

ScreenGenie Telemetry Server

On-Premise Installation Guide

Version 26.4.1

PNQ Software

Introduction

This document describes the installation and configuration of the ScreenGenie Telemetry Server for on-premise deployment on Windows Server 2022 or Windows Server 2025. The guide is intended for IT administrators and system administrators who are responsible for deploying the telemetry infrastructure within their organization.

The ScreenGenie Telemetry Server receives monitor configuration data from ScreenGenie client installations across the organization and presents this information through a secure web-based dashboard. All data remains within the organization's own infrastructure.

The installation process is fully automated through a dedicated Windows installer. The installer verifies prerequisites, creates the database, configures IIS, and provisions the initial administrator account in a single guided workflow.

Copyright © 2026 — PNQ Software BV. All rights reserved.

1. Architecture Overview

The on-premise telemetry server consists of three logical components that work together to provide a complete monitoring solution.

The web application is an ASP.NET Core 8 service that exposes both a REST API for receiving telemetry data from clients and a web-based dashboard for administrators. The application is hosted in IIS with the ASP.NET Core Module V2 providing the bridge between IIS and the managed runtime.

The database is a PostgreSQL instance (version 17 or higher) that stores monitor telemetry records, tenant information, and dashboard user accounts. A dedicated database user with restricted privileges is created specifically for the application.

The dashboard is a browser-based interface accessible through HTTP (and HTTPS when a certificate is configured) that allows administrators to view monitor configurations, search and filter data, export reports, and manage user accounts.

2. Prerequisites

Before running the installer, the following components must be installed and operational on the target Windows Server. Each component must be installed in the order described in this section.

2.1 Operating System

The installer is tested on the following Windows Server editions:

- Windows Server 2022 (all editions)
- Windows Server 2025 (all editions)

The server must be a 64-bit installation with at least 4 GB of RAM and 20 GB of available disk space.

2.2 Internet Information Services (IIS)

IIS must be installed with the following components enabled:

- Common HTTP Features: Default Document, Static Content, HTTP Errors
- Health and Diagnostics: HTTP Logging
- Performance: Static Content Compression
- Security: Request Filtering
- Application Development: ISAPI Extensions, ISAPI Filters
- Management Tools: IIS Management Console

IIS can be installed through Server Manager under Add Roles and Features, or via PowerShell with the `Install-WindowsFeature` cmdlet.

2.3 PostgreSQL Database

PostgreSQL 17 or higher must be installed and running on the same server. The installer downloaded from the official PostgreSQL website guides through a graphical setup wizard. During this wizard, the administrator sets a password for the postgres superuser account. This password is required later when running the ScreenGenie Telemetry Server installer.

When the wizard completes, it offers to launch Stack Builder to download optional add-ons. Stack Builder is not required for the telemetry server and can be skipped by clearing the checkbox before clicking Finish.

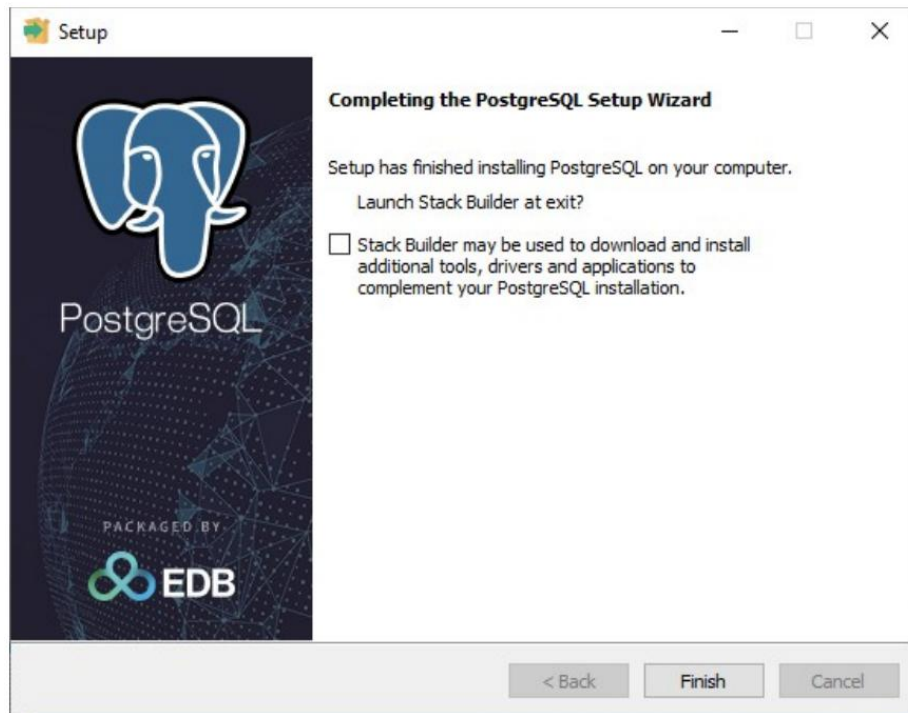


Figure 1 — PostgreSQL installer completion screen. Stack Builder is not required.

After installation, verify that the PostgreSQL service is running. The service is typically named postgresql-x64-18 (or similar, depending on the installed version) and should start automatically.

PostgreSQL must be listening on localhost (the default configuration). Remote database connections are not supported by the installer.

2.4 ASP.NET Core 8 Hosting Bundle

The ASP.NET Core 8 Hosting Bundle is the final prerequisite. This bundle includes the .NET Runtime, the ASP.NET Core Runtime, and the ASP.NET Core Module V2 (ANCM) that integrates the application with IIS.

The bundle must be downloaded from the official Microsoft .NET download page and installed after IIS is configured. Installing the bundle before IIS results in the ASP.NET Core Module not being registered in IIS.



Figure 2 — .NET 8 Windows Server Hosting installer. Accept the terms and click Install.

After the bundle is installed, restart IIS using the `iisreset` command from an elevated command prompt. The installer verifies the presence of the ASP.NET Core Module V2 during the prerequisites check and will refuse to continue if the module is missing.

3. Running the Installer

The installer is a single executable file (`ScreenGenieTelemetry-Setup.exe`) that contains all application files, supporting tools, and installation scripts. No additional downloads are required during the installation process.

Run the installer with administrator privileges by right-clicking the executable and selecting Run as administrator. The installer opens with a welcome page that introduces the product.

3.1 Prerequisites Check

After the welcome page, the installer displays a summary of the prerequisites described in Section 2. When clicking Next, the installer performs an automated verification to confirm that IIS is installed and the PostgreSQL service is running.

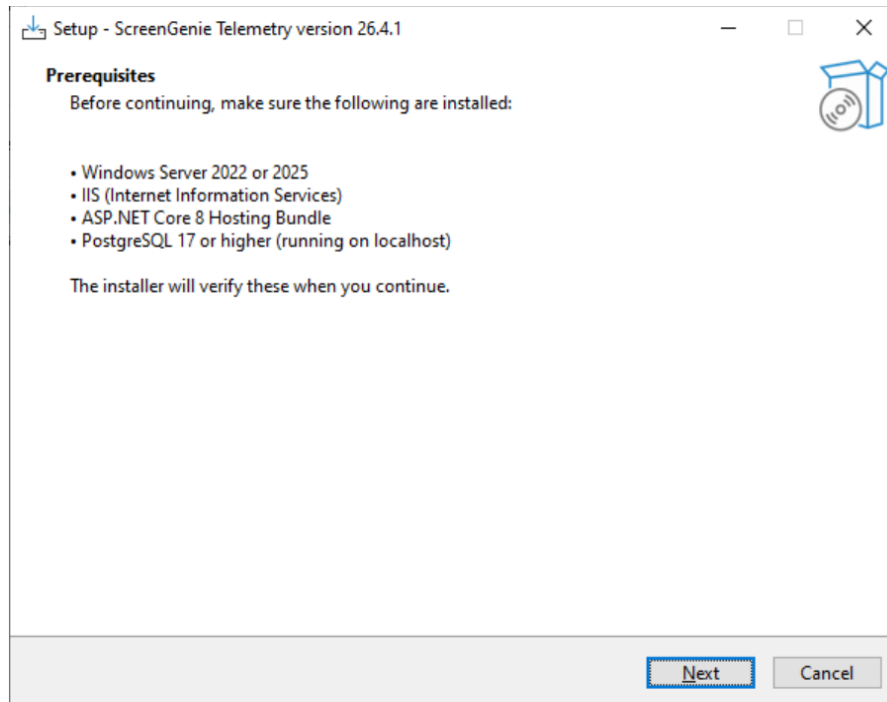


Figure 3 — Prerequisites overview. The installer verifies these automatically.

If either check fails, the installer stops and displays an error message indicating which component is missing. In that case, return to Section 2 to install the missing component and then restart the installer.

3.2 Database Configuration

The database configuration page asks for the PostgreSQL connection details. Three values are required on this page.

- **Postgres superuser password** — The password for the postgres account set during PostgreSQL installation (Section 2.3). This password is used only during the setup process and is not stored by the application.
- **Application user password** — The password to assign to the dedicated sg_user database account. This account is used by the application at runtime to read and write telemetry data. The password must be at least 8 characters and should follow the organization's password policy.
- **Database name** — The name of the database to create. The default value is screengenie_telemetry and can usually be left unchanged. The database must not already exist on the server; if it does, the installer will fail.

3.3 Organization

The organization page identifies the tenant that will own the telemetry data. The telemetry system supports a multi-tenant architecture internally, but for on-premise deployments only one tenant is created during installation.

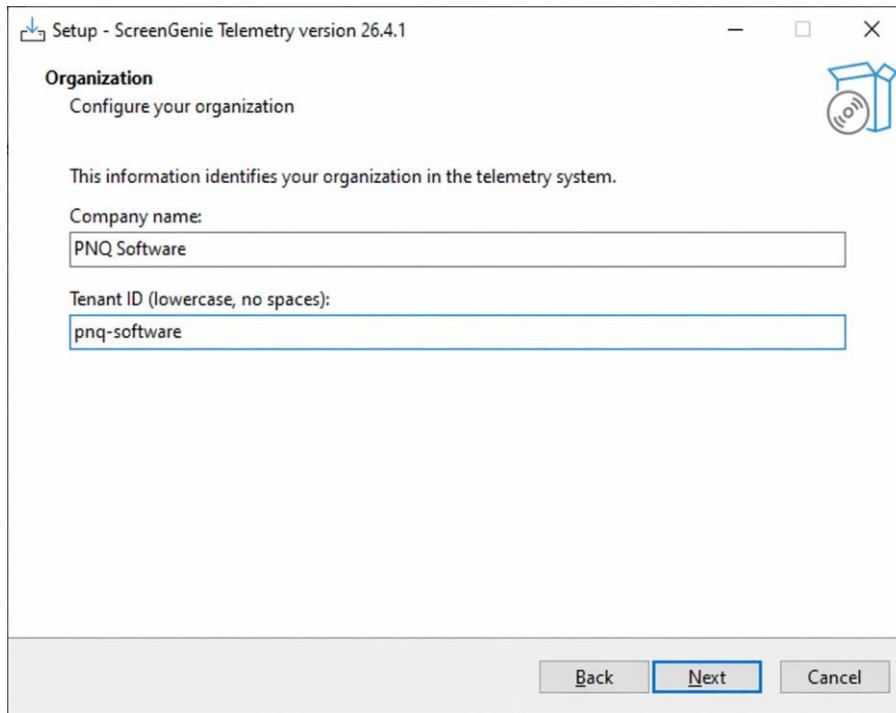


Figure 4 — Organization page. The tenant ID is suggested automatically based on the company name.

- **Company name** — The display name of the organization as it will appear in the dashboard, for example PNQ Software or Acme Corporation.
- **Tenant ID** — A unique identifier used internally and in the telemetry.ini file on client machines. The installer suggests an ID based on the company name but allows it to be changed. The tenant ID must be lowercase and may only contain letters, numbers, and dashes.

3.4 Dashboard Administrator

The administrator page creates the initial dashboard user account. This account has full administrative privileges within the organization's tenant and can create additional user accounts after installation.

Setup - ScreenGenie Telemetry version 26.4.1

Dashboard Administrator
Create the first admin account

This account will be used to log in to the telemetry dashboard.

Username:
pnq-admin

Password:
●●●●●●●●

Confirm password:
●●●●●●●●

Back Next Cancel

Figure 5 — Dashboard administrator account. The password must be entered twice to prevent typing errors.

- **Username** — The username used to log in to the dashboard. Descriptive usernames such as pnq-admin or company-admin are recommended for clarity.
- **Password** — The password for the administrator account. The password must be at least 8 characters and is stored in the database using bcrypt hashing with cost factor 11.
- **Confirm password** — A second entry of the password. The installer verifies that both entries match before continuing.

3.5 Server Configuration

The server configuration page defines how the telemetry server is exposed through IIS. Two values are required.

Figure 6 — IIS server configuration. The hostname must be resolvable from all client machines.

- **Hostname** — The hostname that clients will use to reach the server, for example `telemetry.company.local` or `telemetry.screengenie.local`. This value is used as the IIS host binding and must match the DNS configuration or local hosts file entries on client machines.
- **IIS site name** — The name under which the website is registered in IIS. The default value is `ScreenGenie Telemetry` and can be left unchanged in most cases.

3.6 Installation Progress

After the final configuration page, the installer displays a confirmation summary of all entered values. When clicking `Install`, the installer performs the following operations in order:

- Application files are copied to `C:\inetpub\screengenie-telemetry`.
- The `appsettings.json` configuration file is updated with the database connection string.
- The PostgreSQL database, application user, and schema are created.
- An initial tenant record is inserted, and a unique API key is generated.
- The administrator account is created with a bcrypt-hashed password.
- The IIS application pool and website are configured.
- Windows Firewall rules are added for ports 80 and 443.

Each step is logged to a temporary file and the installer progress bar indicates which operation is currently running. The complete installation typically takes less than a minute on modern hardware.

3.7 Completion

Upon successful completion, the installer displays a summary screen containing:

- The dashboard URL based on the configured hostname.
- The administrator username.
- The API key for use in telemetry.ini on client machines.

The API key is shown only once during installation and must be saved immediately. If the key is lost, a new key must be generated through the Tenants page in the dashboard, and all client telemetry.ini files must be updated accordingly.

4. Post-Installation

4.1 First Login

The dashboard is accessible through a web browser at the hostname configured during installation. The login page presents the ScreenGenie branding and two input fields for the administrator credentials entered during setup.

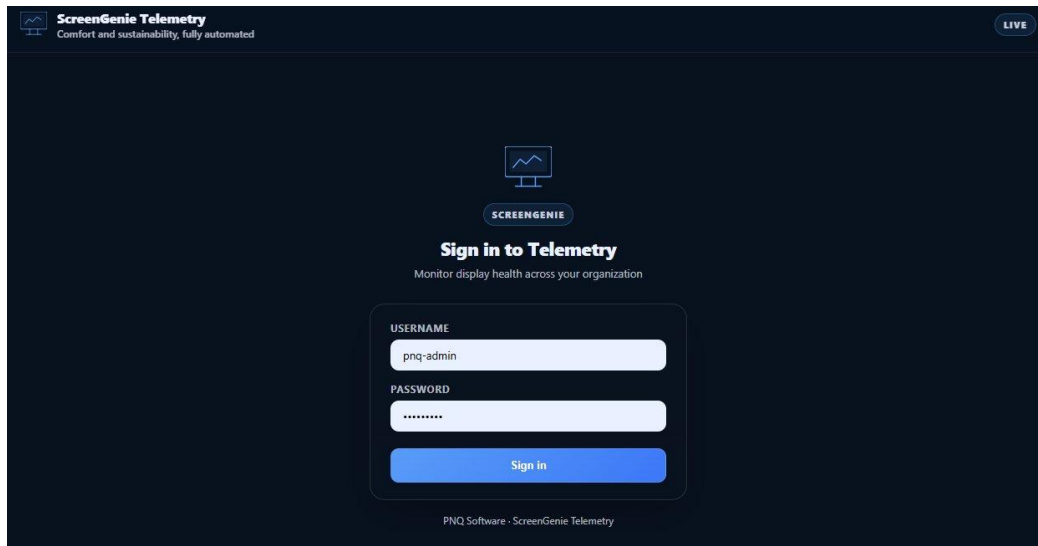


Figure 7 — Dashboard login page. Enter the administrator credentials created during installation.

After entering the administrator credentials, the dashboard displays the monitor overview page. Initially, no monitors are listed because no clients have reported data yet. As soon as ScreenGenie clients are configured to report to the server, their monitors appear in the overview automatically.

4.2 Client Configuration

To enable telemetry reporting from ScreenGenie clients, the `telemetry.ini` file must be distributed to each client machine. The file is placed in the following location:

```
C:\ProgramData\PNQ Software\ScreenGenie\telemetry.ini
```

The contents of the file are as follows, using the hostname and API key from the installation summary:

```
[Telemetry]
Url = http://telemetry.company.local
TenantId = your-tenant-id
ApiKey = sg-abcdef1234567890abcdef
AcceptAnyCertificate = No
IntervalMinutes = 15
```

The file can be deployed through Group Policy, Microsoft Intune, or any other software distribution system. The file is managed by IT and is never modified by ScreenGenie itself.

4.3 Enabling HTTPS

By default, the installer configures the telemetry server for HTTP on port 80. For production environments, HTTPS is strongly recommended. Two configuration options are available depending on the network environment.

4.3.1 Public-facing Deployments

If the server is accessible from the internet through a public domain name, a free certificate can be obtained from Let's Encrypt using Win-ACME. Win-ACME is a command-line utility that automates certificate issuance, IIS binding configuration, and renewal.

After installing Win-ACME, run wacs.exe with administrator privileges and follow the interactive prompts to select the ScreenGenie Telemetry site. Win-ACME configures the HTTPS binding automatically and schedules a renewal task that runs every 90 days.

4.3.2 Internal Deployments

For internal-only deployments without a public domain name, a certificate from the organization's own certificate authority should be used. The certificate must be imported into the local machine certificate store and then assigned to the HTTPS binding of the ScreenGenie Telemetry site in IIS Manager.

4.4 DNS and Client Access

Clients must be able to resolve the hostname configured during installation. For public deployments, a DNS A-record pointing to the server's IP address is sufficient. For internal deployments, either an internal DNS entry or entries in the hosts file of each client machine are required.

5. Ongoing Administration

5.1 User Management

Additional dashboard users can be created from the Users page in the dashboard. Each user is assigned a role: user accounts can view monitor data, while admin accounts can additionally manage users within the organization. Administrators cannot delete their own account to prevent accidental lockout.

5.2 Password Management

Users can change their own password at any time through the Change Password option in the dashboard navigation. The password change requires the current password and a new password of at least 8 characters.

5.3 Monitoring Client Activity

The dashboard automatically refreshes every 60 seconds to show the latest monitor data. The Last Seen column indicates when each monitor last reported. Monitors that stop reporting remain visible in the overview but their timestamps indicate the most recent contact.

5.4 Data Export

The complete monitor overview can be exported to CSV for reporting or further analysis through the Export CSV button on the dashboard. The export includes all monitor fields and respects the current tenant filter.

6. Maintenance

6.1 Application Updates

Application updates are distributed as new installer versions. The installer preserves the existing database and configuration when running an upgrade on a previously installed server. Before running an upgrade, administrators should back up the PostgreSQL database using `pg_dump`.

6.2 Database Backup

Regular backups of the PostgreSQL database are strongly recommended. A basic backup can be performed using the `pg_dump` utility:

```
pg_dump -U postgres -h localhost -d screengenie_telemetry -F c -f backup.dump
```

Backups should be stored on a separate system and rotated according to the organization's data retention policy.

6.3 Log Files

IIS request logs are stored in the default IIS logs directory and can be used for troubleshooting connectivity issues. Application diagnostic logs can be enabled by modifying the `web.config` file in the installation directory and setting `stdoutLogEnabled` to `true`. Diagnostic logging should only be enabled temporarily for troubleshooting and disabled afterwards to avoid excessive disk usage.

6.4 Certificate Renewal

When using Win-ACME, certificate renewal is handled automatically through the Windows Task Scheduler task created during initial setup. When using a certificate from an internal certificate authority, the administrator is responsible for tracking expiration dates and replacing certificates before they expire.

7. Troubleshooting

7.1 HTTP 500 Error on Dashboard

If the dashboard returns an HTTP 500 error after installation, the most common cause is an incorrect database connection string in `appsettings.json`. Verify that the password in the connection string matches the password set for `sg_user` during installation. A second common cause is that the ASP.NET Core Module V2 cannot start the application. Diagnostic output can be enabled by setting `stdoutLogEnabled` to `true` in `web.config` and inspecting the generated log files.

7.2 HTTP 401 Errors from Clients

If client machines receive HTTP 401 Unauthorized responses when reporting telemetry, the API key in the `telemetry.ini` file does not match any active tenant in the database. Verify that the tenant ID and API key match the values shown during installation or generated through the Tenants page in the dashboard.

7.3 Database Authentication Failure

If the application fails to start with a PostgreSQL authentication error, the `sg_user` password has been changed or the connection string is incorrect. The password can be reset through pgAdmin using the `ALTER USER sg_user WITH PASSWORD '...'` statement, and the matching value must then be entered in `appsettings.json`.

7.4 Clients Not Reporting

If client machines do not appear in the dashboard after installation, verify that the hostname in the client `telemetry.ini` file resolves correctly and that the server is reachable on port 80 or 443. The health endpoint can be used for quick verification:

```
http://hostname/api/telemetry/health
```

A successful response returns a JSON object with a healthy status and the current UTC timestamp.

8. Security Considerations

The telemetry server handles configuration data from across the organization and should be secured accordingly.

All communication between clients and the server should use HTTPS in production environments. The installer configures HTTP binding by default, and HTTPS must be enabled separately using either Let's Encrypt or an internal certificate authority as described in Section 4.3.

The PostgreSQL database listens only on localhost, preventing direct external access. The `sg_user` database account has only the minimum privileges required for application operation and cannot access databases other than `screengenie_telemetry`.

API keys are the primary authentication mechanism for clients. If an API key is compromised, it should be rotated immediately by generating a new key for the tenant through the dashboard and updating all client `telemetry.ini` files accordingly.

Dashboard passwords are stored using bcrypt hashing with cost factor 11, providing strong resistance against brute-force attacks even if the database is compromised.

9. PNQ Software Support

For technical support, configuration assistance, or feature requests, contact PNQ Software through the following channels:

- Email: support@pnqsoftware.com
- Website: <https://pnqsoftware.com>

When reporting issues, please include the version of the telemetry server, the version of Windows Server, and any relevant log excerpts or error messages.