Installation and Configuration Guide

July 14, 2025

For use with TrustZero 1.7

Table of Contents

TrustZero Installation and Configuration

TrustZero is CertiPath's high-assurance credential validation solution that provides robust business logic and configurability for a PACS' response to a range of validation conditions.

Using CertiPath TrustMonitor®, TrustZero achieves near real-time knowledge of credentials through a sophisticated layering of status-checking techniques. That knowledge is then provided to the PACS to achieve an immediate cessation of access as may be appropriate.

Feature Summary

- Enterprise-level continuous validation
- Single network location for all validation queries
- Validate all credentials within complex trust communities
- Pairs cloud-based validation with on-premise security
- Advanced validation enforcement options, including:
    - **Extended Validity** – Optionally used to increase the amount of time a credential's status is considered valid for sites with limited or inconsistent network availability
    - **Degraded Mode** – Optionally used to enable Degraded Mode, which is consistent with the U.S. government FICAM standard
    - **VIP Users** – Allows users to bypass conventional validation logic for credentials belonging to individuals with designated user-defined field (UDF) attribute values

Installation Prerequisites

The following sections describe the systems and environments that support successful installation and configuration of **TrustZero 1.7.**

System Prerequisites

TrustZero Admin Application

Description: DMZ Application/Web Server

VM Configuration: 2 cores/8GB memory/64GB VHD

Operating System/Server Configuration:

- Windows Server 2022 or later
- Microsoft IIS, .NET 8.0 or later

Database Server

Description: Microsoft SQL Server

VM Configuration: 2 cores/8GB memory/64GB VHD

Operating System/Server Configuration:

- Windows Server 2022 or later
- SQL Server 2022 Standard Edition or later

Note: TrustZero can integrate with an existing SQL Server.

Environmental Prerequisites

Compatible PACS and Physical Identity Access Manager (PIAM): TrustZero is responsible for communicating certificate validation of credentials to the PACS. Compatible systems:

PACS:

- Lenel OnGuard (8.2)

PIAM:

- CertiPath TrustManager® (2.4)
- CertiPath TrustMonitor (4.6.2)
- Certipath TrustVisitor (4.1.5)

Microsoft SQL Server: SQL Server 2022 Standard Edition (or later) is required as it includes built-in encryption functionality. TrustZero can integrate with an existing SQL server.

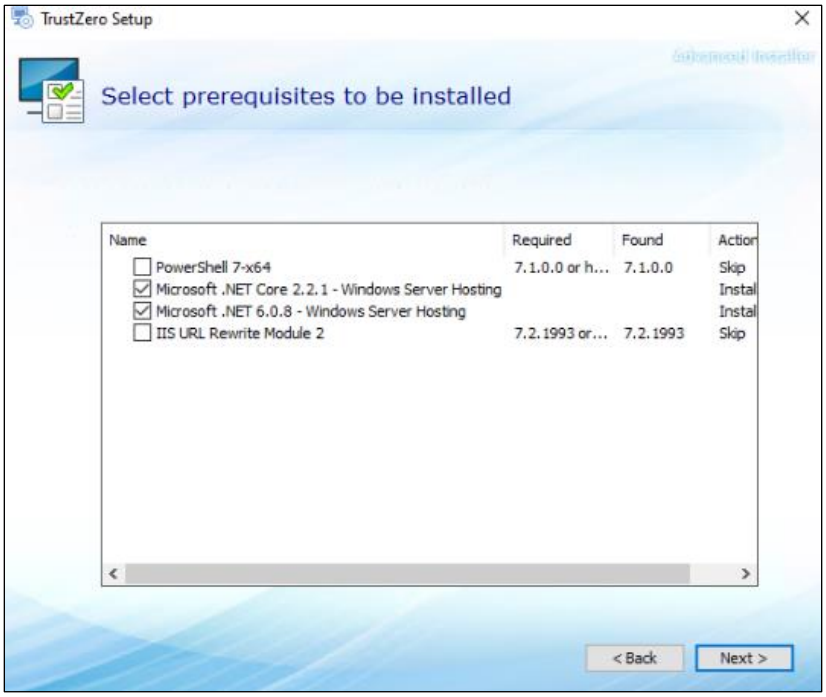
Microsoft Edge: Supported version of Microsoft Edge browser v137 or later (64-bit) to access the TrustZero Administrator Application on a web browser.

Enterprise PKI: Several TrustZero components require TLS certificates for secure operation. If an enterprise PKI is unavailable, commercial publicly trusted TLS certificates may be used instead.

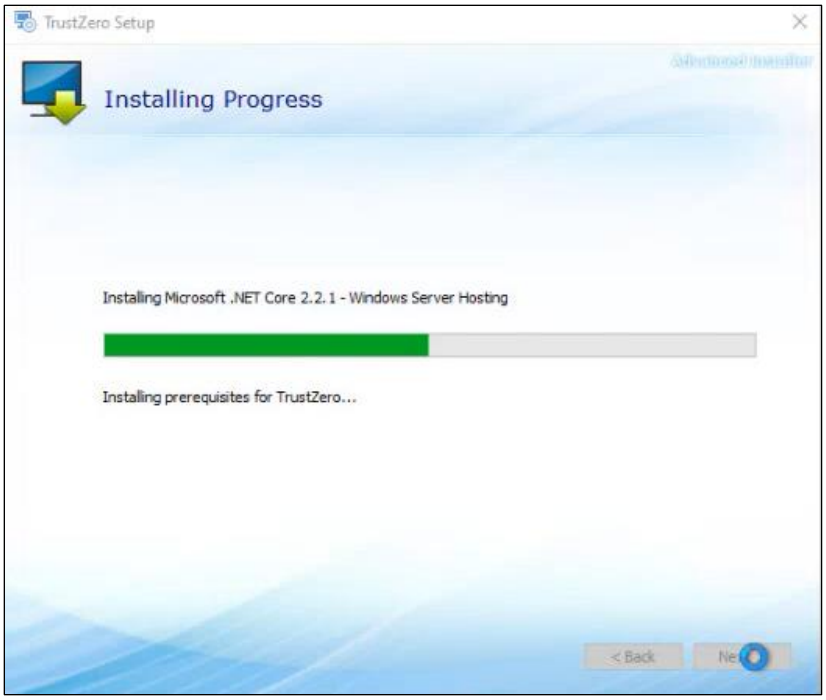
Product Installation

1. Obtain the installer file from your system integrator.
2. Run the installer file. The Prerequisites Setup Wizard displays.
3. Click **Next**.

4. Select the prerequisites to install. For TrustZero, select **.NET Core 2.2.1** and **.NET 8**.
5. Click **Next**.



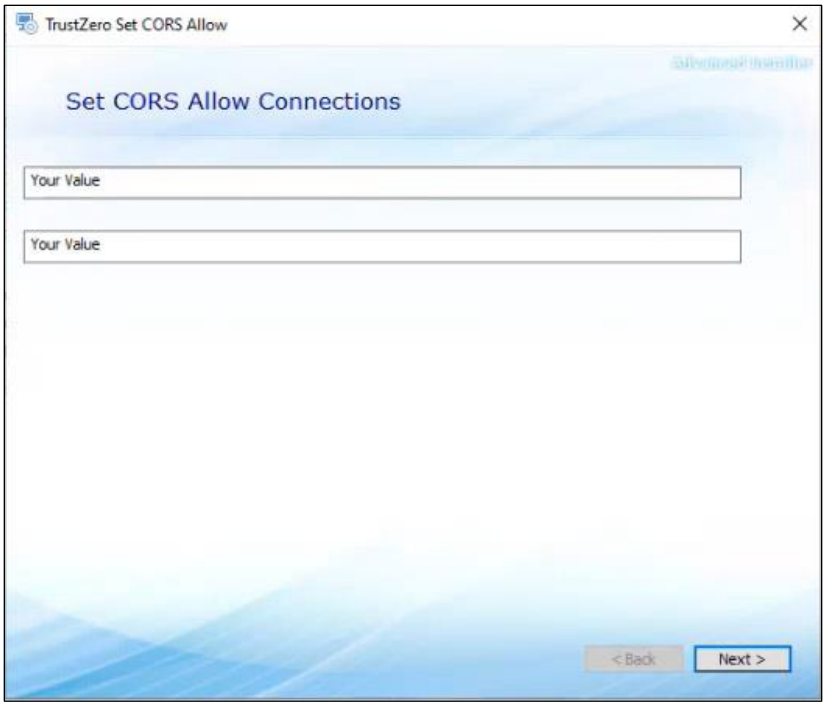
6. The screen displays a progress bar as the prerequisites are installed. Once the installation is complete, click **Next**.



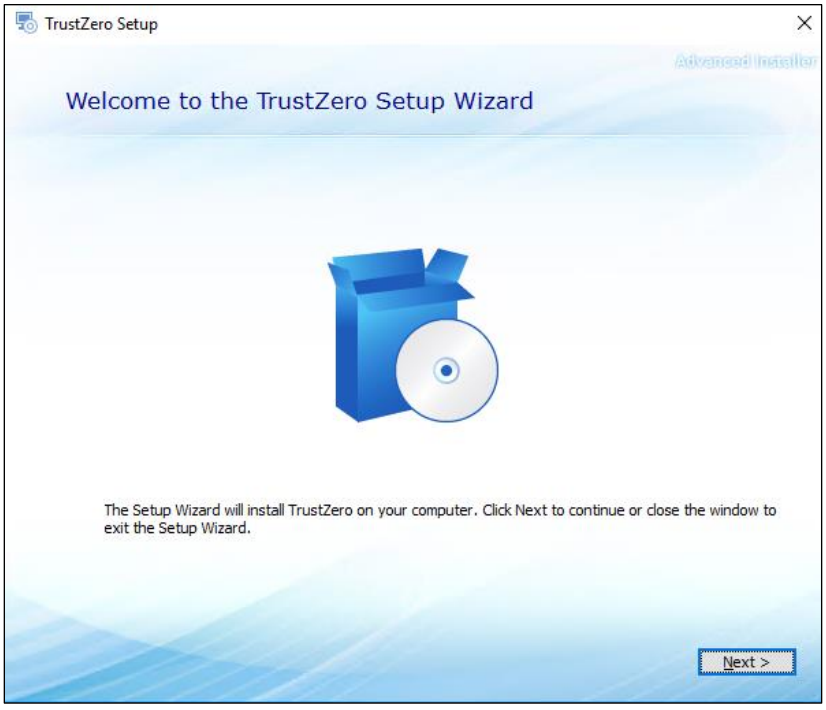
7. In the Set CORS Allow Connections screen, enter the URL for TrustZero in the first **Your Value** field. Leave the second field blank.

> **Note:** The CORS value tells the server if the HTTP request or response is allowed to access the requested resources. The CORS value must match the TrustZero UI's address and port for the application to work as expected.

8. Click **Next**.



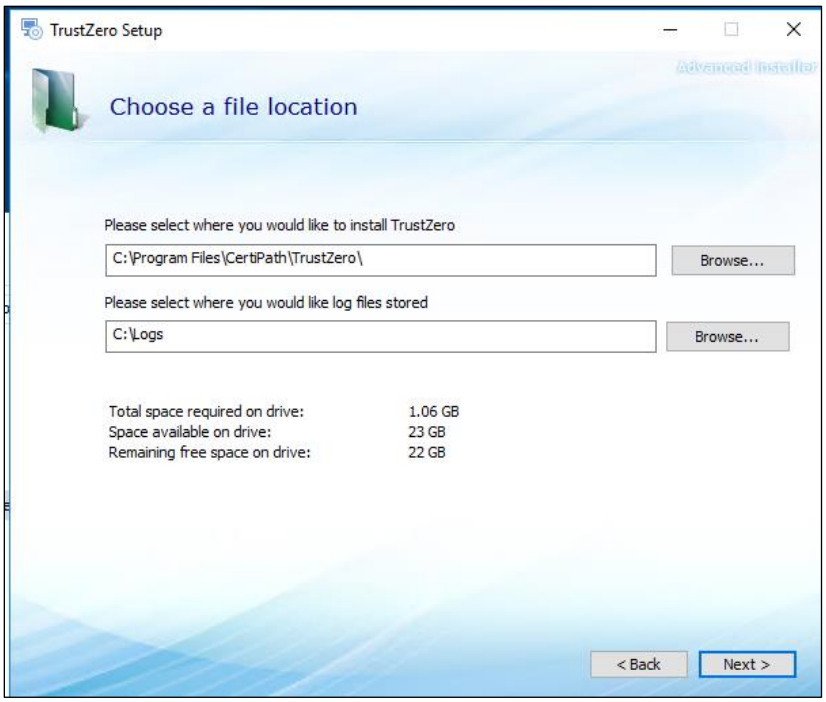
9. In the TrustZero Setup Wizard, click **Next**.



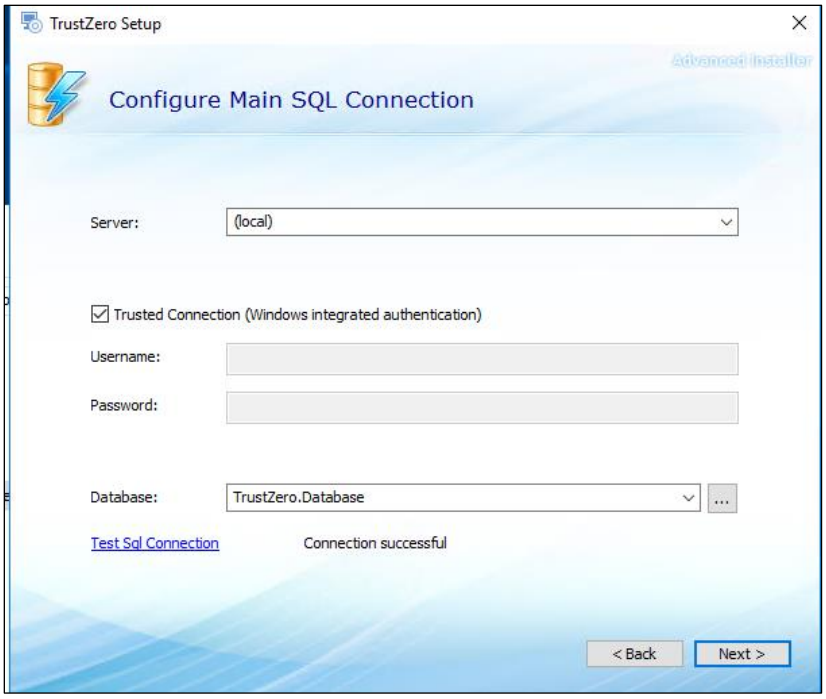
10. Select the file location where you would like to install the TrustZero application and select the location where you would like to store log files.

Note: TrustZero audit logging is written directly to the application database. The location selected in Step 10 for storing log files should be applicable for runtime production use.

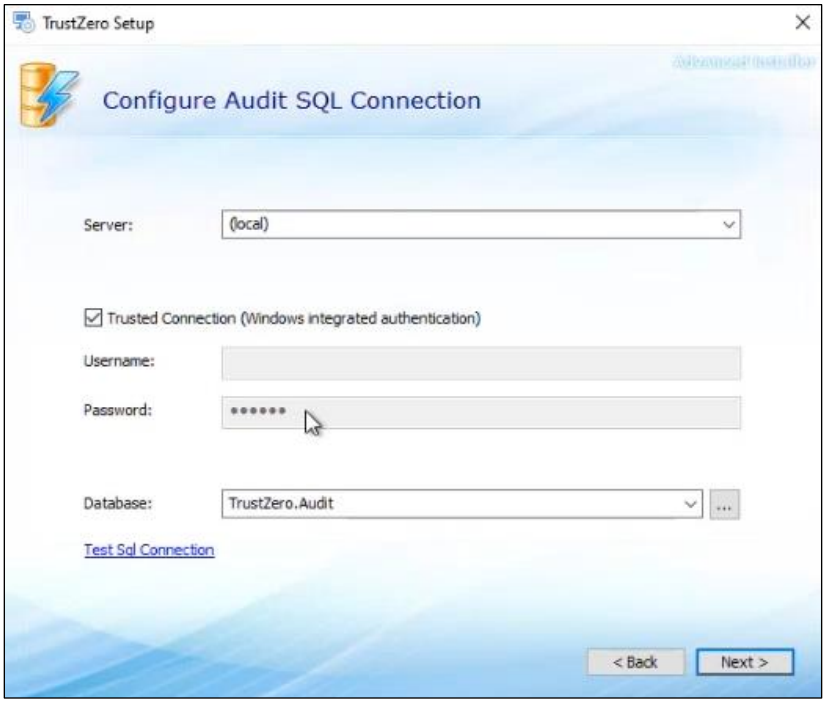
11. Click **Next**.



12. In the Server field, select **(local)**. Check the **Trusted Connection** box.
13. Click the **Test SQL Connection** link and ensure that a “Connection Successful” message displays.
14. Click **Next**.

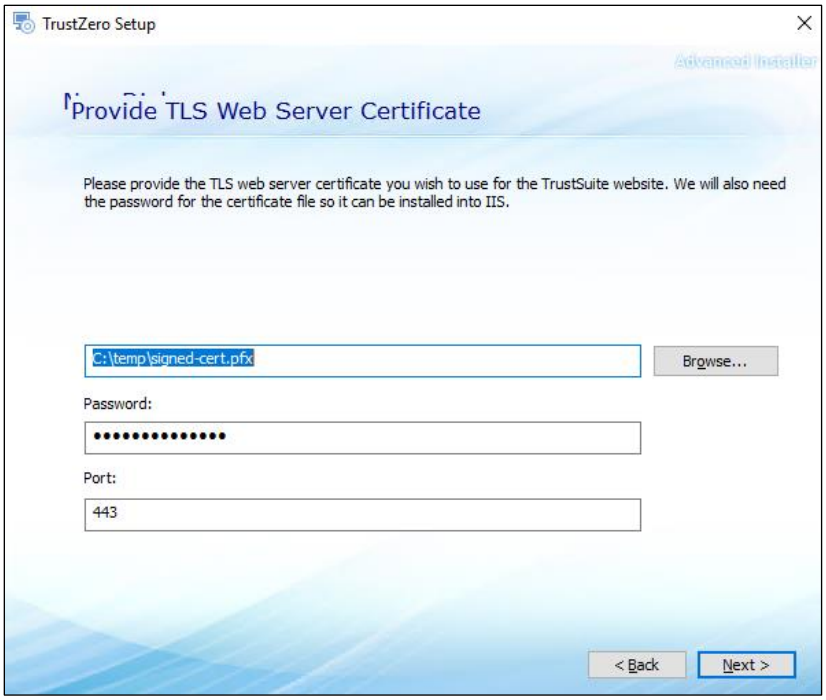


15. In the Server field, select **(local)**. Check the **Trusted Connection** box.
16. In the Database field, enter **TrustZero.Audit**.
17. Click the **Test SQL Connection** link and ensure that a “Connection Successful” message displays.
18. Click **Next**.

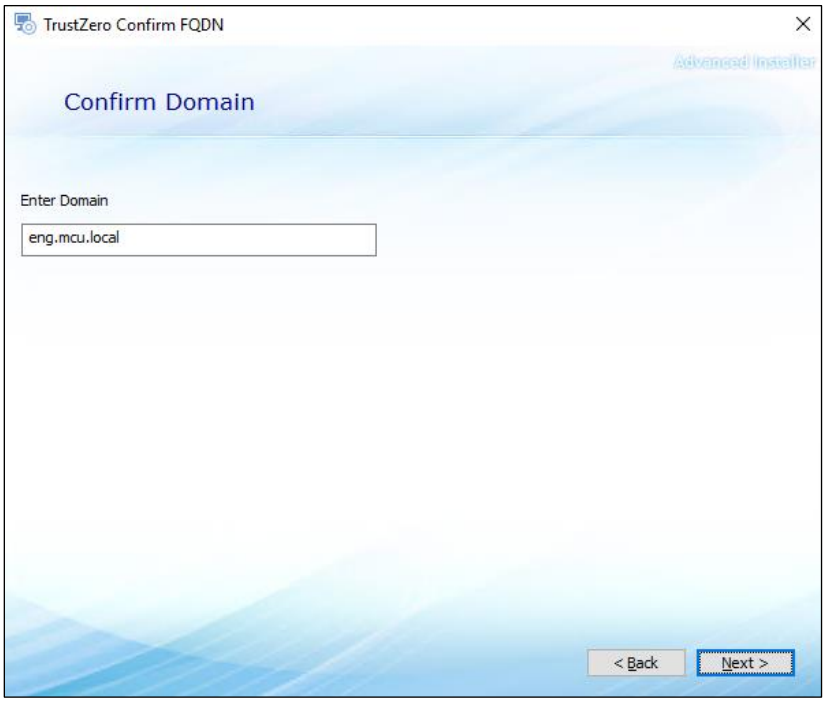


19. In the Provide TLS Web Server Certificate screen, browse to the location where the TLS Certificate is stored.

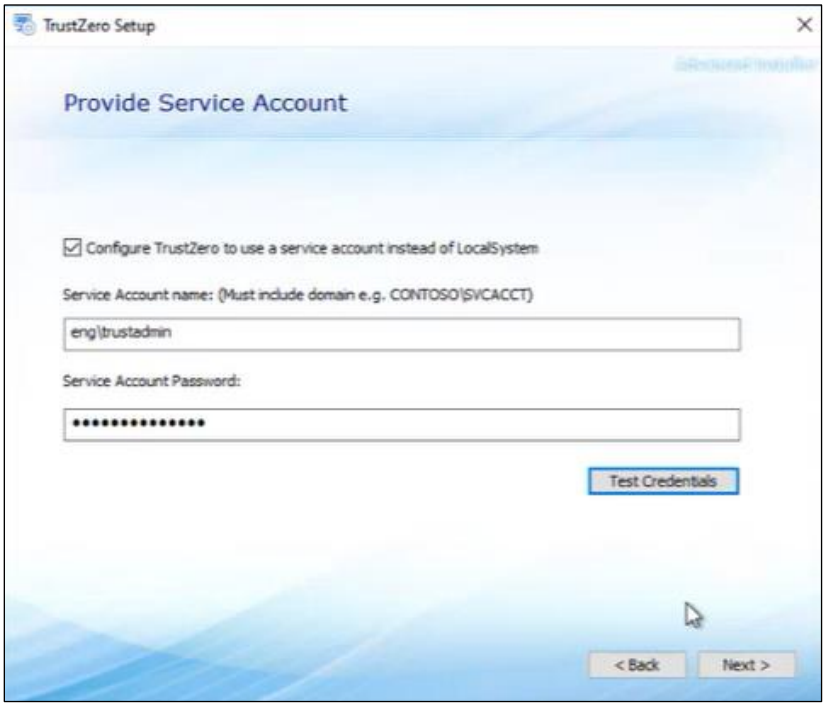
20. In the Password field, enter the password for the certificate file.
21. In the Port field, enter **443**.
22. Click **Next**.



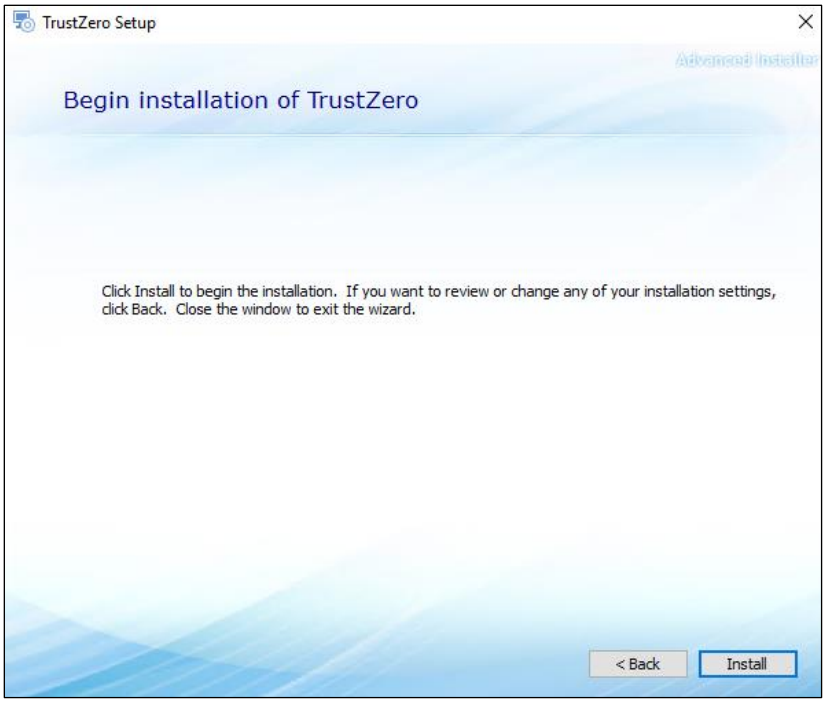
23. In the Confirm FDQN screen, enter the fully qualified domain name for the TrustZero installation.
24. Click **Next**.



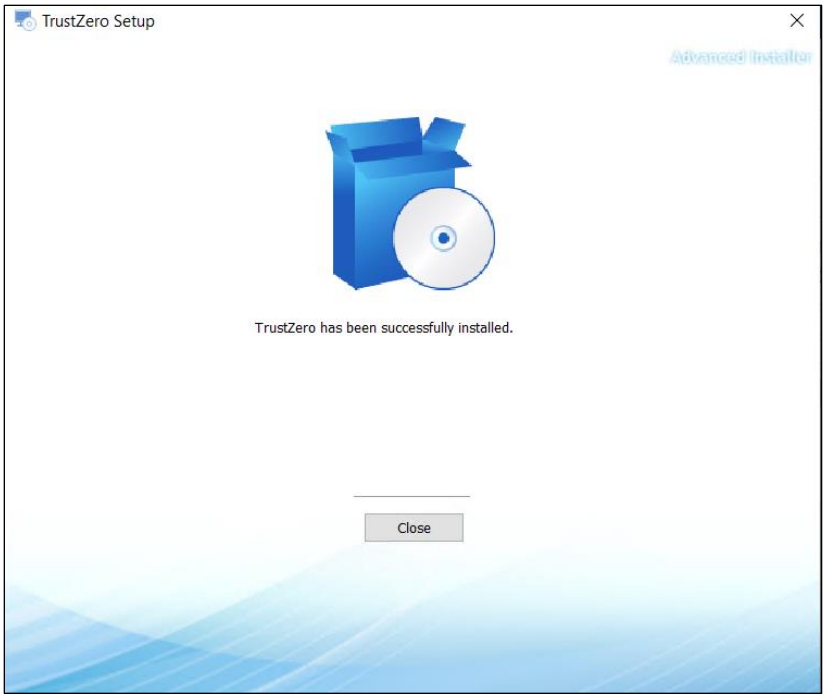
25. Check the **Configure…** box. In the Service Account Name field, enter an account name (including the domain). In the Service Account Password field, enter a password for the service account.
26. Click **Test Credentials**. If the credentials are correct, a “Test was successful” message displays. Click **OK**.
27. Click **Next**.



28. In the Begin Installation screen, click **Install**.



29. When the installation is complete, a “TrustZero has been successfully installed” message displays. Click **Close**.



Initial Post-Installation Configuration

After successfully installing TrustZero, the TrustZero web application and database components may require additional configuration.

These post-installation configuration steps include:

- CertiPath Task Runner Service Configuration
- Microsoft IIS Web Server Configuration
- Smart Card Login Configuration via Microsoft IIS
- Confirmation of Database Encryption Settings
- Configuration of Organizational Components in TrustZero Database
- Change TrustZero JWT Signing Key in Raw App Configs
- TrustZero Application Endpoint and Client Certificates
- Confirm TrustZero Integration Retry Intervals

CertiPath Task Runner Service Configuration

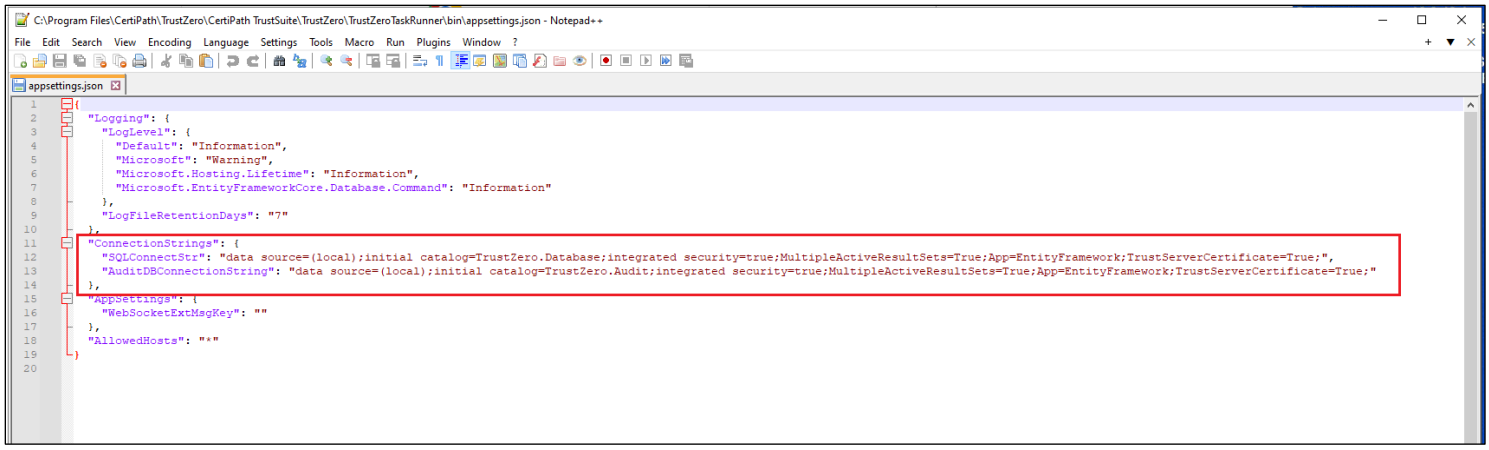
Perform the following steps on the Microsoft Windows server running TrustZero application services to ensure that the Task Runner service is running as expected:

1. Navigate to **…\Program Files\CertiPath\TrustZero\CertiPath TrustSuite\TrustZero\TrustZeroTaskRunner\bin**
2. Open the **appsettings.json** file.
3. Verify that the following lines are in the appsettings.json file under **ConnectionStrings**. If these lines are missing, add them to the file:

"SQLConnectStr": "data source=(local);initial catalog=TrustZero.Database;integrated security=true;MultipleActiveResultSets=True;App=EntityFramework;TrustServerCertificate=True;",

"AuditDBConnectionString": "data source=(local);initial catalog=TrustZero.AuditDB;integrated security=true;MultipleActiveResultSets=True;App=EntityFramework;TrustServerCertificate=True;"
},

Note: If the SQL server is not local, change the “data source=(local)” value to reflect the location of the SQL server.



4. Save and close the file.
5. In the same folder, open the **log4net.json** file.
6. Scroll to lines 123-127.
7. Ensure that the following lines are removed from the log4net.json file:

```
<log4net>
<appender name=”AdoNetAppender” type=”log4net.Appender.AdoNetAppender”>
<connectionString connectionString=”Your Value”/>
</appender>
</log4net>
```

8. Save and close the file.

Microsoft IIS Web Server Configuration

Do the following on the Microsoft Windows Server running Internet Information Services (IIS):

- Configure the deployed web application to use an enterprise-trusted web server certificate (if not set directly during installation Step 17).
- Ensure that all web server security settings are applied in accordance with your organizational standards.

Note: Use of TLS 1.3 and U.S. NIST-approved cryptographic standards is recommended for all production and production-representative systems. Optionally, mutual TLS may be enabled for TrustZero Admin UI access using Smart Card Login as described in the following section.

Smart Card Login (SCL) Configuration via Microsoft IIS

The TrustZero installer applies Windows Authentication directly in the Microsoft IIS web application as part of initial setup. No additional action should be required if your organization requires and enforces Smart Card Login via Microsoft Windows Group Policy.

Confirmation of Database Encryption Settings

Do the following on the Microsoft SQL Server instance used for TrustZero operation:

- Configure the database connection to use both TLS and an enterprise-trusted web server certificate (if not set directly during installation Step 17).
- Configure the database owner/schema to apply Microsoft Transparent Data Encryption (TDE).

Note: Use of Microsoft TDE with strong NIST-approved cryptography is recommended for the protection of production data at rest, particularly for database elements that may store personal or privacy-related attributes.

Configuration of Organizational Components in TrustZero Database

On the Microsoft SQL Server instance used for TrustZero operation:

- If your deployment includes CertiPath TrustManager and TrustMonitor using multiple organizational components, additional configuration records are required in the Components table of the TrustZero database.
- For the single PACS that TrustZero uses, the component name must match the component name in TrustManager.

Note: To configure an organization, an Organization column must be added to the Audit database table.

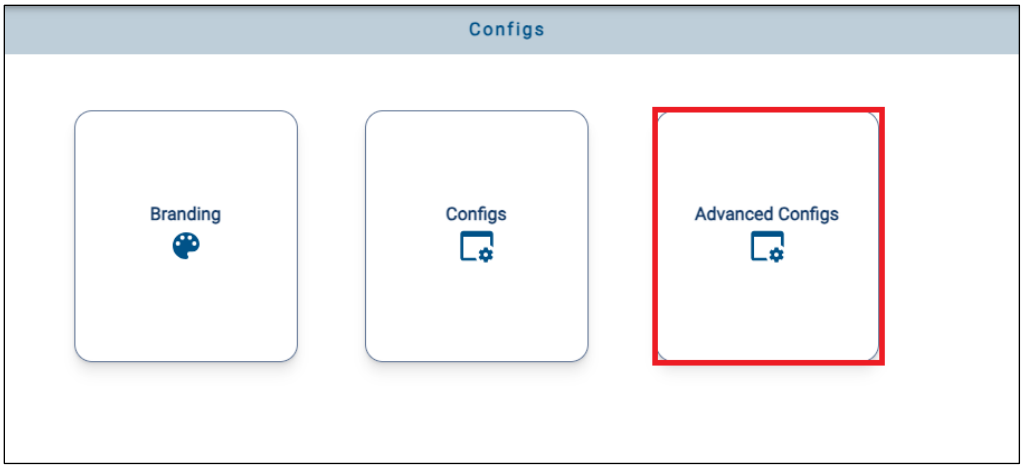
To enable the PACS and Validation Systems page, the database must be initiated with seed data for an organization and a PACS for that organization. After the initialization, the PACS can be configured in the UI by visiting https://SERVER.NAME:8443/pacs-connection/add-edit-connection/?id=1&guid=.

Change TrustZero JWT Signing Key in Advanced Configs

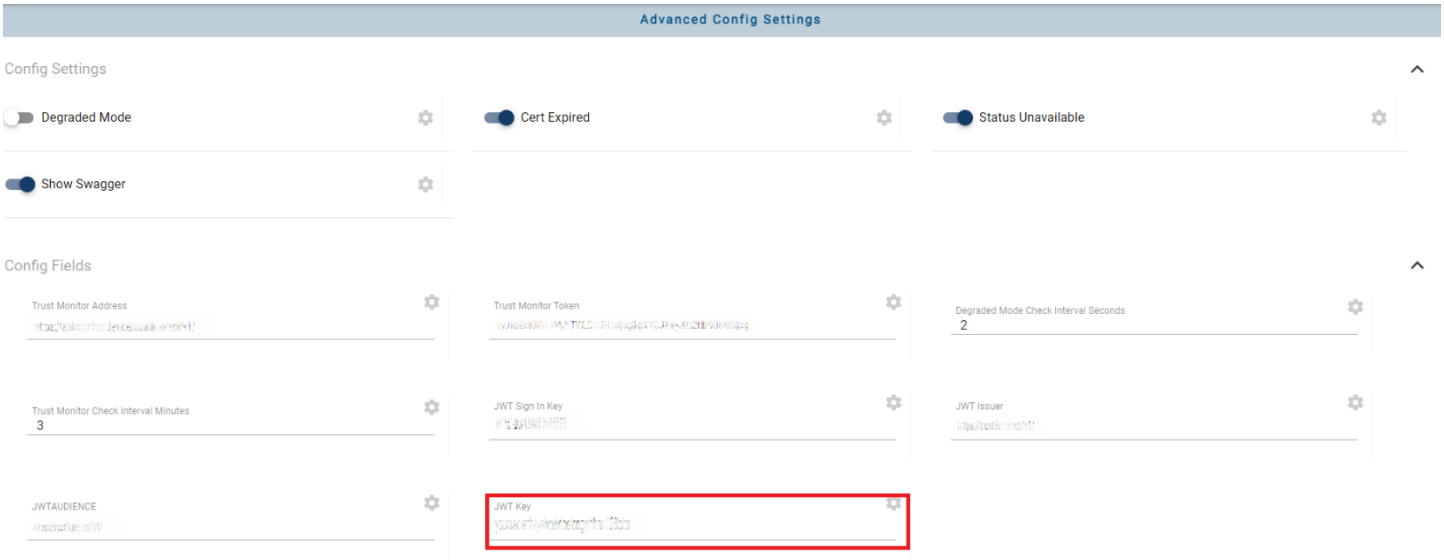
Note: Resetting the JWT signing key is required immediately after installing TrustZero in a production or controlled IT environment.

1. Use the procedures in the Accessing the TrustZero Administrator UI section of the TrustZero 1.5 Administrator and User Guide to access the TrustZero Administrator UI web application.
2. On the home screen, select the **Configuration Settings** card.

3. In the Configuration Settings screen, select the **Advanced Configs** card.



4. Generate a new JWT signing key and replace the key value in the **JWTSIGNINGKEY** field.



5. Click **SAVE CONFIGS** button to save the new value for this field.

TrustZero Application Endpoint and Client Certificates

Do the following on the Microsoft Windows Server running TrustZero application services:

- Configure the deployed TrustZero service to use an enterprise-trusted web server certificate.
- Configure the deployed TrustZero service to use an enterprise-trusted client certificate (where applicable).
- Ensure that all web server security settings are applied in accordance with your organizational standards

Note: Use of TLS 1.3 and U.S. NIST-approved cryptographic standards is recommended for all production and production-representative systems.

Confirm TrustZero Integration Retry Intervals

Recommended settings for production installation:

- Base Retry Intervals between 15 and 60 seconds are recommended for production use.
- A Number of Retries value between 5 and 10 is recommended for production use.
- Validity checking intervals between 5 and 15 minutes are recommended for production use.