





FastViewer - die geniale Lösung,

die verbindet - weltweit und zu jeder Zeit.



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

© 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.





(C) 2010 FastViewer GmbH und Co KG



Installation des Servers

1. Das Setup zur Installation der eigenen Serverlösung finden Sie im Downloadbereich Ihres persönlichen Kundenportals (erreichbar unter <u>http://portal.fastviewer.com</u>). Alternativ können Sie das Setup ebenfalls über folgenden Link beziehen: <u>http://portal.fastviewer.com/customerlicense/downloads/serversetupv32.zip</u>

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 <u>http://localhost/admin</u> navigieren. Wenn die folgende Statusseite des Tunnelservers 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:

ExternalAdress=Change2YourServer

Ersetzen Sie den Wert "Change2YourServer" durch den externen vollständig qualifizierten Domänennamen (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 Domänennamen (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.





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.

Internet Explorer Internet Explorer (54 BR) Windows Lipdate Windows Kotalate Windows and Upgrades	Administrator
Microsoft SQL Server 2005	Dokumente
Wartung	Computer
Ջ Certificate Installer 🔟 Log Viewer	Netzwerk
Erver Admin Server Manager	Systemsteuerung
🕌 Zubehör	Verwaltung +
	Hilfe und Support
	Ausführen
	Windows-Sicherheit
 Zurück 	
Buche starten	00

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

Server Management Wizard	¥1.2	×
	Welcome to the FastViewer Server Management Wizard	
	You can activate your Server or Import your Licenses by pressing the corresponding Button:	
fast viewer	This Server must be activated in order to import Licenses	
	Activate Server Import Libense	:\$

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

Server Management Wizard	V 1.3.4169.18134	X
	Activation - Step 1:	Serverlist
	Please enter a Serverlist-URL:	Check
	Define a valid Serverlist:	
fastviewer	Select a number range: For Server:	from: 10000 == to: 99999 == + -
Restart		Next



4. Geben Sie nun Ihre Lizenznummer ein.

🍓 Server Management Wizard	¥ 1.2	×
	Server Activation	
	Please enter your Serial:	
fastviewer		
Restart	Activate	

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 (<u>serverlicense@FastViewer.com</u>) 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.

Server Management Wizard ¥ 1.2	×
Server has been successfully activated! Now, your license	s will be imported!
	OK

6. Folgender Dialog öffnet sich:

Server Management Wizard	V 1.3.4070.22353	×
	C Use Download C Use Local File:	
fastviewer		
Restart		Start Import

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: <u>http://localhost/admin</u>, 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 <u>http://Ihrserver.Ihredomain</u>. Ersetzen Sie <u>Ihrserver.Ihredomain</u> 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 Tunnelservers eine Einstellung getroffen werden, welche den Fall eines Dienstfehlers betrifft.

Bitte konfigurieren Sie diese Optionen wie folgt:

Erster Fehler:	Dienst neu starten		
Zweiter Fehler:	Dienst neu starten		
Weitere Fehler:	Dienst neu starten		
Fehlerzähler nach	0 Tagen zurücksetzen		
Dienst nach	1 Minuten neu starten		
Programm ausführen-			
Programm:			
	Durchsuchen		
Befehlszeilenparamete	er:		
Eeblerzähler zur Br			



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:

👔 WebConferenceServer		
G - Programme (x86) + WebConferenceServer +	👻 🔯 Suchen	
Datei Bearbeiten Ansicht Extras ?		
💽 Organisieren 🔻 📗 Ansichten 🔻 📄 Öffnen		0
Linkfavoriten	Name 🔶 🚽 Änderungsdatum 🗣 T	ур 🔺
	FastClient 11.01.2011 11:37 A	nwendung
Dokumente	FastViewer.CLib.dll 25.11.2010 17:27 Pi	rogrammbiblioth
🖺 Bilder	FastViewer.CLib.pdb 25.11.2010 17:27 Pl	DB-Datei
📳 Musik	fcdata.dll 25.11.2010 17:27 Pi	rogrammbiblioth
Weitere >>	fcdata.pdb 25.11.2010 17:27 Pl	DB-Datei
Woldso	🔞 fvw16 24.03.2008 22:08 Id	con
Ordnar	🔪 🏟 fyw32 24.03.2008 22:08 Id	con 👘
	Linktpcfg 24.03.2003 23:06 A	nwendung
📕 Programme	Sinstallservice 25.06.2007 20:03 W	vindows-Stapel.
🍌 Programme (×86)	Akey 24.05,2006 16:22 Id	con
📔 Common Files	LogViewer 25.11.2010 17:27 A	nwenduna
📔 Internet Explorer	LogViewer.exe.config 25.11.2010 17:26 C	ONFIG-Datei
Microsoft.NET	LogViewer.pdb 25.11.2010 17:27 P	DB-Datei
Microsoft SQL Server	I onViewerConsole 25.11.2010 17:27 A	www.endung
WebConferenceServer	LogViewerCopsole.e., 25,11,2010 17:26 C	ONEIG-Datei
🚺 Windows Mail	▼ <	

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 Domänennamen (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"

fastviewer	p vn F	T
🚀 Meine Lizenz 👻 🖄 Dokumente 🛛 🐒 Eins	stellungen 👻 🌖 Download 🛛 🛱 Logs 💌	📕 Ausloggen
Konfiguration der Programmodule Hier können Sie alle die Programmmodule betreffenden Einz	stellungen vornehmen! Diese Einstellungen werden jedoch ers	t nach erneutern Download der Module aktiv.
Angezeigtes Profit: Default * Pro	ofil laden Profile verwalten Wechseln zu: Funktione	Änderungen speichern
Allgemein Teilnehmermodul Support Präsen	tation Konferenz Remote	
Servername für Teilnehmermodul-Link	I nicht ausgewä	hlt }
Benutzermanager deaktivieren	Inicht ausgewält 192.168.2.90	sit }
Taste zum Beenden der Fernsteuerung	6 F11 •	
Standardprofil	Ø Konferenz	



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")

SQL Server Configuration Manager					_ 🗆 ×
<u>D</u> atei Aktion <u>A</u> nsicht <u>?</u>					
← → € E E SQL Server-Konfigurations-Manager (Lokal) 5QL Server 2005-Dienste SQL Server 2005-Netzwerkkonfiguration → Protokolle für 'FASTVIEWER' → ● SQL Native Client-Konfiguration	Protokoliname Shared Memory TCP/IP	Status Aktiviert Deaktiviert Deaktiviert	nschaften von TCP/IP otokoll IP-Adressen General Aktiviert Alle überwachen Erhalten Keine Verzögerung	D Ja Ja Ja 30000 Nein	· ·
		A T ^r	ktiviert IP/IP-Protokoll für diese : OK	Serverinstanz aktivieren oder deak Abbrechen Übernehmen	tivieren Hilfe

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

📕 Server-Manager				
Datei Aktion Ansicht ?				
🗢 🧼 🖄 📰 🔯 🗟 🔒				
Server-Manager (FVWSL)	Dienste			Aktionen
 	🖏 Dienste			Dienste 🔺
Image Diagnose Image Di	SQL Server Browser	Name 🔶	Beschreibung 🔺	Weiter >
Aufgabenplanung Aufgabenplanung Windows-Tirewail mit erweil Windows-Tirewail Windows-Tirewail Windows-Tirewail Windows-Tirewail	Den Dienst <u>beenden</u> Den Dienst <u>anhalten</u> Den Dienst <u>neu starten</u> Beschreibung: Provides SQL Server connection information to client computers.	G, Smartcard G, SMIP-Trap Softwarelizenzierung G, SQL Server (FASTVIEWER) G, SQL Server Active Directory Helper G, SQL Server VSS Writer G, SQL Server VSS Writer G, SSIP-Suche G, SSIP-Dienst G, Sperfetch G, Treifnnin Liefnnin	Verwaltet de Empfängt Tra Aktiviert das Provides stor Enables integ Provides 201 Provides 201 Verwaltet s Verwaltet s Rieter Telefn	SQL Server A
	Erweitert / standard /			1



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 <u>http://localhost/</u> 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)

Eigenschaft	ten von We	ebconferenceserver (FVWSL)
Allgemein	Anmelden	Wiederherstellung Abhängigkeiten
Anmelder	n als:	
⊖ Loka ⊡ D	les Systemko atenaustauso	onto ch zwischen Dienst und Desktop zulassen
O Diese	es Konto:	.\Administrator Durchsuchen
Kenn	wort:	•••••
Kenn	wort bestätig	en:
<u>Unterstüt</u> Dienst fü	<u>zung beim K</u> u	onfigurieren der Anmeldeoptionen für Benutzerkonten
Hardwa	areprofil	Dienst
Undoc	ked Profile	Aktiviert
Problemb	iehandlung m	hit Hardwareprofilen Aktivieren Deaktivieren
		OK Abbrechen Übernehmen



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 <u>http://portal.fastviewer.com</u>). Alternativ können Sie das Setup ebenfalls über folgenden Link beziehen: <u>http://portal.fastviewer.com/customerlicense/downloads/serverupdate32.zip</u>

(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 <u>http://localhost/admin</u> 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.asmx" ; 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	O-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
XmIProtocol	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. ; O=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 (fvw.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 stellten 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 Domänennamen (FQDN) oder die IP-Adresse des Servers.

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



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.

Aus	wertung von	01	.02.2009 00:00:00 -	bis 15	.03.2010 23:59:59	-		Anzeige Exportie	en ren
Kos	ten € / min. te Dianuramm	"Anzahl der See	0,00 ssions" Diagramm "Ag	zabi der Teilnehmer"					
Dra	g a column hear	der here to grou	ip by that column						
	Seriennu	Sitzungsn	Startzeit	Endzeit	Start-Info	Windows-Ben	Computername	Ende-Info	Ext. IP I
5	1711536949	27942	15.03.2010 12:10:09	15 03 2010 12:10:22		Fvwtwolf	wolfnc		

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)
- Fvw-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 <u>http://localhost/admin</u> ein.

🥭 Fast Viewer Server Admin - Wi	indows Internet Explorer bereitgestellt von Internet by FastViewer	_ 🗆 🗙
🔆 📀 🗢 🧭 http://localhost/ad	dmin 🔎 💌 🔄 🎸 🗙 🏉 FastViewer Server Admin 🗙	@ ☆ @
	FastViewer Server Admin	
» SYSTEM STATUS	Server status	
» CURRENT SESSIONS	Server information	
» CONNECTED CLIENTS	Version: 3.1.4224.15413 Session ID Range: 10000 - 99999	
» DATABASE STATUS	Network information	
» VIEW CONFIGURATION	Number of connections: U Direct: 0 HTTPS: 0	
	HTTP: 0 Packager clients: 0	
	Session overview Number of sessions: 0 Active: 0 Demo: 0 Number of clients: 0 Online REC elients: 0 Proxy Services: 0 Database status Data source: (local)/fastviewer /fastviewer	
	Last sync: 12.08.2011 09:42:33 Table: sessionlog Process information Working set: 54.468KB Working set maximum: 57.352KB .NET Memory: 5.443KB CPU Time: 00:00:11.3593750 Start time: 12.08.2011 11:42:19 Network throughput (send/recv Kilobytes/s): 0KBytes / 0KBytes	
	Server activated. Server is enabled [Disable s	erver]

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).



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. Mamme
Tanie. [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. <u>B</u> itlänge: 1024
Г <u>K</u> ryptografiedienstanbieter (CSP) für dieses Zertifikat auswählen
< <u>Z</u> urück <u>W</u> eiter > 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
< <u>Z</u> urück <u>W</u> eiter> 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 Inte ist, sollten Sie einen gültigen DNS-Namen verwenden. Falls der Server im Intranet können Sie den NetBIOS-Namen des Computers verwenden. Falls sich der gemeinsame Name (CN) ändert, benötigen Sie ein neues Zertifikat.	rmet tist,
Constitution (CNI)	
<u>d</u> emeinsamer Name (CN).	,
jans i .inredomain.com	
<u><</u> Zurück <u>W</u> eiter>	Abbrechen

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

IIS-Zertifikat-Assistent	×
Geographische Informationen	
Die Zertifizierungsstelle benötigt folgende geographische Informationen:	
Land/Region:	Т
	1
Bundesland/Kanton:	
]
<u>O</u> rt:	
]
Bundesland/Kanton und Ort müssen vollständige und offizielle Bezeichnungen sein un dürfen keine Abkürzung enthalten.	d
< <u>∠urück</u> <u>W</u> eiter> Ab	brechen



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

IIS-Zertifikat-Assistent	×
Name der Zertifikatanforderungsdatei	
Die Zertifikatanforderung wird als eine Textdatei unter dem von Ihnen angegebenen Namen gespeichert.	
Geben Sie einen Dateinamen für die Zertifikatanforderung ein.	
Dateiname:	
c:\certreq1 txt	D <u>u</u> rchsuchen
< <u>Z</u> urück <u>W</u> eit	er > Abbrechen

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".

IIS-Zertifikat-Assistent X
Ausstehende Zertifikatanforderung Eine ausstehende Zertifikatanforderung ist eine Anforderung, auf die die Zertifizierungsstelle noch nicht geantwortet hat.
Es gibt eine ausstehende Anforderung. Was möchten Sie tun?
Ausstehende Anforderung verarbeiten und Zertifikat installieren
O Ausstehende Anforderung Jöschen
< <u>∠</u> urück <u>W</u> eiter > Abbrechen

Danach geben Sie den Pfad Ihres Zertifikates an.

IIS-Zertifikat-Assistent	×
Ausstehende Anforderung verarbeiten	~
Ausstehende Zertifikatanforderung verarbeiten, indem die Datei ermittelt wird, die die Antwort der Zertifizierungsstelle enthält.	
Geben Sie den Pfad und den Namen der Datei ein, die die Antwort der Zertifizierungsstelle enthält.	
<u>P</u> fad und Dateiname:	
C:\fastviewer.cer	Durchsuchen
< <u>∠</u> urück <u>W</u> eite	er > Abbrechen



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)

IIS-Zertifikat-Assistent			×
SSL-Port Geben Sie den SSL-Port für diese Website an.			
SSL-Port, den diese Website verwenden soll:			
	< <u>Z</u> urück	<u>W</u> eiter ≻	Abbrechen

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".

Ausführe	en	? ×
-	Geben Sie den Namen eines Programms, Ordners, Dokuments oder einer Internetressource an.	
Öffnen:	mmc	•
	OK Abbrechen Durchsuche	:n

Es öffnet sich eine leere MMC.

The Konsole 1		_ D ×
Datei Aktion Ansicht Fayoriten	Eerster 2	
+ → 🔟 🗟 😫 🖬		
The Konsolenstamm		
Konsolenstamm	Nane	
	In dieser Ansicht werden keine Elemente angezeigt.	



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

Konsole1			- 🗆 ×
Datei Aktion Ansicht Fayoriten Eer	nster <u>?</u>		
Neu Str	rg+N		
Speichern Str	rg+0 ra+5		
Speichern unter	, , , , , , , , , , , , , , , , , , ,		
Snap-In hinzufügen/entfernen Str Optionen	rg+M	In dieser Ansicht werden keine Elemente angezeigt.	
<u>1</u> C:\WINDOWS\\compmgmt.msc <u>2</u> C:\WINDOWS\system32\secpol.msc			
Beenden			
, , , , , , , , , , , , , , , , , , ,			
1		J] ///	

Es öffnet sich folgendes Fenster:

Snap-In hinzufügen	n/entfernen ?	×
Eigenständig Erwe	eiterungen	
Verwenden Sie die: zu entfernen oder	se Seite, um ein eigenständiges Snap-In von der Konsole hinzuzufügen.	
<u>S</u> nap-Ins in:	Konsolenstamm 💌 💼	
Beschreibung		
	Entremen L <u>D</u> ro	
	OK Abbrechen	



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

Eigenständiges Snap-In hinzufügen		? ×		
Verfügbare eigenständige Snap-Ins:				
Snap-In	Anbieter			
🧊 Sicherheitsvorlagen	Microsoft Corporation			
SQL Server Configuration Manager	Microsoft Corporation			
😽 Telefonie	Microsoft Corporation			
🖳 Terminaldienstekonfiguration	Microsoft Corporation			
🔓 Verteiltes Dateisystem (DFS)	Microsoft Corporation			
Mechselmedienverwaltung	Microsoft Corporation			
🐐 🖓 WMI-Steuerung	Microsoft Corporation			
🗃 Zertifikate	Microsoft Corporation			
🗱 Zertifikatvorlagen	Microsoft Corporation			
📴 Zertifizierungsstelle	Microsoft Corporation	-		
Beschreibung				
Zertifikatspeicher, eines Dienstes oder ei	ines Computers.			
[Hinzufügen Schlie	:Ben		

Wählen Sie "Computerkonto".

Zertifikat-Snap-In	X
Dieses Snap-In verwaltet die Zertifikate für:	
C Eigenes Benutzerkonto	
C <u>D</u> ienstkonto	
Computerkonto	
	< <u></u> ∠gurück <u>W</u> eiter > Abbrechen



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

Computer auswählen
Wählen Sie den Computer aus, den dieses Snap-In verwalten soll. Dieses Snap-In verwaltet: © Lokalen Computer (Computer, auf dem diese Konsole ausgeführt wird)
<u>Anderen Computer:</u> <u>Durchsuchen</u>
Änderungen zulassen, wenn die Konsole von der Befehlszeile aus aufgerufen wird. Dies gilt nur, wenn die Konsole zuvor gespeichert wurde.
< <u>Z</u> urück Fertig stellen Abbrechen

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

Snap-In hinzufügen/	'entfernen	? ×
Eigenständig Erweit	rerungen	
Verwenden Sie diese zu entfernen oder h	e Seite, um ein eigenständiges Snap-In von der Kor inzuzufügen.	nsole
<u>S</u> nap-Ins in:	🔁 Konsolenstamm 💌	
🗐 Zertifikate (Lok	aler Computer)	
Beschreibung		
Hinzufügen	Entfernen I <u>n</u> fo	
	OK Abb	rechen



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".

🚡 Konsole1				
Datei Aktion Ansicht Favoriten Eenster ?				
🚡 Konsolenstamm\Zertifikate (Lo	kaler Computer)\Eigene Zertifikate\	Zertifikate		
Consolenstamm	Ausgestellt für 🔺	Ausgestellt von	Gültig bis	Beabsichtigte Zv
E-1 Zertifikate (Lokaler Computer) Eigene Zertifikate Zertifikate Zertifikate	Fastviewer2.fastviewer.com Öffnen Alle Aufnahen	VeriSign Trial Secure Server Test CA	04.07.2008	Serverauthentif
vertrauenswurdige Stammz vertrauenswurdige Stammz one Divertrauen vertrauenswurdige Ze Divertraute Herausgeber Divertraute Herausgeber Divertraute Herausgeber Divertraute Herausgeber	Ausschneiden Kopieren Löschen	Exportieren		
Vertrauenswürdige Persone Zertifikatregistrierungsanfo SPC	Eigenschaften Hilfe			
Der Speicher "Eigene Zertifikate" enthält	1 Zovříříkat			

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

Zertifikatexport-Assistent	×
Privaten Schlüssel exportieren Sie können den privaten Schlüssel mit dem Zertifikat exportieren.	
Private Schlüssel sind kennwortgeschützt. Wenn Sie den privaten Schlüssel mit dem ausgewählten Zertifikat exportieren möchten, müssen Sie auf einer der folgenden Seiten ein Kennwort eingeben.	
Möchten Sie mit dem Zertifikat auch den privaten Schlüssel exportieren?	
Da, privaten Schlüssel exportieren	
C Nein, privaten Schlüssel nicht exportieren	
< <u>Z</u> urück <u>W</u> eiter > Abbrecher	



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

ertifikatexport-Assistent
Exportdateiformat Zertifikate können in verschiedenen Dateiformaten exportiert werden.
Wählen Sie das gewünschte Format:
C DER-codiert-binär X.509 (.CER)
C Base-64-codiert X.509 (,CER)
C Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)
🔲 We <u>n</u> n 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
< <u>Z</u> urück <u>W</u> eiter > 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.

rtifi	katexport-Assistent
Ke	nnwort
	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:
	•
	< <u>Z</u> urück <u>W</u> eiter > Abbrechen



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

ertifikatexport-Assistent		
Exportdatei Geben Sie die den Namen der zu export	tierenden Datei an.	
Dateiname:		
C:\x2.ptx	Durchsuchen	
	< Zurück Weiter > Abbreche	'n

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.

🚡 Konsole1				
Datei Aktion Ansicht Fayoriten Eenster 2				
🕞 Konsolenstamm\Zertifikate (Lo	kaler Computer)\Figene Zertifikate	Zertifikate		
Konsolenstamm	Ausgestellt für 🔺	Ausgestellt von	Gültig bis	Beabsichtigte Zv
🛓 🗄 🐻 Zertifikate (Lokaler Computer)	Fastviewer2.fastviewer.com	VeriSign Trial Secure Server Test CA	04.07.2008	Serverauthentif
Eigene Zertifikate				
Alle Aufgaben	▶ Importieren			
Unternel Ansicht	*			
Zwischer Neues Fenster				
Nicht ver Neue Aufgaber	nblockansicht			
Drittanbi Aktualisieren				
Vertraue Liste exportiere	en			
	•			•
Fügt einem Speicher ein Zertifikat hinzu.				10

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



Zertifikatimport-Assistent	×
Zertifikatspeicher	
Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert	
Windows kann automatisch einen Zertifikatspeicher auswählen oder Sie können einen Pfad für die Zertifikate angeben.	
\bigcirc Zertifikatspeicher automatisch auswählen (auf dem Zertifikatstyp basierend)	
Alle Zertifikate in folgendem Speicher speichern	
Zertifikatspeicher:	
Eigene Zertifikate Durchsuchen	
	_
< <u>Z</u> urück <u>W</u> eiter > Abbrechen	

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".

Zertifikat	?	×
Allgemein Details Zertifizierungspfad		1
Zertifikatinformationen		
Windows hat keine ausreichenden Informationen, um dieses Zertifikat verifizieren zu können.		
Ausgestellt für: fastviewer1.fastviewer.com	-	
Ausgestellt von: VeriSign Trial Secure Server Test CA		
Gültig von 19.06.2008 bis 04.07.2008		
\mathscr{P} Sie besitzen einen privaten Schlüssel für dieses Zertifikat.		
Ausstellererklärung		
OK		



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:

🎊 fastviewe	r Certificate Installer	_OX
S	SL certificate installer	V1.1
IP Address		•
Certificate	please select a certificate first	
Fingerprint		
Clear all	Select cert Remove cert	İnstali cert

IP Adress: 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 angebundenen Zertifikate können Sie sich über den Befehl "httpcfg query ssl" (im Verzeichnis des Tunnelservers) ausgeben lassen:

ex C:\WINDOWS\system32\cmd.exe		
C:\Programme\TunnelserverU3) IP Hash Guid CertStoreName CertCheckMode RevocationFreshnessTime UrlRetrievalTimeout SslCt1Identifier SslCt1StoreName Flags	httpcfg query ssl : 192.168.2.115:443 : a291ddf521f2c19f6ea422272f aec665ccfea 6 : (841f64d3-63eb-4dde-ba9d-c40186027f61) : (null) : 0 : 0 : 0 : (null) : (null) : (null) : (null) : 0	
IP Hash Guid CertStoreName CertCheckMode RevocationFreshnessTime UrIRetrievalTimeout SslCtlIdentifier SslCtlStoreName Flags	<pre>: 192.168.2.116:443 : 6b a ff76914735125bbbf83f3c2 b4310bb2fc9 : (841f64d3-63eb-4dde-ba9d-c40186027f61) : (null) : 0 : 0 : 0 : 0 : (null) : (null) : (null) : (null) : 0</pre>	
C:\Programme\TunnelserverV3>		_



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 <u>support@FastViewer.com</u> 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 (<u>http://servername/</u>) und von Außerhalb (<u>http://DNS-Name/</u>) 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



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 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



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