

G-Data Endpoint Protection Business

Computer-Viren, Trojaner, Spyware und andere Schadsoftware stellen eine ständige Bedrohung für die PC-Daten dar. Deshalb ist ein zuverlässiger Schutz eine wichtige Voraussetzung für eine funktionierende EDV am Arbeitsplatz. Das kiz der Universität Ulm stellt dazu auf den betreuten PCs einen Virenschanner zur Verfügung. Somit können Sie sich sowohl gegen Viren aus dem Internet wie auch gegen Viren auf internem Wege (CD, USB-Stick, Laufwerkfreigaben usw.) gut absichern.

Installation

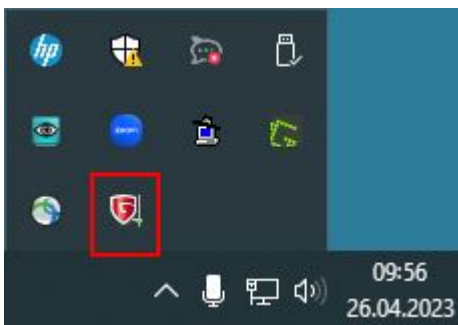
Auf allen vom kiz betreuten PCs, ist zum Schutz vor Schadsoftware **G-Data Endpoint Protection Business** installiert. Besteht eine Verbindung zum G-Data Server der Universität Ulm, werden Signatur- und Programmupdates automatisch installiert.

Konfiguration

Es ist keine Konfiguration erforderlich. Alle Einstellungen werden zentral auf dem Server gemacht.

Bedienung

G-Data finden Sie normalerweise auf Ihrem Desktop rechts unten im [System Tray](#) Bereich.



Mit einem Rechtsklick auf das Symbols des **G Data Security Clients** erreichen Sie die Bedienelemente. Die Bedienelemente **Virenprüfung** und **Optionen** erscheinen nur wenn eine Verbindung zum G-Data Server der Universität Ulm besteht.



- **Virenprüfung:** Damit können Sie Ihren PC, einzelne Daten oder Verzeichnisse oder

Wechseldatenträger überprüfen.

- **Optionen.....**: Bei den vom kiz betreuten PCs können nur die Optionen unter **Virenprüfung** verändert werden. Diese Einstellungen sind bei der manuellen Virenprüfung relevant.
- **Internet-Update**: Bitte hier die Standardeinstellung nicht verändern.
- **Info.....**: Hier kann man sich die Versionen von Programm und Virensignaturen anzeigen lassen. Das Datum der Virensignaturen muss immer aktuell sein.

Hier finden Sie die [Anleitung des Herstellers](#)

Schutzfunktionen

Ein Dateiwächter sorgt für den permanenten Schutz des PCs. Es wird aber kein automatischer Scan über Datenträger ausgeführt. Das sollte in regelmäßigen Abständen, z.B. einmal im Monat, manuell gemacht werden. Vorzugsweise zu Zeiten, an denen am PC nicht gearbeitet wird, da mit Performance-Beeinträchtigungen gerechnet werden muss. Je nach Größe des Datenträgers, kann ein kompletter Scan über eine Stunde dauern. Auch Wechseldatenträger wie USB-Sticks, müssen nach der Verbindung mit dem PC manuell überprüft werden. Wird Schadsoftware entdeckt, erhalten Sie eine Meldung. Ihnen werden dann verschiedene Möglichkeiten angeboten, wie mit der Datei umgegangen werden soll.

Manchmal werden Programme irrtümlich als Schadsoftware erkannt. Bitte melden Sie dem kiz Programme für die das zutrifft. Für diese Fälle gibt es auf dem G-Data Server eine Liste, in die solche Programme eingetragen werden können.

USB Keyboard Guard

G-Data bietet unter anderem eine Schutzfunktion vor "[falschen Tastaturen](#)". Neu angeschlossene Geräte, die vom Betriebssystem als Tastatur erkannt werden, werden als potenziell bedrohlich eingestuft. Das können außer Tastaturen auch [YubiKeys](#) oder Chipkartenleser sein. Es erscheint eine Warnmeldung,



die mit einer Ziffernfolge bestätigt werden muss.




Wird die Ziffernfolge korrekt eingegeben, wird das neu angeschlossene Geräte akzeptiert. Das muss pro PC und neuem Gerät nur einmal gemacht werden. Sollte die Verwendung verweigert, oder falsche Ziffern eingegeben werden, ist das Gerät in der aktuellen Session blockiert. Erst nach einem Neustart kann die Freigabeprozedur wiederholt werden. Will man einmal freigegebene Gräte aus der Liste der akzeptierten Geräte entfernen, geht das nur über das Löschen des entsprechenden Schlüssels in der Windows Registry unter

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\GDKeyboard Guard.

Dafür sind administrative Rechte nötig.

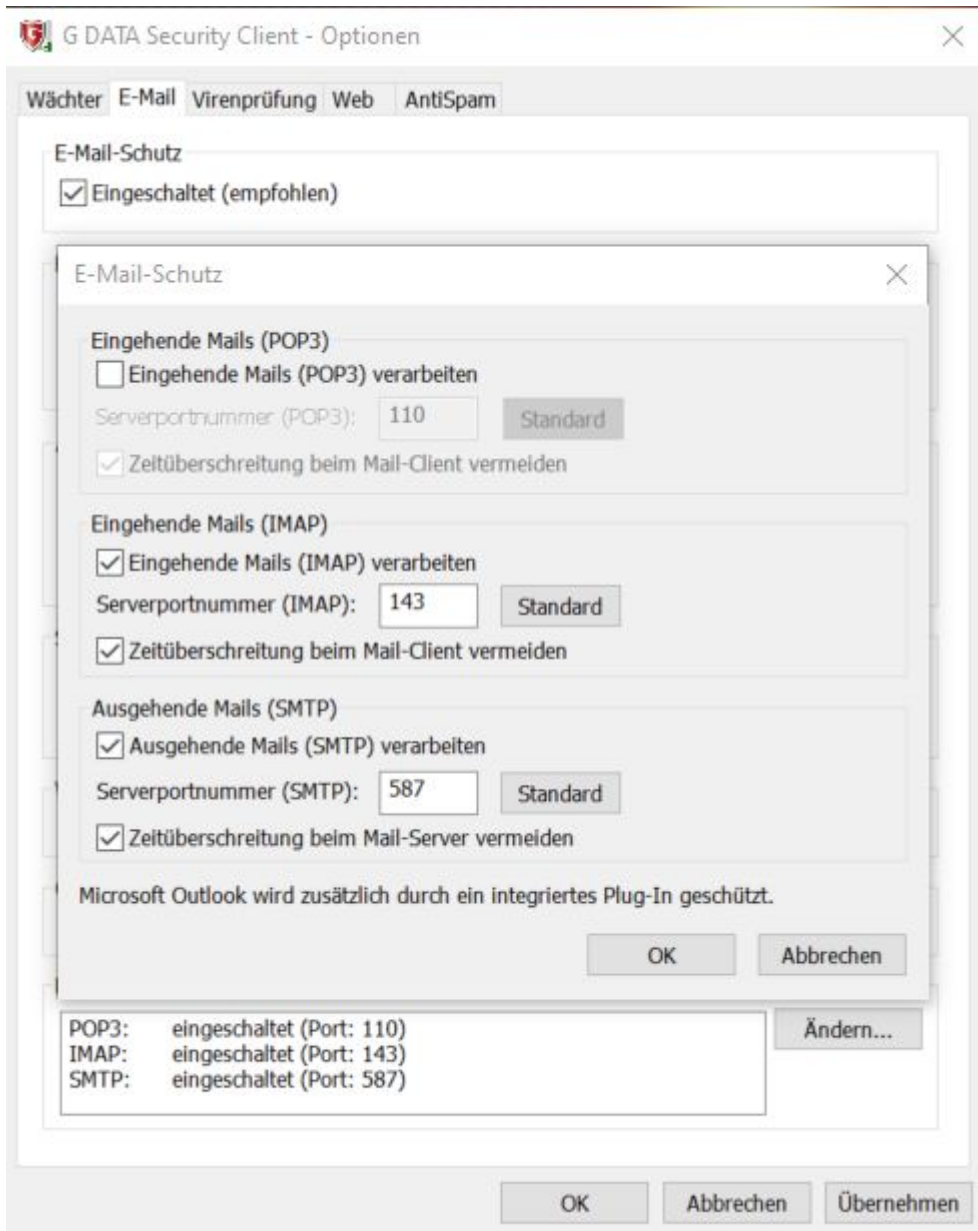
Browser-Erweiterung

Zum Schutz vor betrügerischen Webseiten, auch bei Verwendung von HTTPS, verfügt G-DATA eine Browser-Erweiterungen für die Internet-Browser Mozilla Firefox, Microsoft Edge und Google Chrome.

Sobald die Erweiterung aktiv ist, erscheint im Browser rechts oben das Symbol  von **G DATA WebProtection**. Manchmal werden Web-Seiten zu Unrecht blockiert. Für diese Fälle bietet G-Data eine [Meldeseite](#), in die solche Web-Seiten eingetragen werden können. Die gemeldeten Seiten werden dann von G-Data geprüft und ggf. freigeschaltet.

E-Mail Schutz

Bei den nicht vom kiz betreuten PCs, besteht die Möglichkeit den **E-Mail-Schutz** zu aktivieren. Das geht im **G DATA Security Client** unter der Registerkarte E-Mail. Achten Sie bitte auf die korrekten Ports. Das Mailsystem der Universität Ulm verwendet den SMTP Port 587.



Datenschutz

Der Hersteller G-Data garantiert die Einhaltung der deutschen und europäischen [Datenschutzgesetze](#). Weder das kiz noch die Firma G-Data hat über **G-Data Endpoint Protection Business** Zugriff auf Ihre Daten. Aus Datenschutzgründen wurde bewusst eine [On-Premises](#) Lösung gewählt.

Benötigte Kommunikationsports

Damit sich der G-Data Client mit dem G-Data Server der Universität Ulm verbinden kann, müssen abhängig vom Betriebssystem, diese Ports erreichbar sein:

- 80 TCP (Linux- / Mac-Repository)
- 443 TCP (Linux- / Mac-Client Sync)
- 7161 TCP (Windows Client Sync)

Verbindungen sind sowohl mit IPv6 als auch mit IPv4 möglich.

Das kann in PowerShell mit diesem Kommando geprüft werden: **Test-NetConnection gdata.rz.uni-ulm.de -Port „Portnummer“**

Die Ports sind nur aus diesen Netzen erreichbar: **134.60.0.0/16** bzw. **2001:7c0:3100::/40**.

Die Bedienelemente **Virenprüfung** und **Optionen** im **G Data Security Client** erscheint nur wenn eine Verbindung zum G-Data Server der Universität Ulm besteht.

Boot-Medium erstellen

Hier ist eine ISO zu finden, mit der ein G-Data Boot-USB-Stick erstellt werden kann [G-DATA-BootMedium](#). Damit kann ein Rechner auf Schadsoftware untersucht werden, ohne das darauf installierte Betriebssystem zu starten.

Probleme

- Manchmal werden Programme irrtümlich als Schadsoftware erkannt. Bitte melden Sie dem kiz Programme für die das zutrifft. Für diese Fälle gibt es auf dem G-Data Server eine Liste, in die solche Programme eingetragen werden können.
- Beim Kopieren großer Datenmengen kann in seltenen Fällen der PC sehr langsam werden, da hierbei jede Datei auf Schadsoftware untersucht wird. Ob das an G-Data liegt, kann man im Taskmanager an einer hohen CPU-Auslastung, verursacht durch die G-Data Prozesse, erkennen. Sollte das ein Problem sein, wenden Sie sich bitte an das kiz.
- Besonders auf Servern können bei Verzeichnissen mit hohem Datendurchsatz, durch Scan-Prozesse Performance-Probleme auftreten. Das können z.B. Datendateien einer Datenbank sein. Wir empfehlen diese Dateien vom Scan-Vorgang auszuschließen. Bitte wenden Sie sich dazu an das kiz.

Weblinks

Hier finden Sie die [Anleitung des Herstellers](#)

Abschließende Einrichtung von G Data Antivirus nach der Installation [G DATA Antivirus Mac - First steps after installation](#)

Freischaltung von unbegründet blockierten Web-Seiten:[Meldeseite](#)

Einrichtung der Browser-Erweiterung für den G DATA Webschutz [Webschutz](#) (nicht für die vom kiz betreuten PCs)

Upload für eventuell befallene Dateien [G Data Uploadportal](#)

Leitfaden bei Virenbefall [Leitfaden](#)

From:

<https://help.rz.uni-ulm.de/published/> - **kiz Infrastruktur - Hilfe Wiki**

Permanent link:

<https://help.rz.uni-ulm.de/published/doku.php?id=allgemein:virens scanner>

Last update: **2024/02/13 17:14**

