

NICK INFORMATIONSTECHNIK GMBH

ZeroPortal – Schnellstart

Vom leeren Windows Server zum laufenden Portal

Stand September 2026 (Server 1.0.30)

Diese Anleitung führt in etwa 30 Minuten durch die Installation eines einzelnen ZeroPortal-Servers: Datenbank, Portal, Konfigurationsassistent, erste Anmeldung im Browser. Jeder Schritt ist mit einem Bildschirmfoto belegt. Alles Weitere steht in zwei anderen Dokumenten: Der **Quick-Admin-Guide** bindet den ersten Arbeitsplatz an und verteilt die ersten Anwendungen, das **Administrationshandbuch** beschreibt Hintergründe, Berechtigungen, Betrieb und Hochverfügbarkeit.

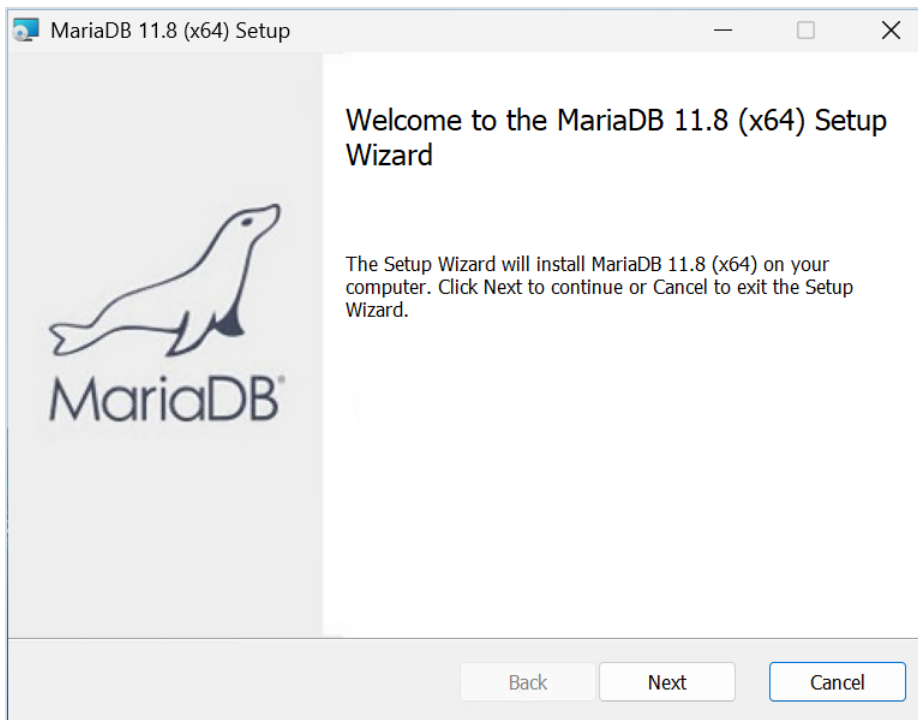
1. Voraussetzungen

Was	Anforderung
Server	Windows Server (64 Bit), lokale Administratorrechte. Domänenmitglied für die Anmeldung mit dem Windows-Konto; ohne Domäne siehe Kasten in Schritt 3 des Assistenten
Datenbank	MariaDB 11.8 oder 12.3 , beides Long-Term-Support-Reihen. Installer von mariadb.org (Windows, x64)
Portal	ZeroPortal-<Version>.msi von https://zeroportal.de/download
.NET	Nichts zu installieren. Das Portal-Paket bringt die Laufzeit mit
Administratoren	Eine AD-Gruppe, deren Mitglieder das Portal verwalten, z. B. Firma\ZeroAdmins
Netzwerk	Ein HTTPS-Port für das Portal, Vorgabe 8080 . Der Assistent öffnet die Windows-Firewall

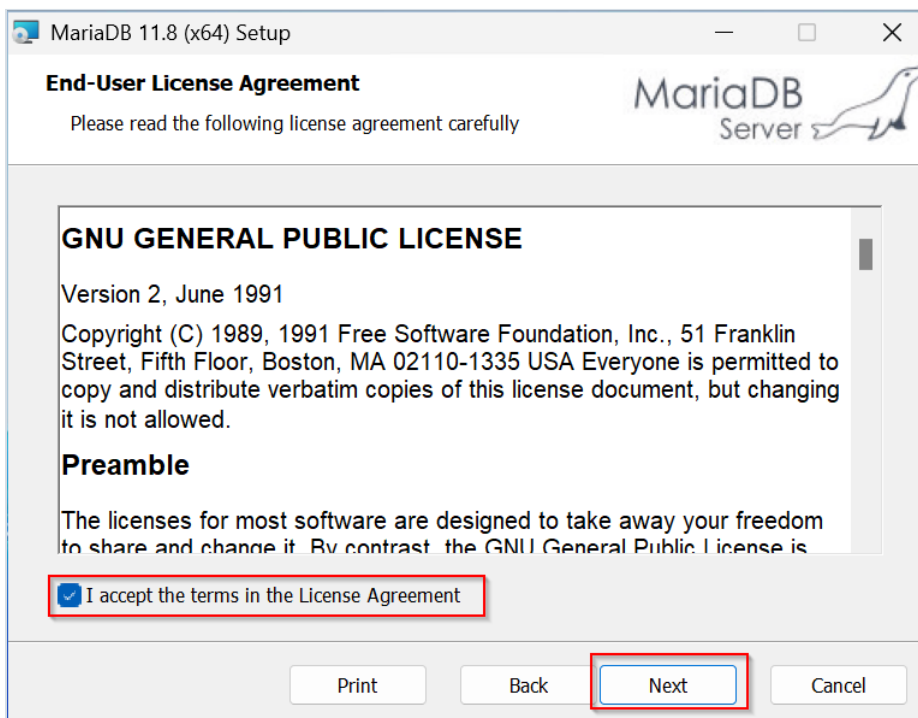
Die Reihenfolge ist fest: erst MariaDB, dann das Portal-MSI, dann der Assistent. Das Setup prüft die installierte MariaDB und warnt, wenn sie fehlt oder älter als 11.8 ist.

2. MariaDB installieren

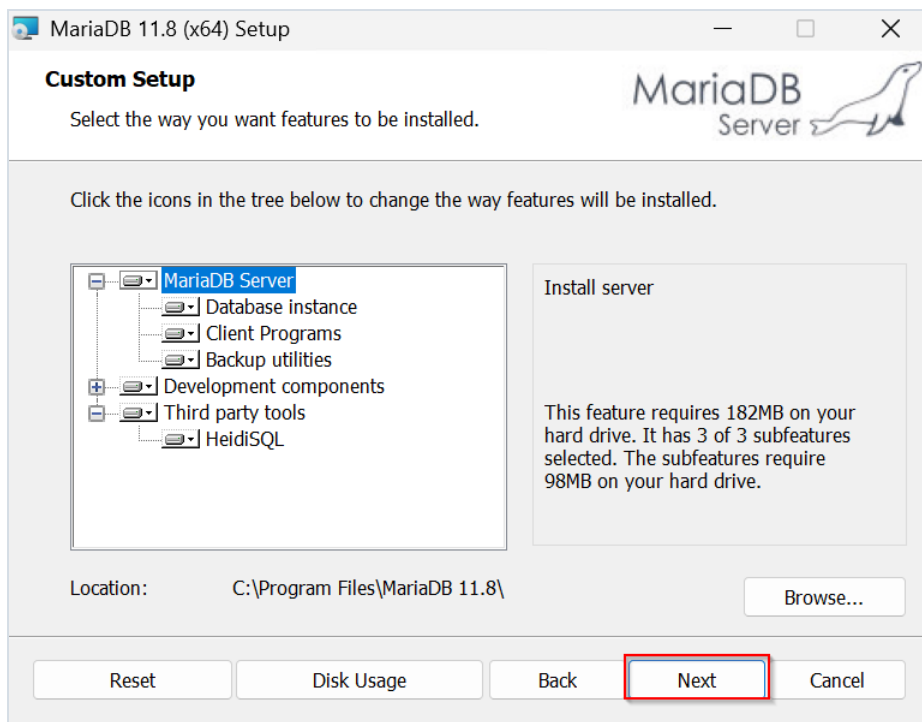
Installer starten und auf der Begrüßungsseite **Next** wählen.



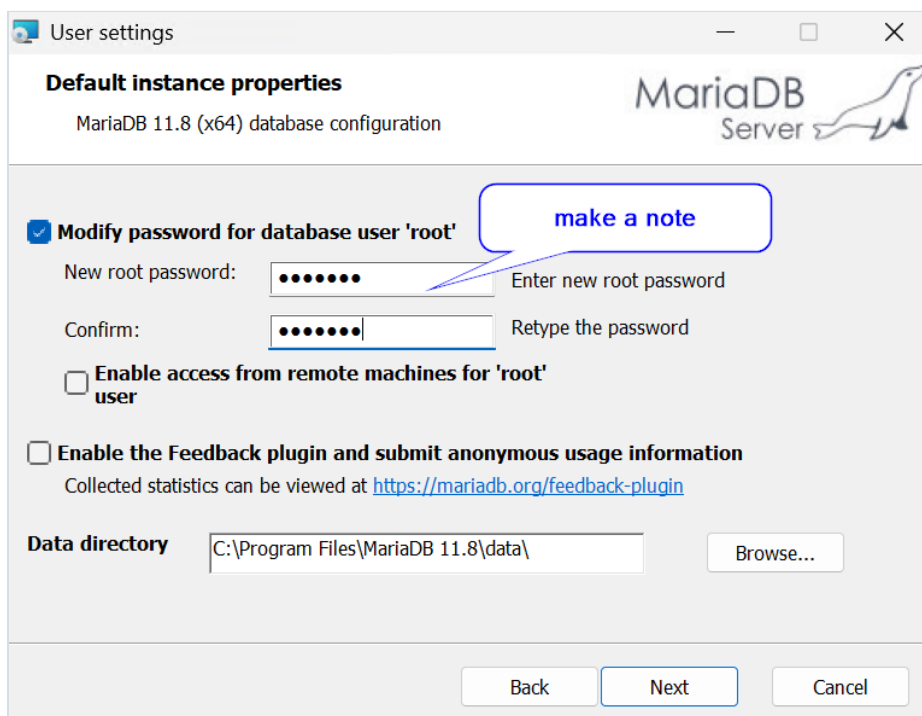
Lizenz (GPL v2) akzeptieren.



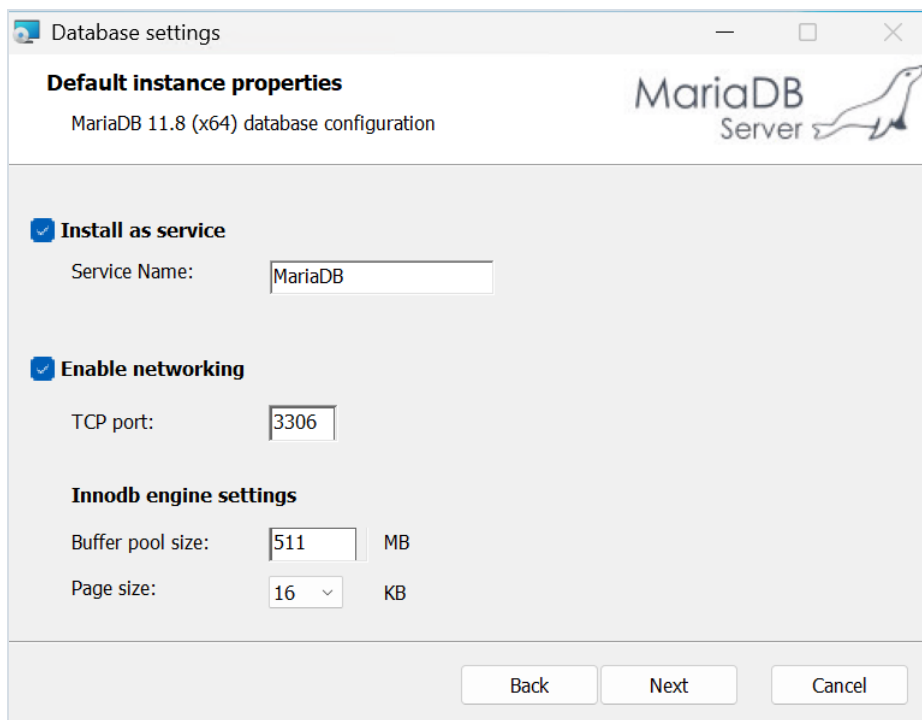
Funktionsauswahl und Installationsordner bei der Vorgabe belassen. ZeroPortal findet die Konfigurationsdatei `my.ini` später nur im Ordner `data` neben `bin`, so wie der Installer es anlegt.



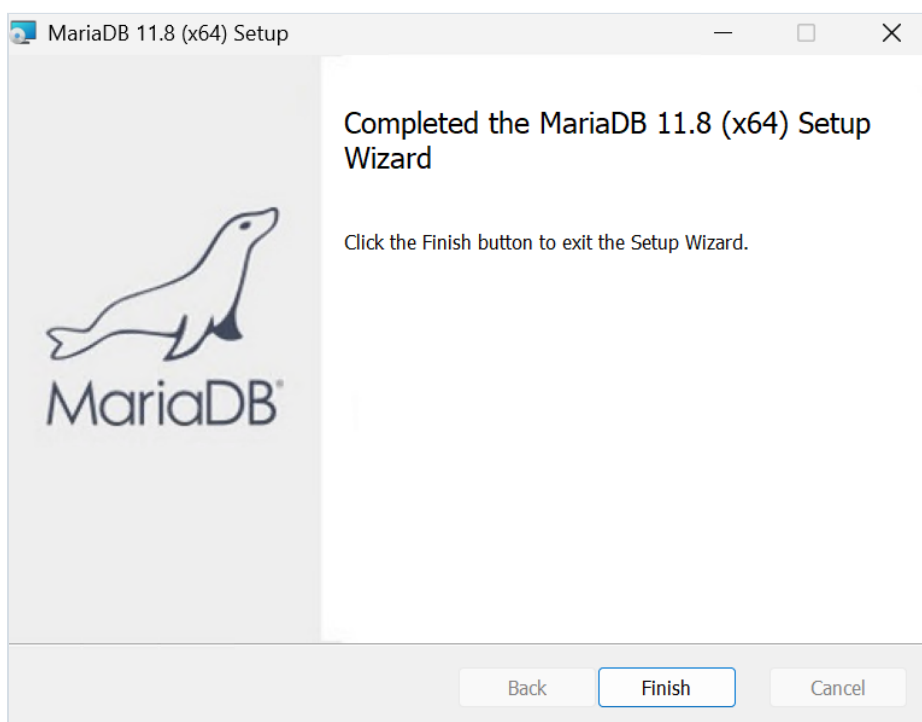
Passwort für **root** setzen und **notieren**. Der Assistent braucht es einmalig, um Datenbank und Benutzer anzulegen. *Enable access from remote machines* bleibt aus, das Datenverzeichnis bleibt bei der Vorgabe.



Als Dienst installieren (Name **MariaDB**), Netzwerk auf Port **3306** eingeschaltet lassen. Die InnoDB-Vorgaben reichen für den Start.

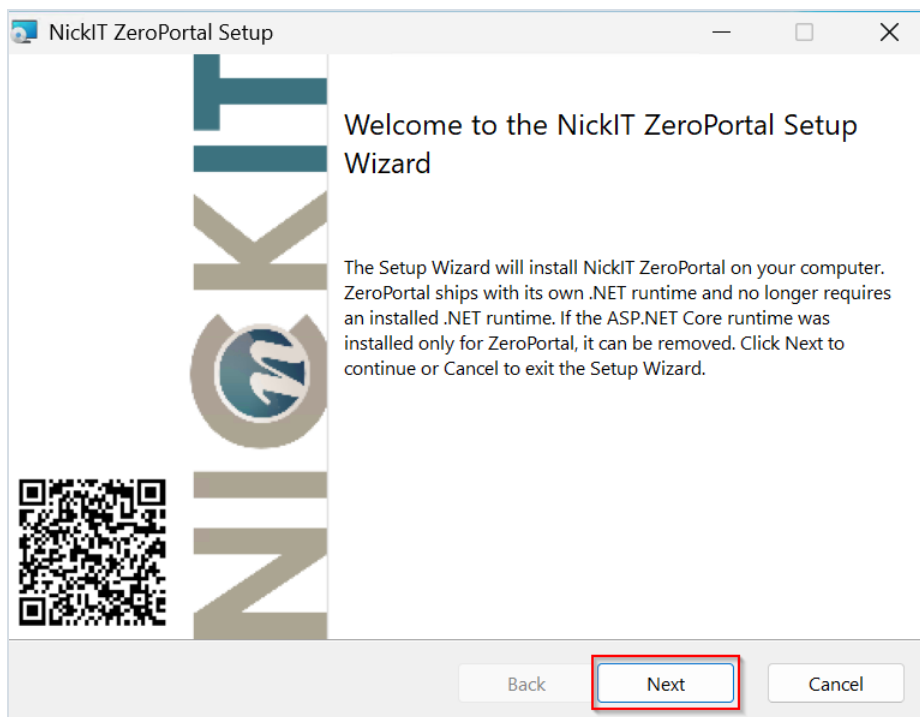


Zusammenfassung mit **Install** bestätigen und den Assistenten mit **Finish** schließen. Der Dienst läuft danach.

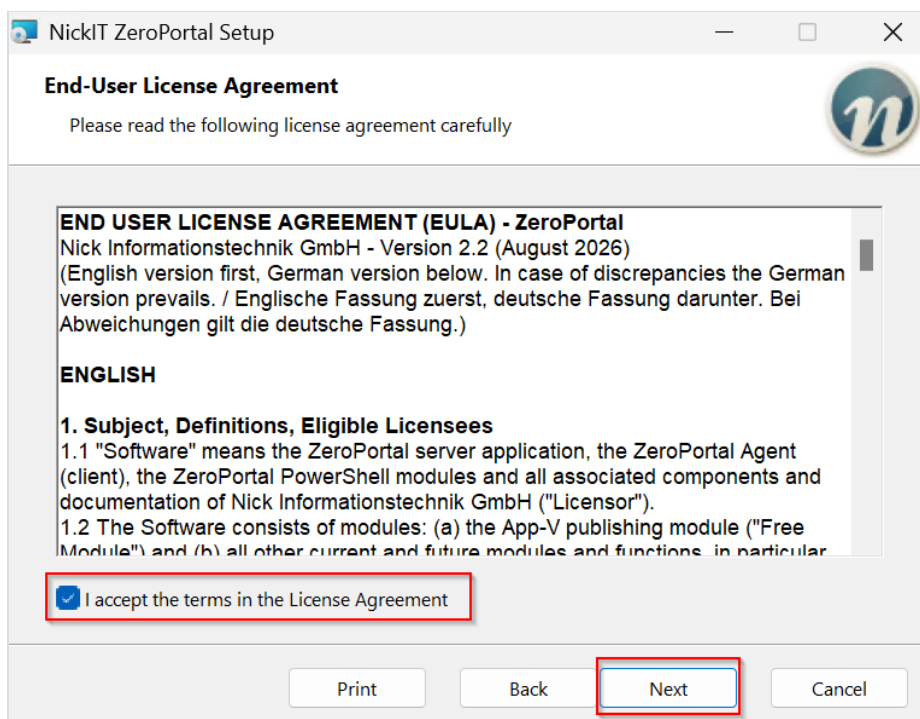


3. ZeroPortal installieren

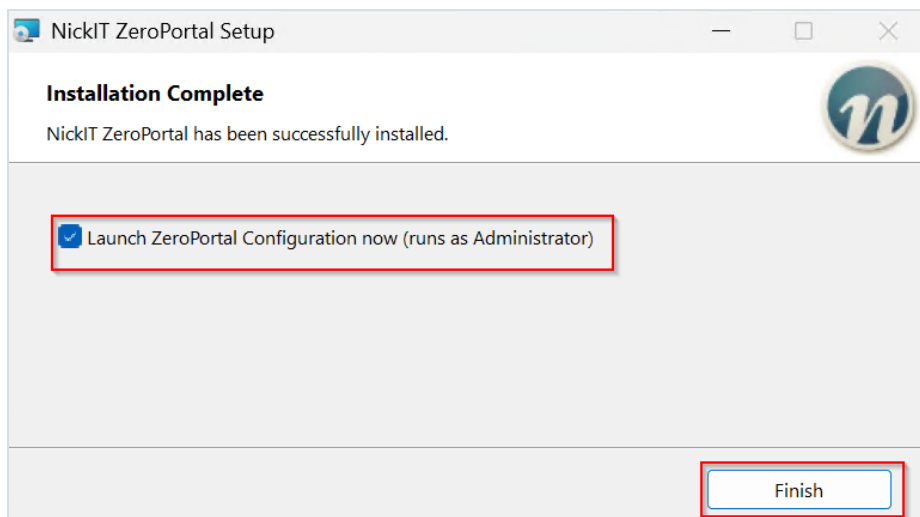
Das MSI von <https://zeroportal.de/download> laden und starten. Die Begrüßungsseite weist darauf hin, dass keine .NET-Laufzeit mehr nötig ist.



Lizenzvereinbarung lesen und akzeptieren.



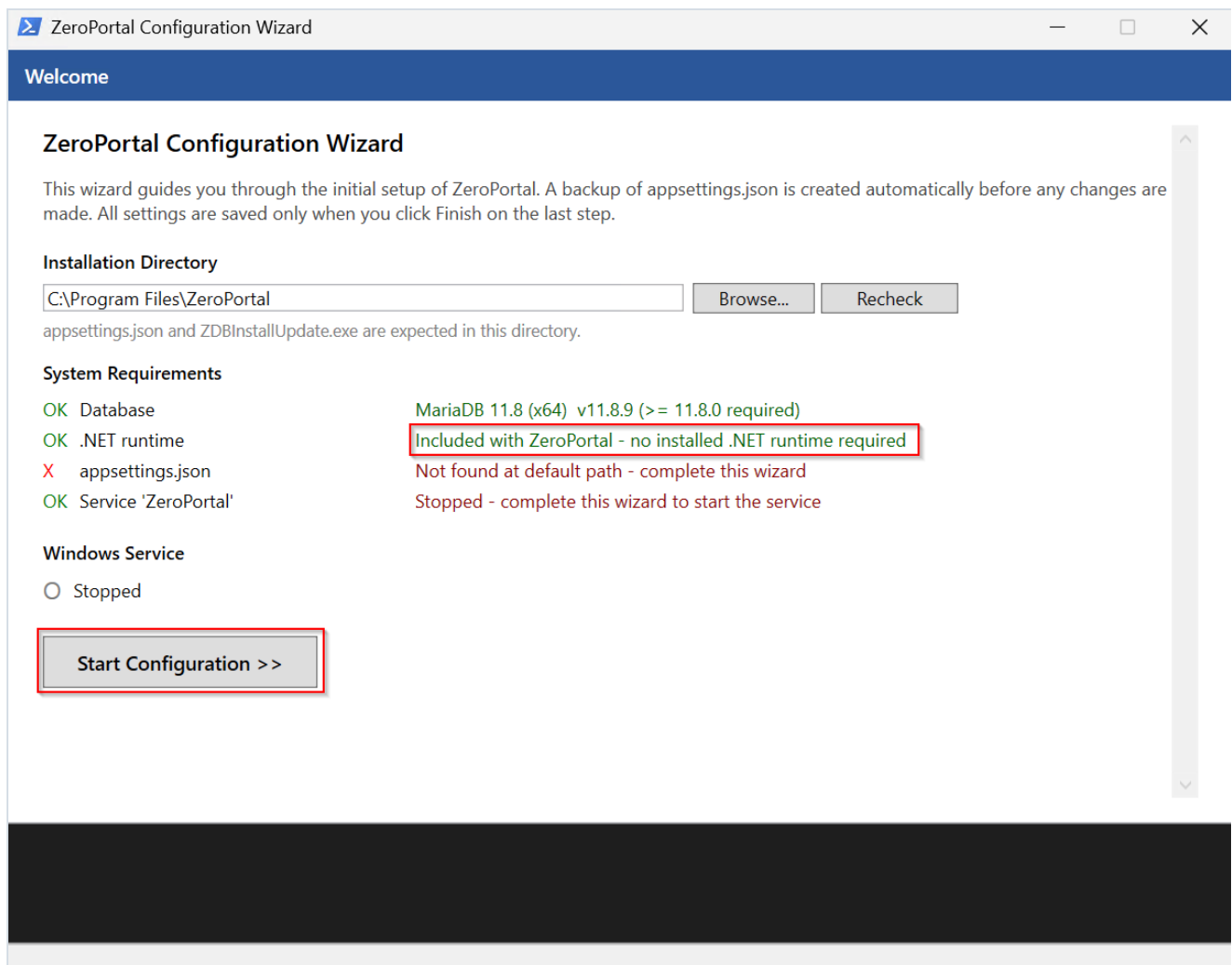
Auf der letzten Seite bleibt **Launch ZeroPortal Configuration now** gesetzt. Der Assistent läuft als Administrator, weil er nach C:\Program Files\ZeroPortal schreibt, den Dienst einrichtet, die Firewall öffnet und das Zertifikat importiert.



Später starten Sie den Assistenten über `C:\Program Files\ZeroPortal\ZeroPortalConfigTool.ps1` (als Administrator) erneut, etwa nach einem Portal-Update oder für eine Änderung.

4. Der Konfigurationsassistent

Die Startseite prüft die Voraussetzungen. **Database** und **.NET runtime** müssen OK sein. Dass `appsettings.json` fehlt und der Dienst gestoppt ist, gehört bei der Erstinstallation dazu, beides erledigt der Assistent. Mit **Start Configuration** geht es los.



Schritt 1: Zertifikat

Das Portal spricht ausschließlich HTTPS. Entweder eine vorhandene PFX-Datei importieren oder ein selbstsigniertes Zertifikat erzeugen. Für den Schnellstart reicht das selbstsignierte: Subject ist der Servername, das PFX-Passwort frei wählen (es wird verschlüsselt gespeichert, Sie brauchen es nicht mehr). *Import to Trusted Root* macht das Zertifikat auf dem Server vertrauenswürdig, *Copy .crt file to Desktop* liefert die Datei, die Sie an die Clients verteilen (Quick-Admin-Guide, Kapitel 3). **Generate Certificate** wählen.

ZeroPortal Configuration Wizard

Step 1 / 5 - Certificate

Step 1 - Certificate

Current certificate status
-

<< Hide Use existing certificate (.pfx)

Certificate (.pfx): Browse...

PFX Password: Check

<< Hide Generate new self-signed certificate

Subject (CN):

Output folder: Browse...

PFX Password:

☒ Import to Trusted Root (server)

☒ Copy .crt file to Desktop

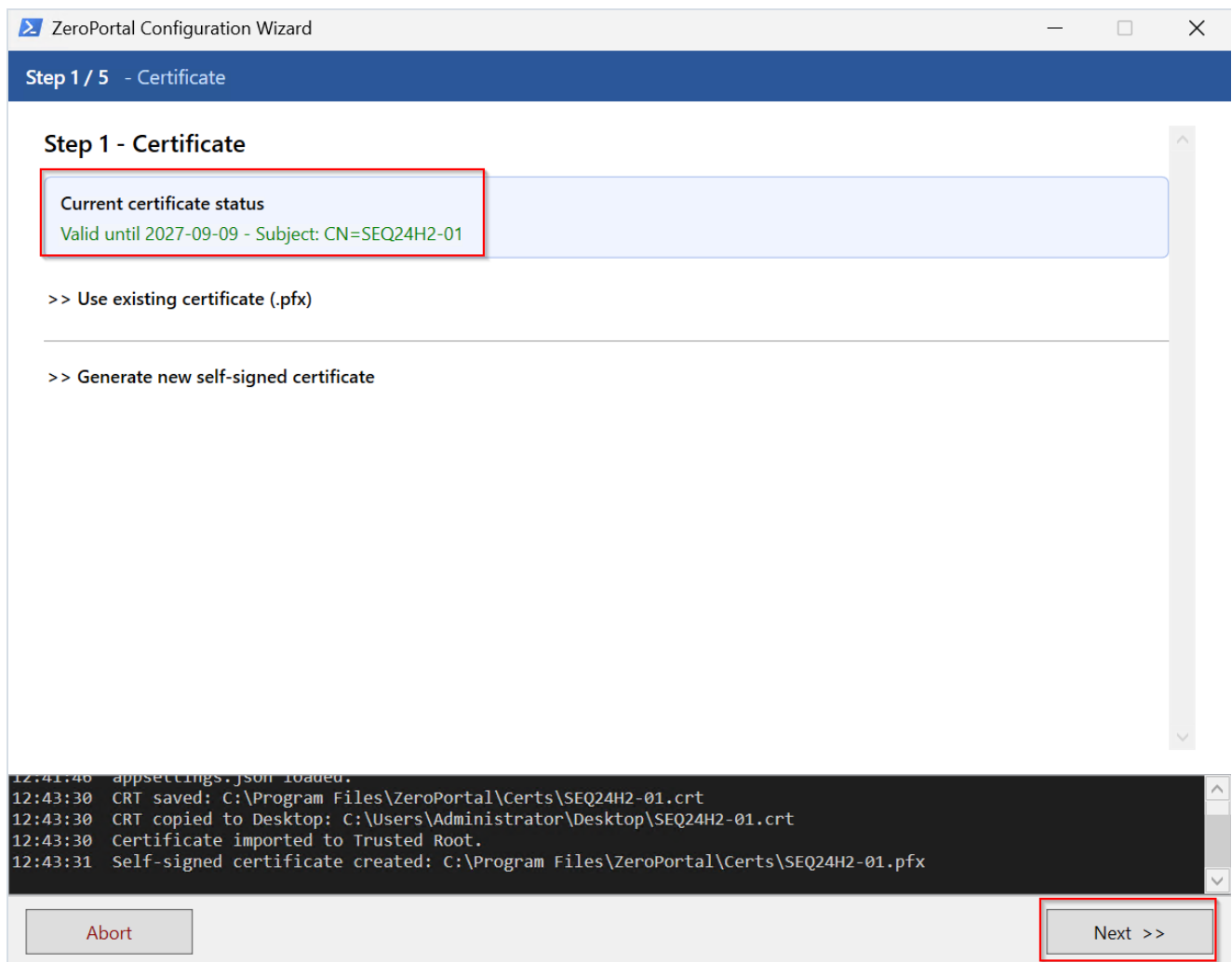
Quickstart Self-Signed

Generate Certificate

```
12:41:46 New appsettings.json created at: C:\Program Files\ZeroPortal\appsettings.json
12:41:46 appsettings.json loaded.
```

Abort Next >>

Die Statuszeile zeigt danach Gültigkeit und Subject. Weiter mit **Next**.



Für den Produktivbetrieb später ein Zertifikat der eigenen PKI einspielen, das alle Clients kennen.

Schritt 2: Grundkonfiguration

- **Endpoint:** Die URL, unter der das Portal erreichbar ist. In einer Domäne den vollständigen Namen verwenden, z. B. `https://zeroportal.firma.local:8080`. Der Port ist frei wählbar. *Open Windows Firewall for inbound traffic* bleibt gesetzt.
- **Database Connection:** Server `localhost`, Port `3306`. Das Passwort gehört dem Anwendungsbenutzer `zeroportal_dbuser`, den der Assistent anlegt. Es ist ein neues, frei gewähltes Passwort, **nicht** das root-Passwort. Das Replikationspasswort ist Pflicht; es wird erst für einen Cluster gebraucht und muss dann auf allen Knoten gleich sein.
- **MariaDB:** Programm- und Datenpfad erkennt der Assistent selbst.

ZeroPortal Configuration Wizard

Step 2 / 5 - Base Configuration

Endpoint

Protocol:

URL:

☒ Open Windows Firewall for inbound traffic

Database Connection

Server: Port:

DB User: Password: (app user - not the root; e.g. zeroportal_dbuser)

Database Name: Min Ver:

Repl. Password: (user: zeroportal_repl - required; must be identical on all nodes)

MariaDB

Bin Path: Auto-detected

Data Path:

Logging

```

12:41:40 appsettings.json loaded.
12:43:30 CRT saved: C:\Program Files\ZeroPortal\Certs\SEQ24H2-01.crt
12:43:30 CRT copied to Desktop: C:\Users\Administrator\Desktop\SEQ24H2-01.crt
12:43:30 Certificate imported to Trusted Root.
12:43:31 Self-signed certificate created: C:\Program Files\ZeroPortal\Certs\SEQ24H2-01.pfx

```

Weiter unten Protokollordner und Protokollstufen bei der Vorgabe lassen (Ordner C:\ProgramData\NickIT\ZPServer\Logs) und **Test DB Connection** ausführen. Erst bei OK weiter.

Logging

Log folder:

Log level: Application: ASP.NET Core: Entity Framework:

TCP localhost:3306 OK

```

17:39:07 CRT saved: C:\Program Files\ZeroPortal\Certs\APPV05.uran.local.crt
17:39:07 CRT copied to Desktop: C:\Users\Administrator.uran\Desktop\APPV05.uran.local.crt
17:39:07 Certificate imported to Trusted Root.
17:39:07 Self-signed certificate created: C:\Program Files\ZeroPortal\Certs\APPV05.uran.local.pfx
17:40:53 DB TCP connection OK: localhost:3306

```

Schritt 3: Administratoren

Die AD-Gruppe der Voll-Administratoren im Format DOMÄNE\Gruppe eintragen und mit **Test in AD** prüfen. Optional eine zweite Gruppe mit reinem Lesezugriff. Beide Gruppen gelten immer, auch wenn im Portal später jede Berechtigung entfernt wird.

ZeroPortal Configuration Wizard

Step 3 / 5 - Admin Users

Step 3 - Admin Users

Configure Active Directory groups that have access to ZeroPortal. Use the format DOMAIN\GroupName.

Full Admins

AD Group: Test in AD Group found in AD. Admin permissions in the portal

ReadOnly Admins

AD Group: Test in AD Group found in AD. Read-only permissions in the portal

```

17:39:07 CRT saved: C:\Program Files\ZeroPortal\Certs\APPV05.uran.local.crt
17:39:07 CRT copied to Desktop: C:\Users\Administrator\uran\Desktop\APPV05.uran.local.crt
17:39:07 Certificate imported to Trusted Root.
17:39:07 Self-signed certificate created: C:\Program Files\ZeroPortal\Certs\APPV05.uran.local.pfx
17:40:53 DB TCP connection OK: localhost:3306

```

Abort << Back Next >>

Server ohne Domäne. Lokale Gruppen wie `BUILTIN\Administrators` funktionieren hier nicht, das Portal löst Gruppen über Active Directory auf. Lassen Sie beide Felder leer und richten Sie nach dem Assistenten das Notfallkonto ein: Auf einem Rechner mit dem ZeroPortal-PowerShell-Modul `New-ZPRootPasswordHash` ausführen, das Passwort eingeben und den ausgegebenen Hash in `C:\Program Files\ZeroPortal\appsettings.json` eintragen:

```
"RootUser": { "UserName": "root", "PasswordHash": "ZPH1:..." }
```

Danach den Dienst ZeroPortal neu starten und sich unter `https://<server>:8080/Account/Login` anmelden. Jede Anmeldung mit diesem Konto wird protokolliert; legen Sie für die tägliche Arbeit interne Konten im Portal an.

Schritt 4: Datenbank anlegen

Hier läuft `ZDBInstallUpdate.exe`, das Datenbank, Anwendungs- und Replikationsbenutzer anlegt und das Schema einspielt. Dafür einmalig **root** und das Passwort aus der MariaDB-Installation eingeben. Diese Zugangsdaten werden nicht gespeichert. Dann **Create / Update Database**.

ZeroPortal Configuration Wizard

Step 4 / 5 - Database Install / Update

Step 4 - Database Install / Update

The database is created when the program is first launched.

Runs ZDBInstallUpdate.exe to create or upgrade the ZeroPortal database schema. Connection settings from Step 2 are used - they will be saved together with all other settings on Finish.

Database Root / Admin Account required
The root or admin account is needed to create the database, application user and replication user. These credentials are used once and are never stored.

Root User:

Admin Password:

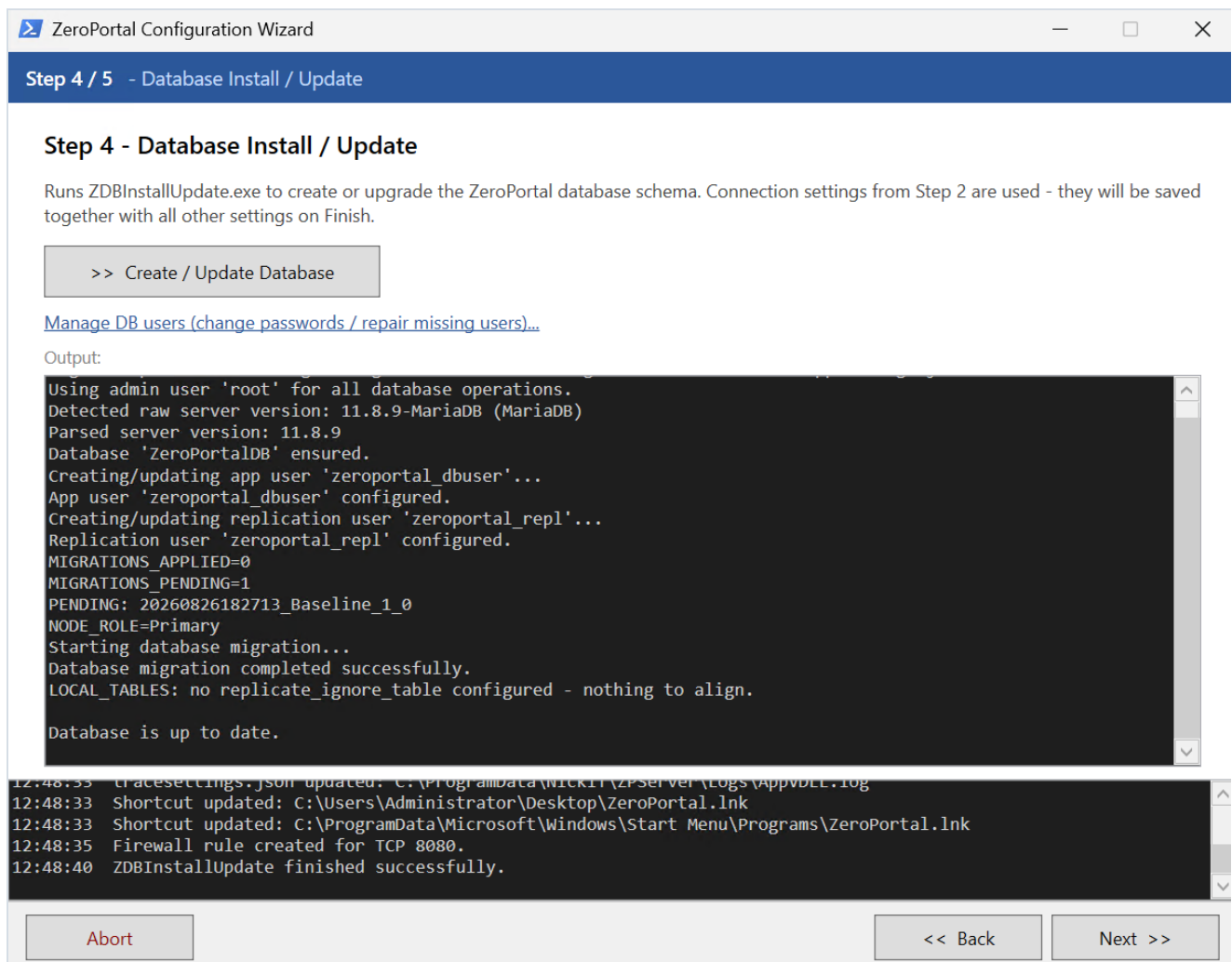
>> Create / Update Database

Output:

```
17:39:07 CRT saved: C:\Program Files\ZeroPortal\Certs\APPV05.uran.local.crt
17:39:07 CRT copied to Desktop: C:\Users\Administrator.uran\Desktop\APPV05.uran.local.crt
17:39:07 Certificate imported to Trusted Root.
17:39:07 Self-signed certificate created: C:\Program Files\ZeroPortal\Certs\APPV05.uran.local.pfx
17:40:53 DB TCP connection OK: localhost:3306
```

Abort << Back Next >>

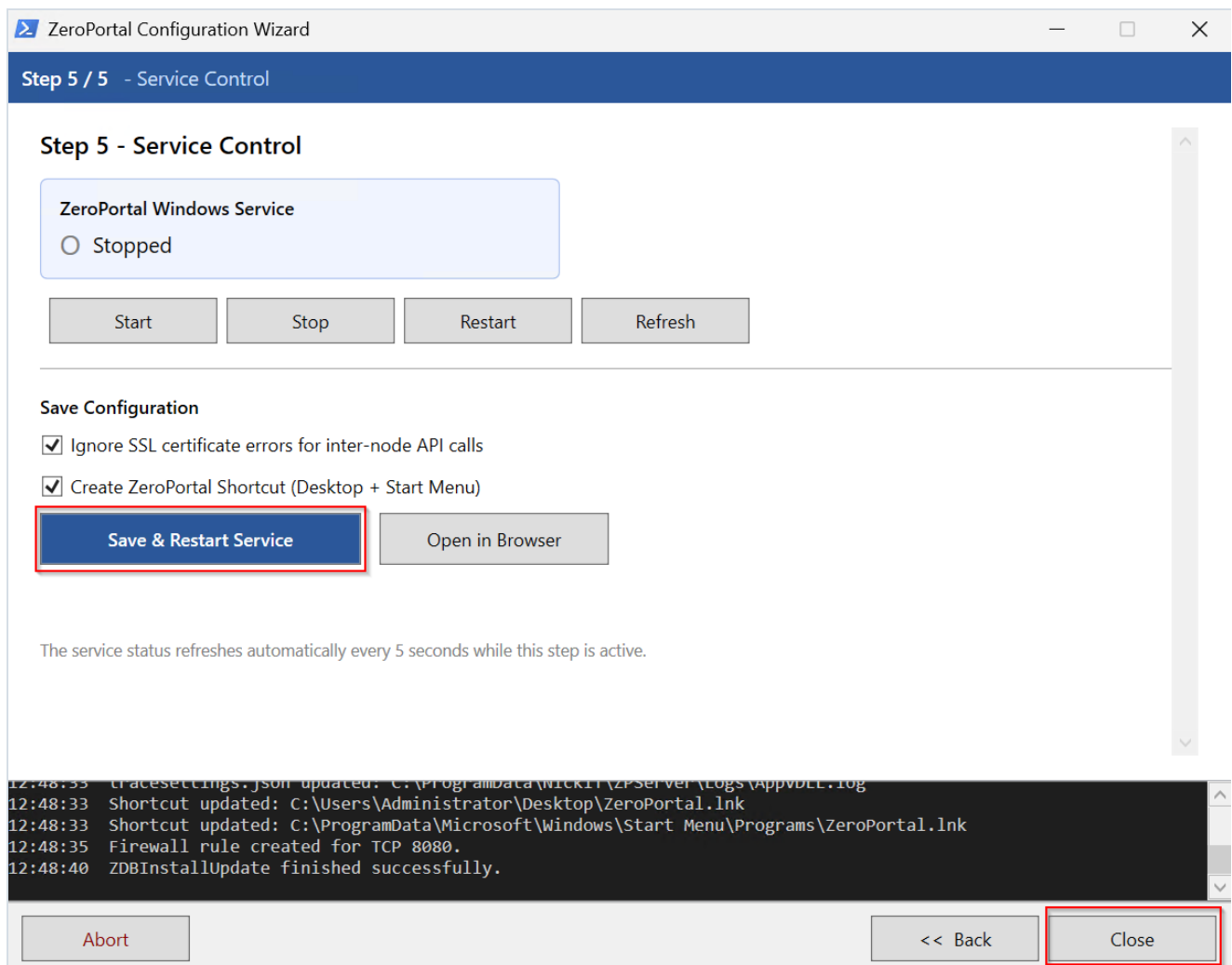
Das Ausgabefenster endet mit *Database migration completed successfully* und *Database is up to date*. Erst dann **Next**.



Nach einem Portal-Update wiederholen Sie diesen Schritt mit demselben root-Zugang, damit Schemaänderungen eingespielt werden.

Schritt 5: Dienst starten

Save & Restart Service schreibt die `appsettings.json`, registriert den Dienst `ZeroPortal`, legt die Firewallregel für den Portal-Port an und erstellt Verknüpfungen auf Desktop und Startmenü. Die Statusanzeige wechselt auf **Running**. *Ignore SSL certificate errors for inter-node API calls* betrifft nur Cluster mit selbstsignierten Zertifikaten und kann gesetzt bleiben. **Open in Browser** öffnet das Portal, **Close** beendet den Assistenten.

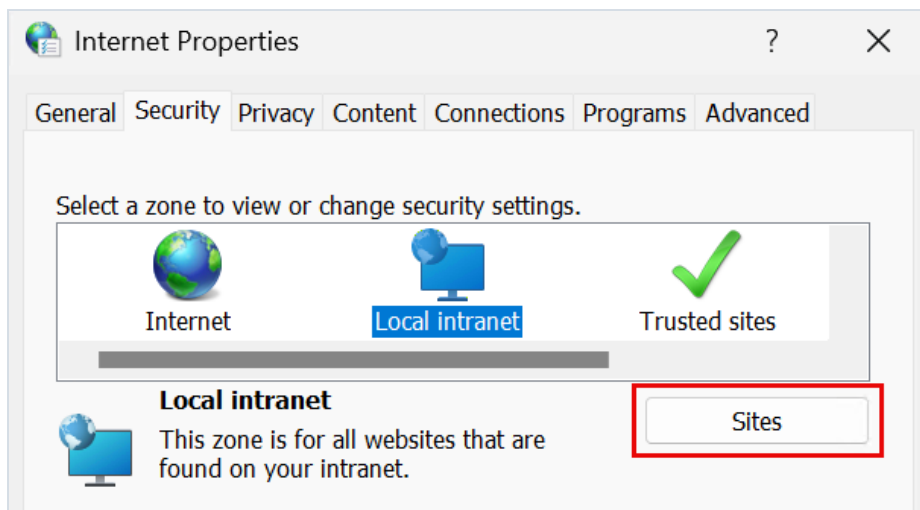


Alle Einstellungen liegen jetzt in `C:\Program Files\ZeroPortal\appsettings.json`. Vor jeder Änderung durch den Assistenten wird eine Sicherung der Datei angelegt. Wer die Datei von Hand ändert, startet danach den Dienst neu.

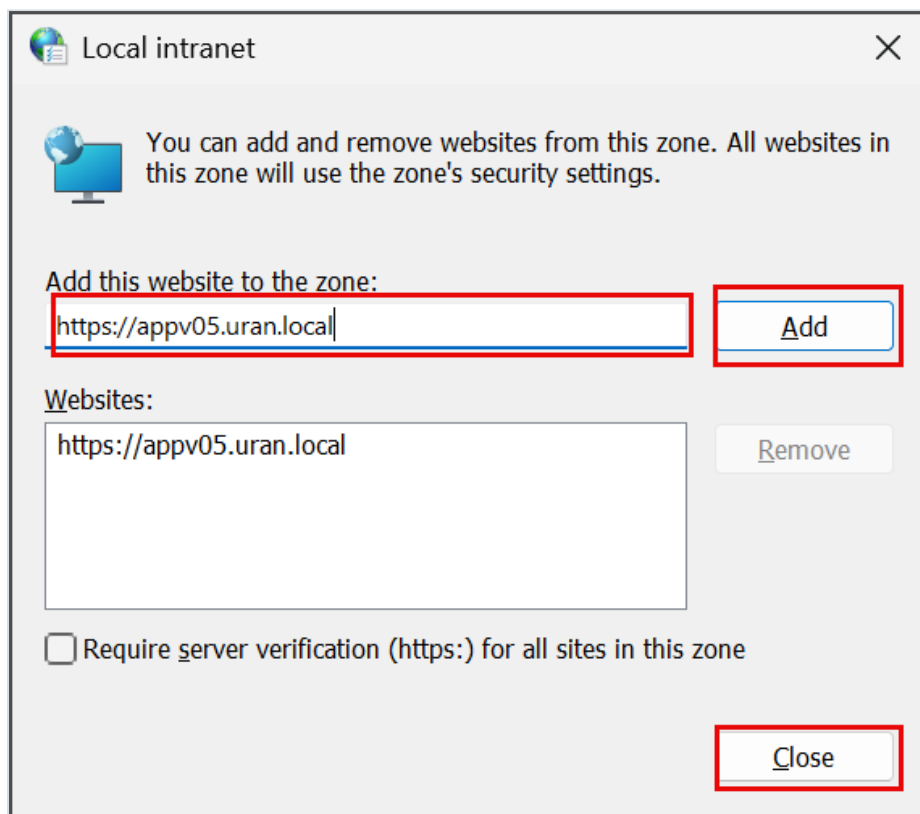
5. Anmeldung im Browser

Auf dem Server selbst öffnet `https://<server>:8080` das Portal ohne Passwortabfrage. Von einem anderen Rechner aus muss der Browser das Windows-Konto still übermitteln dürfen. Dafür muss die Portal-URL in der Zone **Lokales Intranet** liegen.

Für einen ersten Test auf einem einzelnen Rechner: *Internetoptionen* öffnen, Registerkarte **Sicherheit**, Zone **Lokales Intranet**, dann **Sites**.



Über **Erweitert** die Portal-URL hinzufügen, Dialoge schließen, Browser neu starten. Die Einstellung gilt für Edge, Chrome und Internet Explorer gleichermaßen.

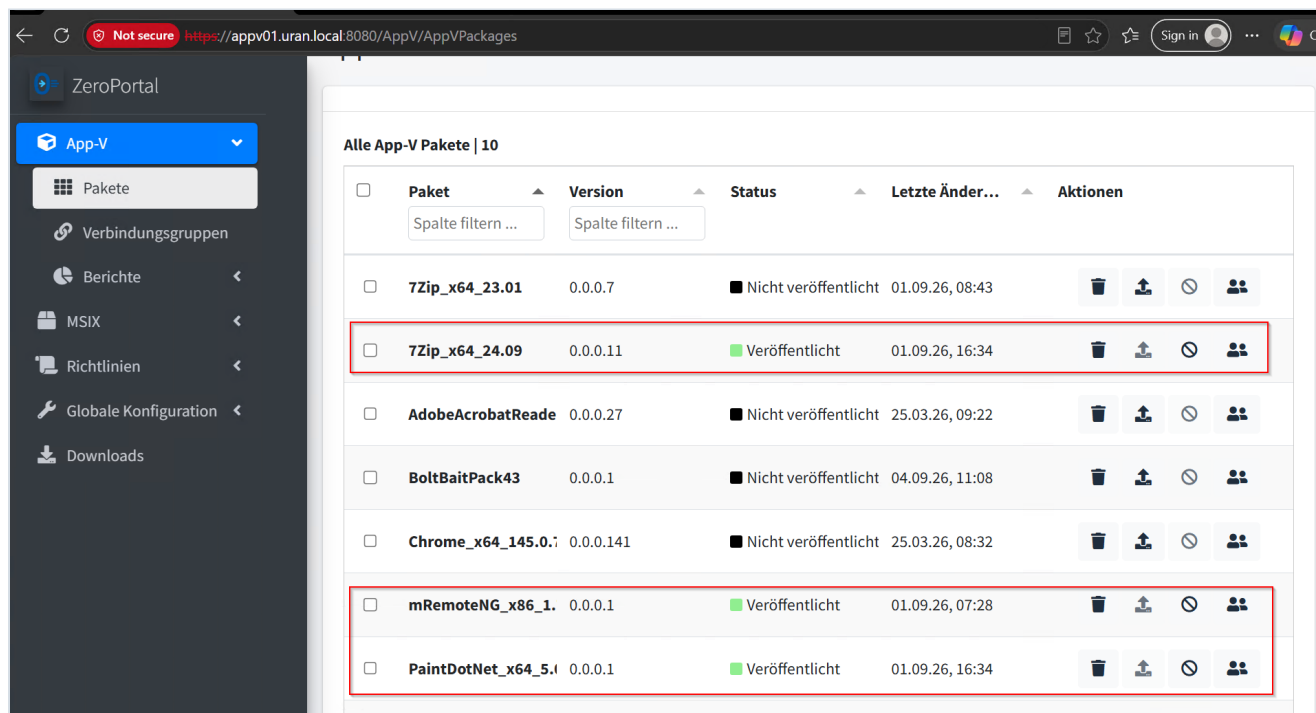


Für alle Rechner erledigt das eine Gruppenrichtlinie: *Benutzerkonfiguration → Administrative Vorlagen → Windows-Komponenten → Internet Explorer → Internetsystemsteuerung → Sicherheitsseite → Site-zu-Zone-Zuweisungsliste*, Portal-URL mit Wert **1**.

Wird das Portal unter dem Namen des Servers aufgerufen, ist für Kerberos nichts weiter zu tun. Nur für einen eigenen Namen (Alias) gehört ein SPN an das Computerkonto: `setspn -S HTTP/zeroportal.firma.local SERVERNAME$`. Ein Anmeldefenster trotz korrekter Gruppenmitgliedschaft bedeutet fast immer, dass die Intranetzzone fehlt.

6. Prüfen und weiter

Das Portal zeigt in der Kopfzeile das angemeldete Konto und das Anmeldeverfahren. Ist ein Mitglied der Administratorgruppe angemeldet, sind alle Menüpunkte sichtbar.



Damit ist der Server fertig. Die nächsten Schritte:

1. **Paketfreigabe** anlegen und im Portal als Repository eintragen (Administrationshandbuch, Kapitel 3 und 4).
2. **Ersten Client anbinden** und Anwendungen verteilen (Quick-Admin-Guide).
3. **Berechtigungen** für weitere Administratoren und Paketierer vergeben (Administrationshandbuch, Kapitel 5).
4. **Zweiten Knoten** für Hochverfügbarkeit hinzufügen, wenn gewünscht (Administrationshandbuch, Kapitel 11).

Was wo liegt:

Was	Wo
Programm und Konfiguration	C:\Program Files\ZeroPortal, darin appsettings.json und ZeroPortalConfigTool.ps1
Zertifikate	C:\Program Files\ZeroPortal\Certs
Protokolle	C:\ProgramData\NickIT\ZPServer\Logs
Datenbank	Dienst MariaDB, Datenbank ZeroPortalDB, Benutzer zeroportal_dbuser und zeroportal_rep1