



Die mobile Kanzlei Vor-Ort-Einsatz mit BiG-Manager unter Microsoft Windows Terminal Server über eine UMTS-VPN-Verbindung ins Firmennetzwerk

Aktualisierungen dieses Artikels

01.02.2008	27.02.2008	18.06.2008			
------------	------------	------------	--	--	--

Hinweise zu BiG-Manager®

BiG-Manager® ist eine Anwendung, die ausschließlich auf Microsoft Office Access 2003 basiert. Es werden ausschließlich Microsoft-Komponenten verwendet. Lediglich für die Datenkomprimierung werden zwei ActiveX-Komponenten des Produkts Dynazip Max Secure 6.0 (Inner Media, USA) verwendet. Alle BiG-Manager-Funktionalitäten basieren auf Microsoft VBA-Projekten. Die GEWIDOR GmbH hat das Produkt Visual Studio Tools für Microsoft Office System Version 2003 käuflich erworben. Mit dem Erwerb ist das Recht verbunden, Microsoft Office Access 2003 Runtime lizenzgebührenfrei an Kunden weiterzugeben.

Vorbemerkungen

Wirtschaftsprüfer sind häufig vor Ort bei ihren Mandanten tätig. Die firmeninternen Ressourcen stehen dann i. d. R. nicht zur Verfügung.

Eine Anbindung der mobilen Mitarbeiter an das Firmennetzwerk ist wünschenswert und kann zu erheblichen Kosteneinsparungen führen. Z. B. könnten Fahrten von Mandanten zurück in die Kanzlei auf ein Minimum reduziert werden, wenn relevante Dokumente zur Ansicht oder Bearbeitung vor Ort verfügbar wären.



Die Lösung ist eine VPN-Verbindung (Virtual Private Network) zwischen Notebook und Firmennetzwerk über UMTS.

Alle im Firmennetzwerk verfügbaren Ressourcen (Software-Applikationen, Interne Dokumente, Jahresabschlüsse anderer Mandate, ...) können so von Notebooks der Mitarbeiter genutzt werden. Die Teamarbeit zwischen Partnern, Prüfungsleitern, Prüfern und Assistenten wird effektiv und flexibel.

Dieser Artikel soll Ihnen zeigen, welche Voraussetzungen erforderlich sind, um den Zugang zu Ihrem Firmennetzwerk zu ermöglichen. Außerdem erhalten Sie Hinweise zur Nutzung der Anwendung BiG-Manager in einer derart vernetzten Arbeitsumgebung.

Projektbeschreibung und Ergebnis

Die GEWIDOR GmbH hat mit freundlicher Unterstützung der E-Plus Mobilfunk GmbH & Co. KG im Januar 2008 eine Arbeitsumgebung geschaffen und 2 Wochen intensiv für ihre Kunden getestet. Die VPN-Verbindung über die UMTS Notebook Card von E-Plus war während der gesamten Testdauer stabil. Die Kommunikation zwischen Firmennetzwerk und Notebook erfolgte mit einem sehr guten Laufzeitverhalten.

Technische Details:

Hardware	Software
E-PLUS UMTS PC-Notebook-Card	Huawei Technologies Hosta 03.11.00.01.06.52
Siemens Convertible T4010	Windows XP Tablet PC Edition 2005
Fujitsu Siemens Server Primergy TX 200	Windows Server 2003 R2
SOHO 6 Watchguard	SOHO 6 Version 6.4.1 (25.03.2005 Build 15) Boot ROM 5.6
	Mobile User VPN-Client (Watchguard Version 10.3.5 (Build 6))

Ressourcen

<http://www.eplus.de>

http://download.microsoft.com/.../terminalserveroverview_ge.doc

<http://www.watchguard.com>

<http://www.gewidor-gmbh.de>

Microsoft Office ist ein eingetragenes Warenzeichen der Microsoft Corporation in den USA und/oder anderen Ländern. BiG-Manager ist ein eingetragenes Warenzeichen der GEWIDOR GmbH, Leverkusen.



Die mobile Kanzlei Vor-Ort-Einsatz mit BiG-Manager unter Microsoft Windows Terminal Server über eine UMTS-VPN-Verbindung ins Firmennetzwerk

Windows Terminal Server, VPN

Microsoft Windows Terminal Server stellt Dienste zur Verfügung, mit denen lokale Computer z. B. Anwendungsprogramme auf dem Server ausführen zu können. Auf dem lokalen Computer sind dabei keinerlei Komponenten der Anwendungssoftware installiert. Der Terminal Server überträgt im Wesentlichen nur Bildschirminhalte auf den lokalen Computer und empfängt Maus- und Tastaturereignisse. Eine Terminal Server-Sitzung unterscheidet sich für den Benutzer nicht von einer Arbeitssitzung, die er mit lokal installierter Software ausführen würde.

Kostenreduzierung mit Microsoft Windows Terminal Server über VPN



Teamwork

- ▶ Kollegen in der Kanzlei können am selben Datenbestand arbeiten, der auch von Kollegen vor Ort bearbeitet wird.
- ▶ Der Aufbau eines PTP-Netzwerkes vor Ort entfällt.
- ▶ Das Help Center der GEWIDOR GmbH kann auch vor Ort genutzt werden.
- ▶ Prüfungsleiter können Dokumente online durchsehen und bearbeiten, auch wenn Sie nicht vor Ort sind.
- ▶ Vor Ort können Dokumente anderer Mandate eingesehen und bearbeitet werden, wenn Kollegen diese Daten in der Kanzlei bearbeiten.



Technik

- ▶ Der lokale Arbeitsplatz (Client) kann kostengünstig sein, denn die eigentliche Verarbeitung der Daten findet auf dem entfernten (Remote) Computer statt.
- ▶ Bei Ausfall, Diebstahl oder Virenbefall des Endgerätes gehen keine Daten verloren.
- ▶ Der TCO (Total Cost of Ownership) sinkt bei großen Installationen erheblich.
- ▶ Die Software muss nur einmal auf dem Terminalserver installiert werden.
- ▶ An den lokalen PC-Systemen müssen keine Veränderungen vorgenommen werden.
- ▶ Der Wartungsaufwand verlagert sich auf das zentrale System. Eine zentrale Änderung betrifft jeden Client. Allerdings gilt anzumerken, dass es auch intelligente Server-Client-Konzepte gibt, die diesen Ansprüchen ebenfalls gerecht werden.

Zur Verwendung von Microsoft Windows Terminal Server werden Lizenzen für die Arbeitsplätze benötigt. Es wird empfohlen je einen Terminal Server für 5 Arbeitsplätze zu verwenden.

WatchGuard Firewall, VPN-Client

Bei der GEWIDOR GmbH wird eine Firewall der Firma WatchGuard Technologies, USA eingesetzt. Zu dieser Firewall wird eine Software (VPN-Client) zur Verfügung gestellt, die auf den lokalen Computern (Clients) installiert wird und über eine verschlüsselte Verbindung Zugriff auf das Netzwerk hinter der Firewall ermöglicht.

E-Plus UMTS Notebook Card

VPN-Verbindungen werden i. d. R. über das Internet hergestellt. Der mobile Arbeitsplatz muss daher eine Internetverbindung herstellen können. Die UMTS Notebook Card wird mit dem Computer verbunden. Sie kann Internetverbindungen über die Standards GPRS/GSM oder UMTS herstellen.

Bei bestehender Internetverbindung stellt die VPN-Client-Software eine sichere Verbindung zum Firmennetzwerk her. Danach kann die Microsoft Windows Terminal Server-Sitzung gestartet werden.



Die mobile Kanzlei Vor-Ort-Einsatz mit BiG-Manager unter Microsoft Windows Terminal Server über eine UMTS-VPN-Verbindung ins Firmennetzwerk

Screenshots

Internetverbindung herstellen

Der Mobilfunkanbieter liefert die UMTS-Karte und eine Verbindungssoftware. Die UMTS-Karte befindet sich in einem PCMCIA-Slot. Die Verbindungssoftware wurde gestartet und zeigt eine ausreichende Signalstärke an.



Um eine VPN-Verbindung zum eigenen Server im Büro herzustellen, ist eine VPN-Clientsoftware erforderlich, die nach Herstellung der Internetverbindung die Verbindung zum Server herstellt.

Nach Verbindungsaufbau ist das entfernt genutzte Notebook bereits im firmeneigenen Netzwerk registriert. Die Verbindung ist sicher, da die VPN-Clientsoftware jeglichen Informationsaustausch zwischen Notebook und Server über das Internet verschlüsselt.



Die Abbildung zeigt den Verbindungsstatus bei Verwendung der Software ‚Watchguard Mobile User VPN Client‘, die für Tests von der GEWIDOR GmbH verwendet wurde.



Die mobile Kanzlei Vor-Ort-Einsatz mit BiG-Manager unter Microsoft Windows Terminal Server über eine UMTS-VPN-Verbindung ins Firmennetzwerk

Mit Firmennetzwerk verbinden

Die Verbindung mit den im Büro verfügbaren Ressourcen erfolgt hier über die Windows-Remotedesktopverbindung, mit der der Benutzer sich am Windows-Terminal-Server anmeldet. In diesem Fall wird eine Verbindung zum Server 192.168.1.2 (dem Terminal-Server) hergestellt.

Die weiteren Schritte unterscheiden sich nicht von der Verwendung der Windows-Terminal-Dienste auf einem lokalen Computer im Büro über das firmeneigene Netzwerk (LAN=Local Area Network).

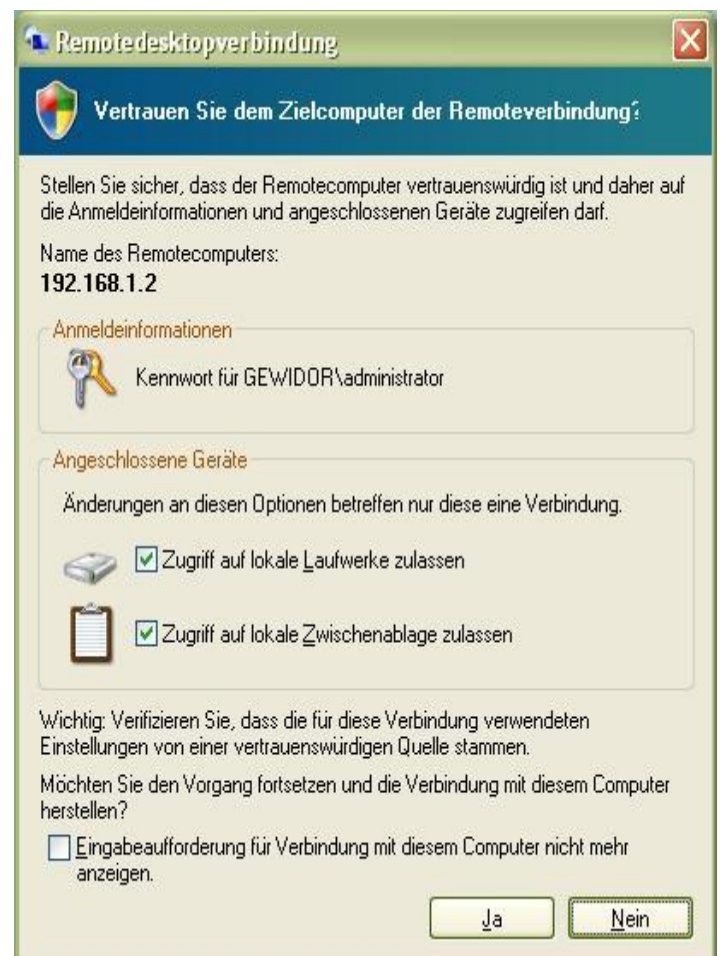


Die Anmeldung am Terminal-Server erfolgt wie gewohnt mit Benutzername und Kennwort.



Wurden der Zugriff auf die lokalen Laufwerke des Notebooks in der Remotedesktopverbindung konfiguriert, erscheint die nebenstehende Sicherheitswarnung.

Der Zugriff auf lokale Laufwerke ermöglicht die Dateiübertragung vom Server auf das über UMTS verbundene Notebook. Damit können Dokumente vom Server auf das Notebook übertragen werden.

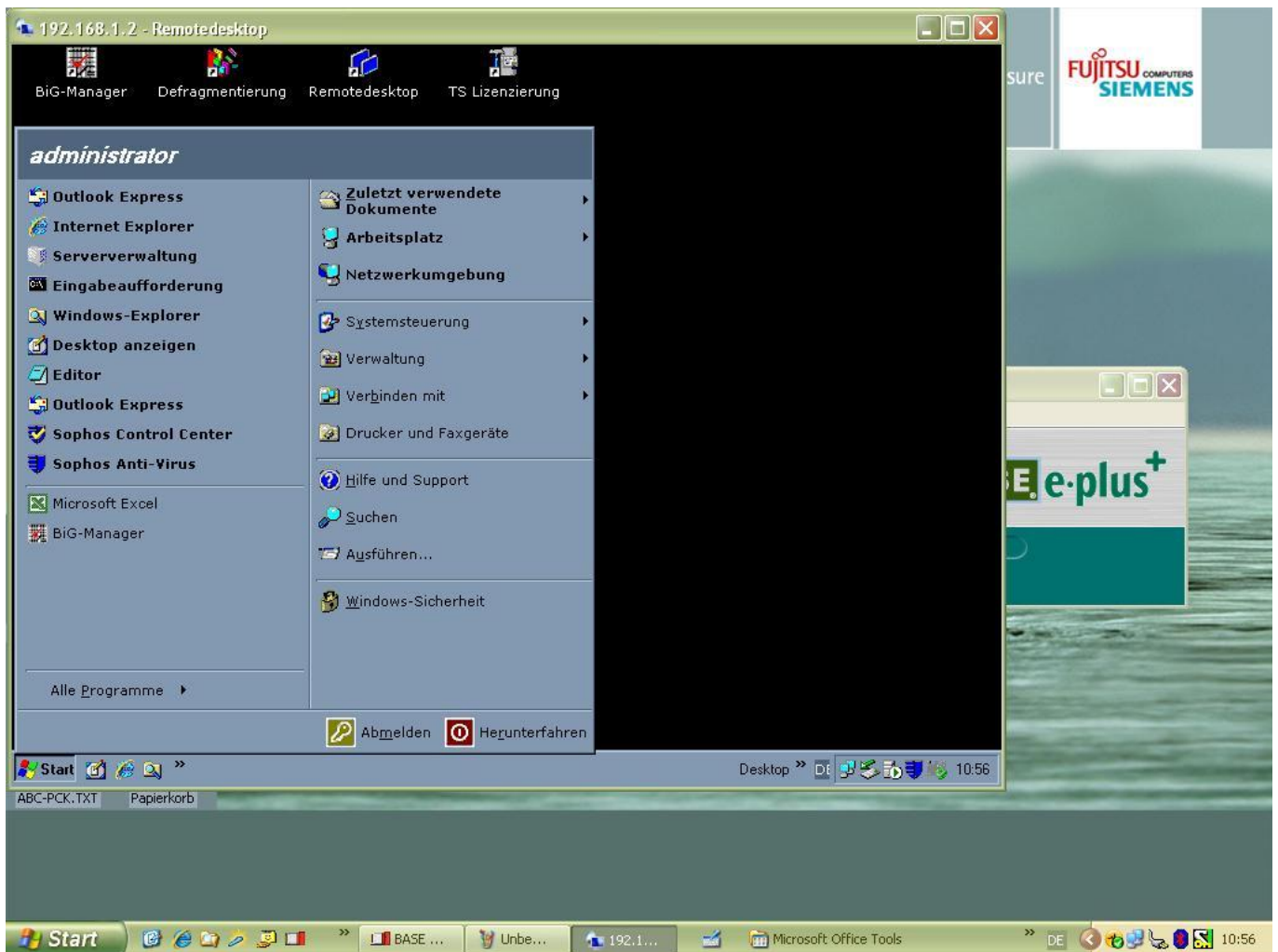




Die mobile Kanzlei Vor-Ort-Einsatz mit BiG-Manager unter Microsoft Windows Terminal Server über eine UMTS-VPN-Verbindung ins Firmennetzwerk

Die Grafik zeigt den Bildschirm des Notebooks nach erfolgreicher Anmeldung am Server. Nun stehen alle Anwendungsprogramme und Daten des Servers zur Verwendung bereit.

Insbesondere können nun auch Daten vom entfernt stehenden Notebook gemeinsam mit Kollegen bearbeitet werden, die sich im Büro befinden. Der bei Wirtschaftsprüfern häufig auftretende Vor-Ort-Einsatz beim Mandanten erlaubt also damit den Zugriff auf die eigenen Netzwerkressourcen im Büro.



In der Remotedesktopverbindung wurde der Zugriff auf die lokalen Laufwerke und die Zwischenablage konfiguriert. Im Windows-Explorer auf dem Terminalserver erscheint der über UMTS verbundene Computer unter **C auf SiemensT4010** (=Computernamen des Notebooks). Dateien können nun vom Server auf das Notebook übertragen werden.

Für BiG-Manager steht eine besondere Funktion unter Datenbank -> eMail-Anlagen, ZIP-Sicherung' zur Verfügung, mit der ganze Firmendatenbestände vom Server auf das Notebook übertragen werden können (s. Abschnitt ,Datenübertragung WTS -> Notebook).

Die Übertragung kann jedoch erhebliche Zeit in Anspruch nehmen, wenn alle Daten, auch die Vorjahresarchive übertragen werden. Es wird daher empfohlen, beim Verlassen des Büros alle evtl. weiter benötigten Datenbestände über die Netzwerkverbindung auf das Notebook zu übertragen.



Die mobile Kanzlei Vor-Ort-Einsatz mit BiG-Manager unter Microsoft Windows Terminal Server über eine UMTS-VPN-Verbindung ins Firmennetzwerk

Terminal Server-Sitzung starten

Windows Terminal Server-Sitzungen werden über die Remotedesktopverbindung (Bestandteil von Microsoft Windows XP, Vista) gestartet.

192.168.1.2 gibt die IP-Adresse des Terminalservers an.

Die Herstellung einer Verbindung wird i. d. R. so konfiguriert, dass sich ein Benutzer mit Benutzername und Kennwort am Netzwerk anmelden muss.





Die mobile Kanzlei Vor-Ort-Einsatz mit BiG-Manager unter Microsoft Windows Terminal Server über eine UMTS-VPN-Verbindung ins Firmennetzwerk

Einstellungen

Einstellung der Remotedesktopverbindung

UMTS-Verbindungen haben eine theoretische Übertragungsrate von ca. 48 KB/s (384 KBit/s). Dies ist jedoch gegenüber einer LAN-Verbindung im firmeneigenen Netzwerk mit 100 MBit/s bzw. 1 GBit/s langsam.

Ein optimiertes Laufzeitverhalten ergibt sich, wenn die folgenden Einstellungen der RDP-Verbindung (Remote Desktop Protocol) mit dem Windows Terminal Server vorgenommen werden.



Die mobile Kanzlei Vor-Ort-Einsatz mit BiG-Manager unter Microsoft Windows Terminal Server über eine UMTS-VPN-Verbindung ins Firmennetzwerk

Eine höhere Farbtiefe verringert die Übertragungsrates.

Eine Farbtiefe von 256 Farben sollte nicht verwendet werden, da dies zu erheblichen Problemen bei der Darstellung von Symbolen und Hintergrundfarben führt. Davon betroffen sind nahezu alle Anwendungen, auch BiG-Manager.



„Drucker“ muss aktiviert werden, wenn ein Drucker am lokalen Computer verwendet werden soll.





Die mobile Kanzlei Vor-Ort-Einsatz mit BiG-Manager unter Microsoft Windows Terminal Server über eine UMTS-VPN-Verbindung ins Firmennetzwerk

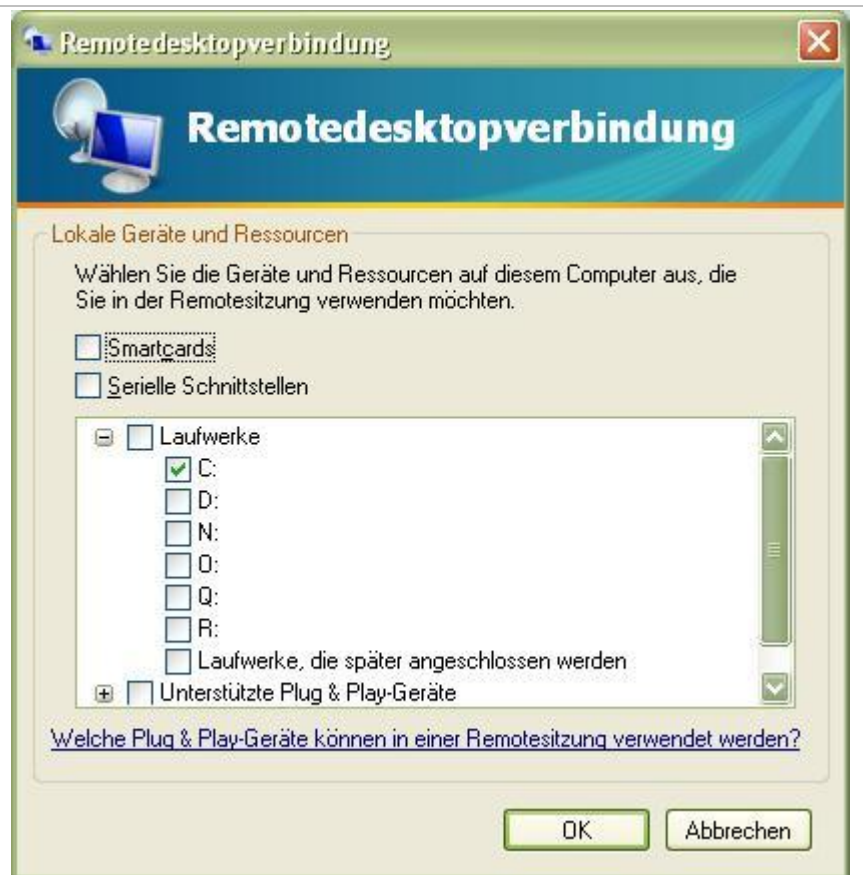
Um Daten vom Firmennetzwerk auf den lokalen Computer zu übertragen, muss die Festplatte des lokalen Computers unter ‚Lokale Geräte und Ressourcen‘ angegeben werden.

Der lokale Computer wird dabei auf dem Terminal Server dargestellt als

C auf SiemensT4010
(=Festplatte auf Computernamen).

Wenn Ihr lokaler Sicherungsordner die empfohlene Bezeichnung JAP-BACKUP für Datenbanksicherungen besitzt, lautet die Ordnerangabe

\\tsclient\C\JAP-BACKUP



Optional





Die mobile Kanzlei
Vor-Ort-Einsatz mit BiG-Manager
unter Microsoft Windows Terminal Server
über eine UMTS-VPN-Verbindung ins Firmennetzwerk



Die mobile Kanzlei Vor-Ort-Einsatz mit BiG-Manager unter Microsoft Windows Terminal Server über eine UMTS-VPN-Verbindung ins Firmennetzwerk

Bitmapzwischenspeicherung sollte immer aktiviert sein.

Jede weitere Option geht zu Lasten der Übertragungsrate, d. h. der Geschwindigkeit mit der Bildschirmanzeigen auf dem lokalen Computer erfolgen..



Optional





Die mobile Kanzlei Vor-Ort-Einsatz mit BiG-Manager unter Microsoft Windows Terminal Server über eine UMTS-VPN-Verbindung ins Firmennetzwerk

Datenübertragung WTS -> Notebook

I. d. R. ist eine Datenübertragung eines vollständigen Firmendatenbestandes aus einer Microsoft Windows Terminal-Server-Sitzung auf den lokalen Computer mit erhöhtem Zeitaufwand verbunden und nur dann erforderlich, wenn ein aktueller Datenbestand an einem Ort benötigt wird, an dem eine UMTS-Verbindung wegen baulicher oder geographischer Gegebenheiten nicht hergestellt werden kann.

Wenn Sie jedoch von einem Standort mit UMTS-Verbindung zu einem anderen Standort ohne Verbindungsmöglichkeit wechseln müssen und die lokal gespeicherten Daten nicht mehr aktuell sind, gehen Sie wie folgt vor:

Geben Sie den lokalen Sicherungsordner in der auf dem WTS gestarteten Anwendung ein.

Ort	eMail-Anlagen, ZIP-Sicherung, -> Register Ordner für Speicherungen verwalten
Eintrag	\\tsclient\C\JAP-BACKUP

The screenshot shows the 'eMail - Anlagen, ZIP-Sicherung, Sicherungsordner, ...' window. It includes fields for 'Mandant' (9999980) and 'Firmenbezeichnung' (BiG-GmbH, Leverkusen). The 'Hinweise zu Ordnern ...' section provides instructions on folder naming and usage. The 'Empfohlene Namensgebungen für Standardordner ...' section lists 'JAP-BACKUP' and 'JAP-MAILING'. The 'Ordner, Freigaben ...' section shows a list of folders, with '1. Ordner' set to 'D:\DATA\JAP-BACKUP'. The 'Duplikateordner verwenden' checkbox is checked, and the path '\\tsclient\C\JAP-BACKUP' is entered. The 'Alternative eMail - Adresse' field contains 'gewidor_gmbh@t-online.de'.



Die mobile Kanzlei Vor-Ort-Einsatz mit BiG-Manager unter Microsoft Windows Terminal Server über eine UMTS-VPN-Verbindung ins Firmennetzwerk

Starten Sie eine Dateiübertragung auf den lokalen Computer über

Ort	eMail-Anlagen, ZIP-Sicherung, -> eMail-Anlagen erzeugen, ZIP-Sicherung
Schaltfläche	Datensicherung ...

Die Firmendaten werden zunächst im komprimierten Format auf dem Microsoft Windows Terminal Server im Ordner d:\data\jap-backup gesichert. Da die Option ‚Duplikat erzeugen‘ aktiviert ist, werden diese Daten anschließend in den Ordner \\tsclient\c\jap-backup kopiert, der sich auf dem lokalen Computer befindet.

The screenshot shows the 'eMail - Anlagen, ZIP-Sicherung, Sicherungsordner, ...' window. It features a sidebar with navigation icons for 'Datenaustausch mit eMail-Anlage' and 'ZIP - Sicherung'. The main area is divided into sections: 'Mandant' (9999980) and 'Firmenbezeichnung' (BiG-GmbH, Leverkusen); 'eMail-Versandoptionen' with radio buttons for 'Mit Neutralisierung...' and 'Ohne Neutralisierung...', and checkboxes for including documents, archives, and HTML indexes; 'Informationen' showing the current folder 'D:\DATA\JAP-BACKUP'; 'ZIP-Sicherung+Duplikat' with a checked 'Duplikat erzeugen' option; and 'eMail-Versand, Upload' with buttons for 'Mittteilung an Empfänger', 'Aufbereiten für Versand', and 'eMail - Anlagen löschen'. A status bar at the bottom shows 'Ordnerinhalte anzeigen...' and 'Beenden'.

Die Dateiübertragung erfolgt über die UMTS-Verbindung. Aus Laufzeitgründen sollte unbedingt darauf geachtet werden, dass alle Vorjahresarchive eines Datenbestandes komprimiert sind. Die Werte wurden von der GEWIDOR GmbH am Standort Leverkusen gemessen.

Datenvolumen	Übertragungszeit	Übertragungsrate	% Übertragungsrate UMTS 384 KBit/sec
pro 1 MB	21 sec	48 KB/sec	100 (nicht erreichbar)
	25 sec	40 KB/sec	83 (sehr günstige Umstände)
	34 sec	30 KB/sec	63 (normaler Tagesbetrieb)
	51 sec	20 KB/sec	42 (in seltenen Spitzenzeiten)

Ein realer Datenbestand mit 5 besetzten Archive (Abschlüsse aus insgesamt 7 Jahren) umfasst als ZIP-Sicherung ca. 24 MB und benötigt daher eine Übertragungszeit von ca. 14 min bei 35 KB/sec.



Anhang

Die beschriebenen Konfigurationen beziehen sich auf die Testumgebung der GEWIDOR GmbH. Dabei wurde eine Lösung gewählt, bei der kostenlose Komponenten der Firma WatchGuard Inc., USA verwendet wurden.

WatchGuard Firewall-Konfiguration

Der Mobile User VPN-Client von WatchGuard kann mit einer dynamisch zugewiesenen IP-Adresse des Servers im Firmennetzwerk arbeiten. Diese Art der Identifikation des Servers spart Kosten, da keine feste IP-Adresse bei einem Provider beauftragt werden muss. Die Adressierung erfolgt über DynDNS (dynamischer Domain-Name-System-Eintrag).

Eintrag der vom Betreiber zugewiesenen Domain.

WatchGuard Configuration Settings - Microsoft Internet Explorer

http://192.168.1.5/dyndns.htm

WatchGuard Configuration Settings

WG WatchGuard

SOHO 6 Configuration LiveSecurity | Help | Support | About Us | Contact Us

System Status
Network
External
Trusted
Optional
Routes
Dual ISP
Network Statistics
DynamicDNS
Administration
System Security
VPN Manager Access
Update
Upgrade
View Configuration File
Firewall
Incoming
Outgoing
Custom Service
Blocked Sites
Firewall Options
Pass Through
Logging
WSEP Logging
Syslog Logging
System Time
WebBlocker
VPN

Network
Dynamic DNS client
Information about Dynamic DNS available [here](#)

Enable Dynamic DNS client

Domain

Name

Password

http://www.watchguard.c Lokales Intranet 75%



Die mobile Kanzlei Vor-Ort-Einsatz mit BiG-Manager unter Microsoft Windows Terminal Server über eine UMTS-VPN-Verbindung ins Firmennetzwerk

Zuweisung der im Firmennetzwerk verwendeten IP-Adresse des Computers, der über UMTS verbindet

WatchGuard Configuration Settings - Microsoft Internet Explorer

http://192.168.1.5/vpnsvr.htm?MU... Live Search

WatchGuard Configuration Settings

WatchGuard SOHO 6 Configuration LiveSecurity | Help | Support | About Us | Contact Us

System Status
Network
External
Trusted
Optional
Routes
Dual ISP
Network Statistics
DynamicDNS
Administration
System Security
VPN Manager Access
Update
Upgrade
View Configuration File
Firewall
Incoming
Outgoing
Custom Service
Blocked Sites
Firewall Options
Pass Through
Logging
WSEP Logging
Syslog Logging
System Time
WebBlocker
VPN

VPN
MUVPN Clients

User	Assigned IP
UMTS-VPN	192.168.1.212

Add... Edit... Remove

Common MUVPN Client Settings
The following settings apply to all MUVPN clients.

Make the MUVPN client security policy read-only.

Virtual Adapter Preferred

DNS Server Address 192.168.1.2 [optional]

WINS Server Address 192.168.1.2 [optional]

Submit Reset

Lokales Intranet 75%



Die mobile Kanzlei Vor-Ort-Einsatz mit BiG-Manager unter Microsoft Windows Terminal Server über eine UMTS-VPN-Verbindung ins Firmennetzwerk

Angaben zur Verschlüsselung der Verbindung und zu Verschlüsselungsalgorithmen

WatchGuard Configuration Settings - Microsoft Internet Explorer

http://192.168.1.5/cfgmuvpn.htm? Live Search

WatchGuard Configuration Settings

WatchGuard **SOHO 6 Configuration** LiveSecurity | Help | Support | About Us | Contact Us

System Status
Network
External
Trusted
Optional
Routes
Dual ISP
Network Statistics
DynamicDNS
Administration
System Security
VPN Manager Access
Update
Upgrade
View Configuration File
Firewall
Incoming
Outgoing
Custom Service
Blocked Sites
Firewall Options
Pass Through
Logging
WSEP Logging
Syslog Logging
System Time
WebBlocker
VPN

VPN > MUVPN Clients
Edit MUVPN Client

User Name UMTS-VPN
Shared Key qx27p15
Virtual IP Address 192.168.1212
Authentication Algorithm MD5-HMAC
Encryption Algorithm DES-CBC
VPN Client Type Mobile User
 All traffic uses tunnel (0.0.0.0 IP Subnet)

Submit Reset Cancel

Fertig Lokales Intranet 75%



Die mobile Kanzlei Vor-Ort-Einsatz mit BiG-Manager unter Microsoft Windows Terminal Server über eine UMTS-VPN-Verbindung ins Firmennetzwerk

Generierung der Konfigurationsdatei für die Client-Software

WatchGuard Configuration Settings - Microsoft Internet Explorer

http://192.168.1.5/vpn.htm

Live Search

WGC

SOHO 6 Configuration

LiveSecurity | Help | Support | About Us | Contact Us

VPN

Remote Gateways

Remote Gateway Support Not Installed. [Upgrade](#)

You must upgrade your WatchGuard SOHO 6 to enable remote gateway support.

MUVPN Clients

MUVPN Clients 1 configured (5 external) [Configure](#)

Secure MUVPN Client Configuration Files

The following secure (encrypted) MUVPN client configuration (.wgx) files are available for download. Once downloaded, these files can be used to configure your MUVPN client software in a manner that is consistent with the currently defined MUVPN settings on the SOHO6.

Client Name	MUVPN Client Configuration Files
UMTS-VPN	UMTS-VPN.wgx

[Regenerate IP Sec Keys](#)

[View VPN Statistics](#)

Lokales Intranet 75%



Die mobile Kanzlei Vor-Ort-Einsatz mit BiG-Manager unter Microsoft Windows Terminal Server über eine UMTS-VPN-Verbindung ins Firmennetzwerk

Öffnen der Firewall für eingehenden Datenverkehr über IPSec (Internet Protocol Security)

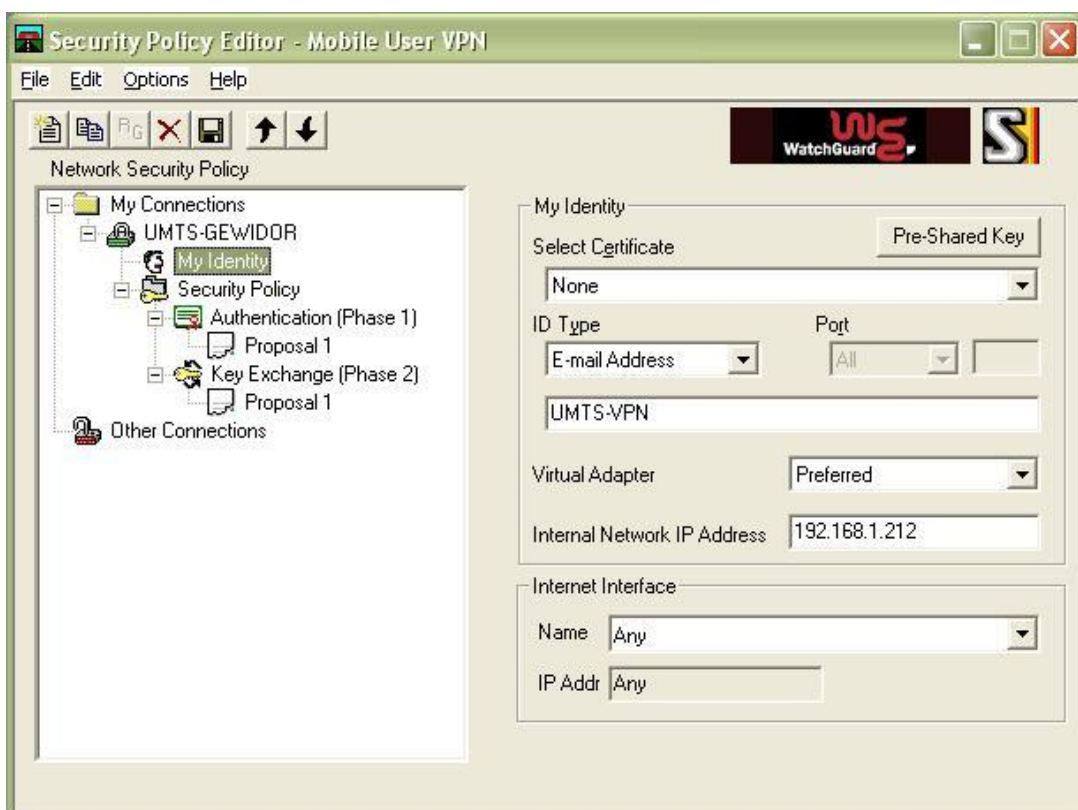
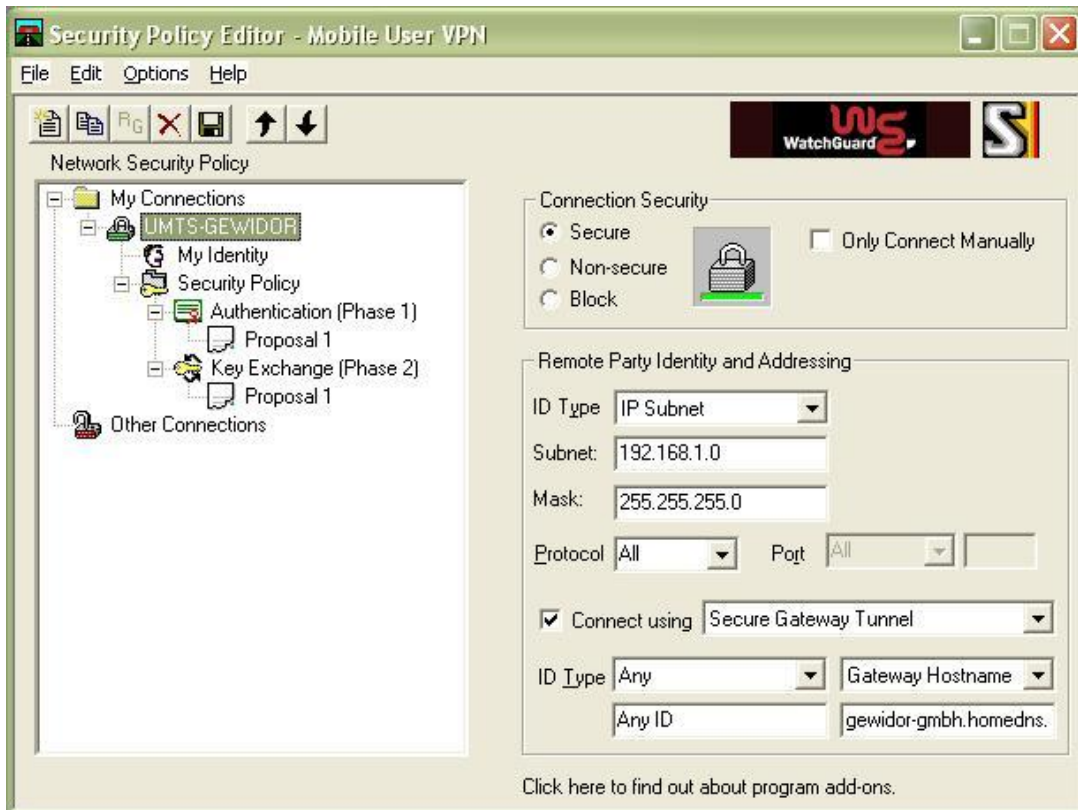
Filter	Service	Service Host
Deny	DNS	0.0.0.0
Deny	FTP	192.168.1.5
Deny	HTTP	192.168.1.5
Deny	HTTPS	0.0.0.0
Deny	IIS	0.0.0.0
No Rule	IPSec	192.168.1.2
Deny	NetMeeting	192.168.1.17
Deny	NNTP	0.0.0.0
Deny	Ping	192.168.1.5
Deny	POP3	192.168.1.1
Deny	PPTP	192.168.1.123
Deny	SMB	0.0.0.0
Deny	SMTP	0.0.0.0
Deny	SNMP	192.168.1.5
Deny	ssh	0.0.0.0
Deny	Telnet	0.0.0.0
Deny	WatchGuard	192.168.1.5



Die mobile Kanzlei Vor-Ort-Einsatz mit BiG-Manager unter Microsoft Windows Terminal Server über eine UMTS-VPN-Verbindung ins Firmennetzwerk

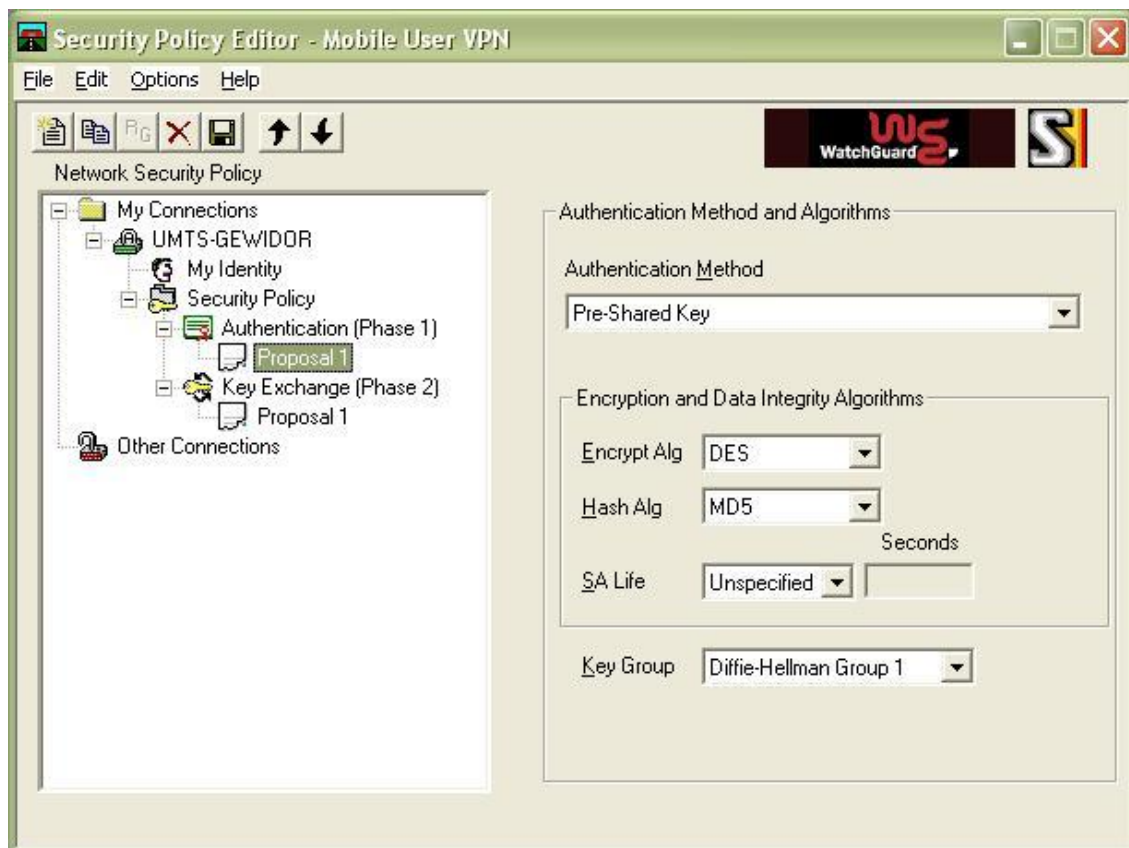
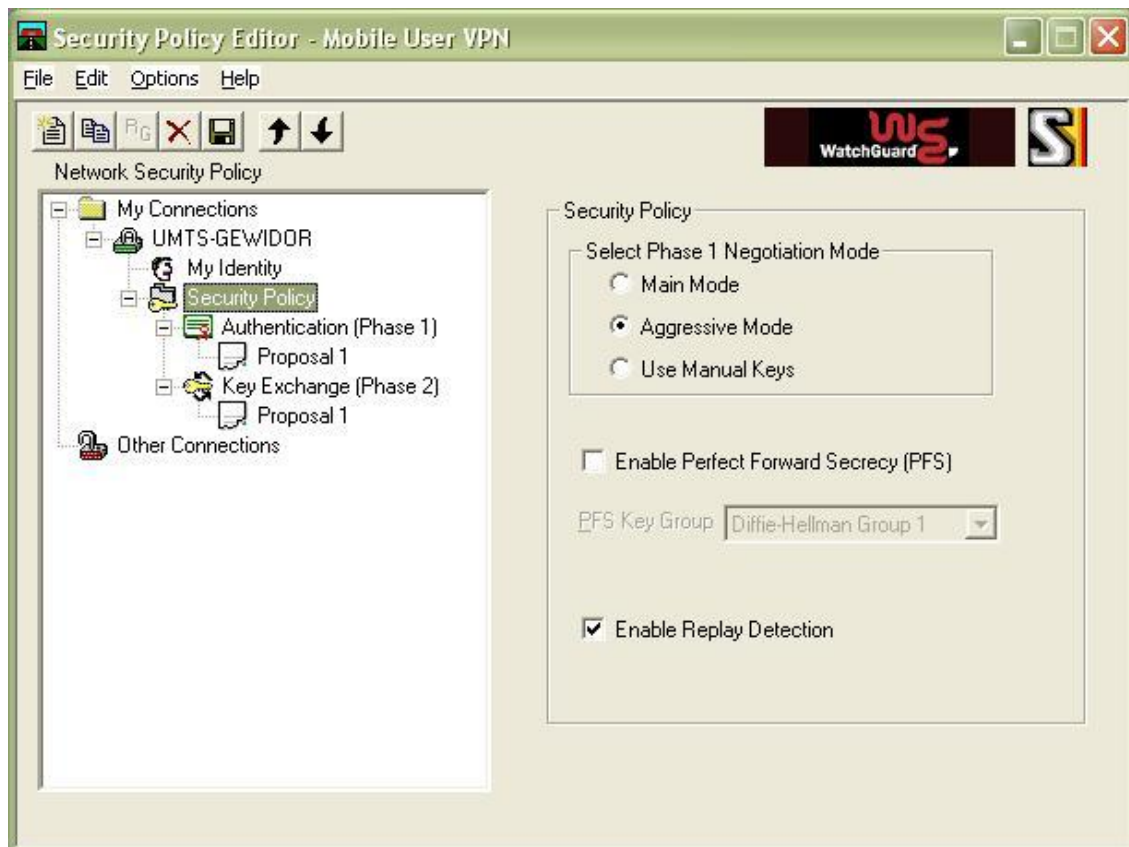
Mobile User VPN-Client-Konfiguration

Der Mobile User VPN-Client wird über die Konfigurationsdatei (.wgx-Import) eingestellt.





Die mobile Kanzlei Vor-Ort-Einsatz mit BiG-Manager unter Microsoft Windows Terminal Server über eine UMTS-VPN-Verbindung ins Firmennetzwerk





Die mobile Kanzlei Vor-Ort-Einsatz mit BiG-Manager unter Microsoft Windows Terminal Server über eine UMTS-VPN-Verbindung ins Firmennetzwerk

