



AEC

ASSOCIATION FOR ELECTRONICS AND COMPUTERS Ltd.



IRONWARE

Security Suite

7

IronWare[®] Security Suite - Servers 7.2

Příručka uživatele

Všechna jména produktů, zmiňovaná v tomto dokumentu, jsou obchodní značky nebo registrované obchodní značky svých vlastníků. Společnost AEC, spol s r.o. nemá žádné vlastnické zájmy na těchto značkách a jménech. Ačkoliv společnost AEC, spol. s r.o. vynaloží veškeré úsilí k zajištění přesnosti informací uvedených v tomto dokumentu, není zodpovědná za jakékoliv chyby nebo opomenutí faktů zde uvedených. Společnost AEC, spol s r.o. si rezervuje právo modifikovat specifikace citované v tomto dokumentu bez předchozího upozornění.

Společnosti, jména a data použitá jako příklady v tomto dokumentu, jsou fiktivní, není-li uvedeno jinak. Žádná část tohoto dokumentu nesmí být reprodukována ani přenášena v jakékoliv formě nebo jakýmikoliv prostředky, elektronickými nebo mechanickými, za jakýmkoliv účelem, bez předchozího výslovného písemného povolení společnosti AEC, spol s r.o.

Copyright © 1997-1999 AEC spol s r.o. Všechna práva vyhrazena.
Technická podpora: +420 (0)5 4123 5468
Váš lokální kontakt: support@aec.cz
srpen 2000

• Obsah

• Obsah	3
• Základní charakteristika	5
Nejdůležitější vlastnosti	6
IronWare® Management Server	8
• Instalace IW Management Serveru	8
• Odinstalace IW Management Serveru	12
• Konfigurace IW Management Serveru	13
• Změna TCP portu IW Management Serveru	13
• Použití licenčních klíčů	14
IW FTP Server	15
• Instalace a odinstalace	15
• Administrační konzola FTP serveru	18
• K čemu je určena	18
• Popis menu Administrační konzoly	19
• Hlavní	19
• Nastavení	20
Záložka Hlavní	21
Záložka Složky a soubory	23
Záložka TCP/IP protokol	24
Záložka Firewall	25
Záložka Log	27
• Náповěda	28
• Nastavení serveru (levé okno)	30
• Virtuální servery	30
• Nastavení virtuálních FTP serverů	31
• Hlavní nastavení	32
Sekce FTP server	33
Sekce Hlášení při vstupu do složky	33
Sekce Přihlašování	34
Sekce Vyrovnávací paměť pro FTP pakety	34
• Ovládací panel	34
• Systémové informace serveru	35
• Zabezpečení	35
• Hlášení	35
• Nastavení uživatelů	36
• Nastavení uživatele	36
Sekce Nastavení složek uživatele	40
Nastavení IP adresy účtu uživatele	40
Nastavení virtuální složky účtu uživatele	41

Nastavení IP adres uživatele	42
Provoz serveru jako NT služba nebo NT aplikace	42
• Logování	43
• Použití šifrovaného tunelu a autentizace	45
• Použití šifrovaného tunelu pro administraci	46
IronWare® Certificate Server	47
• Instalace IW Certificate Serveru	47
• Odinstalace IW Certificate Serveru	48
• Administrační konzola Certifikačního serveru	48
IronWare® LDAP Server	51
• Instalace IW LDAP Server	51
• Konfigurace IW LDAP Serveru	51
Replikace databáze LDAP Serveru	53
• Technická podpora	56

• Základní charakteristika

IronWare® Management Server je databázový server, který zpřístupňuje databázi PKI po síti, k níž se připojuje pomocí bezpečného ODBC ovladače. Je naprogramován tak, aby byl maximálně stabilní a co nejlépe odolával případným útokům ze sítě. Zpřístupňuje také obsah IW Audit Logu na serveru.

Dále IW Management Server kontroluje všechny prováděné akce a oprávnění uživatelů k těmto činnostem. Kontroluje také licenční klíč, který obsahuje informaci o počtu instalací, a pomocí údajů které z tohoto klíče získá kontroluje maximální počet přihlášených uživatelů a uživatelů v databázi. Licenční klíč pro registraci všech uživatelů v síti také administrátor importuje pouze jedenkrát a to do serverového PKI a Server zabezpečuje jeho distribuci po síti při přihlášení uživatele.

IronWare® FTP Server je klasický FTP server rozšířený o zabezpečovací funkce včetně šifrování přenášených dat, vybudování bezpečného tunelu a jednoznačné autentizace klienta pomocí soukromého/veřejného klíče. Ve spojení s IW FTP Clientem je schopen vytvořit virtuální privátní síť (VPN).

Umožňuje správu uživatelských účtů, důkladné a individuální nastavování přístupových práv pro jednotlivé uživatele, zpětnou kontrolu přes DNS LookUp, povolení přístupu podle IP adres (ze kterých internetových adres se uživatelé mohou a ze kterých naopak nemohou připojit), šifrovanou autentizaci založenou na dvojici certifikát (obsahuje mimo jiné veřejný klíč) a soukromý klíč, šifrovaný tunel s FTP klientem IW FTP Client, protokolování vlastního chodu a mnoho dalších užitečných funkcí.

IW FTP Server je jednou ze součástí balíku IronWare® Security Suite. Je vhodným doplňkem subsystému IW FTP Client.

Pokud se k IW FTP Serveru připojuje IW FTP Client, mohou před začátkem přenosu provést oboustrannou autentizaci (tj. ověřit, zda se jedná skutečně o odpovídající server a klient, nikoliv o narušitele) a teprve potom navázat spojení tzv. bezpečným kanálem. V oblasti kryptografie je tato technologie považována za špičkovou.

Nejdůležitější vlastnosti

- program je určen pro systémy Windows 95/98 a Windows NT
- podporuje všechny běžné FTP příkazy a všechny obvyklé funkce FTP serverů
- umožňuje tvorbu virtuálních FTP serverů
- na systému Windows NT umožňuje spouštění v režimu NT služby (services)
- obsahuje modul pro vzdálenou správu serveru z libovolné stanice
- monitorování činnosti uživatelů (ovládací panel a podrobné log soubory)
- monitorování zatížení a činnosti serveru pomocí Windows NT Performance Monitor
- server podporuje automatické navázání přerušeného přenosu
- server podporuje klasické i pasivní sockety
- bezpečná autentizace uživatele na základě veřejného a soukromého klíče
- možnost autentizace uživatele pomocí Windows NT účtů
- možnost kombinace vlastních přístupových práv s Windows NT NTFS právy
- kontrola uživatele pomocí DNS LookUp
- kontrola uživatele pomocí IP adresy
- možnost vytváření virtuálních složek jednotlivě pro každého uživatele IW FTP Serveru
- individuální nastavování přístupových práv pro všechny uživatele
- při spojení s IW FTP Client umožňuje vytvořit šifrovaný tunel

IronWare® Certificate Server slouží jako server pro vytvoření Certifikační autority. Slouží ke správě, generování, odvolávání i dalším operacím s certifikáty veřejných klíčů. Jde o velmi důležitou součást PKI, která umožňuje především velkým společnostem vytvořit skutečně propracovanou a bezpečnou klíčovou infrastrukturu s centrálním managementem. Nemusí však být vždy instalován, pokud si to uživatel nepřeje. Je navržen tak, aby byl schopen pracovat samostatně a podporovat práci s certifikáty veřejných klíčů libovolných aplikací, které dodržují mezinárodně uznávané standardy pro práci s certifikáty. Sám o sobě nemá Certifikační server uživatelské rozhraní, a ovládání se provádí prostřednictvím Administrační konzoly.

IronWare® LDAP Server slouží pro přístup k certifikátům vydaných IW Certificate Serverem (certifikační autoritou) pomocí standardu LDAP. Nedílnou součástí IW LDAP Serveru je i replikační plánovač, který ve stanovených intervalech aktualizuje LDAP databázi certifikátů. IW LDAP Server zde uchovává záznamy o uživateli a jejich certifikátech.

Minimální konfigurace

Jednotlivé produkty vyžadují ke své činnosti minimálně tuto hardwarovou konfiguraci:

IronWare® Management Server

16 MB RAM pro instalaci do Windows 95
32 MB RAM pro instalaci do Windows NT
15 MB diskového prostoru + volný prostor pro databázi uživatelů a klíčů
procesor Pentium a vyšší

IronWare® FTP Server

16 MB RAM pro instalaci do Windows 95
32 MB RAM pro instalaci do Windows NT
15 MB diskového prostoru + volný prostor pro FTP Root
procesor Pentium a vyšší

IronWare® Certificate Server

Operační systém Windows NT Workstation nebo NT Server + Service Pack 3 a vyšší

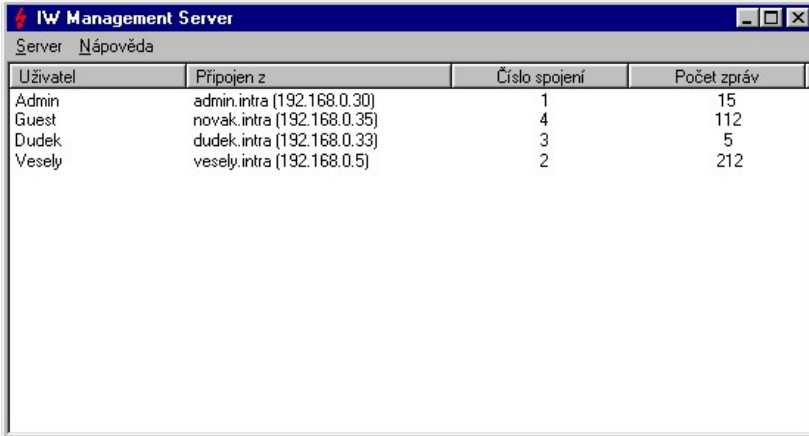
32 MB RAM pro instalaci do Windows NT
15 MB diskového prostoru + volný prostor pro databázi
procesor Pentium a vyšší

IronWare® LDAP Server

Operační systém Windows NT Workstation nebo NT Server + Service Pack 3 a vyšší

32 MB RAM
15 MB diskového prostoru + volný prostor pro databázi
procesor Pentium a vyšší

IronWare® Management Server



The screenshot shows the main window of the IW Management Server. The title bar reads 'IW Management Server'. Below the title bar is a menu bar with 'Server' and 'Nápověda'. The main area contains a table with the following data:

Uživatel	Připojen z	Číslo spojení	Počet zpráv
Admin	admin.intra (192.168.0.30)	1	15
Guest	novak.intra (192.168.0.35)	4	112
Dudek	dudek.intra (192.168.0.33)	3	5
Vesely	vesely.intra (192.168.0.5)	2	212

Obr.1. IW Management Server - hlavní okno programu

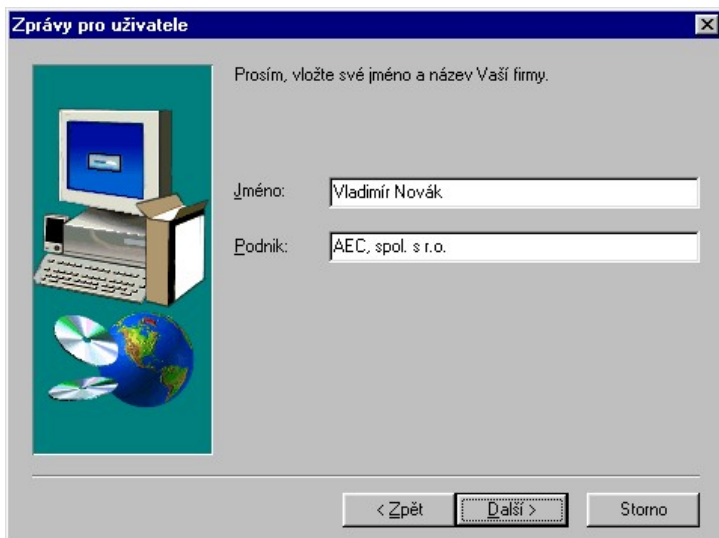


Jelikož v systému Windows NT je IW Management Server spouštěn jako NT služba, nemá v tomto operačním systému žádné uživatelské rozhraní. O tom, že je IW Management Server korektně spuštěn, se může uživatel přesvědčit v pravé části hlavního panelu, kde je zobrazena jeho ikona. Ponecháním kurzoru myši na této ikoně se zobrazí počet připojených uživatelů.

• Instalace IW Management Serveru

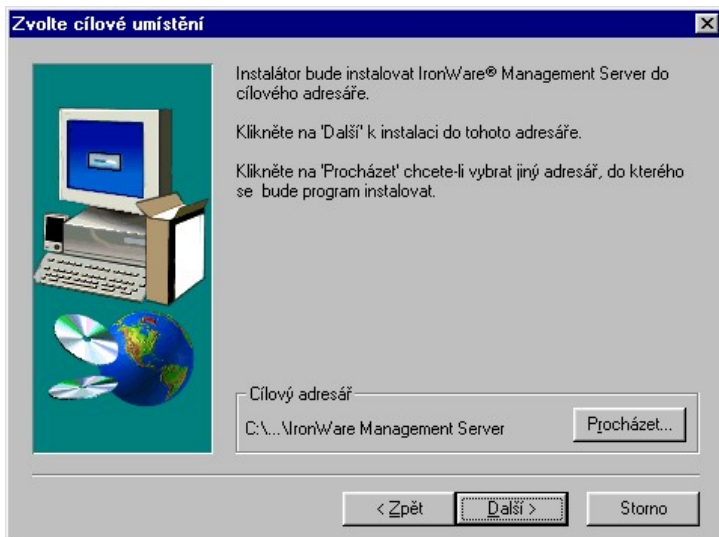
Instalace i odinstalace se provádí formou standardního instalačního průvodce. Je vhodné před instalací zavřít všechny aplikace, neboť instalace vyžaduje restart systému.

Instalace má několik fází, které proběhnou podle potřeby. Nejdříve instalátor znázorní průběh přípravy k instalaci. Poté se spustí vlastní instalační proces, který v prvních krocích upozorní na zákonnou ochranu produktu a vyžádá si souhlas s licenčními podmínkami. Dále je třeba zadat jméno a název firmy uživatele.



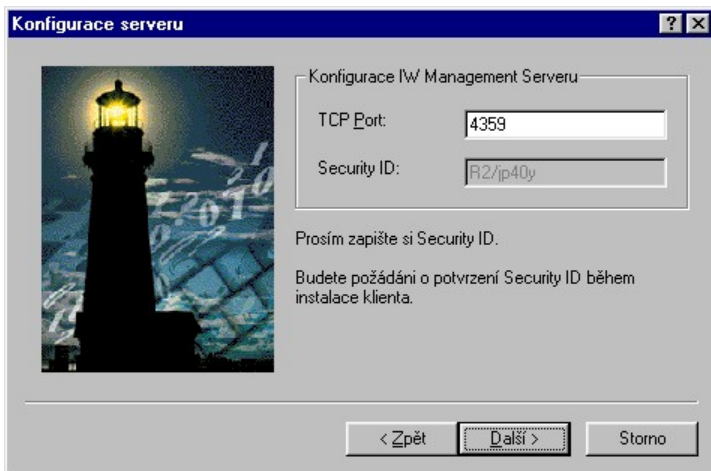
Obr. 2. Instalace IW Management Server – zadání informací o uživateli

Poté se instalátor dotáže na cílovou složku. V tomto dotazu je nastavena implicitní cesta, kam se má IW Management Server nainstalovat. V případě, že přednastavená cesta z nějakého důvodu nevyhovuje, je možné zadat jinou pomocí tlačítka „Procházet“.



Obr.3. Instalace IW Management Server – zadání cesty pro instalaci

Průvodce instalací provede sběr náhodných čísel. Dále je nutné zadat připojovací port (implicitně 4359). Na tento port se budou připojovat všechny klientské aplikace. Zobrazí se unikátní identifikace (Security ID) instalovaného IW Management Serveru vytvořená z těchto nasbíraných náhodných čísel.

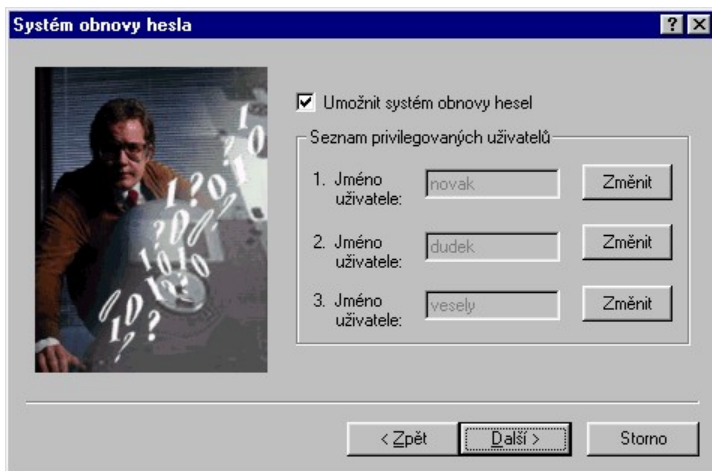


Obr. 4. Instalace IW Management Server – vyplnění čísla portu a zobrazení Security ID

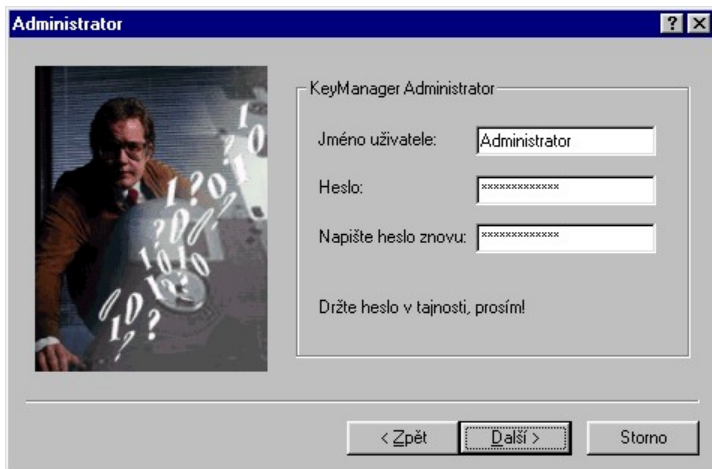
Následuje dotaz na název položky, která po instalaci přibude v nabídce *Start/Programy*.

Po potvrzení, že všechna předchozí nastavení jsou správná, se spustí proces kopírování souborů. Instalátor znázorňuje jeho průběh a část podsystému, která je právě instalována.

Po dokončení kopírování se spustí instalační průvodce, ve kterém bude možné provést nastavení IW Management Serveru. Je třeba vytvořit administrátora PKI a volitelně tři privilegované uživatele zaškrtnutím volby *Umožnit systém obnovy hesel*. Zadání uživatelských jmen a hesel privilegovaných uživatelů se provede v okně vyvolaném příslušným tlačítkem „Změnit“.



Obr. 5. Instalace IW Management Serveru - zadání privilegovaných uživatelů



Obr. 6. Instalace IW Management Server - vytvoření administrátora lokálního PKI

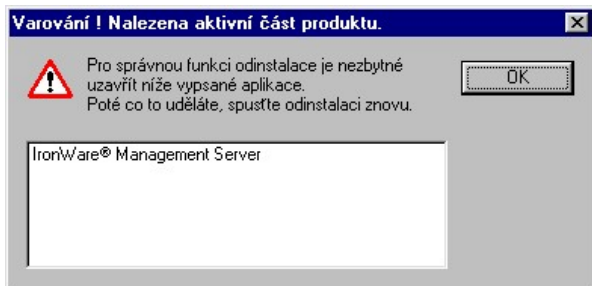
Průvodce instalací na závěr oznámí úspěšné dokončení instalace a po restartu systému je IW Management Server připraven k použití. Bude se spouštět automaticky při startu Windows.



Vzhledem k možnostem systému obnovy hesel z bezpečnostních důvodů doporučujeme privilegovaným uživatelům, aby svá hesla zadali ihned při instalaci IW Management Serveru.

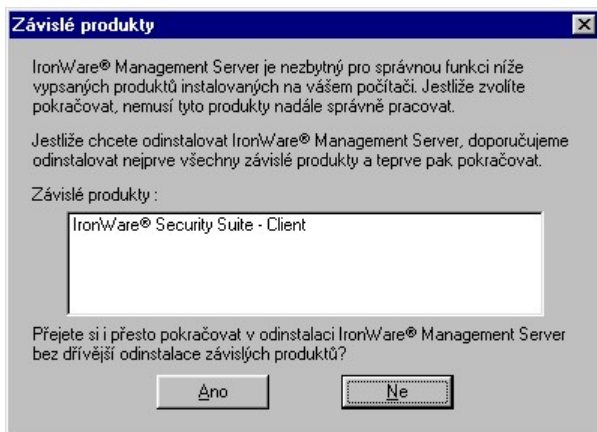
- **Odinstalace IW Management Serveru**

Spustí se část instalačního průvodce zajišťující odinstalaci. Vyžádá si potvrzení provedení odinstalace. Před odinstalací je nutné činnost IW Management Serveru ukončit, jinak není možné odinstalaci provést. Průvodce tuto skutečnost oznámí.



Obr. 7. Odinstalace IW Management Server - upozornění na běžící IW Management Server při odinstalaci

Je-li instalován produkt IW Security Suite Client a IW Management Server na stejném počítači, je nutné nejdříve odinstalovat Client a teprve potom IW Management Server. Průvodce odinstalací tuto skutečnost rozpozná a upozorní uživatele.



Obr. 8. Odinstalace IW Management Server - varování před odinstalací serveru na počítači, kde je současně nainstalován klient

Poté je zahájeno odstraňování souborů. Protože některé z nich mohou být sdílené i pro jiné aplikace, bude pro jejich smazání vyžadáno zvláštní potvrzení.

Při volbě „Ano všem“ se instalátor ještě jednou ujistí, že volba byla provedena úmyslně, neboť smazání některých souborů by mohlo způsobit problémy jiným aplikacím.

Po odstranění všech příslušných komponent informuje o ukončení odinstalace (Ize si nechat zobrazit i detailní seznam všeho, co bylo odstraněno) a vyžádá si restart Windows.

- **Konfigurace IW Management Serveru**

- **Změna TCP portu IW Management Serveru**

Vzhledem ke skutečnosti, že IronWare® Management Server nemá v protokolu TCP/IP vyhrazeno standardní číslo TCP portu, je implicitně zvoleno číslo portu 4359 ze skupiny čísel určených k použití pro software bez čísla portu definovaného normou. Může však nastat případ, kdy některý produkt jiné firmy bude požadovat pro svůj software právě toto číslo portu.

Aby se zabránilo případným problémům, umožňuje Management Server výběr jiného čísla TCP portu.



Obr. 9. IW Management Server - změna čísla TCP portu

Číslo portu je možné nastavit z intervalu 1024 – 32767. V případě výběru nepovoleného čísla portu bude uživatel informován, že jím zadané číslo nelze použít.

- **Použití licenčních klíčů**

Registrace proběhne importem licenčního klíče. Registrační soubor však může být ručně zkopírován do podsložky ...\\Server\ ve složce, kam byl IW Management Server nainstalován.

Pokud uživatel provede registraci IW Management Server, není nutné zaregistrovat jednotlivé klienty, jelikož je implementován mechanismus distribuce licenčního klíče. Po instalaci IW Security Suite Client a prvním přihlášení k IW Management Serveru proběhne registrace klienta automaticky.

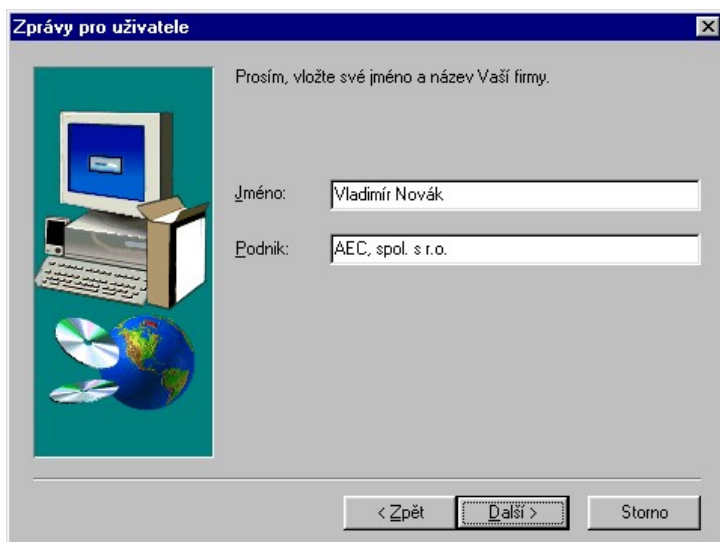
Komunikace mezi IW Management Serverem a klientem probíhá šifrovaně a je digitálně podepsána. Klient a IW Management Server jsou při spojení vzájemně autentizováni podle normy X509.v3

IW FTP Server

• Instalace a odinstalace

Instalace i odinstalace se provádí formou standardního instalačního wizardu. Je vhodné před instalací zavřít všechny aplikace, neboť instalace vyžaduje ve většině případů restart systému.

Nejprve instalátor znázorní průběh přípravy k instalaci. Poté se spustí vlastní instalační proces, který v prvních krocích upozorní na zákonnou ochranu produktu a vyžádá si souhlas s licenčními podmínkami. Dále je třeba zadat jméno a firmu uživatele:



Obr. 10. IW FTP Server - instalace – informace o uživateli

Poté se instalátor dotáže na cílovou složku. V tomto dotazu je nastavena implicitní cestu, kam se má IW FTP Server nainstalovat. V případě, že přednastavená cesta z nějakého důvodu nevyhovuje, je možné zadat jinou, a to buď přímo nebo pomocí tlačítka *Procházet*.

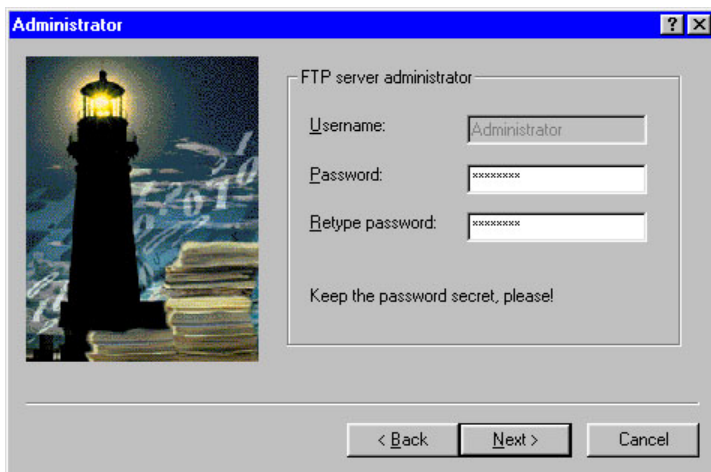


Obr. 11. IW FTP Server - výběr instalační složky

Následuje dotaz na název položky, která po instalaci přibude v nabídce *Start/Programy*, a dotaz na cestu ke kořeni FTP Serveru (složka, která se uživatelům přihlášeným z IW FTP Client zobrazí jako kořenová).

Po potvrzení, že všechna předchozí nastavení jsou správná, se spustí proces kopírování souborů. Instalátor znázorňuje jeho průběh.

V následujícím kroku je nutné zadat heslo administrátora FTP Serveru. Jeho uživatelské jméno není možné měnit!



Obr. 12. IW FTP Server - nastavení hesla administrátora IW FTP Serveru

Tím je vlastní instalace ukončena, je však nutné vygenerovat soukromý klíč a certifikát pro administrátora PKI. Přednastavené jméno klíče je FTPServerKey a jméno certikátu doporučujeme FTPServerCert. Certifikát může být Self-signed nebo může být vygenerována žádost pro certifikační autoritu a poslána k certifikaci do Certifikační Autority. Certifikát obdrženy od Certifikační Autority pak administrátor PKI importuje do PKI.

Následuje vygenerování soukromého klíče a certifikátu pro Administrační konzolu FTP Serveru. Přednastavené jméno klíče je RemoteAdminKey a jméno certifikátu doporučujeme RemoteAdminCert. Certifikát může být Self-signed nebo může být vygenerována žádost pro certifikační autoritu a poslána k certifikaci do Certifikační Autority. Certifikát obdrženy od Certifikační Autority pak administrátor PKI importuje do PKI .

Po restartu Windows je IW FTP Server připraven k použití.

Před instalací subsystému IW FTP Server zkontrolujte, že máte nainstalovaný TCP/IP protokol a nakonfigurovaný FTP protokol.

Jestliže chcete program IW FTP Server spouštět jako systémovou službu NT, je nutno v *Ovládacích panelech - Služby* nastavit položku IW FTP Server *Service Při startu* na *Automaticky*.

Program můžete odinstalovat pomocí volby *Přidat nebo ubrat programy* v *Ovládacích panelech* nebo opětovným spuštěním instalačního průvodce a vybráním si volby *Odinstalovat program*. Pokud stále ještě existuje složka, kde byl program instalován, vymažte ji.

Volitelně můžete smazat FTP Root, pokud jej již nebudete nadále potřebovat.

• Administrační konzola FTP serveru

• K čemu je určena

Administrační konzola je určena k lokální nebo vzdálené správě FTP Serveru. V rámci každého produktu (zde IW FTP Serveru) lze spravovat libovolné množství jeho instalovaných kopií.

Administrační konzola používá ke spojení s administrovanou aplikací speciální protokol založený na TCP/IP. Jako výchozí je používán port 721, který však lze změnit (viz pravé tlačítko na Aplikaci - Vlastnosti, položka Port). Pokud chcete změnit číslo portu pro administraci, nesmíte zapomenout toto číslo portu změnit také na spravované aplikaci.

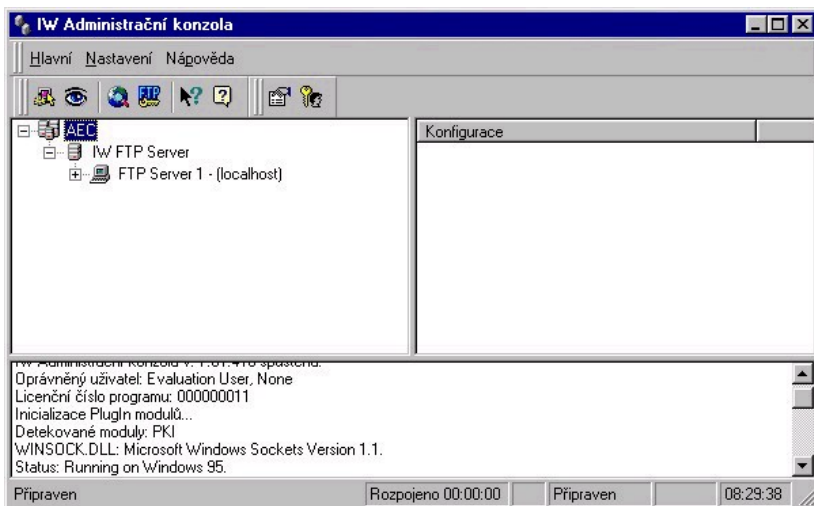
Pro zvýšení bezpečnosti administrace je možno zapnout používání šifrovaného tunelu mezi Administrační konzolou a spravovanou aplikací. Zvolte aplikace, ke které se chcete připojit. V panelu nástrojů administrační konzoly klikněte na tlačítko *Připojit* nebo použijte pravé tlačítko na dané aplikaci a zvolte položku *Připojit* nebo použijte dvojklik na dané aplikaci.

Poté vyčkejte na připojení Administrační konzoly k dané aplikaci. Po připojení k aplikaci se "rozbalí" strom s jednotlivými položkami správy aplikace.

Průběh připojování a příkazy pro vlastní správu lze monitorovat v protokolovacím okně.

Zvolte aplikace, od které se chcete odpojit. V panelu nástrojů administrační konzoly klikněte na tlačítko *Odpojit* nebo použijte pravé tlačítko na dané aplikaci a zvolte položku *Odpojit*.

Poté vyčkejte na odpojení Administrační konzoly od dané aplikaci. Po odpojení od aplikaci "zmizí" strom s jednotlivými položkami správy aplikace. Průběh odpojování lze monitorovat v protokolovacím okně.



Obr. 13. IW FTP Server - Administrační konzola

- **Popis menu Administrační konzoly**

- **Hlavní**

Nabídka *Hlavní* nabízí uživateli programu IW FTP zobrazit log protokol, odsdkoky na asociované programy a vlastní ukončení programu.

Zobrazit protokol o činnosti - příkaz provede otevření log souboru ve zvláštním okně. Jedná se o textový soubor (jméno a prohlížeč log souboru lze změnit), ve kterém jsou zaznamenány všechny důležité události v systému, především informace o úspěšném přihlášení se, spojení s FTP serverem, o přenosu dat apod. Každá položka v tomto souboru je opatřena časovým razítkem. Povolení zapisování do *log souboru* najdete v menu *Nastavení - Možnosti - záložka Log* . Umístění log souboru lze nastavit v menu *Nastavení - Možnosti - záložka Složky a soubory*.

Zobrazit protokol o zabezpečení - příkaz provede otevření log souboru ve zvláštním okně. Jedná se o textový soubor (jméno a prohlížeč log souboru lze změnit), ve kterém jsou zaznamenány všechny důležité události týkající se zabezpečení systému. Každá položka v tomto souboru je opatřena časovým razítkem. Povolení zapisování do *log souboru* najdete v menu *Nastavení - Možnosti - záložka Zabezpečení* . Umístění log souboru lze nastavit v menu *Nastavení - Možnosti - záložka Složky a soubory*.

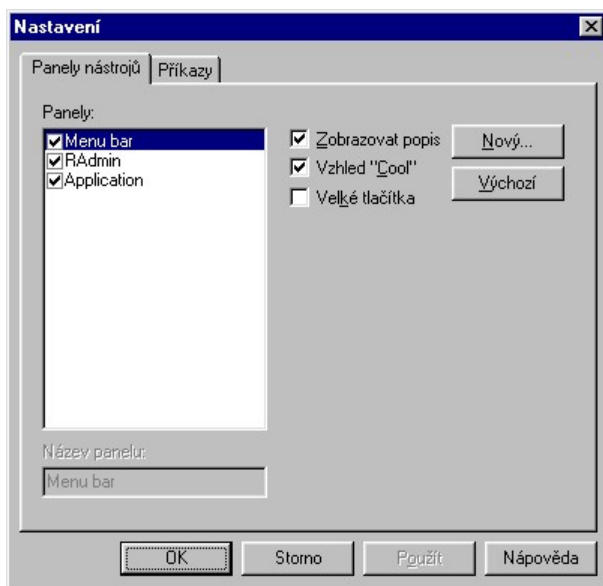
WWW Browser - příkaz spustí asociovaný program WWW prohlížeče (např. *Microsoft Internet Explorer*), který máte nastavený v menu Nastavení - Možnosti - záložka Složky a Soubory.

Konec - kliknutím ukončíte program IW FTP.

• Nastavení

Nabídka *Nastavení* vám umožní snadno a přesně nakonfigurovat celý systém programu IW FTP.

Panely nástrojů - definování vzhledu panelu nástrojů na základě přání a potřeb uživatele.



Obr. 14. IW Administrační konzola – nastavení panelů nástrojů



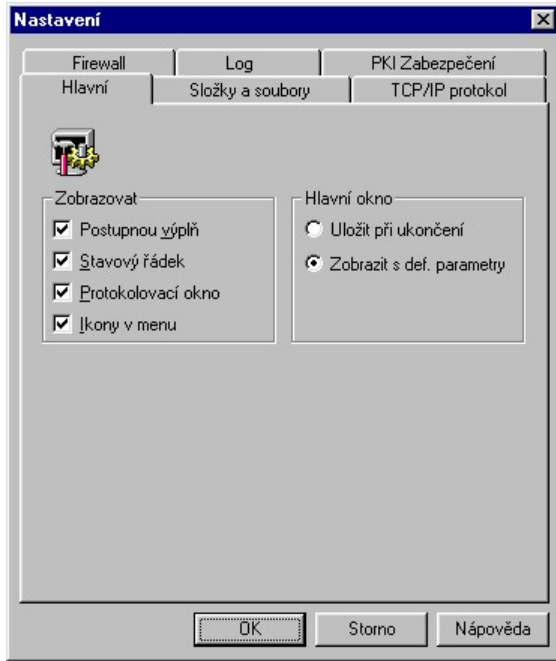
Obr. 15. IW Administrační konzola – změna tlačítek v panelech nástrojů

Příkazy - definování vzhledu jednotlivých příkazů z panelů nástrojů na základě přání a potřeb uživatele.

Můžete zde vybrat kategorii tlačítek (danou kategorií panelu nástrojů - liší se nainstalovanými zásuvnými moduly) a následně některé z tlačítek pomocí myši přidat (přetáhnout) do Vámi nadefinované tlačítkové lišty. Samozřejmě, že opačný postup (odejmutí požadovaného tlačítka z lišty) je také možný. Po klepnutí myši na některé tlačítko v tomto okně se Vám zobrazí jeho popis v sekci *Popis*.

Záložka Hlavní

Záložka *Hlavní* nabízí základní konfigurace Administrační konzoly.



Obr. 16. IW Administrační konzola – záložka Hlavní v Nastavení

Postupná výplň - je-li zatrhnuto, záhlaví okna bude vyplněno barevným přechodem z černé do modré.

Stavový řádek - po zatrnutí bude ve spodní části okna Administrační konzoly zobrazen vodorovný pruh - stavový řádek. Jsou v něm uvedeny informace o aktuálním stavu a aktuální čas. Je-li políčko nezatrhnuto, stavový řádek se nebude zobrazovat vůbec.

Protokolovací okno - je-li zatrhnuto, značí zobrazení okna Log souboru ve spodní části Administrační konzoly.

Ikony v menu - v menu Administrační konzoly zobrazují malé ikony.

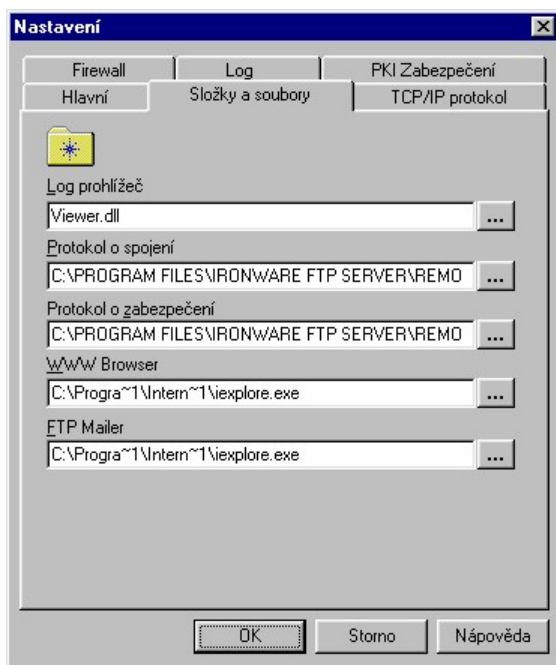
Sekce *Hlavní okno* umožňuje pomocí dvojice přepínacích tlačítek zvolit nastavení velikosti a umístění hlavního okna Administrační konzoly.

Uložit při ukončení - jestliže je tato volba zatrhnuta, znamená to uložení velikosti a umístění okna na obrazovce při správném ukončení Administrační konzoly. Při příštím otevření Administrační konzoly se jeho hlavní okno otevře v takové velikosti a na tom místě, kde ho uživatel před ukončením programu zanechal.

Zobrazit s def. parametry - zatrhnutá položka znamená to, že okno se vždy zobrazí v předdefinované velikosti a místě dle aktuálního rozlišení, nezávisle na tom, v jakém stavu uživatel před tím aplikaci ukončil. Tato varianta se nastaví automaticky vždy při přenastavení rozlišení vlastností monitoru v systému počítače.

Záložka Složky a soubory

V záložce *Složky a soubory* nastavujeme úplnou cestu ke složkám (adresářům), nebo k jednotlivým souborům a doplňkovým aplikacím, které je možné spouštět přímo z okna programu IW FTP. K jednoduššímu zadání cesty k souboru využijte tlačítko „...“ na konci každého vstupního pole.



Obr. 17. IW Administrační konzola – záložka Složky a soubory v Nastavení

Popis jednotlivých položek:

Log prohlížeč - uživatel definuje aplikaci, ve které se zobrazují jednotlivé log soubory. Standardně je nastaven zabudovaný prohlížeč, který je součástí programu IW FTP.

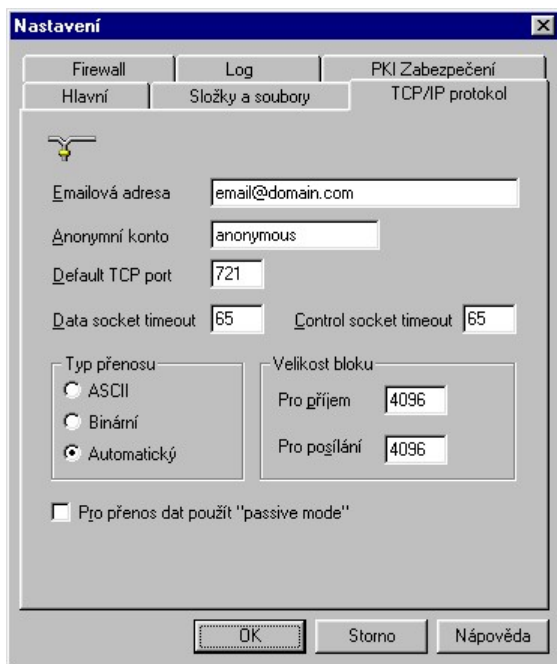
Protokol o spojení - uživatel definuje soubor, do kterého se zapisuje detailní protokol o spojení, ukončení spojení, o přihlášení na vyrovnávací FTP server, o přenosu souborů, o spuštění, přerušení a ukončení událostí, atd.

Protokol o zabezpečení - uživatel definuje soubor, do kterého se zapisuje detailní protokol o zabezpečení, např. zřízení šifrovaného tunelu.

WWW Browser definuje cestu k jakémukoli WWW prohlížeči, který máte nainstalován, a který je potom možné spouštět přímo z okna aplikace FTP Client. Zadáním této cesty se stane funkční ikona v panelu nástrojů znázorňující WWW Browser. (např. *Microsoft Internet Explorer*)

Záložka TCP/IP protokol

Záložka *TCP/IP protokol* umožňuje předdefinovat obecné vlastnosti FTP protokolu.



Obr. 18. Záložka s nastavením TCP/IP protokolu

Emailová adresa - do této položky uživatel zapíše svou e-mail adresu, která bude použita jako heslo v případě použití anonymního přístupu k FTP serveru, vzdálenému počítači.

Anonymní konto - položka pro uživatelské jméno v případě anonymního přístupu k FTP serveru (implicitně *anonymous*).

Default TCP port - číslo FTP portu, na kterém pracuje FTP server (implicitně **21**).

Data Socket Timeout - jde o čas v sekundách potřebný k úspěšnému provedení datových FTP příkazů. Po uplynutí této doby je datový FTP příkaz považován za neúspěšný a program stornuje probíhající krok FTP klienta.

Control Socket Timeout - jde o čas v sekundách potřebný k úspěšnému provedení kontrolních FTP příkazů. Po uplynutí této doby je kontrolních FTP příkaz považován za neúspěšný a program stornuje probíhající krok FTP klienta.

V sekci *Typ přenosu* uživatel definuje pomocí přepínacího tlačítka, jaký typ přenosu souborů zvolit:

- ASCII - lze použít pouze pro textové soubory

- binární - pro všechny soubory kromě textových souborů uložených pod operačním systémem UNIX

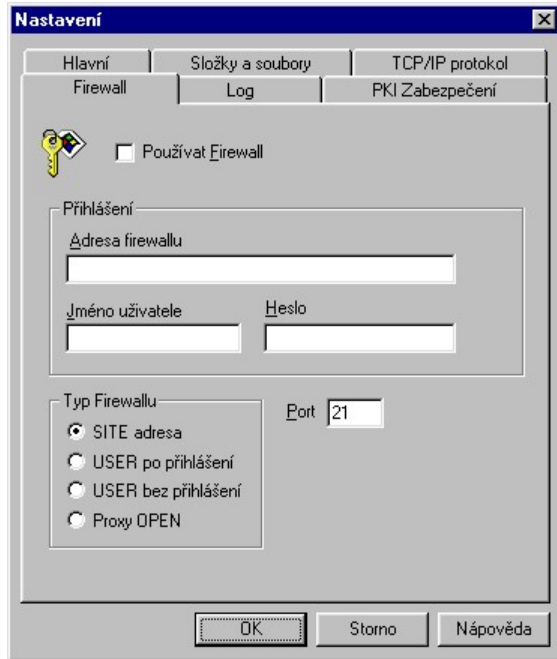
- automatický - program rozhodne podle přípony souboru.

V sekci *Velikost bloku* stanoví uživatel velikost bloku v bytech pro příjem a posílání souborů – při spojení pomocí sítě LAN je možno tuto velikost zvětšit, a tím zrychlit přenos souborů. Doporučená velikost by však neměla přesáhnout 16384 bytů.

Při přenosu dat použít „passive mode“ - zatrhnutím této volby bude pro všechny datové přenosy použit pasivní mód spojení. V tomto módu vyše klient serveru příkaz PASV (RFC967) a provede přímé připojení k serveru na jím zasláný port. Oproti tomu v případě standardního navazování spojení čeká klient na listen portu na spojení, které zahájí server. Passive mod se používá zejména pro připojení přes firewally, které neumožňují zpětné spojení od serveru ke klientovi, nebo pro rychlejší spojení s FTP servery. IW FTP má implementovanou automatickou detekci serverů, které pasivní mód nepodporují a při spojení s takovým serverem a při zatrhnuté volbě *Passive mode* dojde k automatickému dočasnému vypnutí pasivního módu.

Záložka Firewall

Záložka *Firewall* slouží k připojení IW FTP klienta k Internetu přes Proxy Server nebo Firewall a nastavení jeho příslušných parametrů.



Obr. 19. IW Administrační konzola – záložka Firewall v Nastavení

Používat Firewall - uživatel zatrhne v případě pokud chce přistupovat k Internetu přes Proxy Server nebo Firewall.

V poli *Přihlášení* stanoví uživatel v kolonce *Adresa firewallu* jméno stanice, na které běží Proxy server. K dispozici je také kolonka pro definování přihlašovacího jména uživatele a uživatelského hesla.

Do položky *Port* je třeba zadat číslo portu, na kterém pracuje příslušný Proxy server (implicitně **21**).

V sekci *Typ Firewallu* nalezne uživatel čtyři přepínací tlačítka s jednotlivými předvolenými typy Proxy serverů a metod, které používají pro připojení na Internet :

SITE adresa - Proxy server žádá uživatelské jméno a heslo. Nejdříve se uživatel přihlásí na Proxy server a pak teprve je spojení navázáno se vzdáleným počítačem s použitím SITE adresy.

USER po přihlášení - Proxy server žádá jméno uživatele a jeho heslo. Uživatel je přihlášen na Proxy server a spojení se vzdáleným počítačem je navázáno s použitím příkazu USER

UserNameOnRemote@RemoteHost.

USER bez přihlášení - Jméno uživatele a jeho heslo se ignorují. USER UsernameOnRemote@RemoteAddress se posílá na Proxy server po úvodním spojení.

Proxy OPEN - žádosti Proxy serveru o uživatelské jméno a heslo jsou ignorovány. OPEN remote_host se posílá Proxy serveru po úvodním spojení.

Příklad:

Například pro proxy server Wingate nebo WinProxy nastavte:

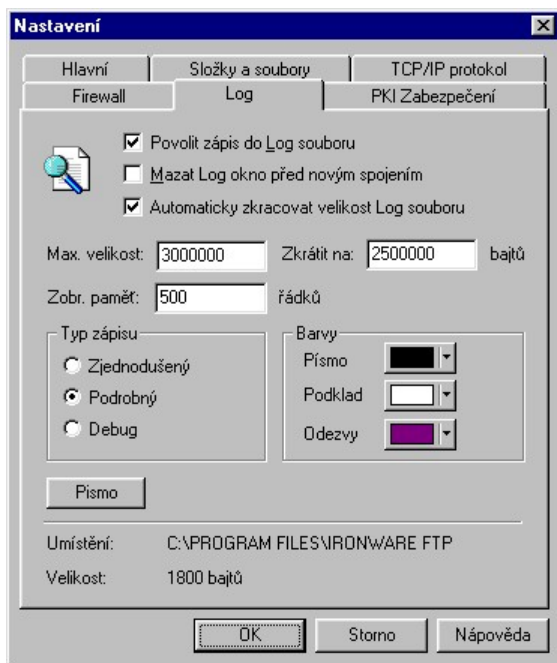
Používat Firewall - zatrhnuto.

Adresa firewallu - vepište IP stanice, na které je spuštěn Wingate.

V sekci *Typ Firewallu* si vyberte položku USER.

Záložka Log

Okno nastavení vlastností Log souboru zobrazí všechny možnosti vzhledu Log souboru.



Obr. 20. IW Administrační konzola – záložka Log v Nastavení

Zatrhnutím položky *Povolit zápis do Log souboru* se povoluje nebo zakazuje ukládání informací o průběhu jednotlivých událostí do log souboru. Název a cestu k tomuto log souboru definujeme v záložce *Složky a soubory*.

Pokud je zatrhnuta *Mazat Log okno před novým spojením* pak dojde před spuštěním jakékoli události vymazáno Log okno.

Jestliže zvolíte *Automaticky zkracovat velikost Log souboru* pak lze definovat velikost (v bytech) Log souboru.

Max. velikost určuje největší možnou velikost Log souboru. V případě, že je velikost překročena, je soubor automaticky redukován na velikost souboru, která je definována v kolonce *Zkrátit na*.

V sekci *Typ zápisu* je k dispozici volba formy zápisu Log souboru z hlediska podrobnosti zápisu, k dispozici *Zjednodušený*, *Podrobný* a *Debug*. Jako výchozí hodnota je přednastavena *Podrobný*, který plně vyhovuje standardnímu výpisu funkcí programu IW FTP a vystačuje svým výpisem administrátorům programu IW FTP.

Nevyhovují-li vám barvy okna Log souboru, máte možnost nadefinovat svůj vlastní barevný vzhled okna Log souboru v sekci *Barvy* u položek jako je písmo, podklad a čas zápisu události.

Písmo - možnost změny fontu písma v Log okně.

Ve spodní části okna vlastností Log souboru jsou k dispozici informace o umístění a velikosti Log souboru.

• **Nápověda**

Nabídka *Nápověda* slouží k vyvolání kontextové nápovědy (popis a vysvětlení pojmů k Vámi vybranému místu programu) a k získání informací o programu IW FTP.

Obsah - příkaz, který Vám zobrazí Nápovědu na své úvodní stránce.

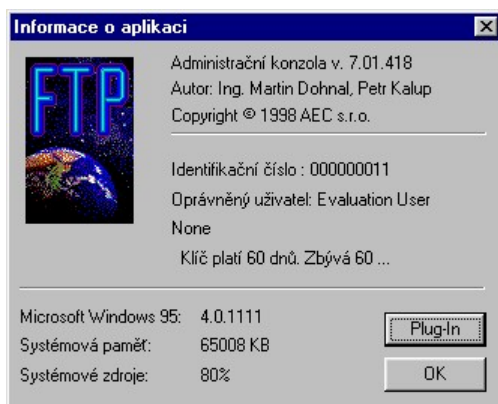
Jak používat nápovědu- po stisknutí této nabídky se zobrazí okno sloužící k seznámení se s používáním Nápovědy.

Tipy pro práci s programem - po stisknutí této nabídky se zobrazí okno, kde je zobrazen tip dne, který informuje uživatele o možnostech systému IW FTP. Další tip zobrazíte kliknutím na tlačítko „*Další tip*“.

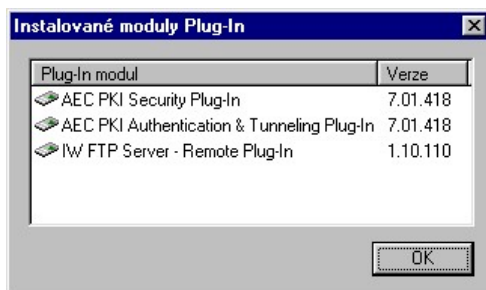
Aktuální informace z WWW - podmenu obsahující nabídku *On-line podpora* a *WWW Server AEC*. Dovíte se aktuální informace o současných produktech firmy AEC spol. s r.o.. Podívejte se na naše WWW stránky a věříme, že na nich najdete informace a data právě pro vás.

Technická podpora - EMail - kliknutím spustíte svého předvoleného poštovního klienta. Automaticky vepsaná e-mail adresa Vám umožní se okamžitě dotázat na vše, co se týká programu IW FTP. Než nám napíšete, prostudujte prosím velmi pečlivě tuto nápovědu.

O *aplikaci* - po kliknutí se otevře okno, které Vás bude informovat kromě informací o systému také o verzi programu IW FTP, o autorech, o identifikačním čísle, o Vás jako o oprávněném uživateli produktu IW FTP, o nainstalovaných zásuvných modulech (poklepáním na tlačítko *Plug-in* máte možnost zjistit verze zásuvných modulů),



Obr. 21. IW Administrační konzola - informace o aplikaci



Obr. 22. IW Administrační konzola - informace o instalovaných zásuvných modulech



Je nutné znát identifikační číslo programu IW FTP a jednotlivé verze zásuvných modulů (plug-in) při kontaktování

firmy AEC spol. s r.o. se servisními požadavky ohledně tohoto programu.

- **Nastavení serveru (levé okno)**

- **Virtuální servery**

Virtuální servery jsou u IW FTP Serveru dvojího druhu. Každá instalace obsahuje jeden administrační server pro vzdálenou správu pomocí Administrační konzoly a libovolný počet virtuálních FTP serverů (toto množství je limitováno pouze hardwarovými nároky). Administrační server může být jen jeden a nemůže být odstraněn.

Každý virtuální FTP server je vždy jednoznačně určen dvojicí - *IP adresa* a *TCP Port*. Pokud zadáte IP adresu jako 0.0.0.0 znamená to, že pro daný virtuální FTP server budou použity všechny dostupné IP adresy na daném počítači (například pokud má počítač 3 síťové karty, bude daný FTP server přístupný přes všechny 3 IP adresy)



Nelze kombinovat IP 0.0.0.0 pro jeden virtuální FTP server s dalšími IP adresami pro další virtuální FTP servery! Pokud požadujete spustit více virtuálních FTP serverů musí každý obsahovat konkrétní IP adresu, případně mohou mít tyto servery i stejnou IP adresu, musí se však lišit číslem portu.

K virtuálním serverům se vážou následující příkazy dostupné, jak z panelu nástrojů, tak na po kliknutí pravým tlačítkem myši na příslušných virtuálních serverech:

Přidat virtuální server - vybráním této položky umožníte přidat další virtuální FTP server. Podrobný popis nastavení nového nebo již používaného virtuálního FTP serveru naleznete zde.

Vymazat virtuální server - pokud kliknete, dojde k vymazání vybraného virtuálního FTP serveru

Start - kliknutím spustíte vybraný virtuální FTP server.

Stop - kliknutím zastavíte vybraný virtuální FTP server.

Pauza - kliknutím pozastavíte přihlašování nových uživatelů na vybraný virtuální FTP server. Již přihlášení uživatelé zůstanou přihlášení i nadále.

Nastavení virtuálních FTP serverů

FTP Root - cesta ke složce, která slouží jako výchozí FTP root pro daný virtuální FTP server.

IP Adresa - obsahuje konkrétní IP adresu síťového rozhraní, případně univerzální IP adresu 0.0.0.0 pro provoz na všech dostupných IP adresách.

Port - číslo TCP portu pro daný virtuální FTP server (implicitně 21). Toto číslo portu musí být shodné s číslem TCP portu v nastavení FTP klienta u koncového uživatele.

Popis - libovolný text, popis virtuálního FTP serveru.

Standardní přístupová práva - tyto přístupová práva platí implicitně pro všechny uživatele daného virtuálního FTP serveru. Tyto práva platí pro FTP root a všechny jeho podsložky.

Tyto standardní přístupová práva mají nižší prioritu než přístupová práva definovaná pro konkrétního uživatele a jeho virtuální složky!

Standardní přístupová práva mají ovšem vyšší prioritu než případná přístupová práva definovaná na NTFS partition.



U přístupových práv se nejdříve kontrolují práva jednotlivých uživatelů k jejich virtuálním složkám, poté se kontrolují standardní přístupová práva pro daný virtuální FTP server a nakonec práva na NTFS partition.

Standardní práva pro soubory:

R: čtení - právo otevřít soubor pro čtení

W: zápis - právo otevřít soubor pro zápis

D: výmaz - právo vymazat soubor

E: spuštění - právo spustit soubor

H: zobrazit „hidden“ - právo zobrazit soubor s atributem hidden (skrytý)

Standardní práva pro složky:

L: výpis složky - právo zobrazit seznam souborů ve složce

C: vytvoření složky - právo vytvořit novou složku

X: výmaz složky - právo vymazat složku

Maximální počet současných připojení - maximální počet uživatelů, kteří mohou být současně připojeni na daný virtuální FTP server

Maximální počet anonymních připojení - maximální počet anonymních uživatelů, kteří mohou být současně připojeni na daný virtuální FTP server.



Nezapomeňte, že maximální počet současně připojených uživatelů na všechny virtuální FTP servery lze nastavit v Hlavním nastavení a má větší prioritu než nastavení maximálního počtu současně připojených uživatelů na jednotlivých virtuálních FTP serverech! Dále je také možno nastavit maximální počet současně připojených uživatelů na dané uživatelské konto viz. Nastavení uživatelů.

Povolit anonymní uživatele - zatržením této položky povolíte přístup k virtuálnímu FTP serveru na uživatelská konta, která mají zatrženou volbu Anonymní uživatel viz Nastavení uživatelů (tyto konta nevyžadují zadávání hesla)

Povolit pouze anonymní uživatele - zatržením této položky povolíte přístup k virtuálnímu FTP serveru pouze na uživatelská konta, která mají zatrženou volbu Anonymní uživatel.

- **Hlavní nastavení**

V okně *Hlavní nastavení* uživatel IW FTP Serveru specifikuje vlastnosti všech vytvořených virtuálních FTP serverů.

Obr. 23. IW Administrační konzola - okno Hlavní nastavení

Sekce FTP server

Maximální počet současných připojení - maximální počet uživatelů, kteří mohou být současně připojeni na všechny virtuální FTP servery.

Čas pro vypršení FTP příkazu - doba v sekundách, po kterou zůstane uživatel připojen k FTP serveru, jestliže nepošle žádný FTP příkaz nebo nepřenášejí žádná data.

Složka pro default FTP root - cesta ke složce, která slouží jako default FTP root pro všechny virtuální FTP servery. Větší prioritu má ovšem nastavení na konkrétním virtuálním FTP serveru a nejvyšší prioritu případně nastavení FTP rootu u virtuální složky uživatelského konta.

Sekce Hlášení při vstupu do složky

Odeslat obsah souboru při vstupu do složky - zatrhnutím této volby umožníte zobrazování obsahu Vámi definovaného textového souboru na FTP konzole koncového uživatele při vstupu do dané složky.

Jméno souboru - jméno textového souboru, který se zobrazí na FTP konzole koncového uživatele při vstupu do dané složky. Doporučujeme tomuto souboru nastavit atribut hidden (skrýt).

Sekce Přihlašování

Odpojit uživatele po X chybných pokusech - tato volba umožňuje odpojit uživatele v procesu přihlašování pokud zadá *N* krát po sobě chybné heslo.

Maximální doba pro přihlášení X sekund - tato položka určuje dobu v sekundách, v rámci které se musí uživatel korektně přihlásit. Po uplynutí této doby bude uživatel odpojen z procesu přihlašování na FTP server.

Sekce Vyrovnávací paměť pro FTP pakety

Velikost bloku pro příjem - velikost vyrovnávacího bufferu pro příjem dat (implicitně 4096 bytů).

Velikost bloku pro odeslání - velikost vyrovnávacího bufferu pro odesílání dat (implicitně 4096 bytů).

Minimální volné místo před příjmem souboru [MB] - Tato položka umožňuje nastavit minimální množství volného místa na disku v MB, které je nutné pro poslání dat na FTP server. Pokud toto místo není k dispozici, bude zaslání dat od klienta FTP serverem odmítnuto.

Task Priority - v této položce je možno vybrat prioritu pro jednotlivé thready FTP serveru. Implicitně je nastavena priorita Normal. Pro běžný provoz doporučujeme tuto položku neměnit.

Download z CD-ROM disku - tato sekce umožňuje nastavit speciální možnost kopírování dat z pomalých CD-ROM disků do rychlé vyrovnávací paměti na disku.

Disková jednotka CD-ROM - písmeno CD-ROM disku následované dvojtečkou a zpětným lomítkem.

Kopírovat soubory před odesláním do složky - cesta ke složce na disku, která slouží jako vyrovnávací buffer pro data.

• Ovládací panel

Okno *Ovládací panel* slouží k přehledu připojených uživatelů na všech nebo na jednotlivých virtuálních FTP serverech, k odpojování uživatelů nebo monitorování jejich činnosti.

Virtuální server - filtr pro výběr zobrazení uživatelů z konkrétního virtuálního FTP serveru.

Odpojit uživatele - odpojení vybraného uživatele.

Odpojit všechny - odpojení všech uživatelů.

Obnovit - opětovné načtení aktuálního stavu připojených uživatelů.

Monitor příkazů uživatele - zobrazí okno pro monitorování příkazů uživatele. Pokud je tato volba nevysvícena, tak tato verze administračního plug-inu monitorování uživatelů nepodporuje.

- **Systémové informace serveru**

Okno *Systémové informace serveru* informuje o aktuálním stavu IW FTP serveru, počtech připojených uživatelů, statistikách, atd.

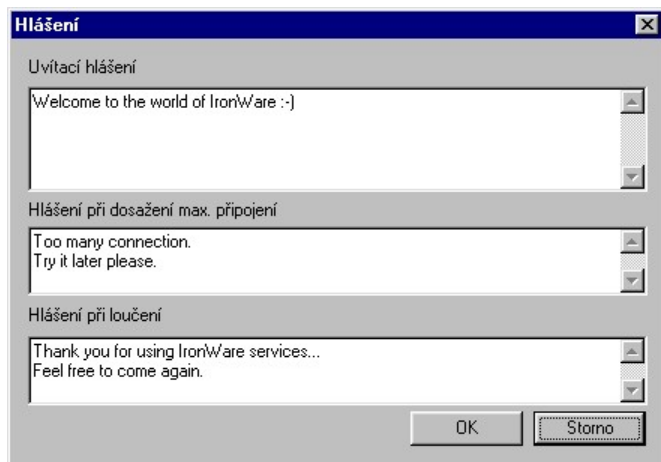
Většinu těchto veličin lze také monitorovat pomocí Windows NT Performance Monitoru!

Obnovit- znovunačtení aktuálních informací

- **Zabezpečení**

Záložka *Zabezpečení* slouží k nastavení soukromého klíče IW FTP serveru. Tento klíč bude použit k bezpečné autentizaci administrátora při připojení k spravované aplikaci, případně k vybudování šifrovaného tunelu pro uživatele serveru.

- **Hlášení**



Obr. 24. IW Administrační konzola - hlášení

Okno *Hlášení* slouží k nadefinování potřebných hlášení pro FTP klienta.

Uvítací hlášení - toto hlášení se zobrazí klientovi po přihlášení na FTP server

Hlášení při dosažení max. připojení - toto hlášení se zobrazí klientovi při překročení maximálního počtu připojení na FTP server.

Hlášení při loučení - toto hlášení se zobrazí klientovi při odpojení od FTP serveru.

• **Nastavení uživatelů**

K uživatelským účtům se vážou následující příkazy dostupné, jak z panelu nástrojů, tak na po kliknutí pravým tlačítkem myši na stromu Administrační konzoly programu IW FTP Server:

Přidat uživatele - vybráním této položky umožníte přidat další uživatelský účet IW FTP Serveru. Podrobný popis nastavení nového nebo již používaného uživatelského účtu naleznete zde.

Vymazat uživatele - pokud kliknete, dojde k vymazání vybraného uživatelského účtu.

Kopírovat uživatele - kliknutím na tuto volbu dojde k vytvoření kopie u vybraného uživatelského účtu včetně všech jeho nastavení, stačí jen zadat jméno nového uživatelského účtu.

Přejmenovat uživatele - kliknutím jste vyzváni k přejmenování vybraného uživatelského účtu.

Nastavení uživatele

slouží k nadefinování parametrů uživatelského účtu.

Nastavení uživatele

Účet uživatele: Administrator

Heslo: *****

ID Certifikátu: [všechny možnosti]

Plné jméno: Zabudovaný účet správce

Správce FTP serveru K přihlášení použít NT účet
 Anonymní uživatel Použít NTFS práva pro NT účet
 Účet vyžaduje autentifikaci Vyžadovat šifrované heslo (S/Key)
 Účet je uzamčen Kontrolovat DNS

Nastavení složek uživatele Max. souběžných připojení: 1

Složka	Alias	Přístup

Nastavení IP adres uživatele

--

Platí do: 21. 4 .1998

OK Storno

Obr. 25. IW Administrační konzola – nastavení uživatelského účtu administrátora

Nastavení uživatele

Účet uživatele: 

Heslo:

ID Certifikátu:

Plné jméno

Správce FTP serveru K přihlášení použít NT účet

Anonymní uživatel Použít NTFS práva pro NT účet

Účet vyžaduje autentifikaci Vyžadovat šifrované heslo (S/Key)

Účet je uzamčen Kontrolovat DNS

Nastavení složek uživatele Max. souběžných připojení:

Složka	Alias	Přístup	Přidat
			Opravit
			Vymazat

Nastavení IP adres uživatele

Platí do:

Obr. 26. IW Administrační konzola - nastavení uživatelského účtu anonymního uživatele

Obr. 27. IW Administrační konzola - nastavení anonymních uživatelských účtů

Účet uživatele - název pro přihlašovací účet uživatele

Heslo - heslo pro přihlášení uživatele. Pokud je zatržena volba Anonymní uživatel není toto heslo vyžadováno. Místo hesla je nutno zadat e-mail adresu.

ID Certifikátu - certifikát uživatele, který bude použit pro bezpečnou autentizaci.

Plné jméno - libovolný text upřesňující daného uživatele.

Zatržením u následujících položek se nastaví požadované vlastnosti uživatele:

Správce FTP serveru - je-li zatržena tato volba bude daný účet uživatele umožňovat správu FTP serveru pomocí Administrační konzoly.

Anonymní uživatel - je-li zatržena tato volba nebude vyžadováno heslo uživatele k tomuto účtu. Místo hesla je nutno zadat e-mail adresu.

Účet vyžadující autentifikaci - je-li zatrhnuta tato volba účet umožňuje přihlášení pouze uživatelům používající software podporující bezpečnou autentizaci, kteří mají správně zadané klíče a příslušná nastavení viz. Bezpečná autentizace.

Účet je uzamčen - je-li zatrhnuta tato volba nelze se na tento účet přihlásit.

K přihlášení použít NT účet - je-li zatrhnuta tato volba bude k přihlášení uživatele použit vybraný NT účet včetně všech jeho nastavení a příslušného hesla (lze například využít časové omezení NT účtu, přihlašování v povolených hodinách, atd.).

Použit NTFS práva pro NT účet - je-li zatrhnuta tato volba je nutno také použít volbu K přihlášení použít NT účet! Jestliže použijeme NTFS práva pro přístup k souborům a složkám je nutné mít na zřeteli, že se nejdříve kontrolují přístupová práva k virtuálním složkám, poté standardní přístupová práva pro virtuální FTP server a nakonec NTFS práva.

Vyžadovat šifrované heslo (S/Key) - je-li zatrhnuta tato volba bude vyžadováno po klientovi při každém přihlášení heslo vygenerované algoritmem S/Key. Pokud je tato volba nevysvícena, tak stávající verze tuto volbu nepodporuje.

Kontrolovat DNS - je-li zatrhnuta tato volba, bude kontrolován pro IP adresu přihlašujícího se uživatele platný zápis v reverzní DNS doméně.

Max. souběžných připojení - maximální počet souběžně připojených uživatelů na tento uživatelský účet.

Sekce Nastavení složek uživatele

Přidat - umožní přidat/nastavit virtuální složku pro daného uživatele.

Upravit - umožní nastavit/opravit parametry pro virtuální složky.

Vymazat - umožní vymazat virtuální složku.

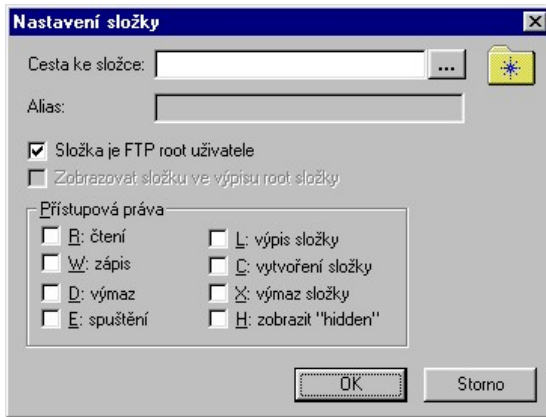
Nastavení IP adresy účtu uživatele

Přidat - umožní přidat/nastavit IP adresy ze kterých má daný uživatel povoleno/zakázáno přihlášení k danému účtu.

Upravit - umožní nastavit/opravit příslušné IP adresy.

Vymazat - umožní vymazat zvolené IP adresy.

Platí do - tato položka určuje dobu platnosti uživatelského účtu. Pokud je tato volba aktivní a vyprší doba platnosti, nebude umožněno další přihlašování na tento účet.



Obr. 28. IW Administrační konzola - nastavení virtuální složky účtu uživatele

Cesta ke složce - zde je nutno zadat absolutní cestu k dané složce ve tvaru DISK:\CESTA (např. D:\Data\Test]

Alias - zde zadáte název virtuální složky ve tvaru /ALIAS (např. /Data)

Složka je FTP Root uživatele - je-li tato volba zatrhnuta, bude příslušná virtuální složka FTP rootem uživatele.

Zobrazovat složku ve výpisu složky - je-li tato volba zatrhnuta bude virtuální složka přimapována na FTP root uživatele a tomuto uživateli bude zobrazována. Pokud tato volba zatrhnuta není, uživatel složku nevidí a musí o její existenci vědět (Může zvýšit stupeň bezpečnosti).

Souborová přístupová práva:

R: čtení - právo otevřít soubor pro čtení

W: zápis - právo otevřít soubor pro zápis

D: výmaz - právo vymazat soubor

E: spuštění - právo spustit soubor

H: zobrazit 'hidden' - právo zobrazit soubor s atributem hidden (skrytý)

Standardní práva pro složky:

L: výpis složky - právo zobrazit seznam souborů ve složce

C: vytvoření složky - právo vytvořit novou složku

X: výmaz složky - právo vymazat složku



U přístupových práv se nejdříve kontrolují práva jednotlivých uživatelů k jejich virtuálním složkám, poté se kontrolují standardní přístupová práva pro daný virtuální FTP server a nakonec práva na NTFS partition.

Nastavení IP adres uživatele



Obr. 29. IW Administrační konzola - přidání adresy účtu uživatele

IP adresa - položka pro zadání IP adresy. Je možno použít i masku pro hromadný přístup z více IP adres.

Např. 192.0.2.* znamená 255 adres ze sítě 192.0.2.0

V sekci *Přístup z IP adresy* je možno povolit/zakázat přístup z dané IP adresy nebo množiny adres.

Provoz serveru jako NT služba nebo NT aplikace

IW FTP Server lze provozovat jako běžný 32-bitový program nebo jako systémovou službu Windows NT.

Spouštění IW FTP Serveru jako NT služba je výhodnější z hlediska automatického spuštění FTP serveru ihned po nastartování systému ještě před nalogováním jakéhokoliv uživatele.

Při spouštění IW FTP Serveru je nutné nejdříve zkontrolovat, jestli neběží na daném počítači již nějaký jiný FTP server (obvykle Microsoft IIS FTP Server). Provoz více FTP serverů na jednom počítači je možný, je však nutno pro každý FTP server nastavit jedinečnou adresaci (IP a Port).

Jestliže chcete provozovat IW FTP Server s možností přihlašování uživatele přes jeho NT účet je nutno (pouze v případě, že IW FTP Server není spuštěn jako systémová služba) nastavit speciální práva pro uživatele, který spouští aplikaci IW FTP Server. Jak nastavit tyto práva je uvedeno v následujícím odstavci pro jednotlivé operační systémy Windows:

A. Windows NT 4.0

- otevřete "User Manager"
- vyberte v menu "Policies" - "User Rights"
- v otevřeném okně zatrhněte volbu "Show Advanced Users Rights"
- v nabídce "Right" vyberte vlastnost "Act as part of operating system"
- pomocí tlačítka "Add" přidejte uživatele pod jehož účtem budete spouštět IW FTP Server
- přelogujte se, případně restartujte počítač

B. Windows 2000

- otevřete "Local Security Policy"
- vyberte složku "User Rights Assigment" v "Local Policies"
- vyberte vlastnost "Act as part of operating system"
- pomocí tlačítka "Add" přidejte uživatele pod jehož účtem budete spouštět IW FTP Server
- přelogujte se, případně restartujte počítač

• Logování

Okno nastavení vlastností Log souboru zobrazí všechny možnosti vzhledu Log Souboru.

Zatrhnutím kolonky *Povolit zápis do Log souboru* se povoluje nebo zakazuje ukládání informací o průběhu jednotlivých událostí do log souboru. Název a cestu k tomuto log souboru definujeme ve složce "Složky a soubory".

Pokud je zatrhnuta položka *Mazat Log soubor před novým spojením*, pak dojde před spuštěním jakékoliv události vymazáno Log okno.

Jestliže zatrhnete položku *Automaticky zkracovat velikost Log souboru*, pak lze definovat:

Max. velikost - velikost (v bytech) Log souboru. určující největší možnou velikost Log souboru.

Zkrátit na - v případě, že je definovaná maximální velikost překročena, je soubor automaticky redukován na velikost souboru, která je zadávána v této kolonce .

Zobr. paměť X řádků - v protokolovacím okně - Log okně (spodní část Administrační konzoly) se zobrazuje takový počet posledních řádků z Log souboru, který je definován v kolonce .

V sekci *Typ zápisu* je k dispozici volba formy zápisu Log souboru z hlediska podrobnosti zápisu, k dispozici jsou *Zjednodušený*, *Podrobný* a *Debug*. Jako výchozí hodnota je přednastavena "Podrobný", který plně vyhovuje standardnímu výpisu funkcí Administrační konzoly a vystačuje svým výpisem administrátorům systému.

Nevyhovují-li Vám barvy okna Log souboru, máte možnost nadefinovat svůj vlastní barevný vzhled okna Log souboru v sekci *Barvy* u položek jako je písmo, podklad a čas zápisu události.

Písmo - možnost změny fontu písma v Log okně.

Ve spodní části okna vlastností Log souboru jsou k dispozici informace o umístění a velikosti Log souboru.

• Použití šifrovaného tunelu a autentizace

Pro zajištění bezpečnosti při přihlašování uživatele na FTP server je možno použít autentizace pomocí certifikátu/soukromého klíče.

A. K bezpečné autentizaci uživatele pomocí certifikátu/soukromého klíče je nutno vykonat následující kroky pro nastavení klientské aplikace.



Jako klientskou aplikaci je nutno použít IW FTP Client.

A.1. Nastavení programu IW FTP Client

1. Pomocí IW KeyManageru vygenerujte soukromý klíč uživatele.
2. Vyexportujte certifikát uživatele z vygenerovaného soukromého klíče. Tento certifikát předejte administrátorovi serveru nebo pokud jste administrátor, nainportujte jej do PKI IW FTP Serveru.
3. Nainportujte do Vašeho PKI certifikát serveru, který získáte od administrátora IW FTP Serveru.
4. V menu *Akce - Připojit* - záložka *Stanice* vyberte "Certifikát serveru pro autentizaci" a „Soukromý klíč pro autentizaci“

B. K bezpečné autentizaci uživatele je nutno také vykonat následující kroky pro nastavení IW FTP Serveru:



Níže uvedené kroky musí provést administrátor IW FTP Serveru z Administrační konzoly, která je nainstalována na stejném počítači jako IW FTP Server.

1. Připojte se pomocí Administrační konzoly k IW FTP Serveru.
2. Nainportujte certifikát uživatele (tento certifikát musíte od uživatele získat).
6. Nastavte soukromý klíč serveru pro autentizaci.
7. V Nastavení uživatelů vyberte požadovaný uživatelský účet a v jeho vlastnostech zatrhněte položku "Účet vyžaduje autentizaci".
8. Do položky *ID certifikátu* zadejte název certifikátu uživatele.

• Použití šifrovaného tunelu pro administraci

Pro zvýšení bezpečnosti vzdálené administrace je možno použít autentizace pomocí veřejného/soukromého klíče a případně šifrovaného tunelu.

K bezpečné autentizaci administrátora pomocí veřejného/soukromého klíče je nutno vykonat následující kroky pro nastavení administrované aplikace:



Níže uvedené kroky je nutno provést z Administrační konzoly, která je nainstalována na stejném počítači jako spravovaná aplikace.

1. Připojit se pomocí IW Administrační konzoly k spravované aplikaci (nyní ještě bez bezpečné autentizace a šifrovaného tunelu).
2. Ve stromu správy aplikace vyberte položku *"Zabezpečení"* a zadejte soukromý klíč serveru.
3. V účtu Administrátora zadejte *"Používat autentizaci"* a zvolte v položce *ID Certifikátu* jméno certifikátu Administrátora.

K bezpečné autentizaci administrátora pomocí certifikátu/soukromého klíče je nutno vykonat následující kroky pro nastavení Administrační konzoly:

1. Stiskněte pravé tlačítko na spravované aplikaci a vyberte položku *Vlastnosti*. Po zobrazení dialogového okna *Vlastnosti* vyberte záložku *Autentizace*.
2. Nastavte soukromý klíč administrátora pro a certifikát administrovaného produktu
3. Pokud chcete používat šifrovaný tunel, zatrhněte odpovídající položku.

• Instalace IW Certificate Serveru

Instalace i odinstalace se provádí formou standardního instalačního wizardu. Je vhodné před instalací zavřít všechny aplikace, neboť instalace vyžaduje restart systému.

Minimální požadavky na systém jsou *Windows NT, Service Pack v.4 a Option Pack v.4*. Nezbytný pro instalaci a běh IW Certificate Serveru je běžící a funkční *Internet Information Server* od firmy Microsoft a *Internet Explorer v. 5*. Obě tyto komponenty jsou součástí *Option Packu v.4*.

Nejdříve instalátor znázorní průběh přípravy k instalaci. Poté se spustí vlastní instalační proces, který v prvních krocích upozorní na zákonnou ochranu produktu a vyžádá si souhlas s licenčními podmínkami. Dále je třeba zadat jméno a firmu uživatele.

Vzhledem k vyšším nárokům na hardware a software se vypíše minimální konfigurace potřebná pro běh IW Certificate Serveru.

Poté se instalátor dotáže na cílovou složku. V tomto dotazu je nastavena implicitní cesta, kam se má IW Certificate Server nainstalovat. V případě, že přednastavená cesta z nějakého důvodu nevyhovuje, je možné zadat jinou pomocí tlačítka *Procházet*.

Následuje dotaz na název položky, která po instalaci přibude v nabídce *Start/Programy*.

Po potvrzení, že všechna předchozí nastavení jsou správná, se spustí proces kopírování souborů. Instalátor znázorňuje jeho průběh a část podsystému, která je právě instalována.

Po dokončení kopírování se spustí instalační průvodce, ve kterém bude možné provést nastavení IW Certificate Serveru. Je třeba vytvořit administrátora PKI a pod jeho jménem pak speciální soukromý klíč Certifikační autority. Tento klíč má speciální název *CaKey* a nelze jej pojmenovat jinak. V průběhu instalace se také vytváří certifikát k soukromému klíči IW Certificate Serveru. Pro lepší orientaci jej doporučujeme pojmenovat *CaCert*. Certifikát může být podepsán sám sebou (Self Signed) nebo může být vytvořena žádost pro certifikační autoritu a ta poslána k certifikaci na vyšší instanci Certifikační autority. Potom bude instalovaná certifikační autorita zapojena do řetězce certifikačních autorit. V případě, že je při instalaci vyroben Self Signed certifikát, je vzniklá certifikační autorita kořenovou (Root) certifikační autoritou.

Instalační průvodce oznámí úspěšné ukončení instalace a po restartu Windows je IW Certification Server připraven k použití.

• Odinstalace IW Certificate Serveru

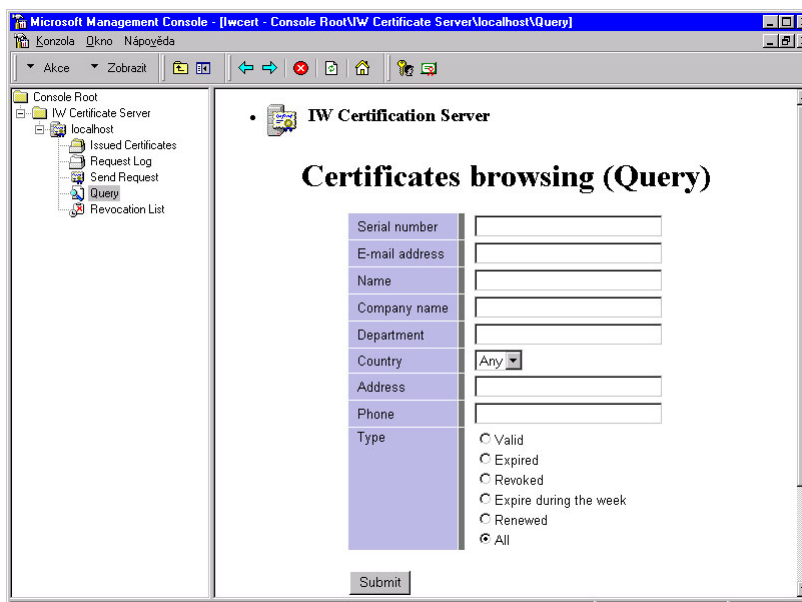
Spustí se část instalačního průvodce zajišťující odinstalaci. Vyžádá si potvrzení provedení odinstalace a spustí se odstraňování souborů. Některé z nich jsou označeny jako sdílené i pro jiné aplikace. Z tohoto důvodu je u nich vyžádáno potvrzení pro definitivní odstranění ze systému.

Při volbě *Ano všem* se instalátor ještě jednou ujistí, že volba byla provedena úmyslně, neboť smazání některých souborů by mohlo způsobit problémy jiným aplikacím.

Po odstranění všech příslušných komponent informuje o ukončení odinstalace (lze si nechat vypsát i detailní seznam všeho, co bylo odstraněno) a vyžádá si restart Windows.

• Administrační konzola Certifikačního serveru

Administrační konzola obstarává uživatelské rozhraní pro IW Certificate Server. Je realizována produktem Microsoft Management Console ve formě snap-in modulu.



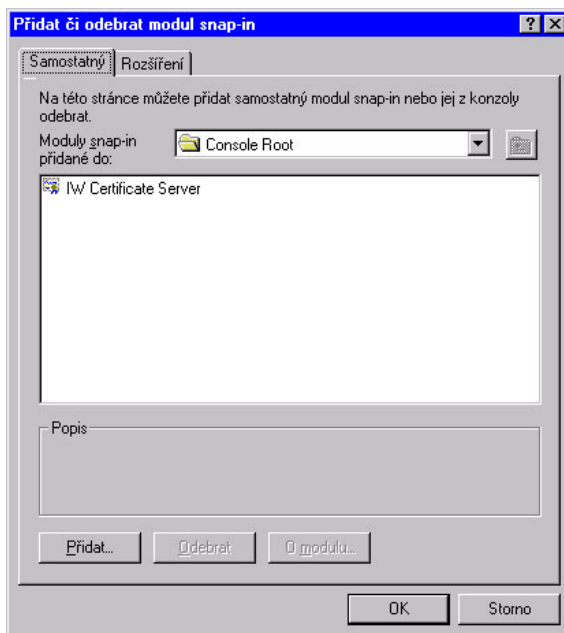
Obr.30. IW Certificate Server – Administrační konzola – dotaz na vyhledání certifikátů

V levé části okna je možné se přepínat mezi jednotlivými funkcemi Administrační konzoly:

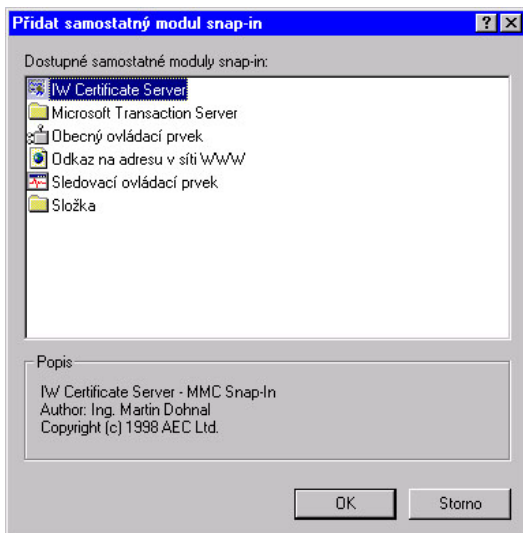
- Seznam vydaných certifikátů (*Issued Certificates*)
- Seznam žádostí o certifikát (*Request Log*)
- Vyřízení žádostí o certifikát, revokaci a obnovení (*Send Request*)
- Dotaz na vyhledání certifikátu(ů) (*Query*)
- Seznam odvolaných certifikátů a certifikátů, kterým vypršela platnost (*Revocation List*)

V pravé části okna se objevují formuláře příslušející jednotlivým položkám.

Do kořenové složky konzoly lze přidávat či odebrat další certifikační servery a některé standardní moduly Windows, a to pomocí volby *Přidat či odebrat modul snap-in...* v nabídce *Konzola*.



Obr. 31. IW Certificate Server - přidat či odebrat modul snap-in



Obr. 32. IW Certificate Server - standardní nabídka snap-in modulů

Menu obsahuje ještě standardní nabídky Windows aplikací *Okno* a *Nápověda*.

• Instalace IW LDAP Server

Instalace i odinstalace se provádí formou standardního instalačního průvodce. Je vhodné před instalací zavřít všechny aplikace, neboť instalace vyžaduje restart systému.

Instalace má několik fází. Nejdříve instalátor znázorní průběh přípravy k instalaci. Poté se spustí vlastní instalační proces, který v prvních krocích upozorní na zákonnou ochranu produktu a vyžádá si souhlas s licenčními podmínkami. Dále je třeba zadat jméno a název firmy uživatele.

Poté se instalátor dotáže na cílovou složku. V tomto dotazu je nastavena implicitní cesta, kam se má IW LDAP Server nainstalovat. V případě, že přednastavená cesta z nějakého důvodu nevyhovuje, je možné zadat jinou pomocí tlačítka „Procházet“.

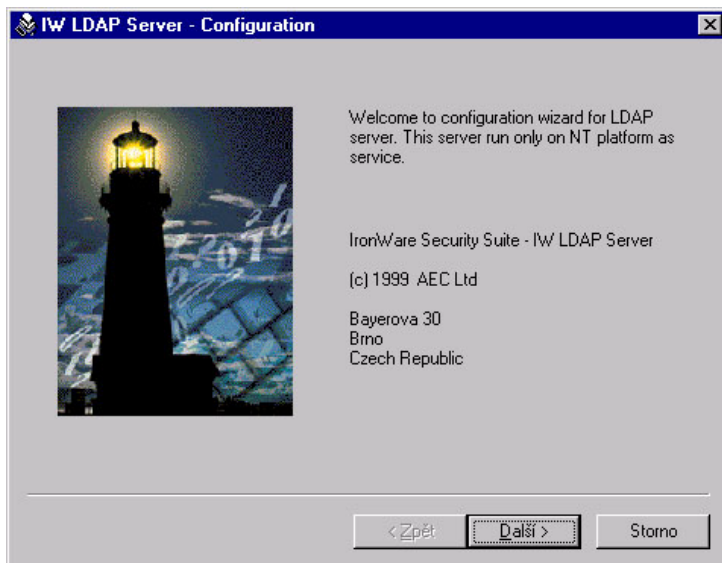
Následuje dotaz na název položky, která po instalaci přibude v nabídce *Start/Programy*.

Po potvrzení, že všechna předchozí nastavení jsou správná, se spustí proces kopírování souborů. Instalátor znázorňuje jeho průběh a část podsystému, která je právě instalována.

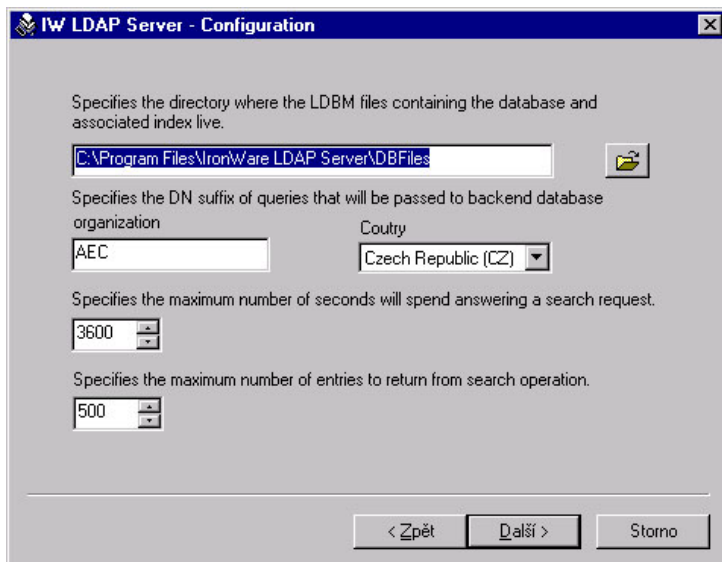
Po dokončení kopírování se spustí instalační průvodce, ve kterém bude možné provést nastavení IW LDAP Serveru.

• Konfigurace IW LDAP Serveru

Konfigurace IW LDAP Serveru se spustí pomocí zástupce *Konfigurace IronWare LDAP Server*. V průběhu instalace je konfigurace spuštěna automaticky.



Obr.33. IW LDAP Server – průvodce konfigurací



Obr. 34. IW LDAP Server - nastavení databáze

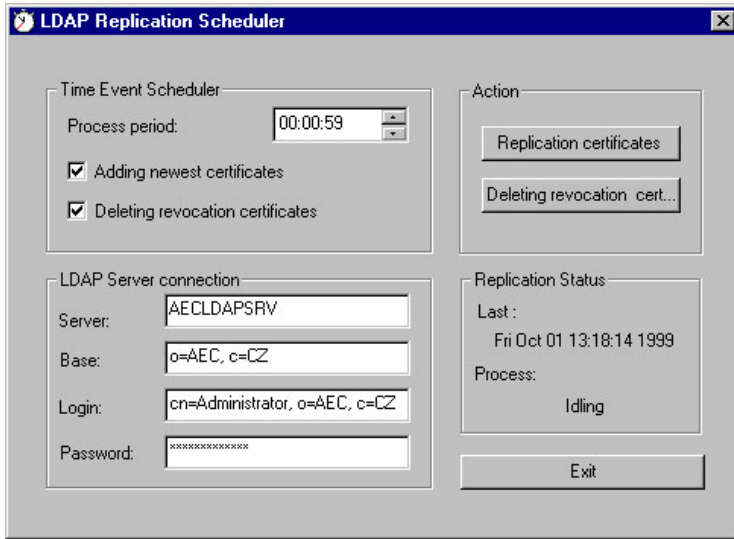
V okně pro nastavení databáze LDAP Serveru je třeba určit jméno adresáře, ve kterém budou databázové soubory uloženy, přičemž daná cesta musí existovat. Dále určit pojmenování databáze – položky *Organization* a *Country* (určuje se tzv. suffix). Je možné modifikovat nastavení maximálního časového intervalu prohledávání databáze (*Specifies the maximum number of seconds will spend answering a search result*) a maximální počet vrácených záznamů (*Specifies the maximum number of entries to return from search operation*).

Obr.35. IW LDAP Server - nastavení přístupových práv uživatelů a účtu administrátora

Posledním krokem konfigurace je nastavení omezení přístupových práv pro neautentifikovaného uživatele (*Default access*). Je nutné též provést definování uživatelského jména a hesla administrátora. Části *Organization* a *Country* je doporučeno volit shodné se jménem databáze. Po zadání hesla a jeho potvrzení je možné dokončit konfiguraci stisknutím tlačítka *Dokončit*.

Replikace databáze LDAP Serveru

Replikační plánovač v nastavených intervalech replikuje nové záznamy z Certifikační autority do přednastaveného LDAP serveru. Aby byla minimalizována náročnost replikace, provádí se vymazání neplatných certifikátů ručně.



Obr.36. IW LDAP Server - nastavení vlastností replikátoru

Spuštěním zástupce LDAP Replication Scheduler je možné nastavit či přímo provést replikaci certifikátů do databáze LDAP Serveru.

V zobrazeném okně je nutné nastavit ve skupině LDAP Server connection DNS jméno serveru nebo IP adresu – položka *Server*, jméno databáze (suffix) – položka *Base*, přihlašovací jméno (v notaci dn dle X.500) – položka *Login* a heslo přihlašovaného uživatele.

Dále se nastaví požadované akce – přidání certifikátů (Adding newest certificates), případně i vymazání odvolaných certifikátů (Deleting revoked certificates). Je možné též změnit časovou periodu provádění těchto akcí.

V okně Replication Scheduleru je možné provést stiskem tlačítka Replication certificates replikaci všech certifikátů do databáze IW LDAP Serveru, a nebo stiskem tlačítka Deleting revocation cert.. replikaci všech revokovaných certifikátů.

Stiskem tlačítka „Exit“ je možné okno uzavřít.

Jako LDAP Server lze využít jak IW LDAP Serveru, tak i kteréhokoliv jiného dodávaného LDAP Serveru.

• Technická podpora

Pokud máte dotaz k libovolnému produktu naší firmy, postupujte následovně:

Prostudujte příslušný soubor manuálu, projděte si příslušné položky nápovědy daného produktu, která je jeho součástí. Pokud zde nenajdete dostačující odpovědi, pokuste se (máte - li možnost) získat informace na elektronických systémech, například WWW stránkách naší firmy.

Pokud se vám přesto nepodaří problém vyřešit, informace o podpoře produktů můžete získat u autora aplikace (viz kontaktní adresa).

Volejte na telefonickou podporu produktu firmu AEC spol. s r.o..

AEC spol. s r.o
Bayerova 30
Brno 602 00

Tel.: ++420-(0)5-41235466
Fax : ++420-(0)5-41235038
Hot line: ++420-(0)5-41235268

Email: **support@aec.cz**
WWW: **http://www.aec.cz**
WWW: **http://www.aec-security.com**

