

ibi systems iris

Systemanforderungen und Installation

Stand: Release 24/R1

25.03.2024



systems

ibi systems GmbH
Rudolf-Vogt-Straße 6
93053 Regensburg
www.ibi-systems.de

Inhalt

1	Einführung.....	4
2	Architektur und Systemanforderungen.....	4
2.1	Architektur.....	4
2.2	Systemanforderungen.....	5
3	Vorbereitungen zur Installation.....	6
3.1	Installations-Reihenfolge.....	6
3.2	Infrastruktur.....	6
3.3	Installation/Einrichtung Datenbankserver.....	7
3.4	Installation/Einrichtung Anwendungsserver.....	16
4	Einrichtung und Konfiguration von Anwendungspool, Website, REST-API.....	17
4.1	Automatisierte Einrichtung.....	17
4.2	Manuelle Einrichtung.....	20
5	Installation und Konfiguration der Anwendung.....	26
5.1	Installation der Anwendung.....	26
5.2	Konfiguration der Anwendung.....	27
5.3	Konfiguration der REST-API.....	31
5.4	Konfiguration der SSO-Authentifizierungsmöglichkeiten.....	31
6	Erster Programmstart.....	32
6.1	Anlage der Datenbank-Strukturen.....	32
6.2	Eingabe der initialen Daten.....	32
6.3	Testen der Anwendungskonfiguration.....	33
6.4	Start der REST-API.....	34
7	Anhang – Zusätzliche Konfigurationsmöglichkeiten.....	34
7.1	Einrichtung der E-Mail-Konfiguration - Nutzung des Kommandozeilen-Tools.....	34
7.2	Einrichten der LDAP-Anbindung.....	35
7.3	Einrichtung SSO - Windows Authentifizierung.....	38
7.4	Einrichtung SSO - Authentifizierung via OKTA (SAML 2.0).....	40
7.5	Einrichtung einer Warm Up Routine für schnelleren Erstzugriff.....	44
7.6	Hinzufügen eines Active Directory Benutzers zur Gruppe IIS_IUSRS.....	45
8	Serverumzug / Servermigration.....	47
9	Übliche Betriebsaufgaben.....	47
9.1	Hersteller Dokumentationen und Know-How.....	47
9.2	Starten der Anwendung - Application Pool (Webseite oder Api).....	48

9.3	Stoppen der Anwendung – Application Pool (Webseite oder Api).....	48
9.4	Starten einer Site.....	49
9.5	Stoppen einer Site	50
10	Update der Anwendung.....	51
10.1	Vorbereitungsschritte.....	51
10.2	Update der Anwendung	52
10.3	Update der Datenbank.....	52
11	Problembehebung	54
11.1	Fehler 500.30 App failed to start.....	54
11.2	Fehler 500.31 Failed to Load Asp.net core runtime.....	54
11.3	Fehler 500.19 Internal Server Error.....	54
11.4	Fehlermeldung (Provided certificate is not valid for ..).....	54
11.5	Fehlermeldung (Die aktuelle Datenbankstruktur ist veraltet).....	55
11.6	Fehlermeldung (Missing Connection String) Update.....	55

1 Einführung

Im vorliegenden Dokument werden die Systemanforderungen, die Installation und Konfiguration der Software iris beschrieben. Der Aufbau der Dokumentation orientiert sich an der Abfolge der einzelnen Installationsschritte. Die Einhaltung der Reihenfolge ist zu empfehlen. Im Anhang werden zudem noch weitere, jedoch nicht für jeden Kunden relevante Konfigurationsmöglichkeiten erläutert.

2 Architektur und Systemanforderungen

2.1 Architektur

Die Software-Iris ist eine .NET Core-Webanwendung, für deren Betrieb ein Windows Server mit installiertem **Microsoft Internet Information Services (IIS)**, eine **MSSQL-Datenbank** sowie ein **SMTP-Server** für den Versand von E-Mails benötigt werden.

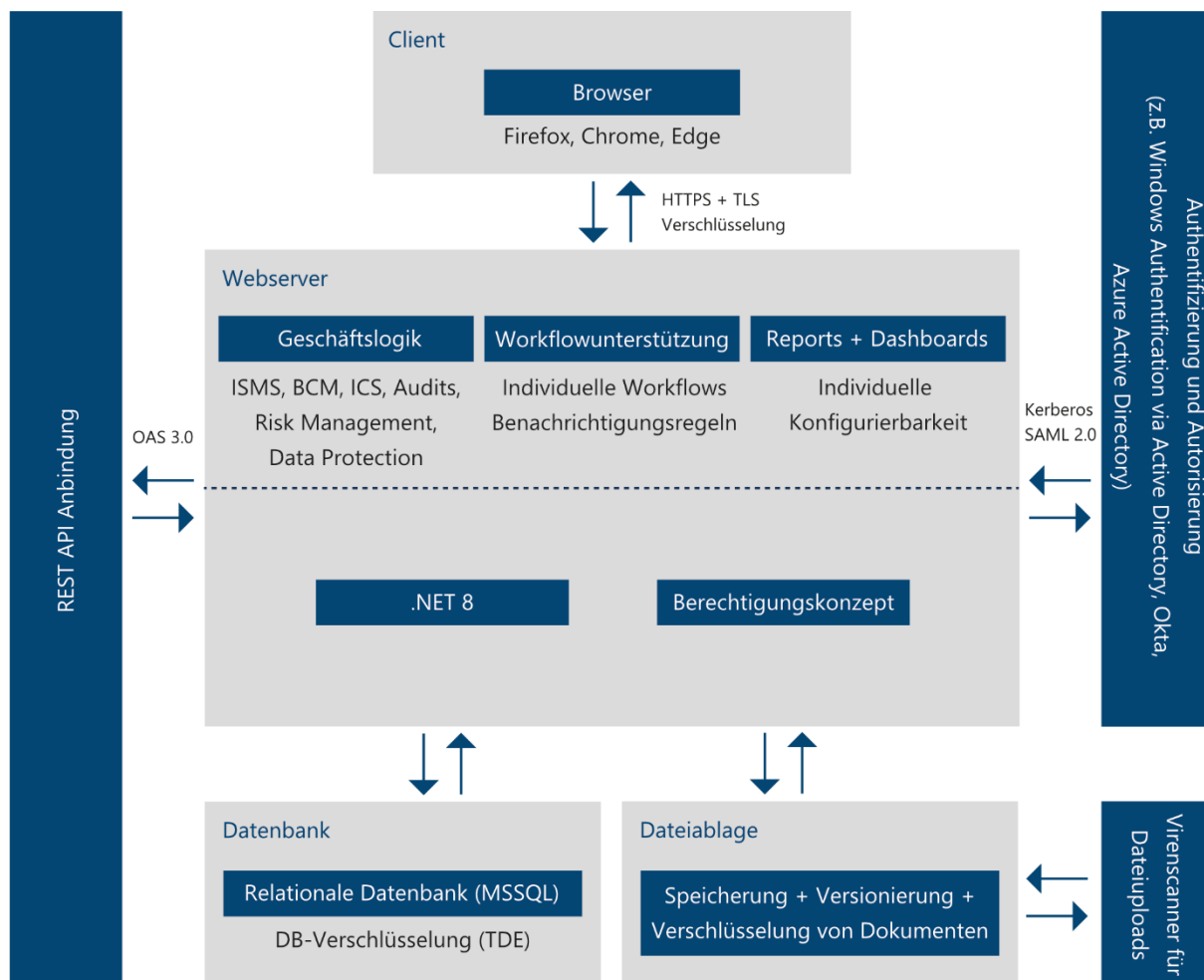


Abbildung 1 - Architekturschaubild ibi systems iris

2.2 Systemanforderungen

Die Anforderungen an die Systeme sind abhängig von der Anzahl der Benutzer und der Nutzungsart der Anwendung. Im Folgenden werden die Mindest- sowie die empfohlenen Systemanforderungen definiert. Abweichende Anforderungen durch kundenspezifische Erweiterungen sind hierbei nicht berücksichtigt.

2.2.1 Server

Komponente	Mindestanforderung	Empfohlen
Prozessor	4 vCore / 4 Core	8 vCore / 8 Core
RAM	4 GB	16 GB
Speicherplatz (Betriebssystem)	40 GB	80 GB
Speicherplatz (Anwendung)	500 MB	
Speicherplatz (Daten)	10 GB mit der Möglichkeit zur flexiblen Erweiterung	

2.2.2 Betriebssystem

Komponente	Mindestanforderung	Empfohlen
Betriebssystem	Windows Server 2016 (x64)	Windows Server 2022 (x64)
IIS	Version 10.0	Version 10.0
.NET-Framework	Version 8 (Hosting-Paket)	
Hostname und SSL-Zertifikat	Es wird empfohlen, für den Anwendungsserver einen Hostnamen (z. B. iris.company.tld) mit zugehörigem SSL-Zertifikat zu definieren.	

2.2.3 Datenbank

Komponente	Mindestanforderung	Empfohlen
Datenbank	Microsoft SQL-Server 2016 (*)	Microsoft SQL-Server 2022
Prozessor	2 vCore / 2 Core	4 vCore / 4 Core
RAM	4 GB	8 GB
Erwartete Größe Datenbestand	Abhängig von der Nutzungsart. Anfangsgröße: ca. 100 MB; Mit steigender Einsatzdauer mehrere GB.	

(*) Grundsätzlich ist der Betrieb auch mit der kostenfreien Express-Edition des Microsoft SQL-Servers (ab Version 2016) möglich. Die Datenbankgröße ist hierbei jedoch auf 10 GB begrenzt. Zudem nutzt die Express-Edition lediglich 1,5 GB RAM und vier Prozessorkerne.

2.2.4 Domänen-Namen (DNS) & Transportverschlüsselung (TLS)

Um Benutzern den Zugriff auf die Anwendung zu ermöglichen, werden 2 DNS-Einträge (je Umgebung) benötigt um den Zugriff auf die Webseite, sowie die Rest-API zu ermöglichen.

Um den Datenverkehr zwischen Client und der Anwendung zu sichern ist, sofern die Transportverschlüsselung (SSL/TLS) nicht über einen Load-Balancer / Reverse Proxy terminiert wird, für jeden der angelegten DNS-Einträge ein gültiges Zertifikat erforderlich

2.2.5 Client

Die Software ibi systems iris wird auf Kompatibilität zu den aktuellen ESR-Versionen der folgenden Browser getestet:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

3 Vorbereitungen zur Installation

3.1 Installations-Reihenfolge

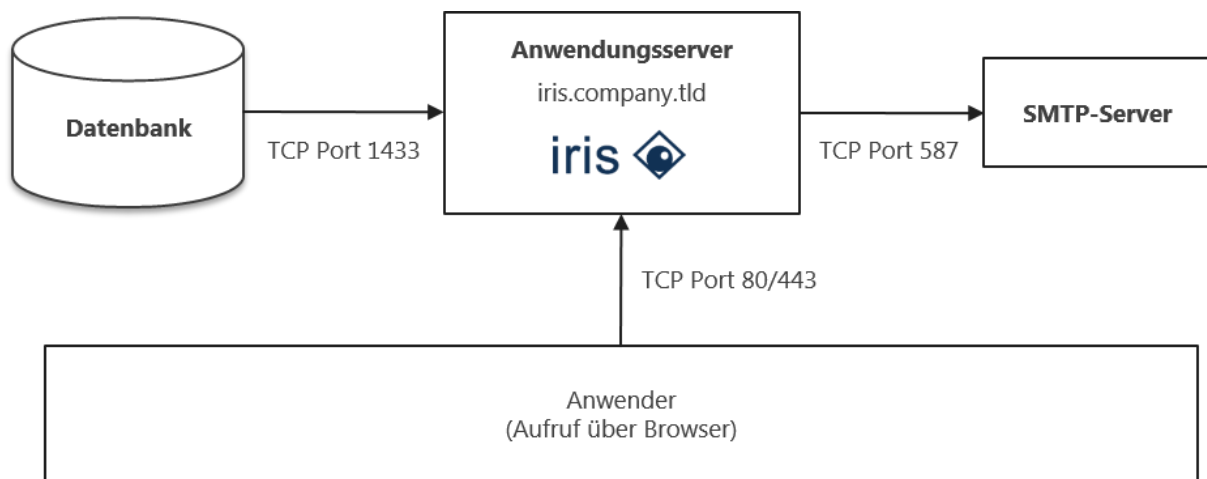
- Installation und Konfiguration des Datenbank Servers
- Installation und Konfiguration der benötigten Serverrollen in Windows
- Installation des Hosting Bundles
- Installation der Anwendung

3.2 Infrastruktur

iris kann sowohl eine **lokale Datenbank** als auch einen **separaten Datenbankserver** anbinden. Im letztgenannten Fall muss eine Portfreischaltung (standardmäßig TCP-Port 1433) zwischen Anwendungs- und Datenbankserver erfolgen.

Zum Zugriff auf den **SMTP-Server** muss ebenfalls ein Port (standardmäßig TCP-Port 587) freigeschaltet werden.

Es wird empfohlen, für den Anwendungsserver einen **DNS-Eintrag** zu hinterlegen (z. B. iris.company.tld). Ein **SSL-Zertifikat** muss installiert werden, um einen sicheren Datenaustausch zwischen Server und Clients (Browser) zu gewährleisten.



Hinweis: Die genannten Ports sind Standard-Ports. Abweichungen sind möglich.

3.3 Installation/Einrichtung Datenbankserver

Zum Betrieb der Anwendung werden zwei Datenbankbenutzer benötigt.

Der privilegierte Anwendungs-Benutzer führt Änderungen an Datenbank Schematas aus und wird für die Erstinstallation und den Update-Prozess benötigt.

Der nicht privilegierte Anwendungsbenutzer wird für den Regel-Betrieb der Anwendung verwendet.

Hinweis: Es wird ausdrücklich empfohlen, für die Datenbank eine entsprechende **Backup-Strategie** zu konzipieren und zu implementieren. Eine Empfehlung finden Sie unter:

<https://learn.microsoft.com/de-de/sql/relational-databases/backup-restore/back-up-and-restore-of-sql-server-databases?view=sql-server-ver16#design-your-backup-strategy>

3.3.1 Datenbank – Konfiguration

Um die Performance bei asynchronen Funktionen zu verbessern und um Datenbank-Deadlocks zu vermeiden, sollte die Datenbank-Option „Is Read Committed Snapshot On“ (zu Deutsch: **Ist aktivierte READ COMMITTED-Momentaufnahme**) auf **True** gesetzt werden.

Öffnen Sie nach einem Rechtsklick auf die iris-Datenbank die **Eigenschaften** und wählen dort den Unterpunkt **Optionen**:

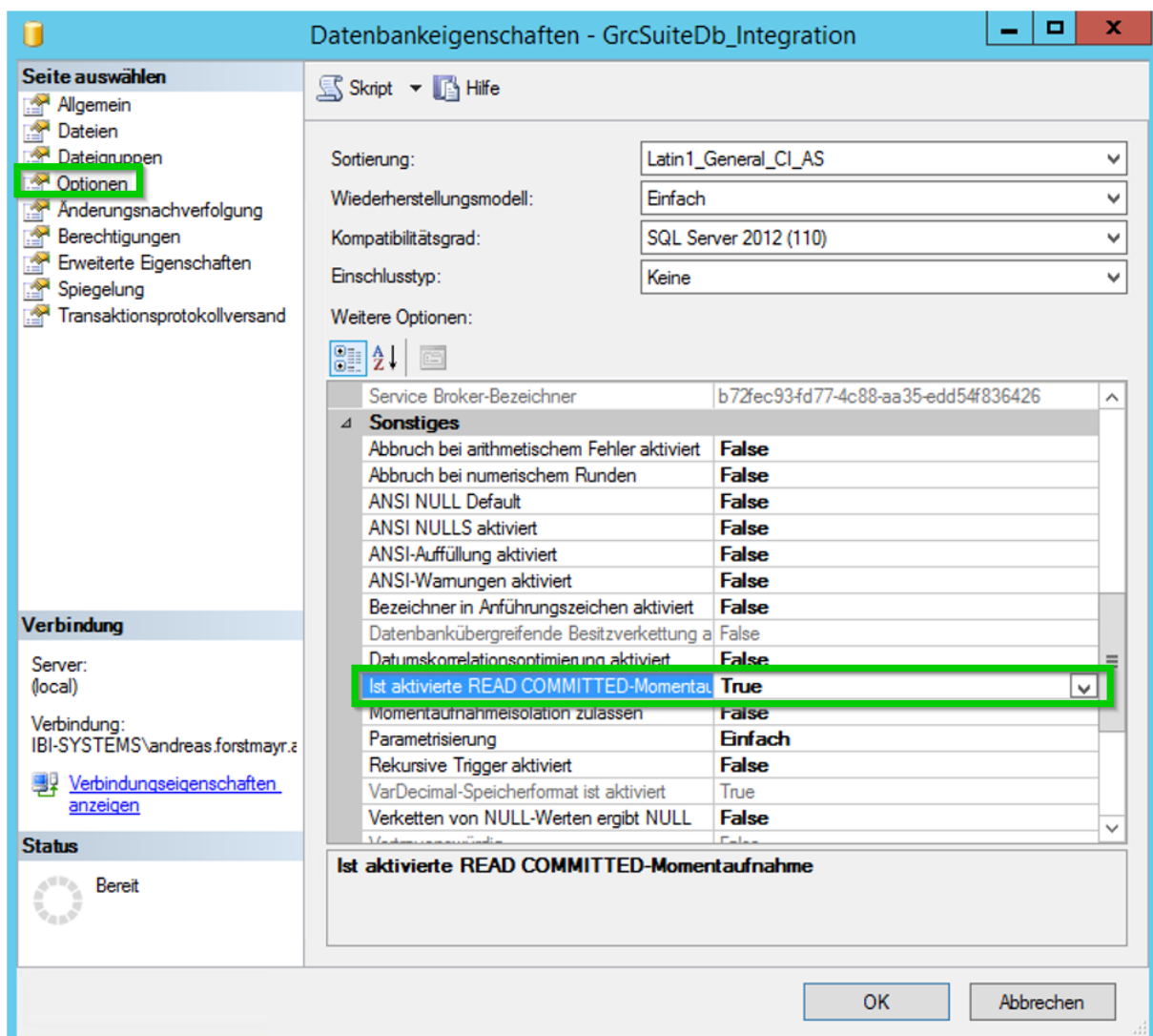


Abbildung 2 – Datenbank Eigenschaften – Optionen - sonstiges (Read Committed)

3.3.2 SQL Server Logins

Benötigte Rollen für den privilegierten Anwendungs-Benutzer (Administrationsbenutzer)

- db_datareader
- db_datawriter
- db_ddladmin
- db_securityadmin

Benötigte Rollen für den nicht privilegierten Anwendungsbenutzer (Anwendungsbenutzer)

- db_datareader
- db_datawriter

3.3.3 besondere Datenbank-Berechtigungen

Außerdem nutzt iris auf Datenbank-Seite auch sogenannte „User-defined functions“. Damit die dem Datenbank-Schema zugeordneten Benutzer diese Funktionen auch verwenden dürfen, ist es notwendig, den Datenbanknutzern die zusätzliche Berechtigung EXECUTE zuzuweisen.

Öffnen Sie nach einem Rechtsklick auf die iris-Datenbank die **Eigenschaften** und wählen dort den Unterpunkt **Optionen**:

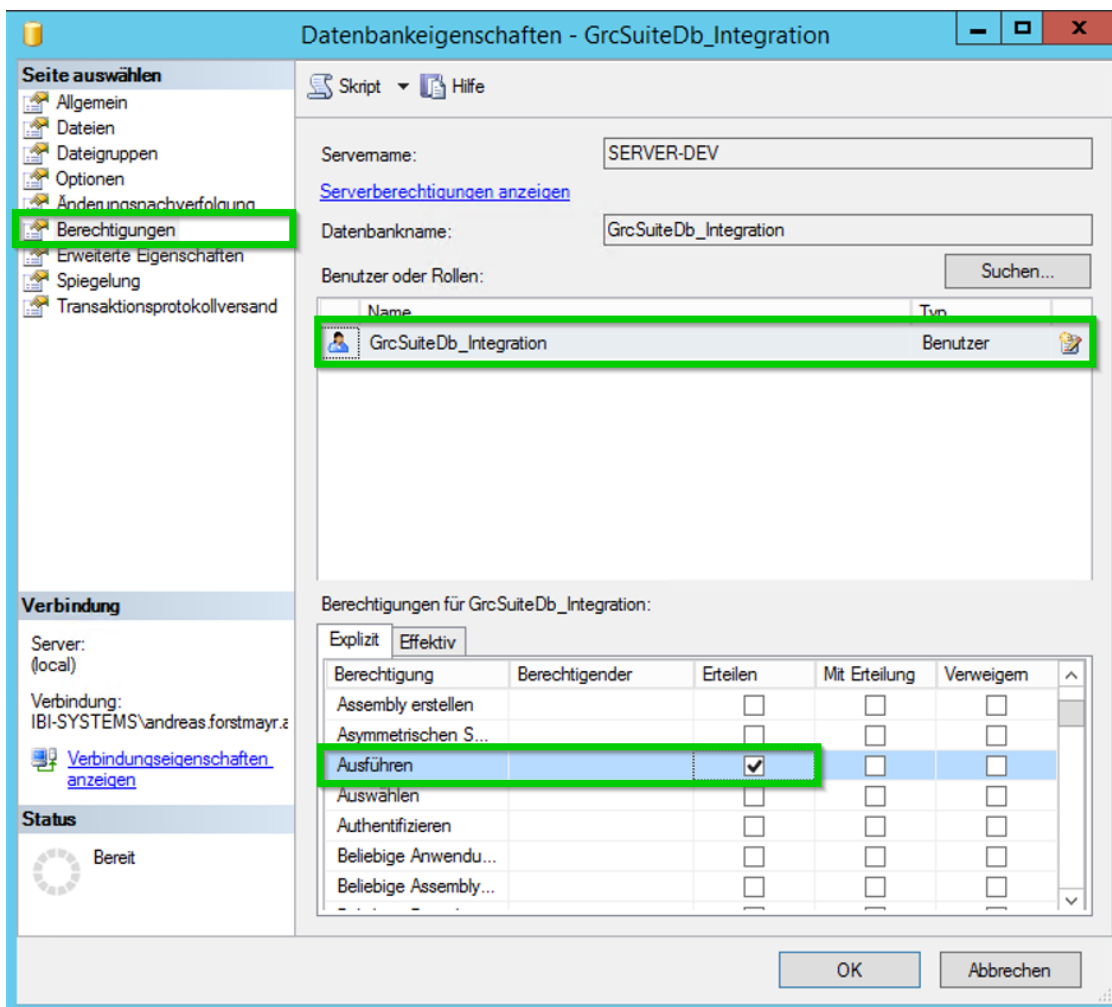


Abbildung 3 Datenbank-Eigenschaften – Berechtigungen - Ausführungsberechtigungen

3.3.4 Einrichtung eines MSSQL-Wartungsplans für Indizes und Statistiken

Im Laufe des Betriebs einer MSSQL-Datenbank werden eine große Anzahl an Bearbeitungsvorgängen - wie das Hinzufügen und Löschen von Tabelleneinträgen - entstehen, welche die Struktur der vorhandenen Datenbankindizes beeinträchtigen.

Um eine gute Reaktionszeit der Anwendung zu gewährleisten, muss ein **Wartungsplan für den Wiederaufbau der Datenbankindizes** eingerichtet werden.

In diesem Kapitel wird mit Hilfe von *Microsoft SQL Server Management Studio* das Vorgehen zur Einrichtung eines Wartungsplans für den Wiederaufbau der Datenbankindizes beschrieben.

Hinweis: Das Feature der Erstellung von Wartungsplänen ist in der *Microsoft SQL Server Express Edition* nicht verfügbar.

3.3.5 Vorbereitung

Verbinden Sie im *Microsoft SQL Server Management Studio* den Datenbankserver, unter dem die *ibi systems iris*-Datenbank läuft.

3.3.5.1 Aktivierung SQL Server Agent

Der **SQL Server Agent** ist für die Ausführung von Wartungsplänen erforderlich und muss aktiv sein. Der **SQL Server Agent** lässt sich mit folgendem Befehl in einem neuen Abfrage-Fenster aktivieren:

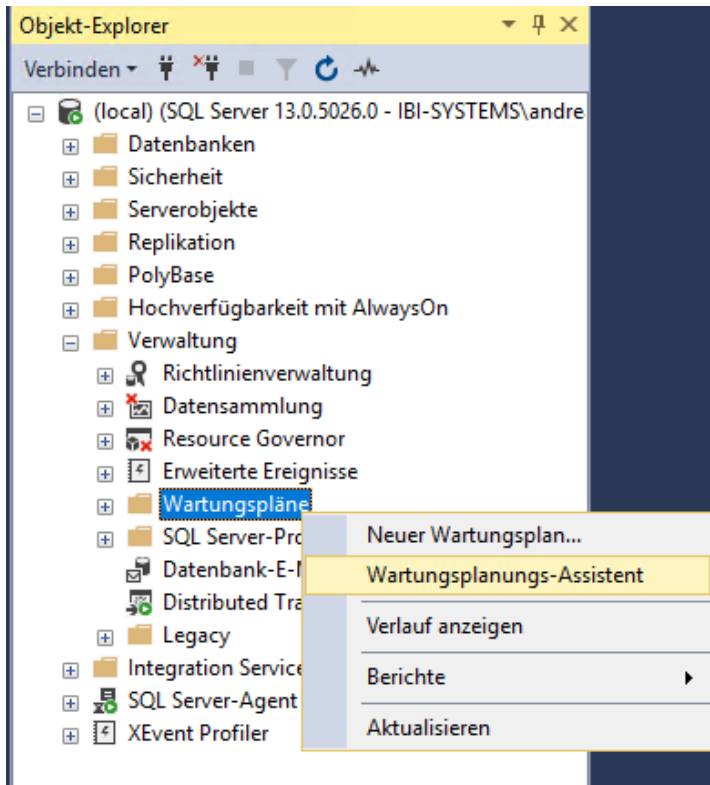
```
sp_configure 'show advanced options', 1;  
GO  
RECONFIGURE;  
GO  
sp_configure 'Agent XPs', 1;  
GO  
RECONFIGURE;
```

3.3.6 Wartungsplan einrichten

3.3.6.1 Wartungsplanungs-Assistent öffnen

Mit verbundenem Datenbankserver erscheint im *Microsoft SQL Server Management Studio* die Server-Baumstruktur. Navigieren Sie in der Baumstruktur zu „**Verwaltung >> Wartungspläne**“.

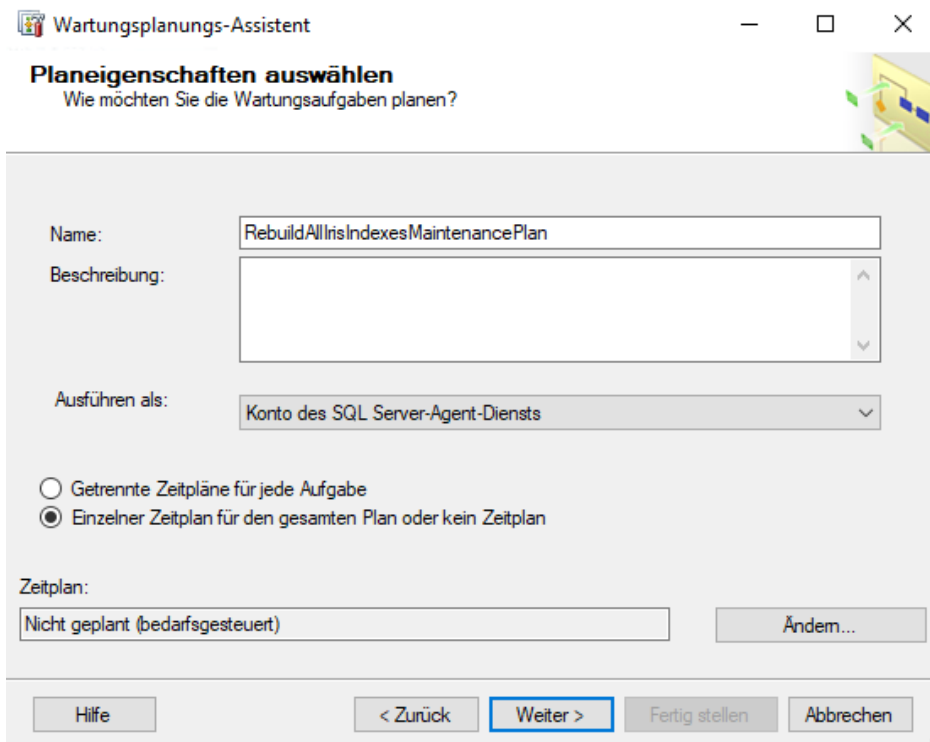
Mit einem Rechtsklick auf den Ordner „**Wartungspläne**“ erscheint das Kontextmenü, in dem der Eintrag „**Wartungsplanungs-Assistent**“ ausgewählt werden muss.



Zunächst öffnet sich das Einleitungsfenster, in dem nur die Schaltfläche „Weiter“ betätigt werden muss.

3.3.6.2 Name und Auftragszeitplan

Im ersten Wizard-Fenster müssen der Name und Zeitplan festgelegt werden. Der empfohlene Name ist unten abgebildet.



Mit einem Klick auf die Schaltfläche „Ändern...“ erscheint das Zeitplanfenster.

Der empfohlene Zeitplan ist abgebildet:

Neuer Auftragszeitplan

Name: Aufträge im Zeitplan

Zeitplantyp: Aktiviert

Einmalig

Datum: Uhrzeit:

Häufigkeit

Auftreten:

Wiederholen alle: Woche(n) am

Montag Mittwoch Freitag Samstag
 Dienstag Donnerstag Sonntag

Häufigkeit pro Tag

Einmalig um:
 Alle: Stunde(n) Start:
 Ende:

Dauer

Startdatum: Enddatum:
 Kein Enddatum:

Zusammenfassung

Beschreibung:

Bestätigt wird der Zeitplan mit der Schaltfläche „OK“ und dann „Weiter“.

3.3.6.3 Wartungstasks auswählen

Im Aufgabenfenster wird festgelegt, was genau geschehen soll. Hier müssen die Aufgaben „Index neu erstellen“ und „Statistiken aktualisieren“ selektiert werden.

Wartungsplanungs-Assistent

Wartungstasks auswählen
 Welche Tasks soll dieser Plan ausführen?

Einen oder mehrere Wartungstasks auswählen:

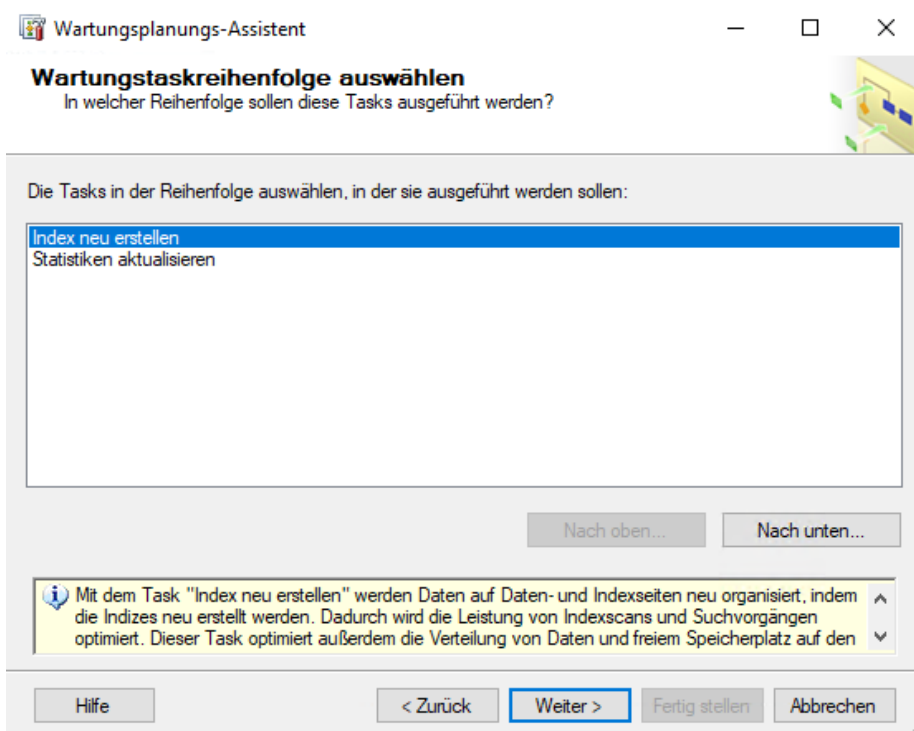
- Datenbankintegrität überprüfen
- Datenbank verkleinern
- Index neu organisieren
- Index neu erstellen
- Statistiken aktualisieren
- Verlauf bereinigen
- Auftrag des SQL Server-Agents ausführen
- Datenbank sichern (vollständig)
- Datenbank sichern (differenziell)
- Datenbank sichern (Transaktionsprotokoll)
- Wartung bereinigen

Der Task "Statistiken aktualisieren" stellt sicher, dass der Abfrageoptimierer über aktuelle Informationen zur Verteilung von Datenwerten in den Tabellen verfügt. Auf diese Weise kann der Abfrageoptimierer fundiertere Entscheidungen zu Datenzugriffsstrategien treffen.

Zur Übernahme der Auswahl muss die Schaltfläche „Weiter“ betätigt werden.

3.3.6.4 Wartungstaskreihenfolge auswählen

Die Aufgaben werden wie abgebildet automatisch richtig sortiert, weshalb die Reihenfolge einfach mit einem Klick auf „Weiter“ bestätigt werden kann. Falls eine andere Reihenfolge erscheint, lässt sich diese mit den Schaltflächen „Nach oben...“ und „Nach unten...“ bearbeiten.

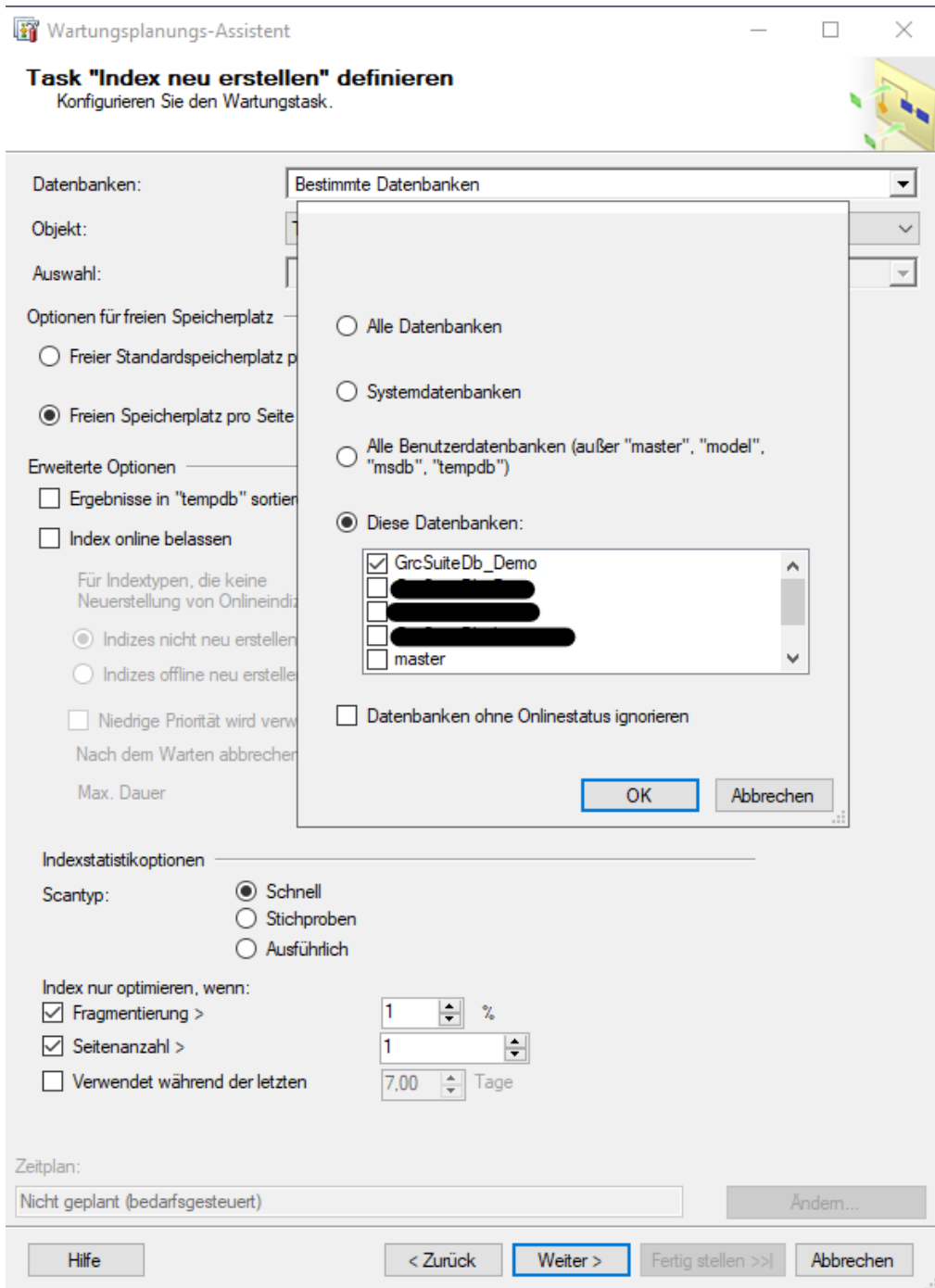


3.3.6.5 Task „Index neu erstellen“ definieren

Zunächst muss die *ibi systems iris*-Datenbank ausgewählt werden, damit der Wartungsplan nicht alle Datenbanken in der aktuellen Serverinstanz bearbeitet. Mit einem Klick auf die aufklappbare Liste „Datenbanken“ erscheint die Datenbankliste, in der die *ibi systems iris*-Datenbank mit Hilfe eines Hakens ausgewählt werden muss.

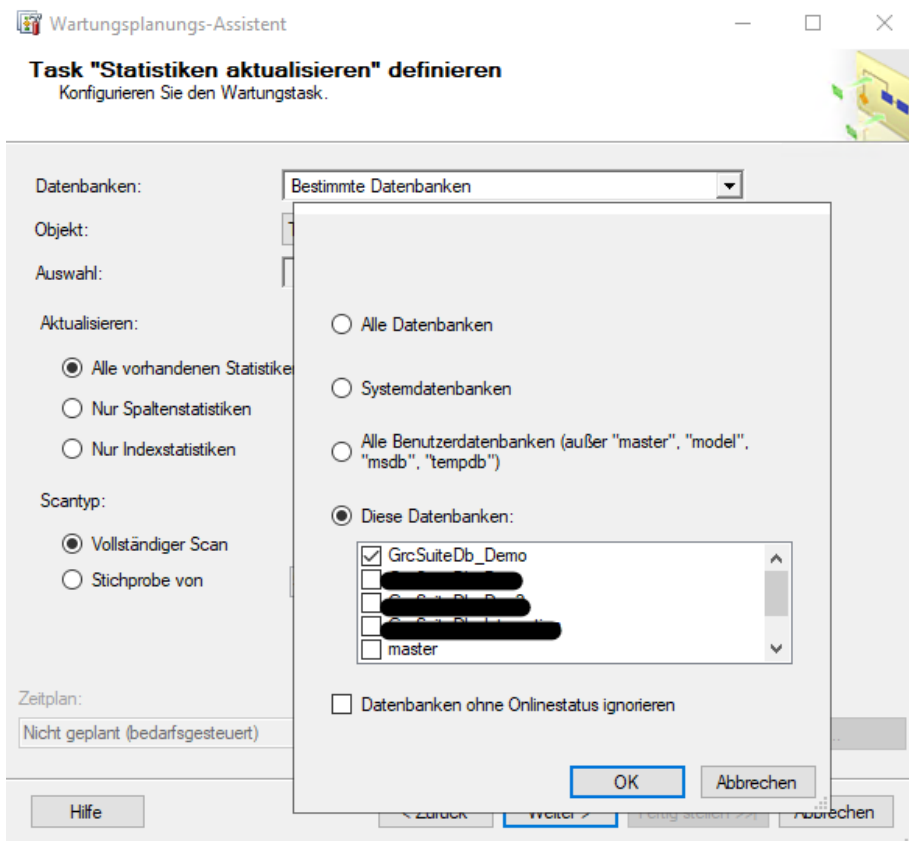
Des Weiteren sind folgende Werte empfohlen:

- Freien Speicherplatz pro Seite ändern in: **20%**
- Fragmentation >: **1%**
- Page Count >: **1**



3.3.6.6 Task „Statistiken aktualisieren“ definieren

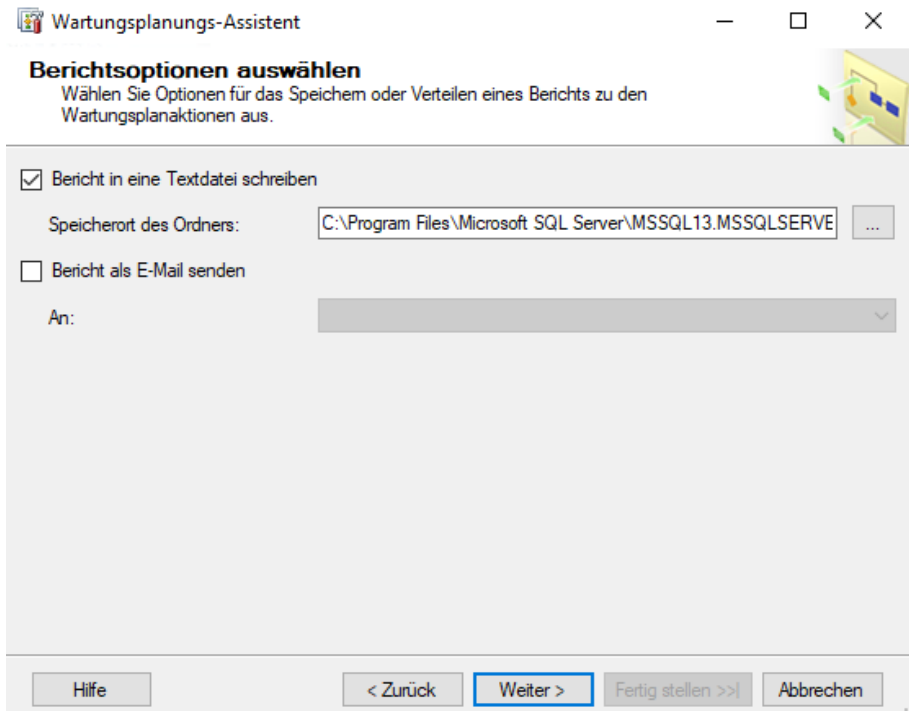
Hier muss nur die *ibi systems iris*-Datenbank über die aufklappbare Liste „Datenbanken“ und mit Setzen des Hakens ausgewählt werden.



Die Bestätigung der Auswahl erfolgt mit Betätigen der Schaltfläche „OK“ und dann „Weiter“.

3.3.6.7 Berichtsoptionen auswählen

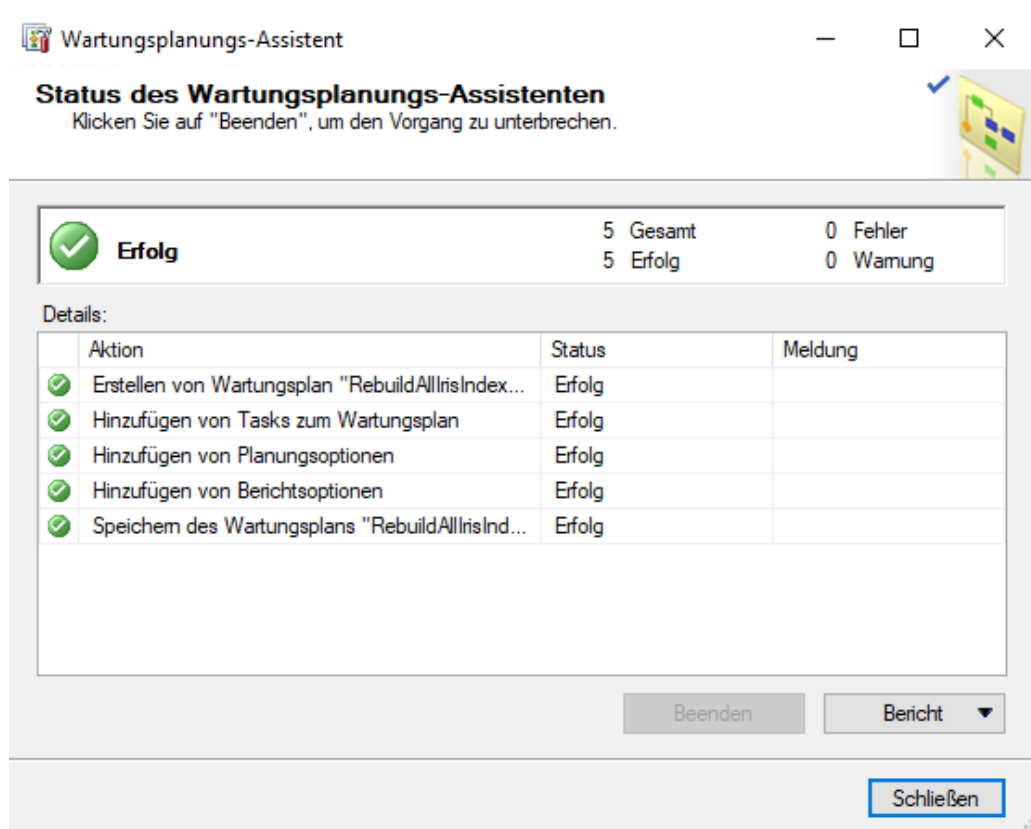
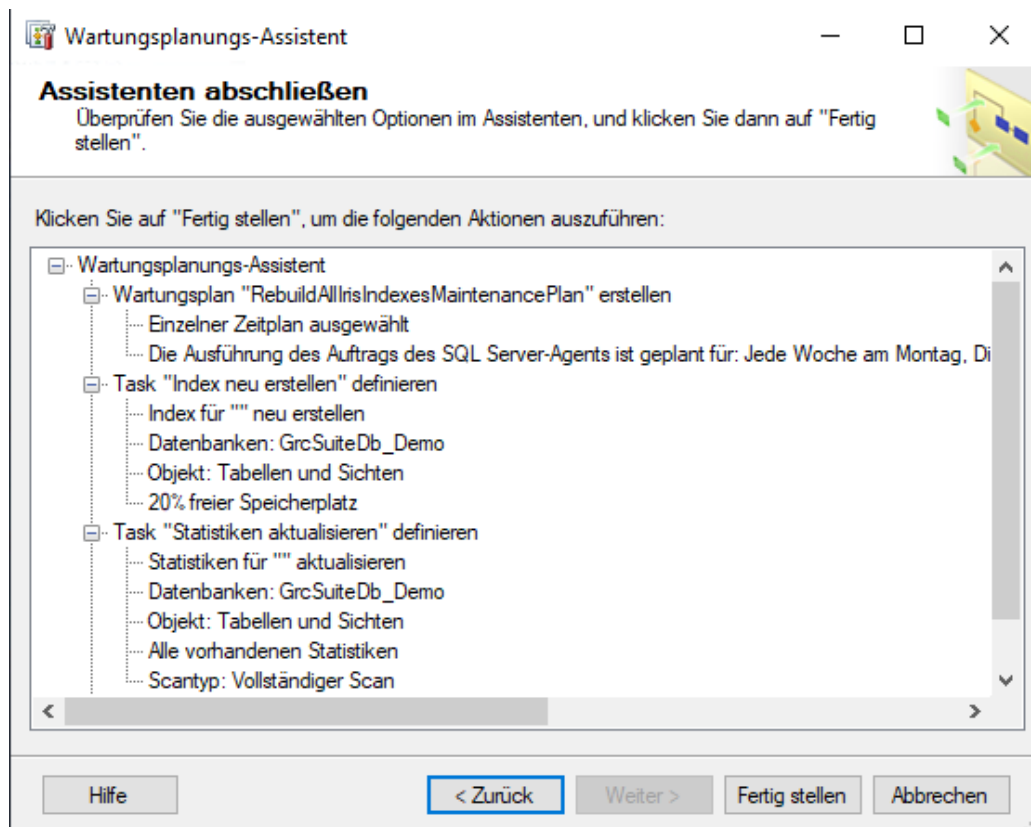
Optional kann für den Wartungsplan eine Log-Datei angelegt werden, damit die Ergebnisse überprüft werden können.



3.3.6.8 Assistenten abschließen

Zum Schluss werden die vorherigen Schritte in einer Übersicht angezeigt.

Mit Betätigen der Schaltfläche „Fertig stellen“ wird der Wartungsplan erstellt.



Der Wartungsplan ist nun erstellt und wird nach dem gewählten Zeitplan automatisch ausgeführt.

Hinweis: Das Feature der Erstellung von Wartungsplänen ist in der *Microsoft SQL Server Express Edition* nicht verfügbar.

3.4 Installation/Einrichtung Anwendungsserver

3.4.1 *Windows-Server-Features / Rollen*

Hinweis: Wahlweise können alle benötigten IIS-Features auch automatisiert über das in Punkt 4.1.1 beschriebene PowerShell-Skript installiert/aktiviert werden.

Folgende Windows-Features müssen bei bereits installiertem IIS zur Ausführung von iris noch zusätzlich aktiviert werden:

- Rollen/Webserver (IIS)/Webserver/Anwendungsentwicklung/Anwendungsinitialisierung
- Rollen/Webserver (IIS)/Webserver/Leistung/Komprimierung statischer Inhalte

Diese Features können über *Systemsteuerung/Programme und Funktionen/Windows-Funktionen aktivieren oder deaktivieren* installiert werden.

3.4.2 *.NET Core Hosting-Paket*

ibi systems iris benötigt für den Betrieb ein installiertes .NET Core Hosting-Paket in der Version 8.0.x. Einen Link zum Download des aktuellen Installationspakets finden Sie auf folgender Seite:

<https://learn.microsoft.com/de-de/aspnet/core/host-and-deploy/iis/hosting-bundle?view=aspnetcore-8.0>

Möglicherweise ist nach der Installation ein Neustart des Servers notwendig.

Bitte beachten Sie außerdem, dass das Hosting-Paket unbedingt erst nach dem IIS (bzw. nach dem Ausführen des in Abschnitt 4.1.1 beschriebenen PowerShell-Skripts) installiert werden muss.

4 Einrichtung und Konfiguration von Anwendungspool, Website, REST-API

Die Einrichtung und Konfiguration von Application Pool, Website und REST-API in IIS kann entweder automatisiert über zwei PowerShell-Skripte oder manuell durchgeführt werden.

4.1 Automatisierte Einrichtung

4.1.1 PowerShell-Skript

Die Einrichtung von Application Pool, Website und REST-API mit den benötigten (Standard-)Einstellungen (inkl. Installation/Aktivierung der benötigten Windows-Features) kann mit Hilfe zweier PowerShell-Skripte größtenteils automatisiert werden. Sie können die Skripte hier downloaden: https://downloads.ibi-systems.de/install_iris.zip.

Die beiden PowerShell-Skripte müssen **zwingend** ausgeführt werden, um Lese- und Schreibberechtigungen für die Anwendungsordner korrekt einzustellen.

Bitte überprüfen Sie vor dem Ausführen die gesetzten Parameter und passen Sie diese bei Bedarf an:

Webseite (install_iris_website.ps1):

Beschreibung der Werte innerhalb des Skripts	
iisAppPoolName	Name des Application Pools
iisAppPoolRestartAt	definiert wann die Anwendung täglich neu gestartet wird, um den Cache zu leeren um die Anwendung performant zu halten
iisAppName	Definiert den IIS-Sitenamen
iisAppDir	Definiert das „Anwendungsverzeichnis“, in dem die Binaries der Anwendung abgelegt werden
iisAppSslPort	Port auf dem die Anwendung veröffentlicht wird (üblicherweise 443)
AppFileDir	Beschreibt den Pfad für das Hauptverzeichnis, in dem alle Arbeitsverzeichnisse durch die Anwendung angelegt werden Hinweis: dieser Ort sollte zur Sicherheit der Arbeitsdaten (Nutzdaten wie z.B. Uploads) nicht im iisAppDir abgelegt sein. Üblicherweise wird hier eine „Daten-Partition“ verwendet, diese von der Betriebssystem-Installation zu trennen.

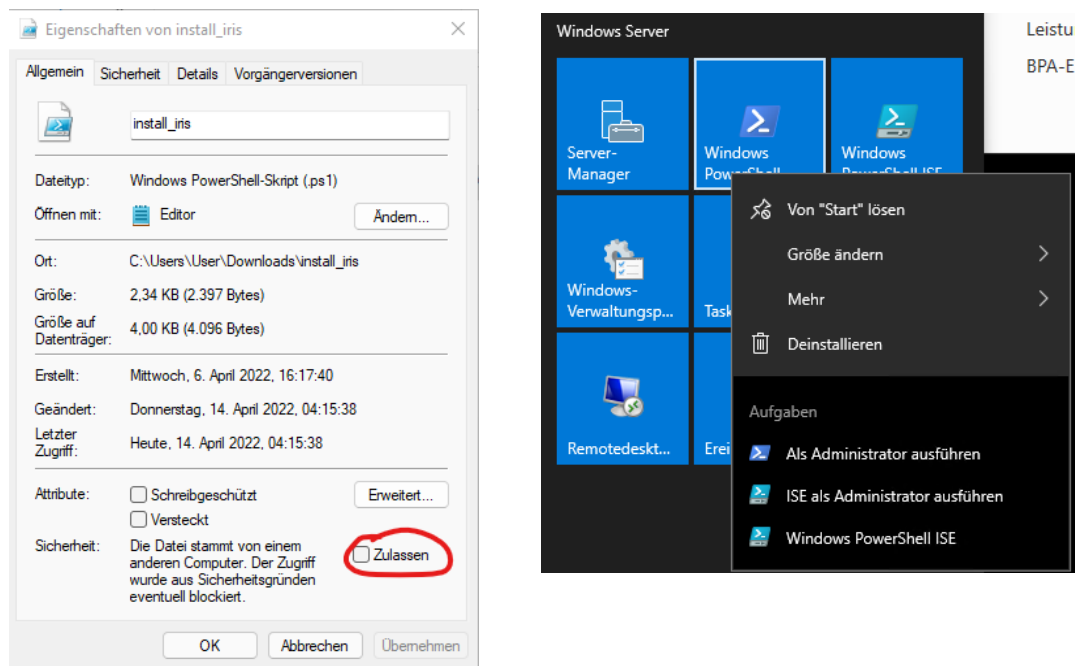
```
# * Configure parameters before executing
$iisAppPoolName = "iris"
$iisAppPoolRestartAt = @"05:00"
$iisAppName = "iris"
$iisAppDir = "C:\inetpub\wwwroot\iris"
$iisAppSslPort = 443
$appFileDir = "C:\inetpub\grc-suite-files\"
```

REST-API (install_iris_restapi.ps1):

```
# * Configure parameters before executing
$iisAppPoolName = "iris-restapi"
$iisAppPoolRestartAt = @"05:30"
$iisAppName = "iris-restapi"
$iisAppDir = "C:\inetpub\wwwroot\iris-restapi"
$iisAppSslPort = 8443
```

Für die REST-API wird standardmäßig der Port 8443 belegt. Dieser kann im PowerShell-Skript beliebig gesetzt werden. Der Port 433 sollte nicht benutzt werden, da dieser für die Webseite reserviert ist.

Für die Ausführung des Skripts müssen evtl. noch die Sicherheitseinstellungen in den Eigenschaften der Datei angepasst und die PowerShell-Konsole als Administrator ausgeführt werden:



Hinweis:

Sollten Sie den IIS erst über die Ausführung des PowerShell-Skripts auf dem Server aktiviert haben, so

```
PS C:\ibi> .\install_iris.ps1
```

müssen Sie vor dem Start von Application Pool und Website unbedingt noch das .NET Core Hosting-Paket installieren. Dieser Schritt wird in Abschnitt 3.4.2 der Anleitung beschrieben.

4.1.2 IIS-Site-Konfiguration

4.1.2.1 TLS-Konfiguration

Die Skripte erzeugen für die Website wie auch für die Rest-API **jeweils** eine Bindung mit aktiviertem SSL/TLS für die neu angelegten Sites.

Da die Konfiguration der Transportverschlüsselung von der Installation des Kunden abhängt muss das Zertifikat durch den Betreiber installiert werden und innerhalb der Bindungen (siehe Bilder) konfiguriert werden.

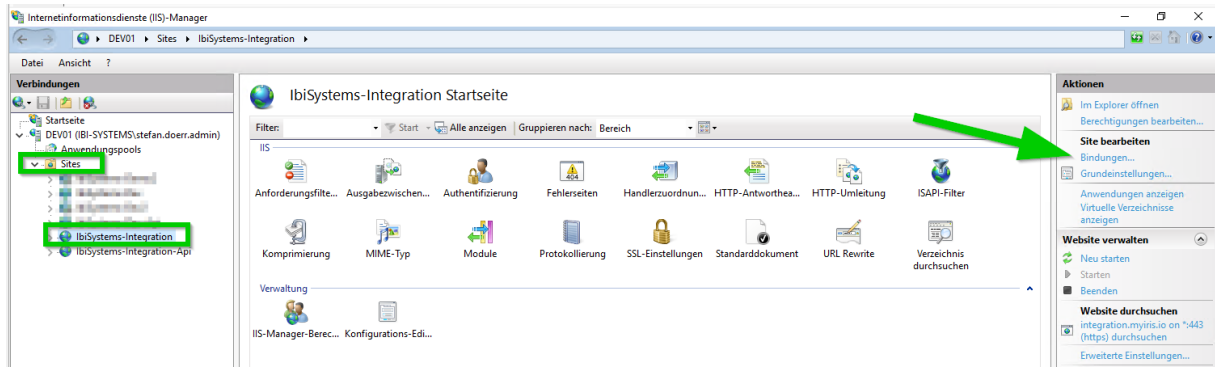


Abbildung 4 - IIS Bindungen bearbeiten 1

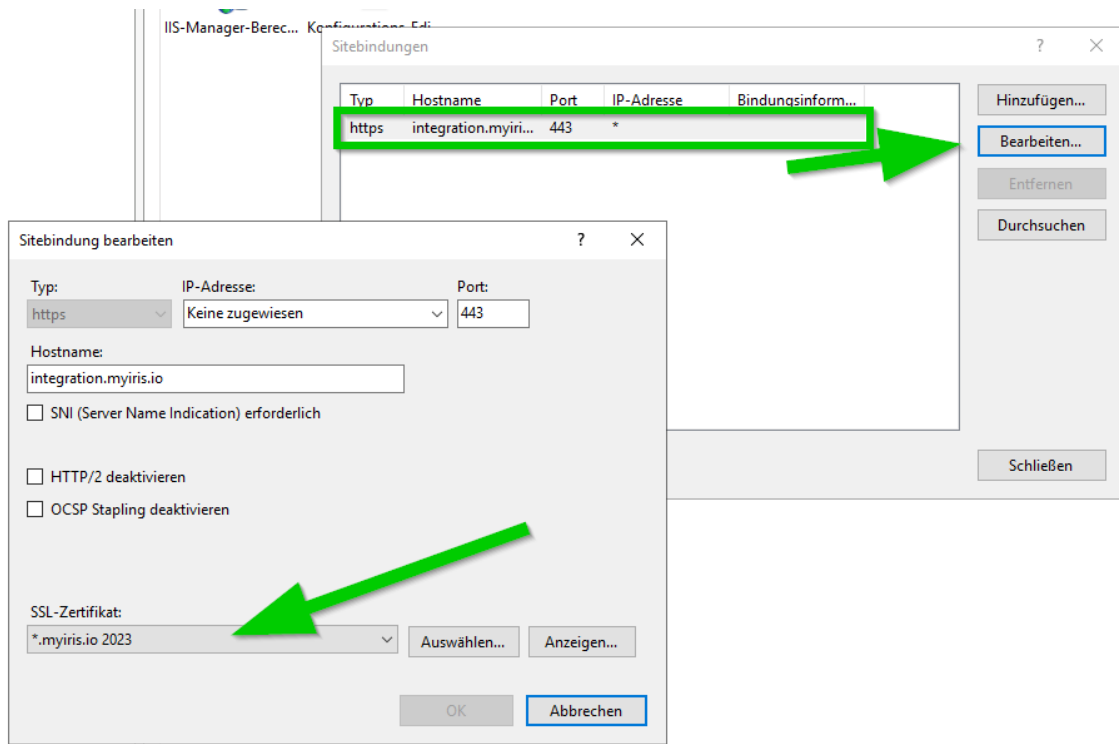


Abbildung 5 - IIS Bindung bearbeiten 2

4.1.3 Benutzer Authentifikation via SAML

Soll SAML z.B. Okta verwendet werden um Nutzer am System zu Authentifizieren müssen die Konfigurationsschritte in Kapitel 4.2.1.6 manuell durchgeführt werden.

4.1.4 SQL Server Authentifikation über "Integrated Security"

Wird ein Active Directory Benutzer verwendet um die Verbindung zwischen der Anwendung und dem SQL Server herzustellen müssen die Konfigurationsschritte in Kapitel 4.2.1.4 manuell durchgeführt werden.

4.2 Manuelle Einrichtung

4.2.1 IIS-Anwendungspool Konfigurieren (Website)

Es wird empfohlen, im Manager der Internetinformationsdienste (IIS) für die neue Website einen eigenen Anwendungspool zu verwenden. Dieser ist mit der ".NET-Framework"-Version (.NET CLR-Version) *Kein verwalteter Code* und als *verwalteter Pipelinemodus integriert* einzustellen:

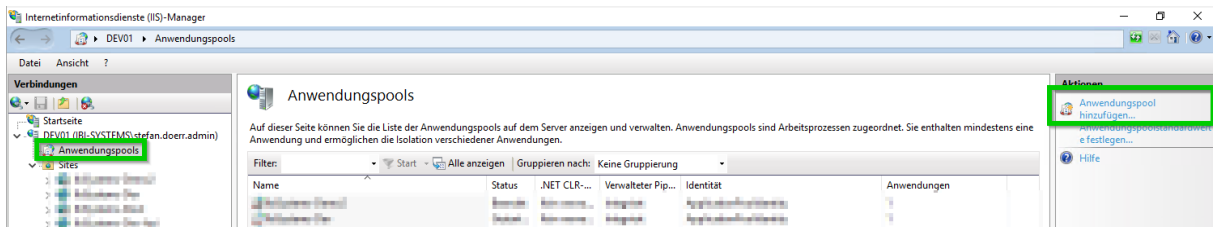


Abbildung 6 – Anwendungspool hinzufügen

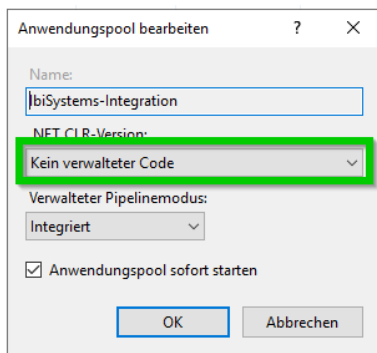


Abbildung 7 – Anwendungspool Konfiguration

Anwendungspool – Erweiterte Einstellungen – Webseite

Standardmäßig wechseln IIS-Anwendungspools nach 20 Minuten Inaktivität in den Standby-Modus. Dies würde unter Umständen die Ausführung von iris Hintergrundaufgaben (Jobs) wie z. B. den Versand von Erinnerungsmails verhindern. Daher muss dieses Verhalten deaktiviert werden.

Durch **Rechtsklick** auf den neu eingerichteten **Anwendungspool** im Internetinformationsdienste (IIS)-Manager können die *erweiterten Einstellungen* geöffnet werden:

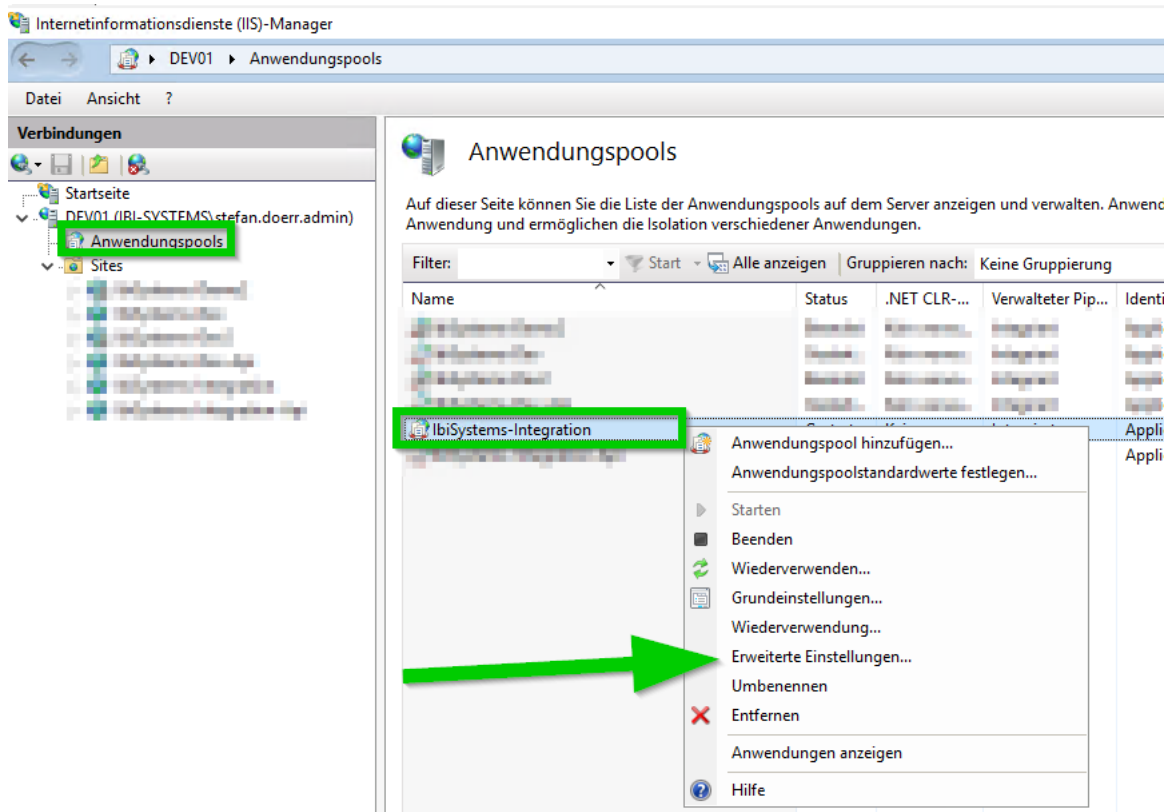


Abbildung 8 - Anwendungspools - erweiterte Einstellungen

4.2.1.1 Startmodus

Allgemein - Startmodus [startMode]: AlwaysRunning

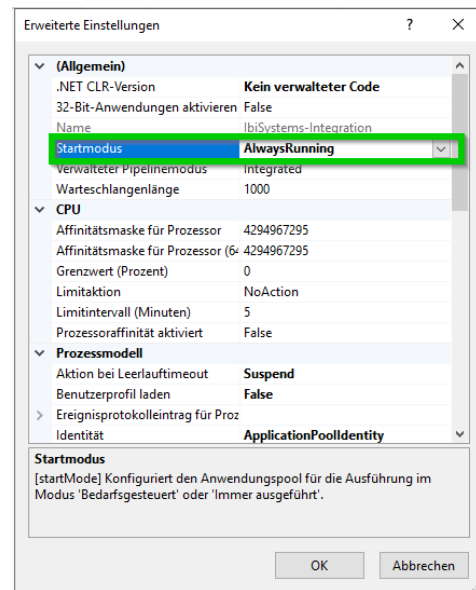


Abbildung 9 - Allgemein - Startmodus

4.2.1.2 Aktion bei Leerlauf timeout

Prozessmodell - Aktion bei Leerlauf timeout [idleTimeoutAction]: Suspend

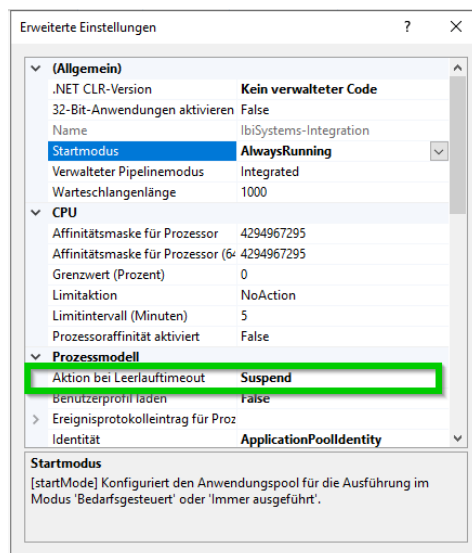


Abbildung 10 - Prozessmodell - Aktion bei Leerlauf timeout [idleTimeoutAction]:

4.2.1.3 Leerlauf timeout (Minuten)

Prozessmodell - Leerlauf timeout (Minuten) [IdleTimeout]: 0

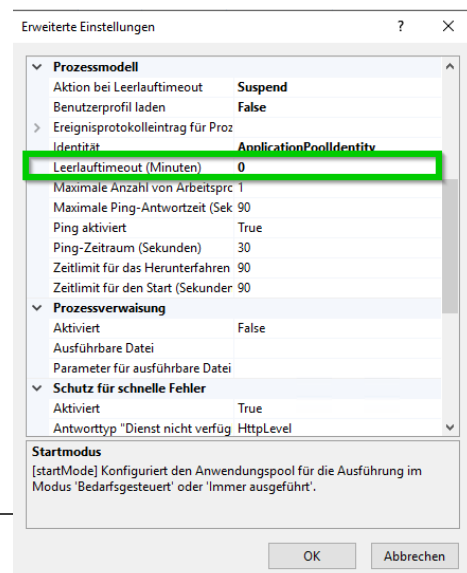


Abbildung 11 - Prozessmodell - Leerlauf timeout

4.2.1.4 ApplicationPoolIdentity (nur erforderlich, falls die Datenbank-Verbindung über einen ActiveDirectory Benutzer stattfinden soll)

- *Identität* [Identity]:
 - **ApplicationPoolIdentity** (bei Nutzung eines SQL-Server-Nutzers für die Datenbankverbindung)

Hinweis:

- Zugangsdaten des Windows/AD-Nutzers (bei Nutzung eines Windows/AD-Nutzers für die Datenbankverbindung); Benutzer muss zusätzlich in die Benutzergruppe *IIS_IUSRS* aufgenommen werden
- Der genutzte Benutzer darf nicht der Windows-Standard-Nutzer sein, der zum Einrichten der Anwendung genutzt wird. Es muss für die Anwendung zwingend ein eigener Nutzer angelegt bzw. im AD angelegt werden.

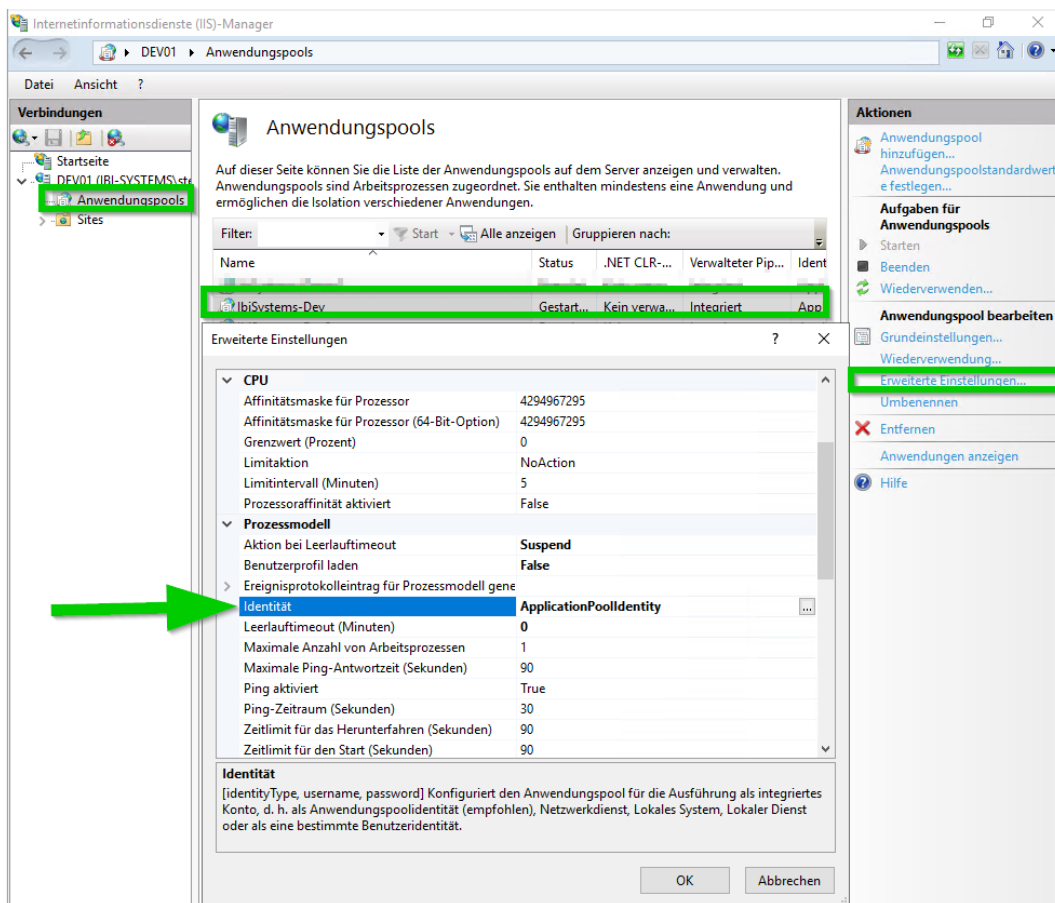


Abbildung 12 - Application Pool Identity Setup

4.2.1.5 Application Pool - Wiederverwendung

Darüber hinaus müssen zudem im Bereich *Wiederverwendung* / *Bestimmte Zeiten* [schedule] eine Zeit außerhalb der Hauptgeschäftszeiten (z. B. 5:20 Uhr nachts) eingetragen werden, an der der Anwendungspool automatisch neu gestartet wird:

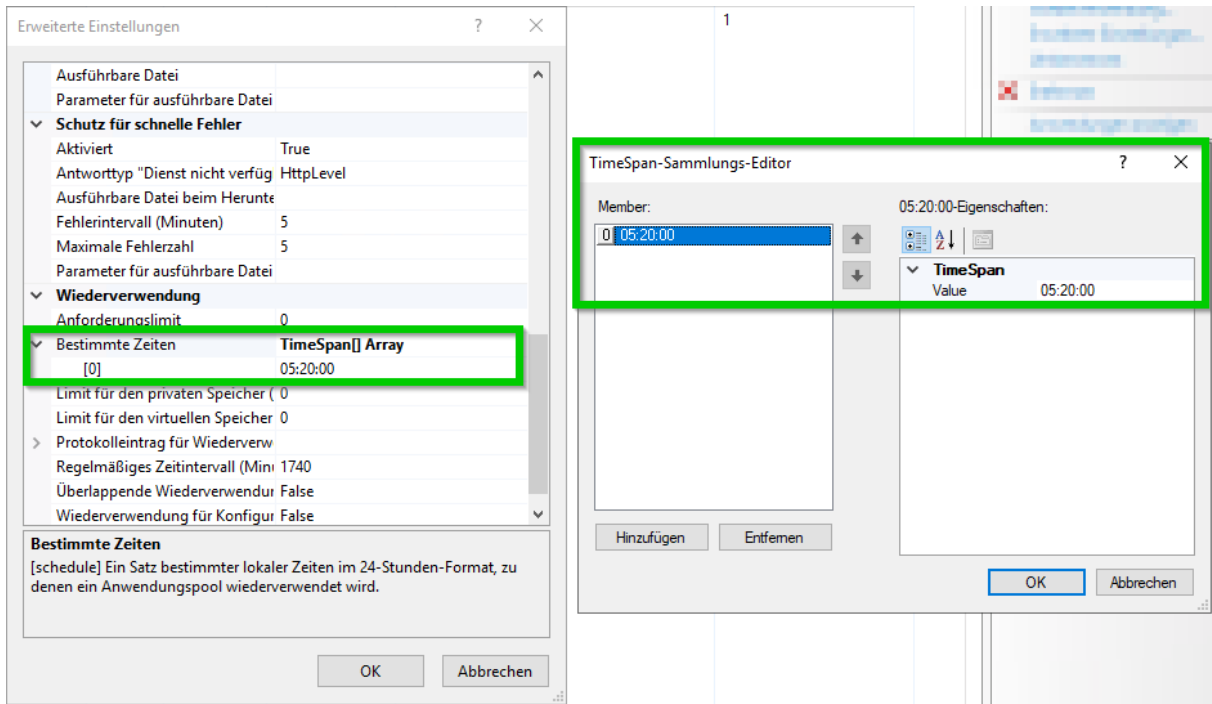


Abbildung 13 - Wiederverwendung - Bestimmte Zeiten [schedule]

Hinweis:

Die Applikation benötigt nach dem Neustart eine Warm Up Phase, die durch den ersten Zugriff nach dem Neustart ausgelöst wird. Um ungewöhnlich lange Reaktionszeiten der Anwendung, beim ersten Zugriff von Nutzern, nach dem Neustart, zu verhindern empfiehlt sich die Aktivierung der **Warm Up Routine**, die in Kapitel 7.6 beschrieben ist. Diese kann nach Abschluss der Installation aktiviert werden.

4.2.1.6 Benutzerprofile Laden (nur erforderlich, falls die SAML-Authentifikation verwendet wird)

Prozessmodell – Benutzerprofile laden [Load User Profiles]: True

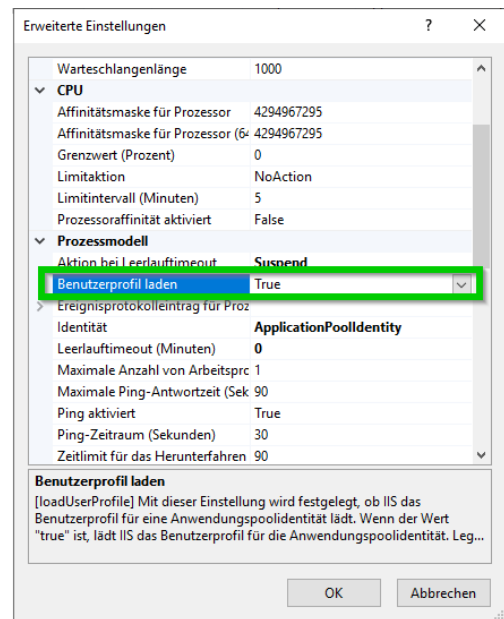


Abbildung 14 - Prozessmodell - Benutzerprofile laden

4.2.2 Site – Erweiterte Einstellungen - Website

Für ibi systems iris wir eine neue Website hinzuzufügen. In den Bindungseinstellungen sollte lediglich der Zugriff über Port 443 mit entsprechendem SSL-Zertifikat und Hostnamen, der gemäß Kapitel 3.2 dem Anwendungsserver als DNS-Name zugewiesen wurde, konfiguriert werden.

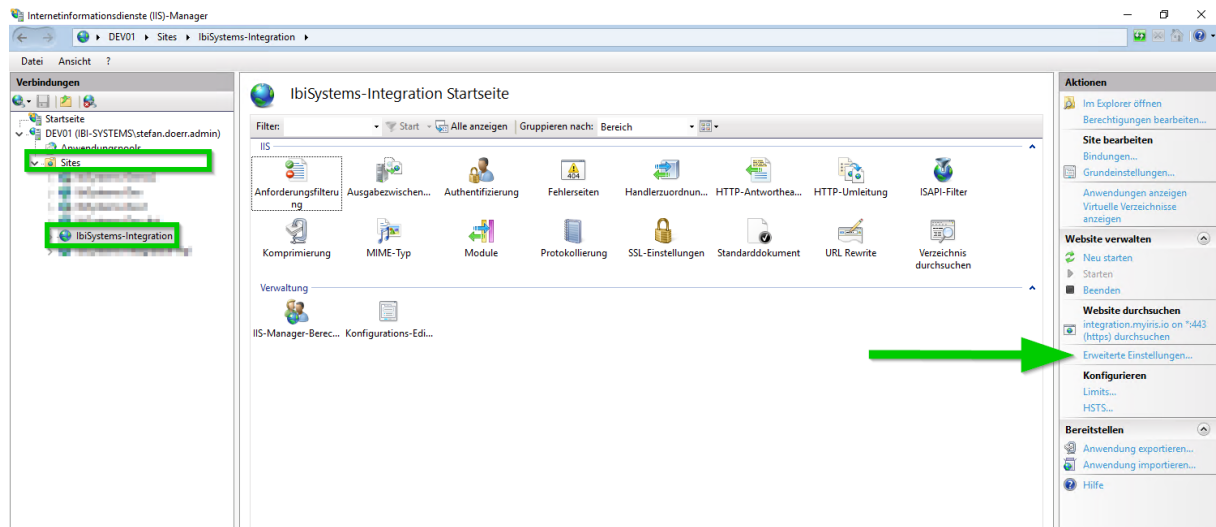


Abbildung 15 - Site Erweiterte Einstellungen

4.2.2.1 Allgemein - Vorabladen

In den *erweiterten Einstellungen* der angelegten Website sollte *Vorabladen* aktiviert werden.

Allgemein Vorabladen aktiviert [preloadEnabled] auf **True** gesetzt werden.

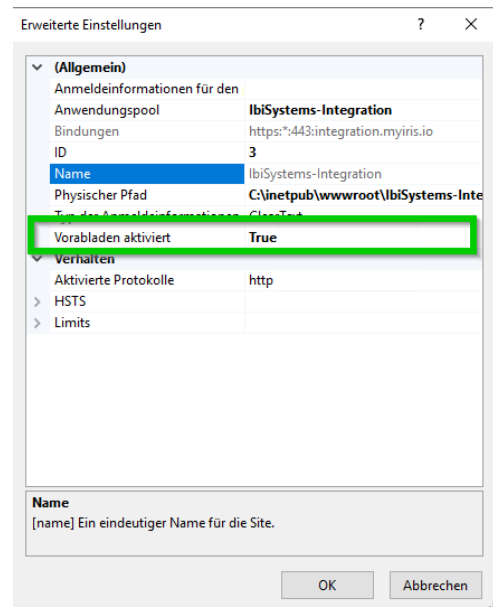


Abbildung 16 - Site - Allgemein - Vorabladen

4.2.3 REST-API

Die REST-API ist analog zu der Webseite einzurichten. Hierfür kann entweder das PowerShell-Skript (siehe 4.1.1) oder die Anleitung zur manuelle Einrichtung (siehe 4.2) verwendet werden.

Hinweis: Die REST-API Installation ist **optional**.

Ob die Anwendung über die benötigten API-Nutzer verfügt, ist von Ihrer Lizenzierung abhängig, diese Nutzerkonten können über die Benutzeroberfläche der Anwendung eingesehen werden.

5 Installation und Konfiguration der Anwendung

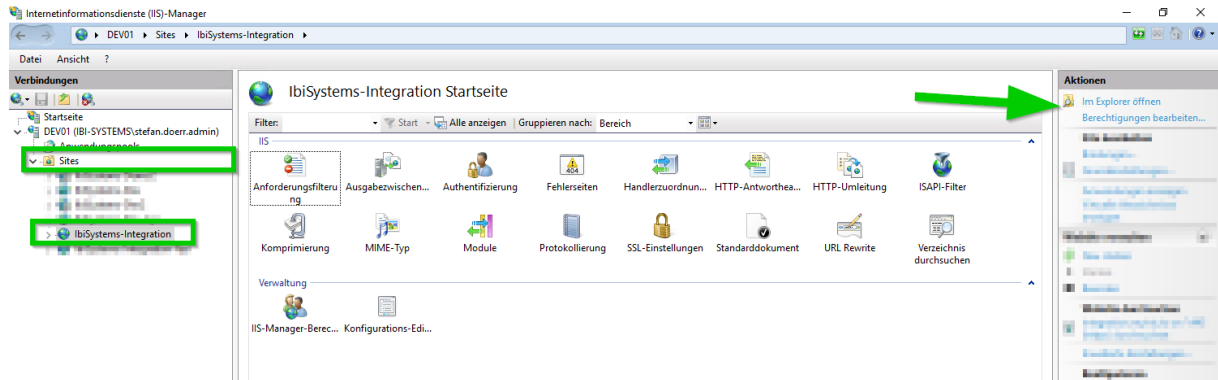
5.1 Installation der Anwendung

Alle Dateien im Ordner *Application* des Installations-Pakets müssen in den *Physischen Pfad* der Website kopiert werden.

5.1.1 Kopieren der Anwendungs-Binaries in das Anwendungsverzeichnis

Alle Dateien im Ordner *Application* des Installations-Pakets müssen in den *Physischen Pfad* der Website kopiert werden.

5.1.1.1 Öffnen des Anwendungsverzeichnisses



5.1.1.2 Prüfen und der Berechtigungen auf dem Anwendungsverzeichnis (IIS_IUSRS)

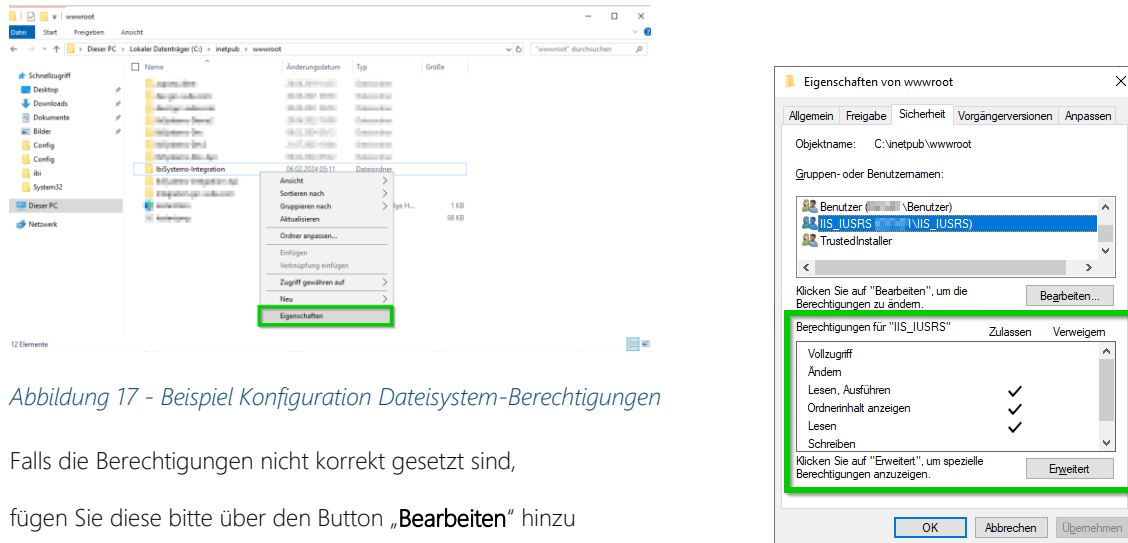


Abbildung 17 - Beispiel Konfiguration Dateisystem-Berechtigungen

Falls die Berechtigungen nicht korrekt gesetzt sind, fügen Sie diese bitte über den Button „**Bearbeiten**“ hinzu

5.2 Konfiguration der Anwendung

Im Unterordner **Config** des Website-Ordners befinden sich die Konfigurationsdateien. Die Anwendung wird bereits vor-konfiguriert ausgeliefert, allerdings sind noch manuelle Anpassungen im Rahmen der Installation erforderlich. Diese werden im Folgenden beschrieben.

Hinweis: Bitte beachten Sie, dass die im folgenden Abschnitt konfigurierten Verzeichnisse zur Ablage von Dateien unbedingt außerhalb des physischen Pfades der Website liegen sollten.

Hinweis: Auf allen Ordnern, die in den folgenden Kapiteln innerhalb der Konfigurationsdateien eingerichtet werden, werden Schreibberechtigungen benötigt.

5.2.1 Berechtigungen auf den „Arbeitsverzeichnissen“

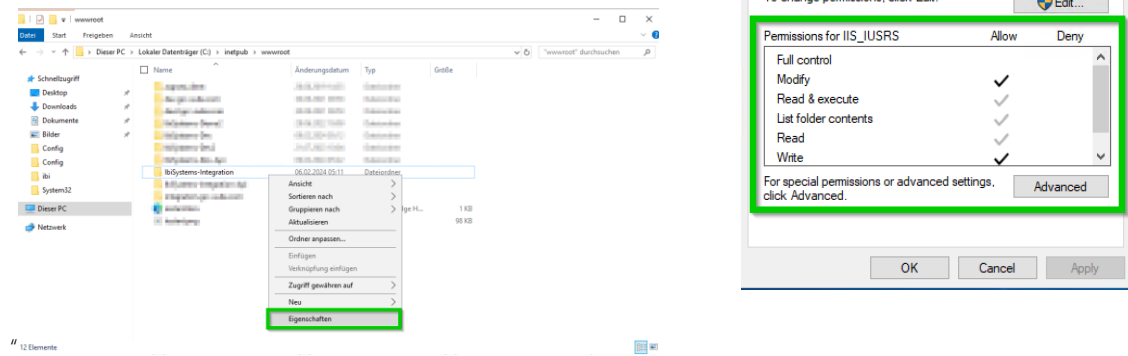


Abbildung 18 - Beispiel Konfiguration Dateisystem-Berechtigungen

Falls die Berechtigungen nicht korrekt gesetzt sind, fügen Sie diese bitte über den Button „**Bearbeiten**“ hinzu

5.2.2 Übersicht der Konfigurations-Dateien und Ordner der Anwendung

Konfigurationsdatei	Beschreibung
ConnectionStrings.config	Enthält alle Konfigurationswerte, die die Anwendung benötigt, um eine Verbindung zur Datenbank herzustellen
MailSettings.config	Enthält alle Konfigurationswerte, die die Anwendung benötigt, um Mails zu versenden
LoggingConfiguration.config	Enthält alle Konfigurationswerte, die die Protokollierung der Anwendung festlegt
InfrastructureSettings.config	Enthält alle Konfigurationswerte, die für die Nutzdaten (z.B. Uploads)
QueueConfiguration.config	Enthält alle Konfigurationswerte, die für die Warteschlangen Konfiguration erforderlich sind
LdapSettings.config	enthält alle Konfigurationswerte zur (optionalen) LDAP-Anbindung, in der Benutzerinformationen aus einem LDAP-Server ermittelt werden

5.2.3 ConnectionStrings.config

Die Verbindungszeichenfolge zur Datenbank wird im Attribut `connectionString` des jeweiligen Connection Strings angegeben. Unter [http://msdn.microsoft.com/de-de/library/bf7sd233\(v=vs.85\).aspx](http://msdn.microsoft.com/de-de/library/bf7sd233(v=vs.85).aspx) stehen dazu weitere Informationen zur Verfügung. Die Website <http://www.connectionstrings.com> bietet eine Zusammenstellung von Connection Strings jeglicher Datenbanksysteme.

Der Connection String mit dem Namen **GrcSuiteDb** ist verpflichtend anzugeben und wird für die Kommunikation mit der Datenbank genutzt. Als Benutzer ist der in Kapitel 3.3 erstellte **Anwendungsbenutzer** zu verwenden.

Optional kann zusätzlich ein zweiter Connection String mit dem Namen **GrcSuiteDb_Admin** eingetragen werden. Dieser wird ausschließlich für das Einspielen von Datenbank Updates über die Software-Oberfläche verwendet. Soll dieses Feature nicht genutzt werden, so kann der Eintrag auskommentiert oder ganz entfernt werden. Als Benutzer ist der in Kapitel 3.3 erstellte **Administrationsbenutzer** zu verwenden.

Bitte beachten Sie, dass bei der Nutzung von Windows/AD-Benutzern statt SQL-Server-Benutzern zur Datenbank-Verbindung die Benutzer nicht in den Connection String aufgenommen werden müssen, sondern stattdessen der Application Pool der Anwendung im Kontext des entsprechenden Nutzers (Einstellung *Identität*) ausgeführt werden muss. (siehe 4.1.4)

Dieser Benutzer muss zur Benutzergruppe *IIS_IUSRS* hinzugefügt werden. Statt den Benutzerdaten (Optionen *User Id* und *Password*) muss folgende Option in den Connection String aufgenommen werden. (siehe 7.6)

Beispiel ConnectionStrings:

Authentifikation mit einem SQL Server Benutzer

```
data source=%SQLSERVERFQDN%,%PORTNUMBER%;User
Id=%DatabaseUser%;Password=%DatabaseUserPassword%;initial
catalog=%DatabaseName%;MultipleActiveResultSets=True;
```

Authentifikation mit einem Active Directory Benutzer

```
data source=%SQLSERVERFQDN%,%PORTNUMBER%;Integrated Security=SSPI;initial
catalog=%DatabaseName%;MultipleActiveResultSets=True;
```

Hinweis: bei dieser Authentifizierung Methode prüfen Sie die Konfigurationseinstellung in Kapitel 4.1.4 und 7.6.

5.2.4 MailSettings.config

Im Knoten `smtp` wird der SMTP-Server zum Versand von E-Mails aus der Anwendung konfiguriert.

Beispiel für den Mailversand über den einen SMTP-Server mit Benutzername und Kennwort

```
<smtp deliveryMethod="Network" from="noreply@grc-suite.com">
  <network host="smtp.company.tld" port="25" enableSsl="false"
    defaultCredentials="false" userName="smtpuser"
    password="smtppassword" />
</smtp>
```

Hinweis:

Wird die Option „defaultCredentials“ auf true gesetzt wird der Account des Application Pools (siehe 4.1.4) verwendet, um sich am Mailserver anzumelden. Die Einträge `userName` und `password` entfallen dann komplett.

Weiterführende Informationen zu den Konfigurationsmöglichkeiten sind unter [http://msdn.microsoft.com/en-us/library/w355a94k\(v=vs.110\).aspx](http://msdn.microsoft.com/en-us/library/w355a94k(v=vs.110).aspx) zu finden.

Die MailSettings.config-Datei der Anwendung muss für die Nutzung der Mailserver Anbindung entsprechend angepasst werden. Damit wir Ihnen die richtig konfigurierte Datei zukommen lassen können, benötigen wir u.a. folgende Angaben von Ihnen:

- Mail Server Hostname
- Mail Server Portnummer
- Mail Server Benutzer und Passwort (sofern erforderlich)
- SSL-Verschlüsselung nutzen
- Absende-Adresse

Um diese Angaben im Vorab testen zu können, erhalten Sie von uns ein Kommandozeilen-Tool, das direkt auf dem Applikationsserver ausgeführt werden muss. Mit Hilfe der vom Werkzeug erstellten TXT-Datei können alle notwendigen Einstellungen vorgenommen werden. Die richtige Nutzung des Tools wird im Kapitel 7.1 *Einrichtung der E-Mail-Konfiguration* - Nutzung des Kommandozeilen-Tools beschrieben.

Hinweis: In der vom Tool erstellten TXT-Datei ist das (optional) genutzte Passwort im Klartext enthalten. Sollten Sie das Passwort auf einem anderen Weg an uns übertragen oder die Information bei jedem Update selbst in die Datei eintragen wollen, entfernen Sie die entsprechende Stelle bitte aus der Datei.

5.2.5 *InfrastructureSettings.config*

Über das Element `infrastructureSettings` werden anwendungsinterne Einstellungen vorgenommen. Die Eigenschaft `gotoIdUrl` legt die Url der Goto-Action fest. Dabei muss die Url im Format `https://[DNS-Name]/General/Search/Goto/{0}` angegeben werden.

Darüber hinaus kann mit der Eigenschaft `isDocumentEncryptionEnabled` die verschlüsselte Speicherung von Dokumenten aktiviert werden.

Mit dem Attribut `isOwnApplicationUserEditable` wird festgelegt, ob es erlaubt ist, den eigenen Benutzer in der Benutzerverwaltung zu bearbeiten.

Zudem werden in den `InfrastructureSettings` diejenigen Ordner festgelegt, in denen von der Anwendung erzeugte Benutzerdateien gespeichert werden. Die angegebenen Ordner müssen auf dem Anwendungsserver existieren. Folgende Tabelle beschreibt die zu definierenden Eigenschaften und die benötigten Zugriffsrechte für die IIS-Benutzergruppe IIS_IUSRS, die bei der Installation manuell gesetzt werden müssen:

Eigenschaft	Beschreibung	Lesezugriff	Schreib-/Änderungszugriff
<code>baseImagePath</code>	Legt den Basispfad für die hochgeladenen Bilder fest. Die Bilder werden durch die Anwendung in weiteren Unterordnern strukturiert.	x	x
<code>baseDocumentsPath</code>	Legt den Basispfad für die hochgeladenen Dokumente fest. Die Dokumente werden durch die Anwendung in weiteren Unterordnern strukturiert.	x	x
<code>baseReportsPath</code>	Legt den Basispfad für die gespeicherten Report-Layouts fest. Die Layouts werden durch die Anwendung in weiteren Unterordnern strukturiert.	x	x
<code>baseDashboardsPath</code>	Legt den Basispfad für die gespeicherten Dashboard-Layouts fest. Die Layouts werden durch die Anwendung in weiteren Unterordnern strukturiert.	x	x
<code>baseCachePath</code>	Legt den Basispfad für Dateien fest in denen Daten für die schnellere Verarbeitung zwischengespeichert werden	x	x

Hinweis: wird die Installation durch das PowerShell Skript durchgeführt müssen die Dateisystem Berechtigungen nicht mehr manuell gesetzt werden

5.2.6 *LoggingConfiguration.config*

Der Abschnitt `loggingConfiguration` kann folgende zwei Elemente enthalten, die das Logging-Verhalten der Anwendung konfigurieren:

Elementname	Beschreibung
<code>LogFileListener</code>	Legt fest, wie das Logging von Anwendungsmeldungen und -fehlern erfolgen soll. Insbesondere sind hier die Attribute <code>fileName</code> und <code>archiveFileName</code> relevant, die die Dateien bestimmen, in der die Logging-Informationen gespeichert werden.
<code>EmailListener</code>	Legt fest, an welche E-Mail-Adresse und über welchen SMTP-Server kritische Anwendungsfehler per E-Mail zu versenden sind.

Hinweis: Auf die angegebenen Pfade benötigt die IIS-Benutzergruppe **IIS_IUSRS Lese- und Schreib-/Änderungsrechte**.

Hinweis: wird die Installation durch das PowerShell Skript durchgeführt müssen die Dateisystem Berechtigungen nicht mehr manuell gesetzt werden

5.2.7 *QueueConfiguration.config*

Im Knoten `queueConfiguration` wird im Attribut `queueSourcePath` festgelegt. In diesem Verzeichnis werden Dateien für eine spätere Abarbeitung durch die Anwendung abgelegt werden.

Hinweis: Auf den angegebenen Pfad benötigt die IIS-Benutzergruppe **IIS_IUSRS Lese- und Schreib-/Änderungsrechte**.

Hinweis: wird die Installation durch das PowerShell Skript durchgeführt müssen die Dateisystem Berechtigungen nicht mehr manuell gesetzt werden

5.2.8 *LdapSettings.config*

Mit Hilfe der LDAP-Anbindung können an mehreren Stellen in der Applikation (z.B. beim Anlegen von neuen Benutzern) Eingabefelder in ibi systems iris aus dem Ergebnis einer LDAP-Abfrage vorbefüllt werden.

Möchten sie eine LDAP-Anbindung konfigurieren sind in Kapitel 7.2 alle notwendigen Schritte beschrieben.

5.3 Konfiguration der REST-API

Nach der Konfiguration der Webseite gehen sie in den Webseiten-Ordner und kopieren sie die angepassten Dateien in die bestehenden „Config“-Ordner des REST-API-Ordners.

5.4 Konfiguration der SSO-Authentifizierungsmöglichkeiten

Es besteht die Möglichkeit, ein Single-Sign-On (SSO) für ibi systems iris mittels Windows Authentifizierung oder mittels OKTA (SAML 2.0) einzurichten.

Sofern Sie eine SSO-Anbindung konfigurieren wollen, sind in Kapitel 7.3 *Einrichtung SSO - Windows Authentifizierung* sowie Kapitel 7.4 *Einrichtung SSO - Authentifizierung via OKTA (SAML 2.0)* alle jeweils notwendigen Schritte beschrieben.

6 Erster Programmstart

6.1 Anlage der Datenbank-Strukturen

Sind alle Einstellungen vorgenommen, kann die Applikation (Anwendungspool und Site siehe Kapitel Übliche Betriebsaufgaben) gestartet werden.

Navigiert man nach dem Start im Browser zur Anwendung, so wird eine Hinweis-Seite angezeigt, dass gerade ein Update der Software ausgeführt wird.

Bitte Folgen Sie dann den Anweisungen in Kapitel Update der Datenbank.

Bitte beachten Sie, dass der erste Start der Anwendung nach dem Datenbank-Update u.a. wegen der Importe der aktuellen Reports und Dashboards durchaus **einige Minuten dauern kann**.

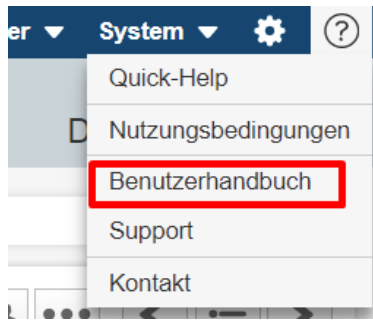
6.2 Eingabe der initialen Daten

Nach einem Neustart der Anwendung werden Sie aufgefordert, die initialen Daten des ersten Nutzers einzugeben:

Hinweis: Soll SAML zur Authentifikation verwendet werden, muss der Benutzername mit dem Benutzername des SAML-anbieters übereinstimmen. (z.B. E-Mail-Adresse oder Okta-Benutzername)

Sind alle Daten gespeichert, können Sie sich mit dem eben angelegten User einloggen. Der neu angelegte Benutzer erhält über die initiale Benutzerrolle nur sehr eingeschränkte Berechtigungen (in der Benutzerverwaltung).

Diese Berechtigungen können nach dem Login über die erweitert bzw. für weitere Benutzer frei vergeben. Details zur Bedienung der Software sowie zum Rechte- und Rollenkonzept finden Sie im Benutzerhandbuch:



Hinweis: Sollte statt dem Formular zur Erstkonfiguration nach dem ersten Start fälschlicherweise die Login-Seite angezeigt werden, so hilft ein erneutes Laden der Seite im Browser.

6.3 Testen der Anwendungskonfiguration

Nach der erfolgreichen Installation der Anwendung und dem Login ist es möglich, die Konfiguration der Anwendung zu überprüfen.

Unter folgender URL stehen verschiedene Testmethoden, beispielsweise für den E-Mail-Versand, das Logging und die Ablage von Dateien auf dem Server bereit: <https://server.your-domain.de/General/Test>

Test-Routinen
Exception Dieser Test löst einen Anwendungsfehler aus, um zu prüfen, ob die nachgelagerten Mechanismen (wie z. B. automatisches Logging) funktionieren. Test ausführen
Iris Exception Dieser Test löst einen Iris Anwendungsfehler aus, um zu prüfen, ob die nachgelagerten Mechanismen (wie z. B. automatisches Logging) funktionieren. Test ausführen
Logging Debug: Test ausführen Info: Test ausführen Warn: Test ausführen Error: Test ausführen
Mailing Mit dieser Test-Routine lassen sich die E-Mail-Einstellungen überprüfen. Dazu wird eine E-Mail an die hinterlegte Adresse des aktuell eingeloggten Benutzers gesendet. Test ausführen
Mailing (extern) Mit dieser Test-Routine lassen sich die E-Mail-Einstellungen überprüfen. Dazu wird eine E-Mail an eine externe E-Mail-Adresse (incident@ibi-systems.de) gesendet. Diese E-Mail enthält keinerlei sensiblen Daten. Test ausführen
Dokumenten-Upload Diese Funktion erstellt ein Test-Dokument im hinterlegten Dokumentenpfad, um die Ordnerberechtigungen zu testen. Test ausführen
Image-Upload Diese Funktion erzeugt eine Bilddatei im hinterlegten Bilderpfad, um die Ordnerberechtigungen zu überprüfen. Test ausführen
Zeitbezogene Benachrichtigungsregeln Mit dieser Test-Routine lassen sich alle aktiven zeitbezogenen Benachrichtigungsregeln testen. Es werden immer alle Benachrichtigungsregeln für den aktuellen Tag ausgeführt. Zudem werden die Benachrichtigungsregeln für den aktuellen Tag ausgeführt. Test ausführen

Hierbei sollte, im Anschluss an die Installation, vor allem die Einstellungen der Mailing-Funktionen getestet werden. Im Zusammenspiel mit verschiedenen Mail-Servern kann es, durch eine falsche Konfiguration, zu Fehlern kommen, die das erfolgreiche Versenden von Emails an Benutzer verhindern können.

6.4 Start der REST-API

Um die REST-API zu starten, initialisieren sie die Webseite mit ihrer Datenbank-Struktur (siehe Anlage der Datenbank-Strukturen) und geben dann folgenden Link in die Url-Zeile ihres Browsers ein: <https://server.your-api-domain.de/docs/index.html>

7 Anhang – Zusätzliche Konfigurationsmöglichkeiten

7.1 Einrichtung der E-Mail-Konfiguration - Nutzung des Kommandozeilen-Tools

7.1.1 Vorbereitungen

Sie erhalten das Tool als ZIP-Datei. Bitte entpacken Sie die Datei auf dem Applikationsserver, öffnen Sie ein cmd-Fenster und wechseln zum Verzeichnis mit den entpackten Dateien. Dort müssen Sie nun das Modul „mail“ des Tools „IbiSystems.GrcSuite.Cmd.Extern.exe“ mit den entsprechenden Parametern aufrufen.

7.1.2 Parameter

Eine Übersicht der Parameter mit den Standardwerten (falls vorhanden) finden Sie hier:

Parameter	Beschreibung	Pflichtangabe	Standardwert
-h	Mailserver Host	Ja	-
-o	Mailserver Port	Nein	25
-c	Default-Credentials benutzen?	Nein	false
-s	SSL aktivieren?	Nein	false
-u	Benutzername	Nein	-
-p	Passwort	Nein	-
-f	Absender	Ja	-
-r	Empfänger	Ja	-

7.1.3 Ergebnis

Das Tool versucht mit den gemachten Angaben eine Test-E-Mail an den angegebenen Empfänger zu schicken. Dieser Vorgang wird in einer TXT-Datei „iris_mail_results.txt“ protokolliert. Falls die E-Mail erfolgreich verschickt wurde, können wir ibi systems iris mit Hilfe der dort enthaltenen Angaben entsprechend konfigurieren und Ihnen bei Bedarf ein neues Update-Paket zur Verfügung stellen.

7.1.4 Beispiele

Hier noch einige Beispiele für Abfragen mit dem Kommandozeilen-Tool:

Mailserver ohne Authentifizierung:

```
C:\tools\IbiSystems.GrcSuite.Cmd.Extern.exe mail -h smtp.test.de -f
iris@test.de -r max.mustermann@test.de
```

Angabe aller Parameter:

```
C:\tools\IbiSystems.GrcSuite.Cmd.Extern.exe mail -h smtp.test.de -o 587 -c true
-s true -u testuser -p password -f iris@test.de -r max.mustermann@test.de
```

7.2 Einrichten der LDAP-Anbindung

Als Voraussetzung für die Konfiguration und Nutzung der LDAP-Anbindung in ibi systems iris sollte die Anwendung bereits installiert sein, um andere Fehlerquellen ausschließen zu können.

7.2.1 Konfiguration der Anwendung

Die LdapSettings.config-Datei der Anwendung muss für die Nutzung der LDAP-Anbindung entsprechend angepasst werden. Damit wir Ihnen die richtig konfigurierte Datei zukommen lassen können, benötigen wir folgende Angaben von Ihnen:

- LDAP-Server
- LDAP-Benutzer und Passwort
- Authentifizierungstyp
- LDAP Query
- LDAP-Eigenschaften, die geladen werden sollen

Um diese Angaben vorab testen zu können, erhalten Sie von uns ein Kommandozeilen-Tool, das direkt auf dem Applikationsserver ausgeführt werden muss. Des Weiteren benötigen wir die vom Tool erstellte XML-Datei, um weitere Einstellungen vornehmen zu können.

Die richtige Nutzung des Tools wird im folgenden Kapitel beschrieben.

Hinweis: In der vom Tool erstellten XML-Datei ist das genutzte Passwort im Klartext enthalten. Sollten Sie das Passwort auf einem anderen Weg an uns übertragen oder die Information bei jedem Update selbst in die Datei eintragen wollen, entfernen Sie die entsprechende Stelle bitte aus der Datei.

7.2.2 Nutzung des Kommandozeilen-Tools

7.2.2.1 Vorbereitungen

Sie erhalten das Tool als ZIP-Datei. Bitte entpacken Sie die Datei auf dem Applikationsserver, öffnen Sie ein cmd-Fenster und wechseln zum Verzeichnis mit den entpackten Dateien. Dort müssen Sie nun das Modul „ldap“ des Tools „IbiSystems.GrcSuite.Cmd.Extern.exe“ mit den entsprechenden Parametern aufrufen.

7.2.2.2 Parameter

Eine Übersicht der Parameter mit den Standardwerten (falls vorhanden) finden Sie hier:

Parameter	Beschreibung	Pflichtangabe	Standardwert
-s	LDAP-Server (inkl. Search base)	Ja	-
-u	Benutzername	Nein	-
-p	Passwort	Nein	-
-t	Suchbegriff	Ja	-

-a	Authentifizierungstyp	Nein	None (Mögliche Werte: None, Secure, Encryption, SecureSocketsLayer, ReadonlyServer, Anonymous, FastBind, Signing, Sealing, Delegation, ServerBind)
-q	LDAP Query	Nein	(&(objectCategory=person)(objectClass=user) ((sn={0}*)(givenname={0}*)(cn={0}*))
-l	LDAP Eigenschaften, die geladen werden sollen (Komma separiert)	Nein	cn,givenname,sn,samaccountname,mail,department, telephonenumber,mobile,facsimiletelephonenumber

7.2.2.3 Ergebnis

War die Abfrage erfolgreich, so generiert das Tool aus den Ergebnissen eine XML-Datei „iris_ldap_results.xml“. Bitte überprüfen Sie, ob alle für Ihren Einsatzzweck benötigten Angaben im XML enthalten sind. Um das am besten überprüfen zu können, bietet es sich an, eine Suche nach dem eigenen Nachnamen zu starten. Folgende Datenfelder in ibi systems iris können aus dem Ergebnis der LDAP-Abfrage befüllt werden:

- Benutzername
- Vor- und Nachname
- Telefon-, Mobil- und Faxnummer
- E-Mail-Adresse
- Abteilung

Bitte lassen Sie uns diese Datei zukommen, damit wir ibi systems iris entsprechend konfigurieren und Ihnen ein neues Update-Paket zur Verfügung stellen können.

7.2.2.4 Beispiele

Hier noch einige Beispiele für Abfragen mit dem Kommandozeilen-Tool:

Nutzen der Standardwerte für Authentifizierungstyp, Query und Eigenschaften:

```
C:\tools\IbiSystems.GrcSuite.Cmd.Extern.exe ldap -u testuser -p password
-s LDAP://ldap.test.de/DC=test,DC=de -t Mustermann
```

Anpassen der LDAP-Eigenschaften:

```
C:\tools\IbiSystems.GrcSuite.Cmd.Extern.exe ldap -u testuser -p password
-s LDAP://ldap.test.de/DC=test,DC=de -t Mustermann
-l cn,givenname,sn,samaccountname,mail,department,telephonenumber,mobile
```

Angabe aller Parameter (LDAP Query sollte in Anführungszeichen gesetzt werden):

```
C:\tools\IbiSystems.GrcSuite.Cmd.Extern.exe ldap -u testuser -p password
-s "LDAP://ldap.test.de/DC=test,DC=de" -t Mustermann -a None
-l
cn,givenname,sn,samaccountname,mail,department,telephonenumber,mobile,facsimile
telephonenumber
```

```
-q  
"(&(objectCategory=person) (objectClass=user) (| (sn={0}*) (givenname={0}*) (cn={0}*)  
))"
```

7.3 Einrichtung SSO - Windows Authentifizierung

7.3.1 Voraussetzungen

Als Voraussetzung für die Nutzung der Windows-Authentifizierung in ibi systems iris muss der Applikationsserver Mitglied der für die Authentifizierung genutzten Windows-Domäne sein.

Zusätzlich muss noch folgendes Windows-Feature installiert werden:

Rollen/Webserver (IIS)/Webserver/Sicherheit/Windows-Authentifizierung

Um die Windows-Authentifizierung nutzen zu können, muss mindestens ein aktiver ibi systems iris-Benutzer eingerichtet sein. Der Benutzername in ibi systems iris muss mit dem Windows-Benutzernamen (sAMAccountName) übereinstimmen.

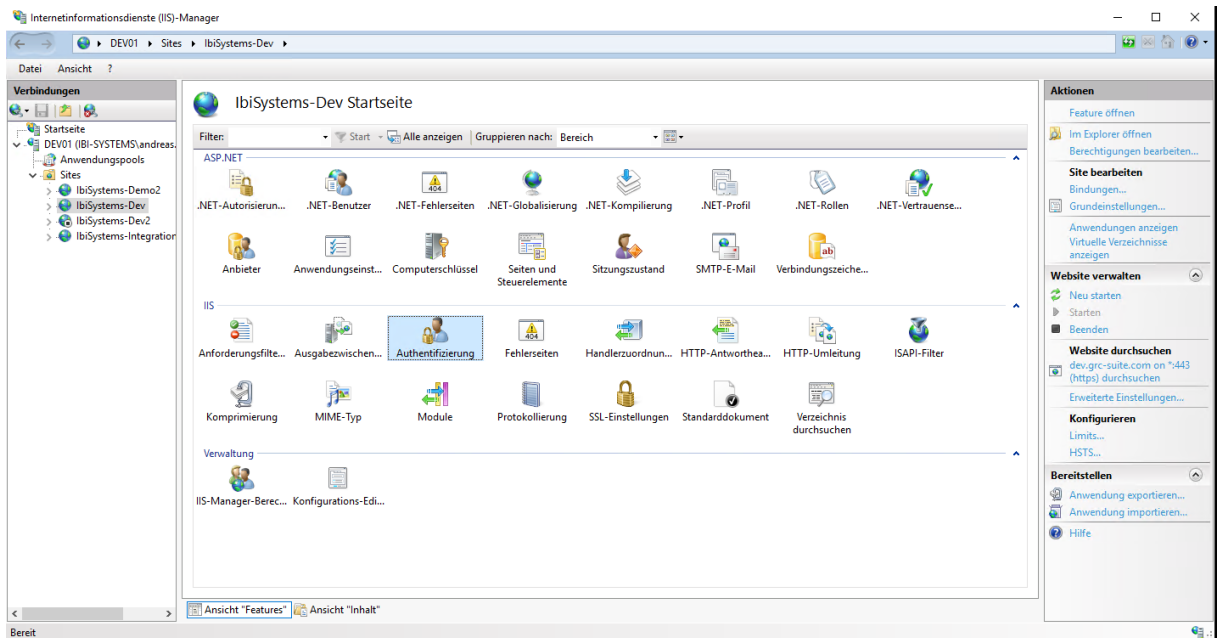
7.3.2 Konfiguration der Anwendung

- **Config-Dateien**

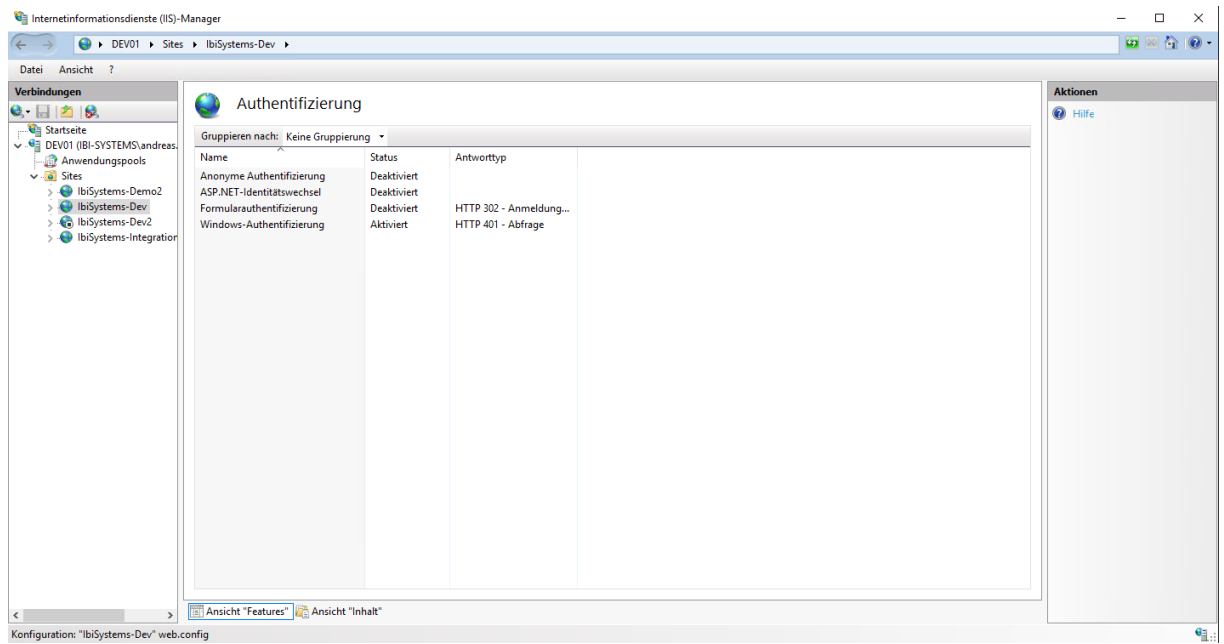
Die Config-Dateien der Anwendung müssen für die Nutzung der Windows-Authentifizierung entsprechend angepasst werden. Damit wir Ihnen die korrekt konfigurierten Dateien zukommen lassen können, teilen Sie uns bitte nur mit, ob Sie bei den ibi systems iris-Benutzernamen die Domäne mit angeben wollen (z.B. „MYDOMAIN\max.mustermann“ – entspricht sAMAccountName) oder ob der Name der Domäne nicht berücksichtigt werden soll („max.mustermann“). Entsprechend dieser Einstellung müssen dann die Benutzernamen der ibi systems iris-Nutzer in der Benutzerverwaltung vergeben werden.

- **IIS – Site Konfiguration**

Zusätzlich müssen im IIS-Manager die Authentifizierungseinstellungen der Anwendung angepasst werden:



Hier müssen alle vorhandenen/installierten Authentifizierungsmethoden außer der Windows-Authentifizierung deaktiviert werden:



Nun ist alles vorbereitet, um die Windows-Authentifizierung mit ibi systems iris zu nutzen.

7.4 Einrichtung SSO - Authentifizierung via OKTA (SAML 2.0)

7.4.1 Voraussetzungen

Als Voraussetzung für die Anbindung von okta an ibi systems iris muss die Anwendung bereits installiert sein.

Die weiteren Schritte der Anleitung gehen davon aus, dass die Anwendung unter der URL `https://iris.company.local` erreichbar ist.

Um die okta Anbindung nutzen zu können, muss mindestens ein aktiver ibi systems iris-Benutzer eingerichtet sein. Der Benutzername in ibi systems iris muss mit dem okta Benutzernamen übereinstimmen.

7.4.2 Konfiguration von okta

Wir empfehlen, für die Konfiguration der Anwendung im okta-Portal die „Classic UI“ zu verwenden. Einige Menüpunkte sind sonst nur sehr versteckt zu erreichen.

7.4.2.1 Anlegen der Applikation im okta-Portal

Als „Sign on method“ für die neue Applikation muss „SAML 2.0“ ausgewählt werden:

✕

Create a new app integration

Sign-in method
[Learn More](#)



- OIDC - OpenID Connect**
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- SAML 2.0**
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- SWA - Secure Web Authentication**
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- API Services**
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.


Cancel Next

Der „App name“ kann frei gewählt werden und mit einem Klick auf den Button „Next“ bestätigt werden:

1 General Settings

App name

App logo (optional)  



App visibility

Do not display application icon to users

Do not display application icon in the Okta Mobile app

[Cancel](#) Next

Um alle benötigten Optionen angezeigt zu bekommen, ist ein Klick auf „Show Advanced Settings“ notwendig:

A SAML Settings

General

Single sign on URL ?

Use this for Recipient URL and Destination URL

Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ?

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

Application username ?

Update application username on

Show Advanced Settings

Folgende URLs müssen in den „SAML-Settings“ eingetragen werden (hier am Beispiel der oben genannten Applikations-URL):

- Single sign on URL: `https://iris.company.local/Admin/SamlAuthentication/Acs`
- Audience URI (SP Entity ID): `https://iris.company.local/Admin/SamlAuthentication`
- Single Logout URL: `https://iris.company.local/Admin/SamlAuthentication/Logout`
- SP Issuer: `https://iris.company.local/Admin/SamlAuthentication`

Außerdem muss der Haken bei „Use this for Recipient URL and Destination URL“ und bei „Allow application to initiate Single Logout“ gesetzt werden.

Das „Signature Certificate“, welches hier mit dem Button „Upload certificate“ hochgeladen werden muss, wird Ihnen von ibi systems zur Verfügung gestellt. Hier noch ein kurzer Überblick über alle benötigten Einstellungen auf der Einstellungs-Seite:

A SAML Settings

General

Single sign on URL ?

`https://iris.company.local/Admin/SamlAuthentication/Acs`

Use this for Recipient URL and Destination URL

Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ?

`https://iris.company.local/Admin/SamlAuthentication`

Enable Single Logout ?

Allow application to initiate Single Logout

Single Logout URL ?

`s://iris.company.local/Admin/SamlAuthentication/Logout`

SP Issuer ?

`https://iris.company.local/Admin/SamlAuthentication`

Signature Certificate ?

okta_signing.cer
Browse

Upload Certificate

7.4.2.2 Benötigte Informationen für Konfiguration der Anwendung

Um die Anwendung ibi systems iris entsprechend konfigurieren zu können, benötigen wir von Ihnen folgende Angaben:

- Identity Provider Single Sign-On URL
- Identity Provider Single Logout URL
- Identity Provider Issuer
- X.509 Certificate

Diese Informationen können im okta-Portal über den Button „View Setup Instructions“ abgerufen werden:

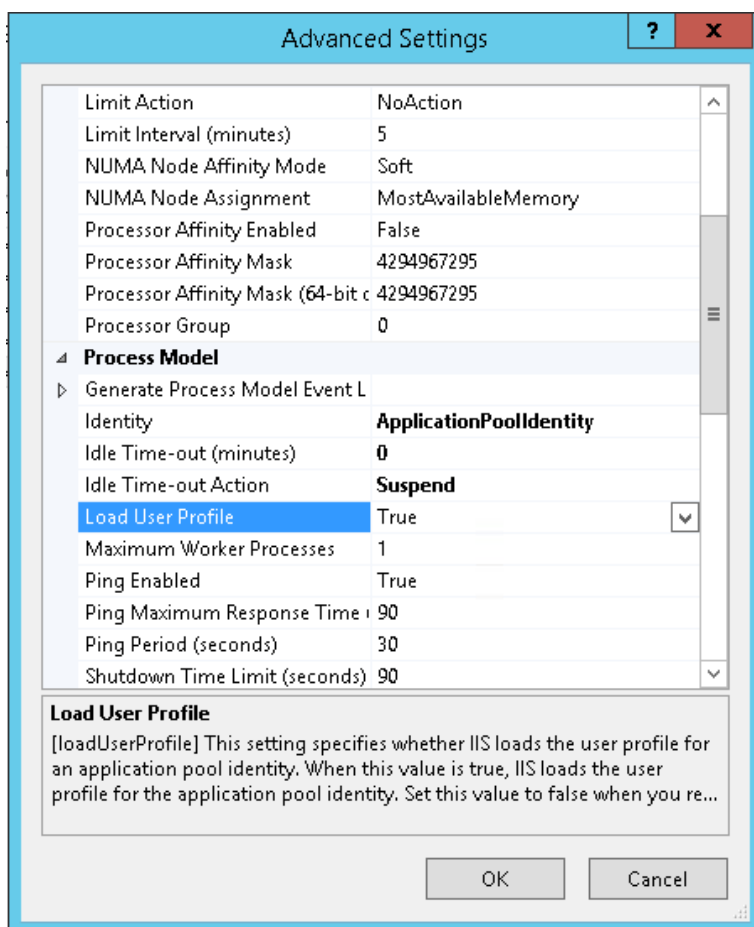
SAML Setup

Single Sign On using SAML will not work until you configure the app to trust Okta as an IdP.

[View SAML setup instructions](#)

7.4.3 Konfiguration der Anwendung in IIS

Zusätzlich zu den in der allgemeinen Anleitung beschriebenen Einstellungen muss in den „Erweiterten Einstellungen“/„Advanced Settings“ des Application Pools der Anwendung noch die Eigenschaft „Benutzerprofil laden“/„Load User Profile“ auf „True“ gestellt werden:



Nun ist alles vorbereitet, um die okta Authentifizierung mit ibi systems iris zu nutzen.

7.5 Einrichtung einer Warm Up Routine für schnelleren Erstzugriff

Um möglichst Ressourcen-schonend zu arbeiten wird die Anwendung über Nacht beendet und bei der ersten Nutzerinteraktion (Anmeldung im System) am Morgen neu gestartet. Da es bei einem Neustart zu etwas ungewohnt, langen Wartezeiten kommen kann, bis die Anwendung für die Nutzung zur Verfügung steht, sollte die Warm Up Routine eingerichtet werden. Diese erlaubt es iris über einen Automatismus bereits vor der ersten Interaktion mit der Anwendung neu zu starten.

Hinweis: die Installation der WarmUp Routine ist nur erforderlich, wenn Sie

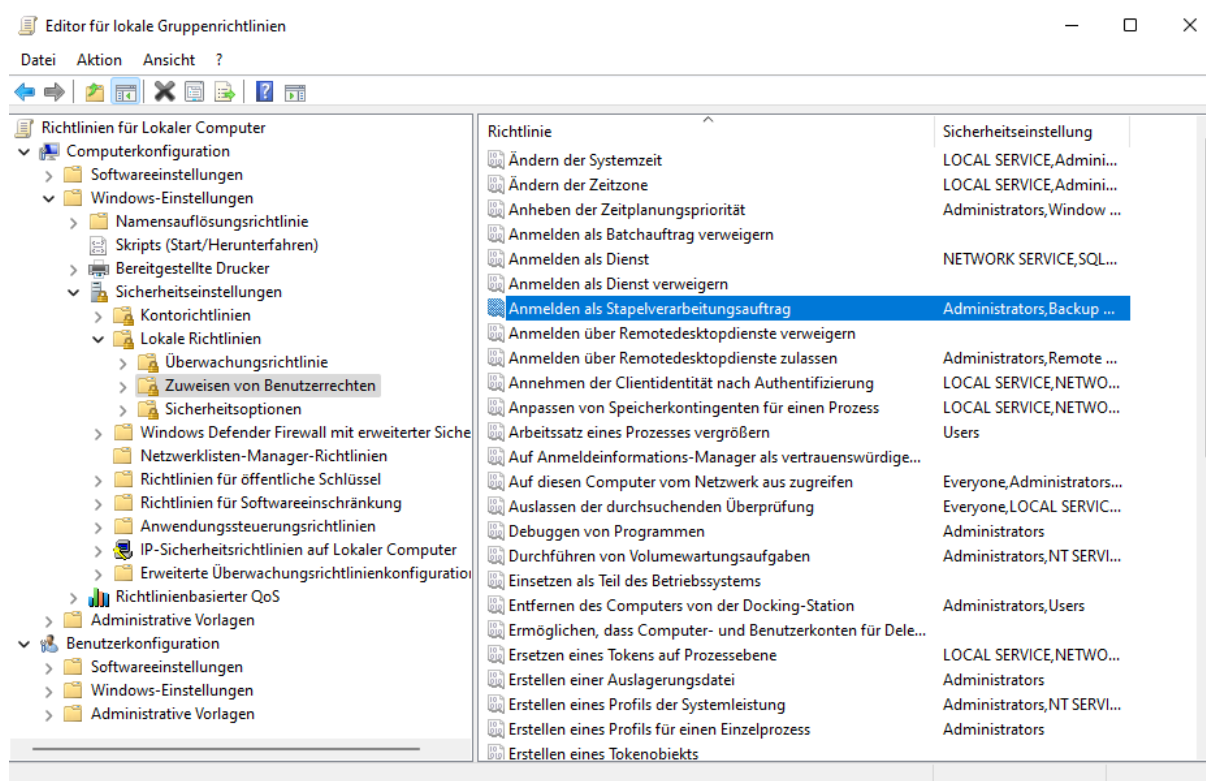
- Mutual TLS einsetzen (diese wird in Verbindung mit der Proxy Authentifizierung meistens eingerichtet)
- Client Zertifikate für den Zugriff auf die Webseite verwenden (siehe Mutual TLS)
- Windows Authentifikation für die Anwendung aktiviert haben (Kerberos)

7.5.1 Voraussetzungen

Um die Geplante Aufgabe anzulegen, benötigen sie einen lokalen Benutzer auf dem Server.

Dieser muss über das Recht zur „Stapelverarbeitung“ verfügen. Dieses kann für den Nutzer in den Gruppenrichtlinien unter **Computerkonfiguration -> Windows-Einstellungen -> Sicherheitseinstellungen -> Lokale Richtlinien -> Zuweisen von Benutzerrechten -> Anmelden als Stapelverarbeitungsauftrag** gesetzt werden.

Sollten sie Windows-Authentifizierung/Kerberos benutzen, muss der Benutzer als Domain Benutzer/AD-Benutzer (ein Service-Account) angelegt werden um sich innerhalb von iris anmelden können.



Um die Aufgabe anzulegen können sie entweder unser PowerShell Skript benutzen oder die nachfolgende Anleitung.

7.5.2 Anwendung des PowerShell-Skripts

Bevor das PowerShell-Skript gestartet werden kann, können einige Parameter angepasst werden. Die „Url“-Variable muss durch die iris-Webseite Url ausgetauscht werden.

```
$Url="https://KUNDE.myiris.io/"  
$Trigger=New-ScheduledTaskTrigger -At 6am -Daily;  
$TaskName = "Wake up iris environnement"
```

Dann kann noch optional der Name der Aufgabe unter „TaskName“ und der Ausführungszeitpunkt unter „Trigger“ angepasst werden. Der Zeitpunkt ist im Beispiel mit Täglich 6 Uhr früh angegeben.

Beim Ausführen des Skripts werden sie nach den Nutzer-Daten gefragt. Geben sie den Benutzernamen, als auch das Passwort in das Fenster ein und bestätigen sie es mit „ok“.



7.5.3 Windows Authentifizierung

Für die Forms-Anmeldung genügt ein lokaler Benutzer auf dem Server. Bei der Windows Authentifizierung wird ein Domain-Benutzer benötigt, welcher sich auch in iris anmelden kann. Zudem muss die „Url“-Variable aus dem PowerShell-Skript auf localhost zeigen, und nicht auf die Webseiten Url. Ansonsten wird durch die „Loopback“-Windows-Sicherheits-einstellung die Anmeldung des ausführenden Nutzers blockiert. Bitte schalten sie auf keinen Fall das „Loopback“-Sicherheitsfeature aus, da dies ein ernstzunehmendes Sicherheitsrisiko darstellt.

7.6 Hinzufügen eines Active Directory Benutzers zur Gruppe IIS_IUSRS

Nach der Installation von IIS werden alle lokalen Benutzergruppen, die von IIS benötigt werden, um auf das Dateisystem zuzugreifen, eingerichtet.

Soll ein Active Directory Konto verwendet werden, um die Datenbankverbindung herzustellen, muss dieser Benutzer auf dem Anwendungsserver in der IIS_IUSRS Gruppe aufgenommen werden.

7.6.1 Lokale Benutzer und Gruppen bearbeiten

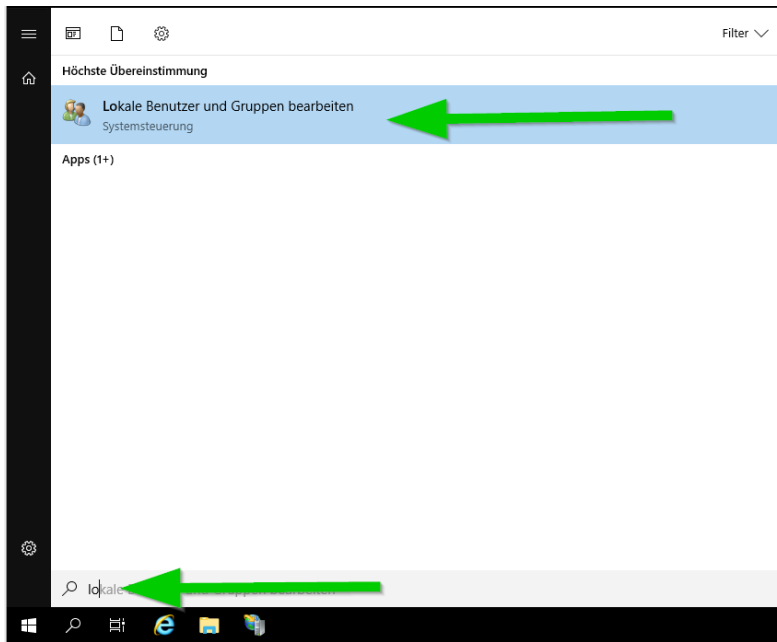


Abbildung 19 - Lokale Benutzer und Gruppen bearbeiten

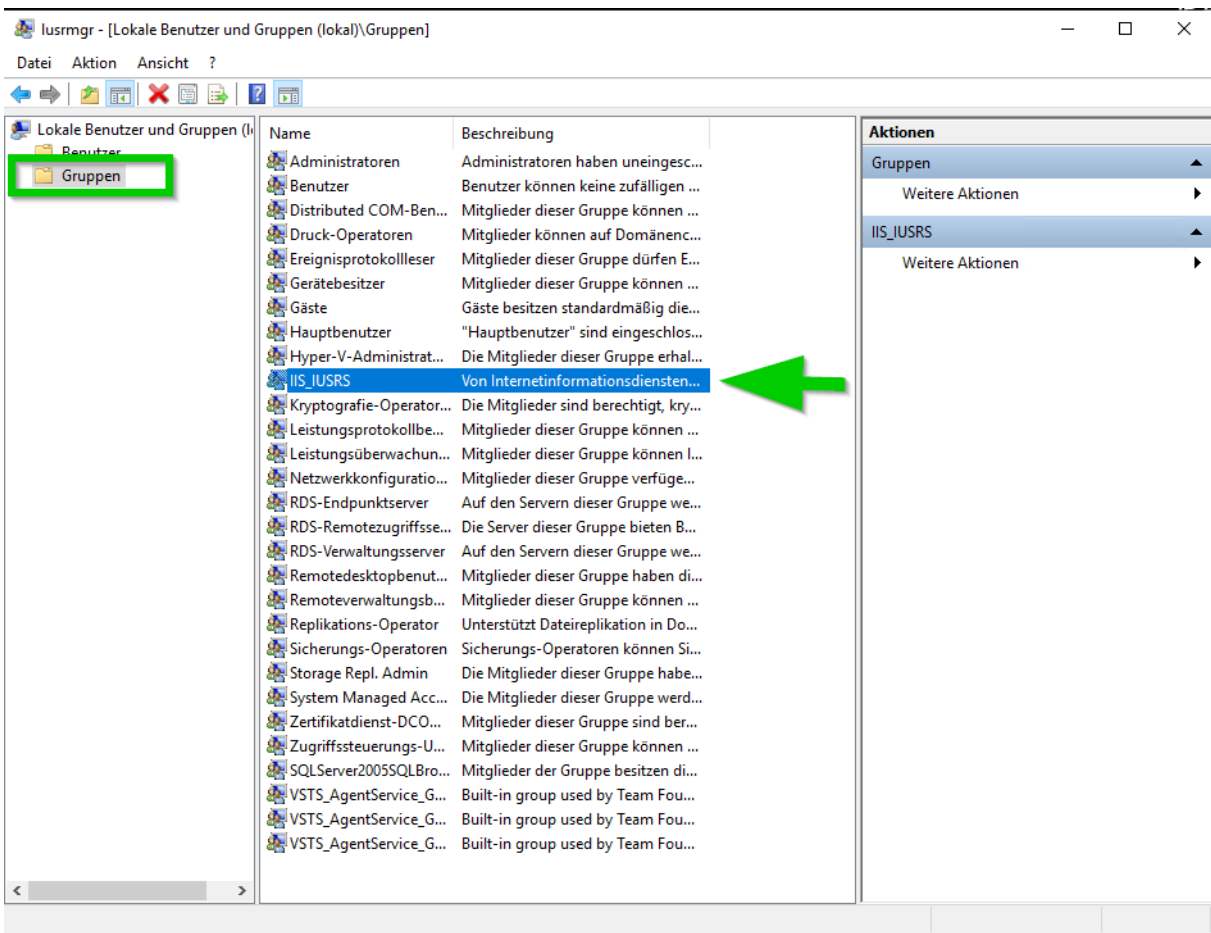


Abbildung 20 – Gruppenverwaltung

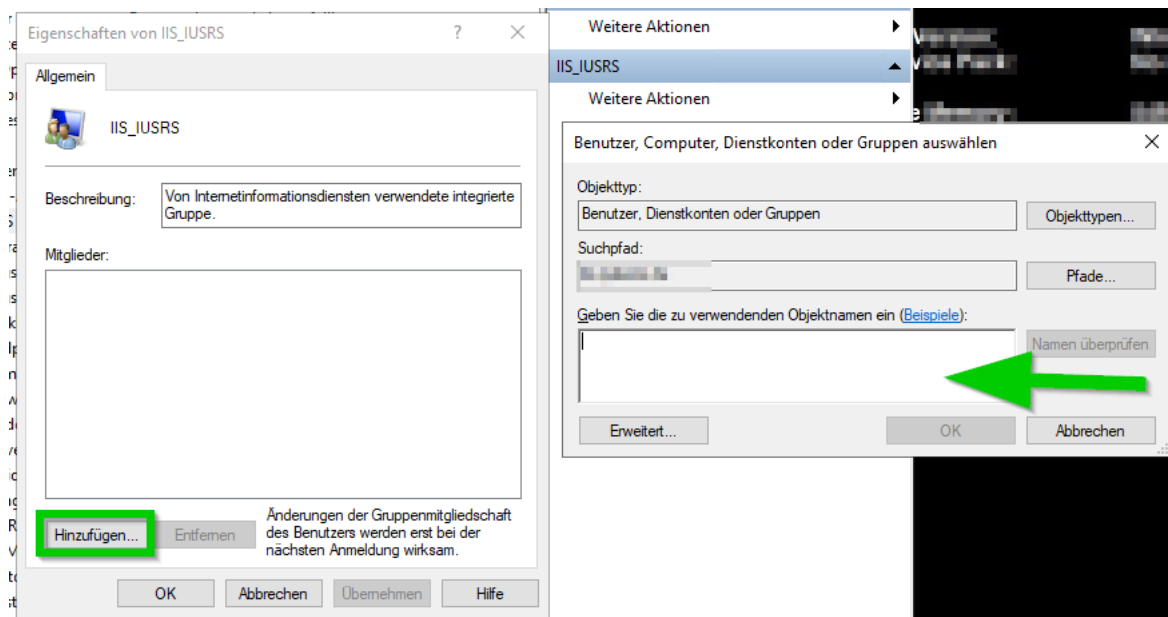


Abbildung 21 - Hinzufügen von Benutzern zur Gruppe IIS_IUSRS

8 Serverumzug / Servermigration

Soll eine existierende iris-Installation auf einen anderen Server umgezogen werden, sind prinzipiell alle Schritte der, bis hier beschriebenen, Neuinstallation notwendig, um den Server für die Datenmigration vorzubereiten. Die folgenden Schritte müssen durchgeführt werden, um die Installation auf das neue System zu übertragen:

1. Beenden Sie die Applikation
2. Ein Backup der Microsoft SQL Datenbank erstellen und auf dem neuen Server einspielen
3. Kopieren Sie den Inhalt des Ordners „C:\inetpub“ ihres alten Systems in den, durch die Installation erzeugten Ordner auf dem neuen System
4. Für gewöhnlich sind die Daten in „inetpub“ gespeichert, sollte dies angepasst worden sein finden sie angepassten Pfade, wie in Kapitel 5.2.3 beschrieben, in der Datei „InfrastructureSettings.config“, auf ihrem alten Server. Diese Ordner müssen ebenfalls auf den neuen Server kopiert werden. Sollten die Daten unter einem neuen Pfad gespeichert werden so müssen die Pfade in der config Datei geändert werden
5. Die in Kapitel 4.1.1 beschriebenen PowerShell-Skripte müssen erneut ausgeführt werden, um sicher zu stellen, dass alle Ordner die korrekten Lese- und Schreibberechtigungen, für die eingerichteten Nutzer auf dem neuen System erhalten. Für den Fall, dass Sie den Pfad für die Datenablage geändert haben muss dieser entsprechend im PowerShell-Skript angepasst werden.
6. Anschließend sollte das System, wie in Kapitel 3.2 beschrieben, erneut auf die Funktionsfähigkeit getestet werden

9 Übliche Betriebsaufgaben

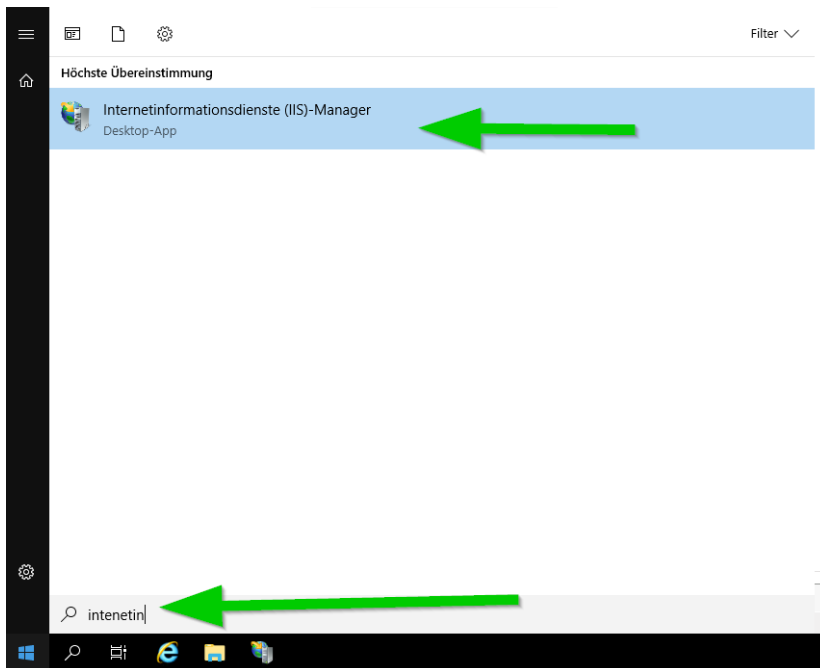
9.1 Hersteller Dokumentationen und Know-How

Hersteller Dokumentationen	
Application Pool	https://learn.microsoft.com/en-us/iis/configuration/system.applicationhost/applicationpools/

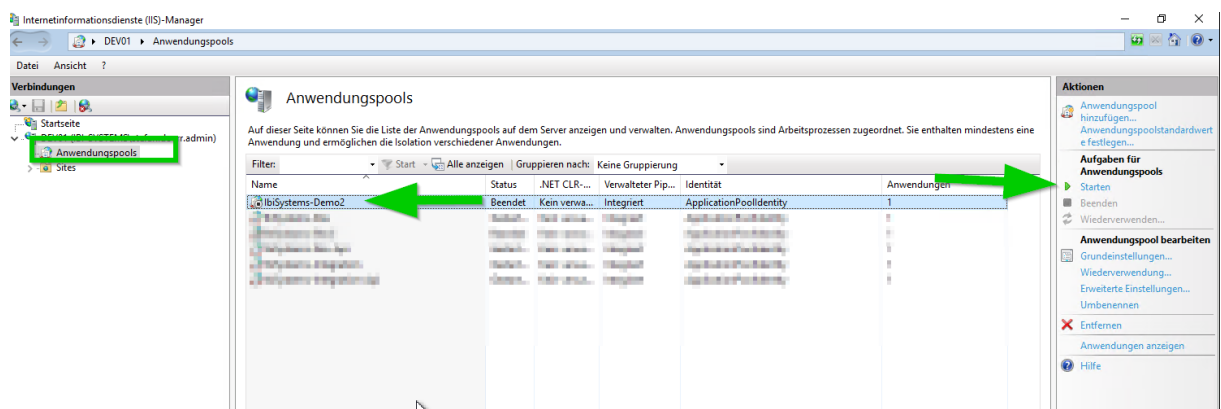
Sites	https://learn.microsoft.com/en-us/iis/get-started/planning-your-iis-architecture/understanding-sites-applications-and-virtual-directories-on-iis
--------------	---

9.2 Starten der Anwendung - Application Pool (Webseite oder Api)

1. Starten der IIS-Management Konsole

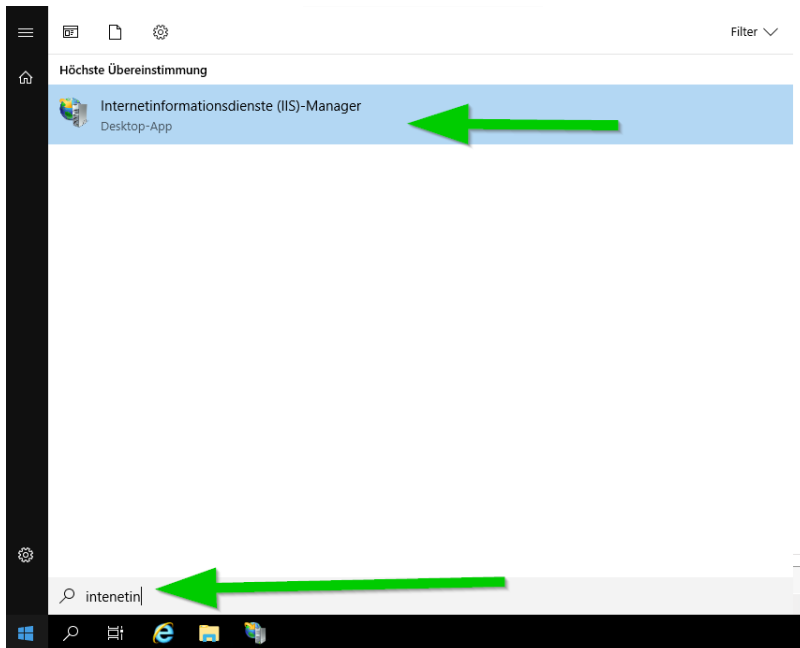


2. Navigation zu den **Anwendungs-Pools**
3. Auswählen des gewünschten Anwendungspools
4. „**Starten**“ der Anwendung

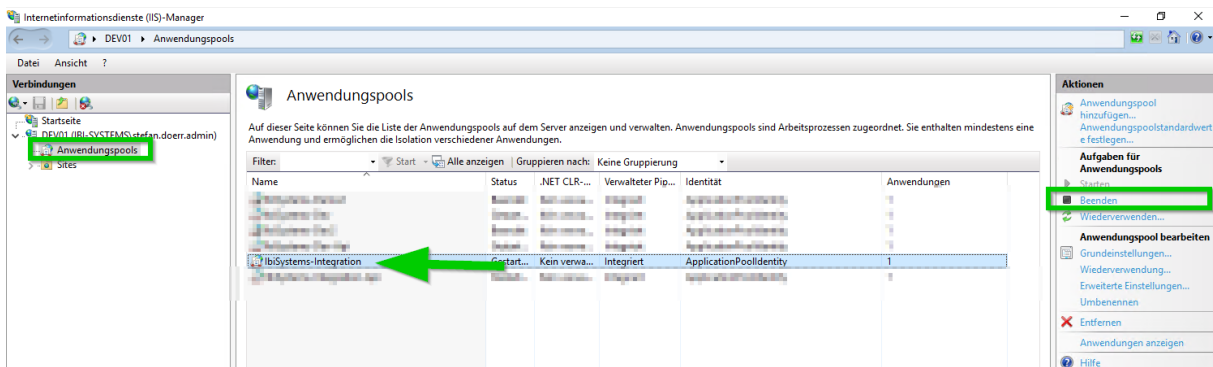


9.3 Stoppen der Anwendung – Application Pool (Webseite oder Api)

1. Starten der IIS-Management Konsole

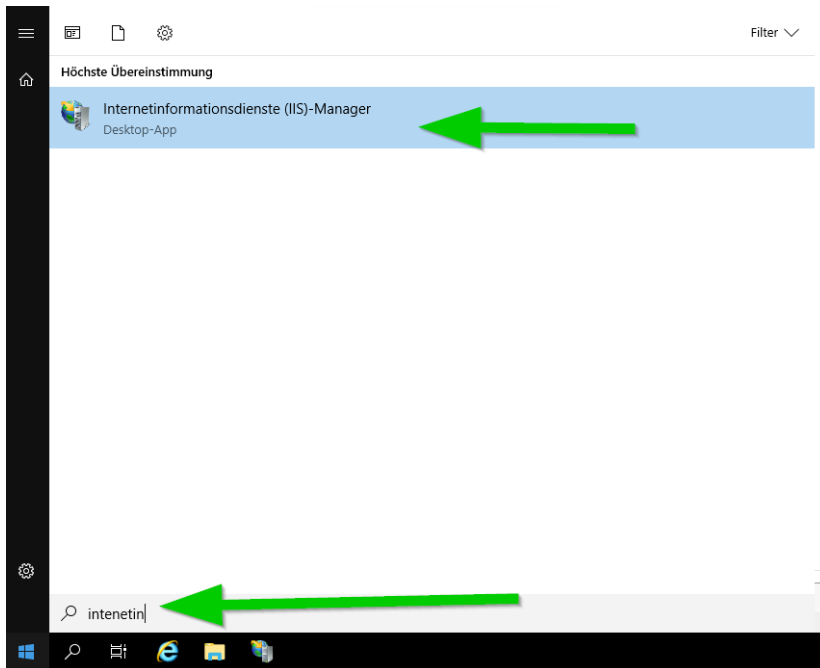


2. Navigation zu den Application Pools
3. Auswahl des gewünschten Anwendungspools
4. „Beenden“ des Anwendungspools

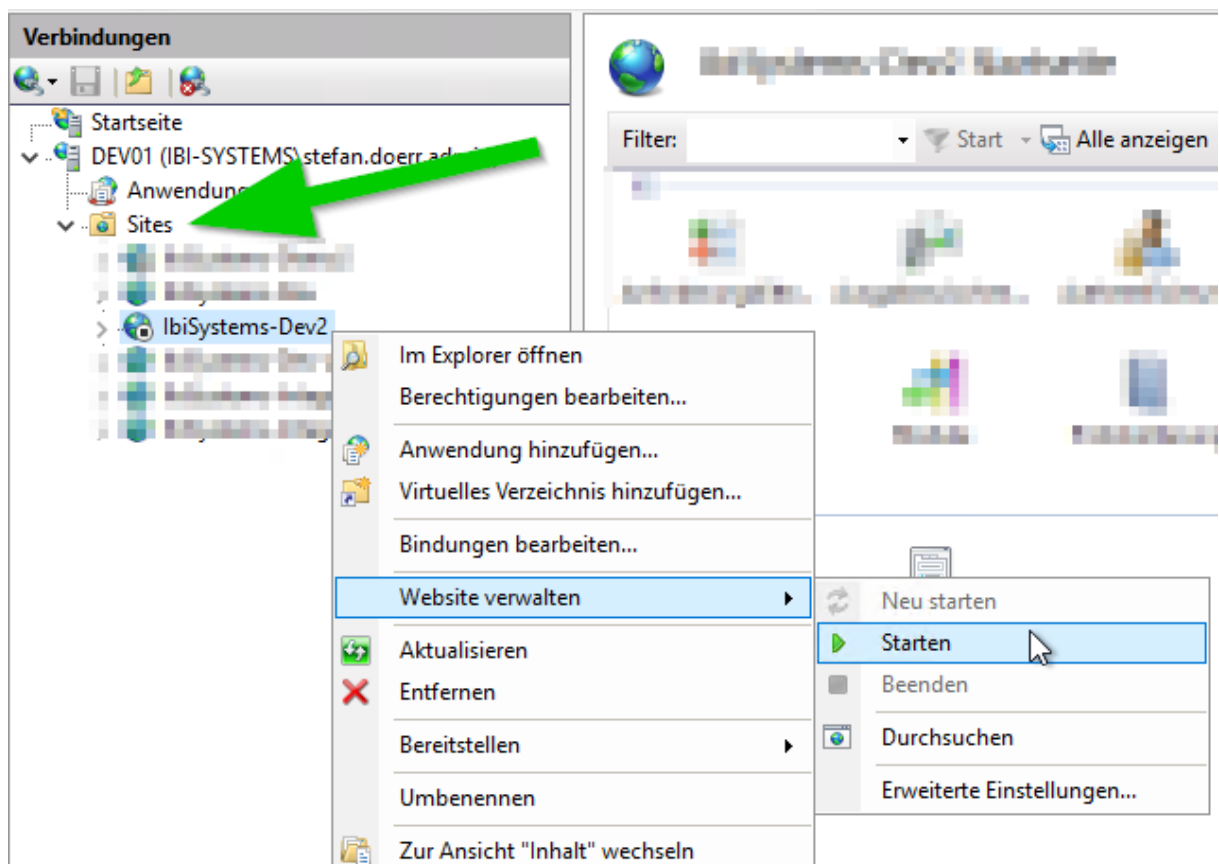


9.4 Starten einer Site

1. Starten der IIS-Management Konsole

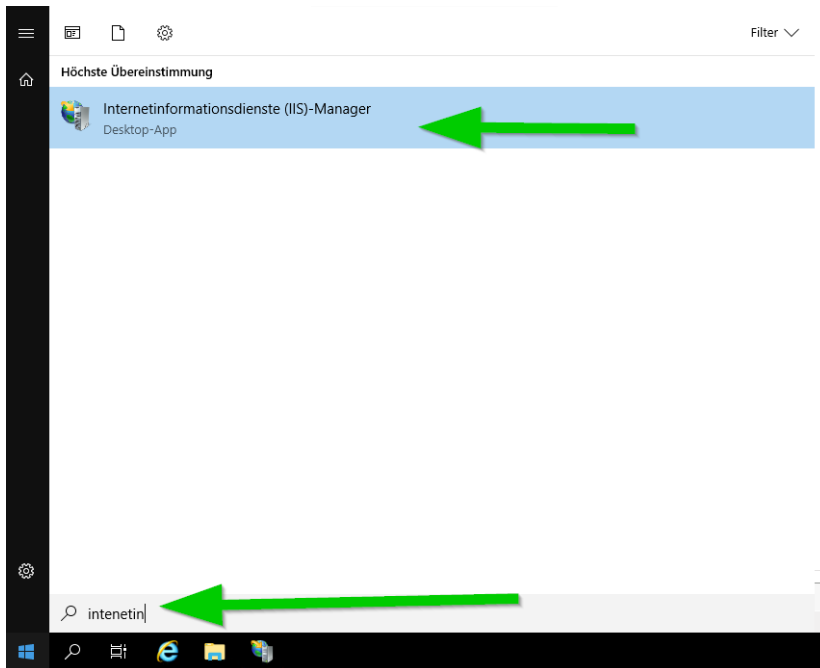


2. Navigation zu den **Sites**
3. **wählen sie die gewünschte Site aus** (z.B. die Website oder die api)
4. Aktivieren Sie über die **rechte Maustaste** das Menü und wählen sie über **Website verwalten / Starten**

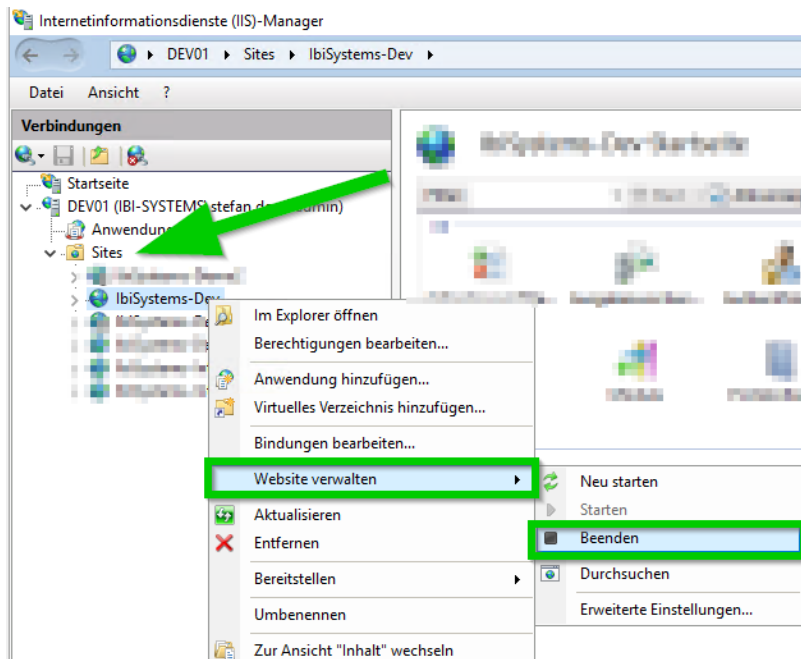


9.5 Stoppen einer Site

1. Starten der IIS-Management Konsole



1. wählen sie die gewünschte Site aus (z.B. die Website oder die api)
2. Aktivieren Sie über die rechte Maustaste das Menü und wählen sie über Website verwalten / Beenden



10 Update der Anwendung

10.1 Vorbereitungsschritte

1. Download des Anwendungspakets
2. Für Major Updates lesen Sie die Upgrade Anweisung, die im Anwendungspaket enthalten ist
3. Download des aktuellen Hosting Pakets (siehe 3.4.2)
4. Installation des Hosting Pakets auf dem Server
5. Entpacken des Anwendungspakets auf dem Server

- Bitte starten Sie den Server neu

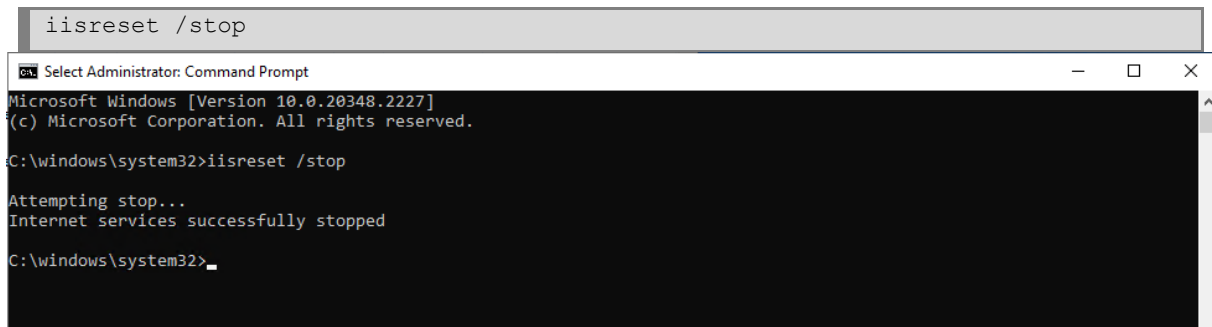
10.2 Update der Anwendung

- Stoppen des IIS-Webservers auf dem Anwendungsserver

Hinweis: Es werden alle Anwendungen (Sites und Application Pools) des Servers angehalten

Command Line:

```
iisreset /stop
```



```
Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.2227]
(c) Microsoft Corporation. All rights reserved.

C:\windows\system32>iisreset /stop

Attempting stop...
Internet services successfully stopped

C:\windows\system32>
```

- Sicherung der SQL-Server Datenbank durchführen
- Umbenennung des Anwendungsverzeichnis (Website)
- Anlegen des Anwendungsverzeichnis (Website)
- Kopieren des „Application“-Verzeichnisses aus dem Installation Paket in das neu erstellte Anwendungsverzeichnis
- Übertragen der Konfigurationsdateien des Anwendungsverzeichnis (alt) in das neue Anwendungsverzeichnis
- Prüfung oder Übernahme der Dateisystemberechtigungen auf dem Anwendungsverzeichnis (Website) -> siehe 5.1.1.2**

- Umbenennung des Anwendungsverzeichnis (RestApi)
- Anlegen des Api-Verzeichnisses (RestApi)
- Kopieren des „Api“-Verzeichnisses aus dem Installation Paket in das neu erstellte Api-Verzeichnis
- Übertragen der Konfigurationsdateien des Anwendungsverzeichnis (alt) in das neue Anwendungsverzeichnis
- Prüfung oder Übernahme der Dateisystemberechtigungen auf dem Anwendungsverzeichnis (RestApi) -> siehe 5.1.1.2**

- Starten der Anwendung

10.3 Update der Datenbank

- Starten der Anwendung

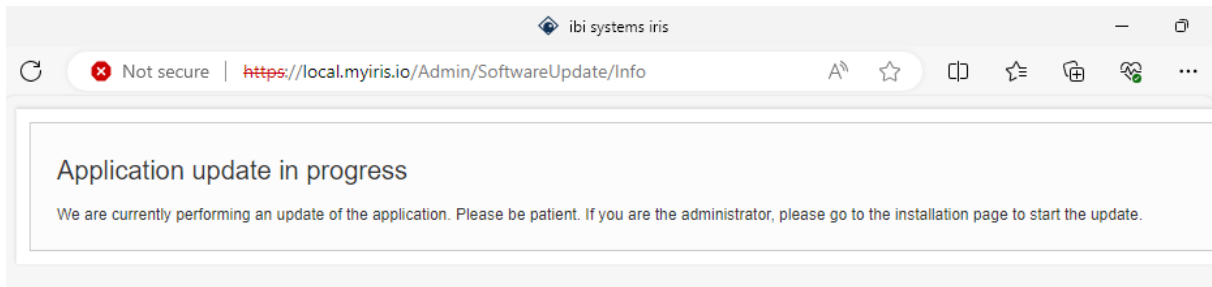
```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.5329]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\windows\system32>iisreset /start

Attempting start...
Internet services successfully started

C:\windows\system32>
```

- Aufrufen der Startseite der Anwendung (sie sollten dabei auf die Software-Update Seite weitergeleitet werden)



- Bitte ändern Sie den letzten Teil der URL von „Info“ auf „Install“ und führen Sie den die Anweisungen des Migrations-Assistenten aus

Variante 1 – Update über den Update Assistenten

Hinweis: Dieser Schritt wird für Sie ausgewählt, wenn Sie den Connection String **GrcSuiteDb_Admin** innerhalb der „Connection Strings“ Konfigurationsdatei hinterlegt haben dabei aktualisiert sich die Datenbank für Sie im Hintergrund

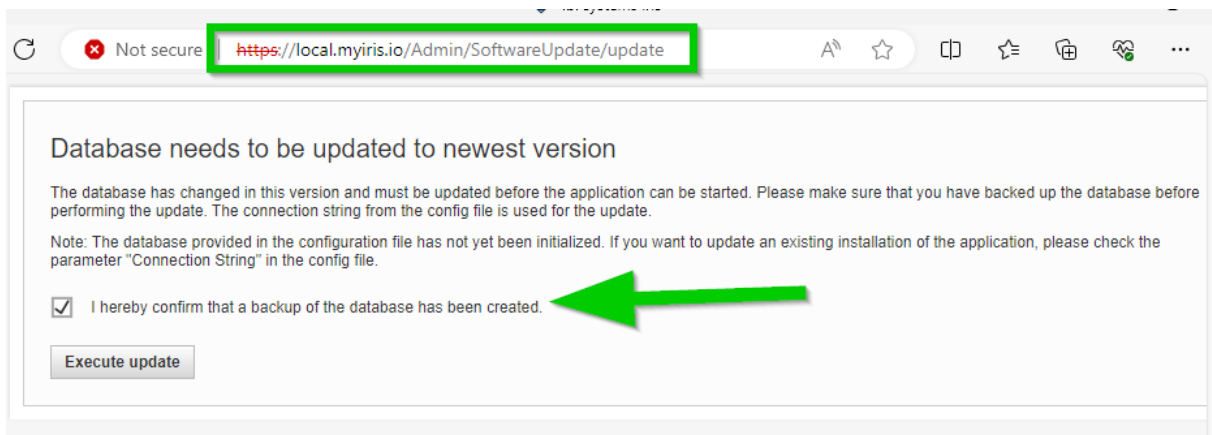


Abbildung 22 - Database Update Assistent

Variante 2 – Manuelles Datenbank Update durchführen (Legacy Verfahren)

Hinweis: Diese Variante wird nicht mehr unterstützt und ist nur aus Gründen der Abwärtskompatibilität hier aufgeführt.

- Bitte laden Sie sich die Datenbank Update Datei herunter und folgen den Anweisungen innerhalb der Zip-Datei

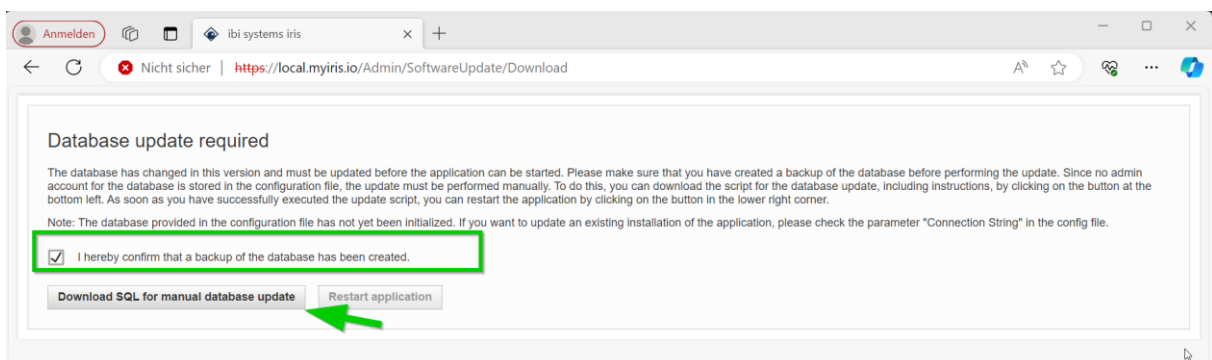


Abbildung 23 - Manuelles Datenbank Update durchführen

Hinweis: In einigen Fällen erscheint beim Neustart der Anwendung nach dem Datenbank-Update eine Fehlerseite, dass die Anwendung nicht gestartet werden konnte. In diesem Fall sollte es helfen, Application Pool und Website nochmals über den IIS-Manager zu beenden und neu zu starten.

Potenzielle Ursachen:

- **Der Anwendungspool ist nicht korrekt konfiguriert**
Bitte prüfen Sie die Konfiguration des Anwendungspools (siehe 4.2.1.6)
- **Das SAML Signing-Zertifikat ist nicht am erwarteten Speicherort abgelegt / oder kann nicht geöffnet werden**
 - Bitte prüfen Sie die Dateisystem Berechtigungen des Zertifikats (siehe 5.1.1.2)
 - Bitte prüfen Sie die Konfigurationsdatei, in der die Pfade für die SAML-Konfiguration hinterlegt sind (siehe 7.4)
- **Das SAML Signing-Zertifikat ist abgelaufen oder nicht korrekt erstellt worden**
 - Bitte kontaktieren Sie den Support von ibi systems iris

11.5 Fehlermeldung (Die aktuelle Datenbankstruktur ist veraltet)

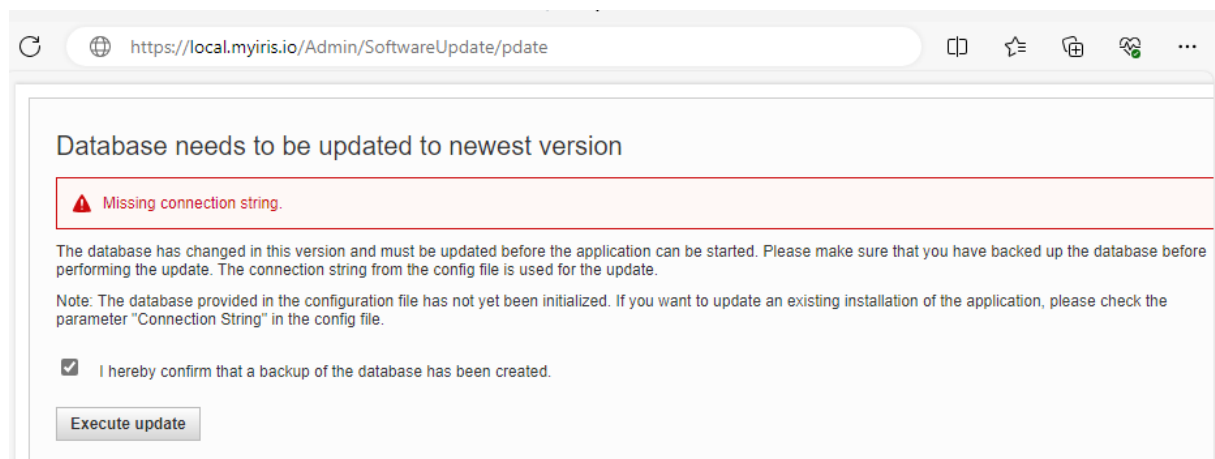
Error Message: Apilifecycle|Die aktuelle Datenbankstruktur ist veraltet. Bitte führen Sie alle ausstehenden Datenbankmigrationen aus.

Potenzielle Ursachen:

- **die Update Installation wurde nicht ausgeführt**
Bitte aktualisieren Sie die Datenbank analog der Ersteinrichtung in Kapitel 6.1
- **der Datenbank Benutzer hat nicht die korrekten Berechtigungen, um die Datenbank Struktur anzulegen**
Bitte prüfen Sie die Berechtigungen der Datenbank Benutzer (siehe Kapitel 2.2.3)
- **die Anwendung verwendet den falschen Benutzer eine Datenbankverbindung aufzubauen**
Bitte prüfen Sie ob der Application (siehe 4.1.4)

11.6 Fehlermeldung (Missing Connection String) Update

Error Message: Missing Connection String



Ursache: Bei der Installation wurde der Connection String „GrcSuiteDb_Admin“ nicht innerhalb der Konfigurationsdatei gespeichert. Um das Update korrekt durchführen zu können prüfen Sie bitte das Kapitel 10.3.