

INGRADA web

Installationsanleitung

Stand: März 2024

Rechtliche Hinweise

Haftungsausschluss

Die beschriebene Software unterliegt den Lizenzvereinbarungen (EULA) und darf nur zu deren Bedingungen verwendet werden. Die Softplan Informatik GmbH steht lediglich für Produkte und Dienstleistungen nach der Maßgabe ein, die in der Vereinbarung über die jeweiligen Produkte und Dienstleistungen ausdrücklich geregelt sind.

Die Weitergabe und Vervielfältigung dieser Publikation oder von Teilen daraus, zu welchem Zweck und in welcher Form auch immer, sind ohne die ausdrückliche schriftliche Genehmigung durch die Softplan Informatik GmbH nicht gestattet.

In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden. Die vorliegenden Angaben werden von der Softplan Informatik GmbH bereitgestellt und dienen ausschließlich Informationszwecken. Das Unternehmen übernimmt keinerlei Haftung oder Garantie für Fehler oder Unvollständigkeiten in dieser Publikation.

Die verwendeten Beispieldaten und Nutzerinformationen sind frei erfunden. Aus den in dieser Publikation enthaltenen Informationen ergibt sich keine weiterführende Haftung.

Markenzeichen

Die angebotenen Softwareprodukte können Softwarekomponenten auch anderer Softwarehersteller enthalten. Alle anderen Namen von Produkten und Dienstleistungen sind Marken der jeweiligen Firmen. Die Angaben im Text sind unverbindlich und dienen lediglich zu Informationszwecken. Produkte können länderspezifische Unterschiede aufweisen.

Microsoft Windows, Windows Server, SQL Server, PowerShell, MSDN, Visual Studio, ActiveX, .NET, Microsoft Office, Word, Excel, Access, Outlook, PowerPoint, Internet Explorer und Edge sind eingetragene Marken der Microsoft Corporation.

AutoCAD, Map3D, MapGuide und AIMS sind eingetragene Marken der Autodesk Incorporated.

GEOgraf ist eine eingetragene Marke der HHK Datentechnik GmbH.

Oracle, Java und JavaScript sind eingetragene Marken der Oracle Corporation.

Adobe Acrobat, Acrobat Reader sind eingetragene Marken der Adobe Systems Incorporated.

Google, Google Maps und Chrome sind eingetragene Marken der Google Incorporated.

HTML, XHTML, XML, XSL, SVG sind eingetragene Marken des W3C, World Wide Web Consortium, Massachusetts Institute of Technology.

OpenGIS Web Service (OWS), CSW, WCS, WFS, WMS, GML und SLD sind eingetragene Marken des OGC, Open Geospatial Consortium, Incorporated.

FDO ist eine eingetragene Marke der OSGeo, Open Source Geospatial Foundation und als Open Source lizenziert unter der LGPL (GNU).

© Copyright Softplan Informatik GmbH. Alle Rechte vorbehalten.

Inhalt

Inhaltsverzeichnis

Inhalt	3
Einleitung	5
Systemvoraussetzungen.....	5
Software-Anforderungen	5
Betriebssysteme.....	5
Wichtige Hinweise:.....	5
Datenbanksysteme Microsoft SQL Server.....	5
Microsoft SQL Server Reporting Services.....	6
Internet Information Server	6
Autodesk Infrastructure 2017	6
MapGuide Open Source 3.1.1	6
Virtual Machine	6
Voraussetzung zur Fortführung eines Projektes aus INGRADA 4.14.....	6
Zusätzliche Software auf dem Client.....	6
Browser	6
INGRADA LocalApp.....	6
Hinweis bei Zertifikatsproblemen in FireFox mit der LocalApp	8
PDF, DOC	9
Security Software	9
Verwendung von Rasterdaten	9
Serverinstallation von INGRADA web	10
Hinweise zur Installation	10
Installation starten	11
Einrichten des Servers für INGRADA web	19
Temporärer Pfad für die .net-Kompilierung.....	19
Webprojekte vorabladen	19
INGRADA web und HTTPS	20
Hinweise zur Serverkonfiguration.....	22
Einrichten eines nächtlichen IIS- und MapGuide-Neustarts via Taskplaner und Skript.....	22
WMS-Dienste für MapGuide konfigurieren	23
Browsereinstellungen für INGRADA web.....	26
Einstellungen in Firefox.....	26
Drucken von Berichten.....	27
Deinstallation von INGRADA web	27
INGRADA web vollständig deinstallieren	27

Anhang 1: SQL Server 2017 Express Installation	28
Anhang 2: Installation SQL Server Management Studio	37
Anhang 3: MS SQL Reporting Services 2017 nachinstallieren und konfigurieren	42
Ergänzung in der Datei <i>web.config</i>	56
Anhang 4: Konfigurieren des MS SQL Reporting Services	58
Windows-Benutzer für Reporting Services anlegen.....	58
Rollenzuweisung in der Berichtsmanager-Oberfläche	60
Anlegen eines SQL-Server Benutzers	61
Ergänzung in der Datei <i>web.config</i>	65
Anhang 5: SQL Server Update Installation	66
Anhang 6: Installation von IIS 10 auf Windows Server 2019	70
Anhang 7: Zusatzpakete Installieren für IIS Installieren.....	80
Anhang 8: Installation und Konfiguration von AIMS 2017	84
Installation des Infrastructure Map Servers.....	84
Autodesk Infrastructure Map Server 2017 lizenzieren	87
Anhang 9: Installation von MapGuide Open Source 3.1.1	90
Parallelinstallation AIMS und MapGuide 3.1.1	95
AIMS Passwörter	96
Anhang 10: Installation von MapGuide Maestro	97
Anhang 11: Sicherheit prüfen	100
Relevante Einstellungen.....	101

Einleitung

Diese Anleitung beschreibt die Installation von INGRADA web mit allen Komponenten auf einem Server.

Systemvoraussetzungen

Bitte beachten Sie die Hinweise in diesem Kapitel, bevor Sie mit der Installation von INGRADA web beginnen. Die aktuellsten Anforderungen an Hardware und Software finden Sie im Internet unter:

<https://www.ingrada.de/systemvoraussetzungen.html>

Software-Anforderungen

Prüfen Sie vor der Installation, ob die erforderlichen Software-Komponenten auf dem Rechner installiert und korrekt konfiguriert sind. Hinweise zur Konfiguration erfahren Sie in dieser Anleitung.

Betriebssysteme

INGRADA web kann unter folgenden Betriebssystemen installiert werden:

- Microsoft Windows Server 2022 (21H2 - LTSC - deutsche Version)
- Microsoft Windows Server 2019 (deutsche Version)
- Microsoft Windows Server 2016 (deutsche Version)

Wichtige Hinweise:

- Microsoft Small Business Server, Domaincontroller, Microsoft Exchange Server und 32 Bit-Systeme werden nicht unterstützt!

Datenbanksysteme Microsoft SQL Server

Die Installation wird beispielhaft im Anhang 1 beschrieben.

INGRADA web unterstützt folgende Datenbanksysteme:

- Microsoft SQL Server 2019
Microsoft SQL Server 2019 Express with Advanced Services
- Microsoft SQL Server 2017
Microsoft SQL Server 2017 Express with Advanced Services
- Microsoft SQL Server 2016
Microsoft SQL Server 2016 Express with Advanced Services

Achtung: Die Microsoft SQL Server-Versionen sind nur aufwärtskompatibel! Bitte klären Sie mit Ihren Datenzulieferern/Dienstleistern die verwendeten Datenbankversionen ab, damit ein Datenaustausch gewährleistet ist!

Microsoft SQL Server Reporting Services

Die Installation des MS SQL Reporting Services wird in Anhang 2 beschrieben. Anhang 3 enthält Informationen zur Konfiguration, zur Installation und Konfiguration eines Berichtsservers sowie zu den notwendigen Ergänzungen in der Datei web.config.

Internet Information Server

Die Installation des IIS10 auf Windows Server 2019 wird im Anhang 6 beschrieben. Das Vorgehen ist beim Windows Server 2016 identisch.

Autodesk Infrastructure 2017

Anhang 10 beschreibt die Installation des Infrastructure Map Server und den erforderlichen Änderungen in der Datei Serverconfig.ini.

Hinweis: AIMS 2017 und AIMS 2015 können nicht parallel installiert werden. Nach der Installation von AIMS 2017 funktioniert der Site-Admin von AIMS 2015 nicht mehr!

MapGuide Open Source 3.1.1

(inkl. WebServerExtensions im gleichen Verzeichnis wie MapGuide Server) Achtung: Die Parallelinstallation zweier MapGuide Open Source Versionen wird nicht empfohlen!

Virtual Machine

Beim Betrieb in einer „VM“ ist darauf zu achten, dass diese nicht auf einen anderen Host übertragen wird, da sonst die Lizenz des Kartenservers ungültig wird.

Voraussetzung zur Fortführung eines Projektes aus INGRADA 4.14

Sollen die Daten des INGRADA web Projektes durch eine Konvertierung aktualisiert werden, so ist eine INGRADA 4.14-Installation auf dem Server notwendig.

Zusätzliche Software auf dem Client

Bitte prüfen Sie vor der Installation, ob die folgenden Software-Komponenten auf dem Client installiert sind.

Browser

Empfohlen werden aktuelle Versionen der folgende Browser:

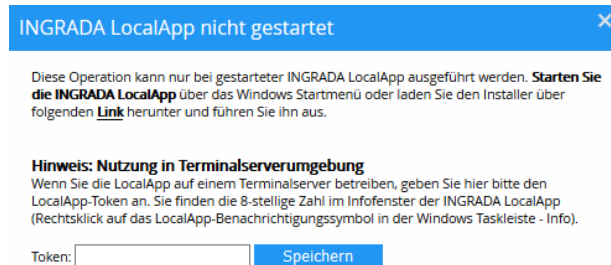
- Google Chrome
- Microsoft Edge
- Mozilla Firefox

INGRADA LocalApp

INGRADA web erfordert kein Java. Die erforderlichen Funktionen wie z. B. lokale Dateizugriffe werden von der *INGRADA LocalApp* übernommen.

Hinweis: Weitere Informationen finden Sie im INGRADA LocalApp Benutzerhandbuch.

Die Installation der LocalApp erfolgt auf jedem Client, der die Funktionen *Dateien und Videos öffnen* sowie *externe Anbindungen über Textdateien* nutzt. Ist die Local App noch nicht installiert oder nicht gestartet, erscheint folgender Dialog beim Ausführen der oben genannten Funktionen:



Dialog zum Herunterladen der LocalApp.

Klicken Sie auf den Link zum Herunterladen und führen Sie die Installation durch. Folgen Sie dabei den Anweisungen auf dem Bildschirm. Für eine lokale Installation lassen Sie den Haken im Dialog „Hinweise und Einstellungen“ wie voreingestellt aktiviert.



Für die Installation auf einem Terminalserver entfernen Sie den Haken und fahren Sie mit der Installation fort.

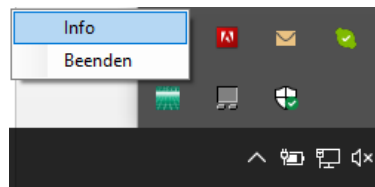
Nachdem die Installation abgeschlossen ist, starten Sie die LocalApp über die Verknüpfung auf Ihrem Desktop um die Funktionen *Dateien und Videos öffnen* sowie *externe Anbindungen über Textdateien* zur Verfügung zu stellen. Nach einem Rechnerneustart wird die LocalApp automatisch gestartet.

Verwendung eines Terminalserver

Um die LocalApp auf einem Terminalserver abzuschließen, muss für jeden Anwender ein Token eingerichtet werden. Das Token wird von der LocalApp automatisch generiert.

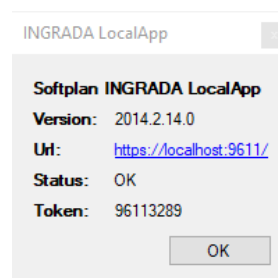
Token einrichten

Öffnen Sie das Infofenster der LocalApp mit einem Rechtsklick auf das Benachrichtigungssymbol in der Windows Taskleiste:



Infofenster der LocalApp öffnen.

Das generierte Token wird angezeigt:



Anzeige des Tokens.

Zum Kopieren doppelklicken Sie auf die 8-stellige Zahl und fügen Sie diese über einen Rechtsklick in das Feld *Token* ein.

Wichtig: Wird ein neuer Benutzer am Terminal Server eingerichtet, so müssen die Zertifikate neu erstellt werden. Um die neuen Zertifikate für den/die neuen Benutzer anzulegen, führen Sie die LocalApp als Administrator mit dem Parameter „addcertterminal“ aus:

```
C:\Program Files (x86)\Softplan\LocalApp\Softplan.Ingrada.LocalApp.exe addcertterminal
```

Anschließend stehen die Funktionen auch unter Terminalserver zur Verfügung.

Hinweis bei Zertifikatsproblemen in FireFox mit der LocalApp

Sollten die LocalApp unter Firefox nicht ausgeführt werden, ist wahrscheinlich das selbstsignierte Zertifikat unter Firefox nicht erlaubt. In diesem Fall gehen Sie wie folgt vor:

Möglichkeit A: Sicherheitsausnahme hinzufügen

1. Adresse <https://localhost:9610/api/info/isrunning> im Firefox öffnen (für Terminalserver öffnen Sie das Infofenster der LocalApp und passen Sie die Portnummer in der Adresse an).
2. Auf *Erweitert* klicken, wenn die Warnung über ein mögliches Sicherheitsrisiko erscheint.
3. Der Fehler *Fehlercode: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT* wird angezeigt, da von Firefox keine selbstsignierten Zertifikate mehr akzeptiert werden. Auf *Risiko akzeptieren und fortfahren* klicken.

Möglichkeit B: Zertifikatsspeicher von Windows automatisch in Firefox übernehmen

Mozilla hat im Firefox bereits mit Version 49 die Option *security.enterprise_roots.enabled* eingeführt. Damit ist es möglich, Zertifikate aus Windows automatisch in den Firefox zu übernehmen. Um diesen Wert zu aktivieren, gehen Sie wie folgt vor:

1. Geben Sie *about:config* in die Adresszeile vom Firefox ein.
2. Klicken Sie auf den Button *Ich bin mir der Gefahren bewusst!*
3. Suchen Sie nach dem Einstellungsname *security.enterprise_roots.enabled*
4. Stellen Sie den Wert von *false* auf *true* um.

Probleme beim Installieren der LocalApp

Die Fehlermeldung „Zertifikat nicht vorhanden..“ beim Ausführen der IngradaWeb-LocalApp können Sie folgendermaßen beheben:

1. Melden Sie sich an dem betreffenden Arbeitsplatz mit einem Administrator-Konto an, das noch nie auf diesem PC angemeldet war.
Wichtig ist, das mit diesem Konto noch niemals auf diesem PC angemeldet wurde.
2. Laden sie sich eine LocalApp von Ingradaweb herunter
3. Deinstallieren sie die vorhandene LocalApp
4. starten Sie die im heruntergeladenen Archiv enthaltene setup.exe „als Administrator“ und wählen Sie „installieren“

PDF, DOC

Zur Anzeige von PDF-Dateien und Office-Dokumenten werden derzeit folgende Softwareversionen vorausgesetzt:

- Adobe Acrobat Reader ab Version 11 oder Foxit Reader ab Version 9
- Microsoft Office ab Version 2013 oder Open Office ab Version 4

Security Software

Hinweis: Falls der INGRADA web Client langsam läuft, können Sie Ihre Security Software kurzzeitig deaktivieren, um Performanceeinbußen festzustellen

Verwendung von Rasterdaten

Verwenden Sie in Ihren Projekten Luftbilder in den Formaten GeoTIFF oder ECW. Rasterbilder im Format JPEG2000 führen zu Instabilitäten und sollten nicht eingebunden werden!

Hinweis: ECW-Dateien können nur in Autodesk Infrastructure MapServer (AIMS) verwendet werden, da MapGuide Open Source keinen ECW-Provider enthält.

Serverinstallation von INGRADA web

Dieses Kapitel beschreibt die Installation von INGRADA web. Bitte beachten Sie die folgenden Hinweise, bevor Sie mit der Installation beginnen.

Hinweise zur Installation



Voraussetzung für INGRADA web

Vor Beginn der INGRADAweb Installation müssen folgende Softwarekomponenten installiert und Konfiguriert sein.

1. IIS
2. SQL Server
3. Reporting Server
4. Kartenserver (AIMS 2017 oder MapGuide OpenSource)
5. Die Konfiguration wird im Anhang beschrieben



Parallele INGRADA Web-Versionen

INGRADA web kann parallel zu bereits bestehenden Versionen installiert werden. Eine Deinstallation von älteren Versionen ist nicht notwendig. Dadurch können INGRADA web Projekte zunächst auf die neueste Version aktualisiert werden, bevor die ältere Version von INGRADA web ggf. deinstalliert wird.

Hinweis: Bitte sichern Sie vor der Deinstallation von INGRADA web, den Registry-Schlüssel "softplan" in *HKEY_Local_Machine\Software* (Exportieren über Regedit). Sollten Sie beim Starten der INGRADA web eine Fehlermeldung erhalten, importieren Sie bitte den Schlüssel "softplan" zurück (Importieren über Regedit).



Die Installation darf nicht über ein Netzlaufwerk gestartet werden!

Kopieren Sie das Installationsarchiv auf eine lokale Festplatte und starten Sie diese von dort aus.



Reportvorlagen sichern

Bei der Installation von INGRADA web werden standardmäßig alle Reportvorlagen älterer Versionen hochgeladen und damit alle bereits installierten Reporte überschrieben. Bitte sichern Sie Ihre benutzerdefinierten Reports vor der Installation. Nach der Installation können Sie diese wieder manuell zurück kopieren.



Einstellungen im SQL Server Konfiguration Manager

Achten Sie beim Einrichten des SQL Servers bitte darauf, dass der „Named Pipes“- und „TCP/IP“-Zugriff aktiviert wird, sonst kann die Datenbankverbindung nicht aufgebaut werden.

Die Optionen finden Sie im *SQL Server-Konfigurations-Manager* unter *SQL Native Client xx-Konfiguration (32-Bit)*, *SQL-Server Netzwerkkonfiguration (Unterverzeichnis Protokolle für „MSSQLSERVER“)* und *SQL Native Client xx-Konfiguration* jeweils in *Clientprotokolle*. xx steht für die SQL Server Version

Die Optionen für „TCP/IP“ und „Named Pipes“ müssen auf „Aktiviert“ eingestellt werden!

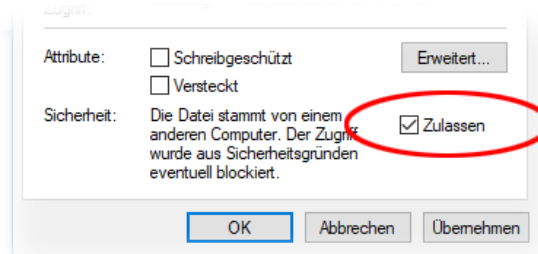
Installation starten

Gehen Sie folgendermaßen vor, um INGRADA web auf einem Server zu installieren:

Achten Sie darauf, dass Sie ausreichende Zugriffsrechte besitzen (Administrator), um die Installation durchzuführen.

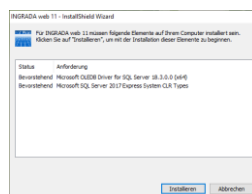
1. Laden Sie das aktuelle Installationsarchiv von www.ingrada.de herunter und speichern und entpacken Sie dieses auf einer lokalen Festplatte.

Hinweis: Aktivieren Sie in den Eigenschaften des heruntergeladenen Installationsarchivs die Checkbox *Zulassen*, bevor Sie die Zip-Datei entpacken, um mögliche Probleme mit Virenscannern während der Installation zu vermeiden!



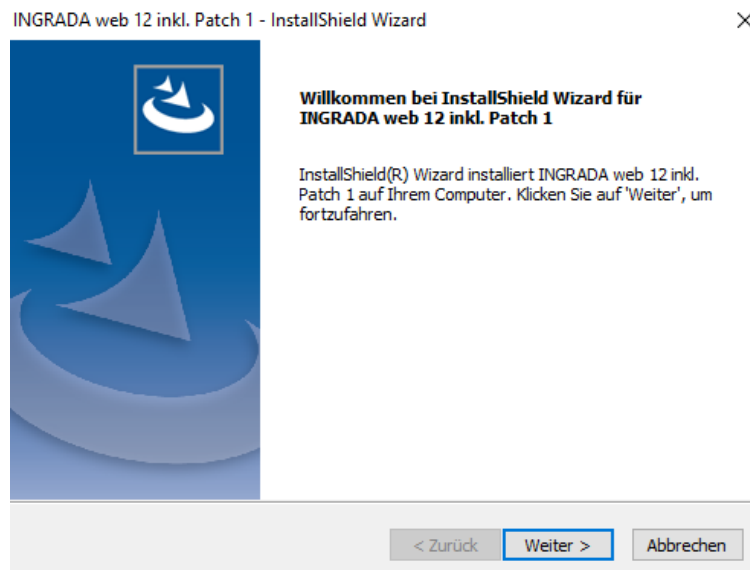
Dateieigenschaften – Reiter Allgemein: Zugriff auf entpackte Inhalte gewährleisten.

2. Starten Sie die Installation durch einen Doppelklick auf die Datei *setup.exe* im Installationsverzeichnis (unter Windows 8: Rechtsklick -> als Administrator ausführen).
3. Das System prüft, ob alle benötigten Systemkomponenten vorhanden sind und installiert diese bei Bedarf nach. Die Installation von *.NET Framework* kann einige Zeit dauern. Sind alle Komponenten vorhanden, startet die Installation direkt.

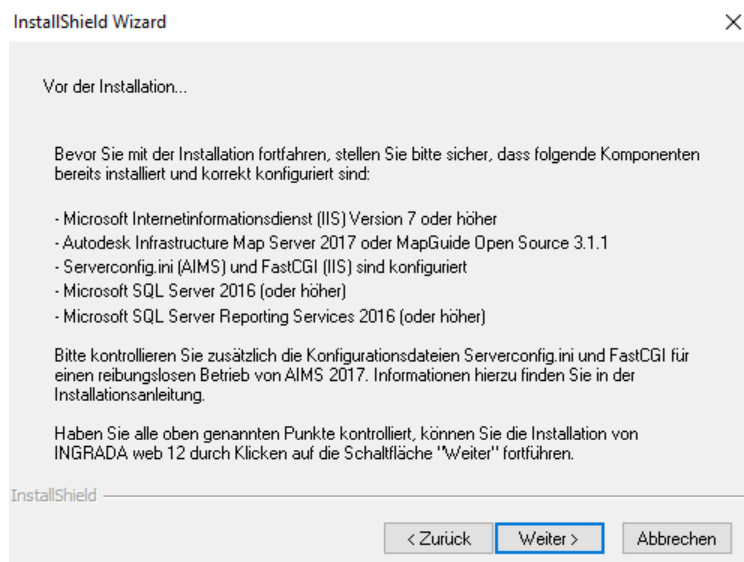


Klicken Sie auf *Installieren*.

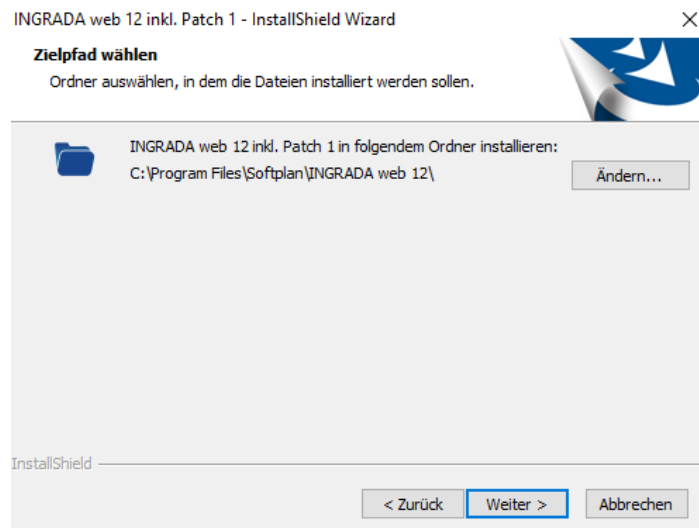
4. Daraufhin erscheint das Startfenster. Klicken Sie dort auf *Weiter >*.



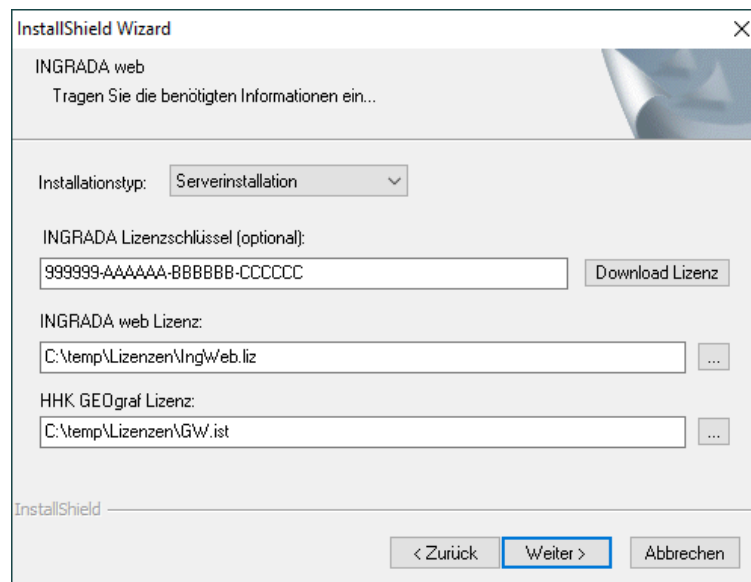
5. Danach erscheint eine Meldung mit den zu beachtenden Voraussetzungen für die Installation. Klicken Sie auf *Weiter >*, wenn die Bedingungen erfüllt sind.



6. Wählen Sie zunächst das INGRADA web Installationsverzeichnis und bestätigen Sie durch einen Klick auf *Weiter >*.



7. Wählen Sie anschließend das Verzeichnis aus, in dem Ihre Lizenzdatei abgelegt ist. Klicken Sie anschließend auf *Weiter >*.



Wählen Sie im Feld *Installationstyp*

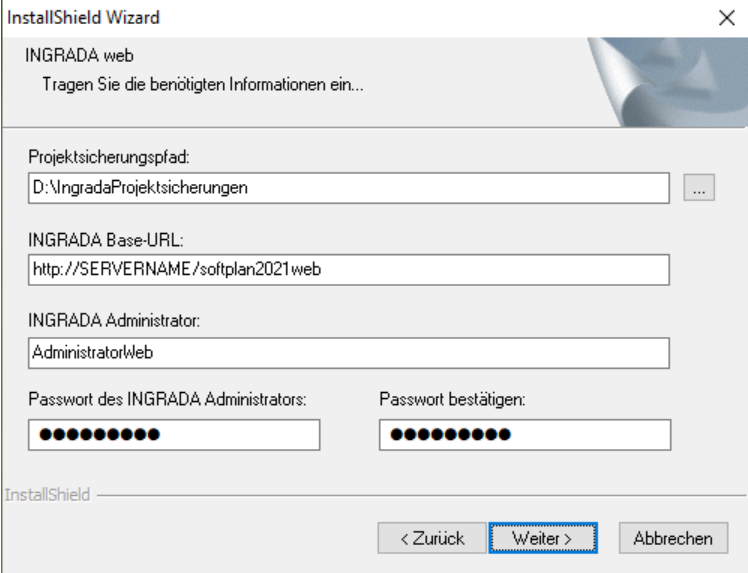
- Serverplatzinstallation: Alle IIS Anwendungspools und Anwendungen werden vorab geladen. Dadurch beschleunigt sich der erstmalige Projektaufruf.
- Einzelplatzinstallation: Anwendungspools und Anwendungen werden bei Bedarf geladen. Dadurch wird die Arbeitsspeicherbelastung verringert. Allerdings erhöht sich die Ladezeit des erstmaligen Projektaufrufs.

INGRADA Lizenzschlüssel (optional)

Mit INGRADA haben Sie die Möglichkeit, Ihre INGRADA web-Lizenz jederzeit selbstständig abzurufen und zu aktualisieren. Tragen Sie in diesem Feld Ihren personalisierten Lizenzschlüssel ein, um über die Schaltfläche *Download Lizenz* die aktuelle Lizenzdatei herunterzuladen. Die Lizenzdatei wird dabei automatisch in den Lizenzordner kopiert.

Hinweis: Der Lizenzschlüssel kann jederzeit im Projektmanager im Dialog Servereinstellungen – Lizenz eingetragen werden.

- Bestätigen bzw. tragen Sie anschließend die Pfade zur Projektsicherung und INGRADA Server ein und vergeben Sie ein Kennwort für den INGRADA Administrator:



Projektsicherungspfad: Vor einer Projektaktualisierung wird eine Sicherung erstellt, um das Projekt im Fehlerfall wiederherstellen zu können. Die Sicherungen werden unter diesem Pfad abgelegt.

INGRADA Base-URL: URL für den INGRADA Server.

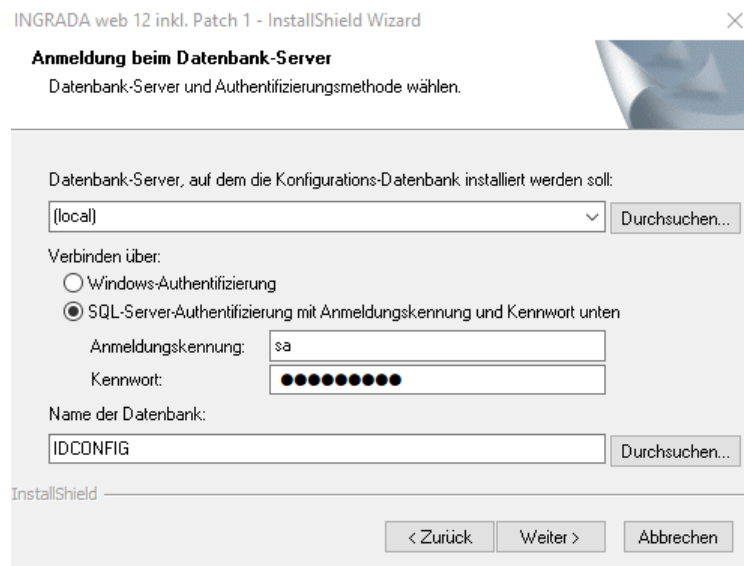
INGRADA Administrator: Tragen Sie für den Administratortnamen eine beliebige Bezeichnung ein.

Passwort: Vergeben Sie ein Administratorpasswort und bestätigen Sie dieses.

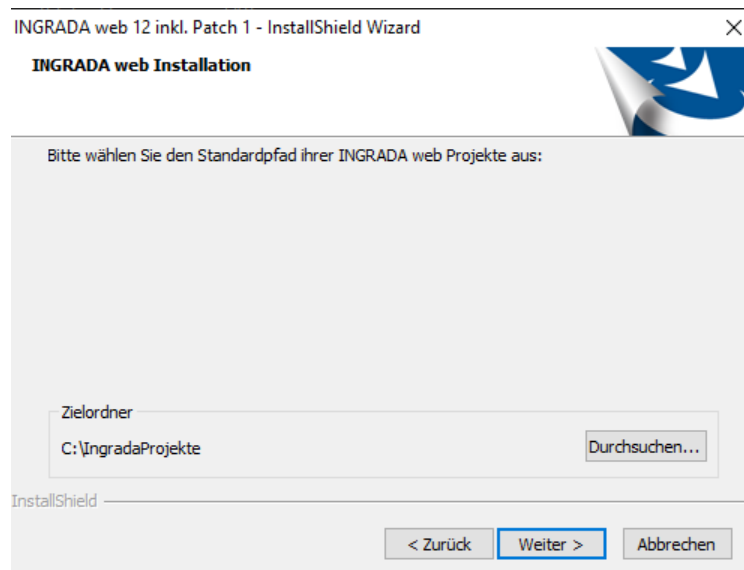
- Legen Sie im folgenden Fenster die SQL-Server Verbindungseinstellungen für die Konfigurationsdatenbank fest. **Windowsauthentifizierung ist nicht möglich.** In der Konfigurationsdatenbank (IDConfig) werden die Projekteinstellungen der INGRADA web Projekte gespeichert. Daher empfehlen wir, dass die Konfigurationsdatenbank auf dem SQL-Server mit den INGRADA web Projekten gespeichert wird. Klicken Sie danach auf *Weiter >*.

Achtung: Haben Sie zeitgleich eine zweite Installation von einer älteren INGRADA web Version auf Ihrem System, so muss der Benutzername des INGRADA Administrator abweichend von der bereits bestehenden Installation sein, oder es muss der gleiche Name mit dem gleichen Passwort verwendet werden.

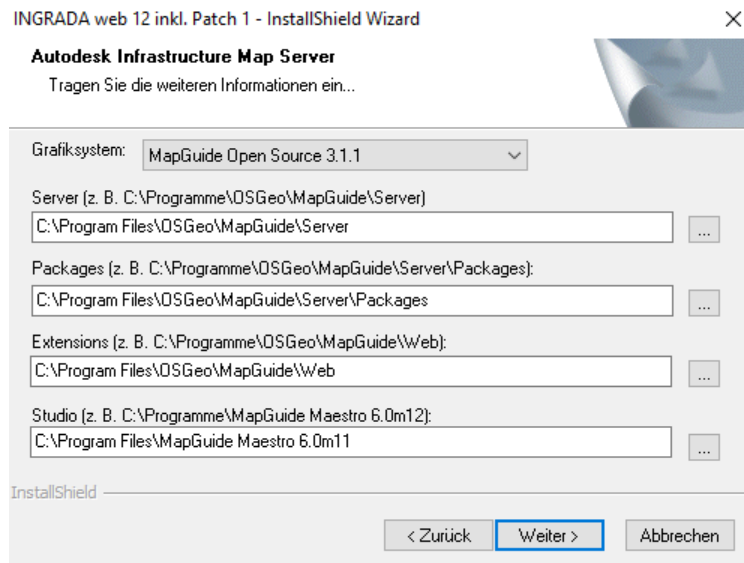
Achtung: Haben Sie mehrere INGRADA web Server im Einsatz, die sich einen SQL Server teilen, muss jeder INGRADA web Server eine eigene Konfigurationsdatenbank haben. Geben Sie für den zweiten INGRADA web Server bei der Installation von INGRADA web einfach einen Datenbanknamen unterschiedlich von *IDCONFIG* ein.



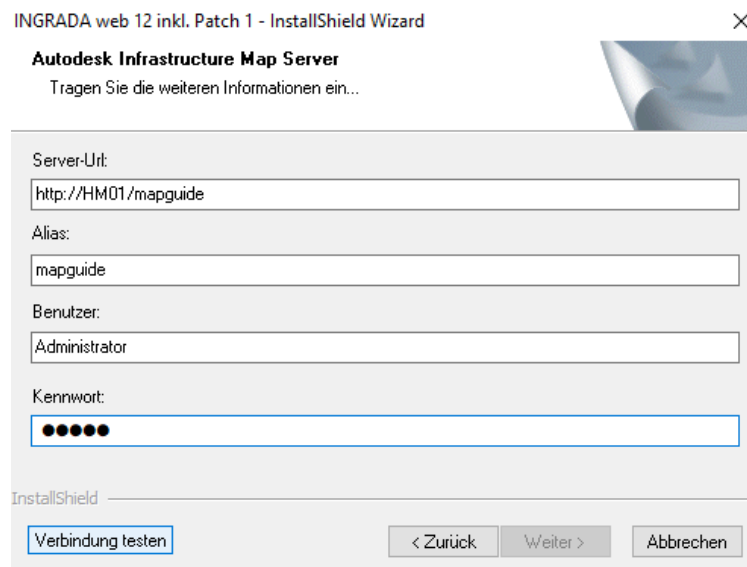
- 10.** Danach können Sie den standardmäßigen Projektpfad auswählen. Standard ist *C:\IngradaProjekte*. Klicken Sie danach auf *Weiter >*.



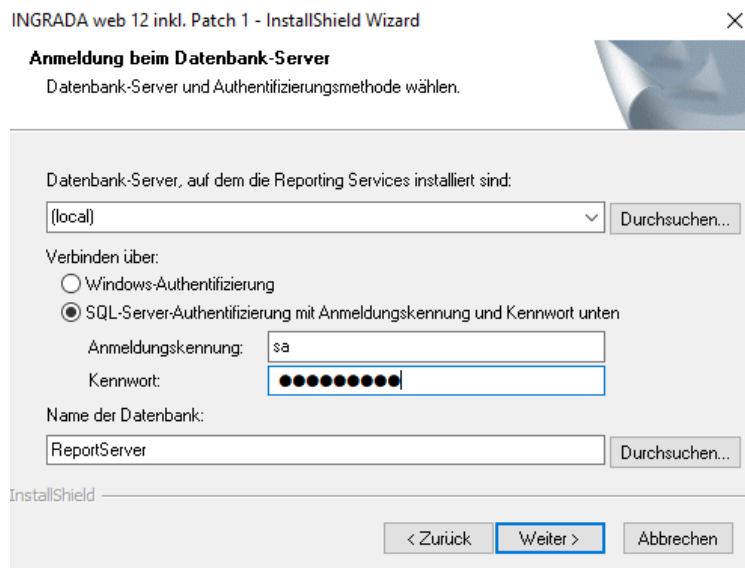
- 11.** Wählen Sie im nächsten Dialog das Grafiksystem aus. Die *Autodesk Infrastructure Map Server*-Installationspfade sollten automatisch eingetragen werden.



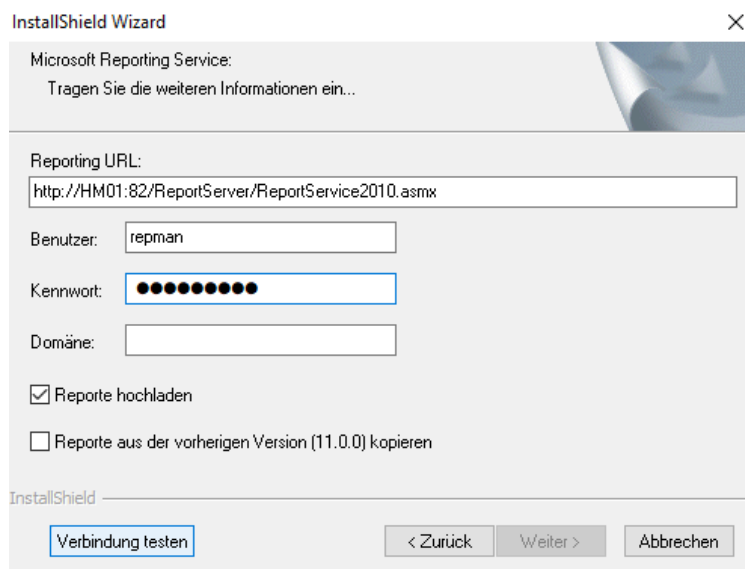
12. Überprüfen Sie die Pfade auf Vollständigkeit. Tragen Sie den *Benutzer* mit *Kennwort* ein. Der AIMS-Benutzer wird zum Upload der Karten-Templates benötigt.



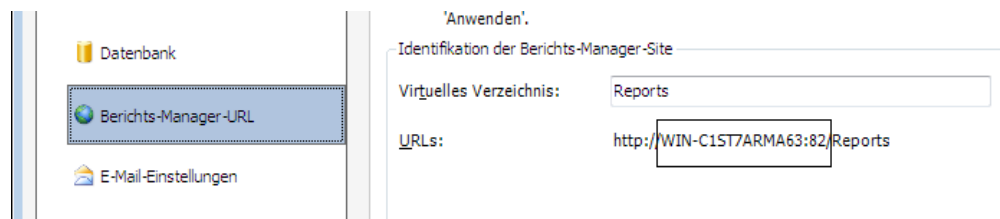
13. Testen Sie die Verbindung. Klicken Sie nach erfolgreichem Test auf *Weiter >*.
14. Geben Sie im nächsten Dialog den Datenbank-Server ein, auf dem die Reporting-Services installiert sind. Tragen Sie die Login-Informationen sowie den Namen der Report Server Datenbank ein und bestätigen Sie mit *Weiter >*.



15. Tragen Sie im folgenden Dialog die Login-Informationen für den Reporting Server ein.

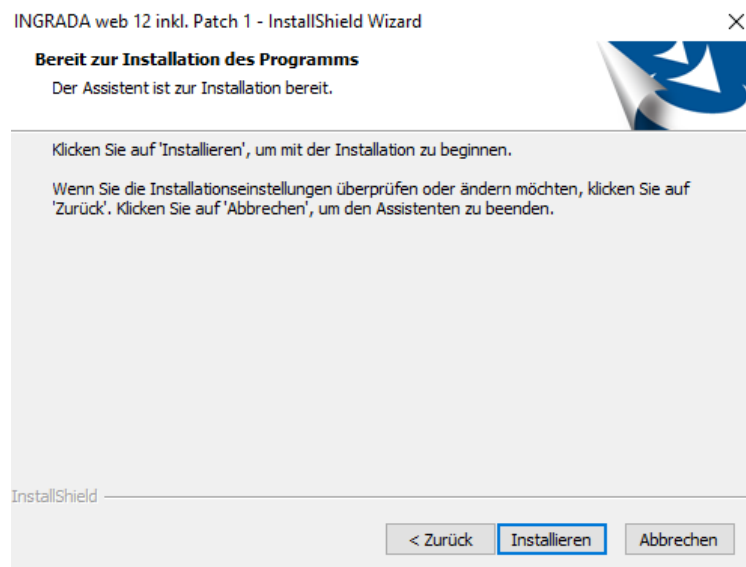


16. Passen Sie zunächst die URL an. Die Anpassungen entnehmen Sie aus der Angabe der URL im Bereich „Berichts-Manager-URL“ in der Konfigurations-Oberfläche des Reporting Services (siehe folgende Abbildung). Wenn Sie die *Express Edition* des SQL-Servers verwenden, erweitert sich die URL eventuell um den Eintrag `_SQLEXPRESS`.

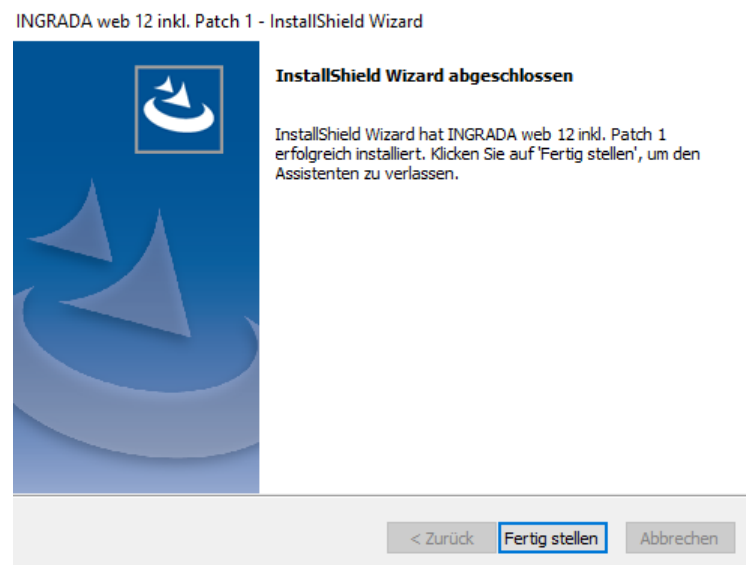


17. Klicken Sie auf „Verbindung testen“, um die Angaben zu prüfen und zu testen ob der Reporting Service Dienst gestartet ist. Klicken Sie danach auf *Weiter >*.

18. Starten Sie die Installation durch einen Klick auf *Installieren*. Alle benötigten Dateien werden auf Ihren Server kopiert.



19. Zum Abschluss der Installation erscheint eine Meldung. Klicken Sie auf *Fertig stellen*.



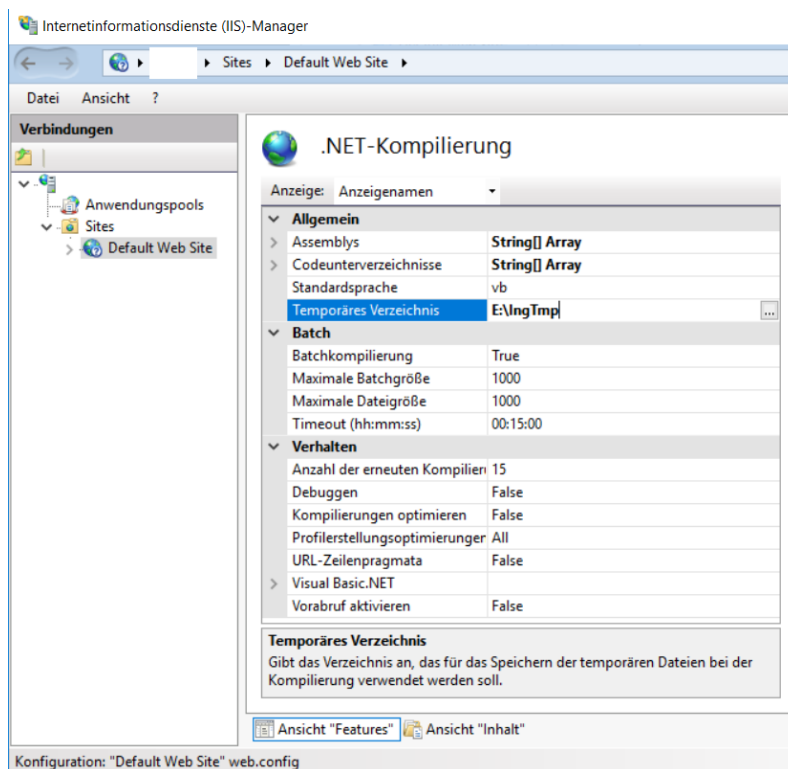
20. Nach der Installation von INGRADA web müssen noch einige Einstellungen im IIS vorgenommen werden, damit die Authentifizierung wieder möglich ist. Eine Anleitung hierzu finden Sie im nächsten Kapitel „Einrichten des Servers für INGRADA web“.

Hinweis: Bei der Erstinstallation von INGRADA web wird automatisch das GEOgraf-Installationsarchiv *setup.exe* im Ordner *Installationsordner\Programme\GEOgraf\bin91* ausgeführt, damit der ALKIS-Import und die Nutzungsartenverschneidung ausgeführt werden können!

Einrichten des Servers für INGRADA web

Temporärer Pfad für die .net-Kompilierung

Der temporäre Pfad für die .net-Kompilierung sollte explizit angegeben und kurz gewählt werden, da bei langen Projektnamen die Softplan.Ingrada.Api und das Softplan.Ingrada.Backend nicht korrekt initialisiert werden könnten. Eine sehr kurze Pfadangabe wie z. B. `E:\IngTmp` auf dem Projekt Laufwerk wird empfohlen



Temporäre Pfadangabe für die .net-Kompilierung.

Webprojekte vorabladen

Es besteht die Möglichkeit, den ersten Projektstart von Webprojekten zu beschleunigen. Die Projekte werden quasi vorab geladen. Dafür müssen die Webprojekte im IIS-Manager angepasst werden.

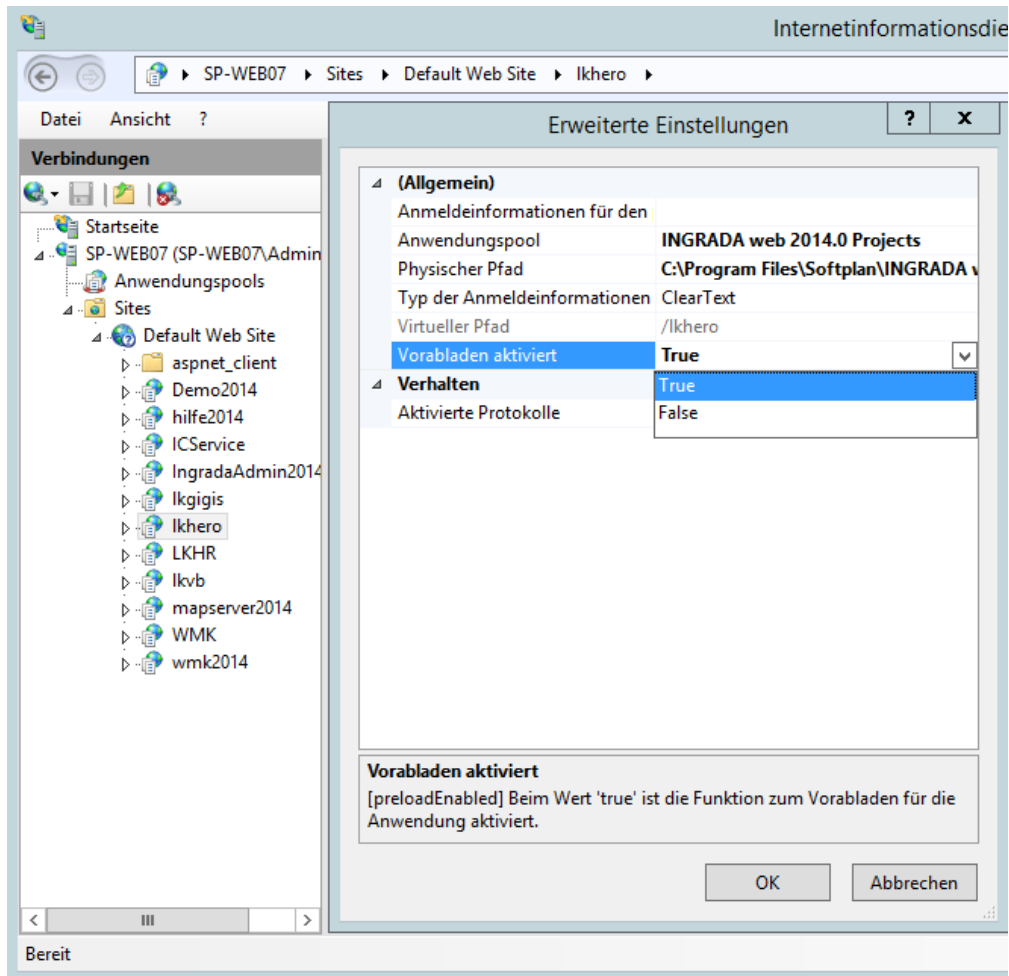
Hinweis: Das Vorabladen von Webprojekten ist nur mit dem IIS Manager ab Version 8 möglich, also mit den Betriebssystemen Windows 8 und Windows Server 2012.

Ein Vorabladen von Webprojekten ist nur für eine geringe Anzahl an Webprojekten (bis zu 3) sinnvoll.

Führen Sie folgende Änderungen in den gewünschten Webprojekten durch:

1. Öffnen Sie den IIS-Manager, wenn noch nicht geschehen.

2. Klicken Sie links im Verzeichnis der Verbindungen auf den Servernamen und öffnen Sie das Verzeichnis *Sites > Default Web Site*.
3. Führen Sie einen Rechtsklick auf das gewünschte Webprojekt aus und wählen Sie den Eintrag *Anwendung verwalten > Erweiterte Einstellungen....*
4. Setzen Sie die Option *Vorabladen aktiviert* auf *True*.
5. Speichern Sie diese Einstellungen, indem Sie auf *OK* klicken.

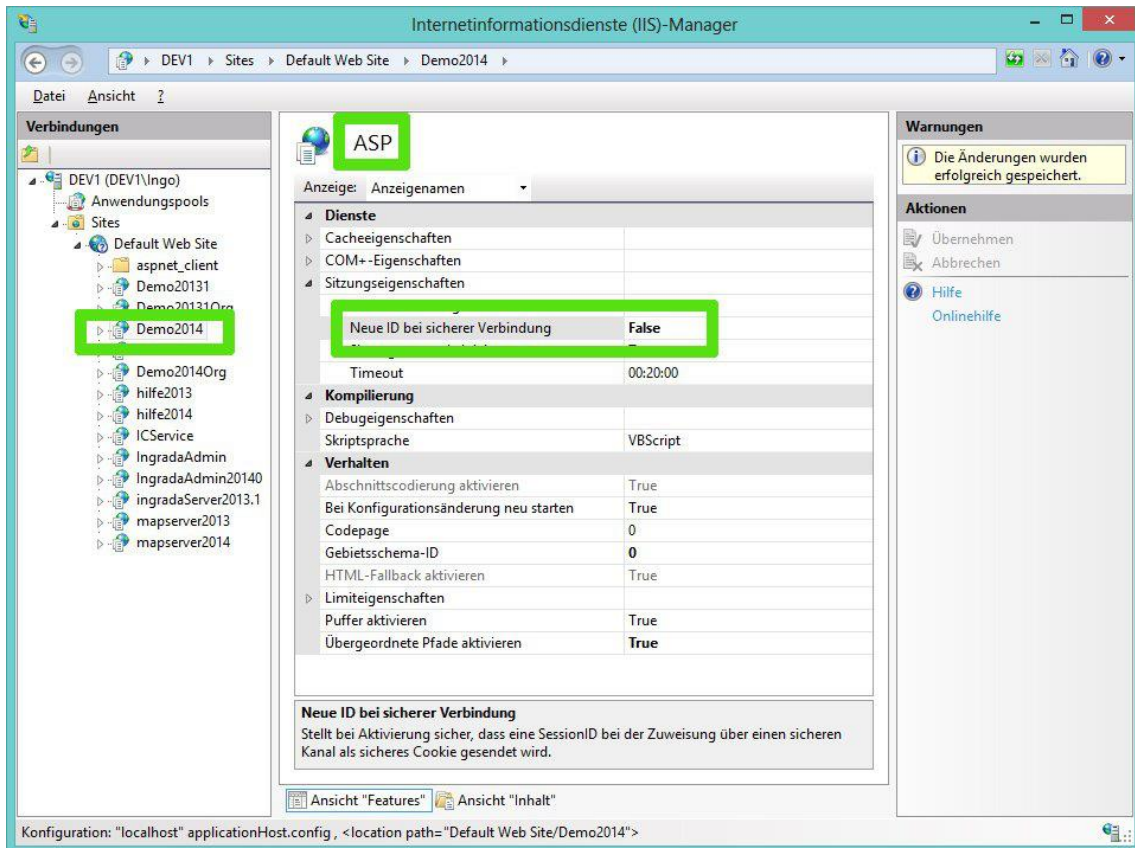


INGRADA web und HTTPS

Überprüfen Sie folgende Einstellungen, damit INGRADA web über eine HTTPS-Verbindung funktioniert. Es darf keine neue *AspSessionID* bei einer sicheren Verbindung erstellt werden. Gehen Sie folgendermaßen vor, um die entsprechende Einstellung über den IIS Manager vorzunehmen (siehe auch Abbildung unten):

1. Öffnen Sie den IIS Manager.
2. Klicken Sie auf das Projekt, für das die Einstellungen vorgenommen werden sollen. Klicken Sie auf *Default Web Site*, wenn die Einstellung für alle untergeordneten Projekte vorgenommen werden soll.

3. Wählen Sie per Klick die Einstellung *ASP* aus.
4. Öffnen Sie im Bereich *Dienste* den Eintrag „Sitzungseigenschaften“ per Klick.
5. Setzen Sie die Option „Neue ID bei sicherer Verbindung“ auf *False*.



Hinweise zur Serverkonfiguration

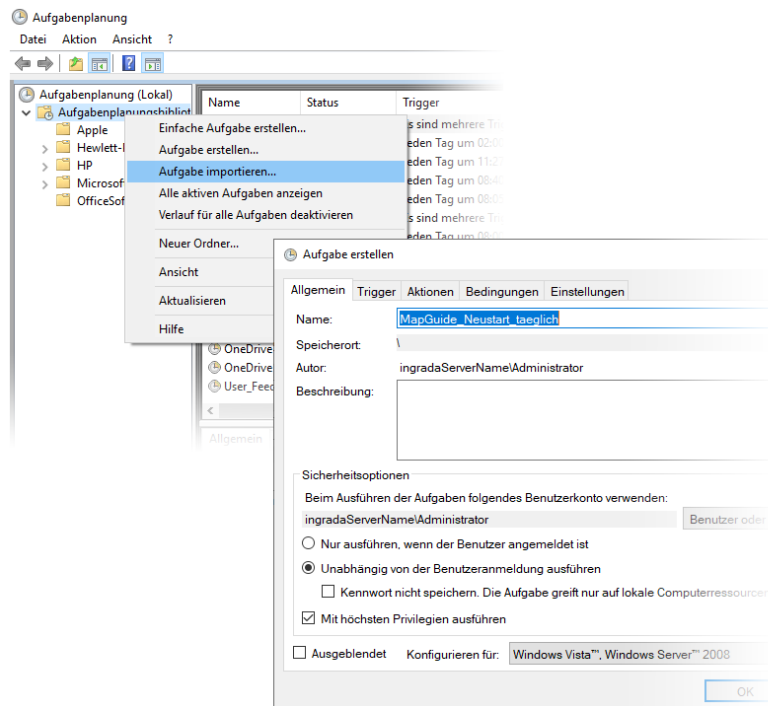
Einrichten eines nächtlichen IIS- und MapGuide-Neustarts via Taskplaner und Skript

Zur Verbesserung der Serverstabilität kann es nützlich sein, auf dem INGRADA web Server den MapGuide-Dienst und den IIS jede Nacht automatisch neu zu starten. Die erforderlichen Dateien befinden sich im Installationsverzeichnis `..\Programme\template\doku\INGRADAweb`. Das Archiv `IngradaWeb_mgrestart.zip` enthält die drei folgenden Dateien:

- `MapGuide_Neustart_taeglich.xml` (exportierte Windows-Aufgabenplanungsdatei : startet die `mgrestart.cmd`)
- `mgrestart_MapGuideServer31.zip` (Batch-Datei `mgrestart.cmd`: startet den Dienst `MapGuideServer3.1` neu)
- `mgrestart_AIMS2017.zip` (Batch-Datei `mgrestart.cmd`: startet den Dienst `InfrastructureMapServer2017` neu)

Einrichtung

1. Öffnen Sie `MapGuide_Neustart_taeglich.xml` mit einem Editor (Notepad++ oder Windows-Editor)
2. Passen Sie den Servernamen, das Verzeichnis, in dem die `mgrestart.cmd` liegt und das administrative Konto, unter dem die Aufgabe ausgeführt werden soll, an:
 - Name des INGRADA web Servers (hier: `ingradaServerName`)
 - `WorkingDirectory` (hier: `C:\temp\`)
 - `UserId` (hier: `ingradaServerName\Administrator`)
3. Entpacken Sie die ihrem Grafiksystem entsprechende `mgrestart.cmd` (AIMS2017 oder `MapGuide OpenSource 3.1`) und kopieren Sie sie nach `C:\temp`
4. Starten Sie die Windows-Aufgabenplanung
 - markieren Sie links die Aufgabenplanungsbibliothek mit der rechten Maustaste und wählen Sie "importieren"
 - geben Sie hier die zuvor angepasste Datei `MapGuide_Neustart_taeglich.xml` an
5. Beim Verlassen der Aufgabe wird das Kennwort des administrativen Kontos abgefragt. Die Aufgabe ist jetzt angelegt und wird jede Nacht um 0.17 Uhr ausgeführt.



Einrichten eines nächtlichen IIS- und MapGuide-Neustarts via Taskplaner.

WMS-Dienste für MapGuide konfigurieren

Folgende Einstellungen sind vorzunehmen, wenn Ihr INGRADA web-Server nur über einen Proxy-Server mit dem Internet kommunizieren kann. Der Server muss ohne Passwortabfrage ins Internet kommen können.

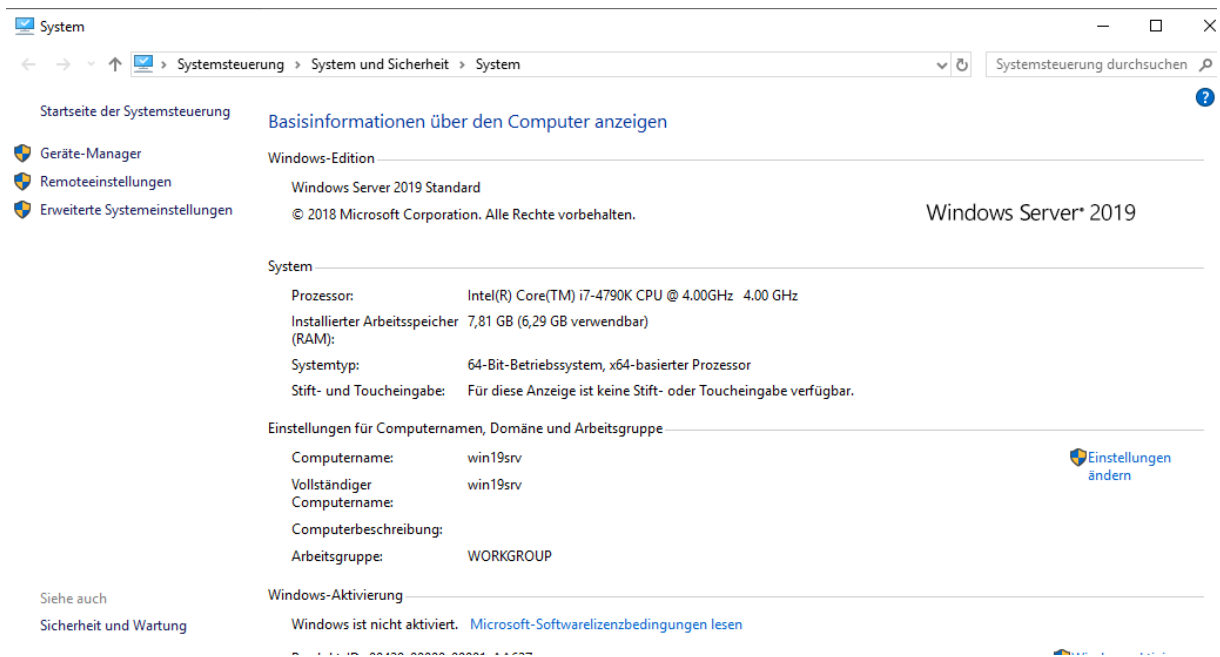
Um WMS-Services in INGRADA web nutzen zu können, sind folgenden Einstellungen vorzunehmen:

- In den Systemvariablen müssen die Variablen *all_proxy* und *NO_PROXY* gesetzt werden.

Zu den Umgebungsvariablen gelangen sie wie folgt:



Öffnen sie das Einstellungsmenü „System“ und klicken sie auf Systeminfo.



The screenshot shows the Windows System Control Panel window. The title bar reads "System". The breadcrumb navigation is "Systemsteuerung > System und Sicherheit > System". The main heading is "Basisinformationen über den Computer anzeigen".

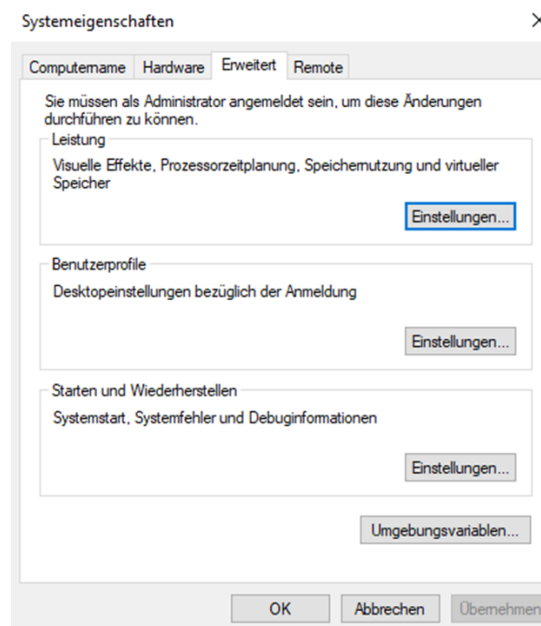
On the left sidebar, there are links for "Geräte-Manager", "Remoteeinstellungen", and "Erweiterte Systemeinstellungen".

The main content area is divided into sections:

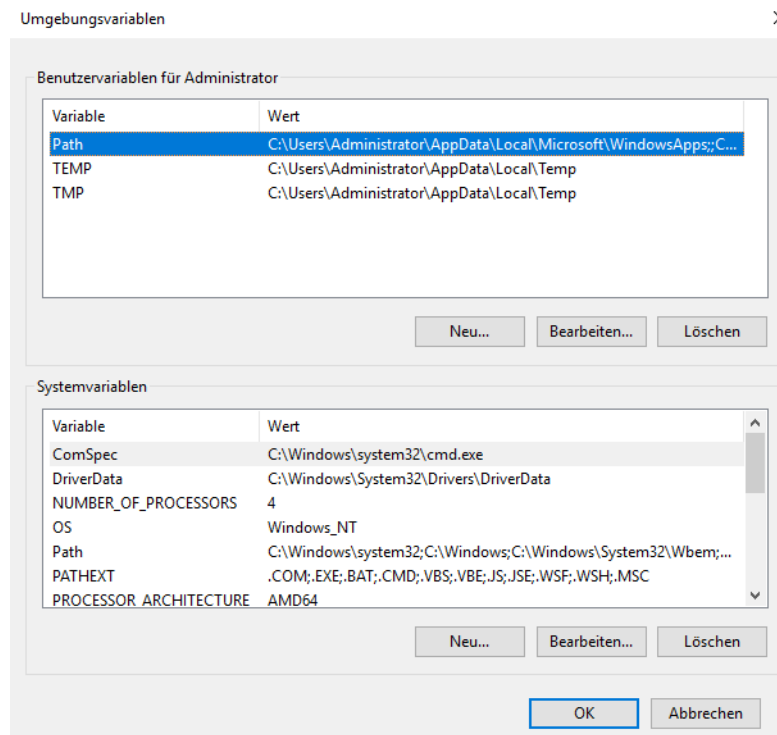
- Windows-Edition:** Windows Server 2019 Standard, © 2018 Microsoft Corporation. Alle Rechte vorbehalten. Windows Server* 2019
- System:** Prozessor: Intel(R) Core(TM) i7-4790K CPU @ 4.00GHz 4.00 GHz; Installierter Arbeitsspeicher (RAM): 7,81 GB (6,29 GB verwendbar); Systemtyp: 64-Bit-Betriebssystem, x64-basierter Prozessor; Stift- und Toucheingabe: Für diese Anzeige ist keine Stift- oder Toucheingabe verfügbar.
- Einstellungen für Computernamen, Domäne und Arbeitsgruppe:** Computername: win19srv; Vollständiger Computername: win19srv; Computerbeschreibung: ; Arbeitsgruppe: WORKGROUP. A link "Einstellungen ändern" is visible.
- Windows-Aktivierung:** Windows ist nicht aktiviert. [Microsoft-Softwarelizenzbedingungen lesen](#)

At the bottom left, there is a link "Sicherheits- und Wartung".

In diesem Fenster öffnen sie „Erweiterte Systemeinstellungen“.



Klicken sie auf den Button „Umgebungsvariablen“.



Klicken Sie im Bereich Systemvariablen auf „Neu“.

Geben Sie beim Namen der Variablen all_proxy ein

Beim Wert der Variablen geben Sie folgendes ein:

http://IPAdresse:PortNummer ODER IPAdresse:PortNummer

Geben Sie beim Namen der Variablen NO_PROXY ein

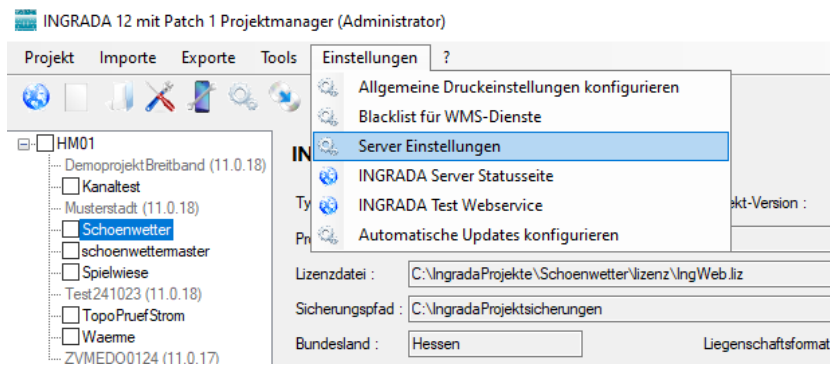
Beim Wert der Variablen geben Sie folgendes ein:

localhost,127.0.0.1

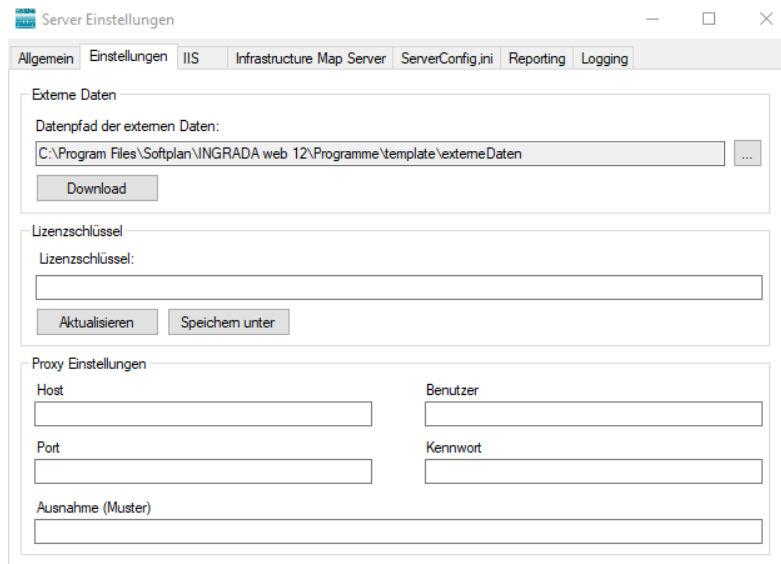
Bestätigen Sie die Eingaben mit OK und starten sie den Server neu. Nun sollte der Kartenserver in der Lage sein, WMS Dienste zu empfangen.

Konfiguration der Proxy-Einstellungen im INGRADA web Projektmanager

Damit auch INGRADA web WMS-Dienste abrufen kann, muss im Projektmager unter Servereinstellungen der Proxy-Server angegeben werden.



Öffnen sie den Projektmanager. Im Menü *Einstellungen* öffnen sie den Eintrag *Server Einstellungen*. Im Reiter *Einstellungen* geben sie die Proxy-Einstellungen an:



Das Muster für eine Proxyausnahme sieht wie folgt aus:

`(?i).*localhost.*|.*127.0.0.1.*`

Ausnahmen müssen im regex-Format formuliert werden. `(?i)` bedeutet *nicht Case-Sensitiv* und muss am Anfang der Zeile stehen. `|` ist das Zeichen für eine Oder-Verknüpfung. Unter der URL <https://regex101.com>

Können Sie prüfen, ob Ihre Einträge korrekt sind.

Browsereinstellungen für INGRADA web

Einstellungen in Firefox

Firefox kann so eingestellt werden, dass er den angemeldeten Domain-Benutzer an die Website übergibt. Dafür muss in der Adresszeile des Firefox „about:config“ eingegeben werden. Diesem

Vorgehen folgt eine Warnung, in der man auf mögliche Risiken hingewiesen wird. Zusätzlich müssen zwei Parameter angepasst werden:

- network.negotiate-auth.delegation-uris
- network.negotiate-auth.trustes-uris

Durch einen Doppelklick auf den jeweiligen Parameter öffnet sich das Eingabefenster. Hier muss die URL des Webservers eingetragen werden (Der Servername, ohne „http“ davor). Mehrere Webserver können, durch Kommas getrennt, eingetragen werden. Der Eintrag sollte bei beiden Parametern identisch sein.

Drucken von Berichten

Für das Drucken im Browser aus INGRADA web heraus ist es notwendig, die Seiteneinrichtung im verwendeten Browser anzupassen. Dabei müssen alle Informationen für den Kopf- und Fußbereich ausgeschaltet werden. Bei den Randeinstellungen darf kein zusätzlicher Rand angegeben werden, da sonst der Maßstab auf dem Ausdruck verfälscht wird.

Deinstallation von INGRADA web

INGRADA web kann parallel zu älteren Versionen 2014.x installiert werden. Eine Deinstallation ist daher nicht erforderlich. Wenn Sie INGRADA web deinstallieren möchten, beachten Sie bitte folgende Hinweise:

Achtung: Sichern Sie vor der Deinstallation von INGRADA web 2012 oder 2013 den Registry-Schlüssel "softplan" in HKEY_Local_Machine\Software (Exportieren über Regedit). Sollten Sie beim Starten der INGRADA web Version 10 eine Fehlermeldung erhalten, importieren Sie bitte den Schlüssel "softplan" zurück (Importieren über Regedit).

Achtung: Klicken Sie nicht auf *Reparieren* oder *Ändern!*

INGRADA web vollständig deinstallieren

Möchten Sie INGRADA web vollständig von Ihrem Rechner entfernen, deinstallieren Sie das Programm über Start → Systemsteuerung → Programme. Projekte, Projekteinstellungen, Karten und Lizenzdateien werden bei der Deinstallation nicht gelöscht.

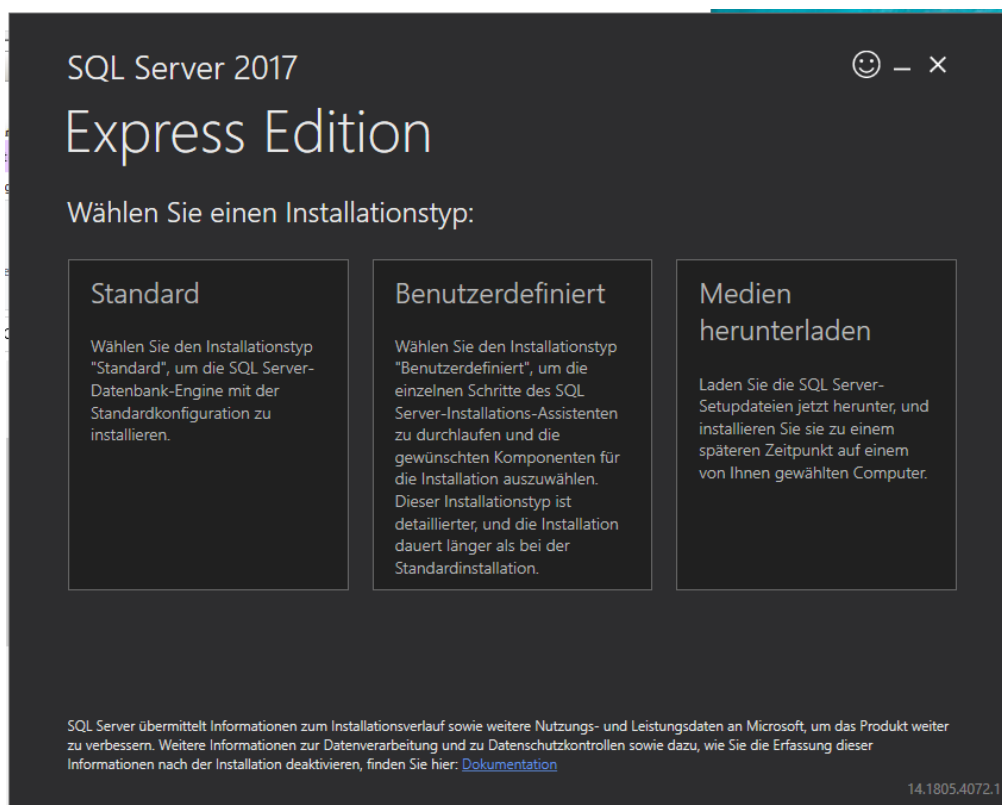
Starten Sie Ihren Rechner neu, falls Sie nach der Deinstallation dazu aufgefordert werden.

Anhang 1: SQL Server 2017 Express Installation

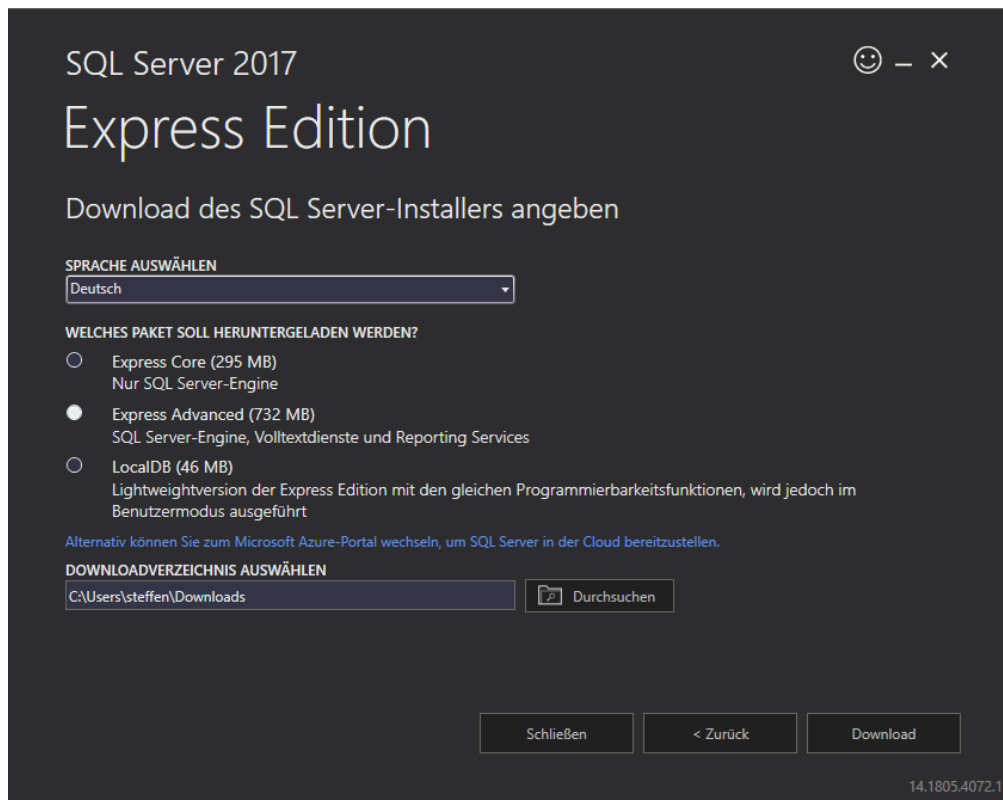
Der Windows Server 2017 Express wird als Online Installer angeboten. Die Version heißt SQLServer2017-SSEI-Expr. Hierüber downloaden Sie dann den gewohnten Installer.

Gehen Sie folgendermaßen vor, um den SQL Server 2017 zu installieren:

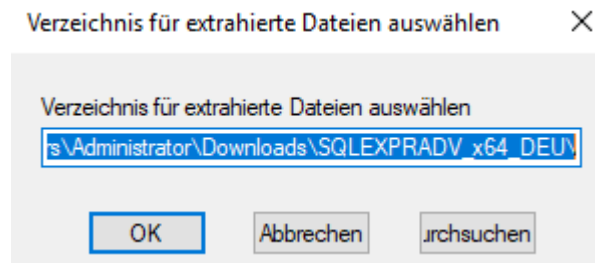
1. Starten Sie die Datei „SQLServer2017-SSEI-Expr.exe“.
2. Klicken Sie auf *Medien herunterladen*, um diesen Installationstypen auszuwählen.



3. Klicken Sie auf *Express Advanced*, um diese Version des Pakets zu downloaden. Prüfen Sie danach das Zielverzeichnis und klicken Sie anschließend auf *Download*.



4. Öffnen Sie nach dem erfolgreichen Download den Speicherort, an dem Sie das Paket gespeichert haben. Öffnen Sie dort das Setup „SQLEXPADV_x64_DEU.exe“.

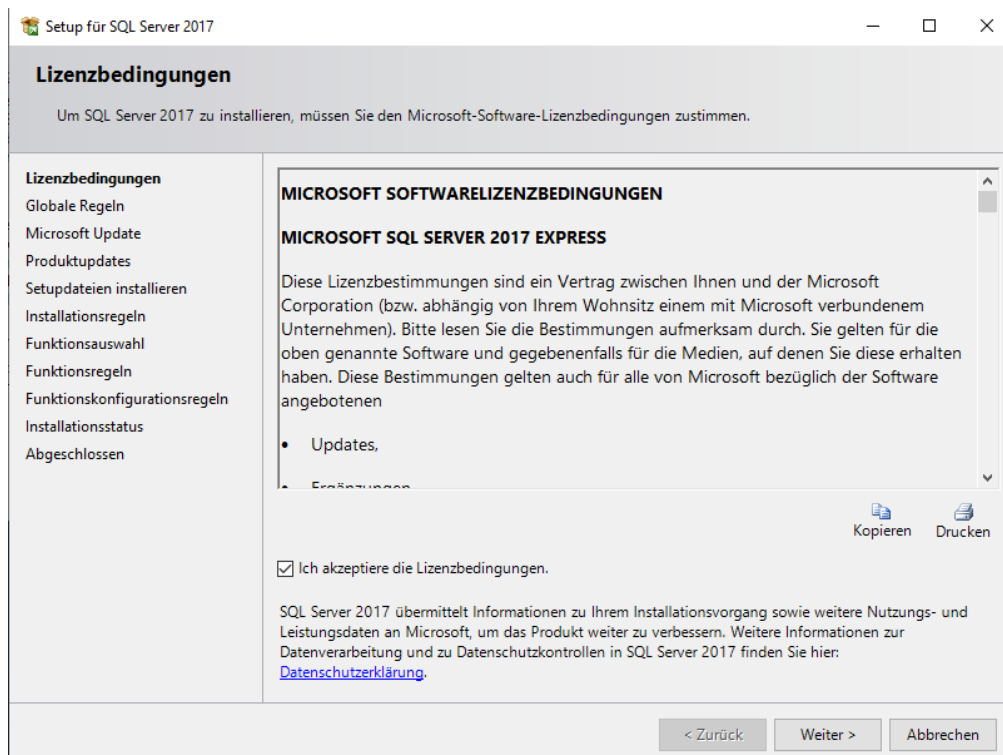


Hinweis: Das Setup sollte eine Größe von ca. 750 MB haben.

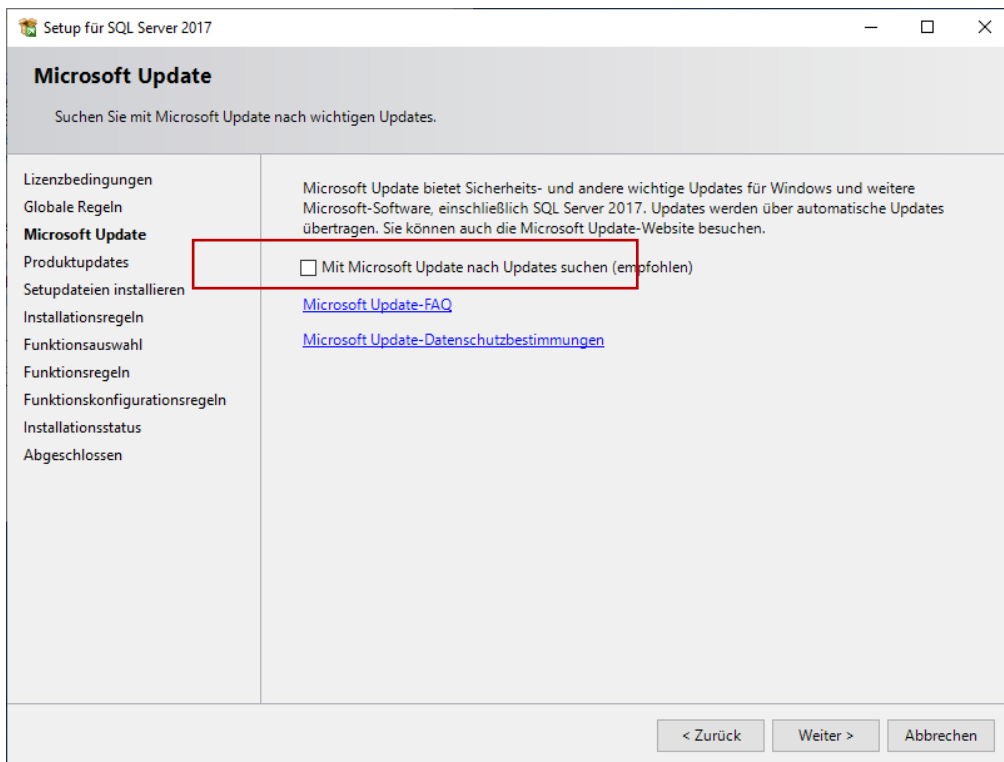
5. Klicken Sie auf *OK*, wenn Sie die Installationsdateien in das ausgewählte Zielverzeichnis entpacken möchten. Klicken Sie auf *Durchsuchen*, wenn Sie die Dateien in einen anderen Pfad entpacken möchten. Nach erfolgreicher Installation können die Installationsdateien ggf. wieder gelöscht werden.
6. Die Installation startet nach dem Entpacken automatisch. Klicken Sie auf „Neue eigenständige SQL Server-Installation oder Hinzufügen von Funktionen zu einer vorhandenen Installation“, um einen neuen eigenständigen SQL Server zu installieren.



7. Akzeptieren Sie die Lizenzbedingungen und klicken Sie auf *Weiter*.

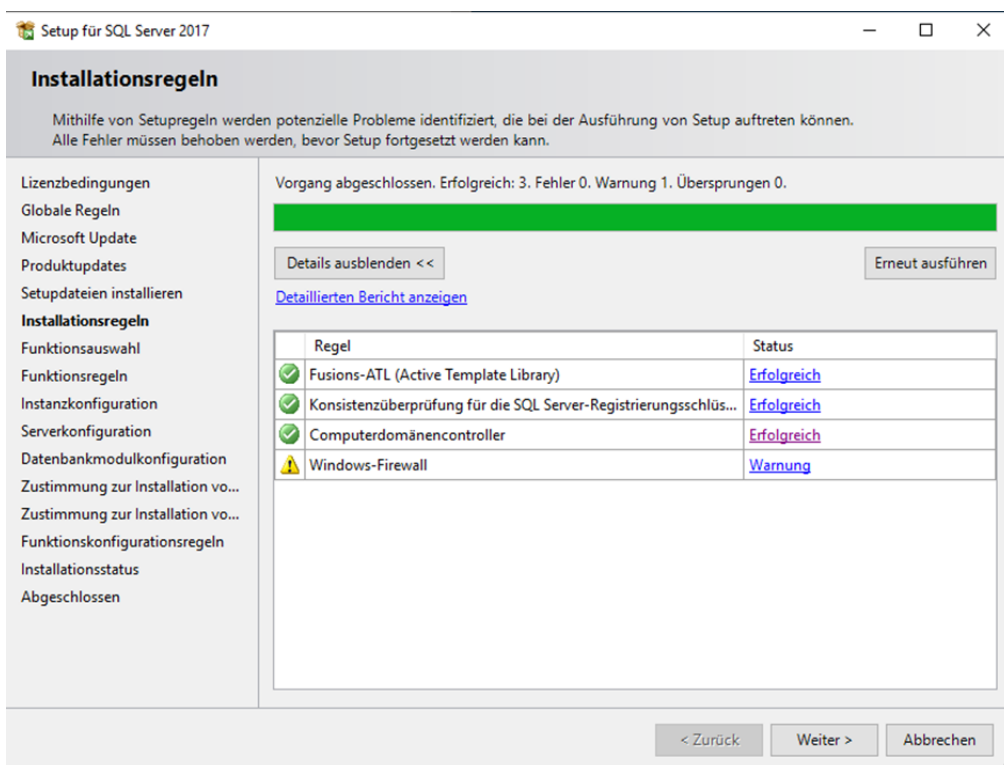


8. Verfügt der Server über eine Internetverbindung, so können Sie nach Updates suchen lassen. Das ist aber nicht zwingend notwendig. Dies kann je nach Geschwindigkeit der Leitung einige Zeit in Anspruch nehmen. Klicken Sie anschließend auf *Weiter*.

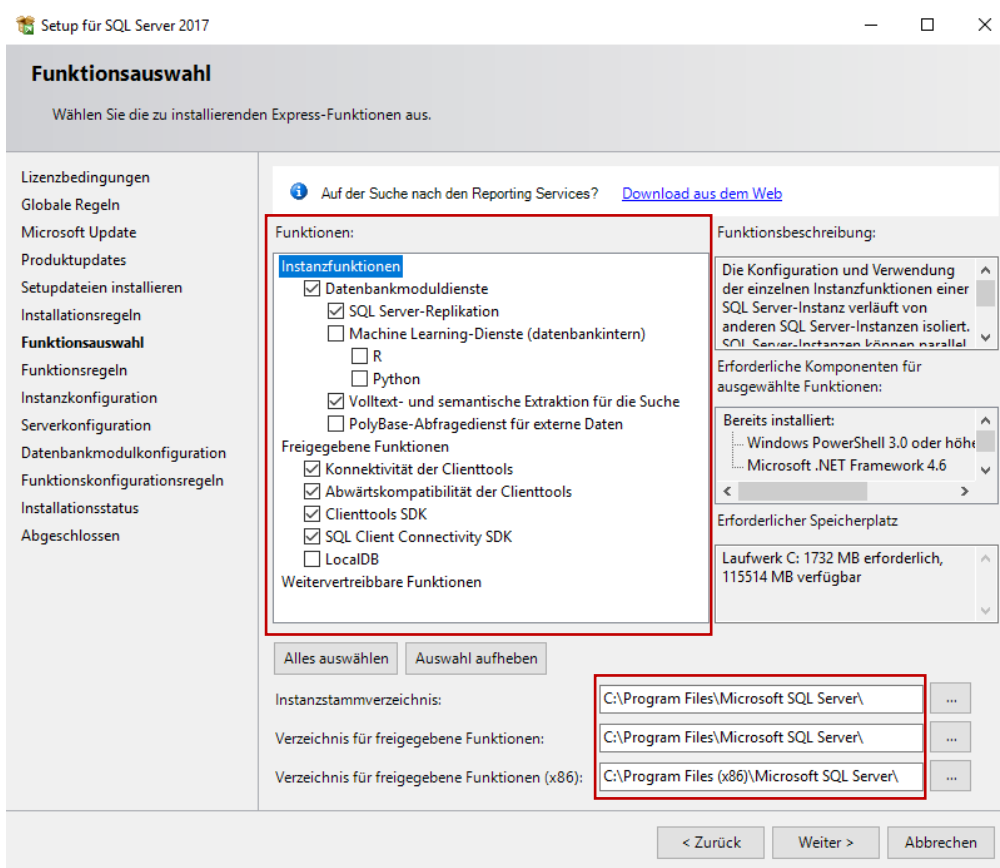


9. Es erfolgt eine Installationsprüfung des Setups, in der potenzielle Probleme identifiziert werden können. Bei erfolgreicher Prüfung klicken Sie auf *Weiter*. Wenn die Prüfung nicht erfolgreich war, wird der jeweilige Fehler rot gekennzeichnet.

Achtung: Beheben Sie diesen Fehler. Der Server, auf dem Sie den SQL Server installieren möchten, darf kein Domänencontroller sein.



10. Bitte wählen Sie die Funktionen wie abgebildet und behalten Sie die Pfade für die Installation bei. Klicken Sie anschließend auf *Weiter*.



11. In dem Fenster „Instanzkonfiguration“ werden Instanzen festgelegt. Eine Instanz ermöglicht, mehrere unabhängige SQL Server auf einer Maschine zu betreiben.

Folgende Instanz-Szenarien sind möglich:

1. Paralleler Betrieb

Hier werden mehrere SQL Server-Versionen, z.B. SQL Server 2014, 2017 und/oder 2019, betrieben. Dies ist nötig, wenn ein Austausch mit Partnern erfolgen muss. Die SQL-Version ist mit dem Partner abzustimmen, da die Versionen nicht abwärtskompatibel sind. In diesem Fall ist es ratsam, die Version im Instanz-Namen aufzuführen, z.B. SQLEXPRESS2017.

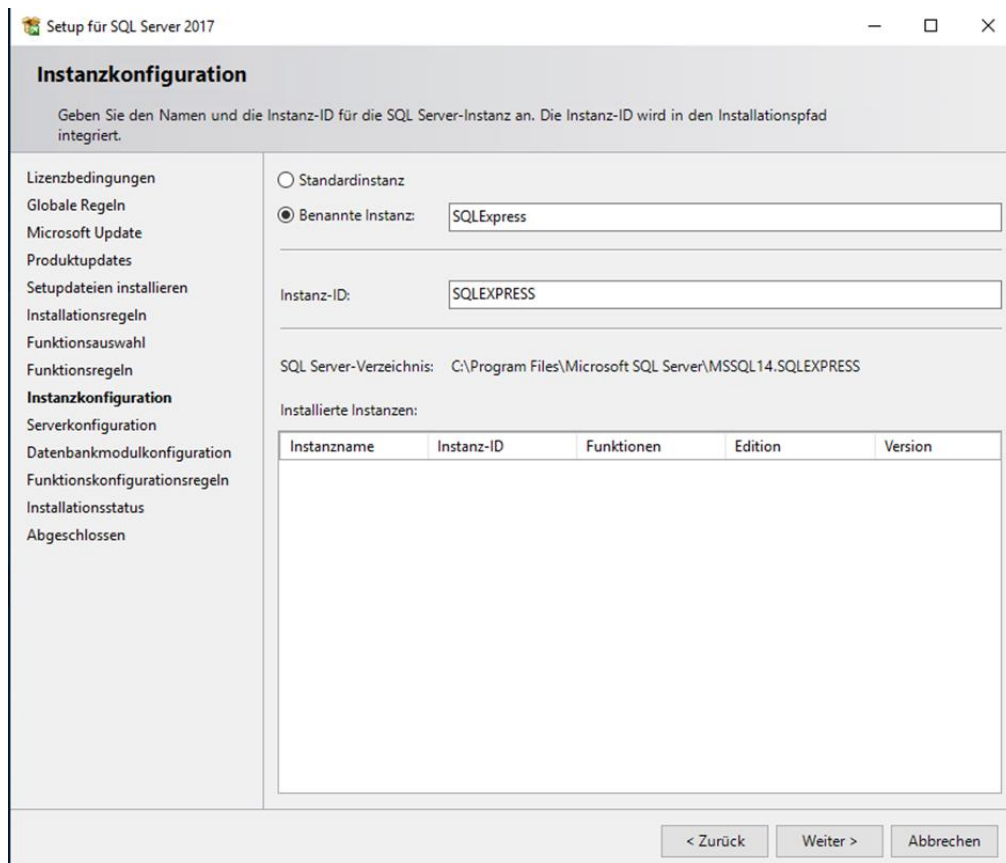
2. Getrennter Betrieb

Hier werden INGRADA Desktop und INGRADA web getrennt betrieben. Zur besseren Trennung der Projekte empfiehlt es sich, 2 SQL-Instanzen für INGRADA Desktop und INGRADA web anzulegen. Dazu starten Sie das Setup im Anschluss einfach erneut. In diesem Fall ist es ratsam, der ersten Instanz den Namen INGRADAdesktop und beim zweiten Setup den Instanz-Namen INGRADAweb zu vergeben.

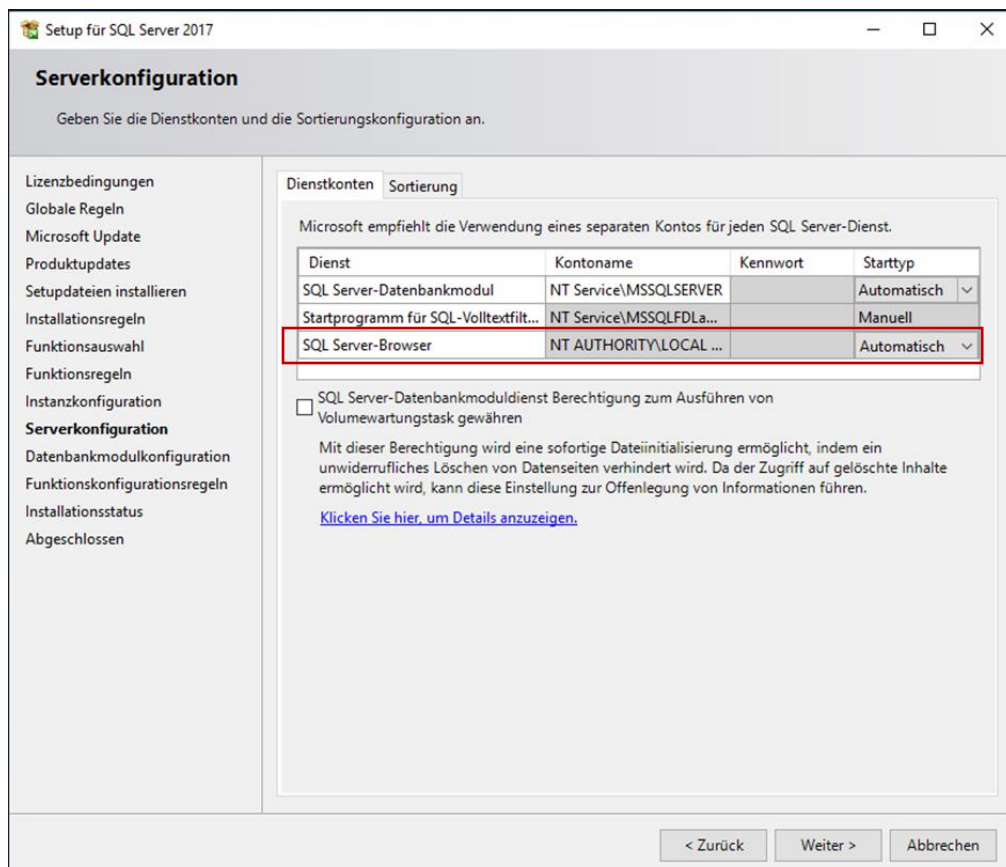
3. Einzelbetrieb

Hier wird nur ein einzelner SQL Server installiert. In diesem Fall können Sie die Auswahl so übernehmen oder eine Standardinstanz anwählen. Auch hier ist das Nachinstallieren weiterer Instanzen möglich.

Wenn Sie eine Auswahl getroffen haben, klicken Sie auf *Weiter*.

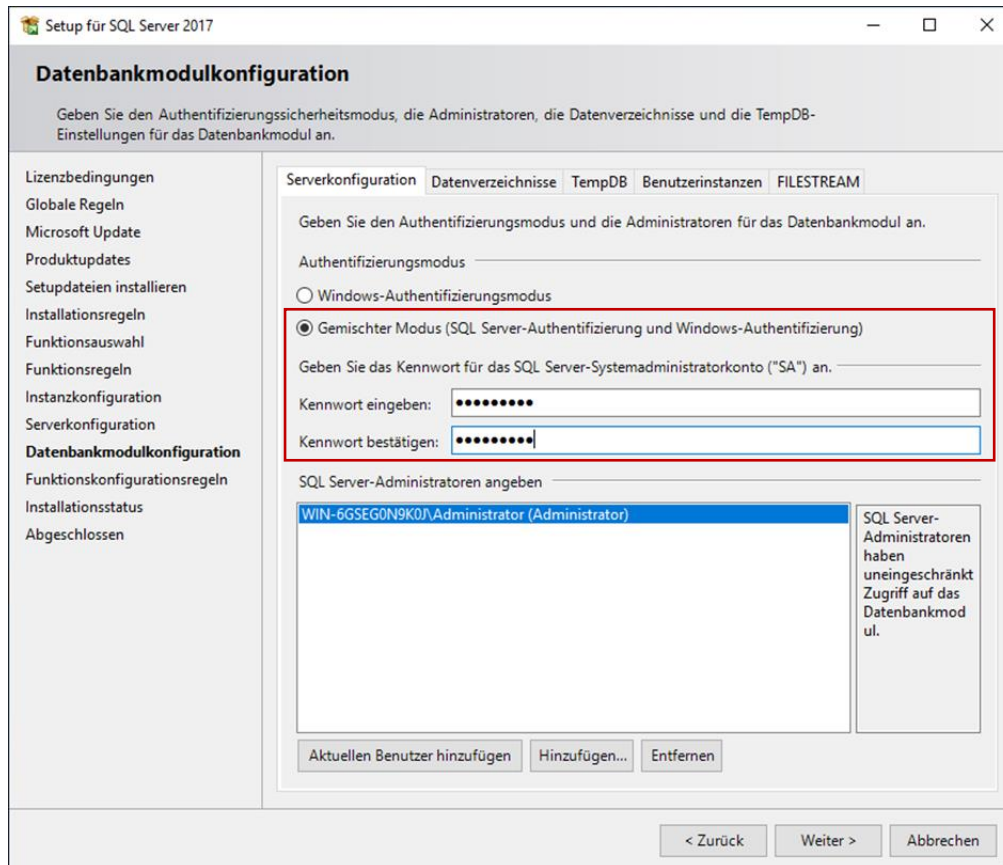


12. Stellen Sie den SQL Server-Browser auf „Automatisch“. Klicken Sie anschließend auf *Weiter*.



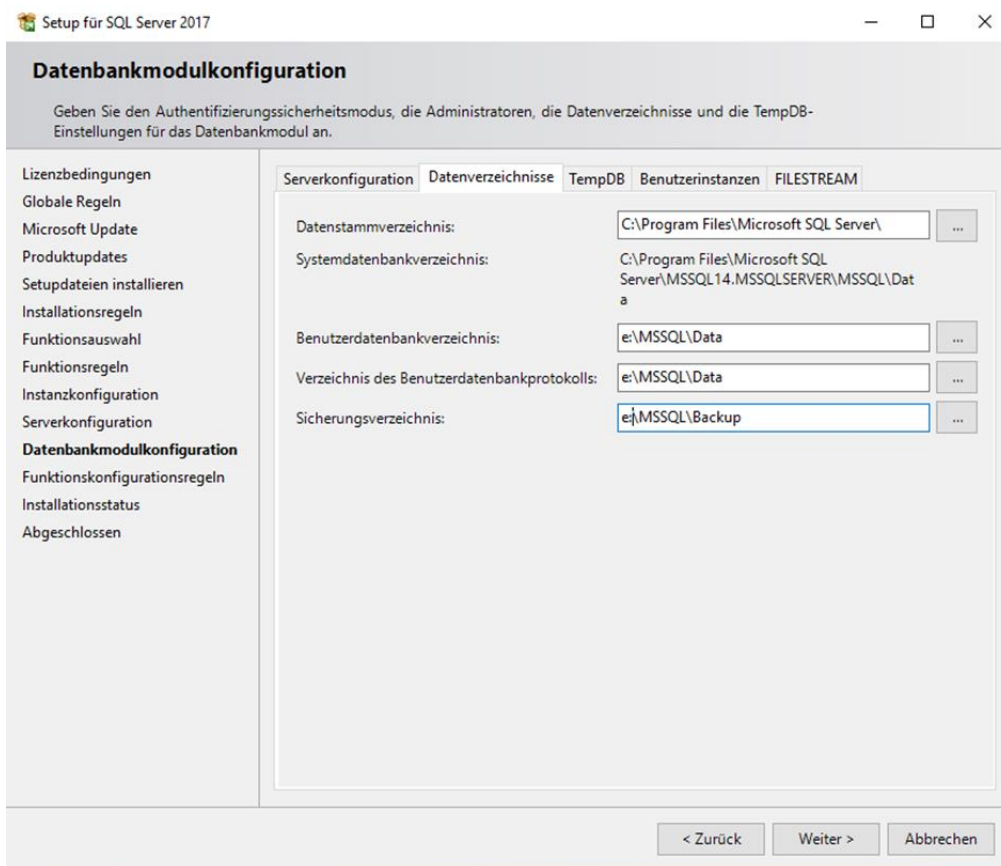
13. Wählen Sie in diesem Fenster für den Authentifizierungsmodus „Gemischter Modus“ und vergeben Sie ein Passwort für den Benutzer „sa“. Wechseln Sie danach auf den Reiter „Datenverzeichnisse“.

Achtung: INGRADA Desktop und INGRADA web können nicht mit dem „Windows-Authentifizierungsmodus“ des SQL Servers betrieben werden!

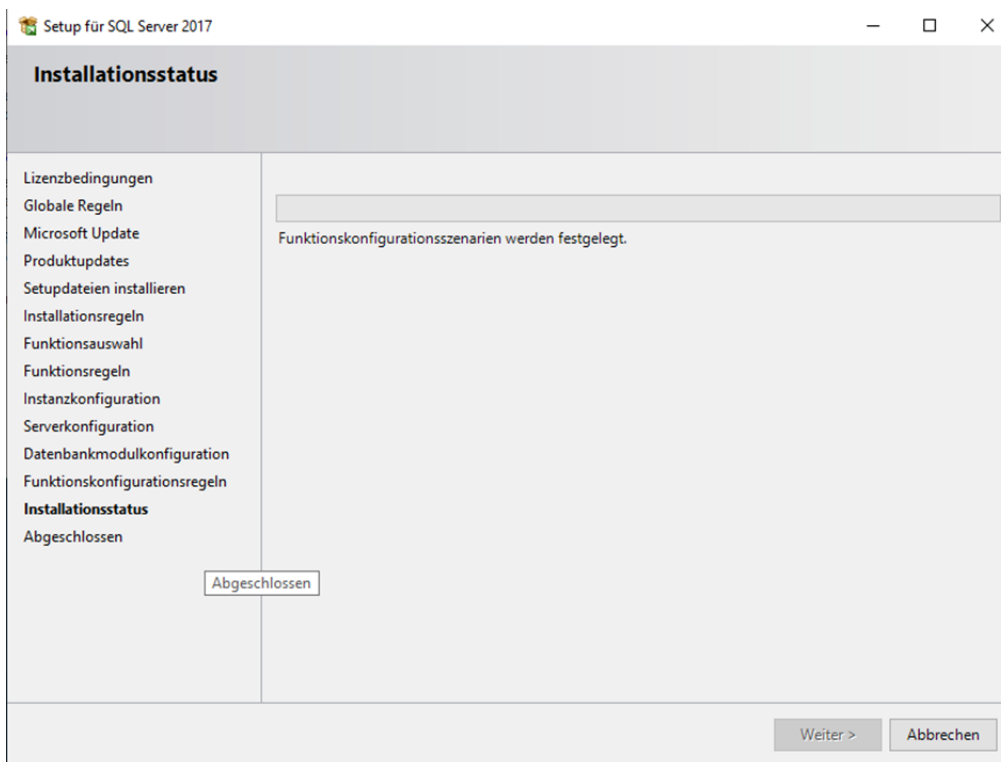


14. Auf dem Reiter „Datenverzeichnisse“ wählen Sie das Laufwerk mit dem größten Speicherplatz für die Datenbanken. Klicken Sie dann auf *Weiter*.

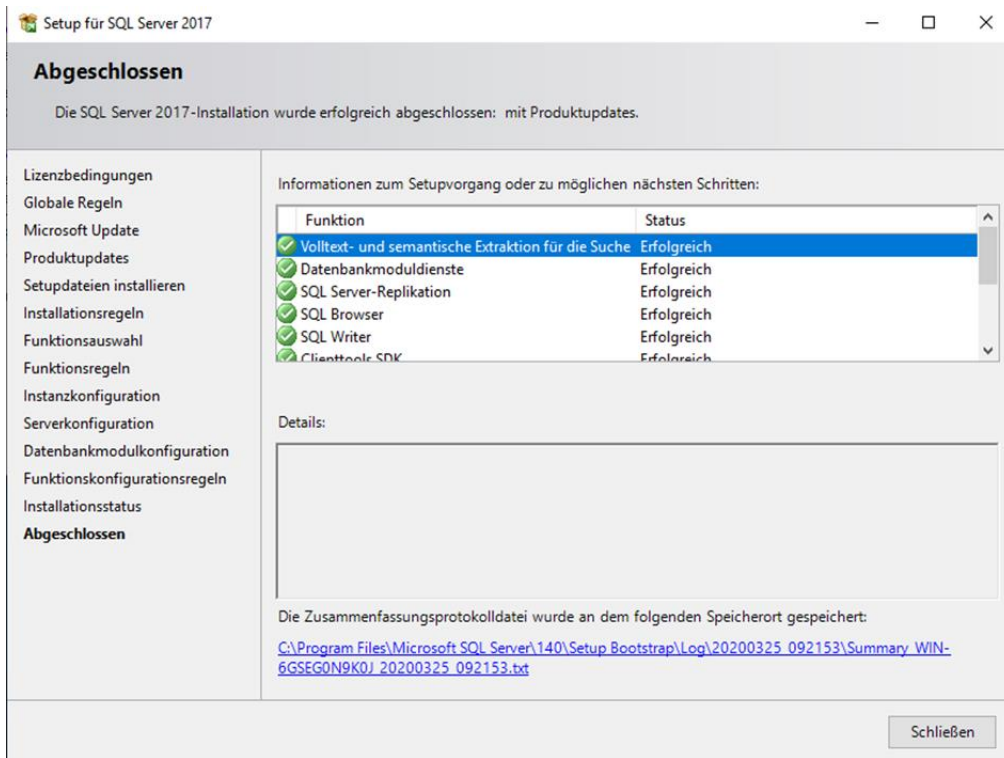
Hinweis: Wenn Sie mehrere Instanzen betreiben, sollten auch die Speicherorte unterschiedlich sein.



15. Danach beginnt die Installation.



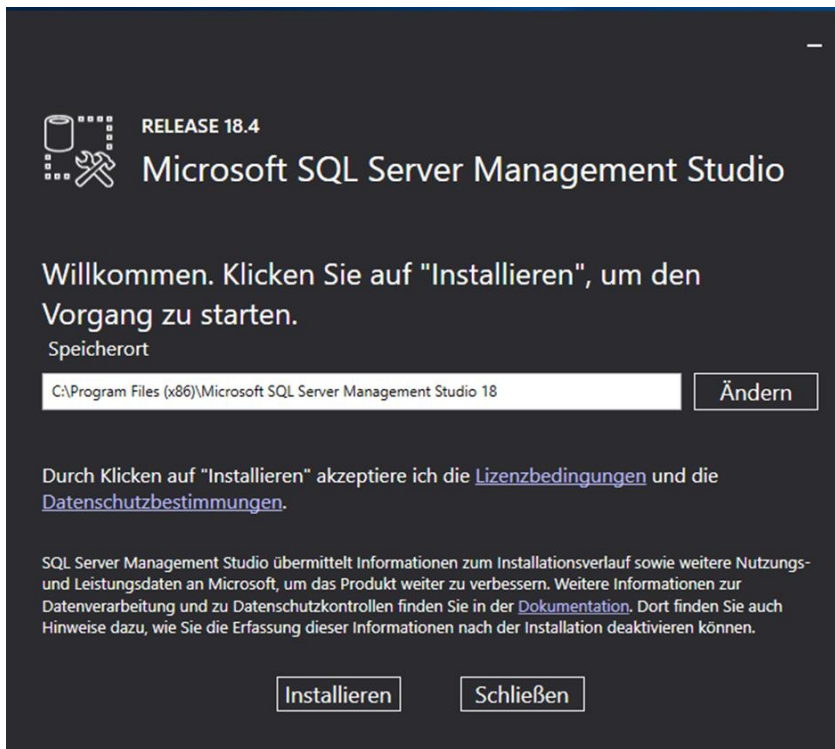
16. Die Installation vom SQL-Server ist abgeschlossen. Danach wird das SQL-Management Studio installiert, welcher ein separater Download ist.



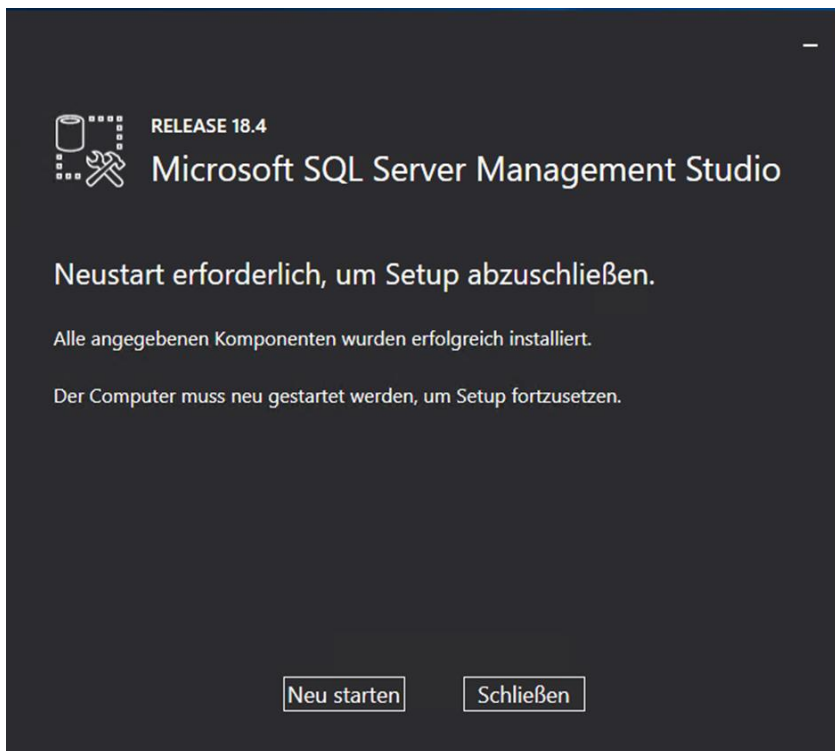
Setup erfolgreich abgeschlossen.

Anhang 2: Installation SQL Server Management Studio

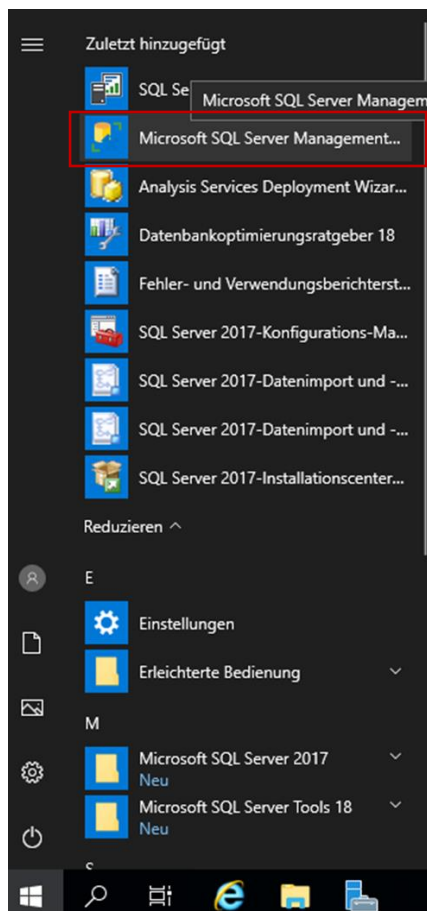
1. Starten Sie die Datei „SSMS-Setup-DEU.exe“. Um das „Microsoft SQL Server Management Studio“ zu installieren, behalten Sie den vorgegebenen Speicherort bei und klicken auf *Installieren*.



2. Nach erfolgreicher Installation muss der Server neu gestartet werden, um das Setup abzuschließen. Klicken Sie dazu auf *Neustart*.

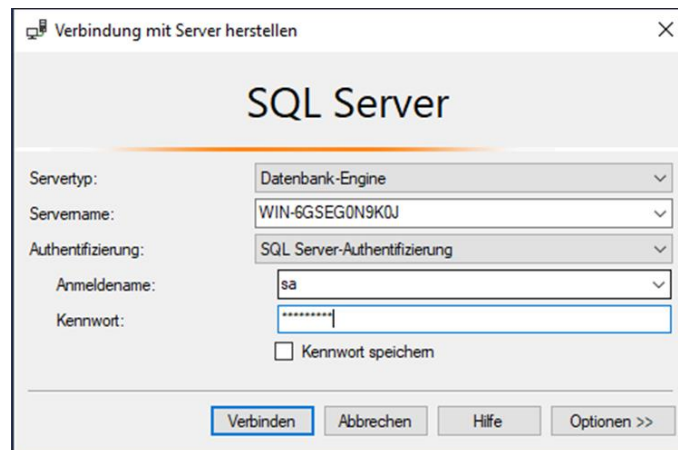


3. Nachdem der Server neu gestartet wurde, starten Sie das Programm über das Windows Start-Menü.



4. Wählen Sie den SQL Server aus. In diesem Fall handelt es sich um einen SQL Server ohne Instanz. Dabei wird nur der Server-Name angezeigt. Wenn eine Instanz vorhanden ist, setzt sich diese wie folgt zusammen: *Server-Name\Instanzname*. Als Authentifizierung wählen Sie bitte „SQL Server-Authentifizierung“. Anmeldung ist „sa“ und das bereits festgelegte Passwort. Klicken Sie auf Verbinden.

Die Installation des „SQL Server-Management Studios“ ist nun abgeschlossen.



5. Führen Sie nun die Installation des SQL Reporting Services durch. Starten Sie bitte nach dem Download die `SQLServerReportingServices.exe`. Klicken Sie auf *Reporting Services installieren*.

Hinweis: Seit der SQL Server 2017 Version ist dies ein separater Download!



6. Wählen Sie „Express“ für die Edition aus. Klicken Sie auf *Weiter*.



7. Akzeptieren Sie die Lizenzbedingungen. Klicken Sie auf *Weiter*.



8. Wählen Sie die Option *Nur Reporting Services installieren* und bestätigen Sie mit *Weiter*.



9. Behalten Sie den Installationspfad bei. Um die Installation zu beginnen, klicken Sie auf *Installieren*.



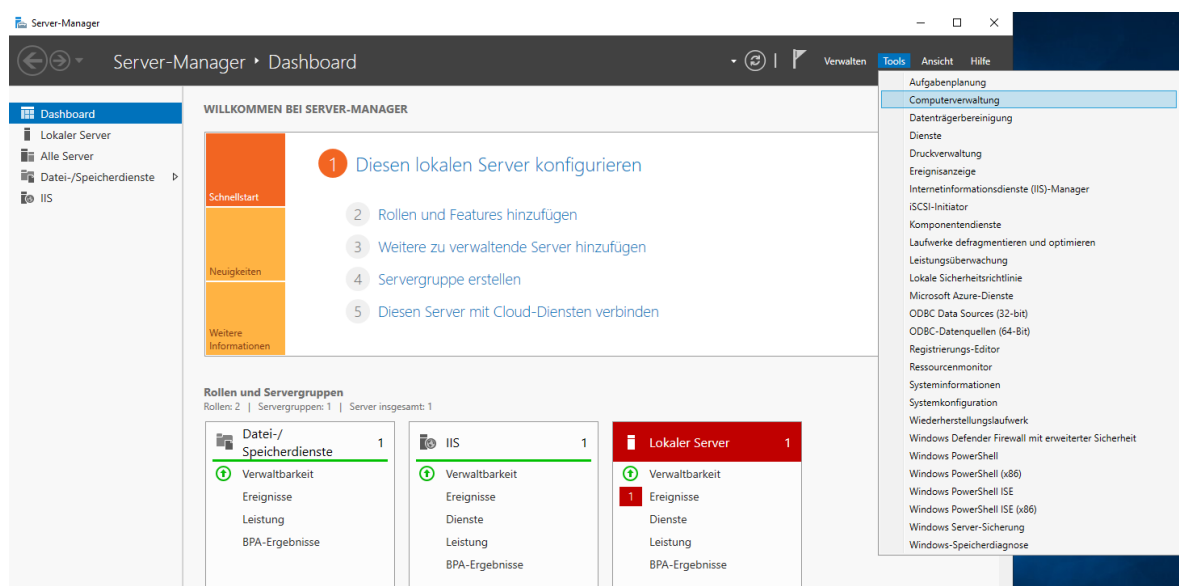
10. Das Setup ist abgeschlossen.



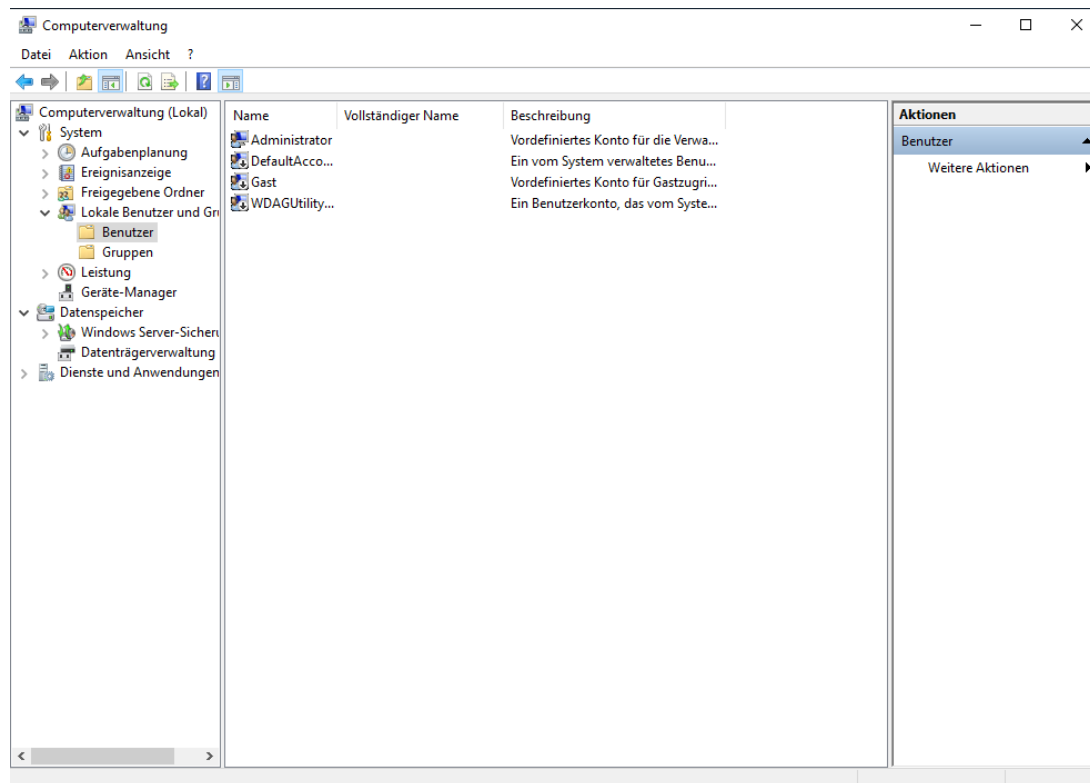
Anhang 3: MS SQL Reporting Services 2017 nachinstallieren und konfigurieren

Achtung: Bevor der nächste Schritt durchgeführt wird, müssen Sie einen Windowsbenutzer anlegen! Bitte noch nicht auf einen der drei Auswahlmöglichkeiten klicken, sondern die nachfolgende Schrittfolge einhalten!

1. Öffnen Sie die Computerverwaltung.



2. Legen Sie einen neuen Benutzer an.



3. Der Benutzer sollte den folgenden Einstellungen entsprechen. Klicken Sie anschließend auf Erstellen.

Hinweis: Erhalten Sie eine Fehlermeldung, so kann es sein, dass das Passwort 1. nicht den Richtlinien entspricht oder 2. dem Benutzernamen zu sehr ähnelt. Korrigieren Sie dann die Eingabe.

Neuer Benutzer

Benutzername: repman

Vollständiger Name:

Beschreibung: INGRADA Reporting Benutzer

Kennwort: ●●●●●●●●

Kennwort bestätigen: ●●●●●●●●

Benutzer muss Kennwort bei der nächsten Anmeldung ändern

Benutzer kann Kennwort nicht ändern

Kennwort läuft nie ab

Konto ist deaktiviert

Hilfe Erstellen Schließen

4. Gehen Sie nun zum SQL Reporting Services- Fenster zurück. Klicken Sie nun auf *Berichtsserver konfigurieren*.

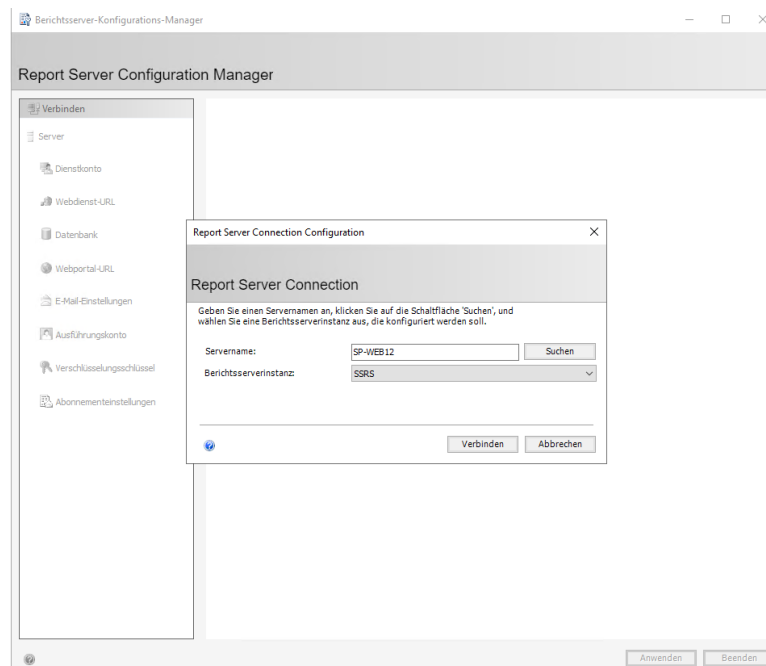


5. Wählen Sie nun die passende Instanz.

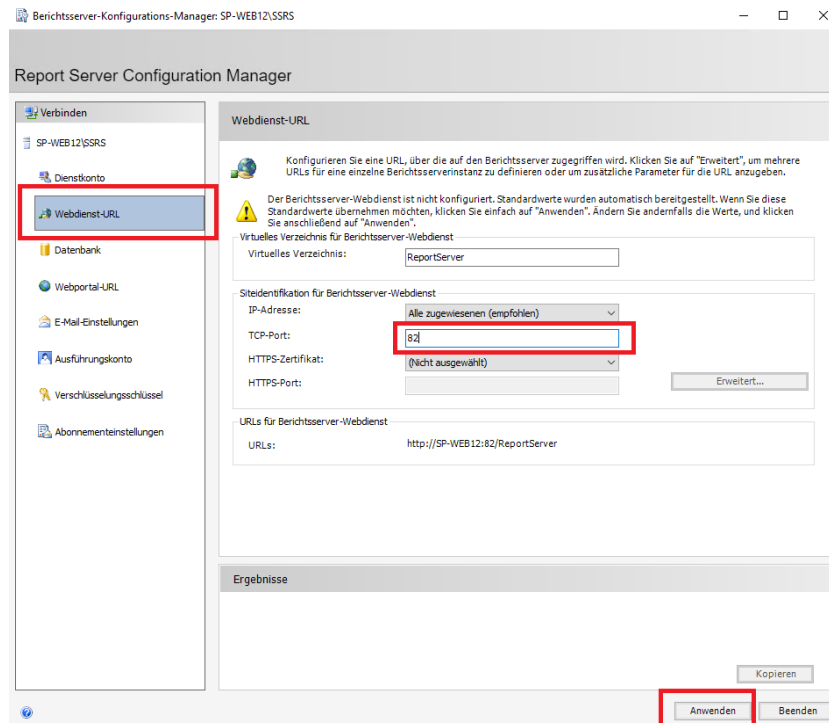
Hinweise zu mehreren Instanzen:

- Der Reportingservice wird nur einmal für INGRADAwEB und Desktop benötigt. Die Desktop und Web Reporte sind identisch.
- Wenn mehrere SQL Server-Versionen im Einsatz sind muss der Reportingservice mit dem jeweiligen Berichtsserver Konfigurationsmanager gestartet werden, d.h. ein 2019er Reportingservice lässt sich nur mit einem Berichtsserverkonfigurations-Manager 2019 bearbeiten.

Klicken Sie anschließend auf *Verbinden*.

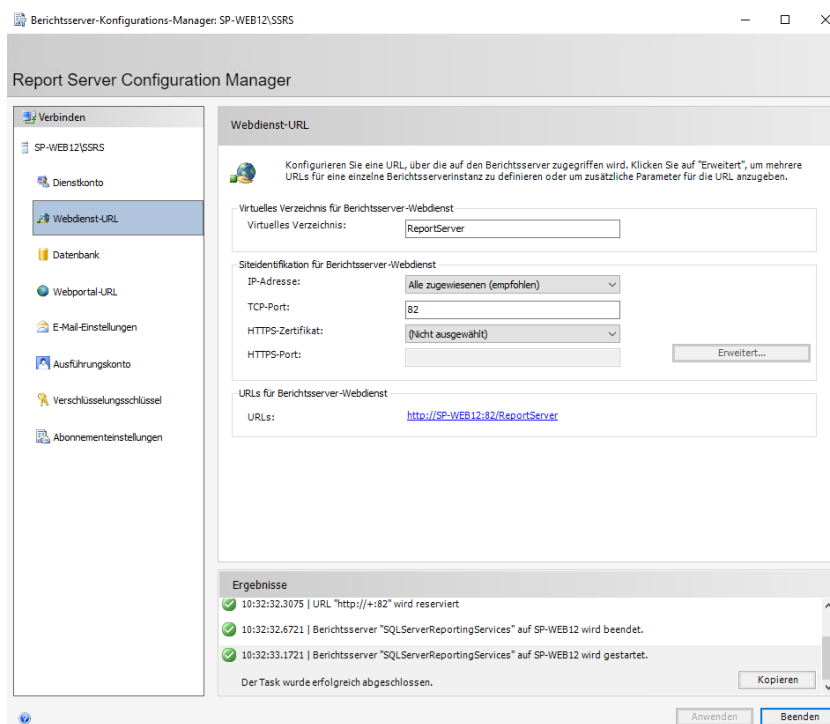


6. Klicken Sie auf „Webdienst-URL“. Ändern Sie den TCP-Port von 80 zu 82. Klicken Sie anschließend auf *Anwenden*.

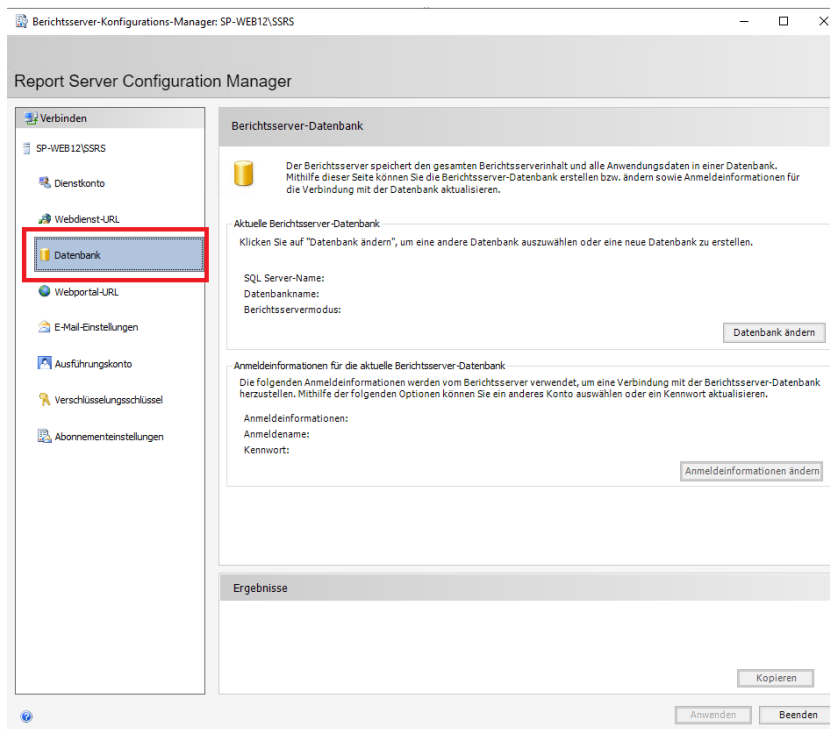


7. Das Fenster sollte anschließend wie folgt aussehen.

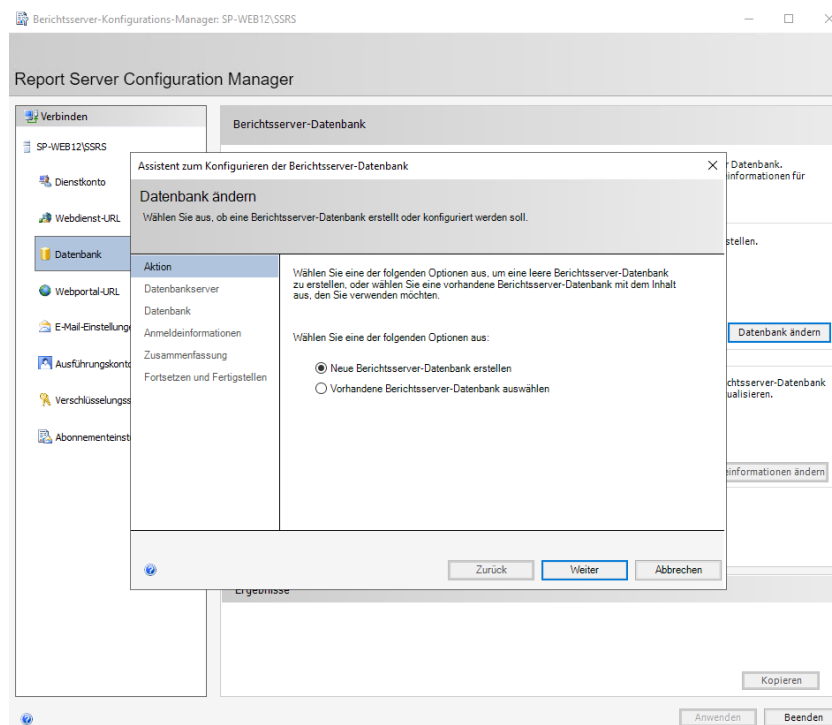
Hinweis: Wenn der Port 82 belegt ist, z.B. durch einen ApacheWeb Server, kann auch ein anderer Port gewählt werden. Dies muss dann in der weiteren Konfiguration berücksichtigt werden.



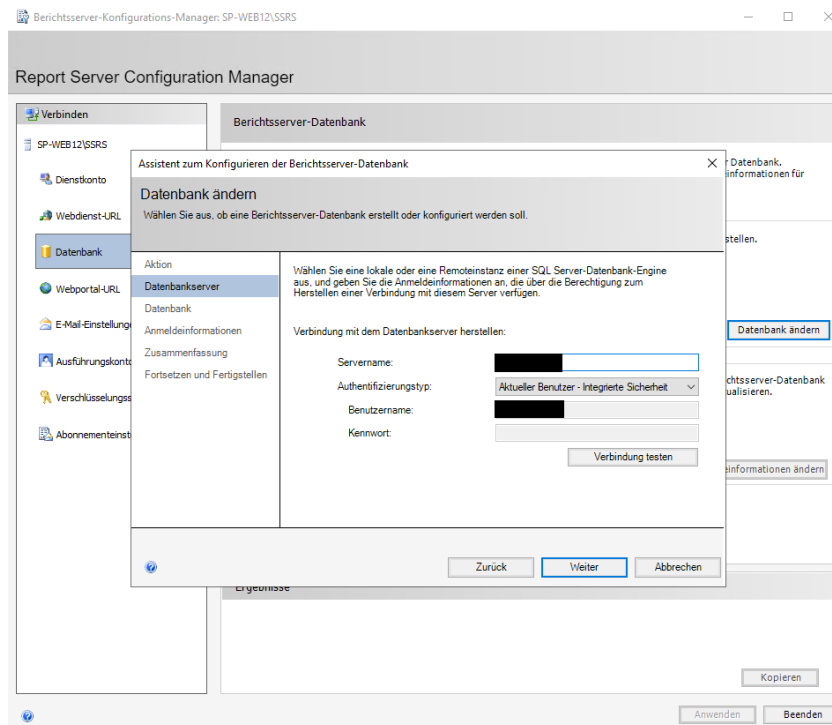
8. Wechseln Sie nun auf den Reiter „Datenbanken“. Um eine Berichtsserver-Datenbank anzulegen, klicken Sie auf *Datenbank ändern*.



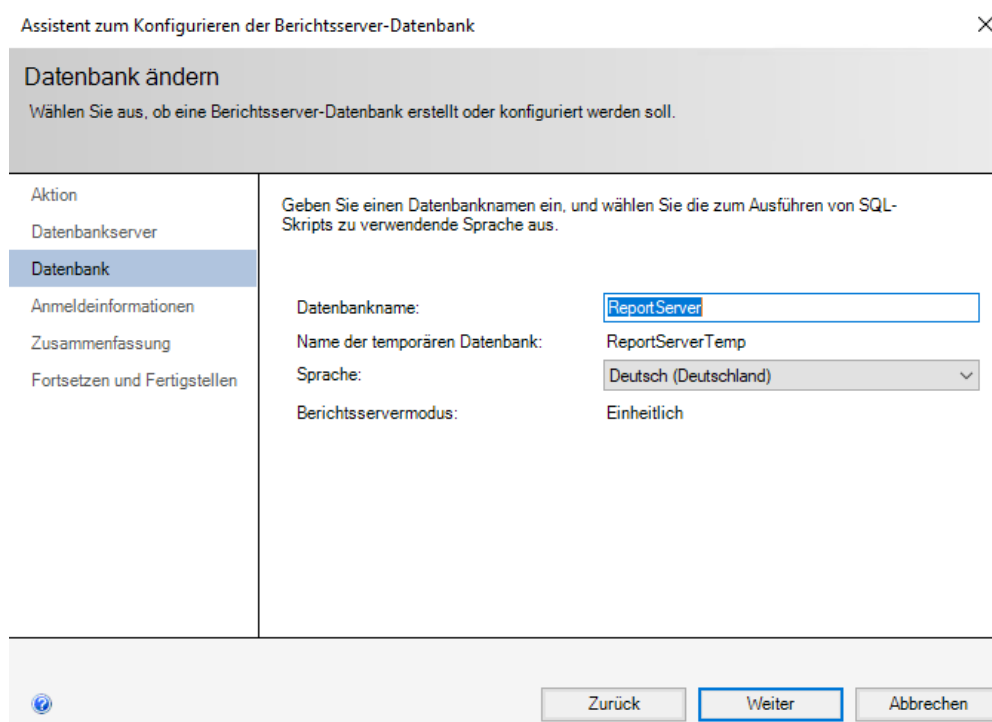
9. Es öffnet sich ein neues Fenster. Lassen Sie den voreingestellten Punkt „Neue Berichtsserver-Datenbank erstellen“ und klicken Sie auf *Weiter*.



10. Um die vorgeschlagenen Zugangsdaten zu prüfen, klicken Sie auf *Verbindung testen*. Ist die Prüfung erfolgreich, klicken Sie anschließend auf *Weiter*.



11. Der vorgeschlagene Datenbankname kann übernommen werden. Bestätigen Sie ihn, indem Sie auf *Weiter* klicken.



12. Klicken Sie auch hier auf *Weiter*.

Assistent zum Konfigurieren der Berichtsserver-Datenbank X

Datenbank ändern

Wählen Sie aus, ob eine Berichtsserver-Datenbank erstellt oder konfiguriert werden soll.

<ul style="list-style-type: none"> Aktion Datenbankserver Datenbank <li style="background-color: #e0e0e0;">Anmeldeinformationen Zusammenfassung Fortsetzen und Fertigstellen 	<p>Geben Sie die Anmeldeinformationen eines vorhandenen Kontos an, das der Berichtsserver zum Herstellen einer Verbindung mit der Berichtsserver-Datenbank verwenden wird. Die Berechtigung für den Zugriff auf die Berichtsserver-Datenbank wird dem angegebenen Konto automatisch erteilt.</p> <p>Anmeldeinformationen:</p> <p>Authentifizierungstyp: <input type="text" value="Anmeldeinformationen des Diensts"/></p> <p>Benutzername: <input type="text" value="NT SERVICE\SQLServerReportingServices"/></p> <p>Kennwort: <input type="password"/></p>
--	---

13. Bestätigen Sie die Zusammenfassung ebenfalls mit einem Klick auf *Weiter*.

Assistent zum Konfigurieren der Berichtsserver-Datenbank X

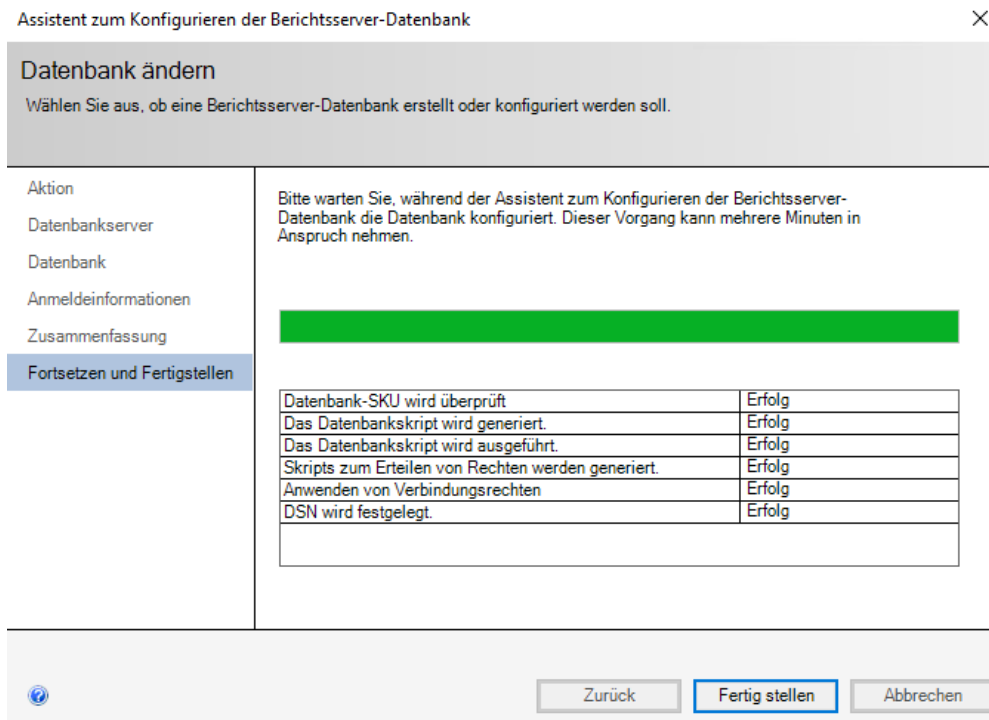
Datenbank ändern

Wählen Sie aus, ob eine Berichtsserver-Datenbank erstellt oder konfiguriert werden soll.

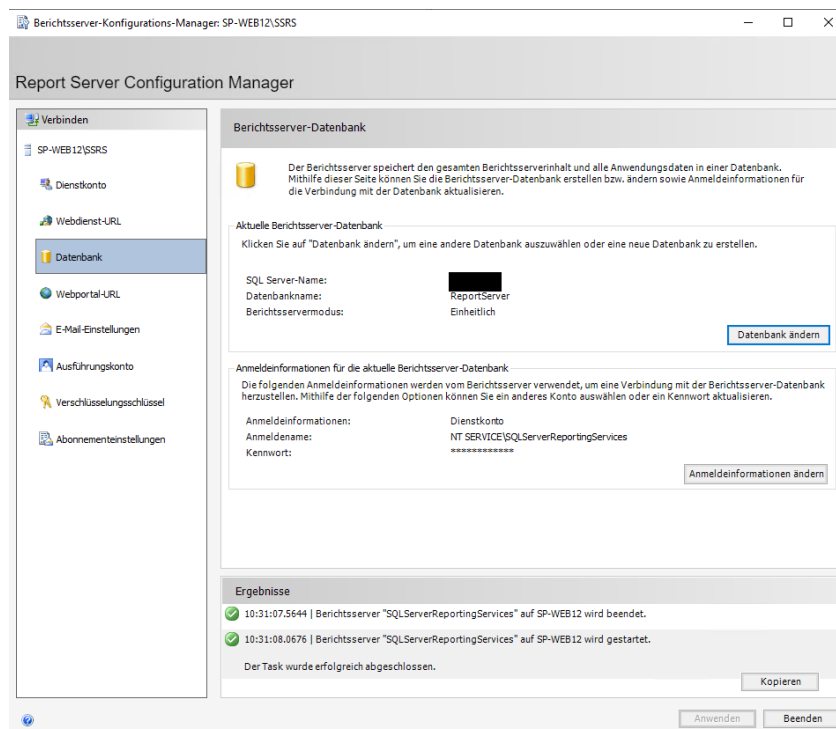
<ul style="list-style-type: none"> Aktion Datenbankserver Datenbank Anmeldeinformationen <li style="background-color: #e0e0e0;">Zusammenfassung Fortsetzen und Fertigstellen 	<p>Die folgenden Informationen werden verwendet, um eine neue Berichtsserver-Datenbank zu erstellen. Überprüfen Sie die Richtigkeit der Informationen, bevor Sie den Vorgang fortsetzen.</p> <p>SQL Server-Instanz: <input type="text" value=""/></p> <p>Berichtsserver-Datenbank: <input type="text" value="ReportServer"/></p> <p>Temporäre Datenbank: <input type="text" value="ReportServerTempDB"/></p> <p>Berichtsserversprache: <input type="text" value="Deutsch (Deutschland)"/></p> <p>Berichtsservermodus: <input type="text" value="Einheitlich"/></p> <p>Authentifizierungstyp: <input type="text" value="Dienstkonto"/></p> <p>Benutzername: <input type="text" value="NT SERVICE\SQLServerReportingServic..."/></p> <p>Kennwort: <input type="password" value="*****"/></p>
--	--

14. Es wird nun eine neue Reportingserver-Datenbank angelegt.

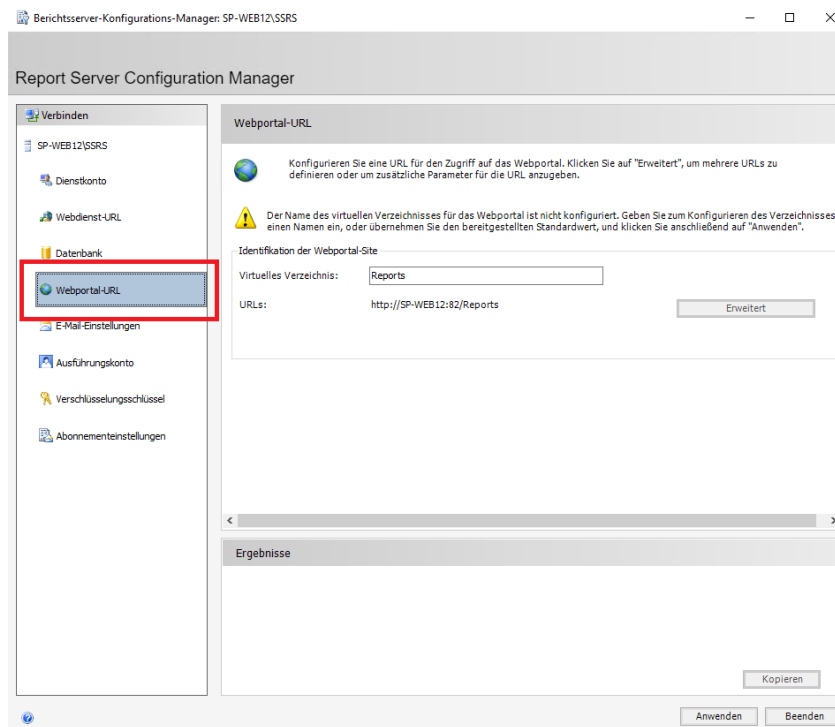
15. Um abschließend alle Änderungen zu übernehmen, klicken Sie auf *Fertig stellen*.



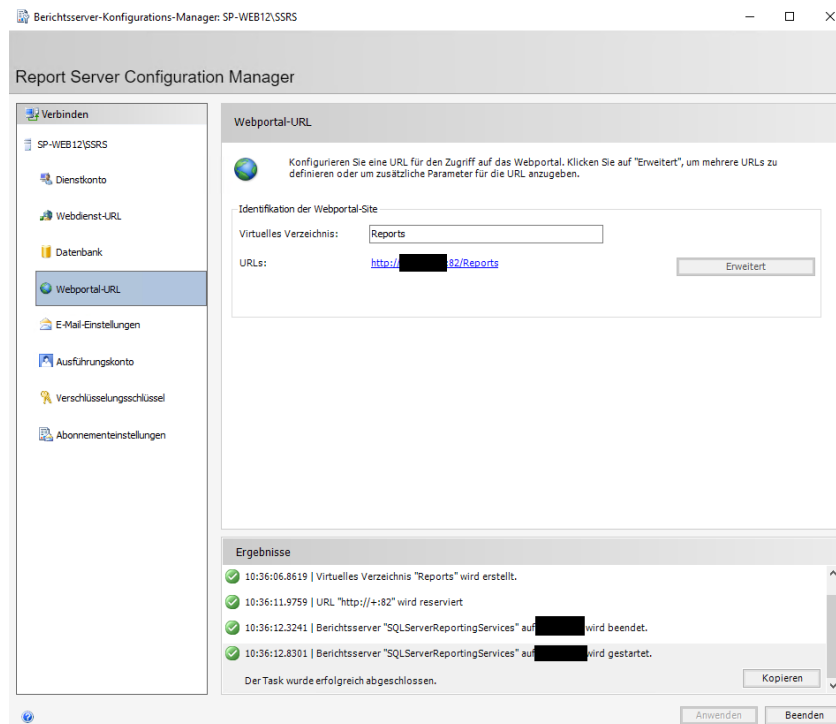
16. Das Fenster sollte nun wie folgt aussehen.



17. Wechseln Sie wieder auf den Reiter „Webportal URL“ und klicken Sie auf *Anwenden*.

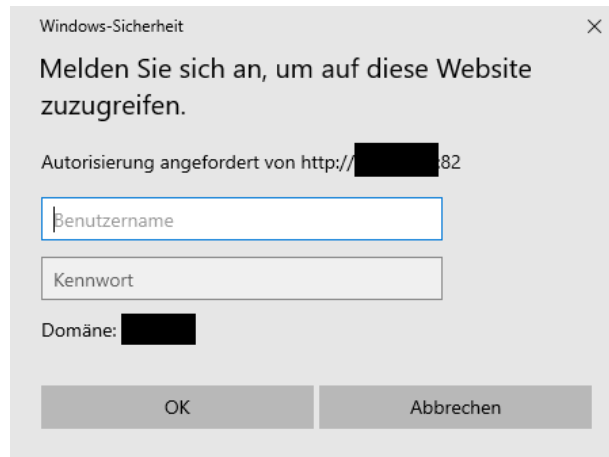


18. Das Fenster sollte nun wie folgt aussehen.

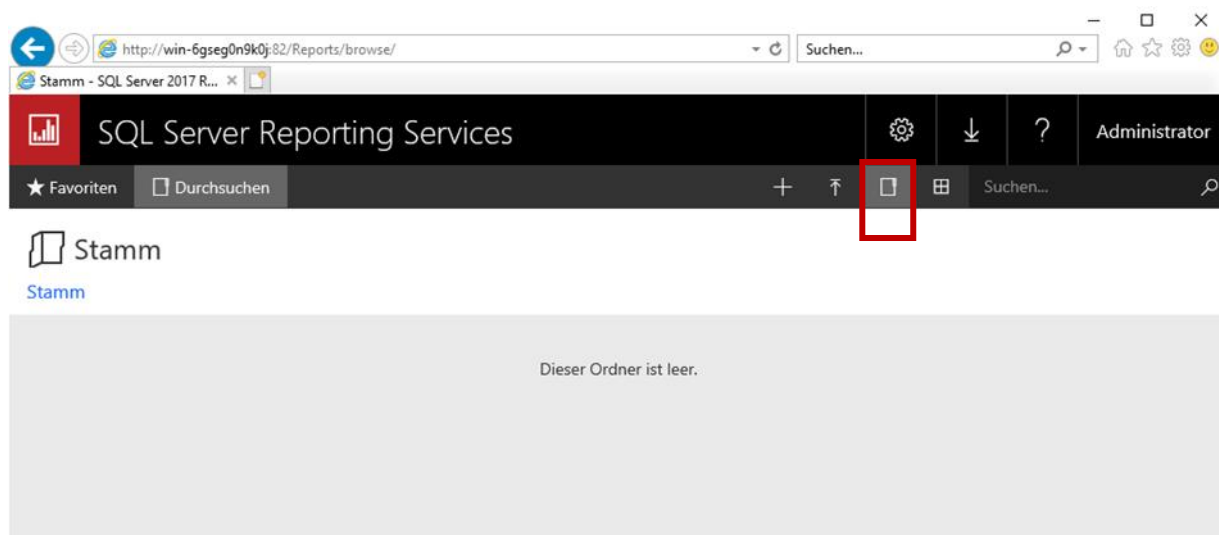


19. Wechseln Sie nun auf eine Webportal-URL. Diese sollte nun blau hinterlegt sein.

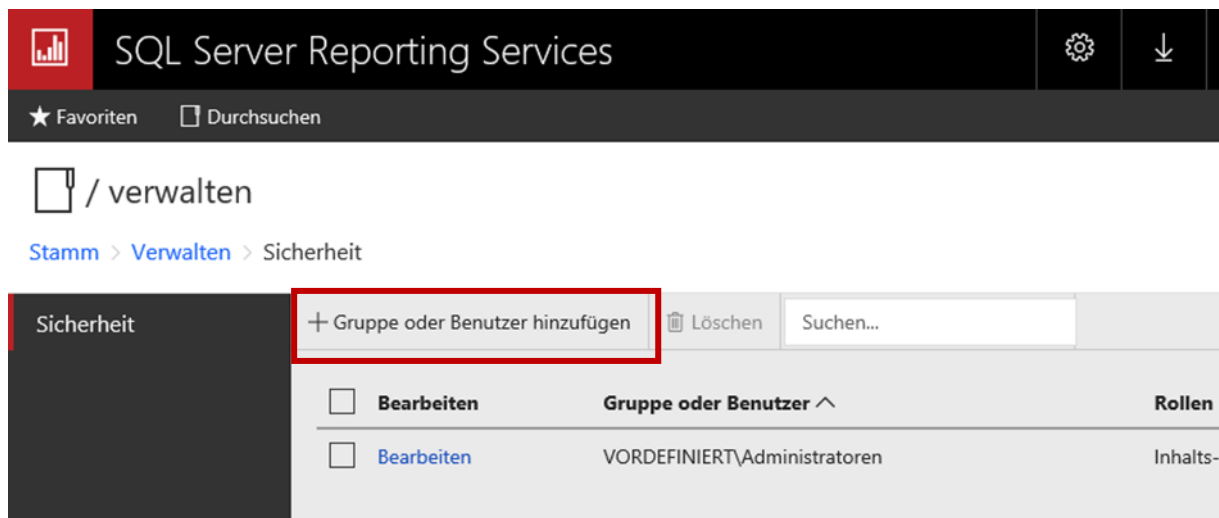
Hinweis: Sollte es beim Öffnen der URL zu einer Passwortabfrage kommen, verwenden Sie ein Adminkonto. Ggf. sollten auch Ausnahme-Seiten eingetragen oder der Browser als Administrator gestartet werden.



20. Wenn alles funktioniert hat, sollte Ihr Fenster wie folgt aussehen. Klicken Sie dann auf Verwalten (das rot eingerahmte Kästchen).

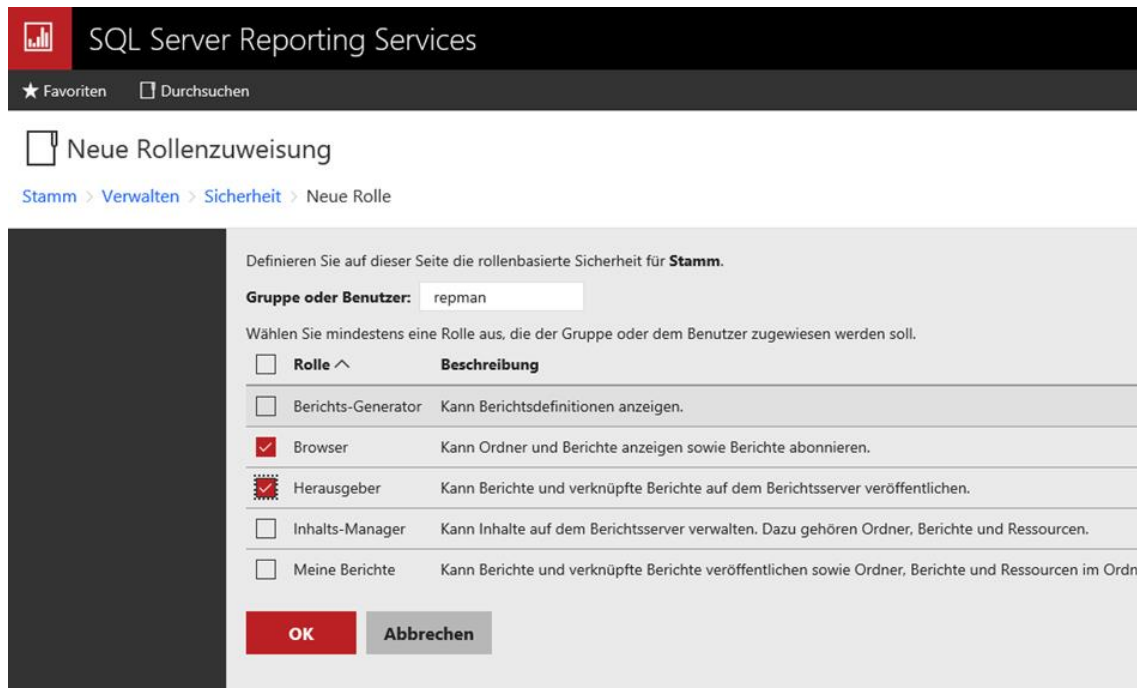


21. Klicken Sie hier auf den Reiter „Sicherheit“ und dann auf *Gruppe oder Benutzer hinzufügen*.

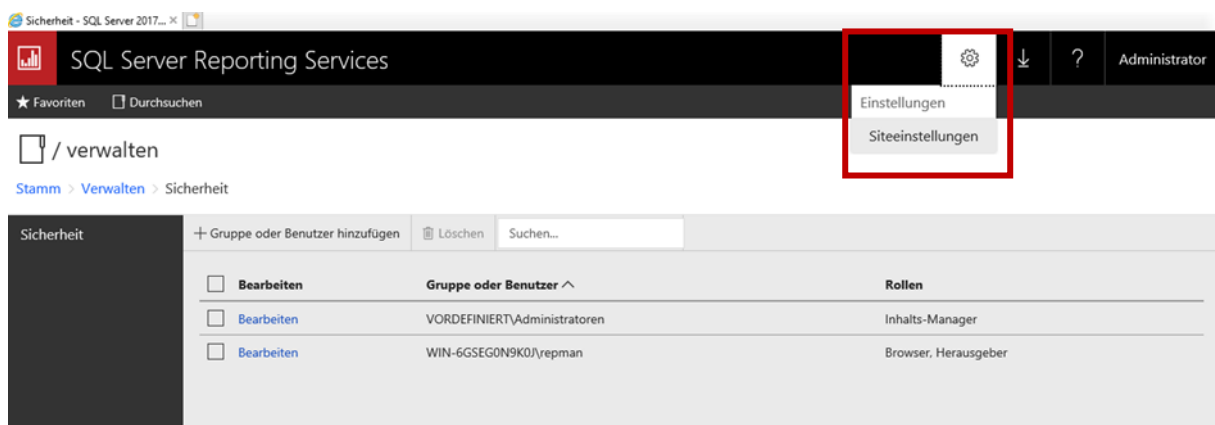


22. Um eine neue Rollenzuweisung vorzunehmen, tragen Sie in „Gruppe oder Benutzer“ den vorher angelegten Windowsbenutzer ein (in diesem Beispiel *repman*) mit den wie folgt angegebenen

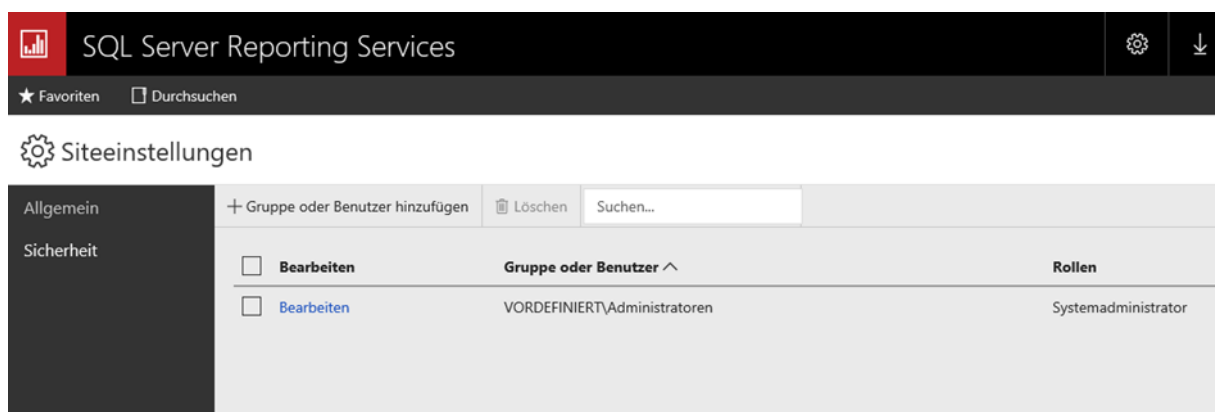
Rollen „Browser“ und „Herausgeber“ an. Um die Einstellungen zu übernehmen, klicken Sie auf **OK**.



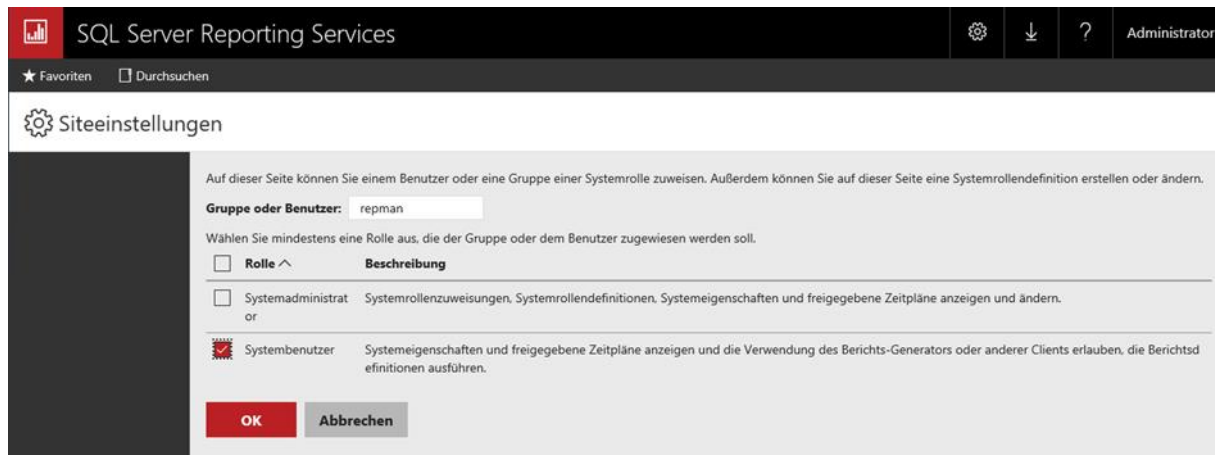
23. Klicken Sie dann auf das Zahnrad > *Einstellungen* > *Siteeinstellungen*.



24. Wechseln Sie auf den Reiter „Sicherheit“. Klicken Sie auch hier wieder auf *Gruppe oder Benutzer hinzufügen*.

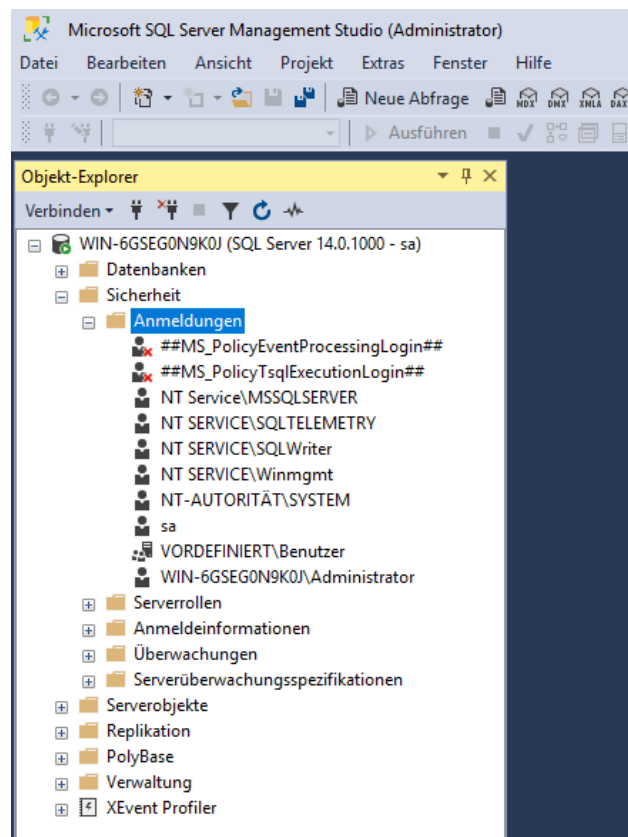


25. Hier tragen Sie erneut den Windowsbenutzer (hier wieder *repman*) ein und vergeben dieses Mal die Rolle „Systembenutzer“. Klicken Sie auf *OK*.

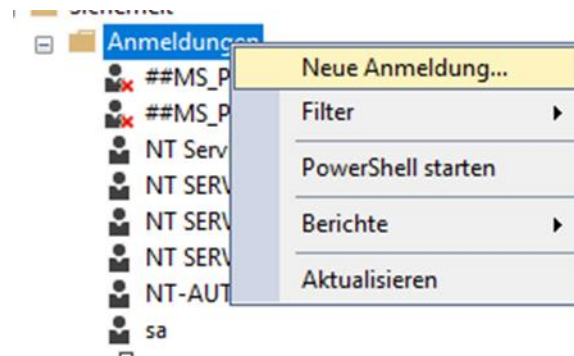


26. Der Browser kann nun geschlossen werden. Öffnen Sie anschließend das SQL Management Studio.

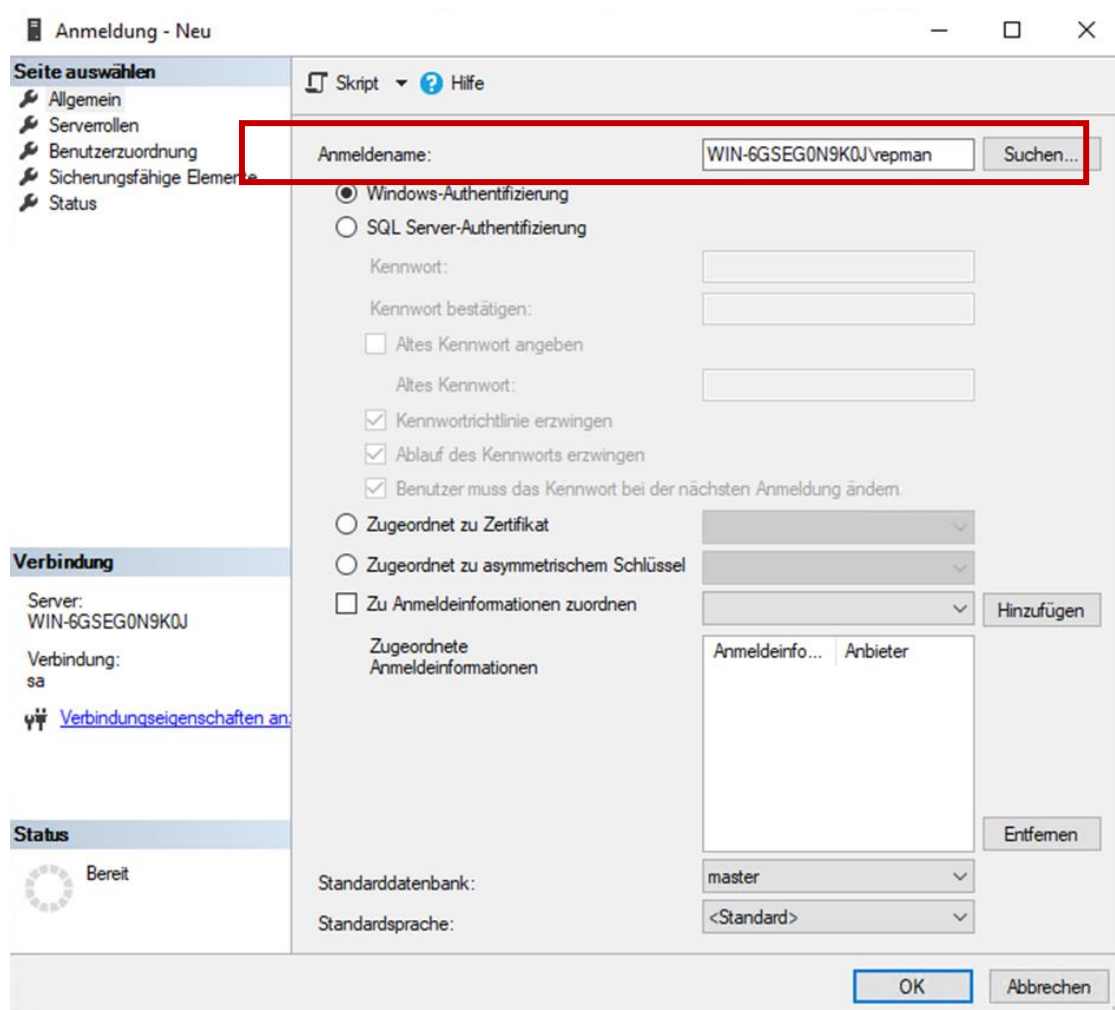
27. Öffnen Sie dort *Sicherheit > Anmeldungen*.



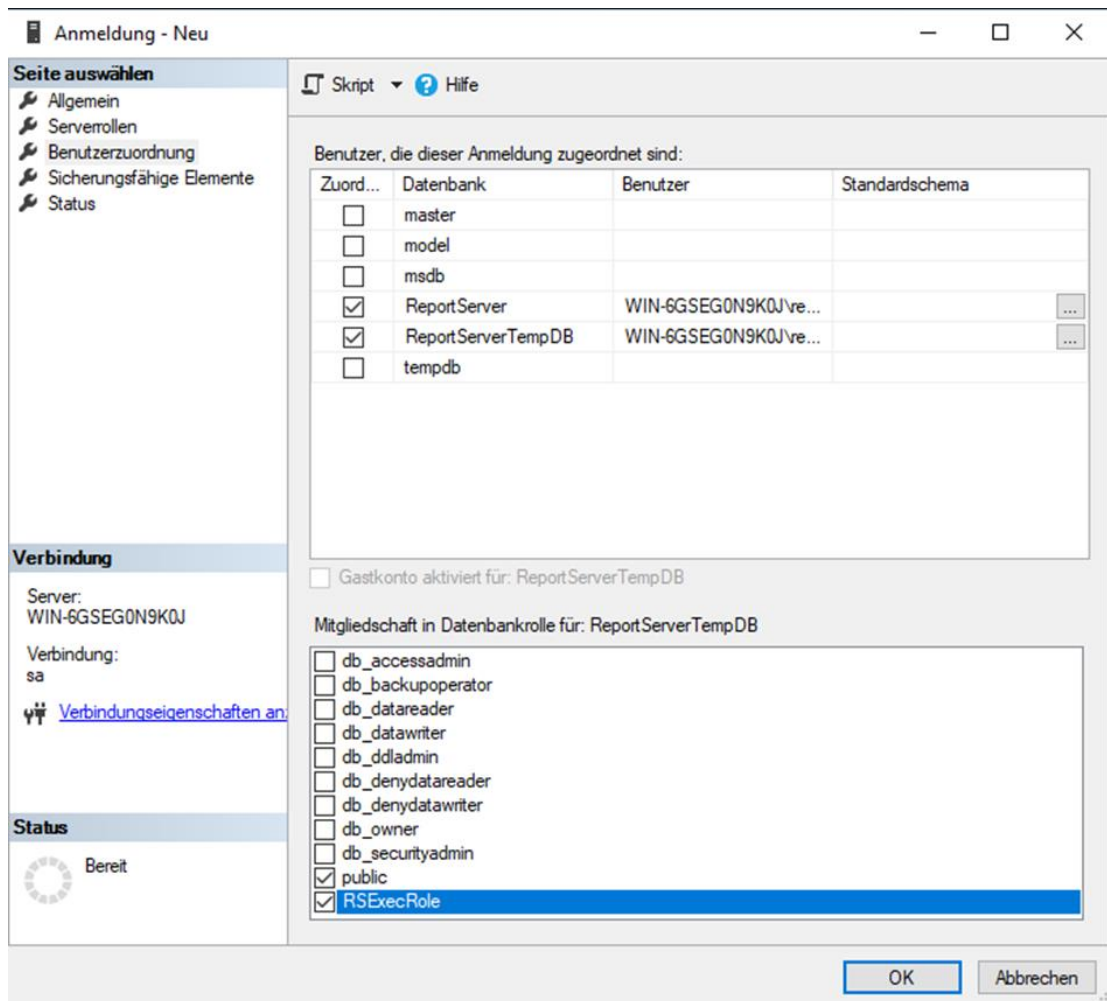
28. Legen Sie hier wie folgt zwei neue Anmeldungen an, indem Sie mit einem Rechtsklick den Dialog öffnen und auf *Neue Anmeldungen* klicken.



29. Klicken Sie in dem neu geöffneten Fenster auf *Suchen...* und wählen Sie als Anmeldename den angelegten Windowsbenutzer für das Reporting aus.



30. Klicken Sie anschließend auf den Reiter *Seite auswählen > Benutzerzuordnung*. Wählen Sie für die *ReportServer* Datenbank und die *ReportServerTempDB* die Datenbank-Rolle *RSExecRole* aus. Dies muss für jede Datenbank einzeln erfolgen. Bestätigen Sie abschließend mit *OK*.



31. Legen Sie nun einen SQL-Benutzer wie folgt an.

Achtung: Deaktivieren Sie das Kästchen *Kennwortrichtlinie erzwingen!* Passiert dies nicht, kann der Benutzer sich später nicht mehr anmelden und es können keine Reporte mehr erstellt werden!

32. Vergeben Sie auch hier in der Benutzerzuordnung die Datenbankrolle *RSExecRole* für die beiden Datenbanken. Klicken Sie abschließend auf OK, um die Einstellungen zu übernehmen.

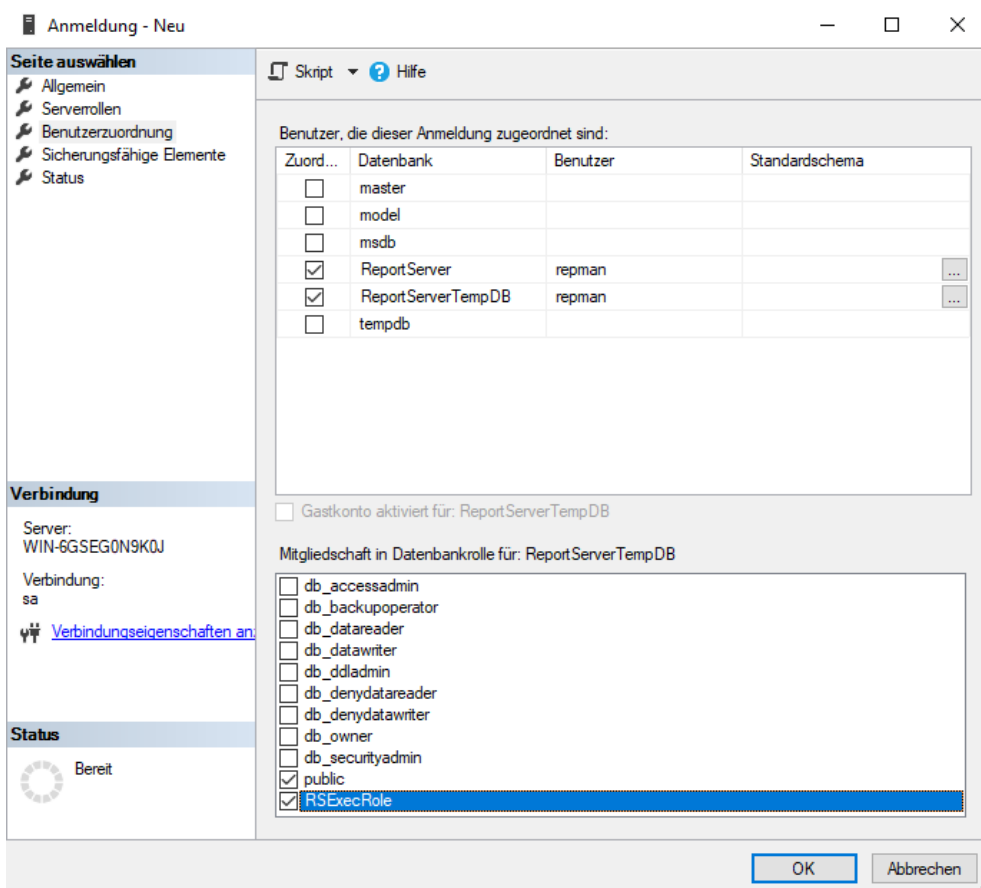
Ergänzung in der Datei *web.config*



Achtung: Bitte passen Sie in der *web.config* des Reporting Server " C:\Program Files\Microsoft SQL Server Reporting Services\SSRS\ReportServer" folgende Zeile an. Erweitern Sie den Knoten „httpRuntime“ um das Attribut „maxRequestLength“ (300000 = 300MB):

```
<httpRuntime executionTimeout="18000" maxRequestLength="300000" />
```

Der Reportingserver ist nun fertig konfiguriert.



Anhang 4: Konfigurieren des MS SQL Reporting Services



Hinweis: Wird der SQL Server mit eine Instanz installiert, so wird an die Reportingserver Datenbank der Instanzname mit \$ angehängt. Die Pfade zur Berichtsmanager URL und zur Webdienst URL werden ebenfalls mit dem Instanzname ergänzt.

Windows-Benutzer für Reporting Services anlegen

Es muss ein neuer Windows-Benutzer angelegt werden, der unter INGRADA web für Zugriffe auf die Microsoft SQL Reporting Services und die Reporting Datenbank genutzt wird. Nennen Sie den Windows-Benutzer zum Beispiel „repman“ und aktivieren Sie die Option „Kennwort läuft nie ab“. Benutzername, Passwort und Domäne werden später verschlüsselt in der Projektkonfigurationsdatei (*SPWebConfig.xml*) abgespeichert. Nur dieser Benutzer kann später in INGRADA web Reporte erzeugen.

1. Gehen Sie in Start → Programme → Microsoft SQL Server 20XX → Konfigurations-Manager für Reporting Services. Klicken Sie im folgenden Dialog auf Verbinden.

Konfigurationsverbindung für Reporting Services

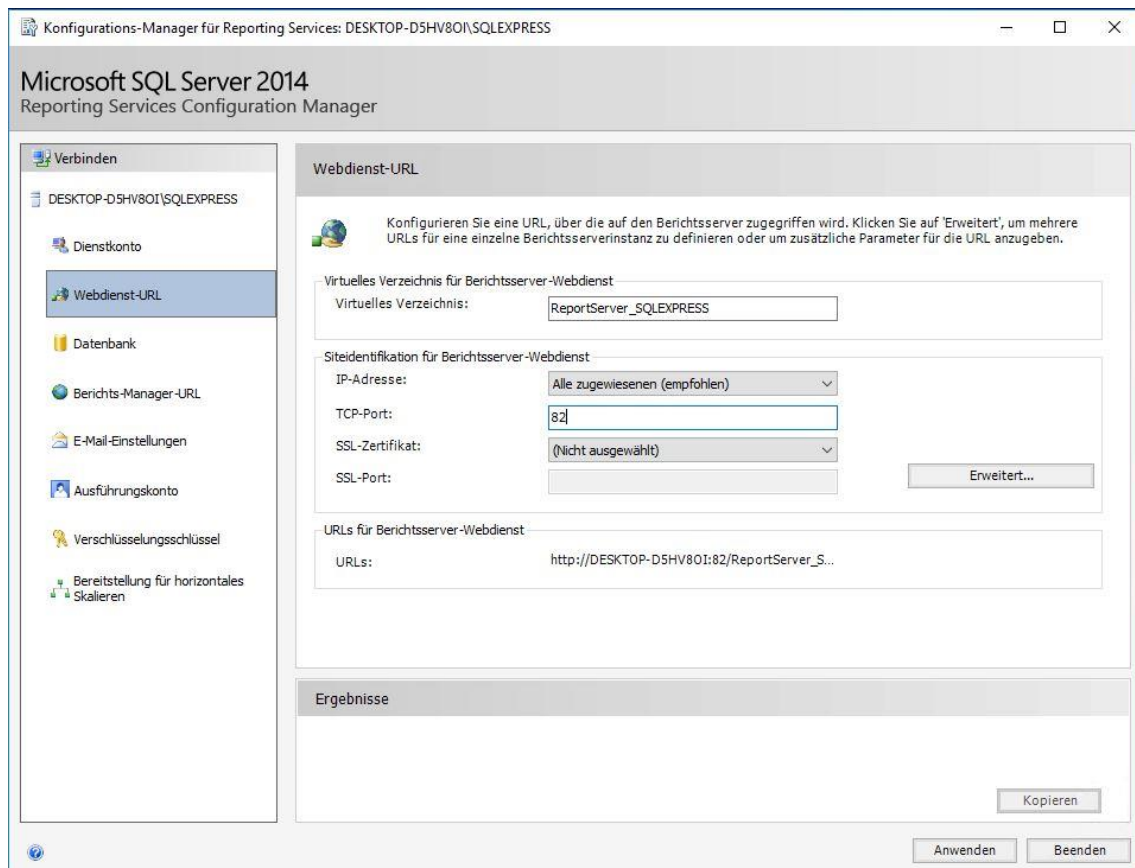
Microsoft SQL Server 2014
Reporting Services

Geben Sie einen Servernamen an, klicken Sie auf die Schaltfläche 'Suchen', und wählen Sie eine Berichtsserverinstanz aus, die konfiguriert werden soll.

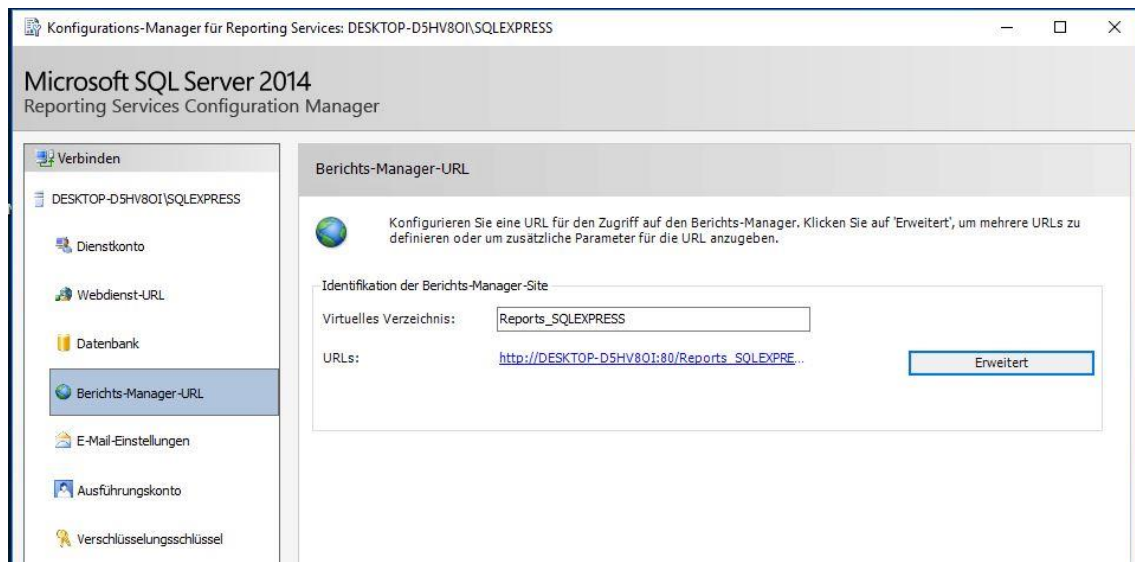
Servername:

Berichtsserverinstanz:

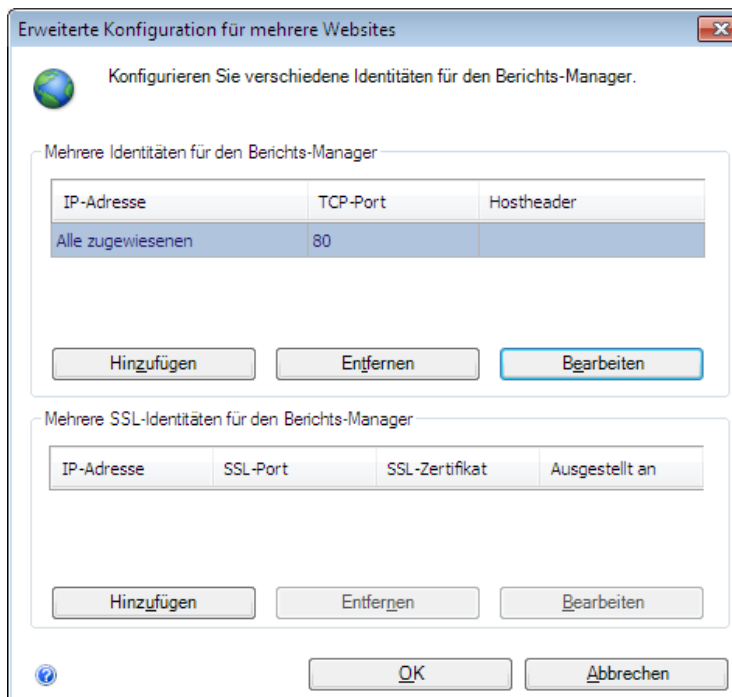
2. Wählen Sie auf der linken Seite „Webdienst-URL“, ändern Sie den TCP-Port in 82 und klicken Sie danach auf Anwenden.



3. Öffnen Sie anschließend den „Berichts-Manager-URL“ und klicken Sie auf Erweitert.

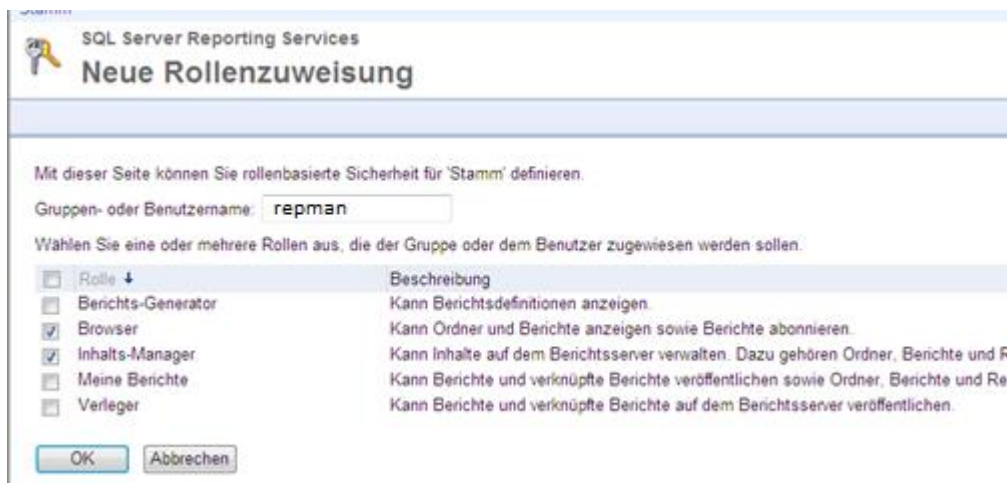


4. Ändern Sie in dem geöffneten Fenster den TCP-Port auf 82. Klicken Sie danach auf OK. Die Änderungen werden in „Berichts-Manager-URL“ unter „Ergebnisse“ aufgeführt.

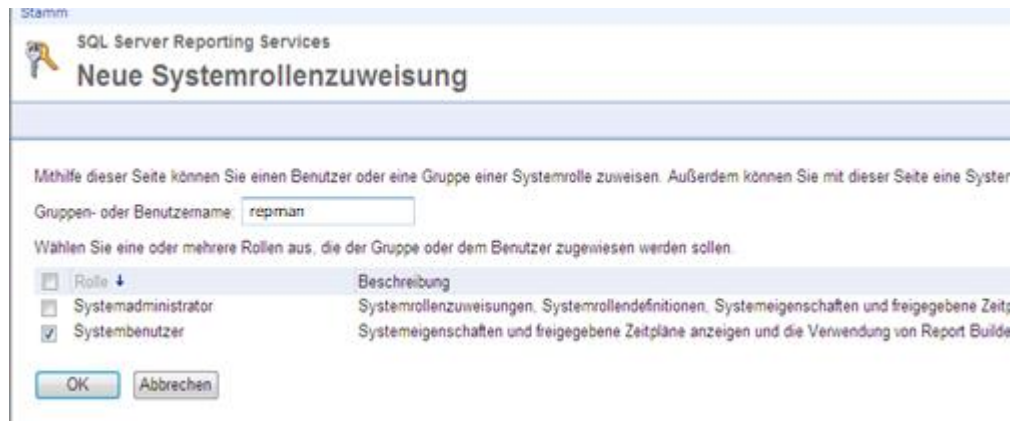


Rollenzuweisung in der Berichtsmanager-Oberfläche

1. Öffnen Sie die URL im Bereich „Berichts-Manager-URL“ und gehen Sie auf „Ordneinstellung“ bzw. „Eigenschaften“ (je nach Version des MS SQL Servers).
1. Wenn eine Anmeldung erforderlich ist, melden sie sich bitte mit den Windows-Admin Konto an.
2. Wählen Sie „Neue Rollenzuweisung“ und geben Sie als Benutzername den Windows-Benutzer für die Reporting Services an. Weisen Sie diesem die Rollen „Browser“ und „Inhalts-Manager“ zu und klicken Sie auf OK.



3. Gehen Sie anschließend oben rechts in die „Siteeinstellungen“ und erstellen Sie eine „Neue Rollenzuweisung“. Geben Sie wieder den zuvor erstellten Windows-Benutzer an und weisen Sie ihm die Rolle „Systembenutzer“ zu.



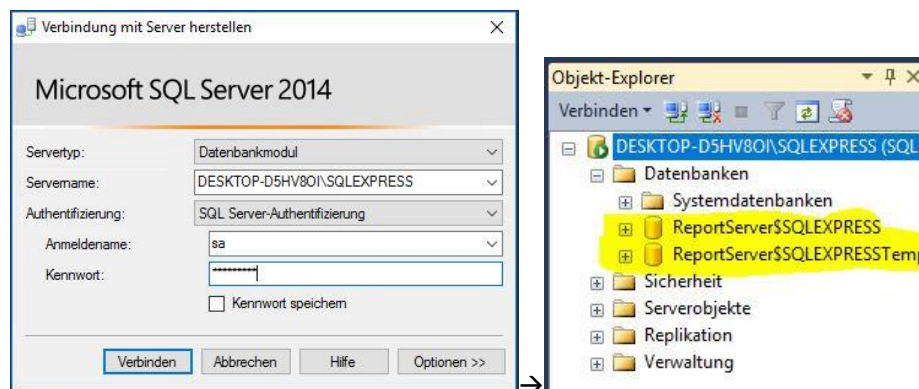
4. Klicken Sie auf OK, um die Rollenzuweisung abzuschließen.

Anlegen eines SQL-Server Benutzers

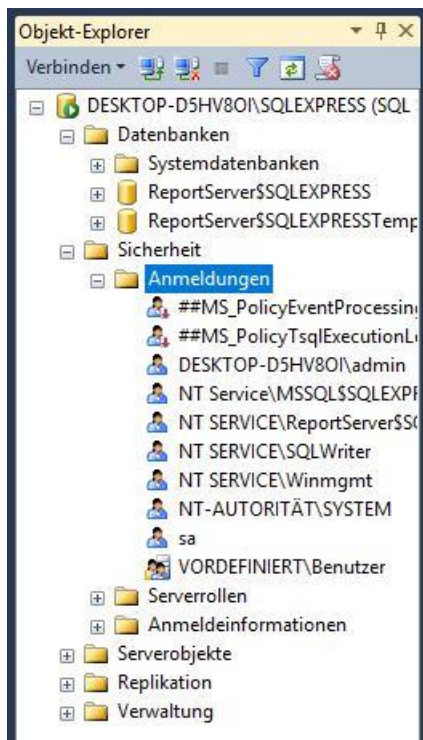
Damit die Reporting Services in INGRADA web korrekt arbeiten, ist es erforderlich einen neuen Microsoft SQL Server Benutzer anzulegen. Über diesen Benutzer werden die Daten aus der Datenbank gelesen, mit denen die Reporte gefüllt werden.

Dieser Benutzer muss den gleichen Benutzernamen und das gleiche Passwort haben wie der Windows-Benutzer, den Sie für die Reporting Services nutzen.

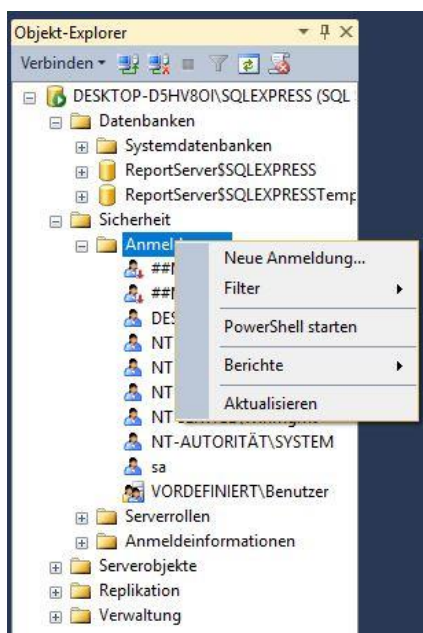
1. Um den SQL Benutzer anzulegen, müssen Sie zunächst das Microsoft SQL Server Management Studio starten. Melden Sie sich an dem SQL Server an, der die ReportServer und ReportServerTempDB Datenbanken beinhaltet.



2. Öffnen Sie hier das Untermenü Sicherheit -> Anmeldungen.



3. Klicken Sie mit der rechten Maustaste auf Anmeldungen und erstellen Sie eine neue Anmeldung.

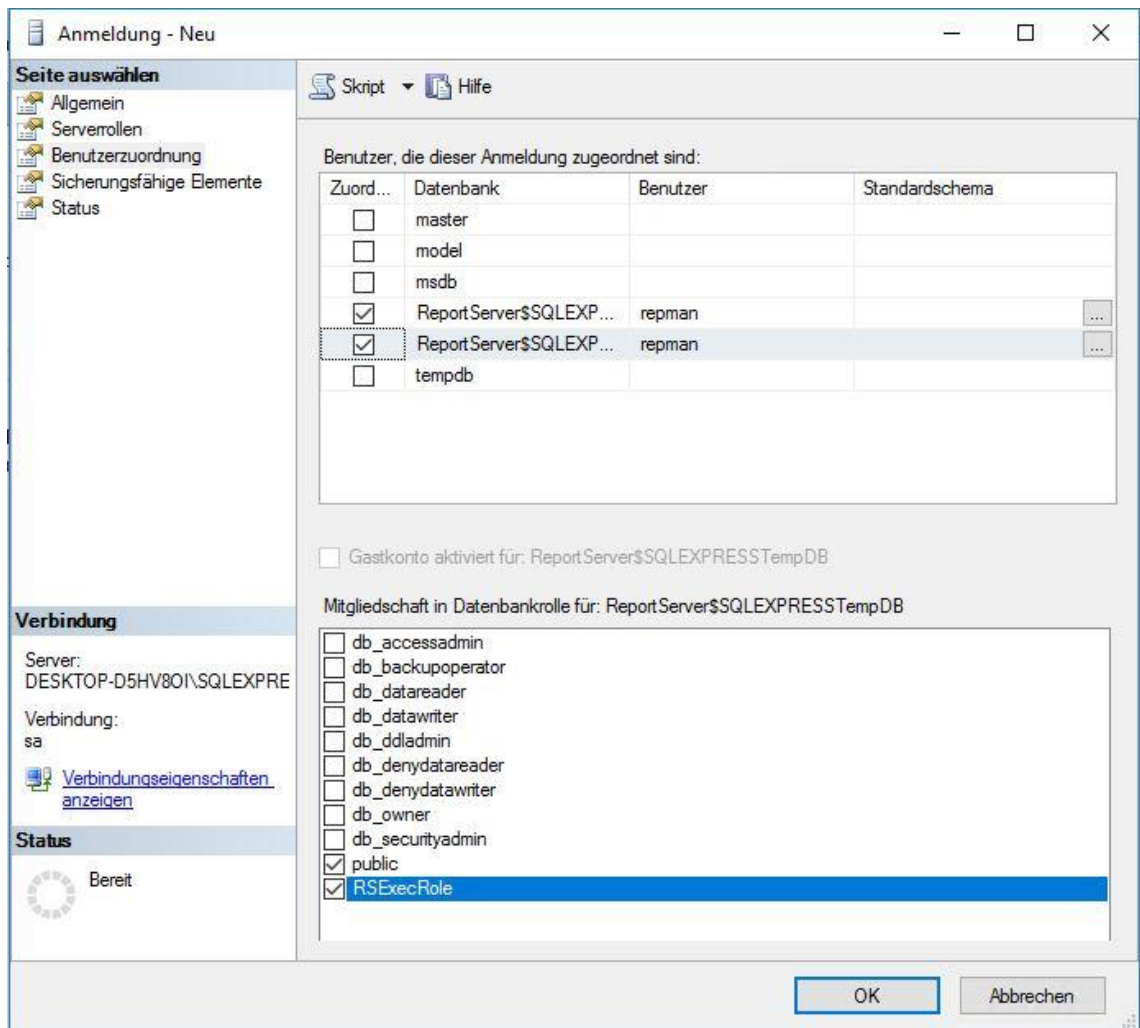


4. Aktivieren Sie im nächsten Fenster „SQL Server-Authentifizierung“ und deaktivieren Sie „Ablauf des Kennworts erzwingen“. Geben Sie als Anmeldenamen und Kennwort die gleichen Anmeldedaten an, die Sie auch für Ihren Reporting Windows-Benutzer nutzen. Dies ist notwendig, da sowohl der Windows-Benutzer als auch der SQL-Benutzer für das Reporting benötigt werden, aber die Anmeldedaten für beide nur einmalig und verschlüsselt in einer Steuerdatei abgelegt werden.

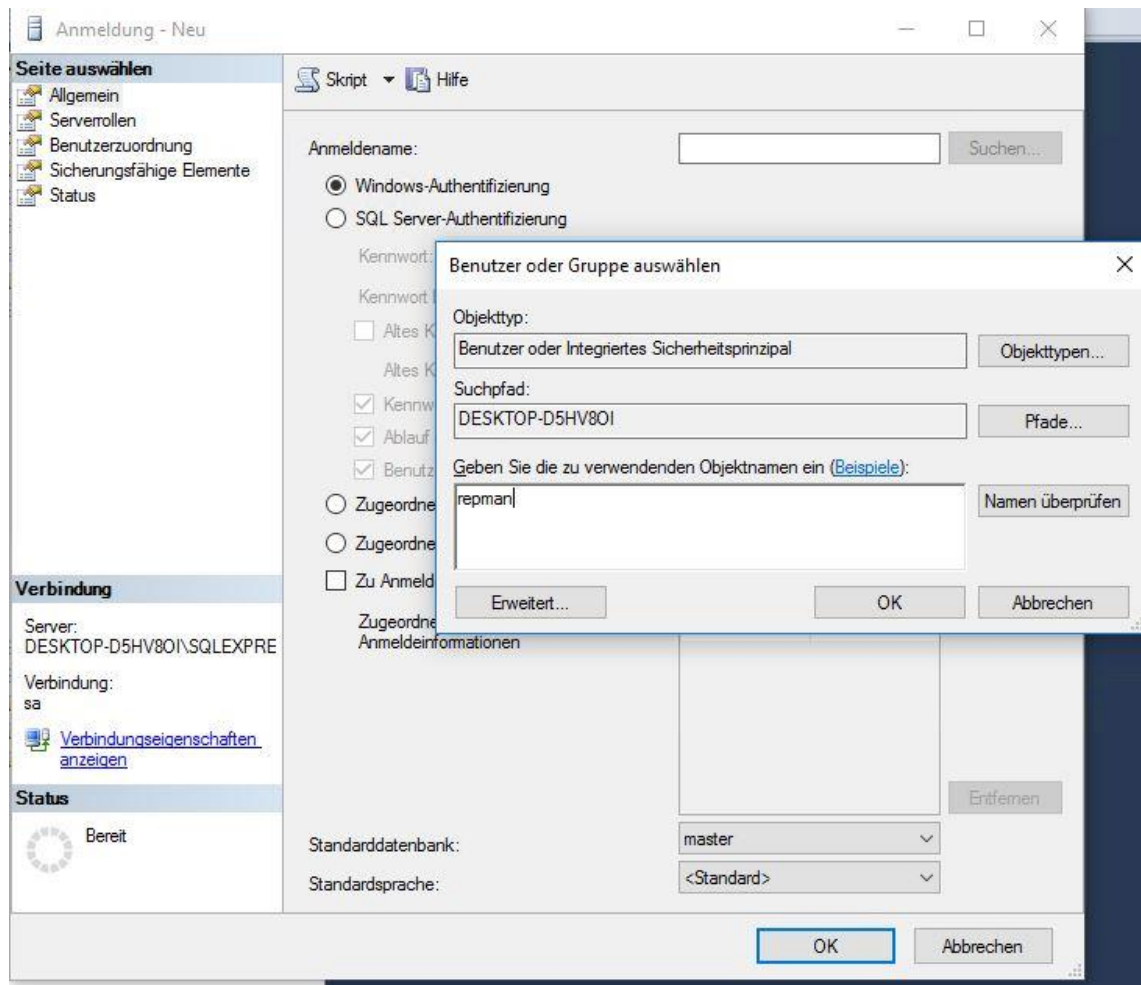
The screenshot shows the 'Anmeldung - Neu' dialog box with the following configuration:

- Anmeldename:** repman
- Authentifizierung:** SQL Server-Authentifizierung
- Kennwort:** [Masked]
- Kennwort bestätigen:** [Masked]
- Altes Kennwort angeben:**
- Altes Kennwort:** [Empty]
- Kennwortrichtlinie erzwingen:**
- Ablauf des Kennworts erzwingen:**
- Benutzer muss das Kennwort bei der nächsten Anmeldung ändern:**
- Zugeordnet zu:** Zugeordnet zu asymmetrischem Schlüssel
- Zu Anmeldeinformationen zuordnen:**
- Zugeordnete Anmeldeinformationen:** [Empty list]
- Standarddatenbank:** master
- Standardsprache:** <Standard>

5. Ordnen Sie als nächstes in der „Benutzerzuordnung“ den ReportServer und ReportServerTempDB zu. Aktivieren Sie für beide Datenbanken die Datenbankrollen public und RSExecRole.



- Bestätigen Sie die Einstellungen mit OK. Der SQL Benutzer wird angelegt.
- Klicken sie erneut auf Anmeldung -> Neue Anmeldung und wiederholen den Vorgang für den Windowsbenutzer. Klicken sie hierfür auf das Feld durchsuchen und geben sie den Namen des Reportingbenutzers in das Feld ein. Anschließend klicken sie auf Name Prüfen“



8. Klicken sie Anschließend ebenfalls auf Benutzerzuordnung und vergeben die gleichen Berechtigungen wie für den SQL Benutzer.

Ergänzung in der Datei *web.config*

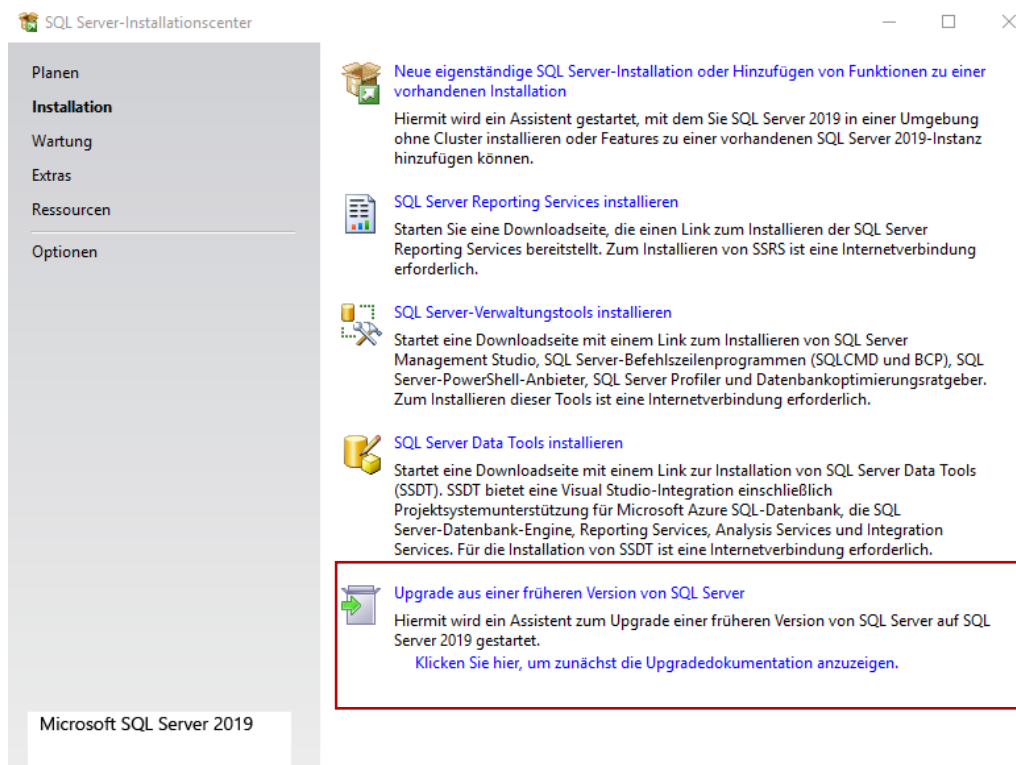


Achtung: Bitte passen Sie in der *web.config* des Reporting Server "C:\Program Files\Microsoft SQL Server\MSRS10_50.MSSQLSERVER\Reporting Services\ReportServer\" folgende Zeile an. Erweitern Sie den Knoten „httpRuntime“ um das Attribut „maxRequestLength“ (300000 = 300MB):
`<httpRuntime executionTimeout="18000" maxRequestLength="300000" />`

Anhang 5: SQL Server Update Installation

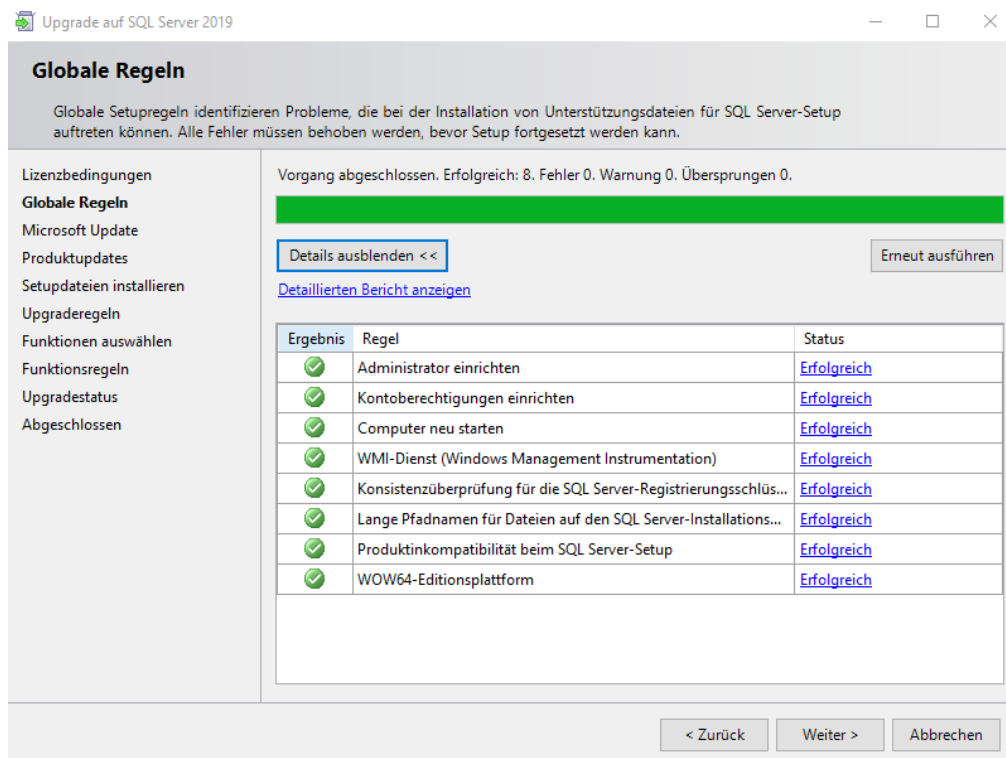
Hinweis: Ein Upgrade auf eine neue SQL Server-Version ist von Zeiten nötig, da Microsoft für die abgekündigten Versionen keine Sicherheitsupdates mehr bereitstellt oder INGRADA Funktionen neuer SQL Versionen benötigt. Ein Upgrade des SQL Servers empfiehlt sich dann, wenn die alte Version nicht mehr benötigt wird. Bitte stimmen Sie dies für einen reibungslosen Datenaustausch vor dem Upgrade mit Ihrem Dienstleister ab.

1. Starten Sie die Datei `sqlxpradv_x64_deu.exe`. Der Inhalt wird entpackt und das Installationscenter startet.
2. Wählen Sie für ein Upgrade eines vorhandenen SQL Servers den Punkt „Upgrade aus einer früheren Version von SQL Server“.



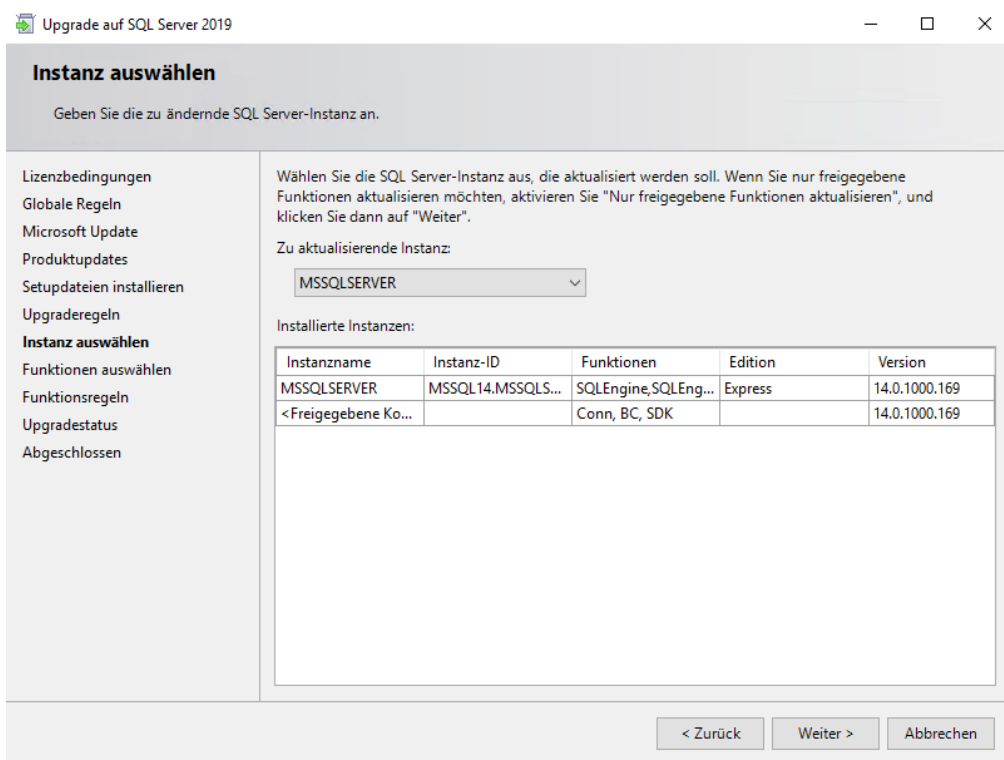
3. Akzeptieren Sie die Lizenzbedingungen und klicken Sie auf *Weiter*.
4. Ein Setup prüft automatisch die Installationsvoraussetzungen und zeigt eventuelle Probleme an, die vor dem Upgrade zu beheben sind.

Hinweis: Es sollten alle Windows und SQL Server Updates der bestehenden Installation gemacht worden sein. Falls eine Installation fehlt, so wird dies angezeigt.

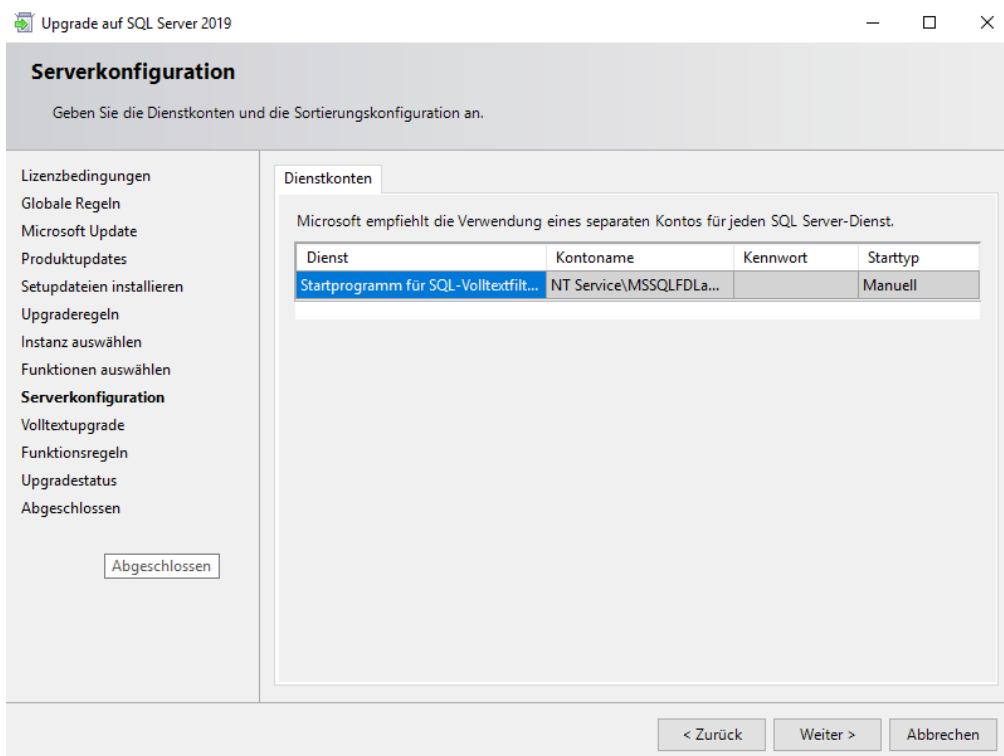


5. Sie haben die Möglichkeit sowohl für Windows als auch für weitere Microsoft-Software, einschließlich dem SQL Server, nach Updates zu suchen:
 1. Möchten Sie nach Updates suchen, setzen Sie ein Häkchen in das Kästchen *Mit Microsoft Update nach Updates suchen*. Klicken Sie anschließend auf *Weiter*. Die Länge des Vorgangs kann je nach Internetverbindung und Umfang der Updates variieren.
 2. Möchten Sie nicht nach Updates suchen, so klicken Sie direkt auf *Weiter*.
6. Im nächsten Schritt wählen Sie die Instanz aus. Prüfen Sie vor jedem Update, ob die richtige Instanz ausgewählt wurde. Klicken Sie dann auf *Weiter*.

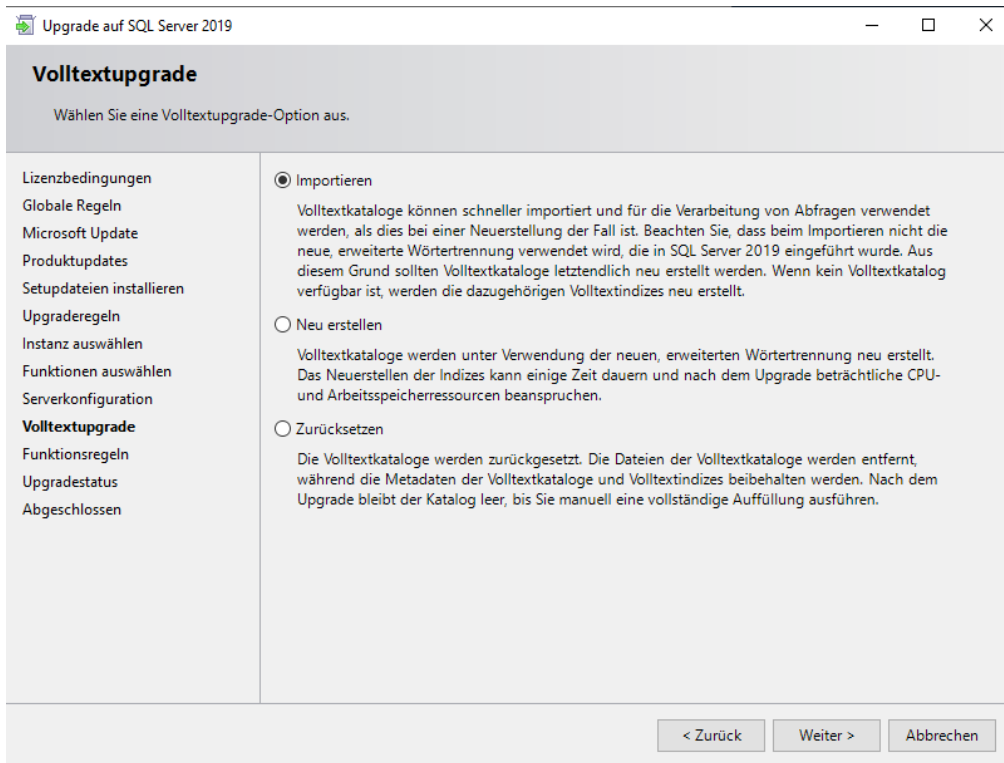
Hinweis: Sollten mehrere Instanzen aktualisiert werden, muss das Setup für jede Instanz erneut ausgeführt werden!



7. Bestätigen Sie dieses Fenster mit *Weiter*.

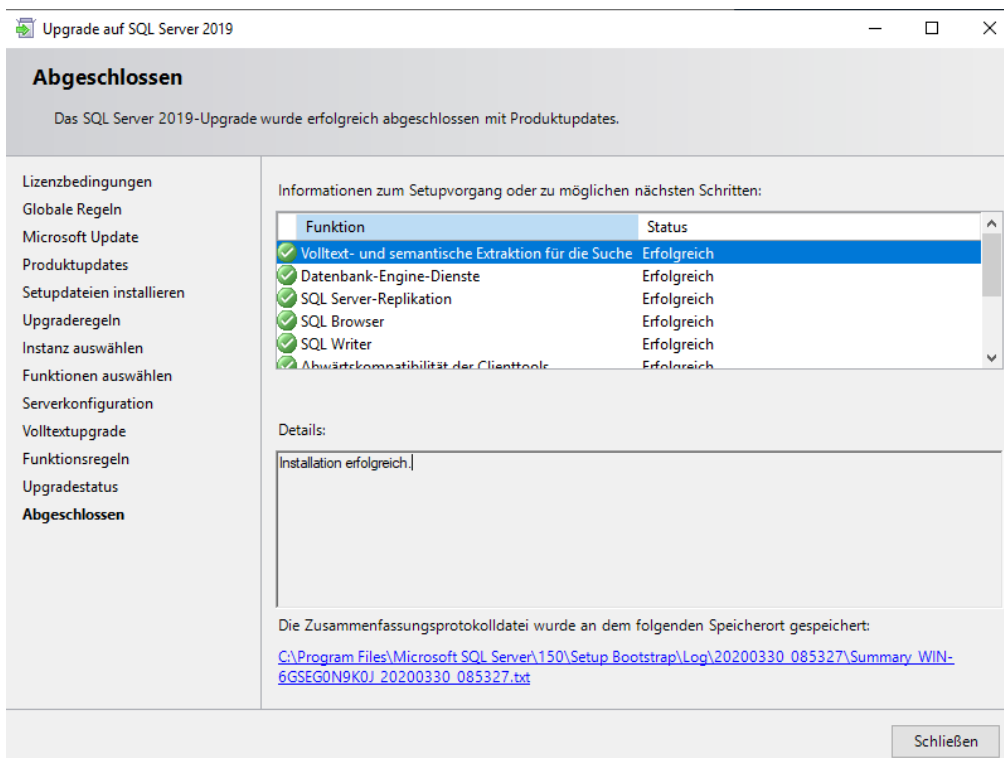


8. In diesem Fenster übernehmen Sie die Voreinstellung. Klicken Sie dann auf *Weiter*.



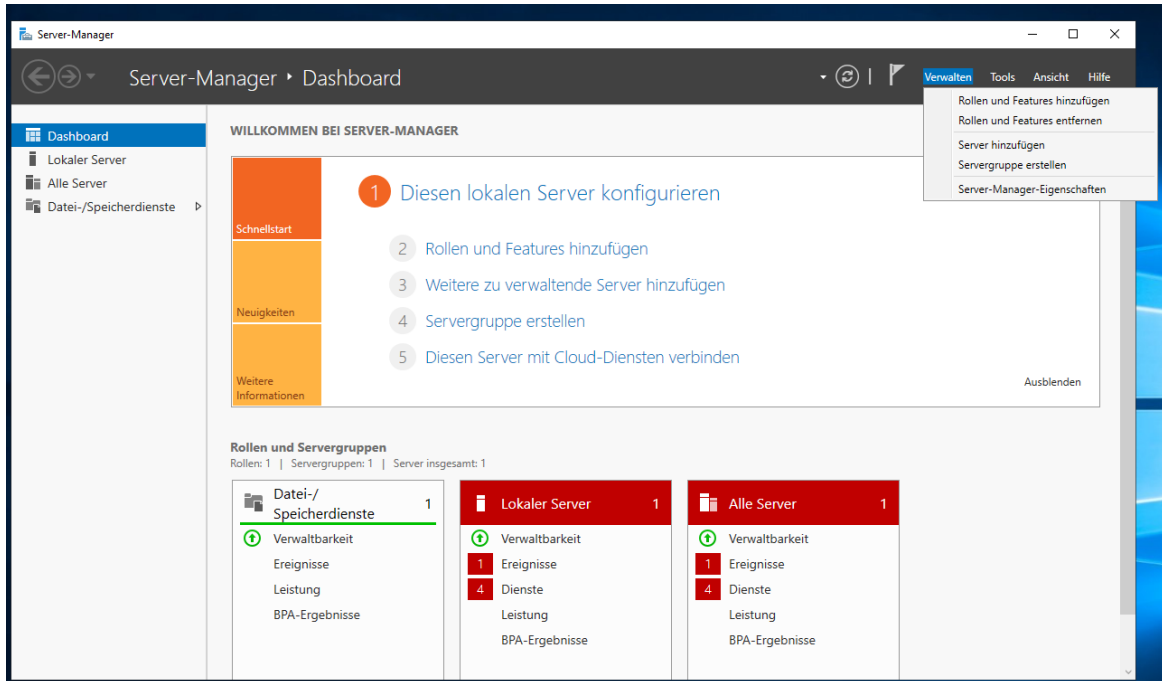
9. Das Upgrade wird nun ausgeführt.

10. Die Installation ist nun beendet. Die Zugangsdaten und Kennwörter haben sich nicht geändert.

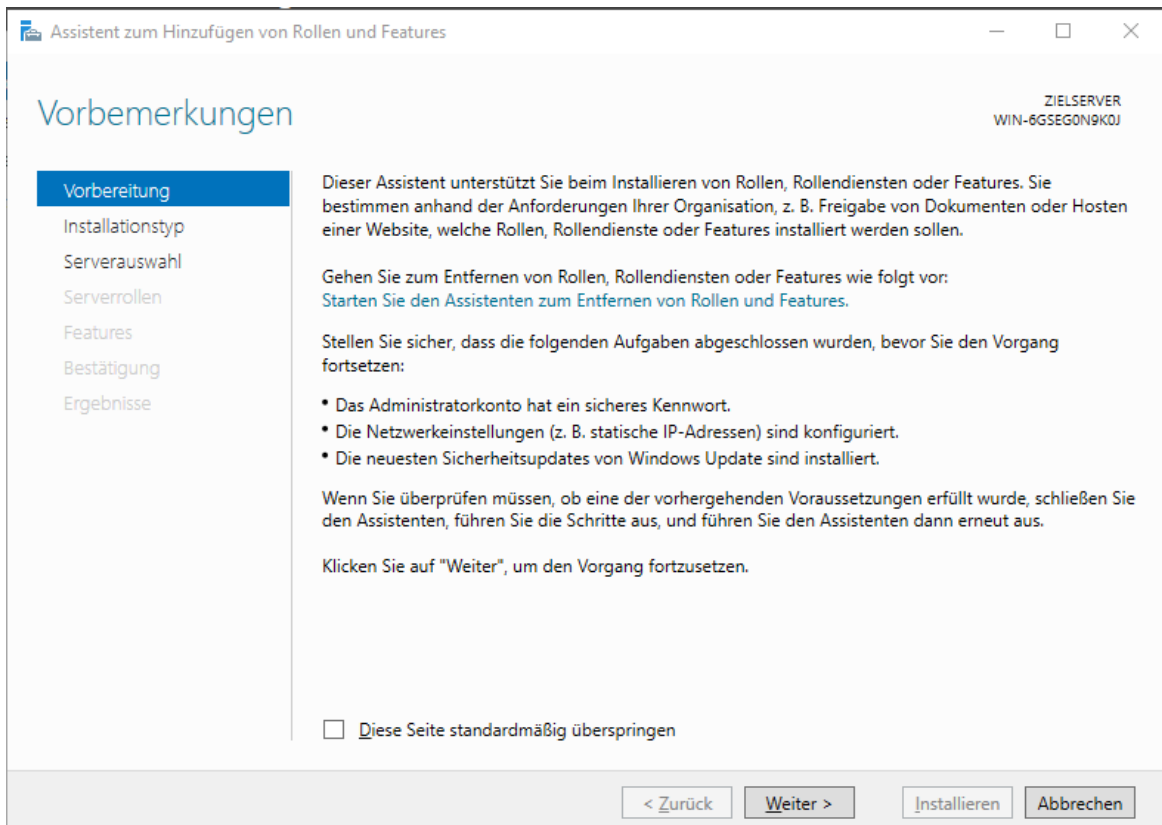


Anhang 6: Installation von IIS 10 auf Windows Server 2019

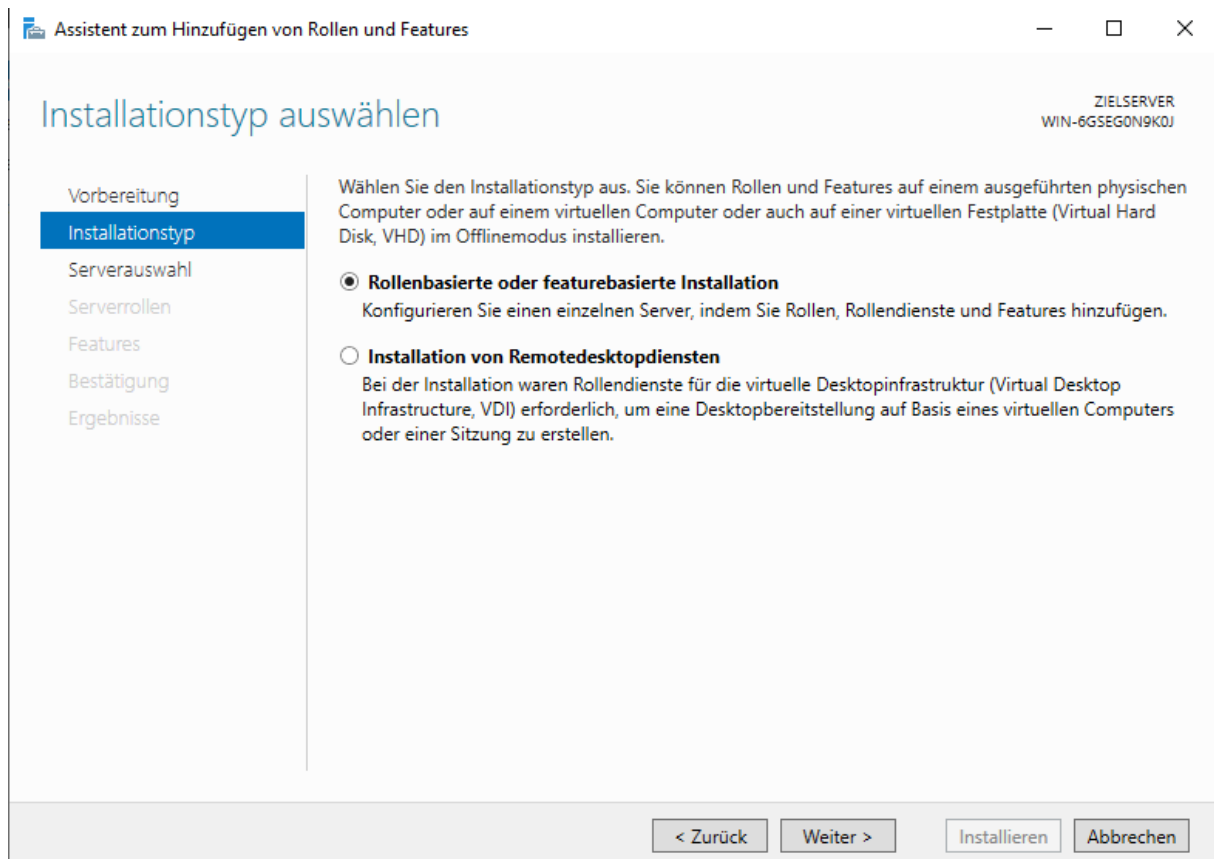
Bitte gehen sie wie beschreiben vor, um IIS 10 auf Ihrem Windows Server 2019. Zu installieren. Die Installation ist ähnlich wie bei Windows Server 2012



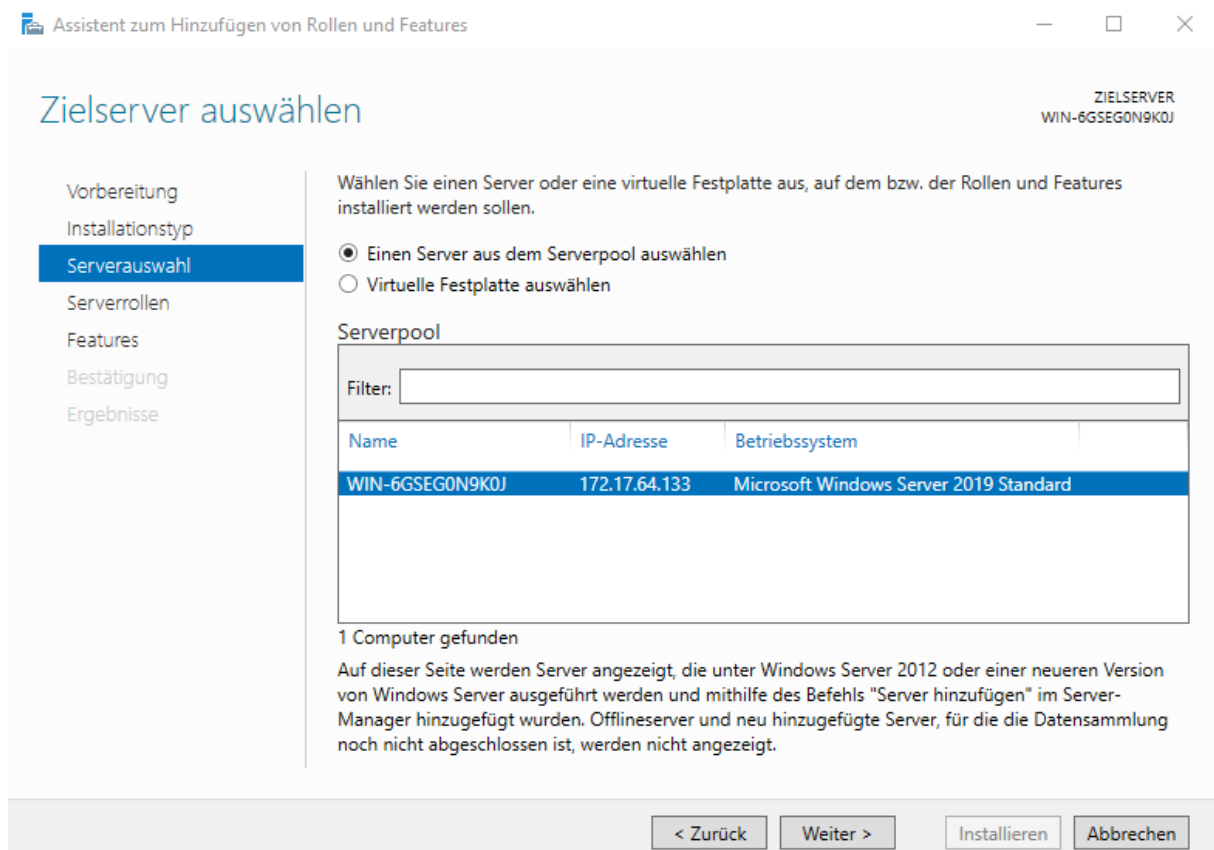
Im Servermanager klicken sie auf Verwaltung – Rollen und Features Hinzufügen



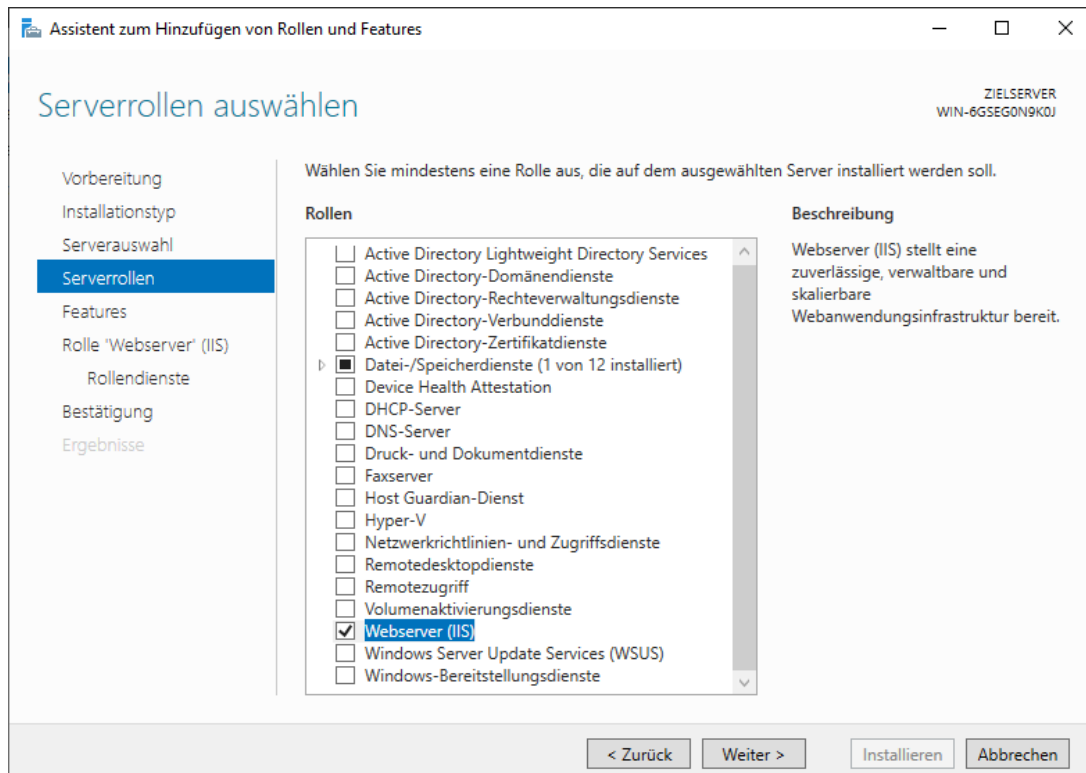
Diese Seite mit Weiter Überspringen



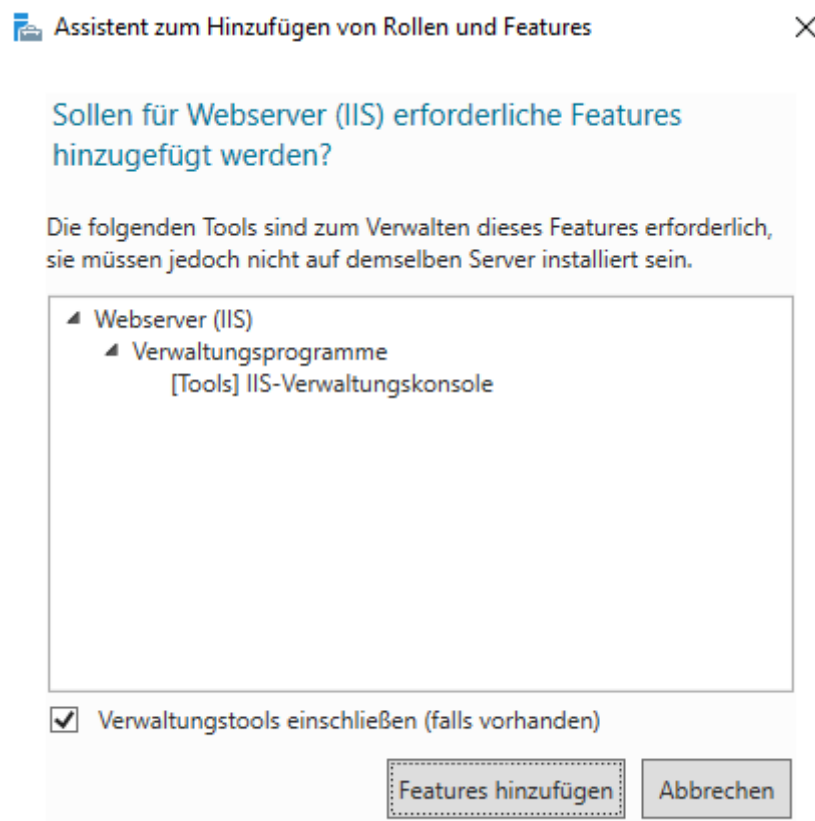
Mit Weiter bestätigen



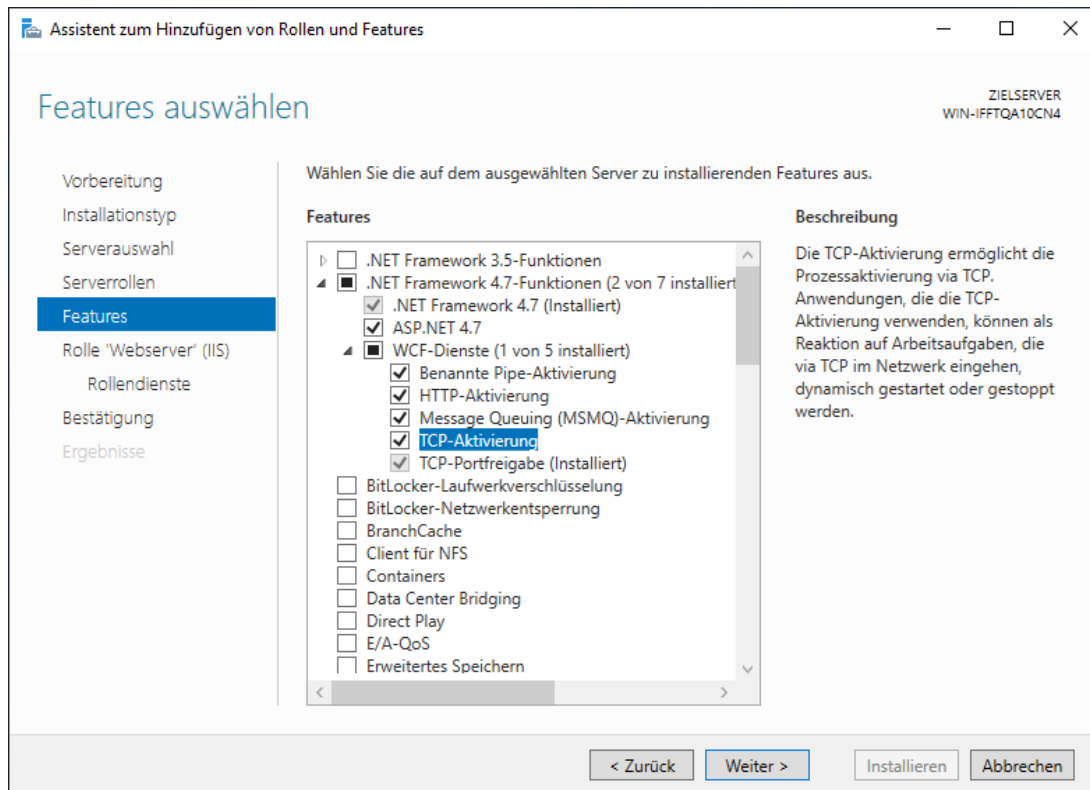
Wir wollen auf dem lokalen Server Installieren die Auswahl ist richtig. Wen Mehrere Server zur Auswahl stehen, bitte den Namen prüfen. Mit Weiter bestätigen



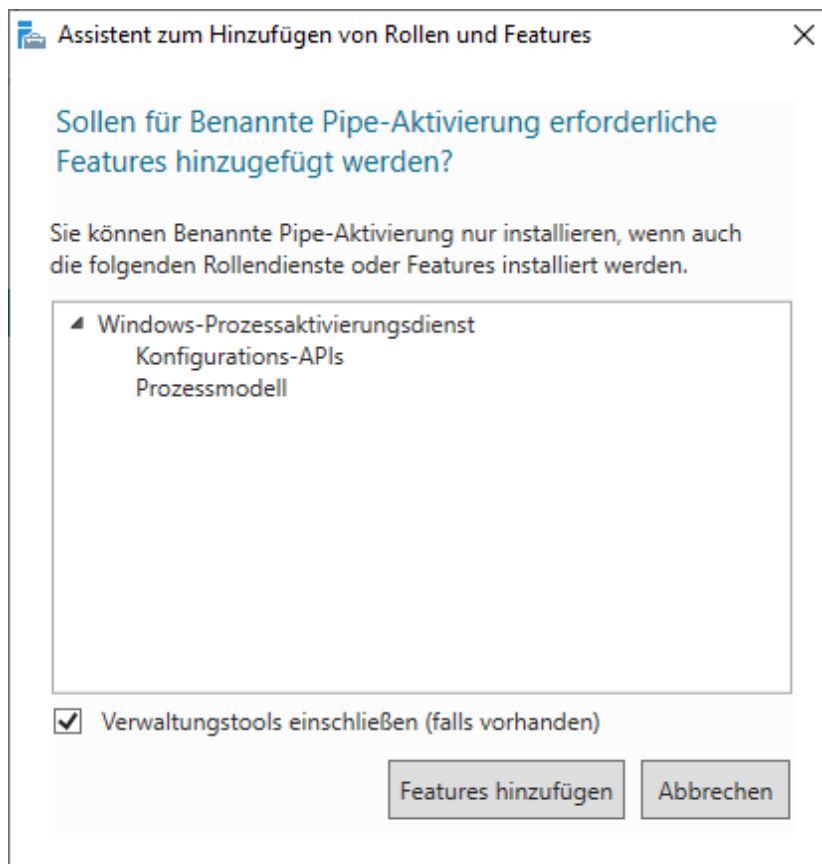
Bitte die Rolle Webserver (IIS) auswählen. Es Öffnet sich ein neues Fenster



Fügen sie dieses Feature hinzu.



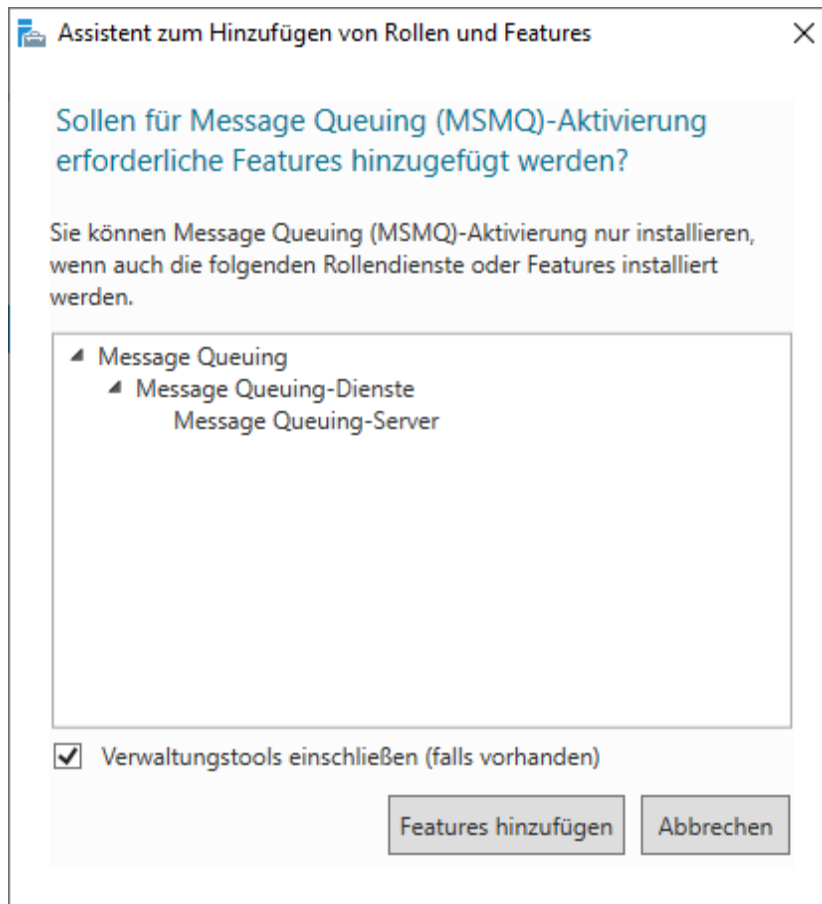
Aktivieren sie .net Framework 4.7 und klicken Sie auf Weiter.



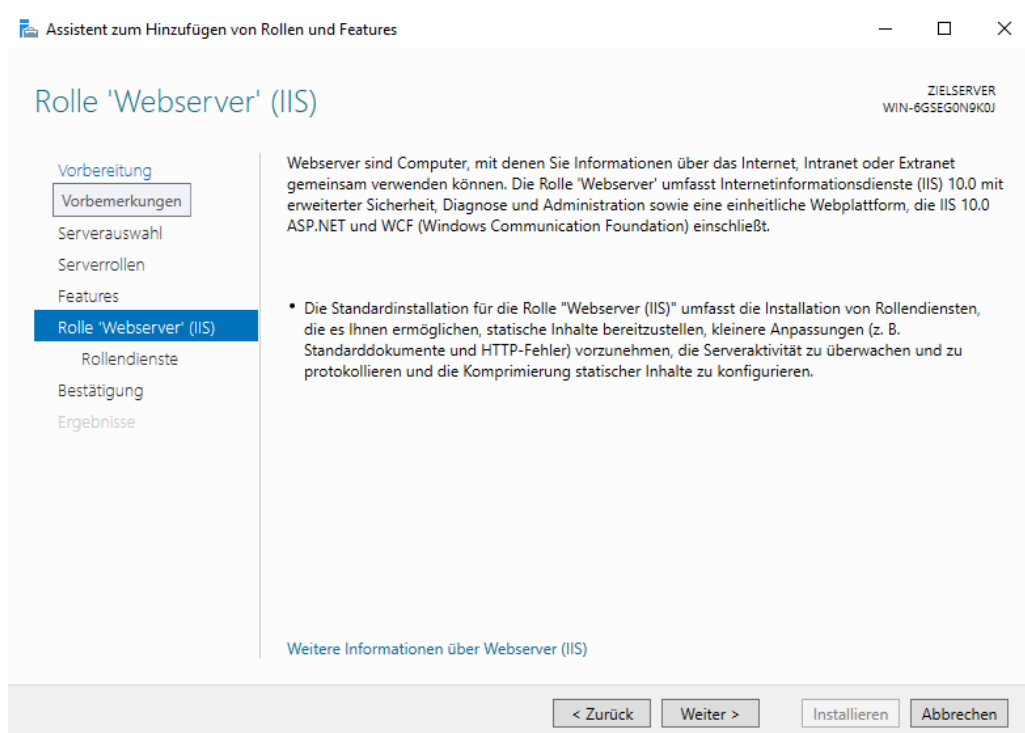
Bestätigen Sie den Dialog mit *Feature hinzufügen*.



Bestätigen Sie den Dialog mit *Feature hinzufügen*.



Bestätigen Sie den Dialog mit *Feature hinzufügen*.



Mit Weiter bestätigen.

Rollendienste auswählen

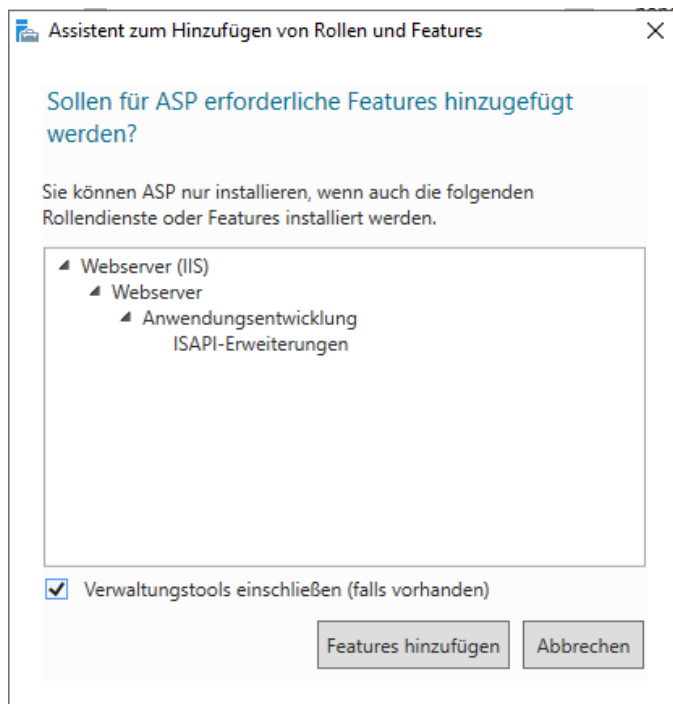
- Vorbereitung
- Installationstyp
- Serverauswahl
- Serverrollen
- Features
- Rolle "Webserver" (IIS)
- Rollendienste**
- Bestätigung
- Ergebnisse

Wählen Sie die Rollendienste aus, die für "Webserver (IIS)" installiert werden müssen.

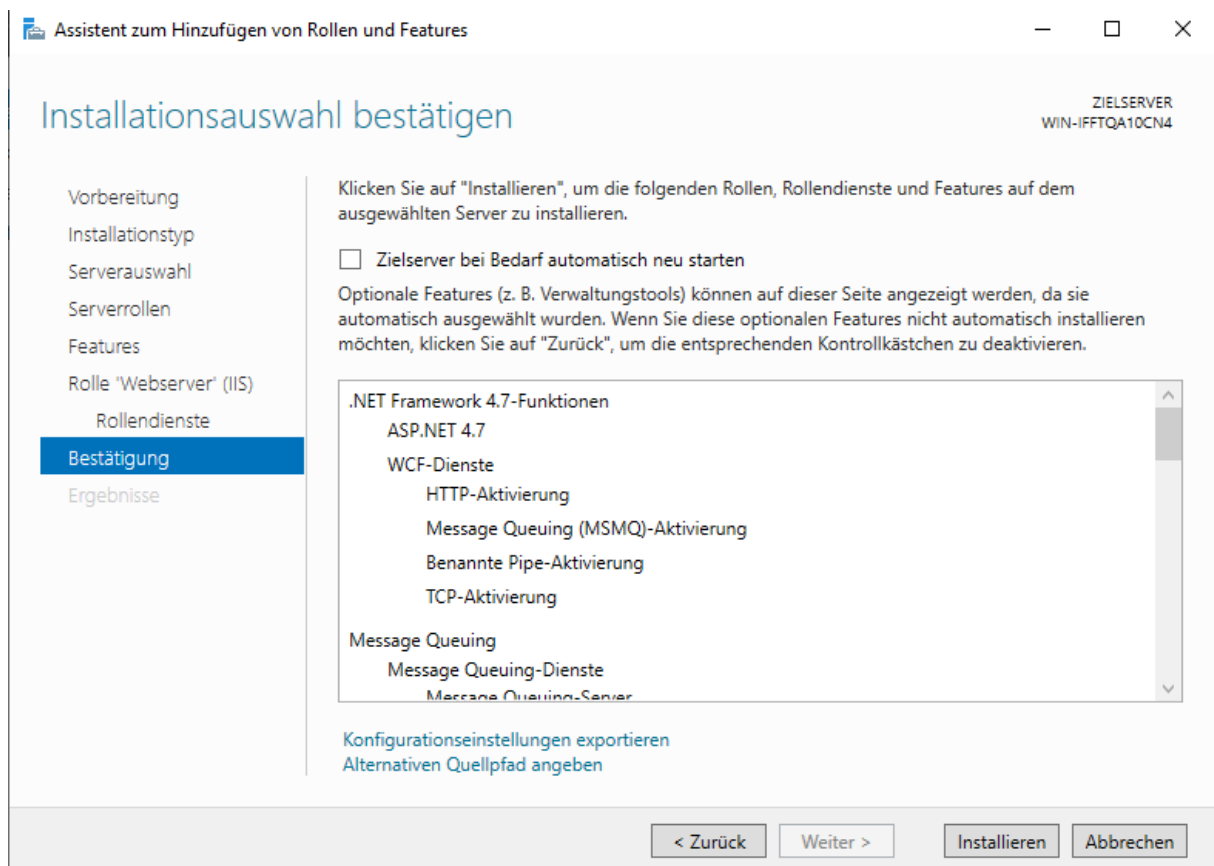
Rollendienste

- Webservers
 - Allgemeine HTTP-Features
 - HTTP-Fehler
 - Standarddokument
 - Statischer Inhalt
 - Verzeichnis durchsuchen
 - HTTP-Umleitung
 - WebDAV-Veröffentlichung
 - Leistung
 - Komprimierung statischer Inhalte
 - Komprimieren dynamischer Inhalte
 - Sicherheit
 - Anforderungsfilterung
 - Authentifizierung über Clientzertifikatzuordnung
 - Authentifizierung über IIS-Clientzertifikatzuordnung
 - Digestauthentifizierung
 - IP- und Domäneneinschränkungen
 - Standardauthentifizierung
 - Unterstützung zentraler SSL-Zertifikate
 - URL-Autorisierung
 - Windows-Authentifizierung
 - Systemzustand und Diagnose
 - HTTP-Protokollierung
 - Ablaufverfolgung
 - Anforderungsüberwachung
 - Benutzerdefinierte Protokollierung
 - ODBC-Protokollierung
 - Protokollierungstools
 - Anwendungsentwicklung
 - .NET-Erweiterbarkeit 3.5
 - .NET-Erweiterbarkeit 4.7
 - Anwendungsinitialisierung
 - ASP
 - ASP.NET 3.5
 - ASP.NET 4.7
 - CGI
 - ISAPI-Erweiterungen
 - ISAPI-Filter
 - Serverseitige Include-Dateien
 - WebSocket-Protokoll
- FTP-Server
- Verwaltungsprogramme
 - IIS-Verwaltungskonsole
 - IIS-Verwaltungsskripts und -tools
- Kompatibilität mit der IIS 6-Verwaltung
 - Verwaltungsdienst

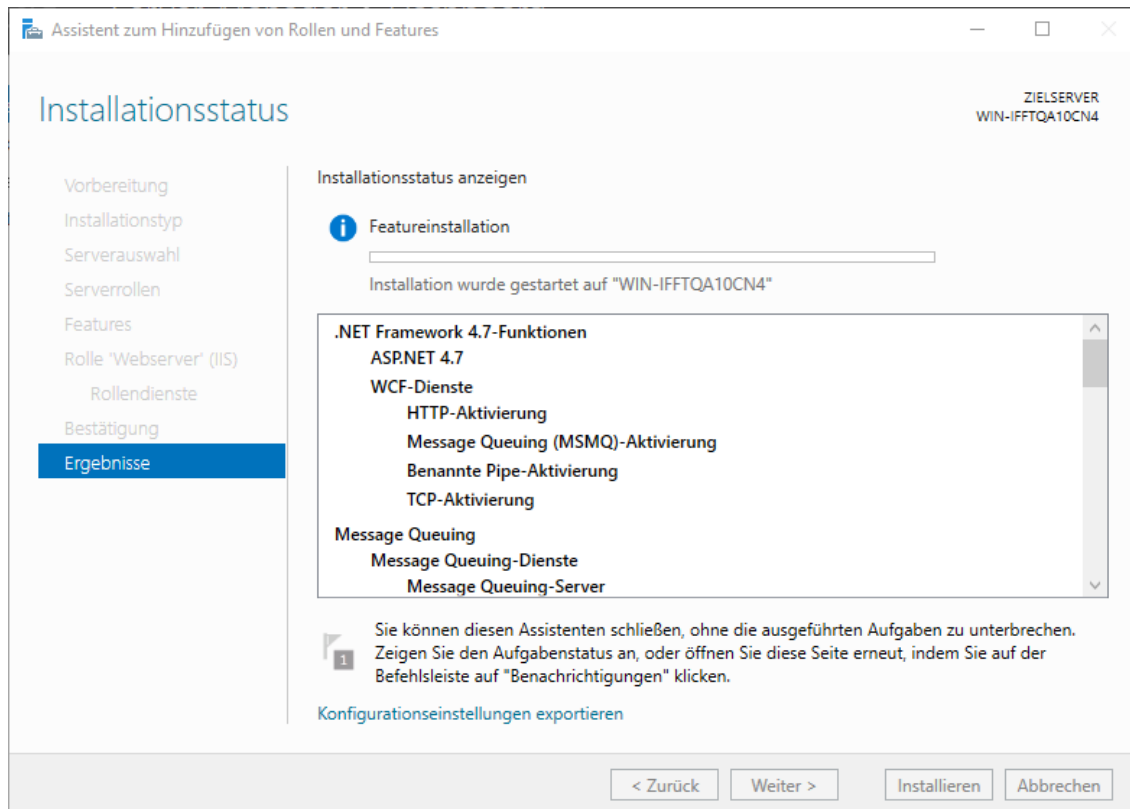
In diesem Fenster wählen sie bitte die Funktionen wie im Bild zu sehen aus. Dabei erscheint ein Fenster (siehe unten) welches sie mit Feature Hinzufügen bestätigen. Anschließend mit Weiter bestätigen.



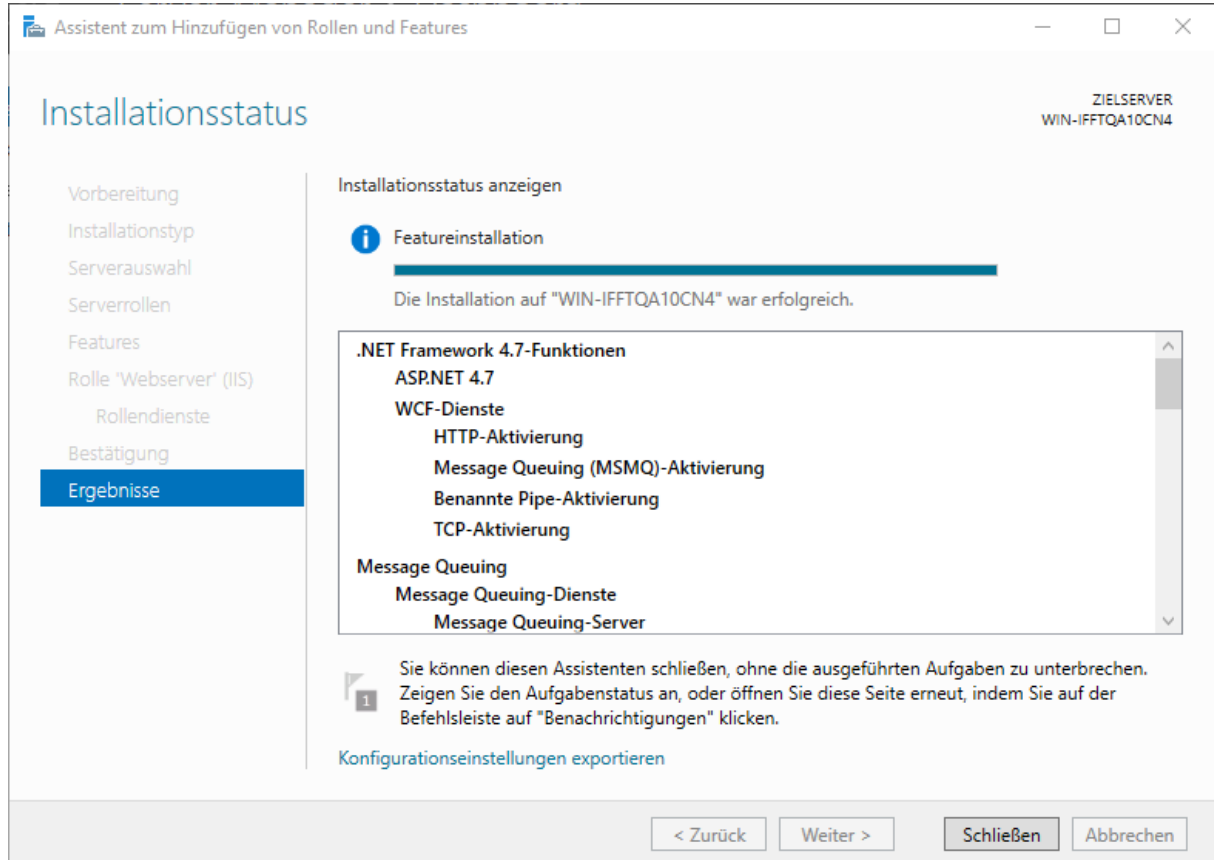
Bestätigen Sie den Dialog mit *Features hinzufügen*.



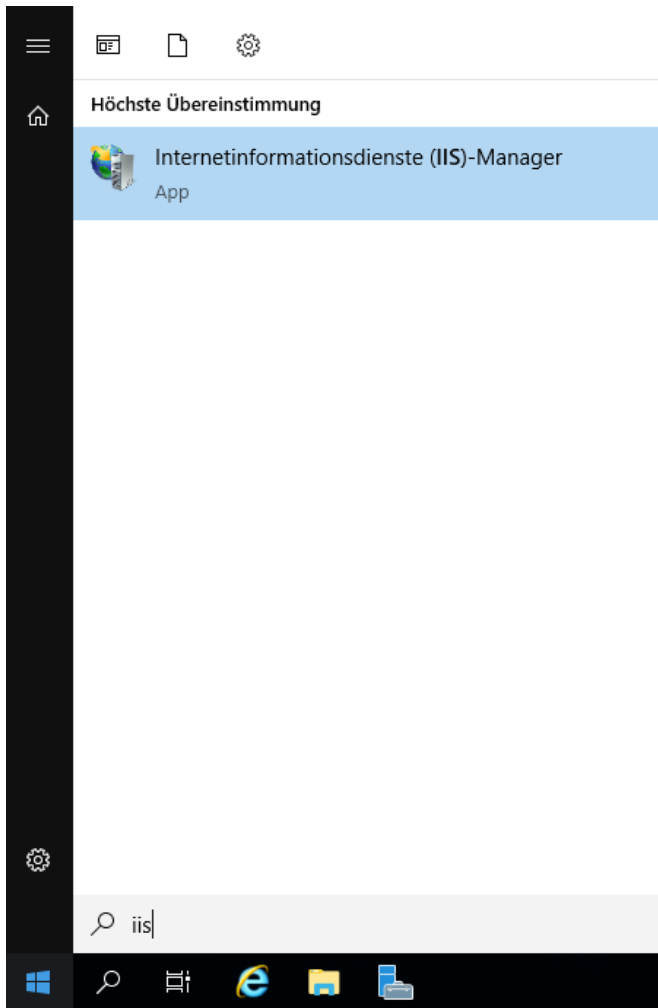
Starten Sie die Installation mit *Installieren*.



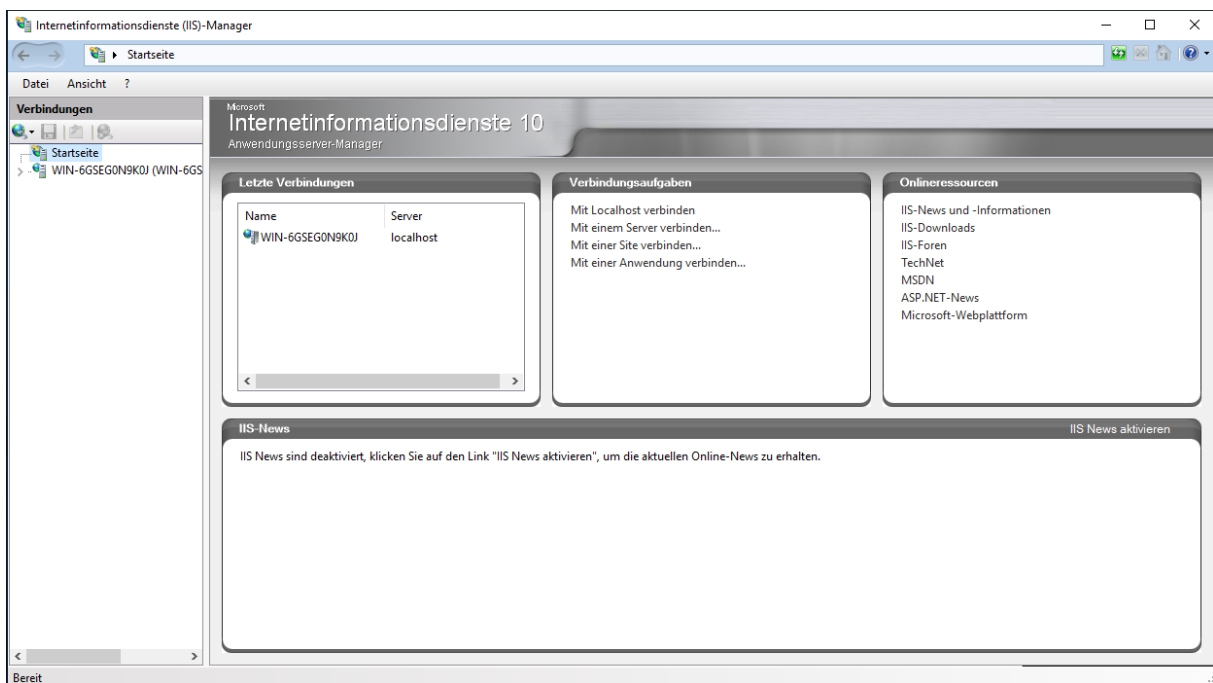
Die Installation wurde gestartet.



Beenden Sie den Dialog nach erfolgreicher Installation mit *Schließen*.



Starten Sie den Internetinformationsdienste (IIS)-Manager.



Herzlich willkommen im IIS 10

Anhang 7: Zusatzpakete Installieren für IIS Installieren

Webplattform-Installer 5.0

- □ ×



Webplattform-Installer 5.0



Nun muss noch das Zusatzpaket IISrewrite für den IIS installiert werden. Mit Doppelklick auf die Exe starten.

Webplattform-Installer 5.0

- □ ×

URL Rewrite 2.0



URL Rewrite 2.0 für IIS 7 verfügt über das regelbasierte Umschreiben von URLs hinaus jetzt über eine neue Unterstützung für ausgehende Umschreiberegeln und eine neue Funktion zum Festlegen von HTTP-Anforderungsheadern und IIS-Servervariablen. Aufgrund dieser neuen Funktionen haben Administratoren die vollständige Kontrolle über die URL-Struktur, die von vorhandenen Webanwendungen oder Legacy-Webanwendungen verwendet wird, die nicht so geändert werden können, dass sie eigene Unterstützung für benutzer- und suchmaschinenfreundliche URLs bieten.

[Weitere Informationen](#)[Herausgeber: Microsoft](#)

Downloadgröße: 5,80 MB

Version: 2.1

Veröffentlichungsdatum: Freitag, 16. Juni 2017

1 [Zu installierende Elemente](#)[Optionen](#)[Installieren](#)[Beenden](#)

Zur Installation muss den Server mit dem Internet verbunden sein.

Webplattform-Installer 5.0 ×

VORAUSSSETZUNG Installieren Konfigurieren Fertig stellen

Prüfen Sie folgende Liste mit zu installierender Drittanbieter-Anwendungssoftware, Microsoft-Produkten und -Komponenten, die zusätzliche unten aufgeführte Software sowie die zu aktivierenden Windows-Komponenten. Drittanbieteranwendungen und -produkte werden von den hier aufgeführten Drittanbietern angeboten; Microsoft gewährt Ihnen keine Rechte an der Drittanbietersoftware. Sie sind selbst dafür verantwortlich, die Lizenzbedingungen der Drittanbieter aufzufinden, zu lesen und zu akzeptieren.

✗ **URL Rewrite 2.0**
[Lizenzbedingungen anzeigen](#) [Direkter Downloadlink](#)
Dateidownloadgröße insgesamt: **5,8 MB**

[Klicken Sie hier, um weitere Software anzuzeigen, die installiert werden muss, und überprüfen Sie die zugehörigen Microsoft-Lizenzbedingungen.](#)

Indem Sie auf "Ich stimme zu" klicken, akzeptieren Sie die Lizenzbedingungen für die oben aufgeführte Drittanbieter- und Microsoft-Software sowie die zusätzliche Software. Wenn Sie den Lizenzbedingungen nicht zustimmen, klicken Sie auf "Ich stimme nicht zu".

Klicken Sie auf *Ich stimme zu*, um die Installation zu starten.

Webplattform-Installer 5.0 ×

VORAUSSSETZUNG **Installieren** Konfigurieren Fertig stellen

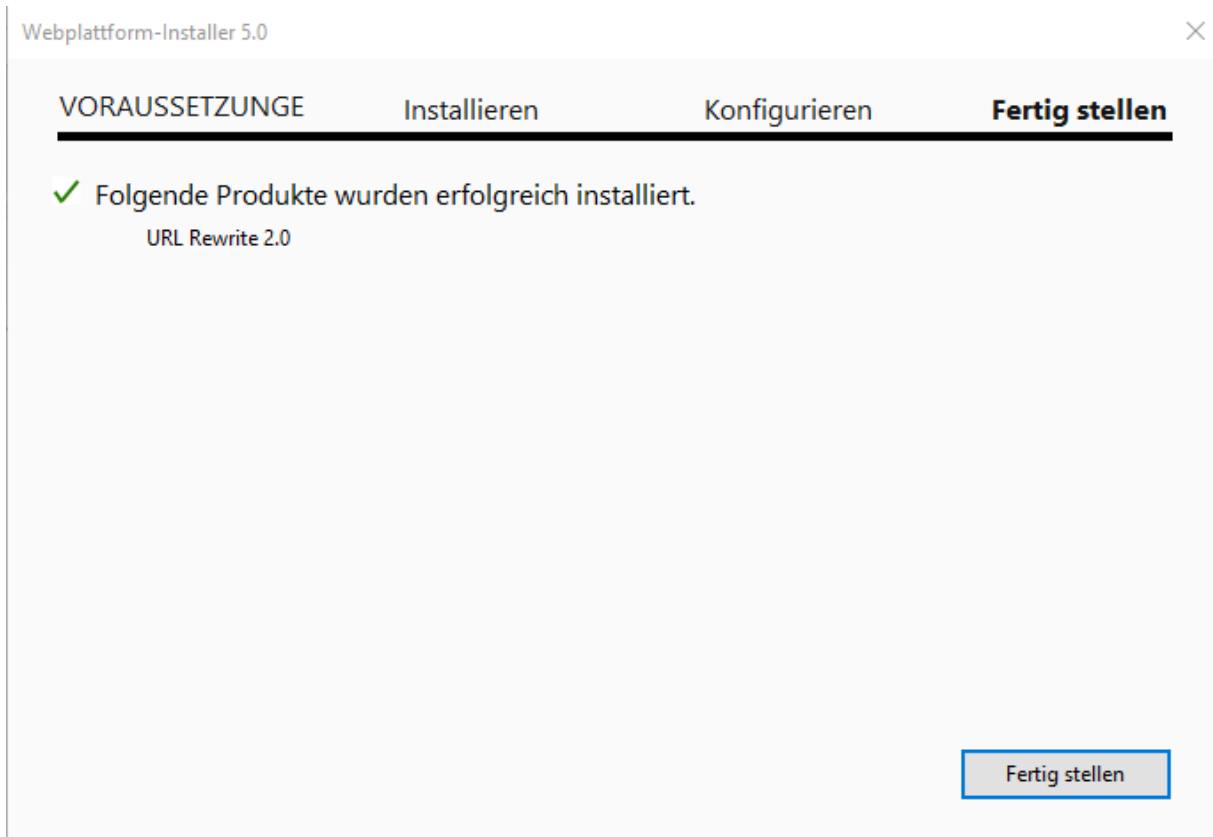
N/A

Microsoft Azure

Microsoft Azure is an open and flexible cloud platform that enables you to quickly build, deploy and manage applications across a global network of Microsoft-managed datacenters. Easily create web sites, virtual machines or databases in a few clicks.
[Try it free now!](#)

Download beendet

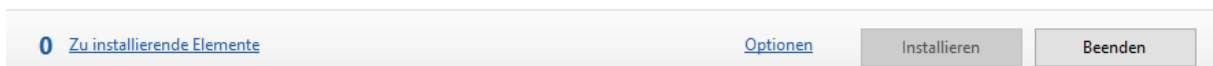
Installationsstatus: URL Rewrite 2.0 wird installiert [1 von 1]

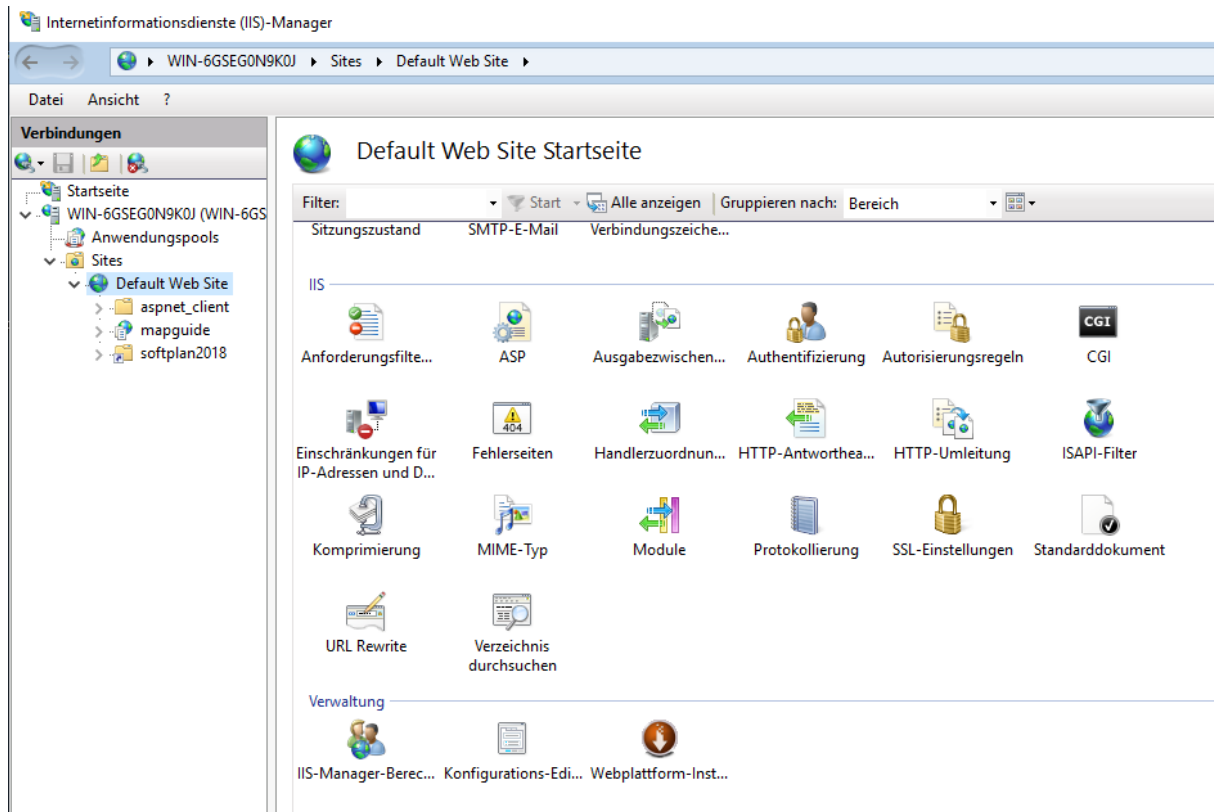


Die Installation ist abgeschlossen.



Es sind keine zu installierenden Produkte oder Anwendungen vorhanden.





Nach erfolgreicher Installation befindet sich unter der *Default Web Site* eine neue Option *URL Rewrite*.

Anhang 8: Installation und Konfiguration von AIMS 2017

Hinweis: Bitte laden sie, vor der Installation von AIMS2017, die neue Installationsdatei für Windows Server 2016 herunter und benutzen Sie diese für Windows Server 2016 und höher. Kopieren sie dazu die neue Setup-Datei in das Installationsverzeichnis von AIMS2017.

Im Anschluss ersetzen sie bitte die Dateien im Programmverzeichnis mit den Dateien aus dem TFS151100.zip. Dies erhöht die Stabilität vom AIMS2017.



The screenshot shows a web browser window with the URL <https://www.ingrada.de/autodesk.html>. The navigation menu includes: NEWS, PRODUKT, UNTERNEHMEN, PARTNER, SERVICE, KONTAKT, IMPRESSUM, LOGIN BEREICH. The sub-menu includes: Service News, Downloads, Uploads, Demo, Partnerinfos, Entwicklerportal, Benutzerkonto. The main heading is "DOWNLOADS". Below it, there is a text block: "Auf dieser Seite stehen die aktuellen Installationsarchive zum Download bereit. Produkt-DVDs für INGRADA web und INGRADA Desktop senden wir Ihnen auf Anfrage zu. Senden Sie uns hierzu eine E-Mail an Bestellpostfach." To the right is a download icon. Below this is a filter bar with buttons: INGRADA web, INGRADA Desktop, INGRADA 4.14, AKIA, HHK, Autodesk (selected), Dokumente. The main content area has a blue header "AIMS 2017". There are two entries:

File Name	Date
install_AIMS2017_on_WinServer2016.zip install_AIMS2017_on_WinServer2016.zip (168,53 KiB)	12.08.2019
TFS151100.zip TFS151100.zip (646,94 KiB)	12.08.2019

Beschreibung
Mit diesem Hotfix stellt Autodesk die Dateien für die Installation von AIMS 2017 unter Windows Server 2016 bereit.

Hinweis
Ausführliche Installationsanleitung unter:
<https://knowledge.autodesk.com/de/search-result/caas/sfdcarticles/sfdcarticles/DEU/Support-von-Windows-Server-2016.html>

Beschreibung
Dieses Hotfix behebt Probleme mit mit Programmabstürzen in Autodesk Infrastructure Map Server 2017 bei einer großen Anzahl

Installation des Infrastructure Map Servers

Gehen Sie folgendermaßen vor, um AIMS zu installieren:

1. Entpacken Sie den AIMS Download und öffnen Sie die Datei *setup.exe*.

2. Wählen Sie *Installieren* aus:

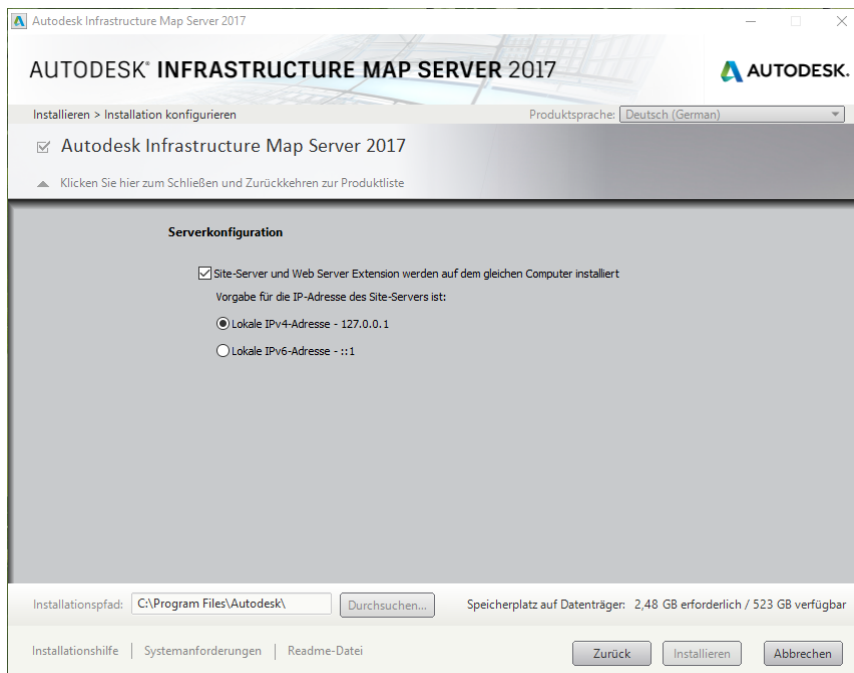


3. Akzeptieren Sie die Lizenzvereinbarung.

4. Klicken Sie auf den Pfeil zum Öffnen und Konfigurieren von „Autodesk Infrastructure Web Server 2017“:



5. Wählen Sie unter „Autodesk Infrastructure Web Server 2017“ die Komponenten wie in der folgenden Abbildung aus. Setzen Sie hierzu Häkchen in den Checkboxes. Durch einen Klick auf *Durchsuchen* können Sie ggf. den Installationspfad anpassen.



Klicken Sie auf „Zurück“ und öffnen Sie die Einstellungen für „Autodesk Infrastructure Web Server Extensions 2017“.

6. Nehmen Sie unter „Autodesk Infrastructure Web Server Extensions 2017“ die Einstellungen für die ausgewählten Komponenten vor, wie in der folgenden Abbildung dargestellt:



Klicken Sie auf „Zurück“ und öffnen Sie die Einstellungen für „Autodesk Infrastructure Studio 2017“.



7. Klicken Sie auf „Zurück“ und dann auf *Installieren*, um die Installation zu starten.



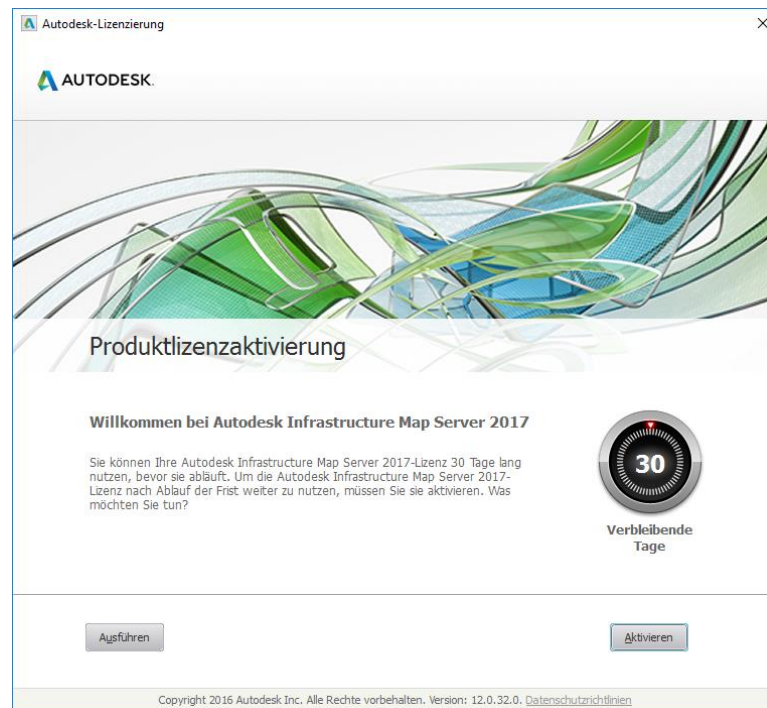
Klicken Sie nach erfolgter Installation auf „Fertig stellen“, um die Installation abzuschließen.

Autodesk Infrastructure Map Server 2017 lizenzieren

Um AIMS 2017 freizuschalten, öffnen Sie den «Autodesk Infrastructure Map Server 2017 Licencing Activator» :

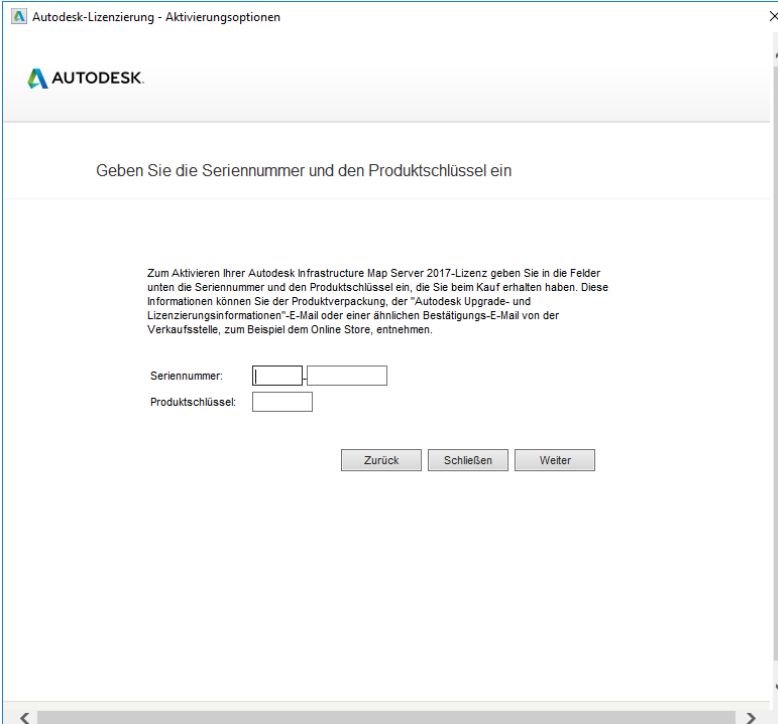


Klicken Sie auf „Seriennummer eingeben“ bzw. „Netzwerklicenz verwenden“ und akzeptieren Sie die Autodesk Datenschutzrichtlinien.



Wählen Sie „Aktivieren“, um AIMS 2017 zu lizenzieren. Über die Schaltfläche „Ausführen“ können Sie die Version 30 Tage lang nutzen, bevor sie abläuft.

Geben Sie Ihre Seriennummer und den Produktschlüssel ein, um die Lizenzierung abzuschließen.

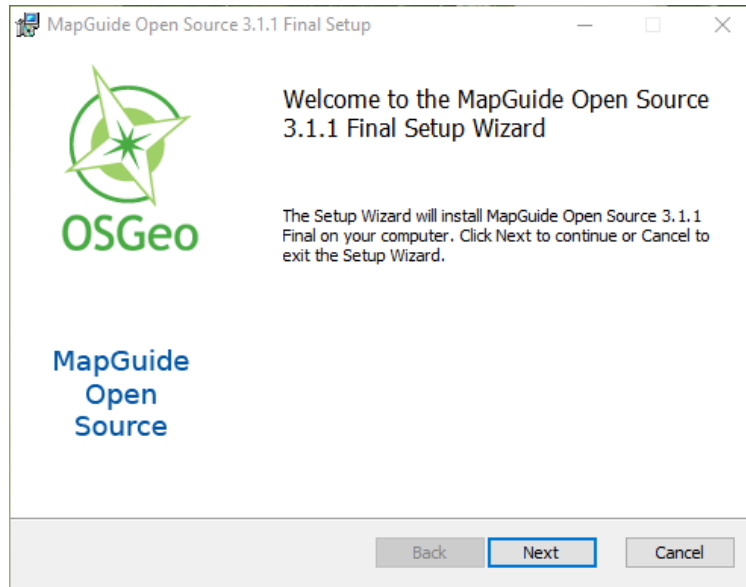


The screenshot shows a dialog box titled "Autodesk-Lizenzierung - Aktivierungsoptionen". At the top left is the Autodesk logo. Below it, the text reads "Geben Sie die Seriennummer und den Produktschlüssel ein". A paragraph of instructions follows: "Zum Aktivieren Ihrer Autodesk Infrastructure Map Server 2017-Lizenz geben Sie in die Felder unten die Seriennummer und den Produktschlüssel ein, die Sie beim Kauf erhalten haben. Diese Informationen können Sie der Produktverpackung, der 'Autodesk Upgrade- und Lizenzierungsinformationen'-E-Mail oder einer ähnlichen Bestätigungs-E-Mail von der Verkaufsstelle, zum Beispiel dem Online Store, entnehmen." Below this text are two input fields: "Seriennummer:" followed by two adjacent text boxes, and "Produktschlüssel:" followed by a single text box. At the bottom of the dialog are three buttons: "Zurück", "Schließen", and "Weiter".

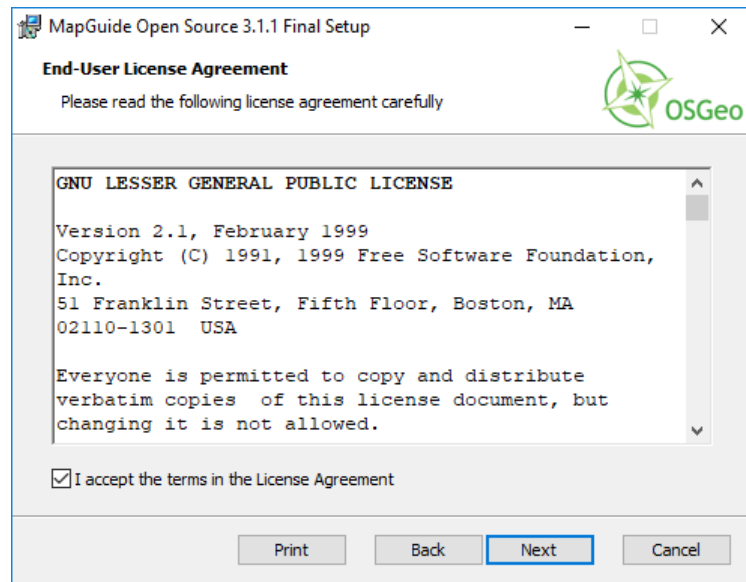
Lizenzierung von AIMS 2017. Der Produktschlüssel lautet 796i1

Anhang 9: Installation von MapGuide Open Source 3.1.1

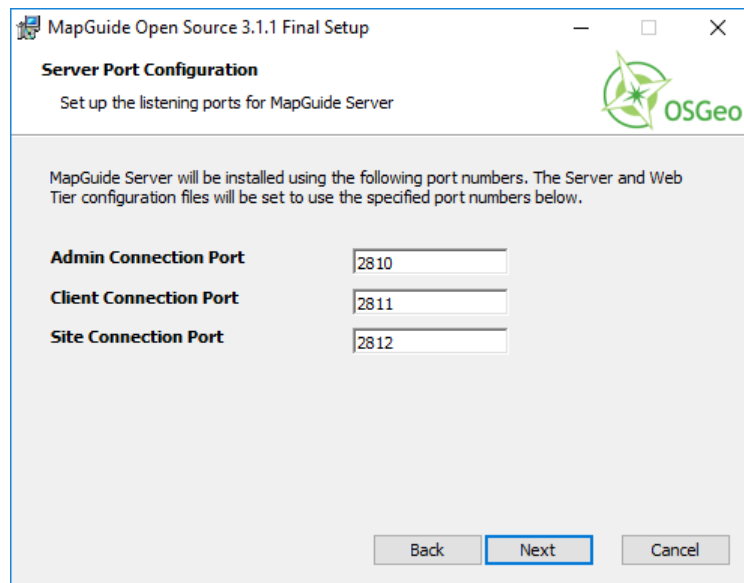
Starten Sie das Installationsarchiv „MapGuideOpenSource-3.1.1.9378-Final-x64.exe“. Neuere Versionen werden nicht unterstützt.



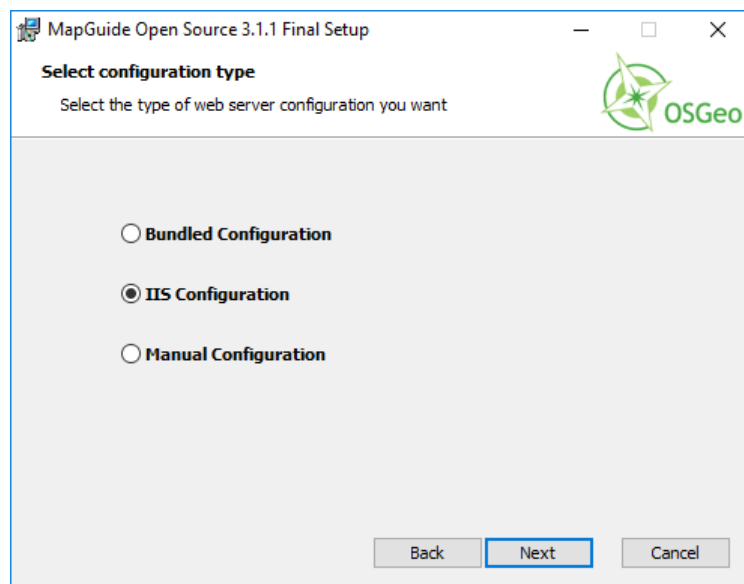
Wählen Sie „Next“ und folgen Sie den Anweisungen auf dem Bildschirm. Wählen Sie die in den folgenden Abbildungen gezeigten Einstellungen:



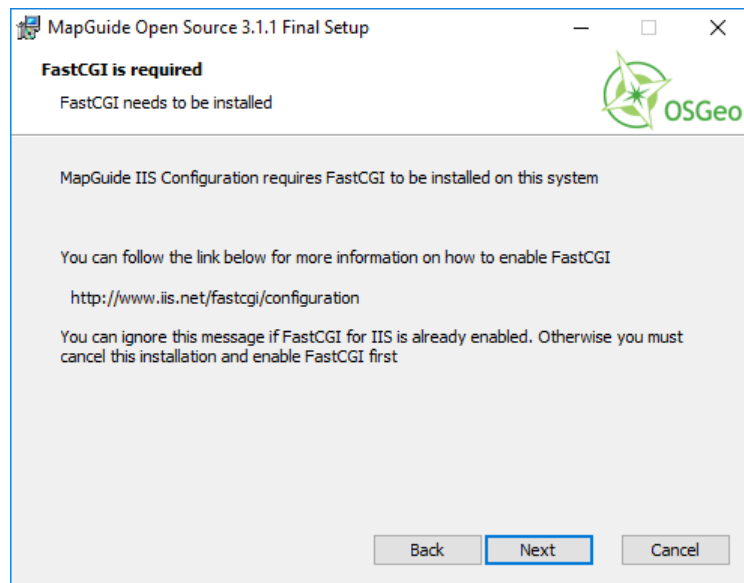
Lizenzbestimmungen akzeptieren.



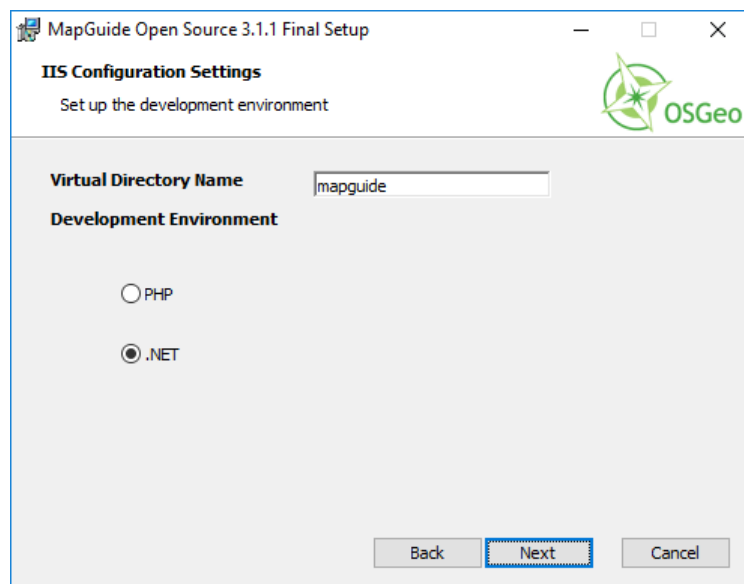
Porteinstellungen übernehmen.



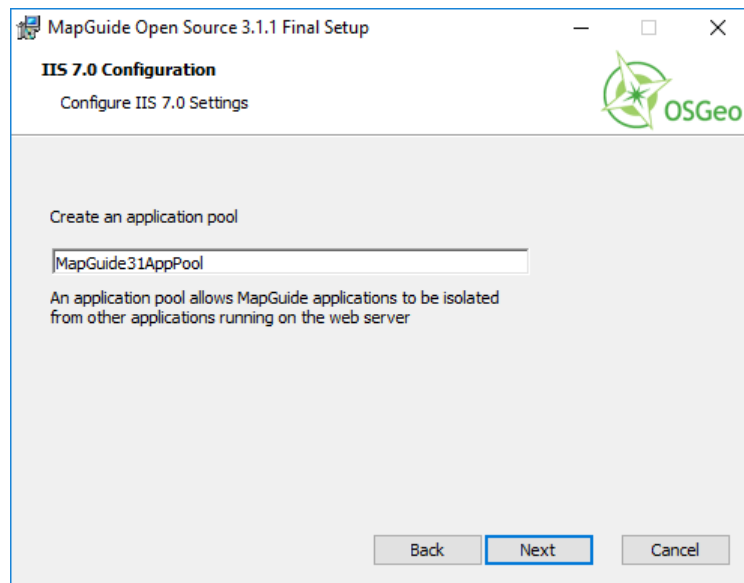
IIS-Konfiguration auswählen.



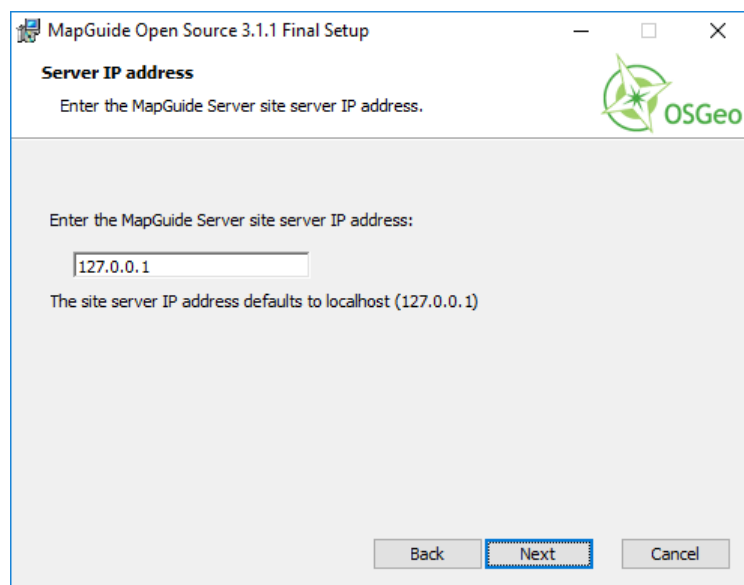
FastCGI muss installiert sein.



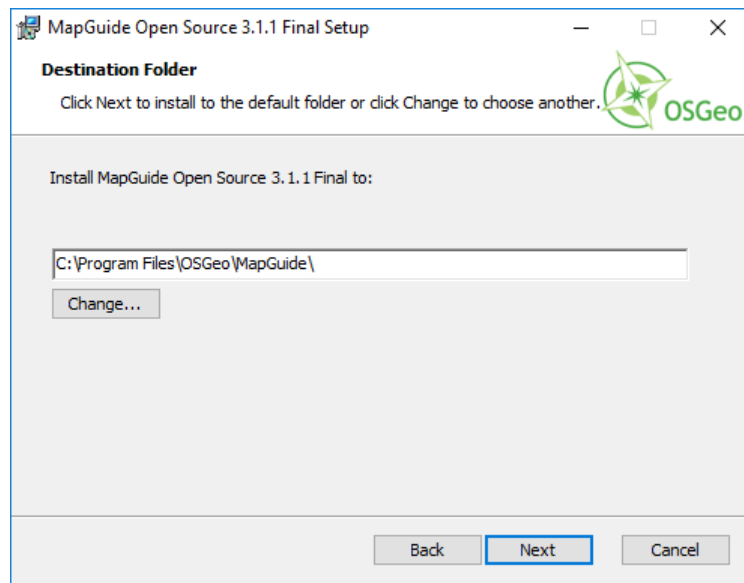
.NET Konfiguration auswählen.



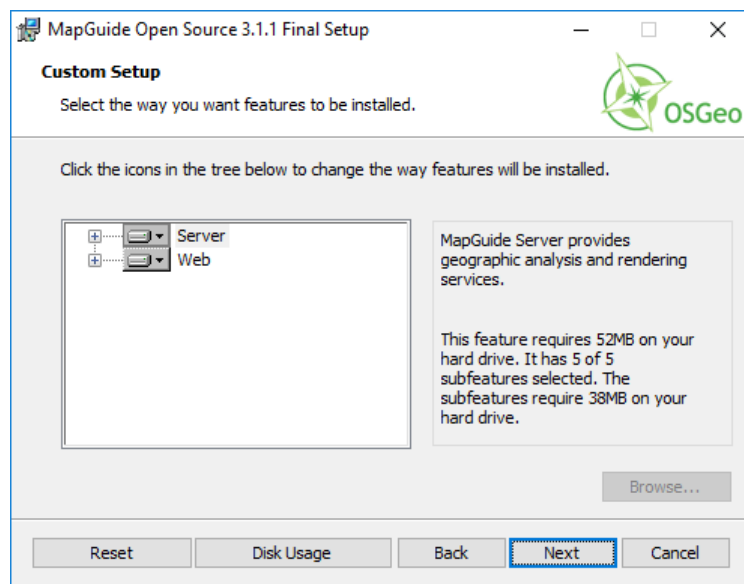
MapGuide Application Pool anlegen.



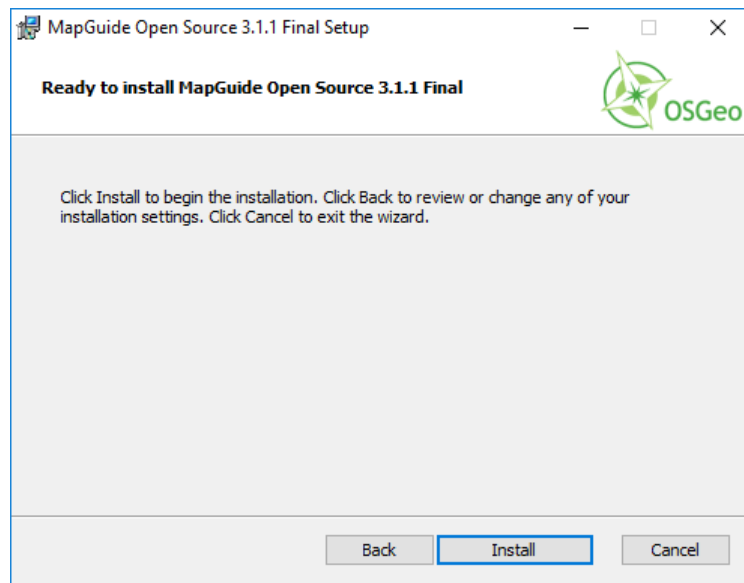
Server IP Adresse übernehmen.



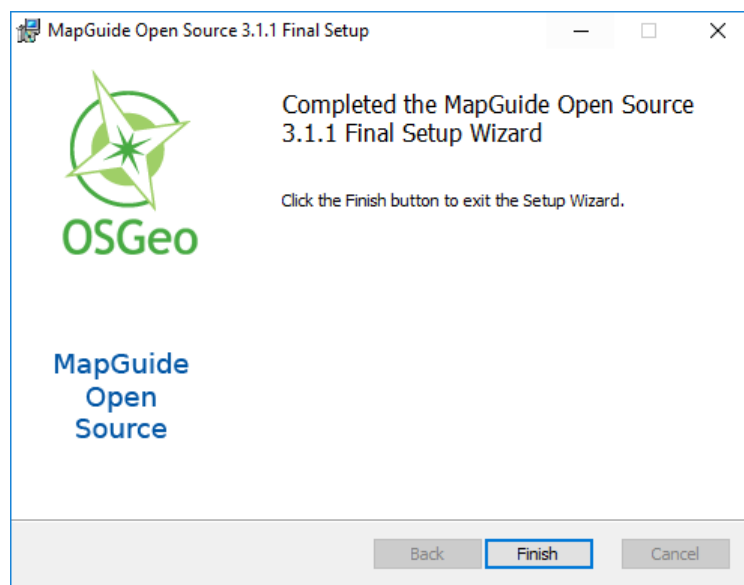
Zielverzeichnis wählen.



Zu installierende Komponenten übernehmen.



Installation starten.



Installation abschließen.

Parallelinstallation AIMS und MapGuide 3.1.1

AIMS 2017 und MapGuide 3.1.1 verwenden gleichsam die Ports 2810, 2811 und 2812 für die Administrative-, die Client- und die Site-Connections. Bei einer Parallelinstallation von AIMS und MapGuide 3.1.1 müssen Sie deshalb die Ports für AIMS umstellen:

1. Serverconfig.ini aus Verzeichnis „...Autodesk\Auto...Server201x\bin“ öffnen.
2. Ändern Sie in der Datei *Serverconfig.ini* die Ports für die Administrative-, die Client- und die Siteconnections auf einen Wert, der noch nicht verwendet wird (z.B. 2820, 2821 und 2822).

3. Stellen Sie in der Datei "C:\Program Files\Autodesk\Autodesk Infrastructure Web Server Extension 201x\www\webconfig.ini" die Ports genauso ein wie in der *Serverconfig.ini*.
4. Starten Sie den Dienst *Infrastructure Map Server 2017* neu. Führen Sie einen IIS-Reset aus.

AIMS Passwörter

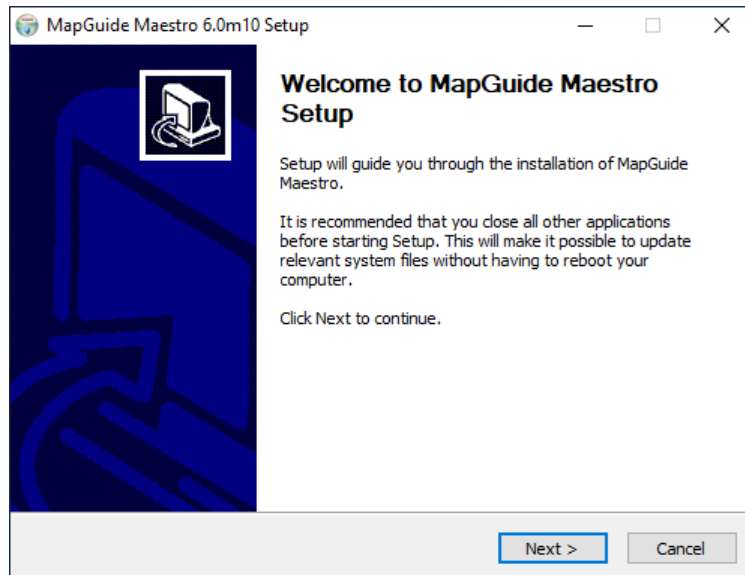
Achtung: Die MapGuide Open Source und AIMS Passwörter sind nach der Installation gleich. Diese Passwörter werden auch für den Site-Administrator benötigt. Bitte beachten Sie Groß- und Kleinschreibung!

Benutzer: **Administrator**

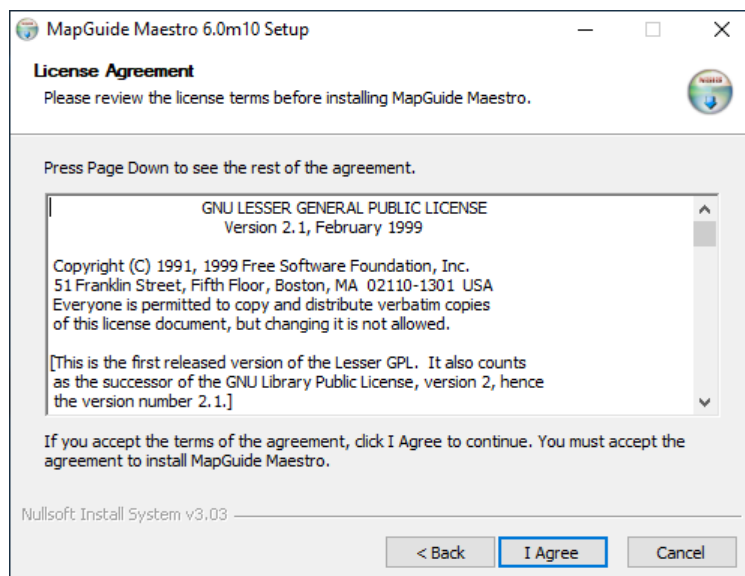
Passwort: **admin**

Anhang 10: Installation von MapGuide Maestro

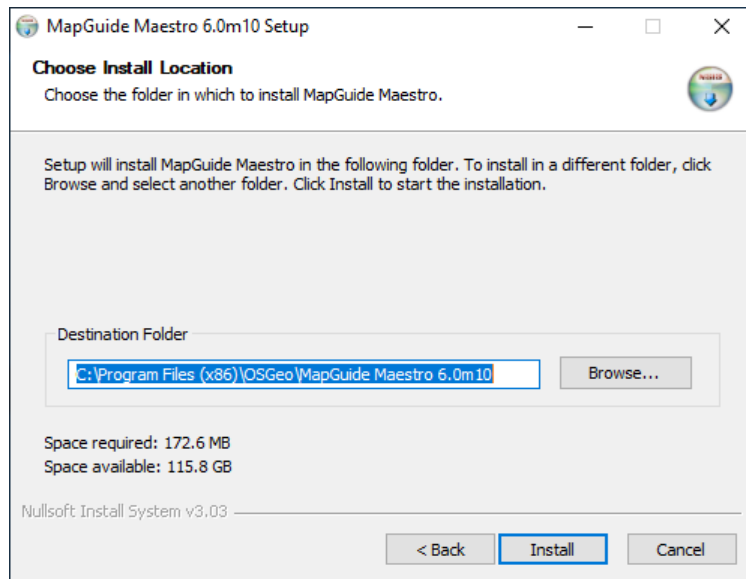
Starten Sie das Installationsarchiv *MapGuideMaestro-Release-6.0m10-Setup.exe* im Ordner */Tools/MapGuide OpenSource 3.1.1* und folgen Sie den Anweisungen auf dem Bildschirm.



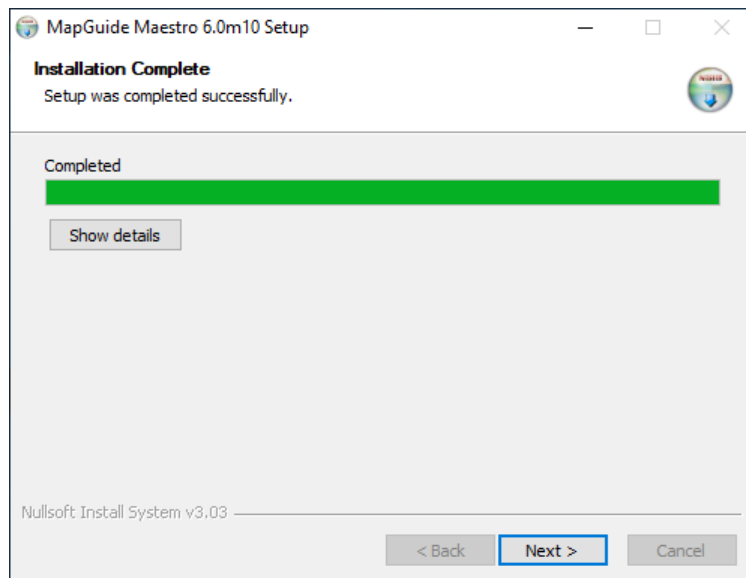
Klicken Sie auf *Next >*, um die Installation zu starten.



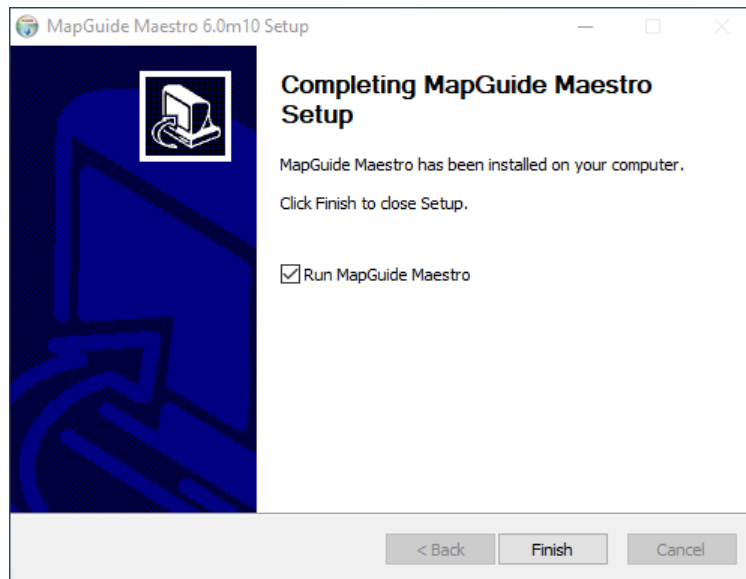
Stimmen Sie den Lizenzbedingungen durch Klicken auf *I Agree* zu.



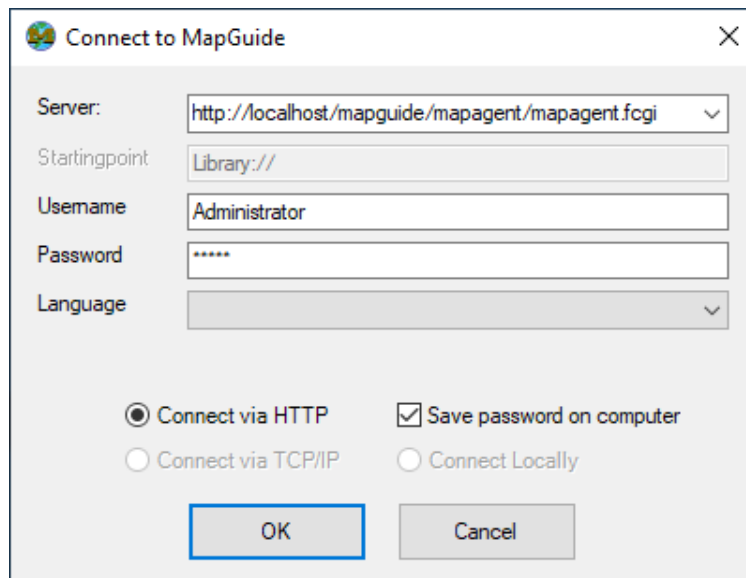
Bestätigen Sie das Zielverzeichnis.



Bestätigen Sie mit *Next >*.



Beenden Sie die Installation mit Klicken auf *Finish*.



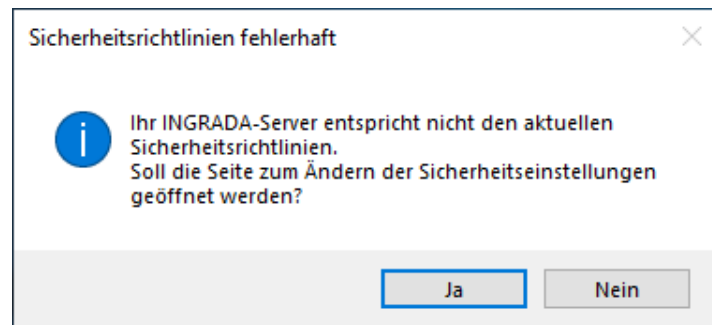
Bestätigen Sie die abgebildeten Einstellungen mit *OK*, um sich mit dem MapGuide Server zu verbinden.

Damit ist die Installation von MapGuide Maestro abgeschlossen.

Anhang 11: Sicherheit prüfen

Nach abgeschlossener Installation sollten Sie die INGRADA Serverseite aufrufen und Ihre Serverkonfiguration anhand der Sicherheitsrichtlinien prüfen und ggf. anpassen.

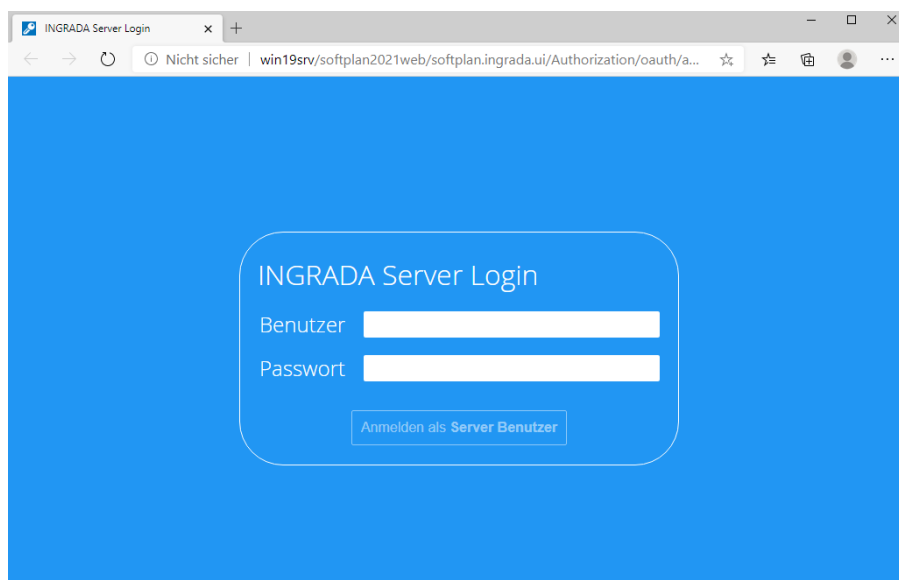
Hinweis: Diese Empfehlungen sind als Richtlinien gedacht. Für die korrekte Absicherung des Webservers ist der Betreiber verantwortlich. Das Prüfung erhebt keinen Anspruch auf Vollständigkeit.



Sicherheitshinweis beim Start des INGRADA web Projektmanagers.

Sie können die INGRADA Server –Seite jederzeit über den Menüpunkt *Einstellungen – INGRADA Server Statusseite* aufrufen. Melden Sie sich mit Ihrem INGRADA Server Administratorknamen und -kennwort an, die Sie bei der Installation festgelegt haben.

Hinweis: Die INGRADA Server-Seite funktioniert nicht mit dem Internet Explorer 11. Wir empfehlen Firefox und Edge.



INGRADA Server Login.

Öffnen Sie anschließend im Block IIS-Einstellungen nacheinander alle dort aufgeführten Punkte.

Relevante Einstellungen

Vorauswahl relevanter Einstellungen



IIS-Einstellungen

	IIS Fehlerseiten	
	HTTPS Caching	
Zustand des HTTPS Caching auf Clientseite		
	Das Caching von Https-Antworten ist noch aktiviert. Prüfen Sie vor dem Umstellen dieser Einstellung, ob die zugehörige URL-Rewrite-Rule nicht bereits unter einem anderen Namen als "RewriteCacheControl" und "RewritePragma" aktiviert wurde. Ist dies der Fall, aktivieren Sie nur eine der beiden Regeln.	<input type="button" value="Korrigieren"/> <input type="button" value="Ignorieren"/>
	HTTP zu HTTPS Weiterleitung	
	Cookie-Attribut secure	
	Cookie-Attribut httpOnly	
	Transport-Verschlüsselung	
	IIS-Standard-Startseite	

IIS-Einstellungen prüfen.

Die Symbole am linken Rand haben folgende Bedeutung:

- Die Konfiguration entspricht den Sicherheitsrichtlinien.
- Die Konfiguration entspricht nicht den Sicherheitsrichtlinien. *Korrigieren* oder *Ignorieren* Sie die Konfiguration.
- Die Konfiguration wurde geändert, entspricht aber nicht den vorgeschlagen Richtlinien (z. B. wurden andere Werte definiert).
- Der Warnhinweis wurde ignoriert, ohne die Konfiguration zu ändern. Dies ist in manchen Fällen sinnvoll. Dadurch wird die Meldung des Projektmanagers unterdrückt.

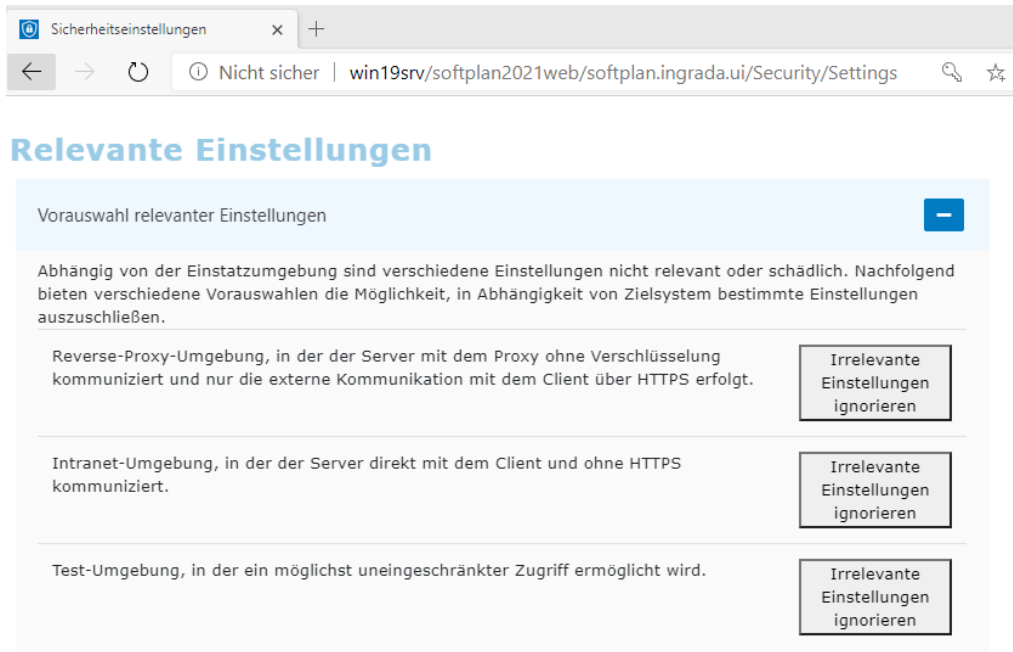
Hinweis: Der Projektmanager meldet so lange fehlerhafte Sicherheitsrichtlinien, so lange rote Warnhinweise in der Liste angezeigt werden.

Relevante Einstellungen

Für die Szenarien

- Reverse-Proxy-Umgebung
- Intranet-Umgebung
- Test-Umgebung

wurde eine Vorauswahl für die Sicherheitseinstellungen entworfen. Klicken Sie im Block *Relevante Einstellungen* auf einen der Schaltflächen *Irrelevante Einstellungen ignorieren*, werden die Einstellungen gemäß der jeweiligen Umgebung konfiguriert bzw. ignoriert.



Sicherheitseinstellungen

Nicht sicher | win19srv/softplan2021web/softplan.ingrada.ui/Security/Settings

Relevante Einstellungen

Vorauswahl relevanter Einstellungen

Abhängig von der Einstatzumgebung sind verschiedene Einstellungen nicht relevant oder schädlich. Nachfolgend bieten verschiedene Vorauswahlen die Möglichkeit, in Abhängigkeit von Zielsystem bestimmte Einstellungen auszuschließen.

Reverse-Proxy-Umgebung, in der der Server mit dem Proxy ohne Verschlüsselung kommuniziert und nur die externe Kommunikation mit dem Client über HTTPS erfolgt.	Irrelevante Einstellungen ignorieren
Intranet-Umgebung, in der der Server direkt mit dem Client und ohne HTTPS kommuniziert.	Irrelevante Einstellungen ignorieren
Test-Umgebung, in der ein möglichst uneingeschränkter Zugriff ermöglicht wird.	Irrelevante Einstellungen ignorieren

Sicherheitseinstellungen für vordefinierte Szenarien.