CGM MEDISTAR

Arztinformationssystem

CGM MEDISTAR
Systemanforderungen

Inhalt

Systemanforderungen für den Betrieb von CGM MEDISTAR

CGM MEDISTAR ist ein System mit vielen Möglichkeiten. Lassen Sie CGM MEDISTAR zu Ihrer rechten Hand werden und profitieren Sie täglich von intelligenten und anwenderfreundlichen Funktionen, die Ihnen das Arbeitsleben erleichtern. Damit Sie CGM MEDISTAR im vollen Umfang nutzen können und ein reibungsloser Umgang realisiert werden kann, möchten wir Sie in diesem Zuge auf unsere Systemanforderungen hinweisen.

Für den Betrieb von CGM MEDISTAR 4.x inkl. aller Module (z.B. MOVIESTAR mind. Version 5.20, Facharztlösungen) gelten die unten aufgeführten Anforderungen.

1. Zugelassene Betriebssysteme MEDISTAR Server

a. Microsoft Windows Server 2025 deutsche Version
(MOVIESTAR Version 5.22 oder neuer, Supportende 10.10.2034)
b. Microsoft Windows Server 2022 Standard deutsche Version
(MOVIESTAR Version 5.20SP1 oder neuer, Supportende 14.10.2031)
c. Microsoft Windows Server 2019 Standard deutsche Version
(MOVIESTAR Version 5.20 oder neuer, Supportende 09.01.2029)
d. Microsoft Windows Server 2016 Standard deutsche Version (Supportende 11.01.2027)

Es werden ausschließlich die 64-bit Versionen der zugelassenen Betriebssysteme von uns unterstützt.
Für alle Betriebssysteme ist die Installation ausschließlich auf NTFS-Partitionen freigegeben.

1.1 Zugelassene Betriebssysteme MEDISTAR Client

a. Microsoft Windows 11 Pro/Enterprise deutsche Version (MOVIESTAR Version 5.20 oder neuer, Supportende 21H2 08.10.2024, 22H2 14.10.2025, 23H2 10.11.2026)
b. Microsoft Windows 10 Pro/Enterprise deutsche Version (Supportende 14.10.2025)
c. alle Betriebssysteme, die unter MEDISTAR-Server aufgeführt sind

Es werden ausschließlich die 64-bit Versionen der zugelassenen Betriebssysteme von uns unterstützt.
Für alle Betriebssysteme ist die Installation ausschließlich auf NTFS-Partitionen freigegeben.

2. Microsoft Word

Für die Verwendung von Microsoft Word zur CGM MEDISTAR Textverarbeitung und/oder CGM MEDISTAR Privatliquidation sind folgende Versionen zugelassen:

a. Microsoft Office 365 mit der Word-Version bis 2024 Desktop
b. Microsoft Word 2024, (MOVIESTAR Version 5.22 oder neuer
Supportende 09.10.2029)
c. Microsoft Word 2021, (MOVIESTAR Version 5.20SP1 oder neuer
Supportende 13.10.2026)
d. Microsoft Word 2019, (MOVIESTAR Version 5.20 oder neuer
Supportende 14.10.2025)

https://technet.microsoft.com/de-de/library/ee624351.aspx?f=255&MSPPError=-2147217396

3. Abkündigungen

Alle zugelassenen Betriebssysteme werden bis zum Ablaufen des „Extended Support“ von Microsoft unterstützt.

https://support.microsoft.com/de-de/lifecycle/search/16715

4. Mindestanforderungen an die Hardware

- Der Server muss die jeweils gültigen Datenschutzrichtlinien erfüllen.
- Der Server wird nicht als Arbeitsplatz verwendet und steht in einem verschlossenen Bereich.
- Der CGM MEDISTAR-Server ist auf einem Server-Betriebssystem zu installieren.

4.1 Empfohlene Hardware auf Basis einer 5-Platz-Anlage

4.1.1 CGM MEDISTAR Server

a. Serverbord mit Server CPU 4 x mind. 3,2 GHz
   *Anmerkung: Die Taktgeschwindigkeit auf dem Singlecore ist wichtiger als die Anzahl der Kerne
b. Arbeitsspeicher mind. 32 GB
c. NVMe, SSD oder SAS-HDD mit redundantem Festplattensystem (RAID)
d. Raid-Controller mit Absicherung des Schreibcache bei Stromausfall / plötzlicher Ausfall des Servers
e. Aktiviertes TPM-Modul mit aktivierter Verschlüsselung der Partitionen.
   Bei Virtualisierungen muss der Host verschlüsselt sein.
f. Netzwerkanbindung mind. 1GBit.
g. DVD-Brenner (für MOVIESTAR Langzeitarchivierung)
h. Bedienkonsole (Klassisch über Monitor, Maus, Tastatur oder über Remote Management Card)

4.1.2 CGM MEDISTAR Workstation

a. Intel CPU i5 Desktop oder vergleichbar mind. 2,4 GHz
b. Arbeitsspeicher mind. 16GB
c. NVMe oder SSD mind. 240 GB
d. Aktiviertes TPM-Modul mit aktivierter Verschlüsselung der Partitionen.
e. Netzwerkanbindung mind. 1GBit.
f. Bei WLAN Anbindung nur per RDP zum Terminalserver

4.2 Mindestanforderungen an die Hardware bis 5-Platz-Anlage

4.2.1 CGM MEDISTAR Server

a. Serverbord mit Server CPU 4 x mind. 2,1 GHz
b. Arbeitsspeicher mind. 16 GB
c. NVMe, SSD oder SAS-HDD mit redundantem Festplattensystem (RAID)
d. Raid-Controller mit Absicherung des Schreibcache bei Stromausfall / plötzlicher Ausfall des Servers
e. Aktiviertes TPM-Modul mit aktivierter Verschlüsselung der Partitionen
Bei Virtualisierungen muss der Host verschlüsselt sein.
f. Netzwerkanbindung mind. 1GBit
g. DVD-Brenner (für MOVIESTAR Langzeitarchivierung)
h. Bedienkonsole (Klassisch über Monitor, Maus, Tastatur oder über Remote Management Card)

4.2.2 CGM MEDISTAR Workstation

a. Intel CPU i3 DualCore Desktop mind. 1,6 GHz oder vergleichbar
b. Arbeitsspeicher mind. 8 GB
c. NVMe, SSD oder SATA Festplatte mit mind. 10 GB freien Speicher für die CGM MEDISTAR-Anwendungen
d. Aktiviertes TPM-Modul mit aktivierter Verschlüsselung der Partitionen.
e. Netzwerkanbindung mind. 1GBit.
f. Bei WLAN Anbindung nur per RDP zum Terminalserver

Die Mindestanforderungen gewährleisten lediglich eine reibungslose Funktionalität. Für effizientes und schnelles Arbeiten sollten die Werte der empfohlenen Hardware nicht unterschritten werden.

5. IT-Sicherheit

Die Gewährleistung von IT-Sicherheit und Datenschutz ist in der Medizinbranche von größter Bedeutung. CGM MEDISTAR verpflichtet sich zu höchsten Sicherheitsstandards, um die sensiblen Daten von Patienten und Praxen zu schützen. Dieses Kapitel gibt allgemeine Empfehlungen zur IT-Sicherheit sowie spezielle Hinweise zu den Sicherheitsmodulen der CompuGroup, den PC Log-In-Funktionen, den Betriebssystemen, Firewall- und Port-Einstellungen und externen Softwarelösungen.

5.1 Allgemeine Empfehlungen zur IT-Sicherheit

- **Regelmäßige Updates**: Halten Sie sowohl Ihre CGM MEDISTAR Software als auch das zugrunde liegende Betriebssystem stets auf dem neuesten Stand. Installieren Sie alle verfügbaren Updates zeitnah, um Sicherheitslücken zu schließen und neue Funktionen zu nutzen.
- **Starke Passwörter**: Verwenden Sie komplexe Passwörter mit **mindestens 12 Zeichen**, die aus **Groß- und Kleinbuchstaben**, **Zahlen** und **Sonderzeichen** bestehen. Vermeiden Sie leicht zu erratende Passwörter und ändern Sie diese regelmäßig. **Ändern Sie Standardpasswörter** auf **allen Geräten und Systemen unverzüglich** nach der Einrichtung.]
- **Zugriffsrechte**: Weisen Sie Benutzern nur die benötigten Zugriffsrechte zu. Nutzen Sie die Möglichkeit, Rollen und Berechtigungen in CGM MEDISTAR zu definieren, um Datenzugriffe zu steuern.

- **Sicherheitsbewusstsein**: Schulen Sie alle Mitarbeiter regelmäßig in Bezug auf IT-Sicherheit und Datenschutz. Sensibilisieren Sie sie für Phishing-Angriffe und andere Bedrohungen.
- **Datensicherung**: Führen Sie regelmäßige Datensicherungen durch und bewahren Sie Sicherungskopien an einem separaten Ort auf. Nutzen Sie die integrierten Backup-Funktionen von **CGM MEDISTAR**.
- **Überprüfen Sie regelmäßig, ob die Backups fehlerfrei wiederhergestellt** werden können. Schützen Sie Ihre Backups zudem vor **unerlaubtem Zugriff, Verlust** und **unbeabsichtigtem Überschreiben** (z. B. durch einen **Verschlüsselungstrojaner**).

5.2 Betriebssysteme

- **Unterstützte Betriebssysteme**: Stellen Sie sicher, dass Sie eine unterstützte Version des Betriebssystems verwenden (z. B. Windows 10, Windows 11). Überprüfen Sie regelmäßig die Kompatibilität mit der neuesten Version von CGM MEDISTAR.
- **Sicherheitseinstellungen**: Aktivieren Sie die integrierten Sicherheitsfunktionen des Betriebssystems, wie Windows Defender, um zusätzlichen Schutz vor Malware und Viren zu gewährleisten.
- **Benutzerrechte**: Für eine optimale tägliche Nutzung des CGM MEDISTAR-Produkts wird empfohlen, dass Benutzer im Regelbetrieb ein Standard-Windows-Konto ohne Administratorrechte verwenden.

5.3 Firewall- und Port-Einstellungen

- **Firewall-Regeln**: Aktivieren Sie die Firewall Ihres Betriebssystems und konfigurieren Sie sie so, dass verdächtige Verbindungen blockiert werden. Erstellen Sie spezifische Firewall-Regeln, um den Netzwerkzugriff auf CGM MEDISTAR zu kontrollieren.
- **Port-Management**: Schließen Sie alle nicht benötigten Ports, um unautorisierte Zugriffe zu verhindern. Prüfen Sie regelmäßig die offenen Ports auf Ihrem System und passen Sie die Einstellungen gegebenenfalls an.
- **Netzwerküberwachung**: Implementieren Sie Werkzeuge zur Überwachung des Netzwerkverkehrs, um ungewöhnliche Aktivitäten zu erkennen. Dies hilft, potenzielle Sicherheitsvorfälle frühzeitig zu identifizieren.
- **Incident Response Plan:** Seien Sie auf **potenzielle Sicherheitsvorfälle** vorbereitet, indem Sie einen **klaren Reaktionsplan** erstellen. Dieser Plan sollte definieren, **wie schnell und effektiv** auf Sicherheitsverletzungen reagiert wird. Legen Sie **Verantwortlichkeiten**, **Kommunikationswege** und konkrete **Maßnahmen zur Schadensbegrenzung** fest, um im Ernstfall handlungsfähig zu bleiben.

5.4 Besondere Module zur IT-Sicherheit der CompuGroup

- **Security Monitoring**: Nutzen Sie das integrierte Monitoring-Tool zur Überwachung von ungewöhnlichen Aktivitäten und Sicherheitsvorfällen. Dies umfasst die Protokollierung von Zugriffen und Änderungen innerhalb der Software.
- **Verschlüsselung**: Alle sensiblen Daten werden sowohl bei der Speicherung als auch bei der Übertragung durch moderne Verschlüsselungstechniken geschützt. Stellen Sie sicher, dass die Verschlüsselungseinstellungen in den Softwareoptionen aktiviert sind.
- **Antiviren-Integration**: Integrieren Sie eine zuverlässige Antivirensoftware, die in Echtzeit Sicherheitsbedrohungen erkennt und blockiert. Halten Sie diese Software stets auf dem neuesten Stand.

5.5 PC Log-In

- **Sichere Anmeldeverfahren**: Nutzen Sie die Möglichkeit der Zwei-Faktor-Authentifizierung (2FA) beim Login in die CGM MEDISTAR Software. Dies erhöht die Sicherheit erheblich und schützt vor unbefugtem Zugriff.
- **Automatische Abmeldung**: Aktivieren Sie die Funktion zur automatischen Abmeldung nach einer festgelegten Inaktivitätszeit. Dies verhindert, dass unbefugte Personen Zugriff auf Ihr System erhalten, wenn ein Benutzer seinen Arbeitsplatz verlässt.
- **Anmeldeprotokolle**: Überwachen Sie regelmäßig die Anmeldeprotokolle, um unautorisierte Zugriffe frühzeitig zu erkennen. Die Protokolle können im Administrationsbereich von CGM MEDISTAR eingesehen werden.

5.6 Externe Softwarelösungen

- **Zuverlässige Software**: Verwenden Sie nur vertrauenswürdige externe Softwarelösungen, die den Datenschutzanforderungen entsprechen. Informieren Sie sich über die Sicherheitszertifikate und Datenschutzrichtlinien der jeweiligen Anbieter.
- **Integration von Drittanbietersoftware**: Stellen Sie sicher, dass integrierte Drittanbietersoftware (z. B. Praxisverwaltungssysteme, Abrechnungssoftware) ebenfalls sicher konfiguriert ist. Überprüfen Sie die Kompatibilität mit CGM MEDISTAR und halten Sie diese Software ebenfalls regelmäßig updated.
- **Datenschutzbestimmungen**: Beachten Sie stets die datenschutzrechtlichen Bestimmungen und stellen Sie sicher, dass die externe Software die notwendigen Maßnahmen zum Schutz sensibler Patientendaten umsetzt.

5.7 Schlussfolgerung

Die Implementierung der oben genannten Empfehlungen und Module ist entscheidend für die Sicherheit Ihrer Praxisdaten und die Einhaltung der gesetzlichen Vorgaben. CGM MEDISTAR unterstützt Sie dabei, Ihre IT-Sicherheitsstrategie zu optimieren. Bei Fragen oder Unterstützung wenden Sie sich bitte an Ihren zuständigen Vertriebs- und Servicepartner.

6. Standardsoftware

a. aktueller Browser
c. Microsoft.net Framework 3.5 SP1, bzw. 4.5
d. Adobe Reader aktuelle Version

7. Unabhängige Stromversorgung (USV)

Um Spannungsspitzen abzufangen und einem plötzlichen Stromausfall entgegen zu wirken ist der Einsatz einer USV am Server zwingend erforderlich. Die Steuerungsinformationen der USV müssen an den Server weitergeleitet werden.

8. Monitor

Der Monitor muss eine Mindestauflösung horizontal von 1280 Bildpunkten und vertikal von 1024 Bildpunkten haben. Für CGM MEDISTAR Black werden mindestens 1920 Punkte horizontal und 1080 Bildpunkte vertikal vorausgesetzt (FullHD). Die Einstellung „Skalierung und Anordnung" darf nicht von der Betriebssystem-Standardeinstellung abweichen.

9. Datensicherung

Es ist eine tägliche Datensicherung der patientenbezogenen Daten gemäß den geltenden Datenschutzbestimmungen durchzuführen. Neben den Dateien aus dem Filesystem ist auf jeden Fall ein täglicher Full-Dump der Oracle-Datenbank notwendig.
Das Datensicherungsmedium muss verschlüsselt sein, bzw. die Sicherungssoftware (Veeam oder ShadowProtect) muss eine verschlüsselte Backup-Datei erstellen.

10. Terminalserverbetrieb

CGM MEDISTAR ist im Terminalserverbetrieb voll funktionsfähig. Für jeden gleichzeitig angemeldeten Benutzer sind mind. 2GB, empfohlen 4GB Arbeitsspeicher vorzusehen.

11. Virtualisierung

Grundsätzlich ist eine Virtualisierung des CGM MEDISTAR-Servers möglich. Die Parameter der virtuellen Maschine müssen den Systemanforderungen von CGM MEDISTAR entsprechen. Als Virtualisierungslayer wird HyperV empfohlen.

12. Außenstellenanbindung

Empfohlen wird eine RDP-Verbindung zum Terminalserver. Die Außenstellenanbindung sollte mit mindestens ein Business DSL mit fester IP-Adresse betragen. Die Latenzzeit der Anbindung sollte konstant (ohne Ausreißer) und gering (<=8ms) sein. Die tatsächlich benötigte Bandbreite ist abhängig von Größe und Nutzen der Außenstelle.

13. MPG – Medizinproduktegesetz

Sämtliche Computerarbeitsplätze, die an ein Medizinprodukt angeschlossen sind und somit einen direkten Patientenkontakt haben z.B. Audiometer, EKG, EEG, Lungenfunktion, Sonographiegeräte, Endoskopiegerät, Perimeter sowie Phoropter, müssen der DIN Norm EN 60601-1 entsprechen.

14. Internet

Für Funktionen wie z. B. Telematik-Anbindung, Fernwartung, Online-Update, Windows-Aktualisierung oder Online-Dienste ist eine KBV-konforme Internetverbindung erforderlich. Die gesetzlichen Bestimmungen zur Nutzung eines Internet-Zugangs sind zu beachten.

15. Virenschutz

Jeder Rechner, auch Rechner ohne Anbindung an das Internet/Intranet, muss über ein aktuelles Virenschutzprogramm verfügen. Die Aktualisierung der Signaturen muss ebenfalls stets erfolgen. Die CGM MEDISTAR-Module sind mit den Produkten „Adaptive Defense 360" „Endpoint Protection" getestet.

16. Hinweise

Sollten die Systemanforderungen in der Praxis von den vorgenannten „Systemanforderungen für den Betrieb von CGM MEDISTAR" abweichen, kann es zu Beeinträchtigungen beim Betrieb von CGM MEDISTAR kommen; etwaige Gewährleistungsansprüche können in diesem Fall nicht akzeptiert werden.

Trotz sorgfältiger Prüfung der CGM MEDISTAR-Module auf den freigegebenen Betriebssystemen kann es bei der Vielfalt an Hardware, Treibern, deren Kombination auch in Abhängigkeit des Betriebssystems zu Inkompatibilitäten kommen.

Für weiterführende Fragen wenden Sie sich gerne direkt an Ihren zertifizierten CGM MEDISTAR-Vertriebs- und Servicepartner.

CompuGroup Medical Deutschland AG
Produktbereich MEDISTAR
Stand: Juni 2025
Versionsnummer 20250612