IMMOBILIEN
WIRTSCHAFTLICHE
BERATUNG

**iwb Immobilienwirtschaftliche Beratung GmbH**

Schleinitzstraße 16
38106 Braunschweig
www.iwb-e.de

Stand: Januar 2026

# Systemanforderungen

IGIS SIX

Geschäftsführer
Oliver Helms
Registergericht
Braunschweig
HRB 3526
St.-Nummer
14/203/08316
USt.-ID-Nummer
DE 153810447
NORD/LB
IBAN: DE50 2505
0000 0001 7585 80
BIC: NOLADE2HXXX

DAS IST DER PUNKT.

## Inhalt

# 1 Vorbemerkung und Geltungsbereich

Dieses Dokument beschreibt die technischen Mindestanforderungen sowie die empfohlenen Systemvoraussetzungen für den Betrieb der Software IGIS$^{six}$. Es richtet sich an IT-Verantwortliche, Systemadministratoren und Projektverantwortliche des Lizenznehmers und gilt für den Einsatz in physischen, virtualisierten sowie terminalserverbasierten Umgebungen.

### Anwendung IGIS$^{six}$

IGIS$^{six}$ ist eine browserbasierte Webanwendung und ist durch den Einsatz von SSL-/TLS-Verschlüsselung abgesichert. Die Anwendung ist über eine HTTPS-Verbindung erreichbar. Für den Betrieb der Anwendung sind keine zusätzlichen Browser-Erweiterungen oder Plug-ins erforderlich.

Für den webbasierten Zugriff werden die Browser Google Chrome, Mozilla Firefox und Microsoft Edge (Chromium-basiert) ab Version 122 unterstützt. Der Einsatz von Google Chrome wird empfohlen, da IGIS$^{six}$ hierfür optimiert ist.

Bei der Nutzung anderer Browser (z.B. Internet Explorer) können Fehler auftreten, die unseren Entwicklern noch nicht bekannt sind.

### Mobile Datenerfassung mit IGIS$^{online}$

Zur Datenerfassung mit mobilen Endgeräten (Tablets) kann das System um die Komponente IGIS$^{online}$ erweitert werden.

IGIS$^{online}$ ist eine browserbasierte Webanwendung und über eine HTTPS-Verbindung erreichbar. Für den Betrieb der Anwendung sind keine zusätzlichen Browser-Erweiterungen oder Plug-ins erforderlich.

Für den webbasierten Zugriff auf IGIS$^{online}$ werden die Browser Google Chrome oder Apple Safari empfohlen.

Bei der Nutzung anderer Browser (z.B. Firefox, Microsoft Edge) können Fehler auftreten, die unseren Entwicklern noch nicht bekannt sind.

### Betriebsmodelle

IGIS$^{six}$ kann sowohl im lokalen Betrieb (On-Premise) innerhalb der IT-Infrastruktur des Lizenznehmers als auch alternativ in einer externen Cloud- bzw. Hosting-Umgebung betrieben werden.

Der Betrieb der Software auf einem extern gehosteten Server wird grundsätzlich empfohlen, sofern keine technischen oder organisatorischen Gründe dem entgegenstehen. Durch die Nutzung der externen Hosting-Infrastruktur können insbesondere Vorteile hinsichtlich Verfügbarkeit, Skalierbarkeit, Wartungsaufwand und Sicherheitsniveau erzielt werden. Die Entscheidung für das Betriebsmodell liegt beim Lizenznehmer unter Berücksichtigung individueller Rahmenbedingungen.

# 2 Betriebsmodell „Extern gehostet“

Der Betrieb erfolgt durch einen spezialisierten Hosting-Anbieter in einer nach ISO/IEC 27001 zertifizierten Infrastruktur innerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums. Die Einhaltung geltender Datenschutzbestimmungen (insbesondere DSGVO) ist sichergestellt.

Zu den bereitgestellten Leistungen in diesem Modell zählen insbesondere die Bereitstellung und der Betrieb der Infrastruktur, Datensicherung sowie Sicherheitsüberwachung.

# 3 Betriebsmodell „On-Premise“

## Pos. 3.1 Hardwareanforderungen – Server

- Prozessor mit 2 CPU-Kernen
- Taktfrequenz von mindestens 2.400 MHz.
- Arbeitsspeicher mindestens 8 GB, empfohlen werden 32 GB.

Der verfügbare Speicherplatz sollte mindestens 10 GB umfassen; für produktive Umgebungen und wachsende Datenbestände werden 100 bis 200 GB empfohlen.

Die Netzwerkanbindung muss mindestens 100 MBit/s leisten, empfohlen wird eine Anbindung mit 1 GBit/s.

## Pos. 3.2 Softwareanforderungen – Server

Als Datenbanksystem wird Microsoft SQL Server eingesetzt. Unterstützt werden die Versionen SQL Server 2019, 2022 und 2025 jeweils in den Editionen Standard und Enterprise.

Für die Applikationsserver werden Microsoft Windows Server 2019, 2022 und 2025 in den Editionen Standard und Datacenter unterstützt.

### Ergänzende Hinweise zum SQL-Server beim Betriebsmodell „On-Premise“

Die Performance von IGIS$^{six}$ ist maßgeblich von der Leistungsfähigkeit des eingesetzten SQL-Servers abhängig. Parallel laufende Prozesse, eingeschränkte Festplatten-I/O-Leistung oder unzureichende Hardwareausstattung können die Reaktionszeiten negativ beeinflussen.

Der Einsatz einer SQL Server Express Edition ist projektspezifisch möglich, jedoch aufgrund der Beschränkung des nutzbaren Arbeitsspeichers und der maximalen Datenbankgröße von 10 GB nur eingeschränkt empfehlenswert und kann zu Performanceeinbußen führen.

In virtualisierten Umgebungen ist sicherzustellen, dass dem SQL-Server dauerhaft ausreichend Ressourcen zugewiesen sind. Es wird empfohlen, dem virtuellen SQL-Server vier bis acht CPU-Kerne sowie mindestens 16 GB Arbeitsspeicher fest zuzuweisen.

Zur Leistungssteigerung nutzt IGIS$^{six}$ die Volltextsuche des SQL-Servers. Das Feature „Volltext- und semantische Extraktion für die Suche“ muss daher zwingend für die jeweilige SQL-Server-Instanz installiert und aktiviert sein.

## Pos. 3.3 Hardwareanforderungen – Client

Clients für den Zugriff auf IGIS$^{six}$ benötigen mindestens

- Prozessor mit 2 CPU-Kernen, empfohlen werden 4 Kerne
- Taktfrequenz von mindestens 2.400 MHz.
- Verfügbarer Arbeitsspeicher mindestens 2 GB betragen, empfohlen werden 4 GB.

Für die lokale Bereitstellung von Programm- und Cache-Daten werden mindestens 5 GB Speicherplatz benötigt, empfohlen sind 10 GB.

Die Netzwerkverbindung sollte mindestens 100 MBit/s betragen, idealerweise 1 GBit/s.

Die minimale Monitorauflösung beträgt 1280 × 1024 Pixel, empfohlen wird eine Auflösung von 1920 × 1080 Pixeln oder höher.

### Pos. 3.4 Softwareanforderungen – Client

Auf Client-Systemen wird IGIS$^{six}$ unter Microsoft Windows 10 und Windows 11 unterstützt. Alternativ ist ein Zugriff über macOS ab Version 10.9 möglich.

### Pos. 3.5 Einsatz in Terminalserverumgebungen

Bei der Nutzung von IGIS$^{six}$ in Terminalserver- oder Remote-Desktop-Umgebungen gelten mindestens die genannten Client-Anforderungen. Zusätzlich ist sicherzustellen, dass die Gesamtressourcen des Terminalservers ausreichend dimensioniert sind, um die geplante Anzahl gleichzeitiger IGIS$^{six}$-Sitzungen performancestabil zu unterstützen.

### Pos. 3.6 Internetzugang und externe Dienste

Für den Betrieb von IGIS$^{six}$ ist ein Internetzugang erforderlich. Aus dem Unternehmensnetzwerk müssen im Betriebsmodell „On-Premise“ die folgenden Domains erreichbar sein:

- tile.openstreetmap.org
- tile.openstreetmap.de
- tile.openstreetmap.com
- tile.openstreetmap.net

### Pos. 3.7 Mail-Versand

IGIS$^{six}$ kann E-Mails über einen vom Anwender bereitgestellten Mail-Server versenden. Hierzu sind die erforderlichen Einstellungen für Serveradresse, Port, Verschlüsselung und Authentifizierung in den Programm-Einstellungen zu hinterlegen. Voraussetzung für den E-Mail-Versand ist die Erreichbarkeit und korrekte Konfiguration des bereitgestellten Mail-Servers.

### Pos. 3.8 Unbeaufsichtigter Fernzugriff für Support- und Wartungszwecke

Für den effizienten Betrieb sowie für Support-, Analyse- und Wartungsmaßnahmen ist ein unbeaufsichtigter, technisch kontrollierter Fernzugriff auf die IGIS$^{six}$ -Systemumgebung bereitzustellen. Ein solcher Zugriff ermöglicht eine zeitnahe Fehlerdiagnose, Systemüberwachung und Wartung auch außerhalb regulärer Betriebszeiten ohne die unmittelbare Interaktion eines Anwenders auf dem Zielsystem.

Der Fernzugriff betrifft ausschließlich System- und Applikationsebenen (z. B. Applikationsserver, Datenbankserver, Konfigurations- und Log-Ebene) und erfolgt nicht auf Benutzerarbeitsplätzen, sofern nicht explizit vereinbart.

Technisch geeignete Zugriffsszenarien sind unter anderem:

- Netzwerkbasierter Zugriff über VPN mit Authentifizierung gegen die Unternehmens-Infrastruktur des Lizenznehmers,
- Zugriff über dedizierte Remote-Desktop- oder Jump-Host-Systeme innerhalb einer abgesicherten Management-Zone,
- Nutzung vom Lizenznehmer freigegebener Remote-Support-Werkzeuge mit rollenbasierter Zugriffsbeschränkung (z.B. TeamViewer),

- alternativ zeitlich begrenzte, wartungsbezogene Zugriffskonten mit Protokollierung und automatischer Deaktivierung.

Die konkrete technische Ausgestaltung, Aktivierung und Freigabe des unbeaufsichtigten Fernzugriffs liegt vollständig in der Hoheit des Lizenznehmers und erfolgt ausschließlich nach vorheriger technischer, organisatorischer und ggf. vertraglicher Abstimmung.

Bei Betrieb von IGIS$^{six}$ auf einem extern gehosteten Server ist kein unbeaufsichtigter Fernzugriff auf Systeme des Lizenznehmers erforderlich.

# 4 Zwei-Faktor-Authentifizierung (2FA)

### Pos. 4.1 Allgemeines

IGIS$^{six}$ unterstützt den Start und Zugriff mit Zwei-Faktor-Authentifizierung (2FA), um die Sicherheit von Benutzerkonten und sensiblen Daten zu erhöhen. Der Einsatz von 2FA wird insbesondere bei externem Zugriff, mobilen Arbeitsplätzen sowie für administrative Benutzerkonten empfohlen.

### Pos. 4.2 Technische Voraussetzungen

Für die Nutzung der Zwei-Faktor-Authentifizierung müssen Server- und Client-Systeme zeitlich synchronisiert sein. Zudem ist eine sichere HTTPS-Kommunikation für den Anmeldeprozess erforderlich. Je nach Konfiguration kann ein Zugriff auf externe oder interne Authentifizierungsdienste notwendig sein.

Benutzer benötigen ein geeignetes zweites Authentifizierungsmedium beispielsweise eine Authenticator-App (z. B. Microsoft Authenticator) oder ein hardwarebasiertes Token.

Für die Umsetzung der Authentifizierung wird der Einsatz eines zentralen, standardisierten Identitätsdienstes empfohlen. Bevorzugt soll hierzu Microsoft Entra ID (ehemals Azure Active Directory) verwendet werden, insbesondere zur Realisierung von Single Sign-on (SSO) und Zwei-Faktor-Authentifizierung (2FA).

Der Einsatz alternativer Authentifizierungsverfahren oder Identity-Provider ist grundsätzlich möglich, bedarf jedoch einer vorherigen technischen Prüfung sowie Abstimmung. Eine Gewährleistung für die Unterstützung, Kompatibilität oder vollständige Integration solcher alternativen Verfahren kann nicht gegeben werden.

### Pos. 4.3 Start von IGIS$^{six}$ mit aktivierter 2FA

Beim Anmeldevorgang werden Benutzer nach Eingabe ihres Benutzernamens und Passworts zur Eingabe eines zweiten Authentifizierungsfaktors aufgefordert. Erst nach erfolgreicher Prüfung beider Faktoren wird der Zugriff auf IGIS$^{six}$ gewährt.

# 5 Anmeldung, Sitzungssicherheit und Zugriff

IGIS$^{six}$ stellt Mechanismen zur sicheren Anmeldung und Sitzungsverwaltung bereit. Ziel ist es, unbefugte Zugriffe zu verhindern und zugleich einen stabilen und benutzerfreundlichen Betrieb sicherzustellen. Die nachfolgenden Regelungen gelten für den Normalbetrieb sowie für den Einsatz externer Authentifizierungsverfahren.

### Pos. 5.1 Automatische Abmeldung bei Inaktivität (Timeout)

Aus Sicherheitsgründen wird ein Benutzer nach einer administrativ konfigurierbaren Zeit der Inaktivität automatisch abgemeldet.

Als Inaktivität gilt ein Zeitraum ohne Benutzerinteraktion innerhalb der Anwendung.

Nach Ablauf der festgelegten Zeit wird die aktive Sitzung beendet. Für die weitere Nutzung von IGIS$^{six}$ ist anschließend eine erneute Anmeldung erforderlich. Die Timeout-Dauer kann an organisatorische Sicherheitsvorgaben und betriebliche Anforderungen angepasst werden. Für produktive Umgebungen wird ein ausgewogener Wert empfohlen, der sowohl Sicherheitsaspekte als auch Benutzerfreundlichkeit berücksichtigt.

### Pos. 5.2 Timeout-Regelung im Normalbetrieb

Im Normalbetrieb mit interner Authentifizierung erfolgt die Sitzungsverwaltung vollständig innerhalb von IGIS$^{six}$.

Die automatische Abmeldung wird ausschließlich durch die konfigurierte Inaktivitätszeit gesteuert. Nach deren Überschreitung wird die Sitzung serverseitig beendet und der Benutzer aktiv abgemeldet.

Diese Regelung dient insbesondere dem Schutz vor unbefugtem Zugriff an unbeaufsichtigten Arbeitsplätzen oder in gemeinsam genutzten Umgebungen.

### Pos. 5.3 Timeout-Regelung bei Betrieb mit OpenID Connect (OIDC)

Wird IGIS$^{six}$ in Verbindung mit einem OIDC-basierten Identitätsprovider (z. B. Single-Sign-On-Lösungen innerhalb eines Unternehmens) betrieben, gelten ergänzend die Sitzungsvorgaben des jeweiligen Identity-Providers.

In diesem Betriebsmodus ergibt sich die maximale Sitzungsdauer aus dem Zusammenspiel von:

- der IGIS$^{six}$ -internen Inaktivitäts-Timeout-Regelung sowie
- den vom OIDC-Provider definierten Session- und Token-Laufzeiten.

Eine automatische Abmeldung erfolgt, sobald entweder:

- die konfigurierte Inaktivitätszeit in IGIS$^{six}$ überschritten wird oder
- die Authentifizierungs-Session bzw. das Zugriffstoken des OIDC-Providers abläuft.

Es wird empfohlen, die Timeout-Parameter in IGIS$^{six}$ und im OIDC-Provider konzeptionell aufeinander abzustimmen, um sicherheitsrelevante oder unerwartete Abmeldungen zu vermeiden.

Die Verantwortung für die Konfiguration, Überwachung und den sicheren Betrieb der OIDC-Integration liegt beim Lizenznehmer.

### Pos. 5.4 Sicherheitshinweis

Die automatische Abmeldung bei Inaktivität stellt eine wesentliche Sicherheitsmaßnahme dar und empfiehlt sich insbesondere bei

- extern zugänglichen Systemen,
- mobilen Endgeräten,

- Terminalserver- und Mehrbenutzerumgebungen,
- bei der Nutzung von Zwei-Faktor-Authentifizierung (2FA)

**Pos. 5.5 Betrieb und Verantwortung**

Die Verwaltung der Zwei-Faktor-Authentifizierung, einschließlich der Ausgabe, Sperrung und Wiederherstellung von Authentifizierungsfaktoren, liegt in der Verantwortung des Lizenznehmers. Bei Verlust von Authentifizierungsmedien oder Benutzerwechseln sind organisatorische und technische Maßnahmen zu treffen, um den sicheren Betrieb zu gewährleisten.

## 6 Ergänzende Hinweise zum Gesamtsystem

Aufgrund der Komplexität moderner Software- und Hardwarelandschaften kann trotz sorgfältiger Entwicklung, Prüfung und Wartung eine vollständige Fehlerfreiheit der Software nicht garantiert werden.

Sollten einzelne Systemvoraussetzungen nicht oder nur eingeschränkt erfüllt werden können, wird zwischen Auftragnehmer und Lizenznehmer gemeinsam eine technisch und wirtschaftlich vertretbare Lösung abgestimmt.