

TightGate-Viewer für Microsoft Windows

Die im Download-Center der m-privacy GmbH bereitgestellte Installationsdatei für den TightGate-Viewer ist ein ausführbares MSI-Paket und enthält bereits alle benötigten Komponenten zur Audioübertragung und für das Drucken. Mit der Installation wird auf dem Desktop des Arbeitsplatz-PCs ein neues Desktop-Icon (**Internet**) sowie eine Verknüpfung im Windows-Startmenü angelegt.

Es gibt zwei Arten von Konfigurationsdateien: eine systemweite und eine benutzerspezifische. Die **systemweite Konfigurationsdatei** befindet sich unter:

```
%PROGRAMFILES%\TightGate-Pro\tgpro.cfg
```

Die **benutzerspezifische Konfigurationsdatei** ist im jeweiligen Benutzerkonto des Klientenrechners zu finden unter :

```
%APPDATA%\vnc\tgpro.vnc
```

Wird der TightGate-Viewer ohne spezielle Parameter gestartet, dann liest dieser seine Konfiguration aus der benutzerspezifischen Konfigurationsdatei. Ist eine solche noch nicht vorhanden, dann liest der TightGate-Viewer die systemweite Konfigurationsdatei aus und legt bei Beendigung der Sitzung eine benutzerspezifische Konfigurationsdatei an. In dieser werden alle Änderungen gespeichert, die der User während einer Sitzung selbst vornimmt.

Installation

Voraussetzung

- Aktueller TightGate-Viewer aus dem [Download Center der m-privacy GmbH](#)
- Computer mit Windows Betriebssystem ab Version 10 und administrativen Rechten.

Durchführung

- Das MSI-Paket des TightGate-Viewers mit administrativen Rechten ausführen.
- Nach der Installation ist die Datei **%PROGRAMFILES%\TightGate-Pro\tgpro.cfg** mit einem Editor zu öffnen und die Parameter **ServerName**, **krbhostname** und **SecurityTypes** für die jeweils gewünschte Anmeldeart laut nachfolgender Tabelle anzupassen:

Wert / Einstellung	Anmeldung mit Passwort	SSO mit Zertifikaten	Anmeldung über Active Directory
ServerName	Ja	Nein	Ja
krbhostname	Nein	Nein	Ja
SecurityTypes (alle anderen auskommentieren)	X509Plain	X509Cert	X509Krb
Anmeldezertifikate	Nein	Ja, Erstellung und Export laut: Benutzerverwaltung per Benutzerzertifikaten	Nein

- Der Start des TightGate-Viewers erfolgt durch ein Doppelklick auf das Desktop-Icon **Internet**

oder auf den Startmenüeintrag für den TightGate-Viewer.

Hinweis

Zur Änderung der systemweiten Konfigurationsdatei **tgpro.cfg** sind Administratorrechte auf dem Zielsystem erforderlich. Nach dem ersten Start des TightGate-Viewers wird für den jeweiligen Benutzer eine spezifische Konfigurationsdatei **tgpro.vnc** angelegt und fortan ausschließlich genutzt. Eventuelle spätere Änderungen an der systemweiten **tgpro.cfg** werden ignoriert, solange eine benutzerspezifische existiert. Änderungen müssen folglich entweder an der benutzerspezifischen Datei erfolgen oder alternativ kann die systemweite Datei angepasst werden, jedoch muss dann die benutzerspezifische Datei gelöscht werden. Sie wird dann beim nächsten Programmstart automatisch aus der systemweiten Datei erzeugt.

Nutzung der automatischen Dateischleuse

Warnung

Im TightGate-Viewer ab Version 4.0.x ist die automatisierte Dateischleuse klientenseitig ausgeschaltet. Sofern diese Funktion verwendet werden soll, ist sie im TightGate-Viewer oder in der Klientenkonfiguration **tgpro.cfg** bzw. **tgpro.vnc** zu aktivieren.

Die automatische Dateischleuse ist eine Alternative oder Ergänzung zur manuellen Dateischleuse in TightGate-Pro. Sie ermöglicht es, **Downloads automatisch** auf den Arbeitsplatzrechner zu übertragen.

- Jeder Benutzer hat innerhalb des Ordners **transfer** auf TightGate-Pro einen Unterordner namens **autotransfer**.
- Dateien in diesem Ordner durchlaufen wie gewohnt den **Malware-** und **MIME-Typen-Filter**.
- Wenn die Prüfung erfolgreich ist, wird die Datei automatisch auf den Arbeitsplatzrechner übertragen.
- Standardmäßig werden Dateien im lokalen Ordner **autotransfer** gespeichert (Unterordner des Windows-Standardordners **Downloads**).
- Das **lokale Zielverzeichnis** kann konfiguriert werden.
- Der **manuelle Abruf** über die TightGate-Schleuse ist weiterhin möglich – jedoch **nicht** für Dateien im Ordner **autotransfer**, sondern nur im übergeordneten Ordner **transfer**.

Hinweis

Wird das Zusatzprodukt OPSWAT für die Dateischleuse verwendet, so ist die automatische Dateischleuse deaktiviert.

Aktivierung der automatischen Dateischleuse (Server-seitig)

1. Anmeldung als Administrator **config**

- Menü **System-Vorgaben** → **Datei-Transfer** auf **Ja** setzen.
 - Menü **System-Vorgaben** → **Auto-Download erlauben** auf **Ja** setzen.
2. Nach Aktivierung erscheint der Menüpunkt **Auto-Download-Klienten-Ordner**:
- Zielordner für automatische Downloads festlegen.
 - Zulässig: Windows-Umgebungsvariablen (z. B. **%USERPROFILE%\Desktop**) oder Serverpfade (**\\Server\...**), auch in Kombination.
 - **Nicht zulässig**: Pfade, die den String **Start Menu** enthalten.
3. **Speichern** und **Anwenden** auswählen.
4. Anmeldung als Administrator **maint**
- Menü **Benutzerverwaltung** → **Auto-Download** öffnen.
 - Für die gewünschten Benutzerkennungen den Wert **Ja** setzen.
 - Einstellung wird mit dem nächsten Start des TightGate-Viewers wirksam.

Hinweis

Bei der Benutzerverwaltung via Active-Directory erfolgt die benutzerspezifische Zuordnung zur automatischen Dateischleuse über die Mitgliedschaft in der Sicherheitsgruppe **TGtransferAuto**. Details zu den Sicherheitsgruppe für TightGate-Pro [finden Sie hier](#).

Aktivierung im TightGate-Viewer

Da die automatische Dateischleuse ab der Version 4.0.x standardmäßig deaktiviert ist, muss sie auch auf dem Client explizit aktiviert werden.

Globale Vorgabe

- In der Datei **%PROGRAMFILES%\TightGate-Pro\tgpro.cfg** den Eintrag hinzufügen:
AutotransferSupport=1
- Für alle bestehenden Benutzer der Anmeldearten **Active Directory**, **LDAP** oder **Benutzername + Passwort** die Datei **%APPDATA%\vnc\tgpro.vnc** löschen.
- Für alle bestehenden Benutzer der Anmeldeart **Zertifikate** den Wert **AutotransferSupport=1** in die Datei **%APPDATA%\vnc\tgpro.vnc** hinzufügen.

Individuelle Vorgabe

- Im TightGate-Viewer (laufend) über **F8** → **Einstellungen** → **Sicherheit** den Haken bei **Auto-Transfer zulassen** setzen.
 - Einstellung wird beim Beenden in **tgpro.vnc** gespeichert.
- Alternativ (bei geschlossenem Viewer) den Eintrag manuell in **%APPDATA%\vnc\tgpro.vnc** hinzufügen: **AutotransferSupport=1**
- Beim nächsten Start ist die Funktion aktiv.

Funktionstest

- Mit einer Auto-Download-aktivierten Kennung am TightGate-Viewer anmelden.
- Im Ordner **transfer** sollte nun ein Unterordner **autotransfer** vorhanden sein.
- Eine für die Dateiübertragung erlaubte Testdatei in den Ordner **autotransfer** kopieren.

- Nach kurzer Zeit sollte sie im Zielordner erscheinen (wird automatisch angelegt, falls nicht vorhanden).

Lokalen Zielordner für Auto-Download anpassen (Client-seitig)

Falls der global konfigurierte Zielordner **nicht** genutzt werden soll, kann pro Benutzer ein individueller Pfad definiert werden.

Vorgehen:

1. TightGate-Viewer **beenden**.
2. Datei **%APPDATA%\vnc\tgpro.vnc** mit einem Editor öffnen.
3. Parameter **AutotransferFolder** hinzufügen und gewünschten Pfad eintragen.
 - Pfade müssen mit **doppelten Backslashes** maskiert werden.
 - Beispiel: **%USERPROFILE%\Desktop\Test** → legt einen Ordner *Test* auf dem Desktop an und speichert Downloads dort.
 - Serverpfade ebenfalls maskieren: **\\test\share** → **\\\\test\\share**
4. **Einschränkung:** Pfade die den Wert **Start Menu** enthalten sind nicht zulässig.
5. Datei speichern und TightGate-Viewer neu starten.
6. Funktionstest:
 - Datei in den **autotransfer**-Ordner auf TightGate-Pro legen.
 - Prüfen, ob sie im definierten lokalen Zielordner erscheint.
7. Falls nicht:
 - Eintrag in **tgpro.vnc** auf Vorhandensein und korrekte Syntax prüfen.
 - Bei Fehlern TightGate-Viewer beenden, Eintrag korrigieren und erneut starten.
 - Bleibt das Problem bestehen, den technischen Support der m-privacy GmbH kontaktieren.

Lokales Mikrofon und Webcam verwenden

Allgemeine Funktion

TightGate-Pro bietet als Schutzsystem einen hervorragenden Schutz gegenüber Angriffen auf das interne Netzwerk. Dazu zählt neben den Schutz vor unberechtigten Zugriff auf Dateien auch der unberechtigte Zugriff auf lokale Geräte. Vermehrt werden aber lokale Geräte benötigt, um den vollen Funktionsumfang im Internet nutzen zu können. Dies ist der Fall bei webbasierten Videokonferenzen. Um Nutzern die Teilnahme an solchen Videokonferenzen zu ermöglichen ist die globale Aktivierung dieser Funktion wie nachfolgend beschrieben notwendig.

- Anmeldung als Administrator **config**.
- Auswahl des Menüpunkts **System-Vorgaben > Webcam-Unterstützung** → **Ja**.
- Über die Menüpunkte **Speichern** und **Anwenden**, die Einstellungen übernehmen.

Weiterführende Hinweise:

- [Teilnahme an Videokonferenzen aus Nutzersicht](#)
- [Übersicht von TightGate-Pro unterstützter Webkonferenz-Systeme](#).
- [Testanleitung zur Nutzung vom lokalem Mikrofon und Webcam mit TightGate-Pro](#)

Sonderfälle

Bei den nachfolgenden Konfigurationen handelt es sich um Sonderfälle bei der Nutzung des TightGate-Viewers.

Hinweise für Terminalserver-Anlagen (z. B. CITRIX)

Die Nutzung von TightGate-Pro über Terminalserver-Anlagen ist möglich. Grundsätzlich erfolgt die Installation des TightGate-Viewers analog zur Vorgehensweise bei dedizierten Arbeitsplatzstationen. Es besteht jedoch eine Besonderheit im Hinblick auf die notwendigen Portfreigaben für die Audioübertragung. Folgende Einstellung vorzunehmen:

- Als **config** unter **System-Vorgaben > Pulseaudio Extra-Ports** ein Wertebereich einzustellen.
- Sofern die Anmeldeart **Zertifikate** verwendet wird, sind im Anschluss als **maint** die Nutzerzertifikate neu zu erstellen und zu verteilen.
- Für die Anmeldeart **Active Directory** sind Anpassungen in den Dateien **%APPDATA%\vnc\tgpro.vnc** (nur für bestehende Nutzer) und **%PROGRAMFILES%\TightGate-Pro\tgpro.cfg** vorzunehmen. Hier sind die Werte **PAPortMin=<Startwert>** und **PAPortMax=<Endwert>** zu ergänzen/anzupassen.

Bei jeder Anmeldung des Benutzers wird nun automatisch ein freier Port gesucht und für die Dauer der Sitzung reserviert und es werden Kollisionen mit anderen Klientenrechnern vermieden.

Hinweise zum Vollbildmodus / Umschaltung zwischen Applikationen

Mit der Tastenkombination **ALT+Tab** kann zwischen laufenden Applikationen umgeschaltet werden. Sofern der TightGate-Viewer im Fenster-Modus betrieben wird, wirkt sich **ALT+Tab** nur auf die Umgebung außerhalb des TightGate-Viewers aus. Im Vollbild-Modus wird hingegen zwischen laufenden Applikationen innerhalb des TightGate-Viewers gewechselt.

Dieses Verhalten kann dahingehend geändert werden, dass auch im Vollbild-Modus **ALT+Tab** nicht an TightGate-Pro weitergegeben wird. Die Tastenkombination wirkt sich dann in jedem Fall ausschließlich auf die Umgebung außerhalb des TightGate-Viewers aus. Um dieses Verhalten zu konfigurieren, kann in der Konfigurationsdatei des TightGate-Viewers der Parameter **FullScreenSystemKeys=0** gesetzt werden.

Alternativ kann im Fenstermenü des TightGate-Viewers (Aufruf mit F8) unter **Einstellungen > Eingabemethoden > Systemtasten direkt zum Server senden** der Haken entfernt werden.

Aufruf des TightGate-Viewers ohne Verwendung von tgpro.conf und tgpro.vnc

Soll z. B. für Testzwecke einmalig eine abweichende Konfiguration verwendet werden, ohne diese zu speichern oder vorherige Werte zu übernehmen, kann der TightGate-Viewer per Konsole mit der Option **-noconfig** und beliebig vielen weiteren Optionen aufgerufen werden. Der Aufruf von der

Konsole würde folgendermaßen aussehen:

```
%PROGRAMFILES%\TightGate-Pro\vncviewer.exe -noconfig
```

Führt man diesen Beispielaufruf aus, werden die IP des Servers und die Zugangsdaten des Benutzers in folgenden Dialogen abgefragt.

Aufruf des TightGate-Viewers mit Logging

Soll für Analysezwecke die Funktionalität des TightGate-Viewers geloggt werden, so ist dieser mit dem zusätzlichen Parameter (-log) aufzurufen. Es wird empfohlen beim Logging den TightGate-Viewer über die Konsole zu starten, damit nicht dauerhaft Log-Dateien erzeugt werden. Der Aufruf von der Konsole würde bei der Benutzerauthentifizierung via Benutzerzertifikat oder Active-Directory folgendermaßen aussehen:

```
%PROGRAMFILES%\TightGate-Pro\vncviewer.exe -log *:file:100
```

Wird der TightGate-Viewer so aufgerufen, wird im Verzeichnis unter **%temp%\tgprotemp** eine Log-Datei mit dem Namen **vncviewer.log** erstellt. Die Datei **vncviewer.log** ist eine Textdatei und kann mit beliebigen Texteditoren gelesen werden.

Aufruf des TightGate-Viewers mit Debugging

Soll für Analysezwecke die genaue Paketfolge des TightGate-Viewers geloggt werden, um Verbindungsabbrüche zu analysieren, so ist der TightGate-Viewer über den Sonderport 5901 und dem zusätzlichen Parameter (-log) aufzurufen. Es wird empfohlen beim Debugging/Logging den TightGate-Viewer über die Konsole zu starten, damit nicht dauerhaft Log-Dateien erzeugt werden. Es wird empfohlen das Debugging nur in Absprache mit dem technischen Kundendienst der m-privacy GmbH zu verwenden.

Achtung

Der Aufruf des TightGate-Viewers mit der Debugging-Option erfordert, dass der TightGate-Viewer sich über den Port 5901 mit TightGate-Pro verbinden darf. Im Normalbetrieb ist nur die Verbindung über den Port 5900 vorgesehen. Daher sind vor der Nutzung die entsprechenden Netzwerkregeln anzupassen.

Der Aufruf von der Konsole erfolgt folgendermaßen:

```
%PROGRAMFILES%\TightGate-Pro\vncviewer.exe -log *:file:100 [IP-Adresse]:5901
```

Wird der TightGate-Viewer so aufgerufen, erstellt er im Verzeichnis unter **%temp%\tgprotemp** eine Log-Datei mit dem Namen **vncviewer.log**. Die Datei **vncviewer.log** ist eine Textdatei und kann mit beliebigen Texteditoren gelesen werden.

Die Datei ist zu Analysezwecken an den technischen Kundendienst der m-privacy GmbH zu senden.

Mit mehreren Benutzern auf einem Rechner arbeiten

Es ist möglich mehrere Verknüpfungen des TightGate-Viewers auf dem Desktop anzulegen und diese mit unterschiedlichen Konfigurationen zu belegen. Hierfür ist per Rechtsklick auf dem Desktop-Icon das Menü **Einstellungen** und der Reiter **Verknüpfung** auszuwählen. Unter **Ziel** ist nun nach der Angabe des Programmpfades mit **-configdir=<Pfad>** der Pfad zu dem Ordner mit der zu nutzenden Konfigurationsdatei anzugeben. In diesem Ordner müssen für das Anmeldeverfahren SSO auch alle Nutzerzertifikate abgelegt werden.

Hinweis

Bei der Angabe des Pfades ist jeder Backslash mit einem weiteren zu maskieren (Bsp.: C:\\Users\\benutzername\\...). Würde man statt der Angabe eines abweichenden **configdir** beliebige andere Optionen angeben, würden diese in die **tgpro.vnc** Datei im Standardverzeichnis (**%APPDATA%\vnc**) übernommen werden. Bei mehreren Verknüpfungen des Tightgate-Viewers würden diese also gegenseitig ihre Konfigurationen überschreiben und sich nur in den in der Verknüpfung angegebenen Werten unterscheiden. Sofern es also gewünscht ist auch alle anderen Optionen, die nicht manuell angegeben wurden, wie z. B. die Größe des Fensters, zu übernehmen, sind zwingend mehrere **tgpro.vnc** Dateien erforderlich.

Appendix zu Konfigurationsoptionen

Soll der TightGate-Viewer aufgerufen werden und dabei Konfigurationsdateien aus einem speziellen Verzeichnis verwenden oder der Viewer ganz ohne Konfigurationsdatei gestartet werden, so können beim Programmaufruf folgende Parameter verwendet werden:

Parameter	Beschreibung
ConfigDir	Gibt das Verzeichnis an, in dem die zu verwendende Konfigurationsdatei tgpro.vnc sowie die Zertifikate für die Benutzeranmeldung liegen.
noConfig	Es wird weder die tgpro.vnc noch tgpro.cfg verwendet und die Einstellungen werden auch nicht beim Schließen gespeichert.
rwConfig	Soll das Standardverzeichnis (%APPDATA%\vnc) weiterhin genutzt werden und nur ein anderer Pfad für den Aufruf der tgpro.vnc Datei verwendet werden, kann dieser hier angegeben werden.

Hinweis

Bei Pfadangaben muss jeder Backslash mit einem weiteren "\\" maskiert werden!

Die nachfolgende Liste gibt eine Übersicht über verschiedene Werte des TightGate-Viewers. Diese gelten für die individuelle Konfigurationsdatei **%APPDATA%\vnc\tgpro.vnc** gleichermaßen wie für die globale Konfigurationsdatei unter **%PROGRAMFILES%\TightGate-Pro\tgpro.cfg**

Wert	Beschreibung
ServerName	Auflösbarer FQDN von TightGate-Pro.

Wert	Beschreibung
krbhostname	Auflösbarer FQDN von TightGate-Pro bei der Benutzeranmeldung per Active Directory.
SecurityTypes	Hiermit wird angegeben, welches Verfahren für die Anmeldung verwendet werden soll. Es ist nur ein Verfahren zu aktivieren. Folgende Verfahren gibt es: X509krb = Anmeldung mit Active Directory Ticket X509Plain = Anmeldung mit Benutzername und Passwort X509Cert = Anmeldung mit Zertifikaten, die auf TightGate-Pro erstellt wurden.
PAPortMin	Beginn des Wertebereichs für Pulseaudio Ports (anzugeben bei Terminal Clients).
PAPortMax	Ende des Wertebereichs für Pulseaudio Ports (anzugeben bei Terminal Clients).
Maximize (1=aktiv)	Der TightGate-Viewer öffnet sich immer in maximaler Größe.
PrintSupport (1=aktiv)	Aktiviert oder deaktiviert die Druckunterstützung von TightGate-Pro auf lokale Arbeitsplatzdrucker.
AdobePrintDialog (1=aktiv)	Öffnet bei Druckaufträgen vom TightGate-Pro am lokalen Arbeitsplatz den Adobe-Druckdialog, sofern der Acrobat Reader dort installiert ist. Voraussetzung ist ebenfalls, dass die Druckunterstützung (PrintSupport=1) aktiviert ist.
QuickPrint (1=aktiv)	Druckaufträge werden ohne Dialog direkt an den Standarddrucker weitergegeben.
SoundSupport (1=aktiv)	Der Ton kann damit aktiviert oder deaktiviert werden. (Wurde der Ton seitens maint oder global als config deaktiviert, ist diese Einstellung wirkungslos.)
AutotransferFolder	Legt den Pfad fest, wohin bei aktivierter automatisierter Dateischleuse Downloads von TightGate-Pro im lokalen Klienten geschrieben werden .
AutotransferSupport (1=aktiv)	Aktiviert, bzw. deaktiviert die automatische Dateischleuse am Klienten. Eine clientseitig deaktivierte automatische Dateischleuse kann serverseitig nicht überschrieben werden.
AcceptClipboard (1=aktiv)	Aktiviert, bzw. deaktiviert die Einzelfallbestätigung der Zwischenablage von TightGate-Pro zum Windows-Klienten.
SendClipboard (1=aktiv)	Aktiviert, bzw. deaktiviert die Einzelfallbestätigung der Zwischenablage vom Windows-Klienten zu TightGate-Pro.
EnforceClipboard (1=aktiv)	Wird diese Einstellung aktiviert, so kann ein Benutzer über das F8-Menü keine Änderungen an den Vorgaben für die Zwischenablage vornehmen.
Menukey (Default=F8)	Viele Einstellungen lassen sich nach Aufruf des TightGate-Viewers über ein Funktionsmenü (im Standard F8) vornehmen, ohne die Konfigurationsdateien manuell anzupassen. Hiermit kann die Funktionstaste definiert werden, mit dem der Menüaufruf erfolgt.
FullScreenSystemKeys (1=aktiv)	Legt fest, ob auch im Vollbild-Modus ALT+Tab an TightGate-Pro weitergegeben wird.

Eine vollständige Liste der verfügbaren Programmparameter für den TightGate-Viewer erhalten Sie, wenn in der **Eingabeaufforderung** unter Windows im Programmpfad **%PROGRAMFILES%\TightGate-Pro** folgendes Programm starten:

```
vncviewer.exe --help
```


From:

<https://help.m-privacy.de/> -

Permanent link:

<https://help.m-privacy.de/doku.php/tightgate-pro:client:windows-vnc>

Last update: **2025/08/09 19:14**

