tetraguard informiert:

tetraguard device & more **Datenblatt**

Funktionsweise:

Ein Treiber auf Kernelebene verschlüsselt alle Dateien automatisch, sobald sie unberechtigt auf ein externes Medium geschrieben werden. Diese Daten sind dann nur innerhalb Ihres Firmennetzwerkes lesbar. Ein Passwort ist nicht nötig. Für Transfers über die Sicherheitsgrenzen sind Autorisierungen möglich.

Verschlüsselung:

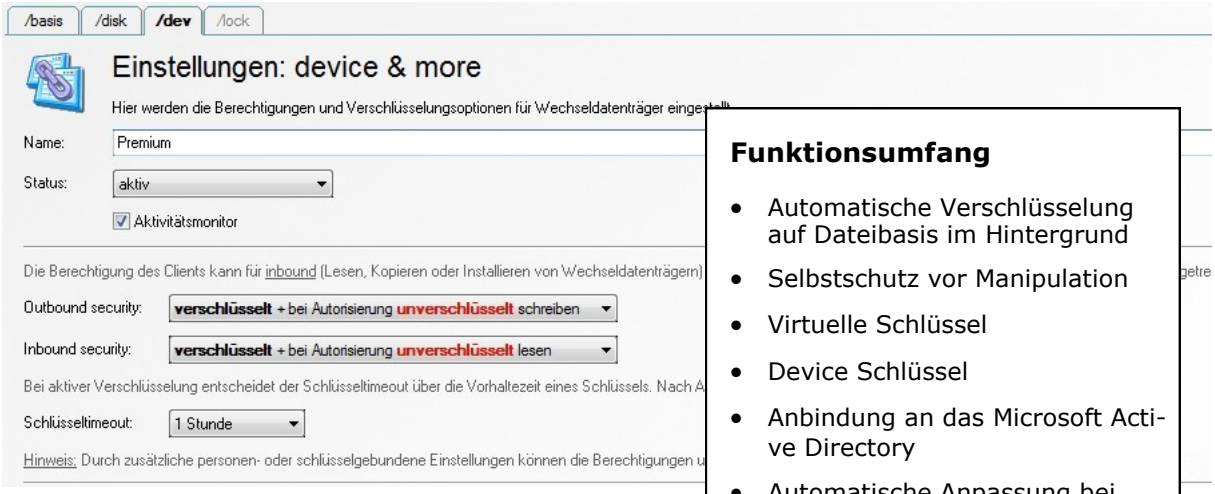
Für die Verschlüsselung wird ein AES-Algorithmus (Rijndael-Algorithmus) verwendet. Die Verschlüsselung greift automatisch im Hintergrund, ohne dass der Benutzer dies bestätigen muss.

Schlüssel:

Zur Autorisierung gibt ein großes Spektrum an Möglichkeiten. Darunter zählen zb. USB-Token, welche zur zusätzlichen Sicherheit noch mit einem Passwort geschützt werden können, eine Anbindung an das Microsoft Active Directory oder gar eine Freigabe eines ganz bestimmten Gerätes.

Administration:

Die Konfiguration und Verwaltung verläuft zentral über den Sicherheitsmanager, mit welchem auch andere Produkte von tetraguard konfiguriert werden können.



Funktionsumfang

- Automatische Verschlüsselung auf Dateibasis im Hintergrund
- Selbstschutz vor Manipulation
- Virtuelle Schlüssel
- Device Schlüssel
- Anbindung an das Microsoft Active Directory
- Automatische Anpassung bei Erweiterung eines Netzwerks
- Wartungsarm und zuverlässig
- 4-Augen-Prinzip
- Client für 32 und 64 Bit
- Lese– und Schreibzugriff getrennt einstellbar
- Overlay - Optische Rückmeldung
- Protokollierung möglich

tetraguard systems GmbH
Gerberstraße 3 Gebäude M
D 53879 Euskirchen
Geschäftsführer: Stefan Kistner

Telefon: +49 2251 81798-0
Telefax: +49 2251 81798-99
E-Mail: info@tetraguard.de
www.tetraguard.de

Amtsgericht Bonn HRB 19541
Steuernummer: 209/5718/1463
USt-IdNr.: DE 268 059 062

Raiffeisenbank Wachtberg
IBAN: DE79577622650000747374
BIC: GENODED1GRO

tetraguard informiert:

tetraguard device & more

Datenblatt

Systemvoraussetzungen:

Betriebssystem	Server	Client
Windows 2003 Server / 2008 Server / 2012 Server	✓✓	✓✓
Windows XP Home 32 Bit	✗	✓
Windows XP Professional 32 Bit	✓✓	✓✓
Windows Vista 32 Home Basic	✗	✓
Windows Vista 32 / 64 ab Home Premium	✓✓	✓✓
Windows 7 32 Bit (Home)	✗	✓
Windows 7 32 / 64 (Professional oder Ultimate)	✓✓	✓✓
Windows 8, 8.1 32 / 64 Bit	✗	✓✓
Windows 8, 8.1 32 / 64 Bit (Pro)	✓✓	✓✓

✓✓ Client– bzw. Serversoftware kann installiert und benutzt werden

✓ Aufgrund eingeschränkter Netzwerkfunktionalität kann die Clientsoftware per Einzelplatzinstallation genutzt werden

✗ Aufgrund der Einschränkungen in der Netzwerkfunktionalität ungeeignet

Minimale Hardware Anforderungen:

Komponente	Server	Client
CPU	Keine besonderen Anforderungen	Keine besonderen Anforderungen
RAM	Keine besonderen Anforderungen	Keine besonderen Anforderungen
Festplatte	Zirka 30 MB	Zirka 2 MB
	Für den Einsatz von **tetraguard.auditing** wird - abhängig von der Menge der aufgezeichneten Daten - ebenfalls Speicherplatz auf dem Server und Client benötigt.	

Hinweis:

Um zuverlässig den Schutz durch die tetraguard Clientsoftware zu gewährleisten, ist für die Systempartition NTFS zwingend erforderlich. Ab Windows Vista ist dies standardmäßig der Fall. Auf Windows XP Rechnern prüfen Sie bitte vorab das Dateisystemformat der Systempartition. Nötigenfalls können Sie dass Format mit dem Kommandozeilenbefehl "convert C: /FS:NTFS" anpassen.

Für den Einsatz von **tetraguard.disk** ist ebenfalls NTFS für alle zu schützenden Partitionen erforderlich. Ist nur der Schutz der Schnittstellen vorgesehen, können Datenpartitionen hingegen in einem beliebigen Format (z.B. FAT32, exFAT, etc.) vorhanden sein.

Informationen erhalten Sie bei:

tetraguard systems GmbH
Gerberstraße 3 Gebäude M
53879 Euskirchen

Tel +49 2251 - 817 98 0
Fax +49 2251 - 817 98 99
E-Mail info@tetraguard.de
Web www.tetraguard.de

Händlerstempel