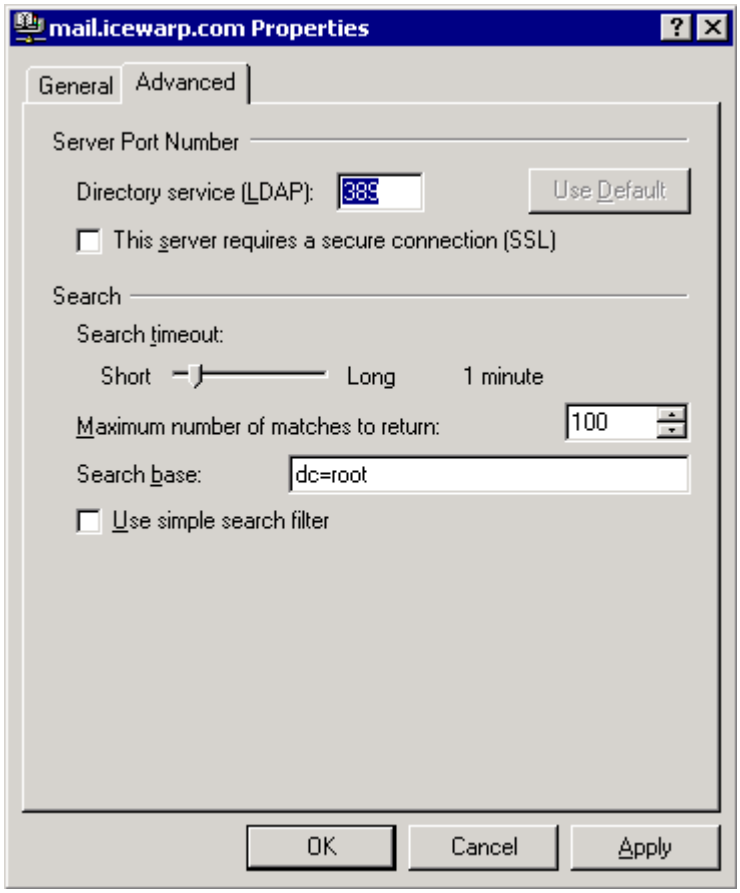


Pokud použijete funkci search, měl by se vyvolat seznam vyhledaných položek. Netscape messagener má opravdu velmi dobrou implementaci a používání LDAP. Vyhledané informace jsou uloženy přímo do programu a je možné s nici pracovat i pozdější.

Outlook Express

Outlook Express je na tom s podporou LDAP o něco hůře. Vždy, když ho chcete použít, musíte informaci znovu vyhledat a zvolit konkrétní adresář, který chcete prohledat. Ke konfiguraci Outlook Expresu použijeme nabídku pro nastavení LDAP. Zvolte Nástroje – Účty – Adresář služeb, potom klikněte na Přidat adresář služeb.





Vyhladávání v Outlook Expresu je komplikovanější. Musíte si otevřít Adresář a v editačním menu použít položky vyhledat osobu. Zvolte si LDAP adresář, vyplňte požadované informace.
Potom klikněte na tlačítko vyledat.

Odkazy

/pozn. Překlad : názvy jsem zcela úmyslně nepřekládal. Já sám předpokládám, že do této sekce dokumentace pronikne pouze technicky erudovanější člověk. Je pro něho lepší znát originální anglický název/

- LDAP Zone
- ldapman.org na této adrese je poměrne hodně informací pro začátek.
- The LDAP Schema Repository Tento server je zcela nepostradatelný proto vědět, kam co a jak dát.

- A System Administrator's View of LDAP od Bruce Markeyho ze společnosti Netscape je zde dostupný velmi zajímavý úvod do použití (jeho styl a plány se podobají našim :-P)
- Další odkazy jsou zajívamé, ale někdy dlouho neaktualizované a poměrně špatne organizované.
- The Yahoo! Kategorie Zde jsou poměrně zajímavé odkazy
- Here's something about the Abstract Syntax Notation Použití pro specifikované protokoly
- Here's something about the Basic Encoding Rules definice toho, jak protokol vypadá na síti
- More about BER, this time LDAP-specific

Příloha A – Nastavení pro většinu antivirových programů

McAfee Virus Scan (testováno ve verzi 4.7.0)

Zajímali jsme se pouze o antivirové programy využívající příkazovou řádku a je vlastně snadnější kopírovat tyto soubory z rozdílného stroje, na kterém je nainstalován software. Ve skutečnosti, pokud máte nainstalované Windows 2000 server, pak je toto jediná cesta jak McAfee Software nemít nainstalovaný na serveru.

Instalujte McAfee na pracovní stanici, nebo na windows 9x a potom přesuňte všechny soubory do následujícího adresáře:

C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.xx

Nakopírujte tyto soubory na váš server a umístěte je do smysluplného adresáře např. antivirus

Název aplikace: c:\antivirus\scan.exe
Parametry: %s /ALL /NOMEM /NOBEEP /UNZIP /ANALYZE /DEL /DAM /MIME /NOEXPIRE /NOBOOT /PROGRAM /SILENT /SUB
Kontrolování smazaných souborů: On

- /ALL – prověřuje všechny soubory
- /NOMEM – neprověřuje paměť
- /NOBEEP – něupozorňuje na nalezení virů pípnutím
- /UNZIP – prověřuje komprimované soubory (.zip .arj soubory)
- /ANALYZE
- /DEL
- /DAM
- /MIME
- /NOEXPIRE
- /NOBOOT
- /PROGRAM
- /SILENT
- /SUB
- %s – proměnné jméno spouštěcího souboru

Více o nové verzi:
a) Nový baliček VirusScan Security Suite obsahuje nástroj NetShield, který obsahuje antivirový nástroj pro příkazovou řádku.

b) Antivirový nástroj určený pro příkazovou řádku se většinou nainstaluje do adresáře /Common Files/Network Associates/VirusScan Engine

c) NeShield standardně automaticky vykonává čištění všech nakažených souboru, které jsou zapsané, nebo čtené z pevného disku jakoukoliv aplikací. Ve chvíli, kdy Merak zapisuje přílohy do adresáře Merak\Temp, jsou soubory autoamticky vyčištěny a antiviru z příkazové řádky nikdy nenajde žádný virus. To je problém, protože zavirované zprávy jsou doručeny příjemci! K vyřešení tohoto problému, musí administrátor nakonfigurovat NetShield tak, aby automaticky nepřoveřoval adresář Merak/Temp.

F-Prot http://www.f-prot.com/

Aplikace: c:\antivirus\f-prot.exe
Parametry: /ARCHIVE /NOBOOT /NOMEM %s
Kontrola smazaných souborů (File deleted checking): Off

- Spouštěcí soubor je pojmenován f-prot.exe
- /ARCHIVE – kontroluje komprimované soubor (.zip .arj)
- /NOBOOT – nekontroluje boot sektor disku
- /NOMEM – nekontroluje pamět
- %s – Jméno soubor je proměnlivé Merak ho nahradí při spuštění

Poznámka: Některé verze F-Prota přestávají s Merakem pracovat. Tento problém je ale velmi vyřešit. Vytvořte odkaz na f-prot.exe a nastavte ve vlastnostech automatické zavírání okna po ukonření programu. Potom nastavte v Meraku spuštění vytvořeného odkazu místo samotné aplikace.

Dr.Solomons (testováno ve verzi 4.0.3a)

Aplikace: c:\antivirus\scan32.exe
Parametry: /NOSPLASH /ALWAYSEXIT /SUB /ALL /COMP /UINONE /CONTINUE %s
Kontrola smazaných souborů: Off

- Spouštěcí soubor je pojmenován scan32.exe
- /NOSPLASH – zabrání zobrazování hlášek programu
- /ALWAYSEXIT – toto nastavení zajistí, že se program vždy ukončí
- /SUB – přověřuje i podaresáře
- /ALL – prověřuje všechny soubory
- /COMP – prověřuje komprimované soubory
- /UINNOE – během běhu programu není k dispozici žádný uživatelský interface – program běží na pozadí
- /CONTINUE – program se přenese přes nalezení viru
- %s – Jméno soubor je proměnlivé Merak ho nahradí při spuštění

AVG Antivirus (testováno ve verzit 6.0) http://www.grisoft.com/

Aplikace: c:\antivirus\avg.exe
Parametry: /NOMEM /SCAN /NOSELF /ARC %s
Kontrola smazaných souborů (File deleted checking): Off

- Spouštěcí soubor je pojmenován avgscan.exe
- /ARC – prověřuje komprimované soubory (.zip .arj)
- /NOMEM – neprověřuje paměť
- /SCAN – prověřuje všechny soubory
- /NOSELF – neprověřuje sám sebe
- %s – Jméno soubor je proměnlivé Merak ho nahradí při spuštění

Norton Antivirus (testováno na verzi Corporate Edition a Standard) http://www.symantec.com/

Corporate Edition

Aplikace: c:\antivirus\vscand.exe
Parametry: /AZ /D /NA /NB /NL /NM /Q /ZIP /C %s
Kontrola smazaných souborů (File deleted checking): On

Soubory, které potřebujete použít při nastavovaní antivirové kontroly v Meraku jsou pod adresářem clt-inst. Nakopírujte tyto soubory počítač s Merakem a potom použijte vscand.exe

- Spouštěcí soubor je nazván vscand.exe
- /AZ
- /D
- /NA
- /NB
- /NL
- /NM
- /Q
- /ZIP
- /C
- %s

Standard verze

Aplikace: c:\antivirus\navwnt.exe
Paramtery: %s /S+ /M /B- /NORESULTS
Kontrola smazaných souborů (File deleted checking): On

Neinstalujte automatické ochrany, které jsou obsaženy v produktu NAV. Po instalaci nastávají dva halvní problémy. Zaprvé žádný z NAV nevrací po dokončení scanování souborů navrátové kódy. Ostatní programy se ukončují s odlyšnými navrátovými kódy a to ať je virus nalezen, nebo ne. A právě podle návratových kódů zjišťuje Merak, ale i ostatní servery, která příloha je nakažena a která ne. Funkce “File Deleted Checking” byla společností IceWarp vymyšlena přávě pro takovou situaci. Zadruhé, není zde žádný paramter, pomocí kterého by bylo možné přes příkazovou řádku nastavit v NAV mazání infikovaných souborů, namísto opravování, nebo jednoduchého detakování. Musíte nakonfigurovat NAV pomocí jeho grafickho rozhraní:

Musíte nakonfigurovat Meraka asi takle:
1) V sekci “Virus Scan Filters” zvolte “File Deleted Checking”, “Scan All Message Parts.”
2) Na "Return Values" (návratových kódech) nezáleží
3) Do "Parameters" pole zadejte (bez mezer): "%S*.* /S+ /B- /NORESULTS"
4) Do pole určujícího spuštění antiviru zadejte aplikaci (navwnt.exe).
5) Pro přidání nastavení použijte tlačítko Add

Potom spusťte administrační konzoli NAV a konfiguraci Manuálního Scanování. Další nastavení proveďte podle následujích instrukcí:
1) Odškrněte pole nastavující scanovaní boot recordu.
2) Nastavte "Delete the infected file" akci.
3) Zvolte"All files".
4) Zvoltet "Scan within compressed files".

- Spouštěcí soubor antiviru je nazván navwnt.exe
- /S+
- /M
- /B-
- /NORESULTS
- %s - Jméno soubor je proměnlivé Merak ho nahradí při spuštění

Příloha B – Přechod na Merak Mail Server

Jedním z hlavních problému systémových administrátorů dneška je přechod ze starého mail serveru na nový. Přechod musí probíhat bez jakýcholiv problemů s uživatelskými jmény a hesly. Klasické řešení tohoto problému spočívalo v přesunu uživatelských dat ze starého serveru na nový. Někdy se přechody z mail serveru na mail servery řeší také pomocí speciálních programů, které přesunují uživatelské účty během běhu pomocí POP importovacího programu. Problémem ale většinou byla nutnost zvolit pro každý produkt vhodný program. Bohužel většina e-mailových serverů nemá ani funkce pro převedení uživatelských účtů a hesel do prostého textu. Přesun je tedy velmi komplikovaný a zdlouhavý. Jak tedy můžeme jednuše přejít z jakéhokoliv mail serveru na Meraka snad a rychle? Odpověď zní Merak Mail server Migration tool.

Merak Mail server Migration tool používá chytrý proxy server, který nezískává uživatelské informace z jakékoliv databáze, ale přímo z POP3 spojení uživatelů. Během uživatelského POP3 spojení, kdy je většinou přenášeno uživatelské jméno a heslo v prostém textu, jednoduše odposleche uživatelská data, automaticky vytvoří na novém mail serveru uživatelský účet s danými parametry a ještě uživatele upozorní, že firma je ve stádiu přechodu na jiný e-mailový server. Všechny zprávy, které se vyberou během spojení se starým serverem, nebudou smazány a budou zanechány na serveru.

Zdroje – icewarp.cz:

http://www.icewarp.cz/mig.php - Stránka věnováná produktu Merak Migration Tool
http://www.icewarp.cz/download.php - Možnost stažení Merak Migration Tool a veškeré nutné dokumentace

Všechny potřebné informace můžete najít na serveru icewarp.cz, kde je také možné Merak Migratio Tool zakoupit.

Příloha C – Přehled toho, jak Merak pracuje

Služby

Merak mail server spočívá na třech službách a konfiguračním programu. V Merakovi je také obsaženo několik nástrojů, jako DNS Query Tools (nástroj na prověřování nastavení DNS), Users Command Line Tools (pomocí kterého je monžné obsluhovat Meraka s příkazové řádky), WebAdmin, Control Panel applet (viditelná konfigurační část Meraka), a Mail Notification (jednoduchý notifikační program). Služby jsou ve skutečnosti programy spuštěné na pozadí Windows a pracující pro vás.

SMTP služba zajišťuje, doručování zpráv, předávání zpráv, monitorování místa na disku a všechny nastavení účtů. Tato služba zajišťuje většinu práce mail serveru a měla by vždy běžet.

POP3/IMAP 4 služba zajišťuje zasílání zpráv emailových klientům, když si chce uživatel vybrat novou poštu. Služba ale také zajišťuje běh Vzdálených účtů a Antivirového systému. Služba by měla pro bezproblémový chod aplikace být vždy spuštěna.

Kontrolní služba zajišťuje DialUp pripojení (spojení pomocí modemu), Vzdálenou administraci, Webovou administraci a hlídací funkce. Pokud nepotřebujete používat žádnou z uvedených funkcí, můžete nechat službu neaktivní.

Soubory a adresáře

V adresáři Meraka se nachází všechny spustitelné soubory, soubory obsahující nápovědu, manuály a soubor default.ini. V HTML adresáři jsou soubory pro Webovou administraci. Konfigurační adresář obsahuje veškeré nastavení. Log adresář obsauje veškeré zaznamenané logy.

SMTP, POP3/IMAP4 a kontrolní logy mohou být zapnuty jednotlivě. Error log (log zaznanenávající chyby v systému) je zapnut, ve chvíli zaznamenání chyby. Struktura logu:

```
[IP adresa] [Identifikace spojení] [Datum cas] [Akce]
```

Příklad:

```
SYSTEM          [00000000] Fri, 19 Jan 2001 11:36:54 +0100 SMTP Service started
```

V adresáři Mail, jsou obsaženy adresáře domén a adresář Forward. V adresáři Forward je umístěna fronta odchozích zpráv čekajících na odeslání. Všechny zprávy mají koncovku .tmp. Ve chvíli, kdy se zpráva začne odesílat se koncovka změní na .tm$. V doménovém adresáři jsou adresáře poštovních schránek a přijmuté zprávy.

V TEMP adresáři jsou ukládány zprávy během přenosu. Po přijmutí jsou přesnuty do cílových poštovních schránek a pak smazány.

Odesílání a přijímání e-mailů

Není žádný rozdíl, mezi lokálním a internetovým příjmem zpráv. Proto, jestliže můžete přijmout lokální zprávu, můžete přijmout také internetovou. Jestliže zpráv nejsou z internetu doručovány, je zřejmé, že doruřování zabraňuje nějaké bezpečnostní nastavení, nebo je DNS MX záznam pro doménu nastaven chybně.

Odesílání pošty funguje odlyšnou cestou. Když odešlete zprávu do lokální domény, je okamžitě uložena do lokální poštovní schránky a mail vůbec necestuje na internet. Mail server sám rozpozná, která domény jsou konfigurovány v konfiguračním programu. Když je ve zprávě uveden příjemce s lokání doménou, je zpráva doručena do lokální domény. Jestliže je zpráva určena externímu příjemci (doméně) je zpráva uložena do adresáře Forward (odchozí fronty) a je proveden okamžitý pokus o odeslání zprávy. Vše je řešeno v oddělených procesech. Merak je plně multi procesový mail server s podporou více procesorů.

Největší výhodou Meraka je bezpečí a bezpečnost. Všechny služby mají implementovanou podporu TSL/SSL (Secure Socket Layer – zabezpečená socketová vrstva) a vy můžete vašim emailovým klientům nastavit podporu a používání těchto funkcí. V takovém případě bude veškerý přenos zpráv ze serveru totálně zabezpečen. Proto síť Merak mail serverů kompletně vyhodí počítačové hackery z práce.

Příloha D - DNS a MX záznamy

DNS – Porozumnění základní problematice DNS a zprovoznění e-mailového serveru

Mámé doménu, např. “mojefirma.cz”, . To je první a nejdůležitější krok, který učiní každý, kdo chce cokoliv nabízet přes internet. Lidé zadávají doména, jako část e-mailové adresy, nebo jako webovou adresu. Ve skutečnosti ale lidé nezadávají jméno firmy, ale jméno, které je přiřazené nějaké IP adrese. Překlad doménového jména na IP adresu probíhá přávě na DNS serveru. Zkratka DNS znamená v angličtině “Domain Name system”. DNS server má mnoho funkcí. Nejdůležitější ale je, že bez DNS serveru byste nebyli schopni zjistit IP adresu pro doménu “mojefirma.cz” a proto se na ni nebylo možné připojit. DNS pracuje na UDP protokolu konkrétně na portu 53.

Na DNS serveru je možné nakonfigurovat více typů DNS záznamů. Pro nás jsou aktuálně nejdůležitější 2. Konkrétně A a MX záznamy. A záznamy konvertují host adresu na IP adresu.

Příklad:
www.icewarp.cz A 12.107.133.12

MX záznam je záznam určený pro výměnu pošty. Používá se při doručování e-mailů na cílový mail server. Standardně je e-mailová adresa složena z aliasu a doménového jména domény: alias@doména. Např. adam@icewarp.cz. Každá doména by měla mít minimálně jeden MX záznam. Pokud doména nemá MX záznam, není na ni možné doručovat e-maily.

Každý MX záznam pro doménu obsahuje preferenční číslo a host adresu cílového serveru pro doručování zpráv. Když je na DNS serveru nastaveno větší množství MX záznamů, nějnížší číslo má nejvyšší prioritu a doručení na něj by mělo být vyzkoušeno jako první. Pokud není mail server s nejvyšší prioritou funkční, mělo by se zkoušet doručit zprávu na mailový server s nižší prioritou. Většinou je ale pro doménu pouze jeden MX záznam.

Příklad:
```
icewarp.cz MX mail.icewarp.cz 10
```

V příkladu ma MX záznam pro doménu icewarp.cz preferenční číslo 10

DNS server jeou většinou administrovány vašimi internetovými poskytovateli. Vy byste si ale měli být schopni ověřit, zda váš internetový poskytovatel nastavil DNS server správně. Pokud potřebujete požádat o korektní DNS záznam postupujte podle následujících kroků:
Zjistěte IP adresu vašeho mail serveru
Požadujte vytvoření A DNS záznamů: např. Mail.vašedoména.cz ukazujícího na IP adresu serveru
Požadujte MX DNS záznam pro vaši doménu, který bude ukazovat na mail.vašedoména.cz s nějakým nastaveným preferenčním číslem, např. 10.

To je opravdu vše, co potřebujete nastavit na DNS serveru, aby jste byli schopni přijímat z Internetu zprávy. V instalačním balíčku Merak Mail server je obsažen nástroj DNS Query Tool, který můžete také nálezt v adresáři Merak\dnsquery.exe. Spusťte tento nástroj. POle DNS by mělo obsahovat korektně fungující DNS server (IP nebo host adresu). Pole Query by mělo obsahovat hodnotu, na kterou se chcete dokázat. V poli Type zvolíte typ DNS záznamu, který Vás zajímá. Nyný můžete bez problému ověřit, zda je vše nastaveno správně.
Výstup by měl vypadat asi nějak takto:

Query: icewarp.cz, Type: MX, Result = mail.icewarp.cz
Query: mail.icewarp.cz, Type: A, Result = {nějaká IP adresa}

Pokud vaše dotazy nebyli správně zodpovězeny DNS serverem, nejsou Vaše DNS záznamy správně nastaveny. V tom případě byste měli zavolat svého internetového poskytovatele a zeptat se na IP adresu jejich DNS serveru a říct jim, aby ověrili správnost nastavení.

Jakmile bude vše fungovat, může Merak, nebo jakýkoliv jiný DNS server přijímat zprávy z internetu. Nyní malá poznámka. Ve chvíli, kdy může váš mail server přijímat poštu lokálně, může ji přijímat i externě z internetu. Mezi tím totiž není žádný rozdíl. Pokud při přijímaní pošty nastává nějaký problém, musí to být v nastavení DNS serveru.

Přijímání zpráv by tedy mělo fungovat bez problému. Někdy můžou nastat problémy při odesílání zprávy. Poznáte to podle toho, že budete mít v odchozí frontě serveru nashromážděné zprávy. V Meraku se veškerá odchozí fronta ukládá do adresáře Merak\Mail\Forward. A opět je to z 99% problém DNS. Nicméně nikoliv problém DNS záznamu, ale problém nastavení DNS v kofiguračním programu Meraka, v polích konfigurace DNS. V takovém případě vyzkoušejte nastavit jiný DNS server (samozřejmě používejte funkci DNS Loopkup). Pokud stále nefunguje odesílání zpráv, prohlédněte si SMTP logy a pokuste se analyzovat problém podle nich. Zkontrolujte záznamy klientských spojení a dotazů na MX záznamy. Korektní záznam by měl vypadat asi takto:

```
Client session MX - Issuing query 194.213.224.2 for "icewarp.cz"
```

Tato řádka nám říká, že MX záznam pro doménu icewarp.cz obsahoval IP adresu 194.213.224.2.

Pro nás nejvíce důležitá informace je obsažena na následujícím řádku:

```
Client session MX - Query response: 0 (1)
```

Tato řádka nám říká, že DNS server odpověděl O (OK) a vrátil výsledek 1. Pokud máte v logu odlyšné hodnoty jako např. “Could not connect”, váš DNS server nepracuje správně a měli byste použít nějaký jiný. Pokud řádek ve vašem logu vypadá takto:

```
Client session MX - Query response: 0 (0)
```

Je to ten samý problém a zkuste použít jiný DNS server

Poslední řádky, které nás zajímají jsou

```
Client session Connecting to "mail.icewarp.com"
Client session Connected
```

Výsledek DNS dotazu vrátil host adresu mail.icewarp.cz a Merak se na ni zkouší připojit. To se mu povedlo. Někdy se ale spojení nemusí povést. To znamená, že je vzdálený server dočasně mimo provoz, nebo se na něho váš server není schopen z nějakého důvodu spojit (firewall, špatně nastavené internetové spojení atp.). Můžete zkusit použít následující příkaz z vaší příkazové řádky:

```
telnet mail.icewarp.com 25
```

Pokud tento pokus funguje, je internetové nastavení v pořadku, ale vzdálený server je zřejmě na nějakou chvíli mimo provoz.

Jak DNS funguje?

DNS je distribuovaná databáze. Služby DNS je nabízena tísici DNS serveru na internetu. Každý je schopný odpovídat za část jmen tzv. zón. Server, které mají přístup k DNS informaci (souboru zón). Po zaslání dotazu DNS server překládá jméno domény na kerespondující IP adresu. Např. doménové jméno www.icewarp.cz by mělo být přeloženo na „195.24.22.209“.

Jakmile je na pracovní stanici Windows nainstalovaný nějaký software využívající protokol TCP/IP, je IP adresa jednoho, nebo více DNS serverů jedním z nastavovaných parametrů. Přes tento nastavený DNS server se budou z počítače dotazovat všechny ostatní aplikace na IP adresy na internetu. Může to být ale také server, který se nadále dotazuje ostatních serverů na internetu, ale v každém případě je stále v kontaktu s pracovní stanicí.

Nicméně to nefunguje tak, že jeden z tisíce name serveru zná klíče pro přeložení doménových jmen na IP adresy naopak každý server zná jména a IP adresy každého uživatelského počítače na internetu. Server pak vyměňuje tyto informace s ostatními DNS servery z jiné části sítě, to umožňuje adresování doménových jmen mezi jednotlivými počítači na odlyšných sítích.

Internet by měl pracovat bez DNS server, pokud se ale chcete připojit na nějaký server, musíte znát jeho IP adresu.

Typy DNS záznamů

Dva nejvíce používané typy záznamů:

- **A: The Address Record.**
  Tento záznam umožňuje přidělovat IP adrese host adresu. A record potřebujete pro jakýkoliv veřejný server, který by měl přístupný z internetu. Nejvíce používaná host adresa je samozřejmě “www” a “mail”, které se používají k identifikaci web serverů a mail serverů.
- **MX: The Mail Exchange Record.** Pomocí tohoto záznamů určujeme, který host v doméně slouží jako e-mailový server. MX záznam má dvě části: jméno počítače, který bude přijímat poštu pro doménu a preferenční čílost. Doména může mít více záznamůl.

Ostatní typy záznamů jsou:

- **SOA: The Start of Authority Record**
  Tento záznam obsahuje hlavní informace o doméně, např. který server je za ní odpovědný, jak dlouho by měla být informace o doméně uchována na jiném počítači atp.

- **CNAME: The Canonical Name Record**
  To je alias pro host jméno (A záznam)

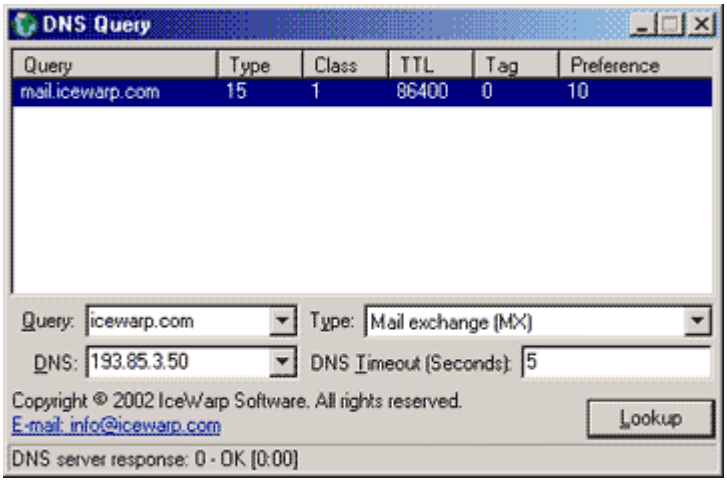
- **PTR: The Pointer Record**
  To je host jméno, nebo IP adresa používána pro reverzní vyhledávíní

- **NS: The Nameserver Record**
  Definuje DNS servery pro doménu.

MX záznam

Pro provoz mail server nás ale opravdu zajímá hlavně MX záznam. MX záznam je skutečně to, co nám umožňuje mít e-mailovou adresu ve formátu “uživatel@domena.cz, ve které se používá doména a ne specifikace host adresy serveru. Pokud enní pro doménu nastavený MX záznam, je možné specifikovat server, který bude přijímat poštu pomocí A záznamu. Výsledný e-mailová adresa ale bude potom vypadat asi nějak takto: uživatel@mail.domena.cz

Můžeme si vykoušet dotázat se na doménu lotus.com. Budeme chtít informace o používáných DNS server. Použijeme k tomu náš nástroj DNS Query Tool:



To nám řekne, že dostupné pro doménu jsou 2 MX záznamy. Když je nějaká zprávy odeslána na doménu lotus.com, posílá se automaticky na server, který má ve svém MX záznamu nižší preferenční číslo. V tomto případě, by měl server zkusit poslat zprávu na server lotus.lotus.com. Pokud primarní e-mailové server z jakéhokoliv důvodu nepřijme zprávu, server se jí pokusí doručit na server lotus2.lotus.com

Pouze po vyzkoušení všech MX záznamů v doméně, označí server zprávu jako nedoručitelnou, poté se jí bude pokoušet odeslat každých X hodin v X čase předtím, než vráti zprávu odesilateli jako nedoručiltenou.

Věci ke kontrole

Je potřeba skutečně zkontrolovat, zda je pro každou doménu nastaven minimálně jeden MX záznam, který koresponduje z host adresou (A) záznamem. Jinak bude dotaz na host adresu mail serveru neuspěšný. Tady je příklad souboru z DNS databáze.:

```
@                       IN  SOA ns3.siwd.net.  support.siwd.net. (
                              15           ; serial number
                              900          ; refresh
                              600          ; retry
                              86400        ; expire
                              14400      ) ; minimum TTL

;
;  Zone NS records
;
@                       NS    ns3.siwd.net.
@                       NS    ns4.siwd.net.

;
;  Zone records
;
@                       MX    5       mail.liquid-matrix.com.
mail                    A     213.165.154.3
www                     A     213.165.154.2
```

Příloha E – API (pouze ENG)

//Pozn. Překlad: Příloha API nebyla přeložena do čestiny. Jsme toho názoru, že by to každému programátorovi bylo spíše na obtíž.

The API

The API (Application Programming Interface) for Merak is designed for those who want to manipulate domains, users, mailing lists, notification accounts and executables from external applications. It allows you to get lists of accounts, add, delete, edit and read the settings.

The API.DLL can be found in the Merak directory and is used by the Users.exe and Domains.exe command line tools. The source code for the tools is written in Delphi and can be found in the API directory. In the API directory there are also other programming languages examples.

Using the API

The API can be used in any programming language such as Delphi, BC++ Builder, MS VC++, ASP, VB etc. All you need to do is to import the functions from the API DLL (Dynamic Linked Library). The API.DLL is not a COM object. If you need to use it as a COM object you have to get a COM wrapper from our site, th download section, SolWeb Tools.

Function Descriptions

```
Function Init(Directory: PChar): Longint; StdCall;
```
Initializes the API. The directory contains the Merak Mail Server installation path. This function should be the first called function. By default the Init function is called once opened the API library with the registry path of Merak installed. If you do not need to specify a different path do not call this function.

```
Procedure UpdateConfiguration; StdCall;
```
Makes all services to reload the global configuration changes.

```
GetUserCount(Domain: PChar): Longint;
```
Returns the number of accounts in the specified domain.

```
GetUserList(Domain: PChar; Var List; Size: Longint): Longint;
```
Returns the list of all accounts in the specified domain. The List must be long enough and the Size must specify the length of the List buffer. A list of all users will be placed into the List buffer. The users will be separated by the #00 byte. The last record contains one more #00 byte.

```
Function GetUserIndex(Domain, Alias: PChar): Longint; StdCall;
```
Returns the index of the user. The domain specifies the domain and alias specifies the user's alias. All records are index based. Therefore when you want to save or load a user you need to know the index first.

```
Function LoadUser(Domain: PChar; Index: Longint; Var Buffer; Size:
Longint): Longint; StdCall;
```
Loads the user settings for the specified domain and the index of the user. Buffer must be long enough to hold the whole user's settings. Make it at least 4192 bytes.

```
Function SaveUser(Domain: PChar; Index: Longint; Var Buffer; Size:
Longint): Longint; StdCall;
```
Saves the user settings from the Buffer.

```
Function AddUser(Domain: PChar; Var Buffer; Size: Longint): Longint;
StdCall;
```
Adds a new user.

```
Function DeleteUser(Domain: PChar; Index: Longint): Longint; StdCall;
```
Deletes the specified user.

```
Function AuthenticateUser(Mailbox, Password, IP: PChar; Var DomainIndex:
Longint; Var FResult; ResultSize: Longint): Longint; StdCall;
```
Authenticates the user to the mail server. Merak uses the same function to find the user during the authentication process. The IP parameter should be the IP address of the mail server to connect to. If you are not using this option leave it empty (NIL) When successful the function returns the DomainIndex the user was found in and the FResult contains the user buffer.

```
Function GetUserSetting(Var Buffer; Size: Longint; Setting: Longint; Var
FResult; ResultSize: Longint): Longint; StdCall;
Function SetUserSetting(Var Buffer; Size: Longint; Setting: Longint; Var
FResult; ResultSize: Longint): Longint; StdCall;
```
These 2 functions are the most important ones. By these functions you can set/get all the settings for the users. Buffer contains the user setting structure and the Size reports its size. Setting specifies the Command. The command list can be found in the APIConst unit. The FResult is the buffer to get/set the value for the particular setting. The ResultSize specifies the size of the FResult buffer. Settings have several data formats:
a) String, size = length of the string
b) Boolean, size = 1
c) Number, size = 4
d) Time, size = 8
The setting command names correspond to the config program option names. The data formats correspond as well.

```
Function GetDomainCount: Longint; StdCall;
```
Returns the number of domains.

```
Function GetDomainList(Var List; Size: Longint): Longint; StdCall;
```
Returns the list of all domains. The List must be long enough
and the Size must specify the length of the List buffer. A list of all domains will be placed into the List buffer. Domains will be separated by the #00 byte. The last record contains one more #00 byte. The first domain in the list is a primary domain.

```
Function GetDomainName(Index: Longint; Var Name; Size: Longint): Longint;
StdCall;
```
Returns the name of the domain specified by the Index. All domains are index
based. Therefor when you want to save or load a domain you need to know the index first.
The Name is a pointer to buffer to receive the domain name, Size specifies the size of the buffer. The function returns the size of the returned domain name.

```
Function GetDomainIndex(Name: PChar): Longint; StdCall;
```
The opposite of the previous above.

The following functions have the same logic as user functions. Please, see the user functions for more information.

```
Function LoadDomain(Index: Longint; Var Buffer; Size: Longint): Longint;
StdCall;
Function SaveDomain(Index: Longint; Var Buffer; Size: Longint): Longint;
StdCall;
Function AddDomain(Name: PChar; Var Buffer; Size: Longint): Longint;
StdCall;
Function DeleteDomain(Index: Longint): Longint; StdCall;
Function GetDomainSetting(Var Buffer; Size: Longint; Setting: Longint;
Var FResult; ResultSize: Longint): Longint; StdCall;
Function SetDomainSetting(Var Buffer; Size: Longint; Setting: Longint;
Var FResult; ResultSize: Longint): Longint; StdCall;


Function GetDomainIP(Index: Longint; Var Buffer; Size: Longint): Longint;
StdCall;
Function SetDomainIP(Index: Longint; Var Buffer; Size: Longint): Longint;
StdCall;
```

These functions get/set the logical IP binding of a domain. If you are not using it do not call these functions.

For more details see the API directory.

Příloha F – Popis ovládání Meraka z příkazové řádky

Uživatelské a doménové ovladací nástroje

Nástroje users.exe a domains.exe jsou ve skutečnosti programy, které vám umožní ovládat Meraka z příkazové řádky. Jsou umístěny v adresáři Meraka. Pokud potřebujete, můžete také najít v adresáři API jejich zdrojový kód. Tyto nástroje mohou být použity pro manipulaci s doménami a uživateslkými účty, např. pro editaci, přidávání, mazání apod. Můžete je také použít pro exportování a importování uživatelů. Tyto nástroje jsou limitovány pouze tím, že je lze použít pouze na jednu doménu. To znamená, že pokud budete potřebovat exportovat a importovat uživatele z více domén, bude nutné spustit je více krát za sebou.

Použití nástroje pro administraci uživatelů

Spuštěním nástroje users.exe bez zadání parametrů, získáte následující výstup:
(pod tímto výstupem jsou detailně popsané všechny funkce)

```
API User Manager - Merak Mail Server
Copyright (c) 2002 IceWarp Software. All rights reserved.
E-mail: info@merakmail.com

Usage: USERS {commands} -u{user|*@[domain]} [properties] [parameters]
Usage: USERS -STATISTICS <from> <to> <filter> <output file>

Commands:
-a                      Add new user
-c                      Change user's properties
-d                      Delete a user
-l                      List a user
-e[delimiter char]      Export users
-g[delimiter char]      Import users from a file into a domain
-STATISTICS             Creates the user statistics file
-h                      This help
```

```
-u{user[@domain]}        Specifies the user's address

Properties:
-n{name}                 Specifies the user's name
-p{password}             Specifies the user's password
-m{mailbox}              Specifies the user's mailbox name
-b{mailbox}              Specifies the user's mailbox path
-i{+/-}{KB}              Specifies the user's max mailbox size
-k{KB}                   Specifies the user''s max message size
-r{address}              Specifies the user's remote address (no local
mailbox)
                         Empty address stands for no remote address
-f{address list}         Specifies the user's forward address list
-4{+/-}                  Specifies that the user can use the IMAP4
-z{+/-}                  Specifies that the user is self configurable
-s{+/-}                  Specifies that the user is the administrator
-x{+/-}                  Specifies that the user is the domain
administrator
-j{+/-}                  Specifies that the user uses the NT Password
-o{+/-}                  Specifies that the user is disabled
-q{file path}            Specifies auto responder file path
-t{+/-}{days}            Delete mail older than x days
-w{+/-}{days};{address}  Forward mail older than x days to y

Parameters:
-cfg{path}               Specifies the full path to the Merak directory
```

Přídávání užitelů:

Umožní pridat utivatele se jménem John Doe, aliasem john, jménem schránky/uživatelským jménem joh a heslém secret do domény icewarp.com. Pokud se jedná o primarní doménu, nemusíte specifikovat jméno domény.

```
users -a -ujohn@icewarp.com -mjohn -psecret -n"John Doe"
```

V případě primární domény, může vypadat použití asi takto:

```
users -a -ujohn -p"my secret" -n"John Doe"
```

Poznámka: Pro prostor, který obsahuje paramtery by se měli používat uvozovky

Mazání uživatele

Umožní smazad vytvořeného uživatele

```
users -d -ujohn@icewarp.com
```

Editace uživatele

Možná budete chtít změnit heslo z původního secret na top secret

```
users -c -ujohn@icewarp.com -p"topsecret"
```

Prohledávání uživatele

Umožní zobrazit informace uživatele. Není možné tuto funkci použít pro více uživatelů.

```
users -l -ujohn@icewarp.com
```

Exportování a Importování uživatelů

Exportovací funkce umožní exportovat seznam uživatelů danou doménovou maskou, nebo všech domén na obrazovku. Pokud je potřebujete uložit do nějakého sobouru, je potřeba přesměroat data do výstupního souboru. Tady je první příklad vypsání všech uživatelů z domény icewarp.com na obrazovku.

```
users -e -u*@icewarp.com
```

nebo ze všech domén

```
users -e -u*@*
```

Exportovaná data obsahují úvod programu na prvních řádkách. Pokud potřebujete data importovat musíte tyto řádky smazat. Ve konečném výstupu je heslo administrátora nahrazeno “*”. Parametry pro exportování uživatelů do souboru export.txt vypadá následovně:

```
users -e -u*@icewarp.com > c:\temp\export.txt
```

Po odstranění programové informace vypadá výstup asi takhle:

```
john@icewarp.com,john,*,icewarp.com\john\,John Doe,,,0,0
support@icewarp.com,support,topme,icewarp.com\support\,Support Team,,,0,0
```

Formát výstupu je následující:

```
[Alias]@[Domena],[Mailbox],[Cesta k mailboxu],[Jmeno]...
```

V případě, že chcete importovat uživatele ze souboru, použijte tento příkaz:

Uživatelská statistiky

Pokud potřebujete použít uživatelské statistiky, může vám právě nástroj users.exe pomoci k jejich exportování do souboru. Potom nebudete potřebovat využít grafický uživatelský interface, nebo webové administrační rozraní. Syntaxe je jednoduchá:

```
users -STATISTICS "2002/02/01" "2002/02/28" "*" "c:\temp\stats.log"
```

Použití nástroje pro administraci domén

Spuštěním domain.exe bez jakýchkoliv parametrů, získate následující výstup:

```
API Domain Manager - Merak Mail Server
Copyright (c) 2002 IceWarp Software. All rights reserved.
E-mail: info@merakmail.com
Usage: DOMAINS {commands} {domain} [properties] [parameters]

Commands:
-a                      Add new domain
-c                      Change domain's properties
-d                      Delete a domain
-l                      List a domain
-e[delimiter char]      Export domains
-g[delimiter char]      Import domains from a file
-h                      This help

Properties:
-s{description}         Specifies the domain's description
-i{+/-}                 Info To Admin
-u{forwardto}           Unknown Users Forward To
-f{alias}               Admin Default Alias
-m{email}               Admin Default Email
```

```
-t{domain type}          Domain Type (0..3)
-v{domain type value}    Domain Type Value

Parameters:
-cfg{path}               Specifies the full path to the Merak directory
```

Přídání domény

Umožní nám přidat novou doménu se jménem icewarp.com a popisem doména icewarp

```
domains -a icewarp.com -s"doména icewarp"
```

Poznámka: Pro prostor, který obsahuje paramtery by se měli používat uvozovky

Mazání domény

Umožní nám smazat přidanou doménu

```
domains -d icewarp.com
```

Editace domény

Umožní nám změnit popis domény
```
domains -c icewarp.com -s"IceWarp Software Domain"
```

Získávání informací o doméně

Umožní nám získat informace o jedné doméně. Není možné tento nástroj použít pro získání informací o více doménách najednou

```
domains -l icewarp.com
```

Exportovaní a importování domén

Exportovací funkce exportují seznam všech domén na obrazovku počítače. Pokud potřebujete uložit, musíte přesměrovat data do výstupního sobuoru. Tasdy je první příklad toho, jak docílit vypsání všech domén na obrazovku počítače.

```
domains -e
```

Exportovaná data obsahují informaci vloženou programem. Pokud potřebujete data importovat je nutné tuto informaci z prvních řádku smazat. Paramtery pro uložení do souboru jsou následující:

```
domains -e > c:\temp\export.txt
```

Pro případ importování domén ze souboru použijte:

domains -g c:\temp\export.txt
.

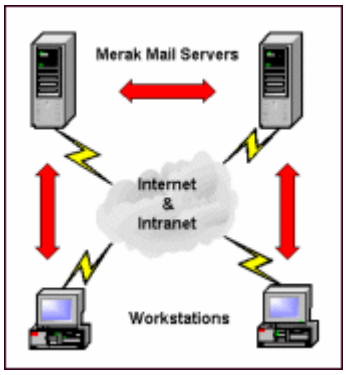
Příloha G – Instant Messaging server

Naše řešení je postaveno na technologii "Jabber open XML protocol", která je využita v našem vlastním jádru zvyšujícím bezpečnost, stabilitu, rychlost a sílu celé technologie. Náš instant messanger není založen na jakémkoliv otevřeném kódu (implemetaci do Merak Mail server jsme

byla hrdě napsána našimi programátory) , ale je plně kompatibilní s protokolem. Je tedy možné použít jakýkoliv Jabber klient, nebo ostatní moduly kompatibilní se standardem Jabber.

Námi doporučený Jabber klient se jmenuje JAJC (Just another Jabber Client). Naši vývojáři v současné době ale pracují na vývoji vlastního klientského prostředí.

Merak Mail server Instant Messaging server má následující vlastnosti:



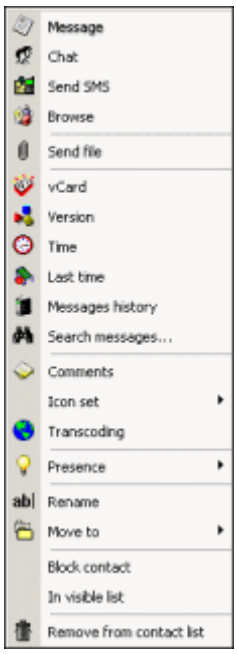
- **Multi-uživatelsky: Uživatelé komunikují spolu lokálně**
- **Multi-doménově: Uživatelé komunikují skrz více serverů**
- **Integrovaný s Merak Mail serverem: Je spuštěn jako služba spolu s Merak Mail serverem**
- **Kompletně zabezpečen: používá zabezpečené sokety (SSL)**
- **Extermně jednoduchá implementace**

Proc používat zabezpečený Instant Messaging?

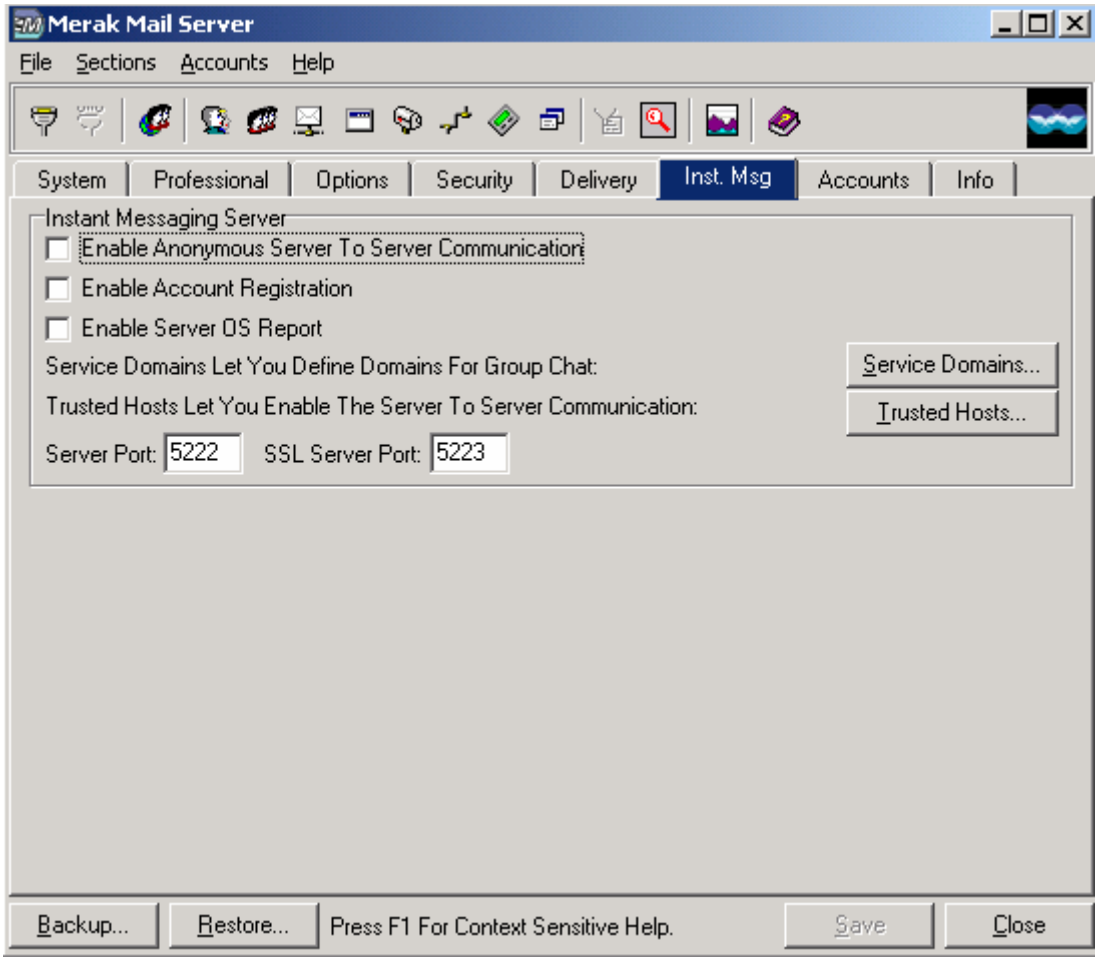
Pomocí instant messing serveru můžete velmi snadno zrychlit a zpřehlednit komunikaci ve firmě. Přináší ale také další výhody, jakými jsou např.:

- Významně zvednout produktivitu zaměstnanců a to tím, že jim umožníte zpracovávat více úkolů najednou.
- Vylepšit spolupráci mimo hranice společnosti.
- Budete si jisti, že komunikace ve Vaši společnosti je bezpečná
- Budete moci kontrolovat veškerou komunikaci.
- Zredukujete telekomunikační poplatky

Základní přehled funkcí:



- Chat
- Více-uživatelský chat (chat dvou a více uživatelů, multi serverové konference atp.).
- Možnost posílání souborů
- Seznam povolených a zakázaných kontaktů
- Možnost uložení soukromých dat
- vCard - vizitky ze soukromými informacemi
- Veškeré kontakty uložený přímo na serveru
- Offline zpracování dat
- Možnost spolupráce více serverů (Server to Server komunikace)
- Funkce Last User Logon, User Server Version + Time
- Notifikace událostí
- Registrace účtu
- Autentifikace
- Změna hesla
- SSL
- Administrátor - může odeslat zprávu všem uživatelům na serveru



Pole	Popis
Enable Anonymous Server To server Communication	Pokud je tato funkce aktivní, je Merak otevřen komunikaci s jakýmkoliv jiným IM serverem a to bez nutnosti nastavení server v Trusted Hosts
Enable Account Registration	Umožní registraci nových uživatelů přes Instant Messenger.
Enable Server OS report	Zasílá uživatelům informace o nainstalovaném operačním systému na server (pokud je tato informace vyžádána klientem). Tuto funkci nedoporučujeme z bezpečnostích důvodů používat.
Service Domains	V IM server je možné nastavit různé služby. Takovou službou může být např. Anonymní chat místnost. Pro každou místnost je ale nutné vytvořit virtuální doménové jméno v Meraku. Typickou doménou pro chat srever bývat “chat.domena.cz”. Tato doména ale nesmí fyzicky existovat v DNS serveru. Slouží pouze pro potřeby nastavení v IM. Syntaxe v souboru je následující: <servicedomain> Příklady: chat.icewarp.comrooms.icewarp.com
Trusted Hosts	Tato funkce specifikuje důveryhodné servery, se kterými bude Merak komunikovat. V každém případě je nutné povolit komunikaci i na druhé straně. Velmi jednoduše lze nadefinovat celou skupinu serverů, na které budete moci tamním uživatelům posílat zprávy, soubory, nebo chatovat v místnostech. Syntaxe souboru trusted hsots je následující: <domain1>;<domain2>...=<hosta>[:<port>][;SSL] <domain3>;<domain4>...=<hostb>[:<port>][;SSL] Příklady: icewarp.cz=im.icewarp.cz:5223;SSL merakmailserver.com=mail.merakmailserver.com:5222
Server port	Číslo portu, které bude IM používat pro standardní komunikaci
SSL Server port	Číslo portu, které bude IM používat pro SSL šifrovanou komunikaci.

Komunikace přes IM v rámci jedné domény

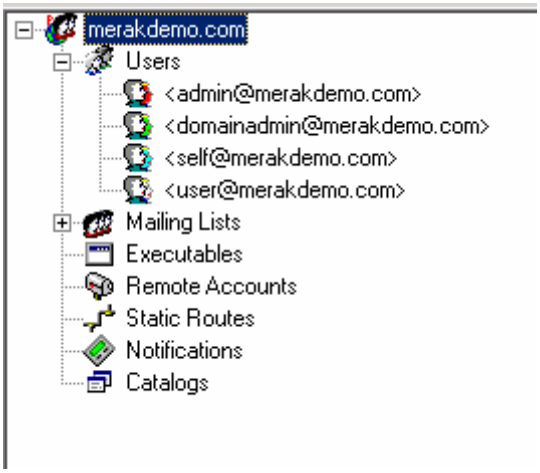
Instalace klientského programu JAJC.

Stáhnout JAJCe je možné přímo na stránkách IceWarp.cz. Celá adresa je:
http://www.icewarp.cz/download/jajccz.zip

Program můžete nakopírovat do libovolného adresáře. Ostatní adresářová struktura se vytvoří automaticky po spuštění programu.

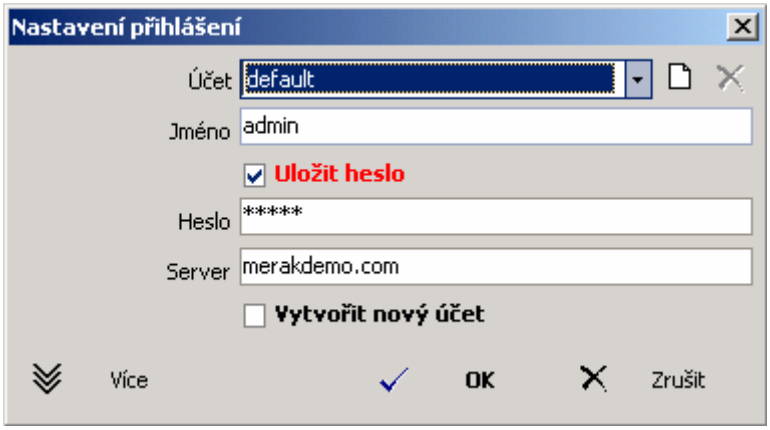
Přípojení JAJC klienta do na Merak Mail server:

Na příkladu si ukážeme, jak přesně nastavit klientský program. Jako příklad použijeme doménu **merakdemo.com**



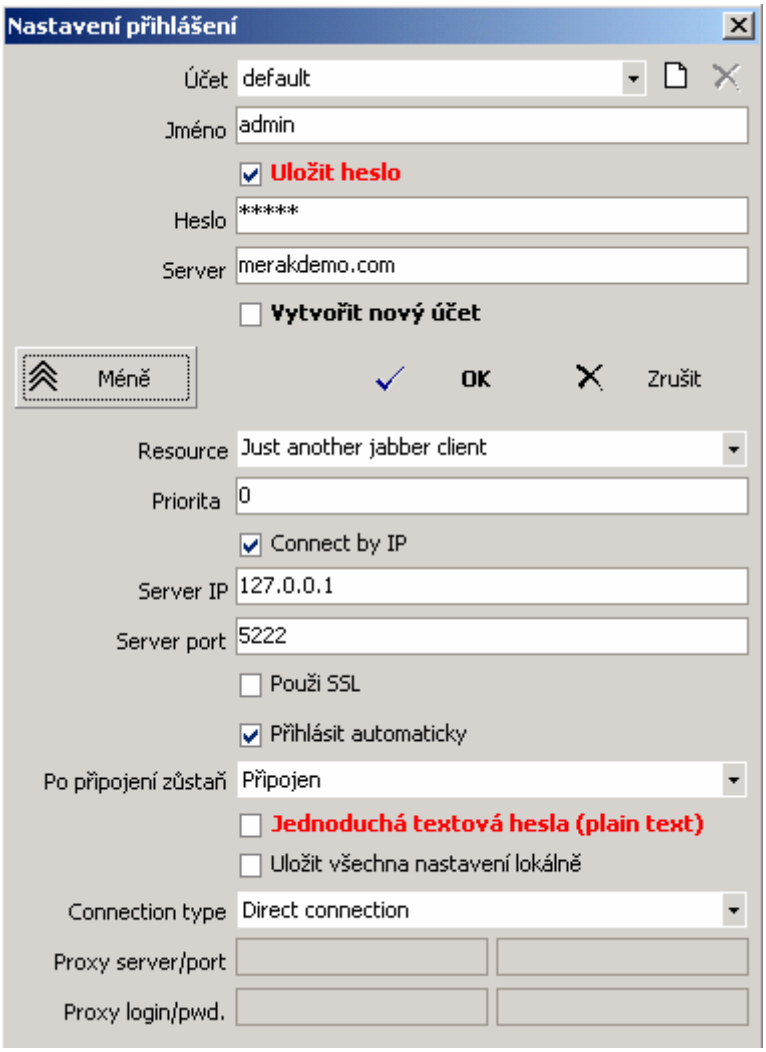
Host adresa našeho mail serveru bude **mail.merakdemo.com**

Pro připojení stačí zadat do programu Vaše přihlašovací údaje a jméno domény.



Pole	Popis
Jméno	Zde použijte Váš **ALIAS** ne uživatelské jméno (mailbox name)
Heslo	Vaše uživatelské heslo
Server	Jméno domény, na kterou se přihlašujete (ne jméno serveru).

Je ale nutné nastavit ještě některé další parametry. Proto zmáčněte tlačítko “Více”.



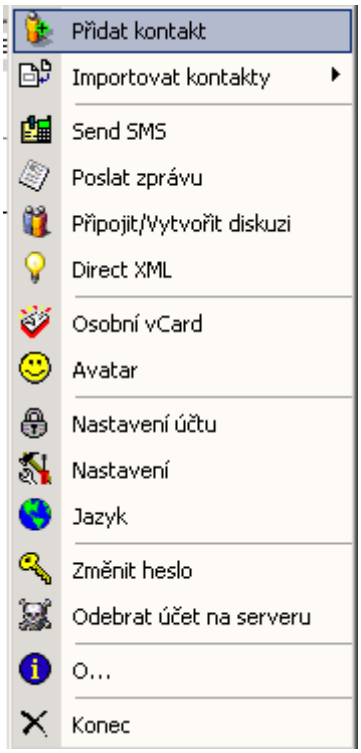
Pole	Popis
Server IP	Zde nastavíte IP adresu IM serveru
Server Port	Port, který má být používán pro spojení. Pokud chcete používat nezabezpečenou formu komunikace, použijte číslo portu 5222, pro zabezpečnou formu (SSL) je číslo portu 5223.
Použít SSL	Pokud chcete zabezpečit svoji komunikaci, stačí zaškrnout toto pole. Funkce je standardně zapnuta.

Ostatní funkce není nutné vyplňovat.

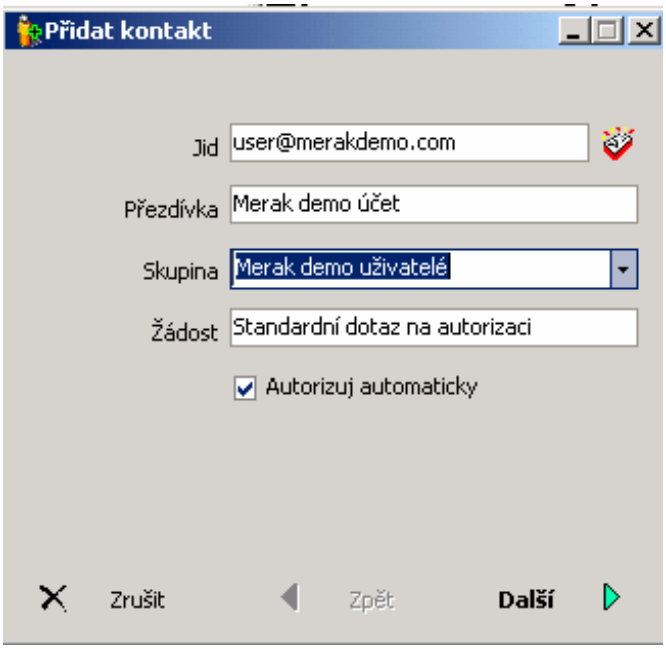
Po připojení by měl klientský program JAJC vypadat asi takto:

Pro komunikaci ale potřebujete přidat uživatele do svého Contact listu. Postup je následující:

Klikněte na horní ikonku žárovky a použijte hned první pole “Přidat kontakt”:

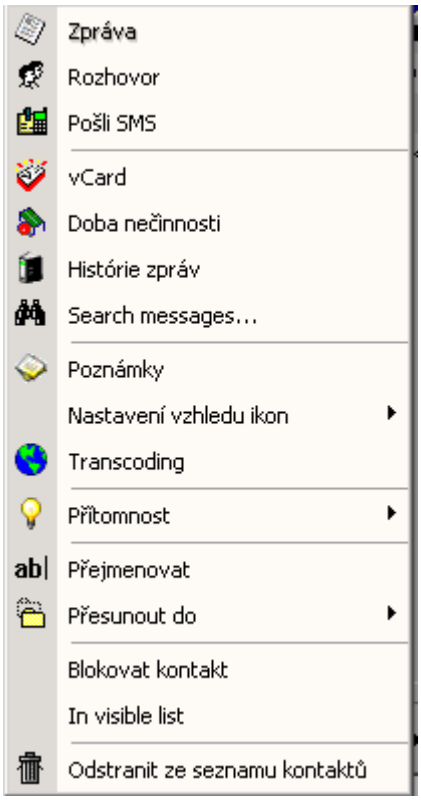


Bude následovat vyvolaná nabídka, vyžadující bližší informace o uživateli, kterého chce přidat do Contact listu.



Po přidaní uživatele se automaticky objeví kontakt ve skupině, kterou jsme definovalo:

Nyní můžeme s uživatelem komunikovat:

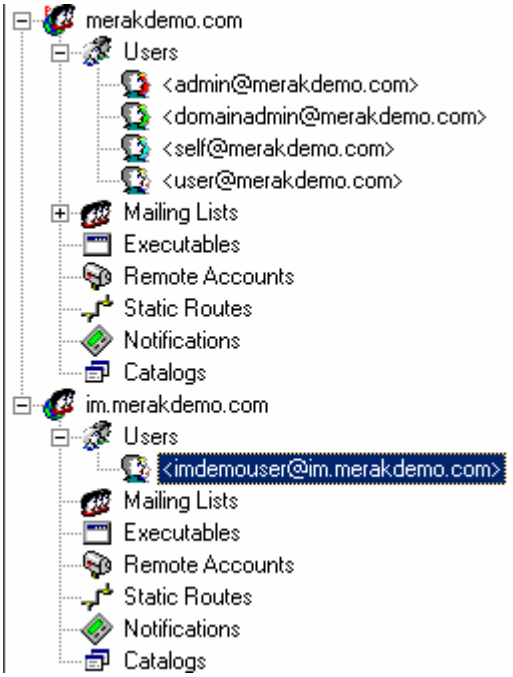


Více doménová komunikace v rámci IM

Muti doménova Instant Messenger komunikace je dostupná pro obě multidoménové verze Merak mail server:

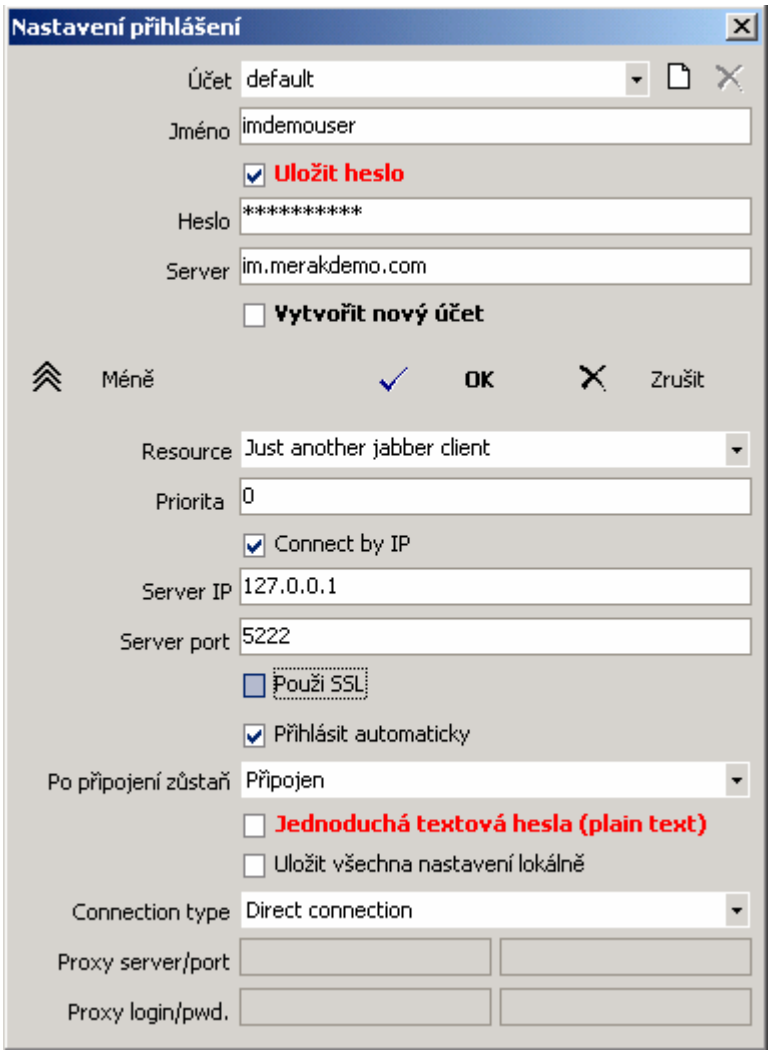
Merak Mail server Standard	Omezená na 500 uživatelů Instant Messengeru a to pro všechny domény.
Merak Mail server Professional Power pack	Verze neomezená na počet IM uživatelů

Na server máme tedy dvě existující domény (**merakdemo.com** a **im.merakdemo.com**).



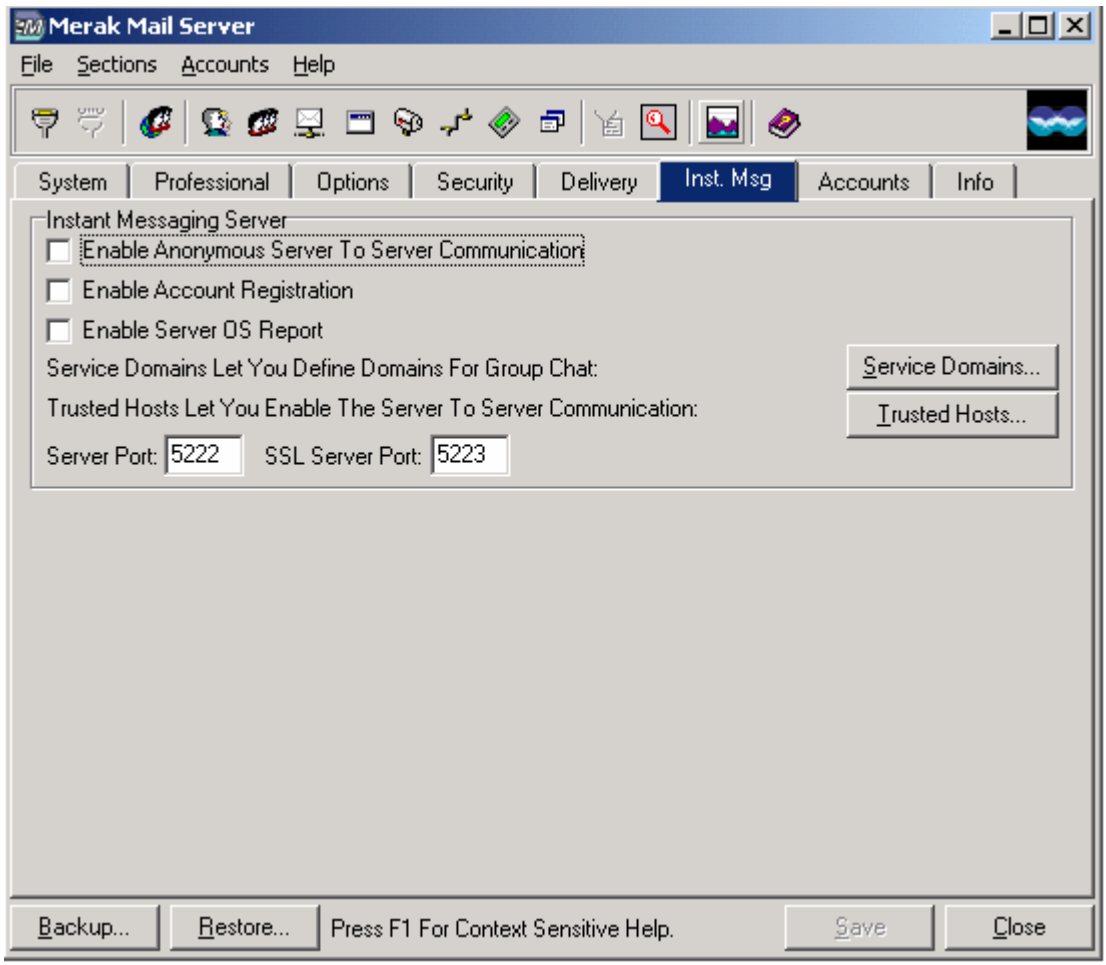
V doméně **merakdemo.com** jsou založeni standardní uživatelé, zatímco v doméně **im.merakdemo.com** je založen pouze jediný testovací uživatel nazvaný **imdemouser**.

Ten se bude do svojí domény připojovat následujícím způsobem:

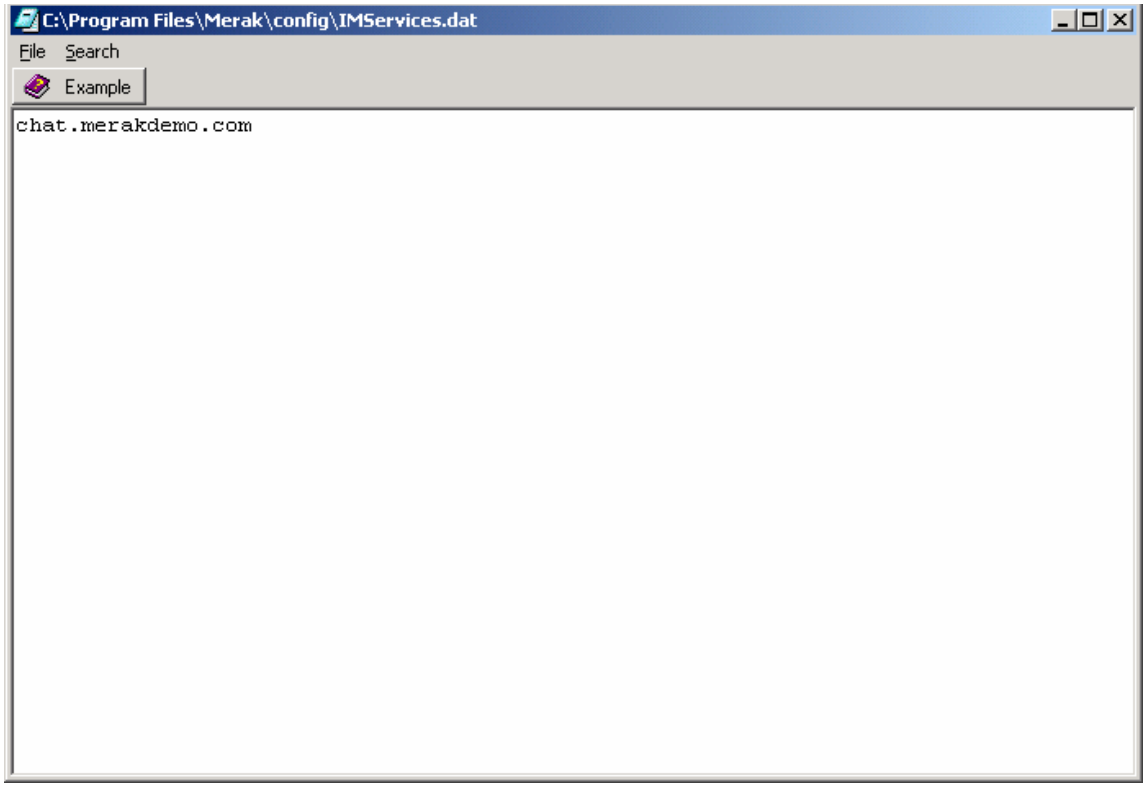


Anonymní skupinový chat

Anonymní skupinový chat umožňuje spojení a komunikaci více uživatelů současně a ve stejné chvíli. Pro připojení je ale nutné nejdřívě definovat chatovou místnost. To nastavíme pomocí Merak konifuračního appletu (v tabulce Inst. Msg. Tab.):



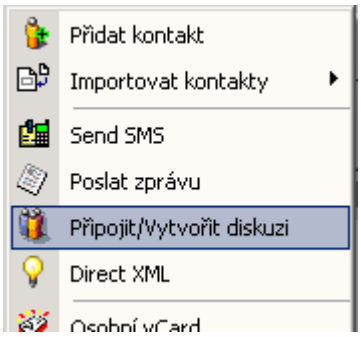
Klikneme na tlačítko Serice Domains a pak nadefinujeme název místnosti

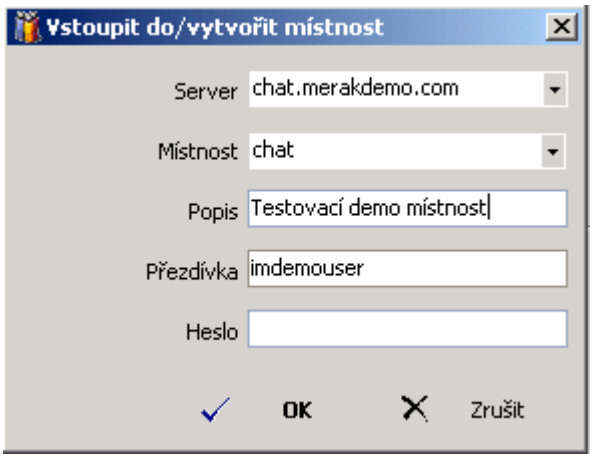


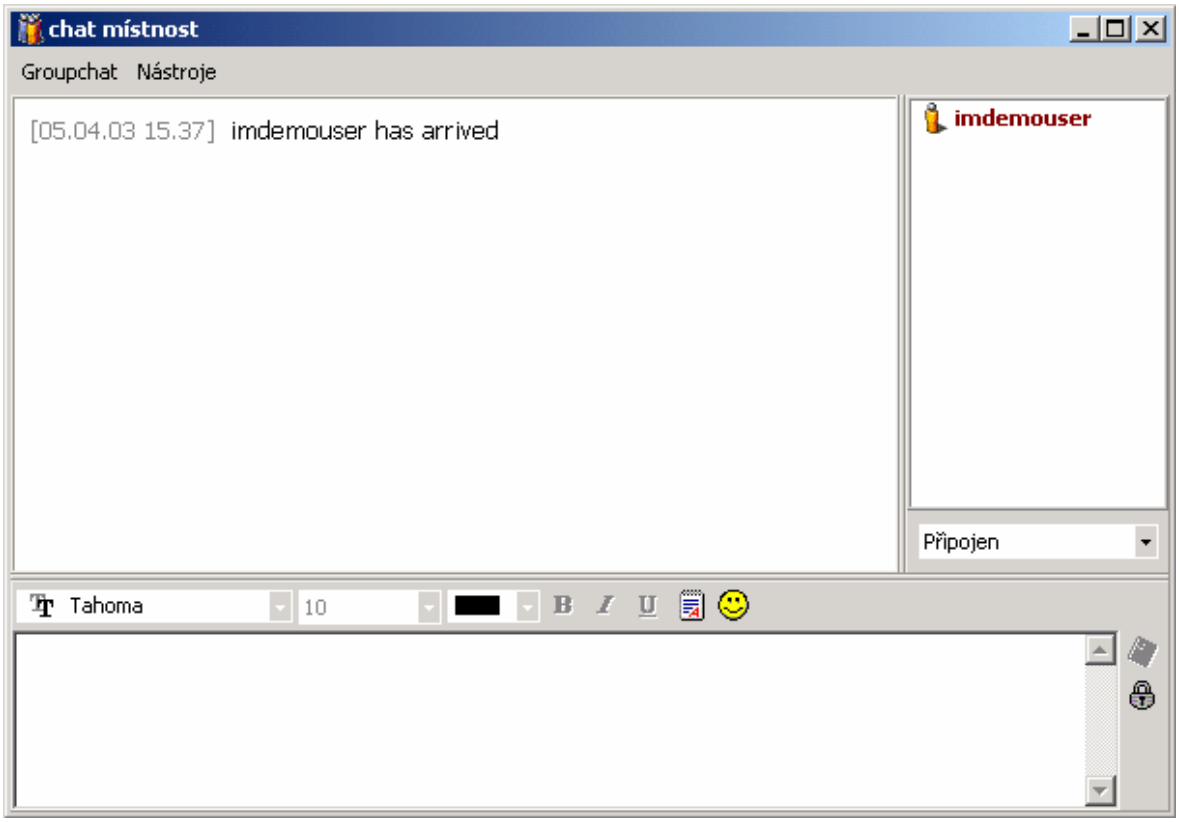
Jméno místnosti ale nesmí být zároveň jméno již jiné fyzicky existující domény. Nejsou potřeba žádné DNS záznamy. Jedná se pouze o nastavení v rámci Merak Mail serveru.

V našem příkladu je jméno místnosti definováno na **chat.merakdemo.com**

Nyní se pokusíme vstoupit do mistnosti. Pro vytvoření/vstup do anonymní chat místnosti z JAJC klienta klikneme na ikonku žárovky.






chat místnost
Groupchat
Nástroje
[05.04.03 15.37] imdemouser has arrived
imdemouser
Připojen
Tahoma
10