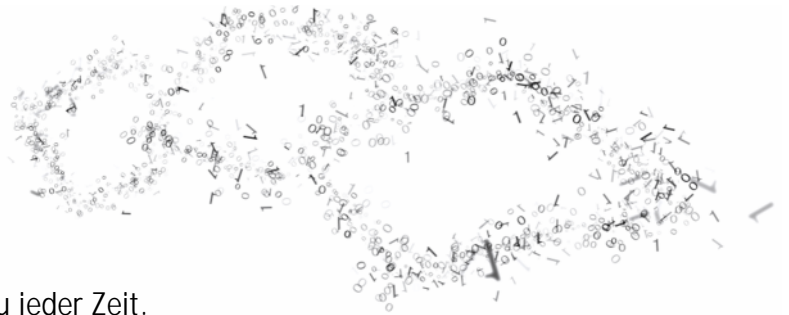




# Serverdokumentation

ab Version 3.1

**FastViewer** - die geniale Lösung,  
die verbindet - weltweit und zu jeder Zeit.





# Serverdokumentation

ab Version 3.1

Inhalt	1
Rechtliche Hinweise	2
Voraussetzungen für den Einsatz eines FastViewer Servers	3
Installation des Servers	5
Konfiguration des Servers	6
Aktivierung des Servers	7
Firewall-Konfiguration & Port-Freigabe	10
Bereitstellen der Soforteinladungsfunktion	11
Installation weiterer Server	12
Update der eigenen Serverlösung	14
Konfiguration des Autoupdate Dienstes	15
Backup der Datenbank	17
Konfiguration der Settings.ini	18
Konfiguration eines Updatepfades	24
Funktionen des Online-LogViewers	25
Server Admin	27
Erstellen von SSL Zertifikaten für Ihren WebConferenceServer	29
Erste Hilfe im Falle eines Verbindungsproblems	46
Kontakt	47

## Rechtliche Hinweise

Für Beschädigung, Verlust oder Zerstörung von Software, Daten oder Programmen die aufgrund der Verwendung von FastViewer verursacht werden, übernimmt die FastViewer GmbH keine Gewährleistung.

Die in diesem Handbuch verwendeten Soft- und Hardwarebezeichnungen sind überwiegend eingetragene Warenzeichen und unterliegen als solche den gesetzlichen Bestimmungen des Urheberrechts. Die Dokumentation, sowie Auszüge daraus, dürfen ohne ausdrückliche schriftliche Erlaubnis weder mit mechanischen oder elektronischen Mitteln, durch Fotokopieren oder auf eine andere Weise übertragen oder vervielfältigt werden. Falls in Beispielen Firmen und Daten verwendet werden, sind diese frei erfunden. Eventuelle Ähnlichkeiten sind daher rein zufällig.

Den in diesem Handbuch enthaltenen Informationen liegt der zur Drucklegung aktuelle Programmstand zugrunde. Ohne Vorankündigung können diese geändert werden und stellen keine Verpflichtung seitens des Verkäufers dar. Die Beschreibungen stellen ausdrücklich keine zugesicherte Eigenschaft im rechtlichen Sinne dar.

Bei der Erstellung dieses Handbuches ist die FastViewer GmbH mit größter Sorgfalt vorgegangen. Fehlerfreiheit kann jedoch nicht garantiert werden. Für Fehler technischer oder drucktechnischer Art haftet die FastViewer GmbH nicht.

Wenn in dieser Dokumentation jeweils nur die männliche Bezeichnung verwendet wird, so erfolgt dies ausschließlich aus Gründen der Vereinfachung und die weibliche Bezeichnung ist stets mit umfasst.

Sollten Sie Korrektur- oder Verbesserungsvorschläge haben, schicken Sie uns bitte hierzu eine E-Mail.

Vielen Dank für Ihre Mühe.

Weitere Informationen über die Produkte von **FastViewer** finden Sie im Internet unter

[www.fastviewer.com](http://www.fastviewer.com)

© Copyright 2011 FastViewer GmbH

## Voraussetzungen für den Einsatz eines FastViewer Servers

### Hardwarevorschlag für eigenen FastViewer Server:

Pentium 4, größer 2GHz, 1GB RAM bis 50 parallele Sessions, 2 GB RAM bis 100 parallele Sessions.

An die Festplatte(n) werden keine speziellen Anforderungen gestellt, da durch den Server kein Festplatten I/O entsteht (außer Logfiles). Es wird eine 100 Mbit Netzwerkkarte empfohlen.

Betriebssystemvoraussetzung Server: Windows Server 2003 (32 oder 64 Bit) oder Windows Server 2008 (32 oder 64 Bit), SQL Server 2005 Express (wird mitgeliefert) oder alternativ SQL Server 2005 und weiter .net Framework 4.0 (wird mitgeliefert).

Es darf auf diesem Server kein IIS oder anderer Webserver laufen.

Die Bandbreite mit welcher der Server mit dem Internet verbunden ist, sollte ca. 15KBit mal Anzahl der maximal gleichzeitig verbundenen Master und Clients sein. Z.B.: 10 parallele Sessions sind 10 Master und 10 Clients, also 300KBit Bandbreite Up- und Download (sollte symmetrisch sein).

Idealerweise steht der Server in einer DMZ, damit er aus dem LAN und dem Internet erreichbar ist. Der Server muss über Port 80 HTTP und Port 5000 TCP erreichbar sein. Optional ist auch die Kommunikation über den Port 443 HTTPS möglich. Um HTTPS nutzen zu können wird ein SSL Zertifikat pro Server benötigt. Die Kommunikation über HTTPS steigert die Performance von FastViewer Sessions über diverse Proxy Server.

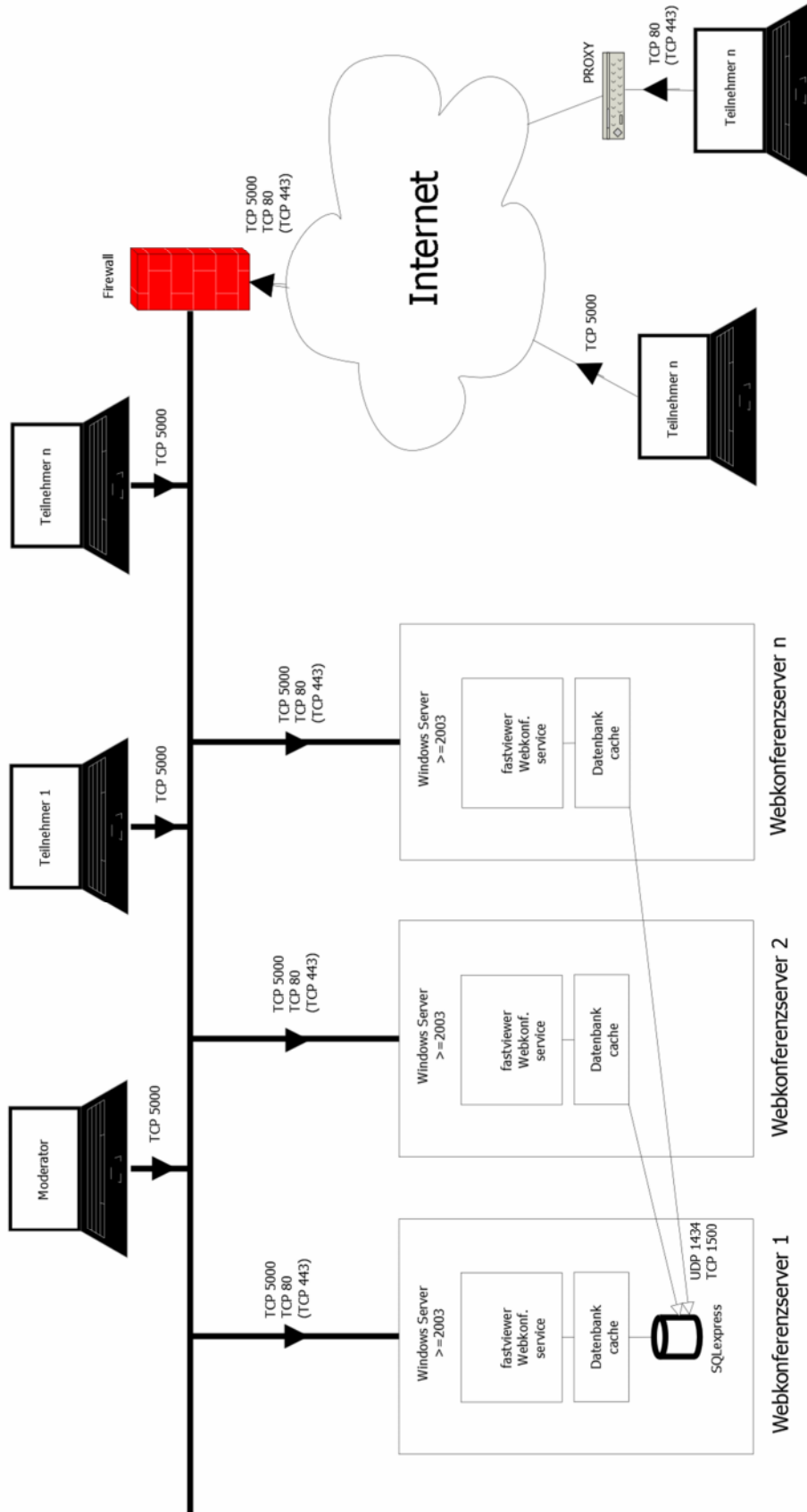
Der Server benötigt eine IP Adresse oder alternativ einen DNS Hosteintrag, welcher auf die entsprechende IP Adresse zeigt.

Es können auch mehrere FastViewer Server parallel betrieben werden somit kann man je nach Anforderung die FastViewer Serverfarm beliebig erweitern. Durch Betrieb mehrerer FastViewer Server kann eine Ausfallsicherheit und dynamische Lastverteilung gewährleistet werden.

Auf der folgenden Seite finden Sie eine Übersicht über den Aufbau einer solchen Konstellation.



## fastviewer Server Topologie



## Installation des Servers

1. Das Setup zur Installation der eigenen Serverlösung finden Sie im Downloadbereich Ihres persönlichen Kundenportals (erreichbar unter <http://portal.fastviewer.com>).

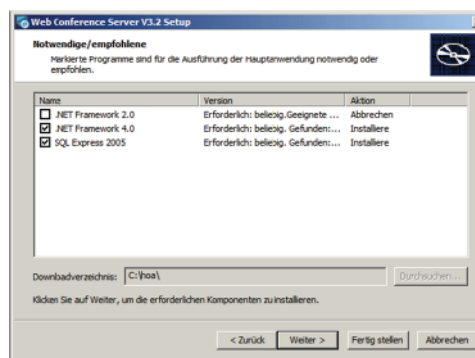
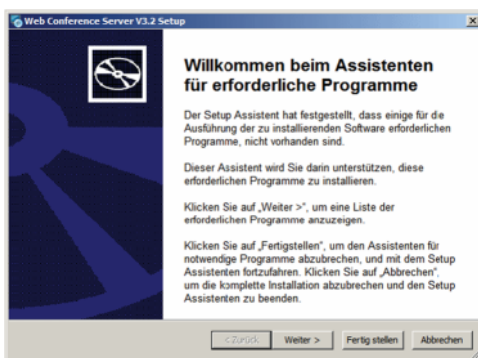
Alternativ können Sie das Setup ebenfalls über folgenden Link beziehen:

<http://portal.fastviewer.com/customerlicense/downloads/serversetupv32.zip>

Entpacken Sie im Anschluss das erhaltene ZIP File.

2. Starten Sie im angelegten Ordner die Datei „**setup.exe**“ mit einem Doppelklick.

Dieses Setupfile installiert die Datenbank (SQL express 2005), das .net-Framework 2.0 und das .net-Framework 4.0, sowie den FastViewer Serverdienst (Webconferenceserver) auf Ihrem Server.



3. Warten Sie bitte ca. 5 Minuten bis die Datenbank vom Serverdienst erzeugt wurde.

Sie können dies kontrollieren, indem Sie in Ihrem Browser am Server zu <http://localhost/admin> navigieren. Wenn die folgende Statusseite des Tunnelserverns angezeigt wird, ist die Datenbank fertig eingerichtet:



## Konfiguration des Servers

Öffnen Sie die Datei „settings.ini“ welche sich im Installationsverzeichnis der Serverlösung befindet (standardmäßig: C:\Program Files (x86)\WebConferenceServer). Bitte passen Sie hier die folgenden Einträge an:

ExternalAddress=**Change2YourServer**

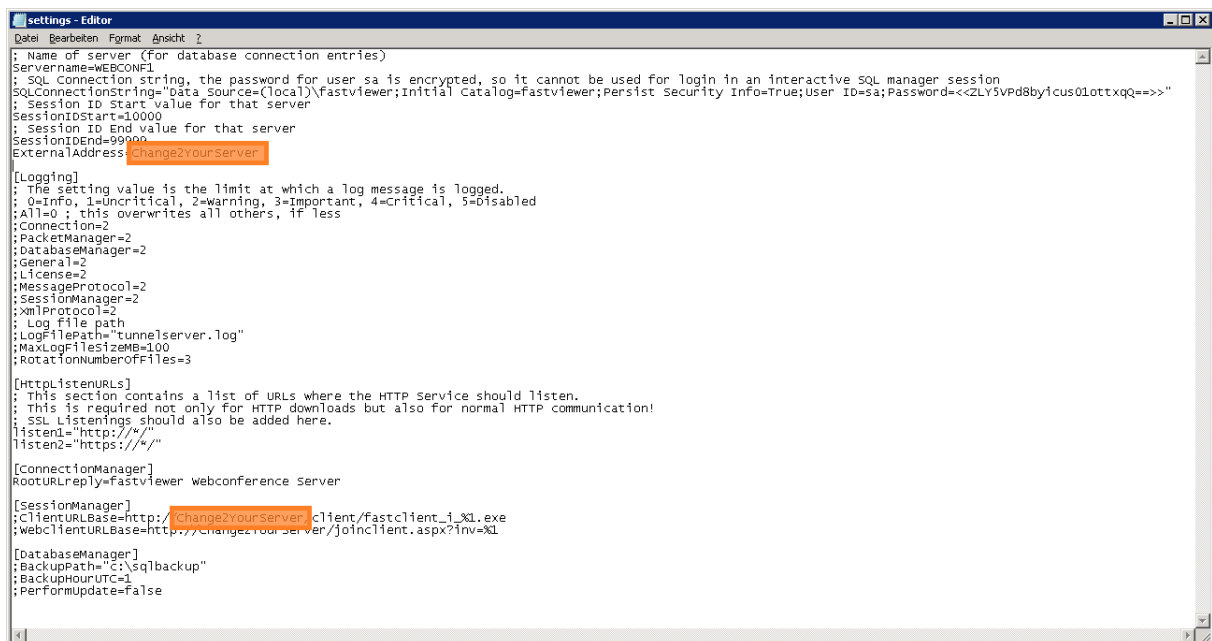
Ersetzen Sie den Wert „Change2YourServer“ durch den externen vollständig qualifizierten Domännennamen (FQDN) oder die IP-Adresse des Servers.

;ClientURLBase=http://**Change2YourServer**/client/fastclient\_i\_%1.exe

Ersetzen Sie den Wert „Change2YourServer“ durch den externen vollständig qualifizierten Domännennamen (FQDN) oder die IP-Adresse des Servers und entfernen Sie das Semikolon (;) am Anfang der Zeile.

**Hinweis:** Bitte beachten Sie, dass die Anpassung der Zeile  
„ClientURLBase=http://**Change2YourServer**/client/fastclient\_i\_%1.exe“  
lediglich erfolgen muss, wenn sich der Servername für die Einladung von der  
ExternalAddress unterscheidet.

Nach der Anpassung speichern Sie bitte die Änderungen.



```
settings - Editor
Datei Bearbeiten Format Ansicht ?
: Name of server (for database connection entries)
ServerName=WEBCONF1
: SQL Connection string, the password for user sa is encrypted, so it cannot be used for login in an interactive SQL manager session
SQLConnectionString="data source=(local)\FastViewer;Initial Catalog=FastViewer;Persist Security Info=True;User ID=sa;Password=<<2LY3Vpd8by1cus01ottxqq=>>"
: Session ID Start value for that server
SessionIDStart=10000
: Session ID End value for that server
SessionIDEnd=99999
ExternalAddress=Change2YourServer

[Logging]
: The setting value is the limit at which a log message is logged.
: 0=Info, 1=Uncritical, 2=Warning, 3=Important, 4=Critical, 5=Disabled
: All=0 ; this overwrites all others, if less
: Connection=2
: PacketManager=2
: DatabaseManager=2
: General=2
: License=2
: MessageProtocol=2
: SessionManager=2
: XmlProtocol=2
: Log file path
: LogFilePath="tunnelserver.log"
: MaxLogFileSizeMB=100
: RotationNumberOfFiles=3

[HttpListenURLs]
: This section contains a list of URLs where the HTTP service should listen.
: This is required not only for HTTP downloads but also for normal HTTP communication!
: SSL Listenings should also be added here.
listen1="http://*/"
listen2="https://*/"

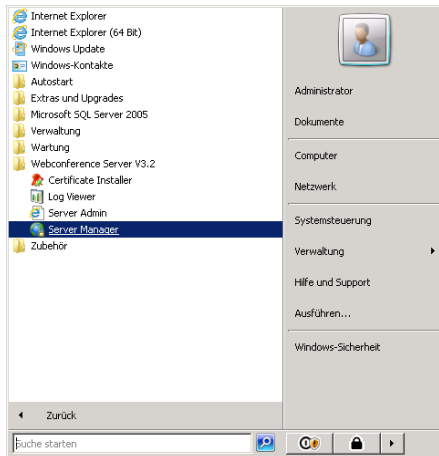
[ConnectionManager]
RootURLReply=FastViewer webconference Server

[SessionManager]
: ClientURLBase=http://Change2YourServer/client/fastclient_i_%1.exe
: WebClientURLBase=http://Change2YourServer/joinclient.aspx?inv=%1

[DatabaseManager]
: BackupPath="C:\sqlbackup"
: BackupHourUTC=1
: PerformUpdate=False
```

## Aktivierung des Servers

1. Klicken Sie auf Start > Alle Programme > Webconference Server V3 und wählen Sie in der angezeigten Liste die Option „Server Manager“ aus.



2. Klicken Sie auf „Activate Server“ um mit der Aktivierung zu beginnen.



3. Definieren Sie den Bereich der möglichen Sitzungsnummern für Ihren Server (standardmäßig 10000-99999) und tragen Sie unter „For Server“ den externen vollständig qualifizierten Domännennamen (FQDN) oder die IP-Adresse des Servers, welchen Sie bereits in der „settings.ini“ hinterlegt haben, ein.





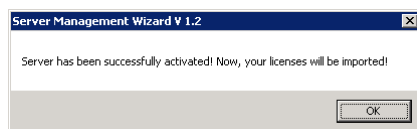
4. Geben Sie nun Ihre Lizenznummer ein.



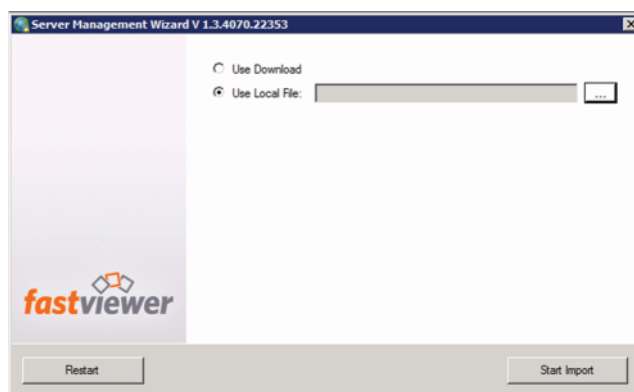
Wenn Sie über eine Internetverbindung verfügen, wird Ihre Serverlösung nach einer kurzen Wartezeit automatisch aktiviert.

Sollten Sie keine Internetverbindung, oder einen Proxy im Einsatz haben, senden Sie uns bitte eine E-Mail ([serverlicense@FastViewer.com](mailto:serverlicense@FastViewer.com)) mit dem erstellten Lizenzcode, wir schicken Ihnen umgehend den Freischaltcode per Email zu. Alternativ können Sie uns telefonisch unter +49 (0) 9181 / 509 56 28 kontaktieren.

5. Schließen Sie die Meldung über den Aktivierungsstatus Ihrer Serverlösung durch Betätigen der Schaltfläche OK.



6. Folgender Dialog öffnet sich:



Nun müssen Sie nach der erfolgreichen Aktivierung der Serverlösung die erworbenen Lizenzen importieren.

Wählen Sie eine der folgenden Optionen:

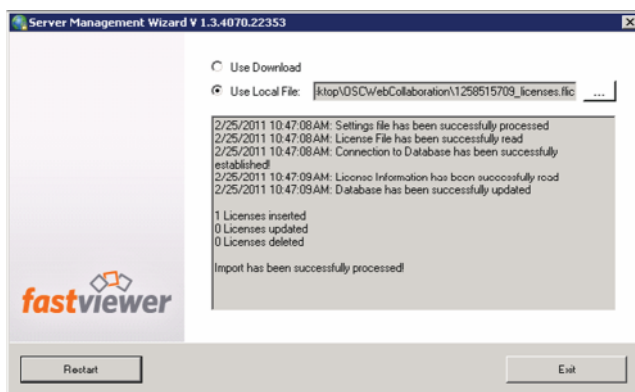
#### Use Download

Aktivieren Sie diese Option, wenn Sie über eine Internetverbindung verfügen. In diesem Fall wird die Datei mit dem Freischaltcode automatisch von dem Aktivierungsserver heruntergeladen.

#### Use Local File

Aktivieren Sie diese Option, wenn Sie über keinen Internetzugang verfügen und die Datei mit dem Freischaltcode per E-Mail zugeschickt bekommen haben. Klicken Sie anschließend auf die Suchschaltfläche ..., um den Speicherort für die Datei mit dem Freischaltcode anzugeben.

7. Betätigen Sie die Schaltfläche „Start Import“.



Klicken Sie anschließend auf die Schaltfläche „Exit“

8. Nach erfolgreicher Aktivierung starten Sie bitte den Serverdienst neu.  
Systemsteuerung – Verwaltung – Dienste – Webconferenceserver

## Firewall-Konfiguration & Port-Freigabe

1. Öffnen Sie in der Windows Firewall (sofern aktiviert) zum Server eingehend die Ports TCP 5000 und TCP 80 (+ HTTPS 443 sofern Sie HTTPS verwenden möchten).
2. Öffnen Sie in Ihrer externen Firewall eingehend zum Server die Ports TCP 5000, TCP 80 und HTTPS 443 wenn FastViewer auch von externen Personen genutzt werden soll.
3. Die Funktionalität des Servers können Sie mit folgendem Link überprüfen:  
<http://localhost/admin>, damit können Sie den Serverdienst auch zu einem späteren Zeitpunkt überwachen. Beachten Sie dass die Überwachung aus Sicherheitsgründen nur direkt am Server aufrufbar ist. Im unteren Bereich des Startschirms sehen Sie die Info „Server activated“.

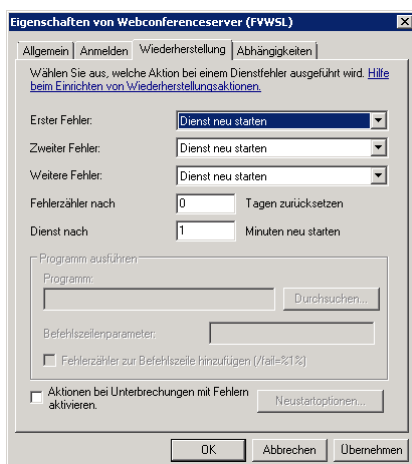
Starten Sie zum abschließenden Test auf einer Workstation in Ihrem Netz einen Webbrowser und gehen Sie zu <http://Ihrserver.Ihredomain>. Ersetzen Sie [Ihrserver.Ihredomain](http://Ihrserver.Ihredomain) mit dem DNS Namen bzw. der IP-Adresse die Sie uns für die Konfiguration des Servers genannt haben. Sie erhalten eine Website mit dem Inhalt:

### fastviewer Webconference Server

Sollte dies nicht der Fall sein, so überprüfen Sie bitte Ihre Firewall-Einstellungen.

4. Abschließend sollte in den Wiederherstellungsoptionen des Tunnelserver eine Einstellung getroffen werden, welche den Fall eines Dienstfehlers betrifft.

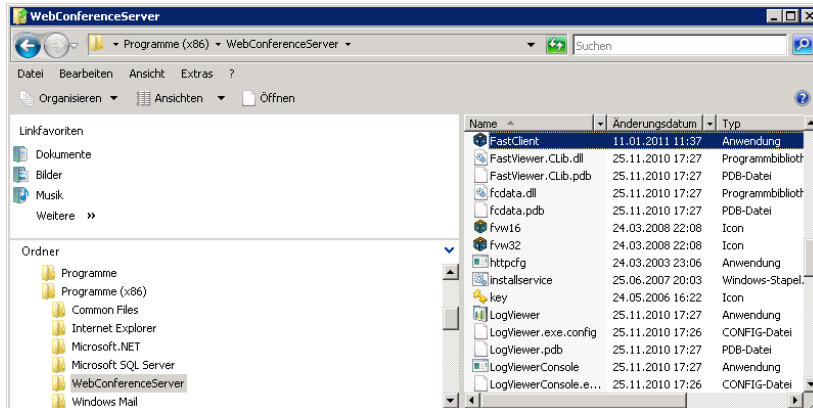
Bitte konfigurieren Sie diese Optionen wie folgt:





## Bereitstellen der Soforteinladungsfunktion

Sollten Sie die Einladungsfunktion von FastViewer nutzen wollen, so muss das Teilnehmermodul im Kundenportal heruntergeladen und im Installationsverzeichnis der eigenen Serverlösung abgelegt werden, so dass das Modul für geplante Sitzungen sowie Soforteinladungen verwendet werden kann. Hierzu laden Sie bitte die entsprechend angepasste FastClient.exe herunter und verschieben Sie diese in das jeweilige Installationsverzeichnis:



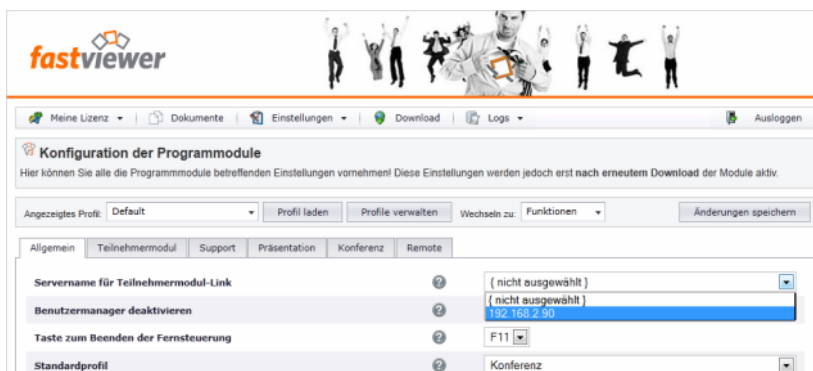
Um die Verwendung der Soforteinladungsfunktion zu ermöglichen, müssen in der "settings.ini" zunächst folgende Werte wie unten angegeben angepasst werden:

```
;ClientURLBase=http://Change2YourServer/client/fastclient_i_%1.exe
```

Ersetzen Sie den Wert „Change2YourServer“ durch den externen vollständig qualifizierten Domännennamen (FQDN) oder die IP-Adresse des Servers und entfernen Sie das Semikolon (;) am Anfang der Zeile.

**Hinweis:** Bitte beachten Sie, dass die Anpassung der Zeile „ClientURLBase=http://Change2YourServer/client/fastclient\_i\_%1.exe“ lediglich erfolgen muss, wenn sich der Servername für die Einladung von der ExternalAddress unterscheidet.

Abschließend ist der jeweilige Server im Kundenportal auszuwählen. Diese Einstellung finden Sie unter: „[Einstellungen V3/Funktionen/Allgemein/Servername für Teilnehmermodul-Link](#)“

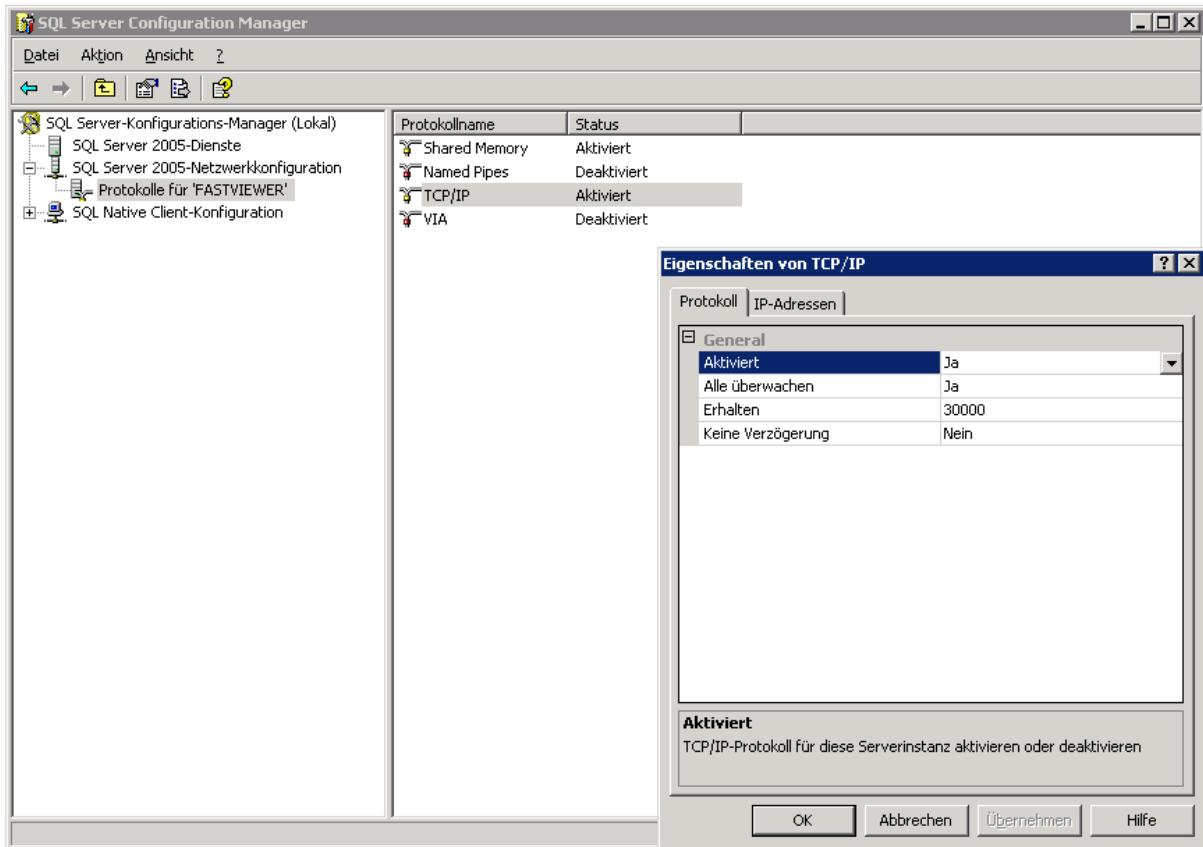


## Installation weiterer Server

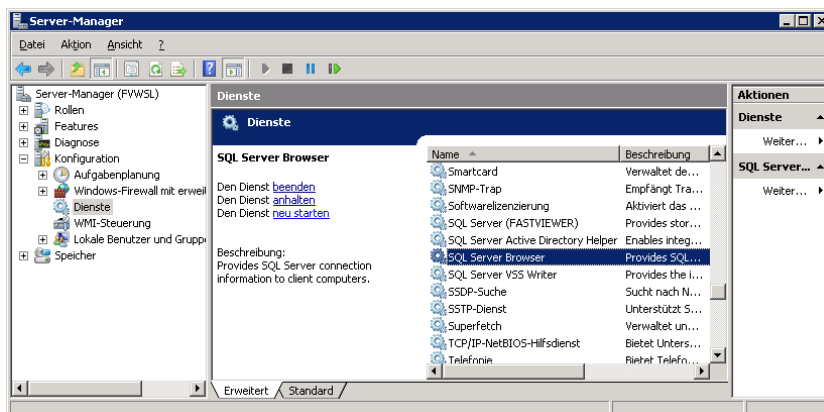
Starten Sie den SQL Server Configuration Manager über "Start/Programme/Microsoft SQL Server 2005/Konfigurationstools/SQL Server-Konfigurations-Manager"

In diesem Manager muss das TCP/IP-Protokoll für diese Serverinstanz aktiviert werden. Wie Sie in die Eigenschaften gelangen sehen Sie im unten stehenden Screenshot:

(Unter Eigenschaften von TCP/IP im Reiter „Protokoll“ den Wert „Aktiviert“ auf „Ja“)



Überprüfen Sie anschließend, ob der „SQL Server-Browser“ Dienst gestartet ist:



Folgende Werte in der Settings.ini (auf beiden Servern!) müssen angepasst werden:

**Server1:**

```
SQLConnectionString=Data Source=(local)\FastViewer;Initial Catalog=FastViewer;Persist  
Security Info=True;Integrated Security=SSPI;  
SessionIDStart=10001  
SessionIDEnd=50000  
ServerName=FASTVIEWER1
```

**Server2:**

```
SQLConnectionString=Data Source="Ihr FastViewer-Server1"\FastViewer;Initial  
Catalog=FastViewer;Persist Security Info=True;Integrated Security=SSPI;  
SessionIDStart=50001  
SessionIDEnd=95000  
ServerName=FASTVIEWER2
```

**Hinweis:** Die Bezeichnung für „ServerName“, in diesem Fall FASTVIEWER1 und FASTVIEWER2 ist frei wählbar!

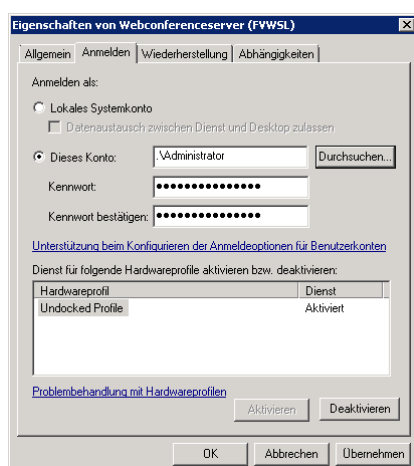
Anschließend muss der Tunneldienst auf beiden Geräten neu gestartet werden.

Bitte überprüfen Sie die Funktionsfähigkeit beider Server durch die Eingabe von <http://localhost/> im Browser des jeweiligen Servers.

Sollte der 2. Server (welcher auf die SQL-Datenbank des 1. Servers zugreift) nicht starten, so hat dieser sehr wahrscheinlich keine Verbindung zur Datenbank.

Überprüfen Sie in diesem Fall, ob beide Geräte das gleiche Administrationskennwort haben und starten Sie am 2. Server den Dienst mit folgenden Authentifizierungsdaten:

(Unter Webconferenceserver/Eigenschaften den Reiter „Anmelden“ anwählen)



## Update der eigenen Serverlösung

Bitte achten Sie beim Einsatz einer eigenen Serverlösung immer auf den Versionsstand, dieser sollte stetig aktuell sein.

Um ein Update der eigenen Serverlösung durchzuführen, müssen Sie zunächst das entsprechende Update wie folgt downloaden:

1. Das Setup zum Update der eigenen Serverlösung finden Sie im Downloadbereich Ihres persönlichen Kundenportals (erreichbar unter <http://portal.fastviewer.com>).

Alternativ können Sie das Setup ebenfalls über folgenden Link beziehen:

<http://portal.fastviewer.com/customerlicense/downloads/serverupdate32.zip>

(Unter Umständen muss vor der Installation des Updates das .NET Framework aktualisiert werden. Diese Information können Sie dem Hinweistext unterhalb des Downloadlinks in Ihrem persönlichen Portal entnehmen.)

2. Unter <http://localhost/admin> überprüfen ob derzeit FastViewer Sessions aktiv sind.

3. Wenn keine Session aktiv ist, den Webconferenceserver Dienst + SQL Server Dienst stoppen.

4. Verzeichnis sichern C:\Program Files (x86)\WebConferenceServer + SQL Datenbank (FastViewer.mdf + FastViewer\_log.ldf < Diese finden Sie im Verzeichnis C:\Program Files (x86)\Microsoft SQL Server\MSSQL.1\MSSQL\Data)

5. Kopieren Sie alle Dateien aus der „serverupdate32.zip“ in das WebConferenceServer-Verzeichnis und überschreiben Sie alle vorhandenen Dateien.

6. Nach dem Start des SQL Server Dienstes kann der Webconferenceserver Dienst gestartet werden.

7. Testsitzung

**Hinweis:** Sollten Sie mehrere Serverlösungen im Einsatz haben, so müssen sich alle Server permanent auf dem gleichen Versionsstand befinden!



## Konfiguration des Autoupdate Dienstes

Um die eigene Serverlösung automatisiert immer auf dem aktuellsten Stand zu halten, wurde ein Autoupdate Dienst integriert. Dieser ist standardmäßig deaktiviert und kann wie folgt konfiguriert werden:

1. Öffnen Sie die Datei „autoupdate.ini“ unter [C:\Program Files \(x86\)\WebConferenceServer\AutoUpdate](#)
2. Tragen Sie unter „timeFrom“ und „timeTo“ den gewünschten Zeitraum, zu welchem die eigene Serverlösung ein Update vollziehen soll, ein. Standardmäßig ist ein Zeitraum von 01:00 bis 04:00 Uhr hinterlegt.
3. Speichern Sie die „autoupdate.ini“ ab.
4. Starten Sie nun den Dienst „WebconferenceserverAutoupdate“.

Somit wird die eigene Serverlösung täglich zwischen 01:00 und 04:00 Uhr überprüfen, ob eine neuere Version zur Verfügung steht und das Update automatisch installieren.

Bitte beachten Sie, dass ein Update lediglich vorgenommen wird, wenn zum gewählten Zeitraum keine Session aktiv ist.

**Hinweis:** Um zu überprüfen, ob eine Aktualisierung zur Verfügung steht, wird die eigene Serverlösung zum festgelegten Zeitpunkt eine Verbindung zu den FastViewer Update-Servern aufbauen und ggf. über diese das Update beziehen.



### Beispiel einer autoupdate.ini Datei:

```
[Time Period]
; The Update Service will only try to Update in the specified range. Please insert the time values in
the format hh:mm (24 hours)!
timeFrom=1:00
timeTo=4:00
; The Service will check every x minutes, if there are no Users connected and the server could be
stopped!
minutesUntilRetry=5
[Server Settings]
; Enter the URL of the update Server
updateServerURL="http://portal.fastviewer.com/AutoUpdate/Update.aspx"
; Enter the URL of the destination Server
destinationServerURL="http://localhost/"
; Enter the Service Name of the TunnelServer
destinationServiceName="Webconferenceserver"
; Enter the local path to the server files. Use only if non standard.
destinationDirectory=""
[Folder Settings]
; Please enter a valid and accessible path in order to Backup the server files. Use only if non
standard.
backupDirectory=""
; Please enter a valid and accessible path in which the update source files will be saved. Use only if
non standard.
updateDirectory=""
; Use only to update from a local folder. Please enter a valid and accessible path from which the
update source files will be taken.
; updateFromPath=""
[E-Mail Settings]
; used for mailnotification in case of failure
smtpServer=""
smtpUserID=""
smtpPWD=""
smtpPORT=25
mailSender=""
mailReceiver=""
[License Settings]
; Use only to overwrite the serial for special purposes
;serial=YourSerialNumber
[Logging]
; If full logging is set to true, a detailed log will be written
fullLogging=false
```

## Backup der Datenbank

Sollten Sie eine Sicherung der Datenbank erstellen wollen, so gehen Sie bitte wie unten beschrieben vor. Hierbei gibt es zwei Möglichkeiten:

1. SQL Server Dienst stoppen, Datenbankfiles kopieren (sichern) aus SQL Server Verzeichnis\DATA (FastViewer.mdf und FastViewer\_log.ldf), SQL Server Dienst starten

*Alternativ, während der SQL-Server-Dienst aktiv ist:*

2. Konsoleneingabe: Webconferenceserververzeichnis\OSQL -S (local)\FastViewer -E, dann BACKUP DATABASE FastViewer TO DISK='SICHERUNG.BAK', anschließend initiieren Sie den Vorgang mit dem Befehl „go“.

3. Um die Konsole zu verlassen geben Sie bitte „exit“ ein und kopieren Sie das Backupfile aus dem SQL-Serververzeichnis\BACKUP



## Konfiguration der settings.ini

Im Folgenden finden Sie eine Zusammenstellung aller möglichen Einstellungen, die in der Konfigurationsdatei „settings.ini“ des WebConferenceServers vorgenommen werden können:

### Section GENERAL

Einstellung	Beschreibung	Wertangabe
SessionIDStart	Start of session PIN numbers Default = 10000	10.000 – 99.999
SessionIDEnd	End of session PIN numbers Default = 99999	10.000 – 99.999
SQLConnectionString	Database connection string No default value	String
ServerName	Internal name of the server for the connections log table entries in the database Default = TUNNEL_[hostname]	String (50)
ExternalAddress	FQDN of the Webconference server, used for download of the clients. Please change before starting the server with OpenScape=true Default = Change2YourServer	String
OpenScape	Set to true for OpenScapeUC, enables the XMLRPC interface with OpenScape licensing Default = false	Bool (true/false)
XMLRPC	Enables the XMLRPC interface with internal fastviewer licensing Default = false	Bool (true/false)
UpdateURL	Overrides the AutoupdateURL. If you use the Webconference server also for autoupdating the clients, you have to create an update folder in the webconference server folder. In this folder create a folder for every version, eg. 3.10.0012 Default = "http://update1.fastviewer.com/update"	String



## Section [HttpListenURLs]

Einstellung	Beschreibung	Wertangabe
listen1	First URL on which the server listens to HTTP requests. This is used like hostheaders in IIS. No default value	String
listen2	Second URL on which the server listens to HTTP requests. This is used like hostheaders in IIS. No default value	String

## Section [ConnectionManager]

Einstellung	Beschreibung	Wertangabe
RootURLreply	Reply message when the root URL of server is called via a browser. Default = fastviewer Server	String (100)
DirectListenIP	IP Adresse auf der Port 5000 abgehört wird. Für http(s) bitte httpcfg verwenden Default alle IPAdressen des Servers	IP Adresse

## Section [HTTPServer]

Einstellung	Beschreibung	Wertangabe
CustomizedClientDownload	Only for ASP Server version. When enabled, the server looks for customized clients in the "CustomizedClientPath" Default = false	Bool (true/false)
CustomizedClientPath	Path where the server could find the customized files. Only for ASP server version Default = \clients\	String

## Section [SessionManager]

Einstellung	Beschreibung	Wertangabe
ClientURLBase	Sets the value for the invitation link to fastclient.exe, for one click startup of the client. Use variable [clienturl] in the invitation text in the fastviewer portal. http://yourserver.com/client/fastclient_i_%1.exe - No default value	String
WebClientURLBase	Sets the value for the invitation link to the webclient. Use variable [webclienturl] in the invitation text in the fastviewer portal. Also used in XMLRPC answers - No default value	String



## Section [HttpServerPaths]

Einstellung	Beschreibung	Wertangabe
/update/	Set the value to the mapped filesystem path of each virtual directory. E.g. /update/=c:\dir1\update Use a new line for each virtual directory Default = /update/=.update	String

## Section [DatabaseManager]

Einstellung	Beschreibung	Wertangabe
BackupPath	Set the path to the folder where the backup should be stored. The backup creates one backupfile for each weekday, the files are overwritten each week. E.g. backupPath=c:\dir1\ No default value	String
BackupHourUTC	Set the hour, when the backup should start. The hour is always set in UTC. No default value	0-23
ClientLog	If set to true, each client connection data is recorded in the serverlog. It can be viewed with the logviewer tool Default = false	Bool (true/false)
PerformUpdate	Enable database schema updates on startup of service. Set to false on second server. Default = true	Bool (true/false)

## Section [DatabaseManager]

**Hinweis:** Please use only lower values for loglevels than default, when requested by support.

Einstellung	Beschreibung	Wertangabe
Connection	Set the logging value for the connection manager Default = 2	0-5
PacketManager	Set the logging level for the internal packet manager Default = 2	0-5
DatabaseManager	Set the logging level for database queries Default = 2	0-5
General	Set the logging level for general messages, like start, stop of server Default = 2	0-5
License	Set the logging level for license related functions Default = 2	0-5
MessageProtocol	Set the logging level for the internal message protocol from and to the clients Default = 2	0-5
SessionManager	Set the logging level for the session manager, which handles the complete session management of the Webconference server Default = 2	0-5
XmlProtocol	Set the logging level for the XMLRPC interface Default = 2	0-5
All	Set the logging level for all above, overwrites the above values. For debugging purpose only. No default value	0-5
LogFilePath	Full path to the logfiles, please use " at beginning and end of string Default = "tunnelserver.log"	String
MaxLogFileSizeMB	Value in MB for the maximum logfile size, before a new logfile is created Default = 100	1 - 8000
RotationNumberOfFiles	Number of logfiles to create, before oldest logfile is overwritten Default = 3	1 - 99

### Für alle Parameter gilt:

- Groß/Klein Schreibung beachten
- Parameter und Wert werden durch ein Gleichheitszeichen getrennt
- Keine Leerzeichen zwischen Parameter und Gleichheitszeichen
- Defaultwerte existieren nur sofern angegeben

### Beispiel einer settings.ini Datei:

```
; Name of server (for database connection entries)
Servername=WEBCONF1
; SQL Connection string, the password for user sa is encrypted, so it cannot be used for login in an
interactive SQL manager session
SQLConnectionString="Data Source=(local)\fastviewer;Initial Catalog=fastviewer;Persist Security
Info=True;User ID=sa;Password=<<xxxxxxxxxxxxxx==>>"
; Session ID Start value for that server
SessionIDStart=10000
; Session ID End value for that server
SessionIDEnd=99999
ExternalAddress=Change2YourServer
```

### [Logging]

```
; The setting value is the limit at which a log message is logged.
; 0=Info, 1=Uncritical, 2=Warning, 3=Important, 4=Critical, 5=Disabled
; All=0 ; this overwrites all others, if less
; Connection=2
; PacketManager=2
; DatabaseManager=2
; General=2
; License=2
; MessageProtocol=2
; SessionManager=2
; XmlProtocol=2
; Log file path
; LogFilePath="tunnelserver.log"
; MaxLogFileSizeMB=100
; RotationNumberOfFiles=3
```

### [HttpListenURLs]

```
; This section contains a list of URLs where the HTTP Service should listen.
; This is required not only for HTTP downloads but also for normal HTTP communication!
; SSL Listenings should also be added here.
listen1="http://*/"
listen2="https://*/"
```

[ConnectionManager]

RootURLreply=fastviewer Webconference Server

[SessionManager]

;ClientURLBase=http://Change2YourServer/client/fastclient\_i\_%1.exe

;WebclientURLBase=http://Change2YourServer/joinclient.aspx?inv=%1

[DatabaseManager]

;BackupPath="c:\sqlbackup"

;BackupHourUTC=1

;PerformUpdate=false

### **Erklärung:**

SQLConnectionString zeigt auf die lokale SQL Datenbank mit integrierter Windows Authentifizierung. LogVerboseLevel 10 loggt nur Informationen beim Start und schwere Fehler. Durch SSLListenOn können die Module (fww.exe und DLL) auch SSL als Transportprotokoll verwenden. Vorausgesetzt Sie haben die SSL Zertifikate installiert. Mit HttpFileServer wird der Tunnelserver auch zum Webserver und bietet in diesem Fall zwei virtuelle Webs an, nämlich /update und /kunde. Im Updatepfad wird bei jeder neuen Version ein neuer Ordner angelegt, z.B. bei Version 2.6.013 der Ordner 2.93. Der Ordnername wird von FastViewer bei jedem Update bekannt gegeben.



## Konfiguration eines Updatepfades

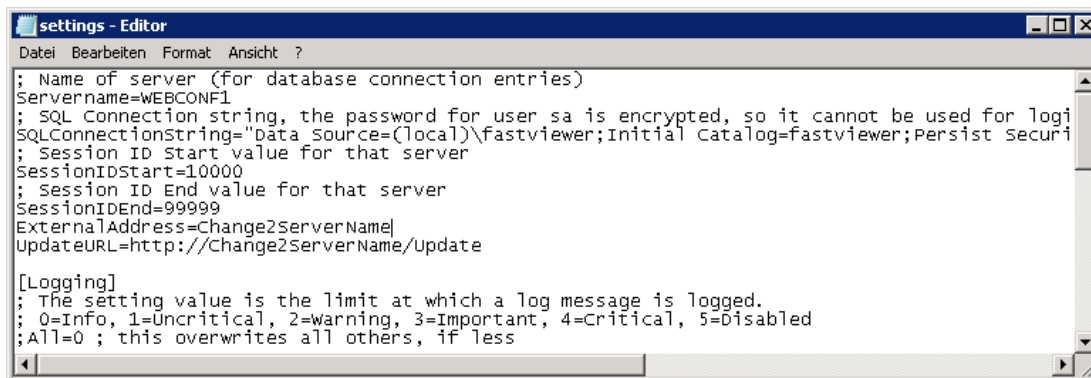
Sollten Sie Updates für die Versionsanpassung selbst bereit stellen wollen, so besteht die Möglichkeit einen eigenen Updatepfad zu hinterlegen. Somit können Updates auch ausschließlich über das interne LAN verteilt werden.

Der Pfad ist wie folgt in der „settings.ini“ einzutragen:

**UpdateURL=http://Change2ServerName/Update**

Ersetzen Sie den Wert „Change2YourServer“ durch den externen vollständig qualifizierten Domännennamen (FQDN) oder die IP-Adresse des Servers.

**Hinweis:** Ist kein Serverpfad bezüglich des Updates hinterlegt, so wird automatisch der Updatepfad der FastViewer-Server verwendet!



```
settings - Editor
Datei Bearbeiten Format Ansicht ?
; Name of server (for database connection entries)
Servername=WEBCONF1
; SQL connection string, the password for user sa is encrypted, so it cannot be used for logi
SQLConnectionString="Data Source=(local)\fastviewer;initial Catalog=fastviewer;Persist Securi
; Session ID Start value for that server
SessionIDStart=10000
; Session ID End value for that server
SessionIDEnd=99999
ExternalAddress=Change2ServerName|
UpdateURL=http://Change2ServerName/Update

[Logging]
; The setting value is the limit at which a log message is logged.
; 0=Info, 1=Uncritical, 2=warning, 3=Important, 4=Critical, 5=Disabled
; All=0 ; this overwrites all others, if less
```

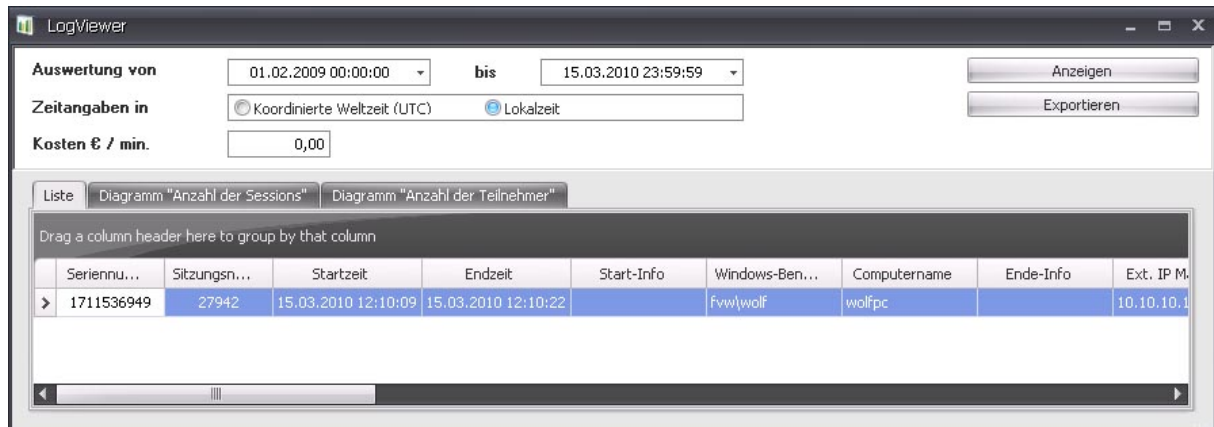
Legen Sie nun den Ordner „Update“ im Installationsverzeichnis des WebConferenceServers an. Die Module müssen immer in Unterordnern abgelegt werden. Erstellen Sie daher im Falle einer neuen Version einen entsprechenden Ordner, z.B. für die Version 3.20.0009 den Ordner mit dem Namen: 3.20.0009

In dem erstellten Pfad ist die „FastClient.exe“ (Teilnehmermodul) und die Dateien „FastREClient.exe“ und „FastRemoteUpdate.exe“ für den Remote Zugriff des FastViewer Secure Advisor (sofern verwendet) zu hinterlegen.

**ACHTUNG!** Bitte beachten Sie bei der Pfadangabe den Versionsstand!

## Funktionen des Online-LogViewers

Dieses FastViewer-Tool ermöglicht Ihnen, sich eine Gesamtübersicht über alle gehaltenen Sessions zu verschaffen. Zusätzlich bietet der OnlineLog-Viewer die Möglichkeit, diese nach diversen Kriterien zu sortieren und einen Export (in ein .csv-File) durchzuführen. Eine Selektion der Sessions, welche in einem bestimmten Zeitraum (von DATUM, bis DATUM) abgehalten wurden, ist möglich.



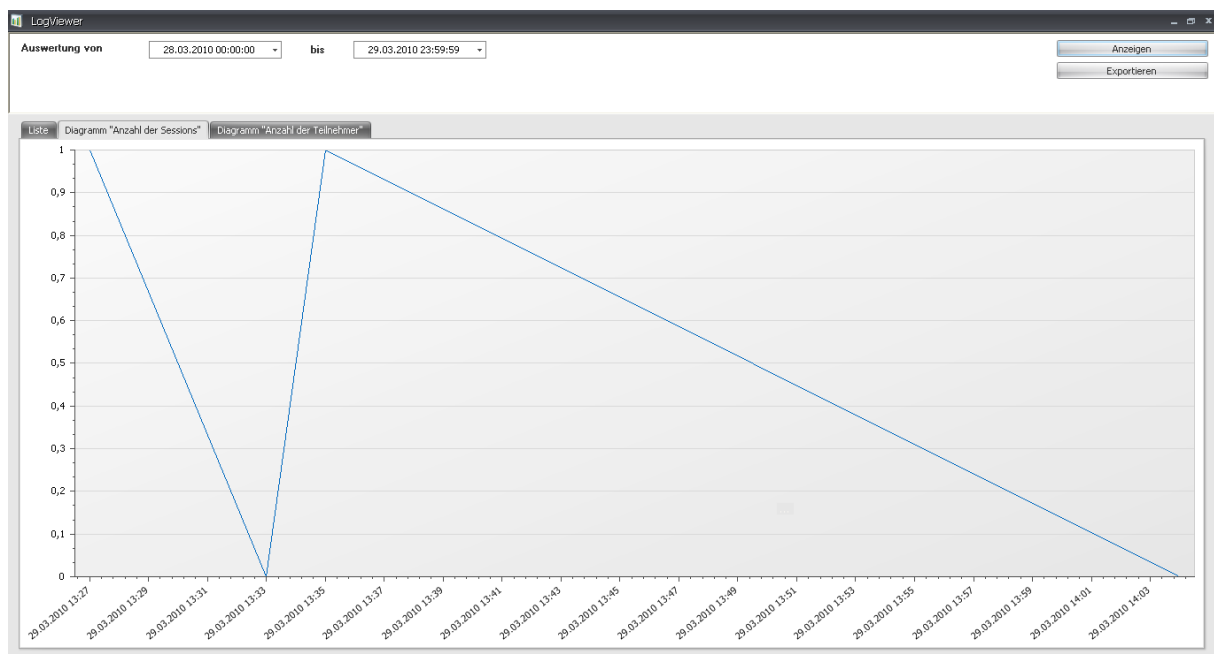
Folgende Informationen werden angezeigt:

- Seriennummer
- Sitzungsnummer
- Startzeit der Session
- Endzeit der Session
- Dauer (in Minuten)
- Start-Info (Information welche vor Beginn der Session eingetragen wurde)
- Windows-Benutzername des Masters
- Computername des Masters
- Ende-Info (Information welche am Ende der Session eingetragen wurde)
- Fwv-Benutzer
- Kundenname (Wenn im Master eingegeben)
- Externe IP (des Masters)
- Interne IP (des Masters)
- Externe IP Client
- Anzahl der Teilnehmer
- RE Username (Nur bei Verwendung des Remote Zugriffs von Secure Advisor relevant)
- RE Computername (Nur bei Verwendung des Remote Zugriffs von Secure Advisor relevant)
- RE Info 1-9 (Nur bei Verwendung des Remote Zugriffs von Secure Advisor relevant)
- Abgebrochen (wurde die Sitzung, z.B. durch Verbindungsverlust abgebrochen, so ist hier ein Haken gesetzt)

Es wurde zusätzlich eine Funktion zum Gruppieren nach den oben genannten Informationen hinterlegt. Hierzu „ziehen“ Sie einfach die entspr. Info in das dafür vorgesehene Feld. Ein Wechsel zwischen UTC und Lokalzeit ist ebenfalls möglich.

Durch eine Umrechnungsfunktion können Sie eine Auswertung nach EURO-Beträgen fahren. Hierzu geben Sie einfach den gewünschten Minutensatz in das Feld „Kosten € / min.“ ein, anschließend klicken Sie auf „Anzeigen“.

Durch einen Klick auf den Reiter Diagramm „Anzahl der Sessions“/Diagramm „Anzahl der Teilnehmer“ erhalten Sie folgende Ansicht:

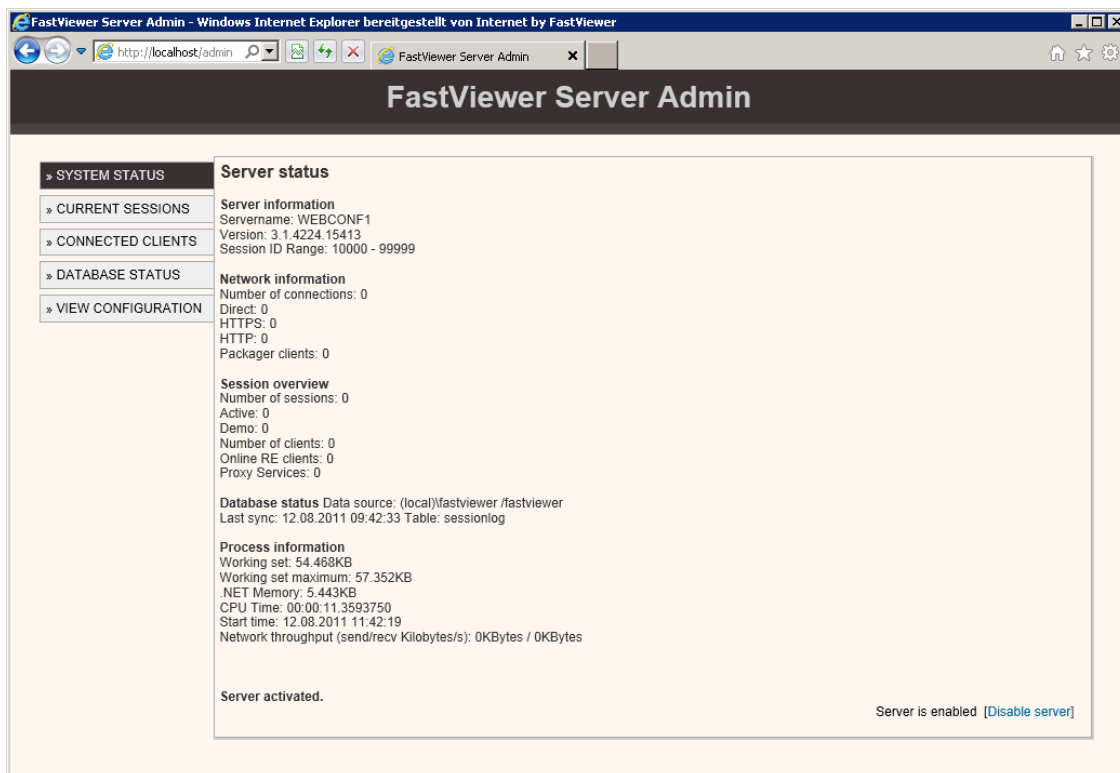


Es handelt sich hier um eine Übersicht der gehaltenen Sessions bzw. der beteiligten Teilnehmer im zuvor definierten Zeitraum, um Spitzen der Lizenzauslastung frühzeitig zu erkennen. Auf der x-Achse ist der gewählte Zeitraum und auf der y-Achse die Anzahl der parallel gehaltenen Sessions bzw. Anzahl der Teilnehmer ersichtlich.

## Server Admin

Der Server Admin ist ein browserbasiertes Tool, das die Anzeige des Server- bzw. Datenbankstatus, der Anzahl der aktuell gestarteten Sitzungen und der verbundenen Client-Module ermöglicht. Die Anzeige der aktuellen Serverkonfiguration (settings.ini) ist hierüber ebenfalls möglich.

Sie können auf dieses Tool auch direkt über Ihren Webbrowser zugreifen. Geben Sie hierfür in die Eingabezeile <http://localhost/admin> ein.



Durch Betätigen einer der folgenden im linken Seitenbereich dargestellten Schaltflächen können Sie sich die entsprechenden Informationen anzeigen lassen:

### SYSTEM STATUS

Diese Seite wird standardmäßig beim Starten des Server Admin angezeigt. Sie enthält allgemeine Informationen über den Server (z. B. Servername, Sitzungs-ID-Bereich), Netzwerk-Informationen (z. B. Art (direkte, über http oder HTTPS) und Anzahl der Verbindungen), sowie den Zustand des Servers (aktiviert oder nicht aktiviert).

Außerdem können Sie mit einem Klick auf „Disable server“ alle zukünftigen Verbindungen zum Server verweigern. Somit können keine neuen Verbindungen mehr ausgebaut werden, alle zu diesem Zeitpunkt bestehenden Verbindungen bleiben jedoch bestehen (z. B. wenn Sie eine Wartung planen, jedoch keine bestehenden Verbindungen abbrechen möchten).



# Serverdokumentation

ab Version 3.1

## CURRENT SESSIONS

Durch Klicken auf diese Schaltfläche erreichen Sie die Anzeige aller aktuellen Sitzungen.

## CONNECTED CLIENTS

Durch Klicken auf diese Schaltfläche können Sie sich einen Überblick über alle aktuell verbundenen Clients verschaffen.

## DATABASE STATUS

Die einzelnen Tabelleneinträge in der Tabellenspalte Table können in XMLFormat exportiert bzw. angezeigt werden. Diese Informationen sind ausschließlich für Supportzwecke relevant.

## VIEW CONFIGURATION

Ermöglicht den schnellen Zugriff auf die in der Konfigurationsdatei „settings.ini“ enthaltenen Servereinstellungen.

## Erstellen von SSL Zertifikaten für Ihren WebConferenceServer

Um eine SSL Zertifikatanforderung zu erstellen, nutzen Sie den IIS Webserver eines beliebigen Servers. Der IIS kann für die Zertifikatserstellung auch auf dem FastViewer Tunnelserver installiert werden. Allerdings muss dieser nach dem erstellen des Zertifikats deaktiviert werden.

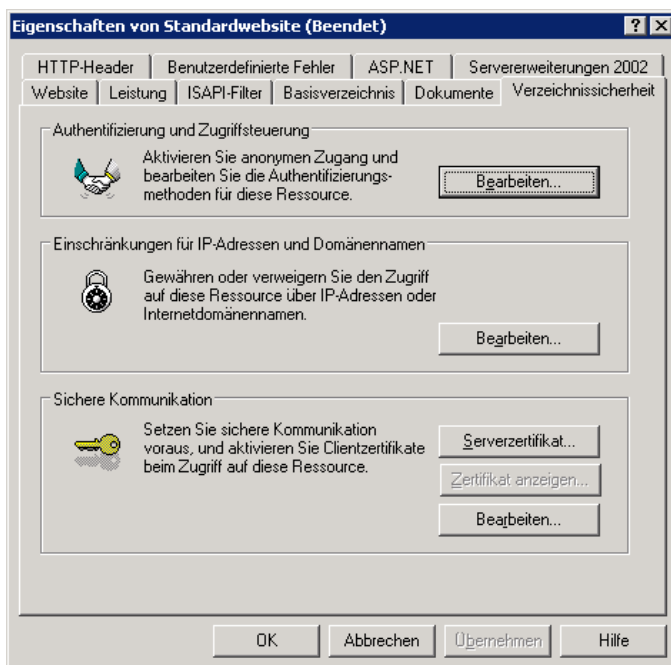
Führen Sie folgende Schritte durch, um SSL für Ihren FastViewer Tunnelserver (Installiert auf Windows Server 2003) zu konfigurieren.

Klicken Sie auf Start, Verwaltung, Internetinformationsdienste-Manager.

Klicken Sie in der Baumstruktur der linken Konsole auf Internetinformationsdienste, SERVERNAME (lokaler Computer).

Führen Sie einen Rechtsklick auf Ihrer Standard Webseite aus und wählen Sie "Eigenschaften".

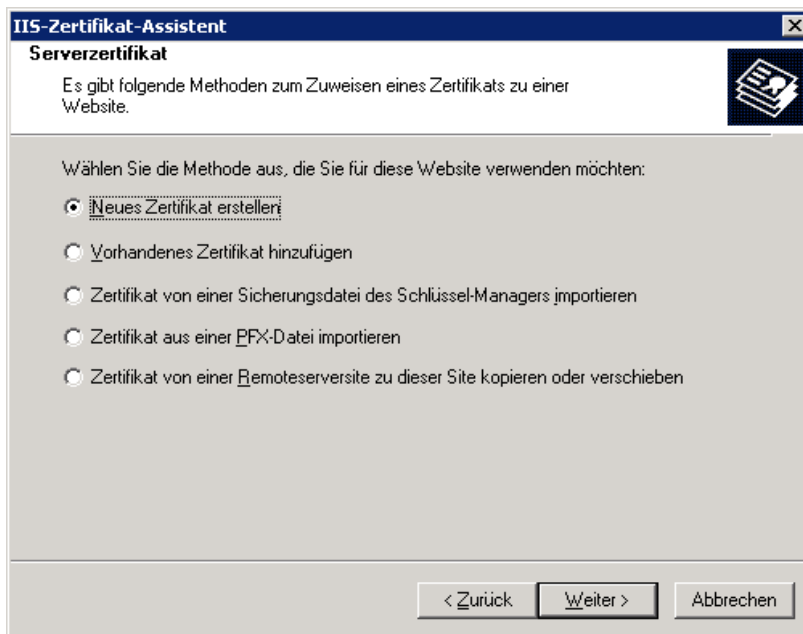
Im Menü "Eigenschaften" Ihrer Standard Webseite klicken Sie auf "Verzeichnissicherheit".



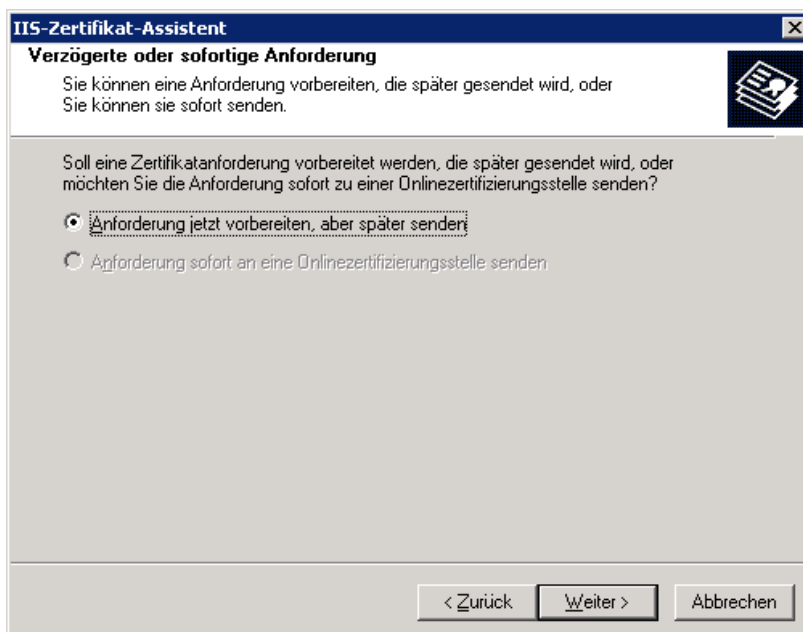
Im Register "Verzeichnissicherheit", klicken Sie auf "Serverzertifikat".

Nun öffnet sich der "IIS-Zertifikat-Assistent". Klicken Sie auf "Weiter".

Vergewissern Sie sich, dass "Neues Zertifikat erstellen" ausgewählt ist und klicken Sie auf "Weiter".



Als nächstes wählen Sie "Anforderung jetzt vorbereiten, aber später senden".



Definieren Sie einen beliebigen Namen für Ihr Zertifikat und wählen Sie bei "Bitlänge" die Zahl "1024" aus. Im danach folgenden Fenster, geben Sie Ihre Organisation und Organisationseinheit an. Was Sie hier eingeben hat keinerlei Relevanz, da die Eingaben später im Zertifikat nicht ersichtlich sind.



**IIS-Zertifikat-Assistent**

**Name und Sicherheitseinstellungen**

Das neue Zertifikat muss einen Namen und eine Bitlänge haben.

Geben Sie einen Namen für das neue Zertifikat ein. Der Name sollte einfach zu merken sein.

Name:  
[fastviewer1]

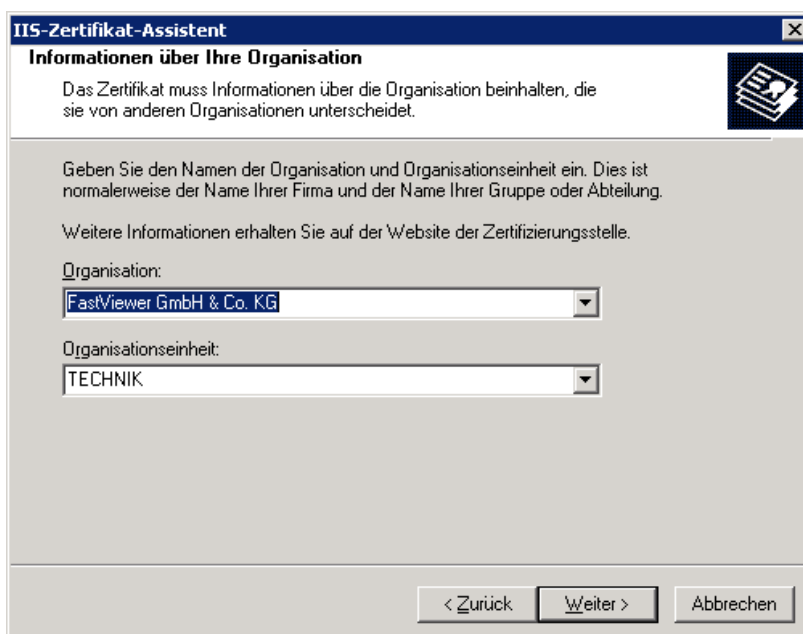
Die Bitlänge des Schlüssels bestimmt die Verschlüsselungsstärke des Zertifikats. Je größer die Bitlänge ist, desto größer ist die Sicherheit. Jedoch kann eine größere Bitlänge die Leistung verringern.

Bitlänge: [1024]

Kryptografiedienstanbieter (CSP) für dieses Zertifikat auswählen

< Zurück Weiter > Abbrechen

Geben Sie hier bitte Ihren Firmennamen und die entsprechende Organisationseinheit an:



**IIS-Zertifikat-Assistent**

**Informationen über Ihre Organisation**

Das Zertifikat muss Informationen über die Organisation beinhalten, die sie von anderen Organisationen unterscheidet.

Geben Sie den Namen der Organisation und Organisationseinheit ein. Dies ist normalerweise der Name Ihrer Firma und der Name Ihrer Gruppe oder Abteilung.

Weitere Informationen erhalten Sie auf der Website der Zertifizierungsstelle.

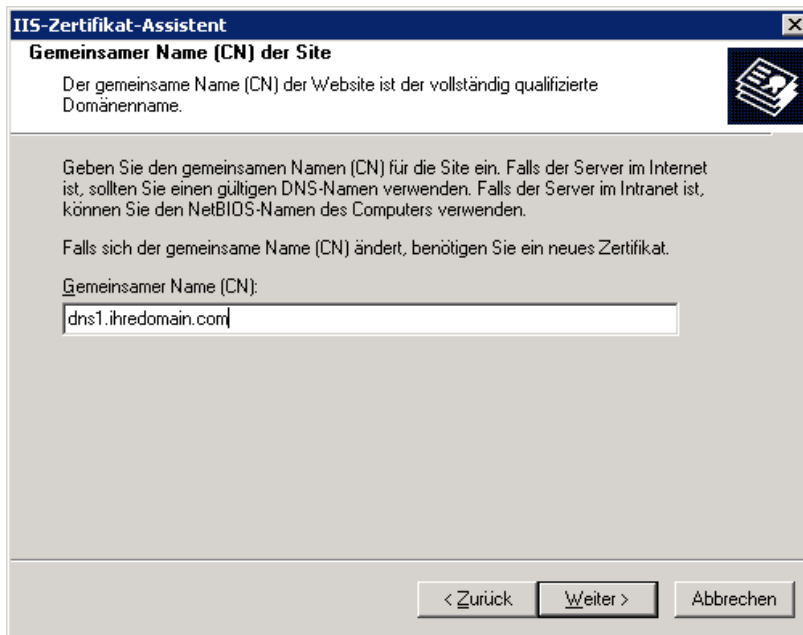
Organisation:  
[FastViewer GmbH & Co. KG]

Organisationseinheit:  
[TECHNIK]

< Zurück Weiter > Abbrechen



ACHTUNG: Als nächstes geben Sie Ihren DNS Namen für den Tunnelserver ein. Dieser Schritt ist sehr wichtig. Achten Sie auf die korrekte Eingabe. Der Name MUSS exakt mit dem DNS Namen übereinstimmen, andernfalls ist das Zertifikat ungültig!



**IIS-Zertifikat-Assistent**

**Gemeinsamer Name (CN) der Site**

Der gemeinsame Name (CN) der Website ist der vollständig qualifizierte Domänenname.

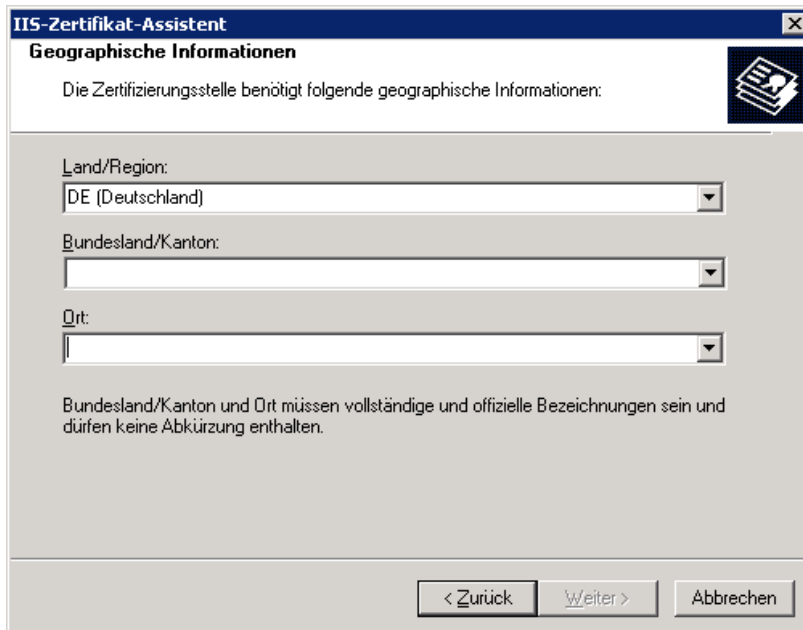
Geben Sie den gemeinsamen Namen (CN) für die Site ein. Falls der Server im Internet ist, sollten Sie einen gültigen DNS-Namen verwenden. Falls der Server im Intranet ist, können Sie den NetBIOS-Namen des Computers verwenden.

Falls sich der gemeinsame Name (CN) ändert, benötigen Sie ein neues Zertifikat.

Gemeinsamer Name (CN):

< Zurück Weiter > Abbrechen

Danach geben Sie Ihr Land, Bundesland und Ihren Ort an.



**IIS-Zertifikat-Assistent**

**Geographische Informationen**

Die Zertifizierungsstelle benötigt folgende geographische Informationen:

Land/Region:

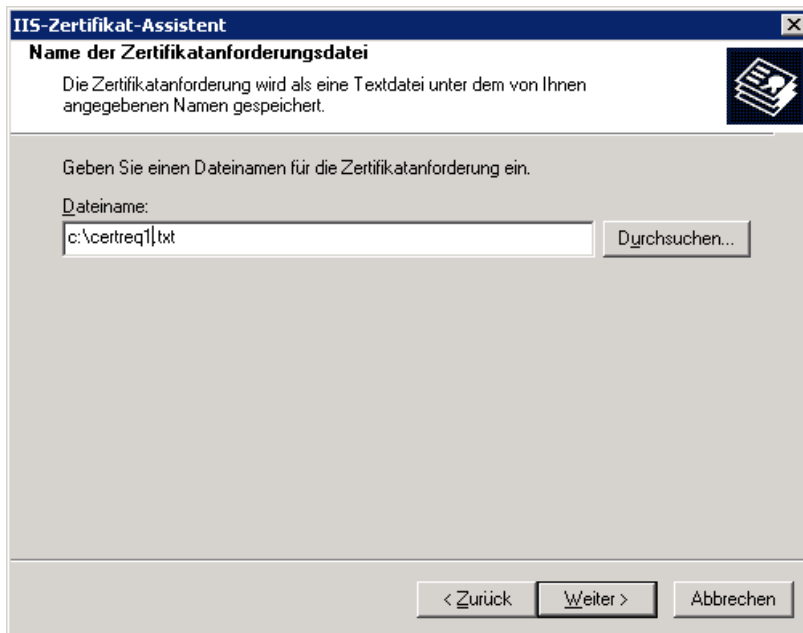
Bundesland/Kanton:

Ort:

Bundesland/Kanton und Ort müssen vollständige und offizielle Bezeichnungen sein und dürfen keine Abkürzung enthalten.

< Zurück Weiter > Abbrechen

Definieren Sie den Namen der "Zertifikatanforderung" und klicken Sie auf "Weiter".



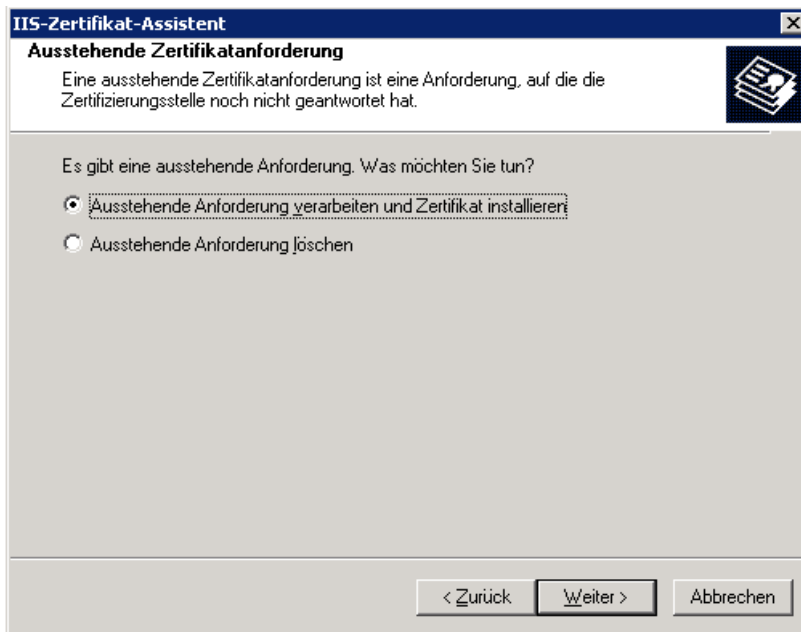
Im nächsten Fenster, klicken Sie erneut auf "Weiter" und danach auf "Fertig stellen".

Starten Sie Ihren Browser, navigieren Sie zu Ihrer gewünschten Zertifizierungsstelle (z.B. eg. VeriSign oder Thawte) und erwerben Sie ein "SSL Zertifikat".

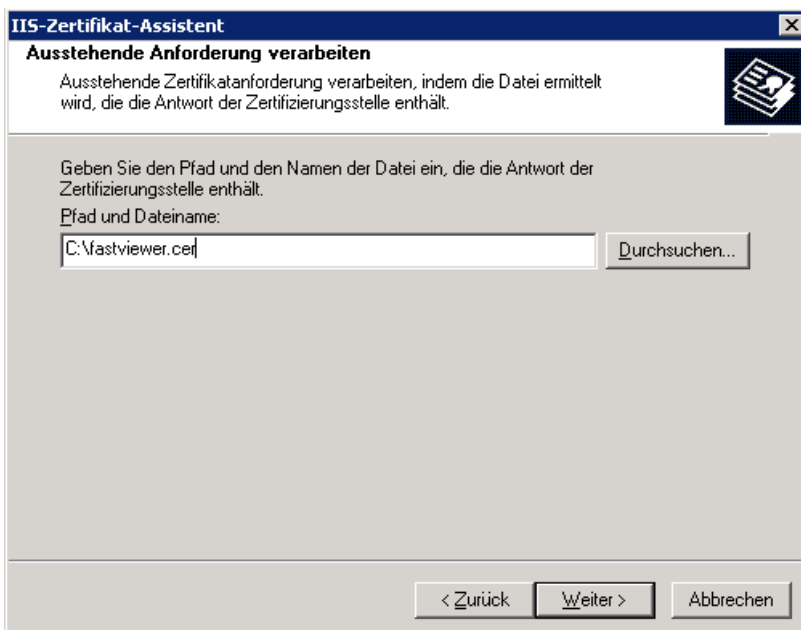
Öffnen Sie nun die vorher erstellte TXT Datei und kopieren Sie den gesamten Inhalt in das CSR Feld. Folgen Sie den Anweisungen auf der Webseite um den Erwerb des Zertifikates zu vervollständigen.

Üblicherweise wird Ihr Zertifikat per E-Mail an Sie gesendet – Speichern Sie das Zertifikat auf Ihrem Webserver ab.

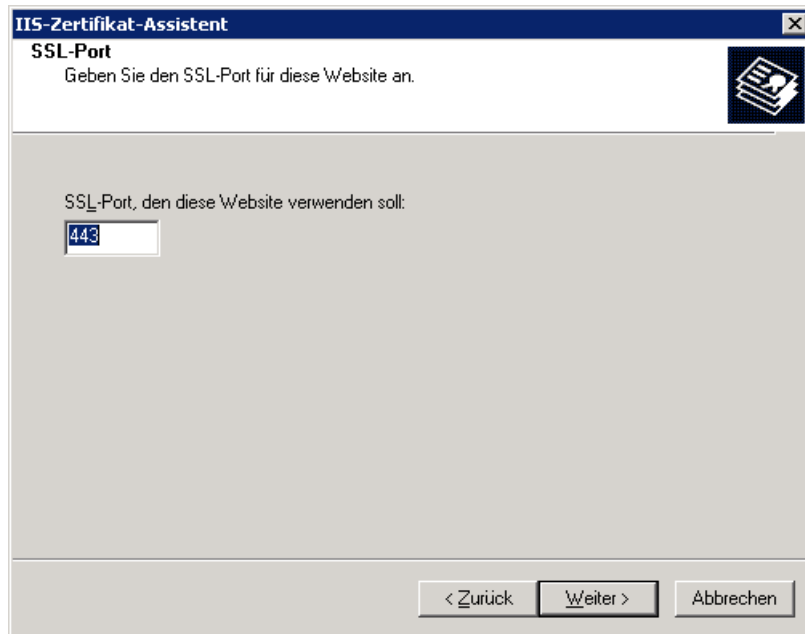
Öffnen Sie im Internetinformationsdienste-Manager das Menü "Eigenschaften" und wählen Sie das Register "Verzeichnissicherheit". Klicken Sie auf "Serverzertifikat". Im nächsten Fenster klicken Sie auf "Weiter".



Danach geben Sie den Pfad Ihres Zertifikates an.



Hier ist der SSL-Port, über welchen kommuniziert werden soll anzugeben. In unserem Fall 443 (Bei einer Kommunikation über HTTPS wird IMMER der Port 443 verwendet)

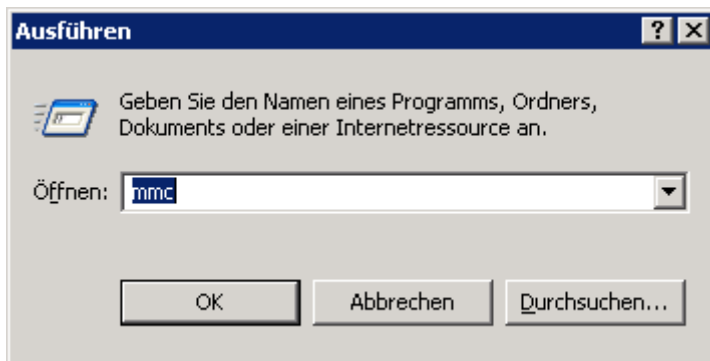


Klicken Sie im nächsten Screen auf „Weiter“ und beenden Sie den Assistenten über den Button „Fertig stellen“.

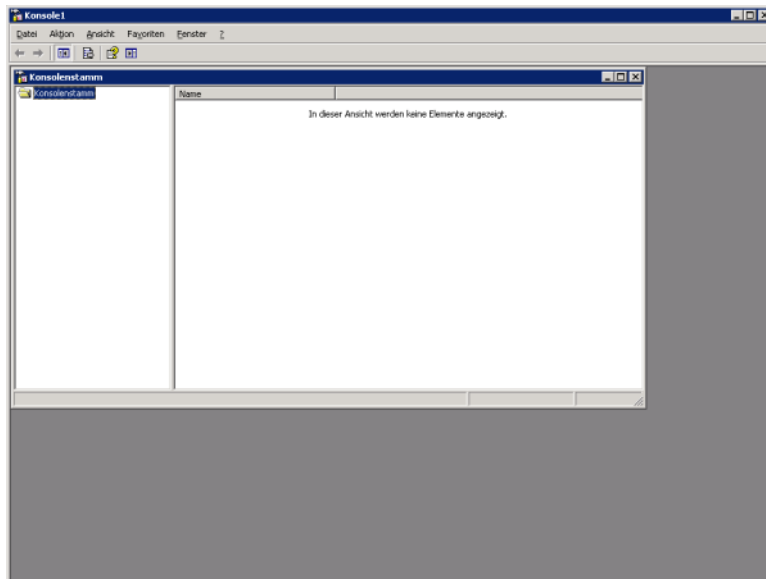
Als nächstes exportieren Sie das Zertifikat und Ihren "private key" auf den FastViewer Tunnelserver. Falls Sie die Zertifikatanforderung auf dem FastViewer Tunnelserver durchgeführt haben, ist der Export nicht notwendig.

Zertifikat exportieren:

Klicken auf "Start", "Ausführen", geben Sie "mmc" ein und bestätigen Sie mit "OK".

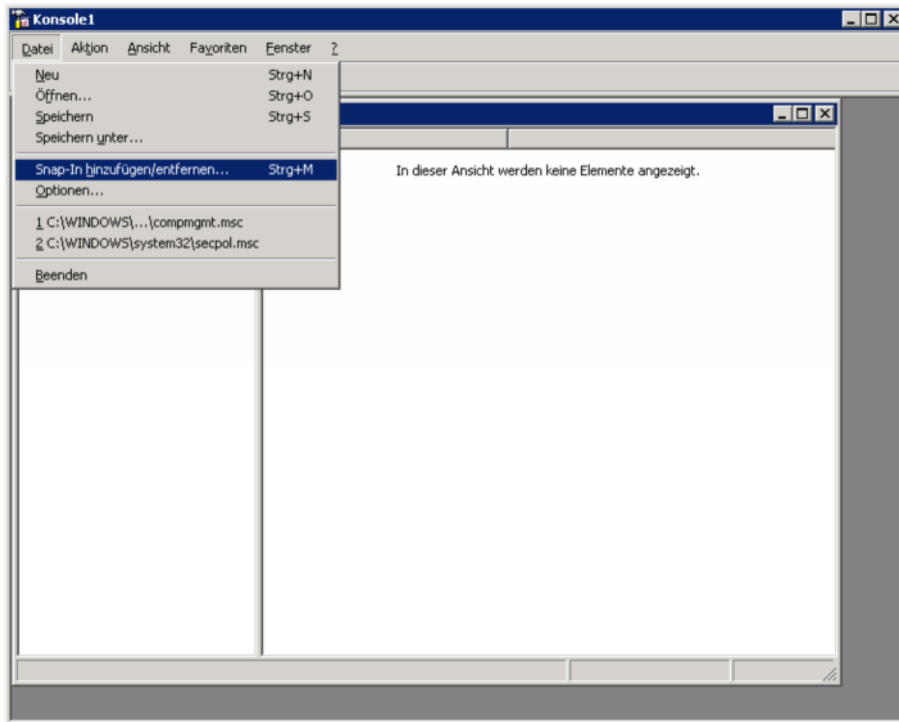


Es öffnet sich eine leere MMC.





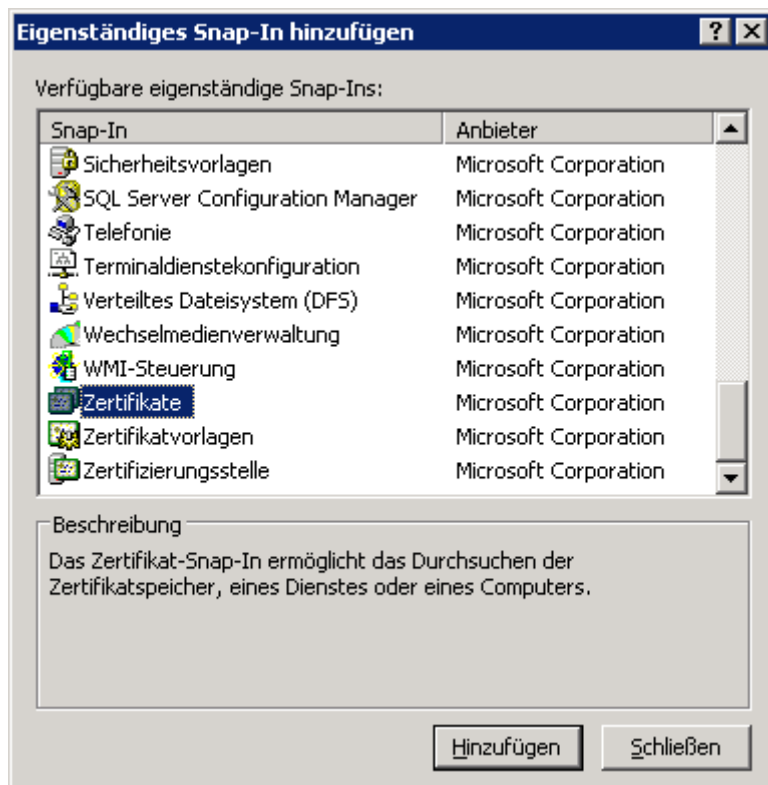
Danach klicken Sie auf "Snap-In hinzufügen/entfernen...".



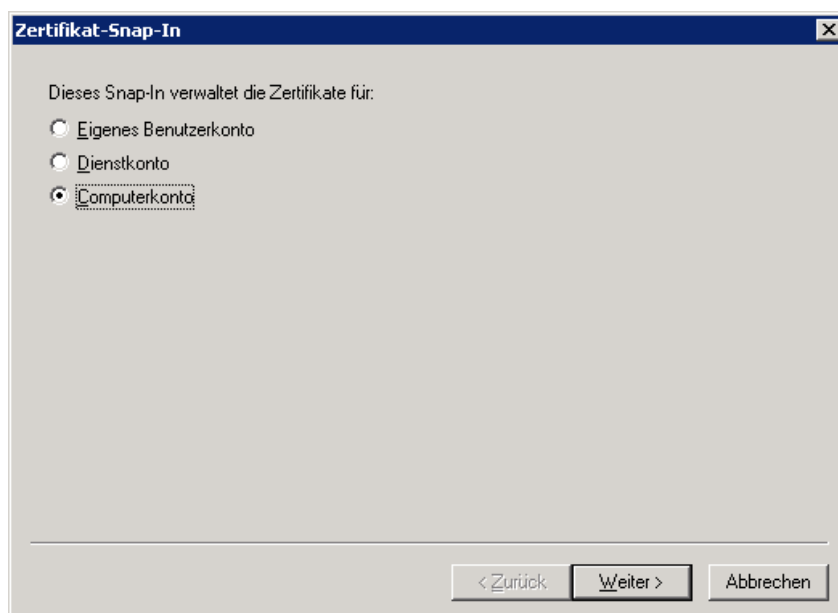
Es öffnet sich folgendes Fenster:



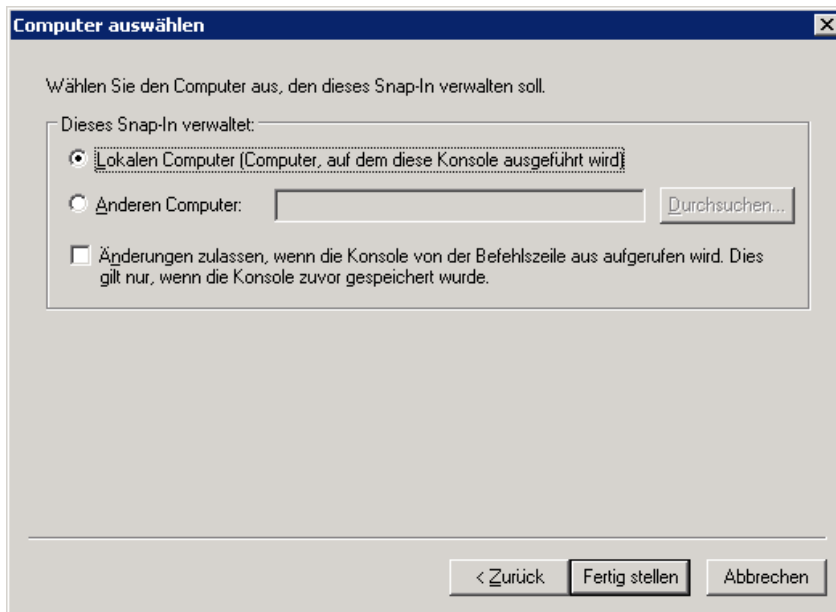
Klicken Sie auf "Hinzufügen" wählen Sie "Zertifikate".



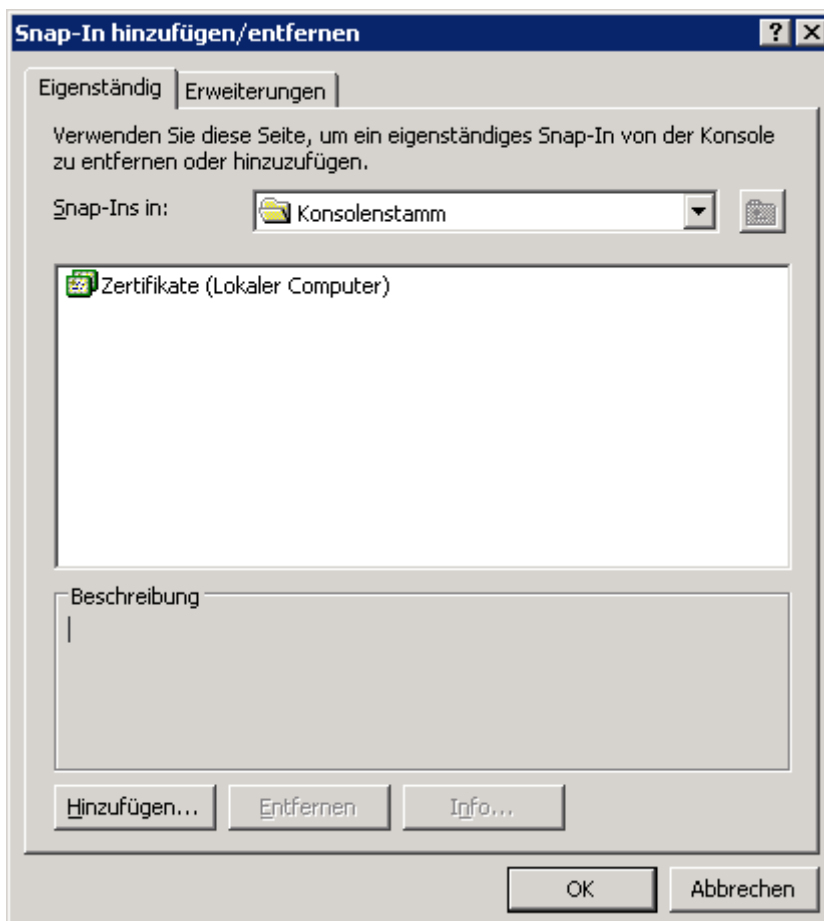
Wählen Sie "Computerkonto".



Im folgenden Fenster wählen Sie "Lokalen Computer" und klicken auf „Fertig stellen“.

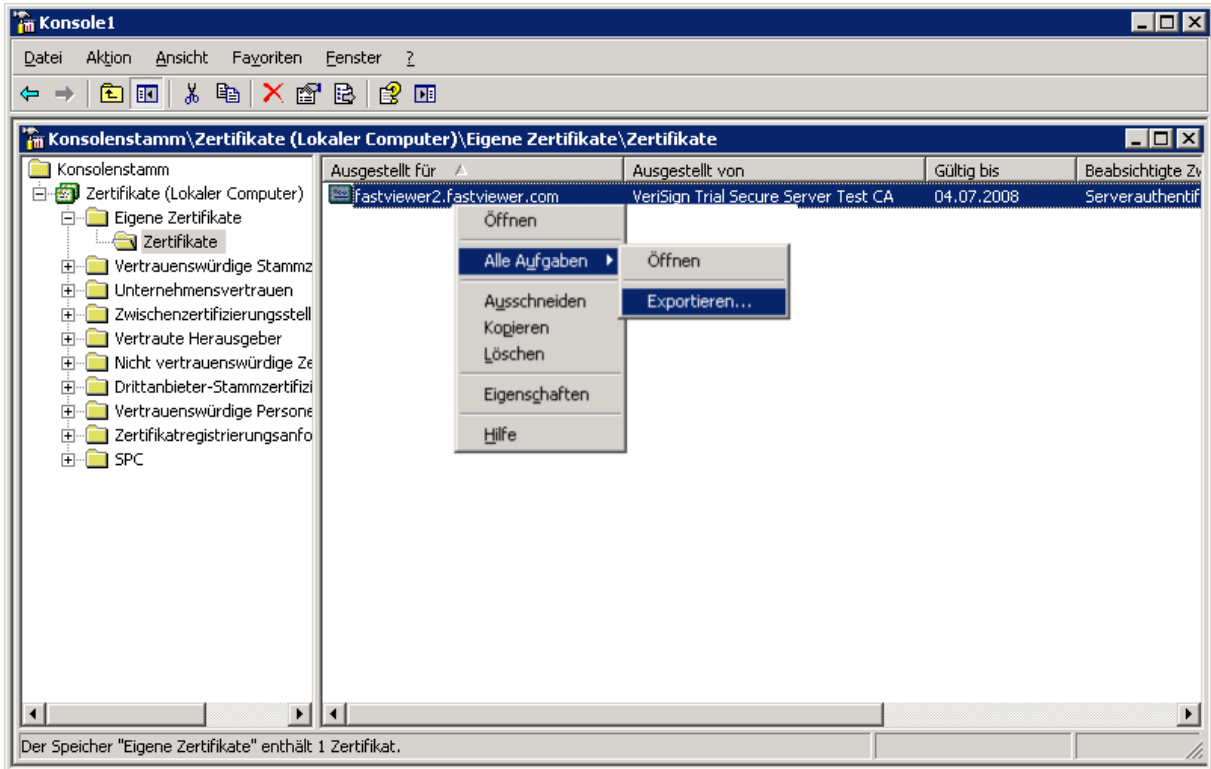


Nun sollten Sie folgende Ansicht sehen, klicken Sie auf "OK".

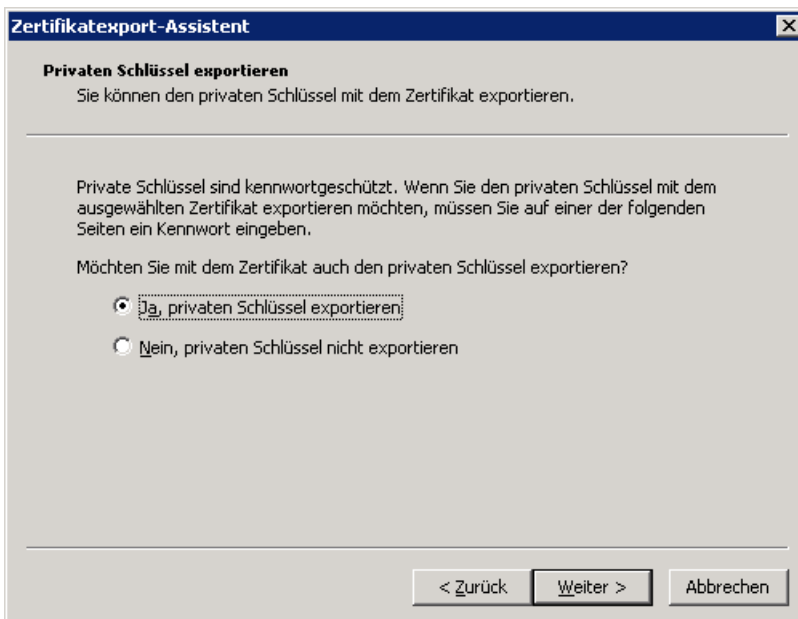




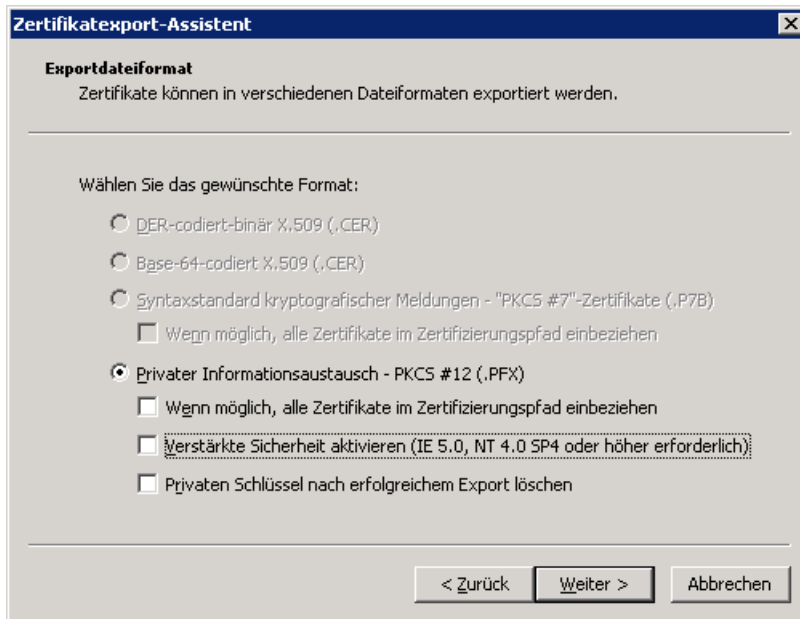
Klicken Sie auf den Ordner "Eigene Zertifikate/Zertifikate". In der rechten Spalte führen Sie einen Rechtsklick auf das entsprechende Zertifikat aus und wählen Sie "Alle Aufgaben", "Exportieren".



Im nächsten, sehr wichtigen Schritt wählen Sie "Ja, privaten Schlüssel exportieren".



Im nächsten Schritt wählen Sie die Optionen wie im unten stehenden Bild und klicken sie auf „Weiter“.



**Zertifikatexport-Assistent**

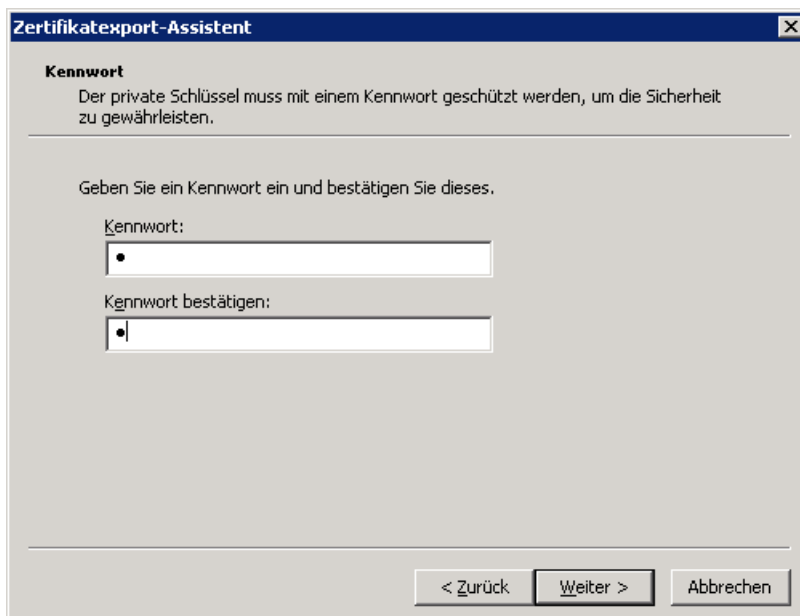
**Exportdateiformat**  
Zertifikate können in verschiedenen Dateiformaten exportiert werden.

Wählen Sie das gewünschte Format:

- DER-codiert-binär X.509 (.CER)
- Base-64-codiert X.509 (.CER)
- Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)
  - Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
- Privater Informationsaustausch - PKCS #12 (.PFX)
  - Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
  - Verstärkte Sicherheit aktivieren (IE 5.0, NT 4.0 SP4 oder höher erforderlich)
  - Privaten Schlüssel nach erfolgreichem Export löschen

< Zurück   Weiter >   Abbrechen

Nun wählen Sie ein Passwort für ihren "private key" aus. Später werden sie dieses Passwort benötigen, um das Zertifikat in den FastViewer Tunnelserver zu importieren.



**Zertifikatexport-Assistent**

**Kennwort**  
Der private Schlüssel muss mit einem Kennwort geschützt werden, um die Sicherheit zu gewährleisten.

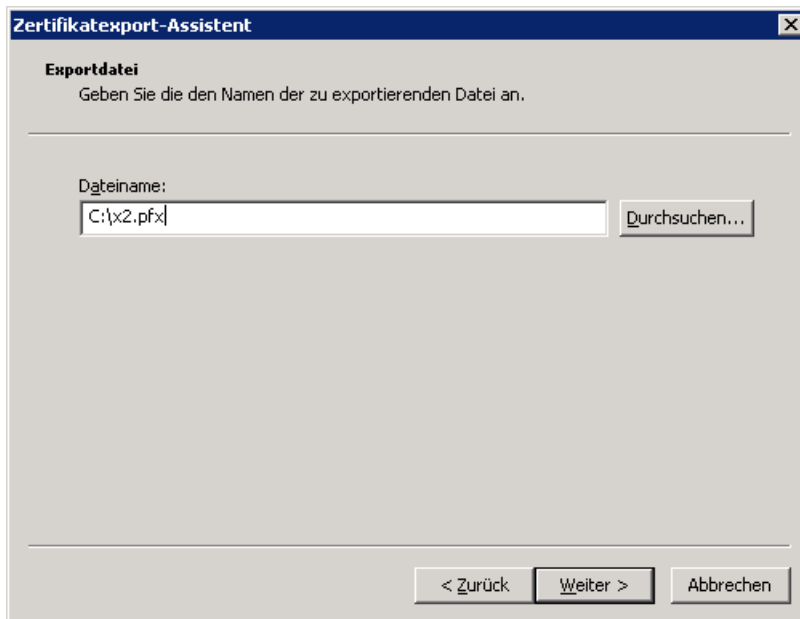
Geben Sie ein Kennwort ein und bestätigen Sie dieses.

Kennwort:

Kennwort bestätigen:

< Zurück   Weiter >   Abbrechen

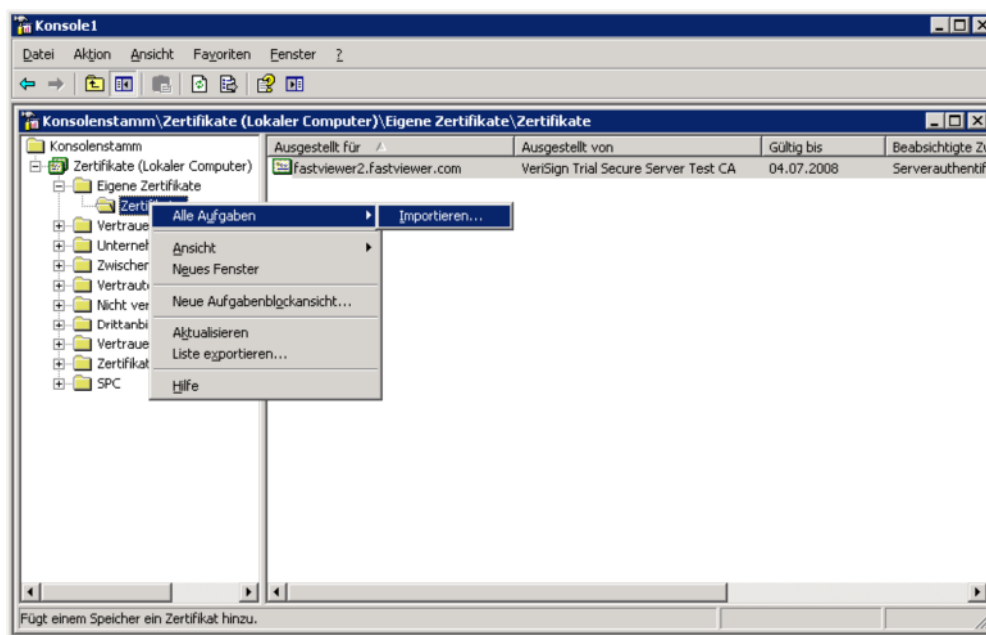
Wählen sie Pfad und Dateiname für Ihr Zertifikat aus und klicken Sie auf „Fertig stellen“.



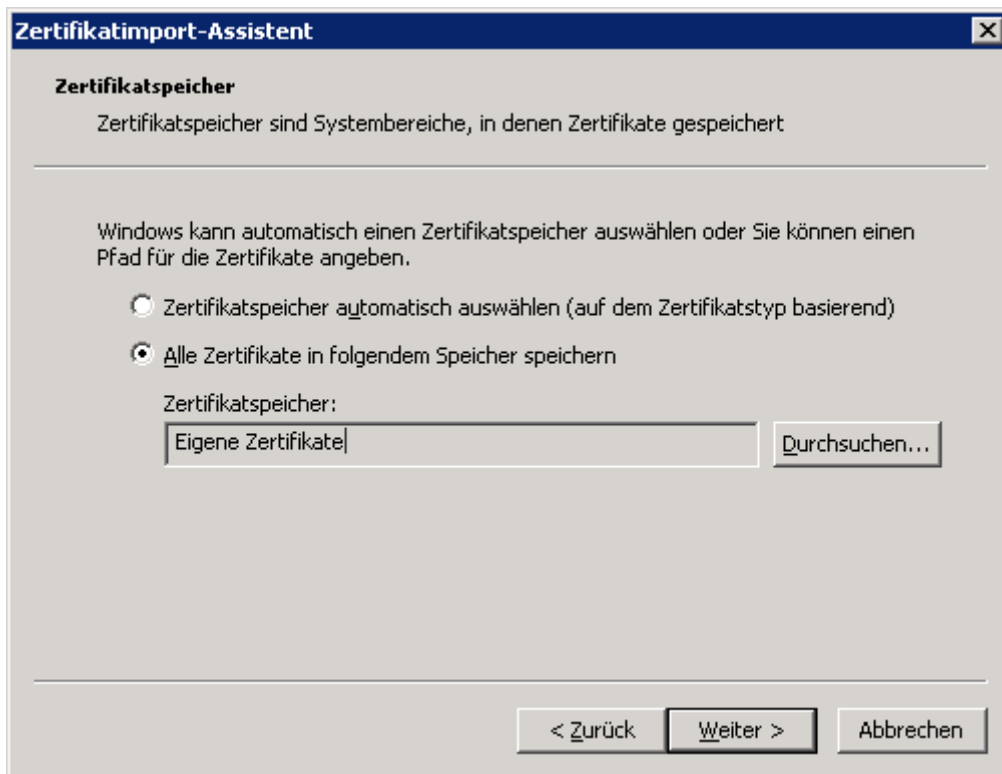
Kopieren Sie nun das exportierte Zertifikat auf Ihren FastViewer Tunnelserver.

Abschließend importieren Sie das Zertifikat in den FastViewer Tunnelserver.

Klicken erneut auf "Start", "Ausführen". Geben Sie "mmc" ein und bestätigen Sie mit "OK". Führen Sie die gleichen Schritte aus wie oben beschrieben.

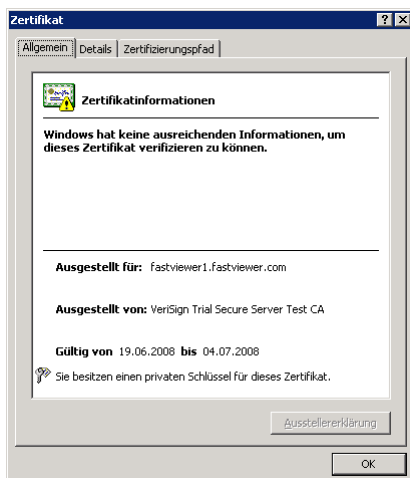


Nun wählen Sie das Zertifikat, klicken auf "Weiter" und geben das vorher generierte Passwort ein. Klicken Sie danach auf "Fertig stellen".



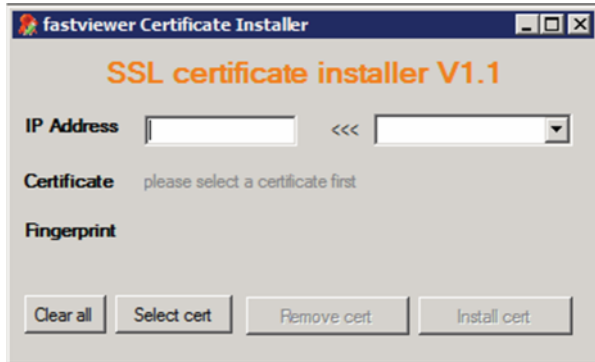
Die Installation der Zertifikate ist nun abgeschlossen.

Um zu überprüfen, ob das Zertifikat inkl. Private Key am Server verfügbar ist, öffnen Sie bitte alle hinterlegten Zertifikate. Wichtig hierbei ist die Info "Sie besitzen einen privaten Schlüssel für dieses Zertifikat".



## Anbindung eines Zertifikats an eine IP-Adresse

Um Ihnen die Anbindung der Zertifikate an die entspr. IP-Adressen zu erleichtern, wird Ihnen nach der Installation unter „Start/Programme/WebConferenceServer“ der „FastViewer Certificate Installer“ angeboten:



**IP Address:** Hier ist die IP-Adresse anzugeben, an welche das Zertifikat gebunden werden soll (Die IP Adresse kann entweder manuell eingegeben werden oder über das nebenstehende Dropdown-Menü gewählt werden)

**Certificate:** Gewähltes Zertifikat (siehe „choose cert“)

**Fingerprint:** Fingerprint-Wert

**Clear all:** Löscht alle Eingaben

**Select cert:** Wählen Sie hier das Zertifikat aus, welches an die bei „IP Adress“ genannte IP gebunden werden soll

**Remove cert:** Mit diesem Button ist es möglich ein Zertifikat von einer IP zu trennen

**Install cert:** Insofern alle benötigten Eingaben getätigt wurden, wird durch einen Klick auf den „install-Button“ das Zertifikat an die entspr. IP gebunden



Den Status der angebotenen Zertifikate können Sie sich über den Befehl „httpcfg query ssl“ (im Verzeichnis des Tunnelserver) ausgeben lassen:

```
C:\WINDOWS\system32\cmd.exe
C:\Programme\TunnelserverU3>httpcfg query ssl
IP                : 192.168.2.115:443
Hash              : a291ddf521f2c19f6ea422272f aec665ccfea 6
Guid              : {841f64d3-63eb-4dde-ba9d-c40186027f61}
CertStoreName     : <null>
CertCheckMode     : 0
RevocationFreshnessTime : 0
UrlRetrievalTimeout : 0
SslCtlIdentifier  : <null>
SslCtlStoreName   : <null>
Flags             : 0
-----
IP                : 192.168.2.116:443
Hash              : 6b a ff76914735125bbb83f3c2 b4310bb2fc9
Guid              : {841f64d3-63eb-4dde-ba9d-c40186027f61}
CertStoreName     : <null>
CertCheckMode     : 0
RevocationFreshnessTime : 0
UrlRetrievalTimeout : 0
SslCtlIdentifier  : <null>
SslCtlStoreName   : <null>
Flags             : 0
-----
C:\Programme\TunnelserverU3>
```



## Erste Hilfe im Falle eines Verbindungsproblems

Sollten Sie mit den FastViewer-Modulen in Verbindung mit einer eigenen Serverlösung keine Verbindung herstellen können, so würden wir Sie bitten uns die „tunnelserver.log“ zukommen zu lassen. Hierbei gehen Sie bitte wie folgt vor:

1. Stoppen Sie den FastViewer-Dienst (tunnelserverv3)
2. Überprüfen Sie im Taskmanager ob der FastViewer Task beendet ist
3. Stellen Sie den Wert „LogVerboseLevel“, welcher in der „Settings.ini“ zu finden ist auf den Wert „1“.
4. Starten Sie den FastViewer-Dienst (tunnelserverv3)
5. Starten Sie das entsprechende Modul, bzw. stellen Sie die Aktion, bei welcher der Fehler aufgetreten ist, nach.
6. Sichern Sie die „tunnelserver.log“ (verschieben in ein anderes Verzeichnis) und lassen Sie uns diese per Mail an [support@FastViewer.com](mailto:support@FastViewer.com) zukommen.
7. Stoppen Sie den FastViewer-Dienst (tunnelserverv3)
8. Setzen Sie den „LogVerboseLevel“, welcher in der „Settings.ini“ zu finden ist zurück, auf den vorherigen Wert.
9. Starten Sie den FastViewer-Dienst (tunnelserverv3)

Überprüfen Sie bitte auch, ob der Server innerhalb des LANs (<http://servername/>) und von Außerhalb (<http://DNS-Name/>) erreichbar ist.

**Hinweis:** Beachten Sie bitte, dass wenn Sie FastViewer Secure Advisor mit Remote Zugriff einsetzen, Sie beim Einloggen in die Remote-Übersicht als Benutzername und Passwort nicht Ihre Lizenznummer und das entsprechende Passwort, sondern in beide Felder „admin“ eingeben müssen! Anschließend kann der Benutzername und das Passwort geändert werden.

Sollte keiner der oben genannten Schritte das Verbindungsproblem beheben, so kontaktieren Sie bitte unsere Supporthotline:

### Supporthotline

Tel. +49 9181 509 56 28

[support@fastviewer.com](mailto:support@fastviewer.com)

## Kontakt

Sehr geehrter Kunde / Interessent,

sollten Sie Fragen zum Produkt haben, wenden Sie sich bitte an:

### **FastViewer Deutschland:**

Schwesterhausgasse 11  
92318 Neumarkt

fon. +49 (9181) 509 56 -0  
fax. +49 (9181) 509 56 -29  
e-mail. [info@fastviewer.com](mailto:info@fastviewer.com)  
[www.fastviewer.com](http://www.fastviewer.com)

### **Technischer Support:**

Sollten Sie technische Unterstützung benötigen, wenden Sie sich bitte an unsere Hotline:

fon. +49 (9181) 509 56 -28  
fax. +49 (9181) 509 56 -29  
e-mail. [support@fastviewer.com](mailto:support@fastviewer.com)



**FastViewer** - die geniale Lösung, die verbindet - weltweit und zu jeder Zeit.