

# Server

- [Windows Server 2008 - Ping aktivieren](#)
- [Bad Request \(Invalid Hostname\)](#)
- [Tomcat - SSL Certificate Keystore](#)

# Windows Server 2008 - Ping aktivieren

Ein frisch installierter Windows 2008 Server blockiert in der Standardeinstellung fast alle Verbindungen. Möglicherweise ist dies nun die erste Windowsversion, die nicht sofort durch Trojaner, Viren und sonstige Bots verseucht wird, wenn man sie in ein ungeschütztes Netz hängt. Sogar ICMP wird gnadenlos geblockt. Will man den Server also via Ping überwachen, muss dies erst freigeschaltet werden. Wie das geht zeige ich hier:

Abfrage der aktuellen Einstellungen (Admin-Konsole aka DOS-Box öffnen):

```
netsh firewall show icmpsetting
```

Um eingehende Ping-Requests (echo request) zuzulassen genügt die Eingabe des folgenden Kommandos:

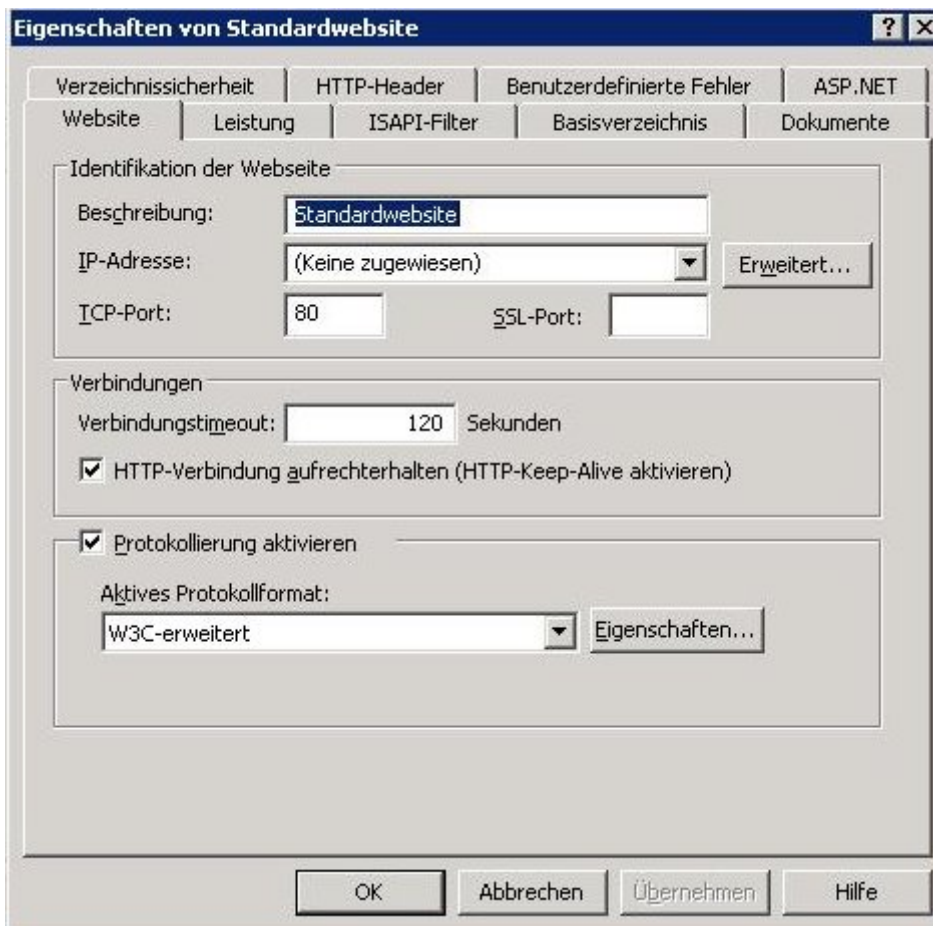
```
netsh firewall set icmpsetting 8
```

# Bad Request (Invalid Hostname)

Fehler 400 beim Windows IIS Server: Bad Request (Invalid Hostname)

Dieser Fehler trat bei einer neu installierten Instanz auf einem Windows 2003 Testserver auf. Auf beide Server konnte via Browser zugegriffen werden, statt jedoch die Standard-Webseite anzuzeigen, kam dieser Fehler.

Bei der Installation/Konfiguration wurde dem IIS eine fest IP zugewiesen, etwa 127.0.0.1 o.ä. Allen Anfragen, die nun nicht über diese IP kommen, kann der IIS nicht korrekt antworten.



Es gibt nun mehrere Möglichkeiten das Problem zu lösen:

- Umstellen auf „(Keine zugewiesen)“ in den Einstellungen der Standard-Webseite des IIS. Das funktioniert in allen Umgebungen, auch wenn der Server mehrere NICs konfiguriert hat, kann aber Probleme verursachen, wenn die Webseite nicht auf allen Interfaces verfügbar sein soll
- Zugriff auf die Webseite nicht über die IP-Adresse, sondern nur über den Computernamen bzw. DNS-Namen, z.B. `http://server-x.de`, solange eine spezifische IP für den IIS festgelegt wurde. Das kann aber immer noch fehlschlagen, wenn die Rückroute über eine andere Netzwerkkarte läuft.
- Anpassen des HOSTS-File (normalerweise „%systemroot%\system32\drivers\etc\HOSTS“), um dem Server die korrekte lokale IP-Adresse zuzuweisen. **Achtung:** dies könnte eventuell andere Dienste beeinträchtigen, die auf dem Server laufen.

# Tomcat - SSL Certificate Keystore

## SSL Zertifikat verwalten/erneuern

Diese Anleitung funktioniert mit Tomcat4 und 5. Folgendermaßen können dort die SSL-Zertifikate erneuert werden.

Das Java-SDK muss installiert sein, in dem Verzeichnis gibts das Verwaltungstool bin/keytool.exe mit dem der Keystore administriert wird.

Das **Standard-Kennwort** für den Keystore (wenn man der Tomcat-Anleitung folgt) lautet: changeit

Aliase der angelegten Zertifikate im Keystore anzeigen:

```
keytool -list -keystore c:\tomcat5\conf\mystore.keystore
```

MD5-Fingerabdruck eines Zertifikats im Keystore anzeigen:

```
keytool -list -alias myalias -keystore c:\tomcat5\conf\mystore.keystore
```

ein CSR erzeugen:

```
keytool -genreq -alias myalias -keystore c:\tomcat5\conf\mystore.keystore
```

Ein neues Zertifikat installieren (das Zertifikat muss im PKCS#7-Format bereits auf dem Server abgelegt sein):

```
keytool -import -alias myalias -trustcacerts -file c:\new-cert.cer -keystore c:\tomcat5\conf\mys
```