



Zákaz přístupu do aplikace při úpravách

ESO9 intranet a.s.
U Mlýna 2305/22, 141 Praha 4 – Záběhlice
tel.: +420 585 203 370-2
e-mail: info@eso9.cz
www.eso9.cz

Zpracoval: Havlena Stanislav
Dne: 20.5.2013

Revize: 4.7
Dne: 21.5.2013

Tento dokument popisuje, jak je možné zastavit nebo zamezit přístup do aplikace uživatelům například při provádění hromadných akcí přes T-SQL, při instalaci verze apod. Všechny níže uvedené postupy používají standardních vlastností IIS serveru.

1. Zastavení vybrané aplikace - pro všechny uživatele

Pokud se v aplikačním webu aplikace (ASP.NET 2.0 a vyšší) nachází soubor pojmenovaný **app_offline.htm**:

- ukončí se běh celé aplikace
- uvolní se všechny soubory, které by aplikace mohla používat
- uzavřou se všechna databázová spojení
- uživateli se zobrazí obsah souboru *app_offline.htm*

Můžete použít připravený soubor *_app_offline.htm* uložený ve složce instalačního DVD */AppSrv.NET/Redist*, který stačí pouze přejmenovat.

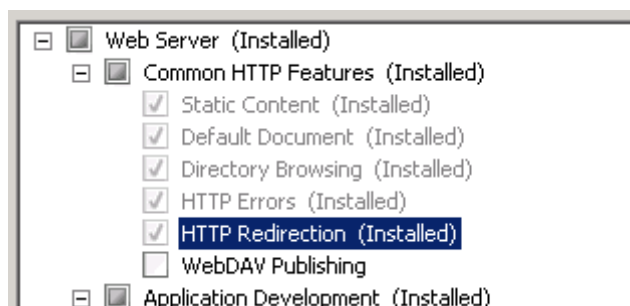
Poznámka: Velikost souboru musí být větší než 512 bajtů.

2. Přesměrování na jiný server – HTTP Redirect

Během servisního zásahu je možné všechny požadavky přesměrovat na jiný aplikační server.

Podmínka:

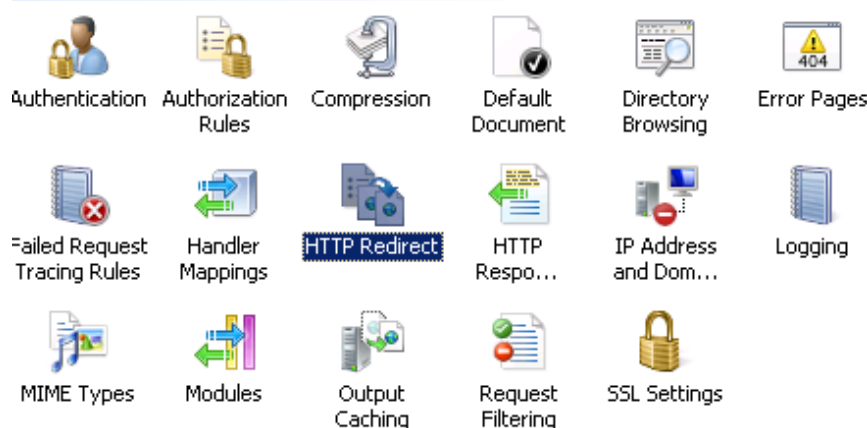
Ve vlastnostech role IIS musí být aktivována volba **HTTP Redirection** (Přesměrování protokolu HTTP)



Nastavení:

- Spusťte Internet Information Services (IIS) Manager
- Vyberte si požadovaný aplikační web
- Vyberte *HTTP Redirect* a zadejte adresu, na kterou má být dočasně aplikace přesměrována.

IIS



HTTP Redirect

Use this feature to specify rules for redirecting incoming requests to another file or URL.

☒ Redirect requests to this destination:

Example: <http://www.contoso.com/sales>

Redirect Behavior

☒ Redirect all requests to exact destination (instead of relative to destination)

☐ Only redirect requests to content in this directory (not subdirectories)

Status code:

3. Povolení přístupu k aplikaci pouze ze serveru nebo z určené IP adresy

Během servisního zásahu je možné povolit přístup k aplikaci pouze ze serveru nebo z vybrané IP adresy (např. PC správce).

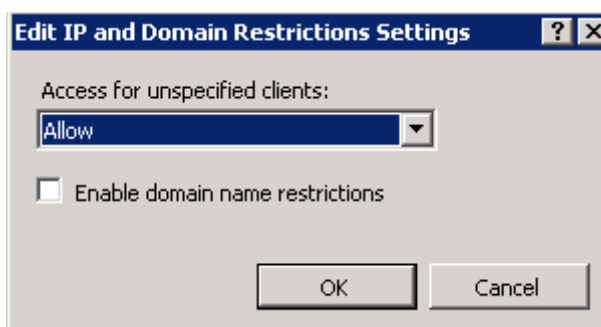
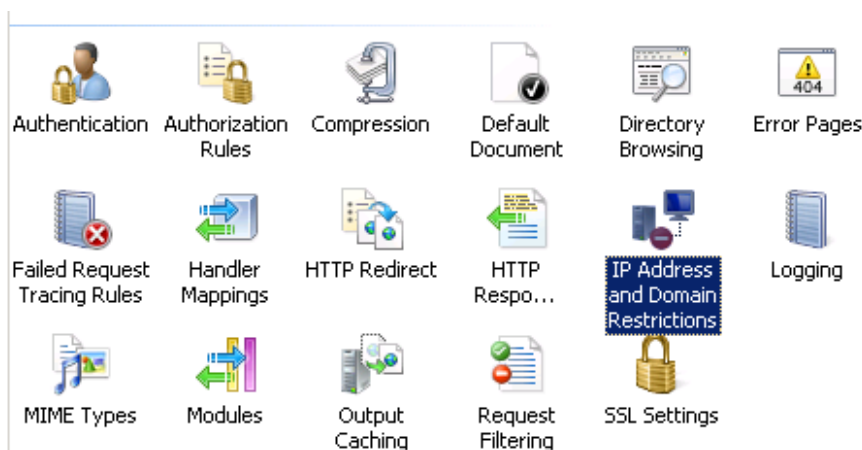
Podmínka:

Ve vlastnostech role IIS musí být aktivována volba **IP and Domain Restriction** (Zabezpečení protokolu IP)



Nastavení:

- Spustíte Internet Information Services (IIS) Manager
- Vyberte si požadovaný aplikační web
- Vyberte *IP Address and Domain Restrictions*
- Změňte v *Edit Feature Settings* přístup na *Deny* (zamezení přístupu pro neurčené klienty)
- V *Add Allow Entry* zadejte IP adresy, ze kterých bude možné k aplikaci přistupovat (127.0.0.1 je lokální adresa serveru, na kterém úpravu provádíte)
- Pro přístup do aplikace ze serveru použijte adresu ve tvaru <http://localhost/aplikace>



Use this feature to restrict or grant access to Web content based on IP addresses or d

Group by: No Grouping			
Mode	Requestor	Entry Type	
Allow	127.0.0.1	Local	

Pokud chcete nastavení použít pro všechny aplikace na serveru, postupujte stejně, jen nastavení provedte pro celý website.