Installation and Configuration Guide

July 14, 2025

For use with TrustManager 2.4

Table of Contents

TrustManager Installation and Configuration

TrustManager is CertiPath's integration solution for provisioning and lifecycle management of personnel records and high-assurance credentials across physical access control systems (PACS). With TrustManager alone, these credentials can be managed within a client enterprise. When TrustManager is paired with TrustMonitor®, community federated credential provisioning is also supported.

Feature Summary

- Ability to manage identity and access across diverse PACS infrastructure, including intercommunity federal provisioning for end-to-end identity lifecycle management
- Leverage data from smart cards to establish a common identity across government agencies
- Interoperable with multiple IDMS, CMS, and PACS
- Enables policy automation across the enterprise to eliminate multi-organization or community policies
- Built-in workflow tool to customize API connections
- Ability to log in and authenticate with a smart card
- Supports standalone proximity-based credentials and dual-hybrid smart cards and proximity tokens
- FICAM v2 compliant

Installation Prerequisites

The following sections describe the systems and environments that support successful installation and configuration of **TrustManager 2.4.**

System Prerequisites

TrustManager Admin Application

Description: Application/Web Server

VM Configuration: 4 cores/16GB memory/64GB VHD

Operating System/Server Configuration:

- Windows Server 2022 or later
- Microsoft IIS, .NET8 or later

Database Server

Description: Microsoft SQL Server

VM Configuration: 4 cores/16GB memory/64GB VHD

Operating System/Server Configuration:

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

Note: TrustManager can integrate with an existing SQL Server.

Environmental Prerequisites

Compatible PACS and Validation System: Must perform proper certificate validation of credentials on a regular basis. Compatible systems:

PACS:

- Gallagher PIV Command Centre (9.0)
- Identiv Hirsch Velocity (3.8 and 3.7)
- Lenel OnGuard (8.2 and 8.1)
- Tyco C•CURE 9000 (2.9 and 3.00.2 with Innometriks HA)

Validation Systems:

- HID pivCLASS (5.31 and 5.30 pivCLASS Client)
- Innometriks HA Service (2.5.2.18)
- CertiPath TrustZero® (1.7 configured with Lenel 8.2)

Compatible Credential Management Systems:

- **Intercede MyID (**12.13 or later)

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

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

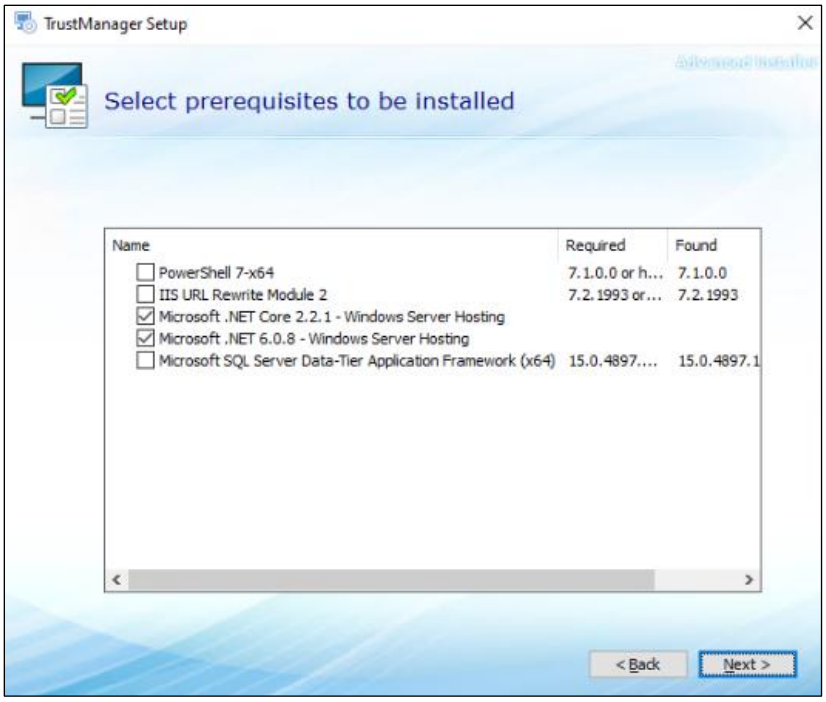
Enterprise PKI: Several TrustManager components require TLS certificates for secure operation. If an enterprise PKI is unavailable, commercial publicly trusted TLS certificates may be used instead.

Product Installation

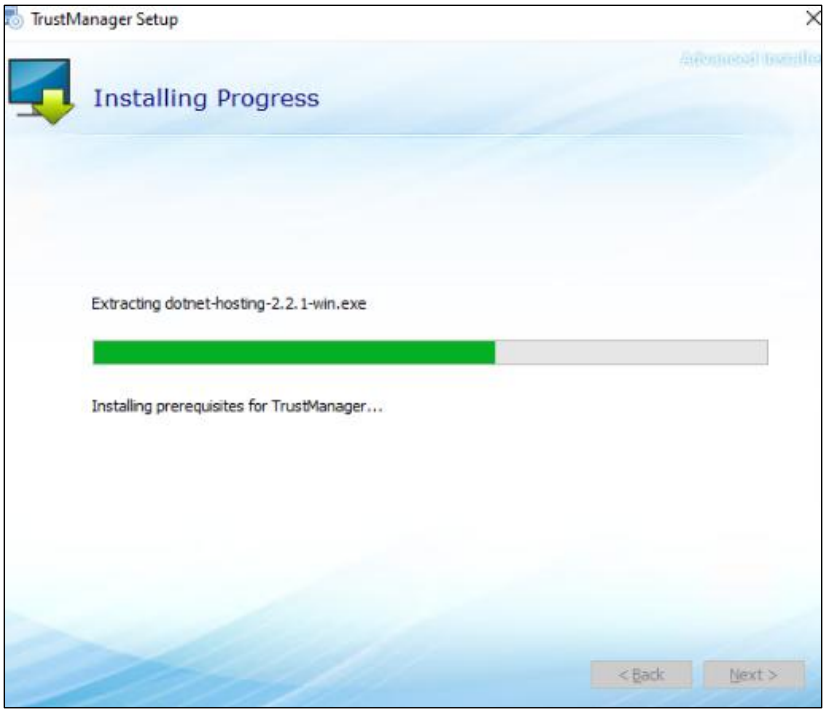
Note: For upgrades of the TrustManager application, the existing application must first be uninstalled. Once the uninstall is complete, proceed with the following steps.

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 TrustManager, select **.NET Core 2.2.1** and **.NET 8**.
5. Click **Next**.

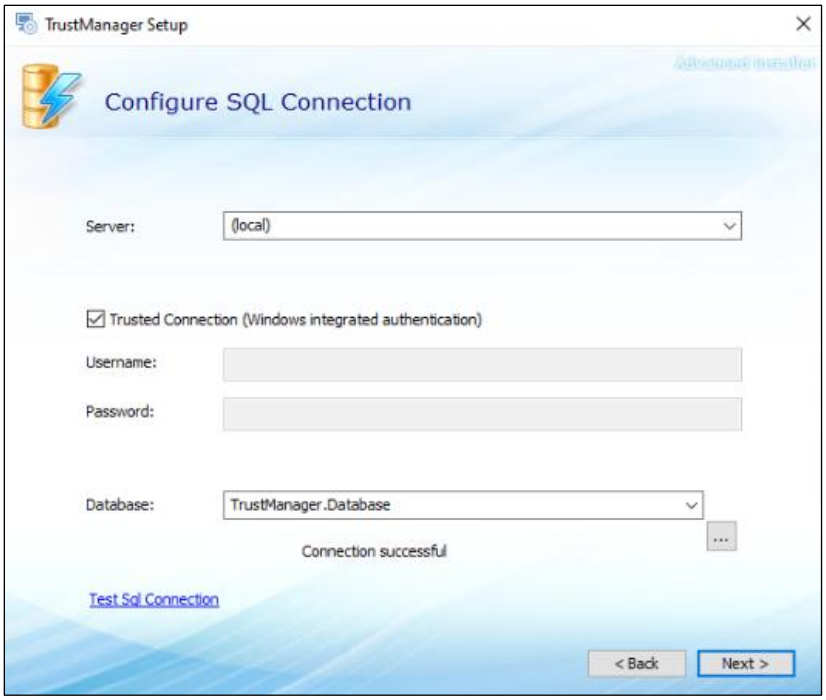


6. The screen displays a progress bar as the prerequisites are installed. Once the installation is complete, click **Next**.



7. In the TrustManager Setup Wizard, click **Next**.

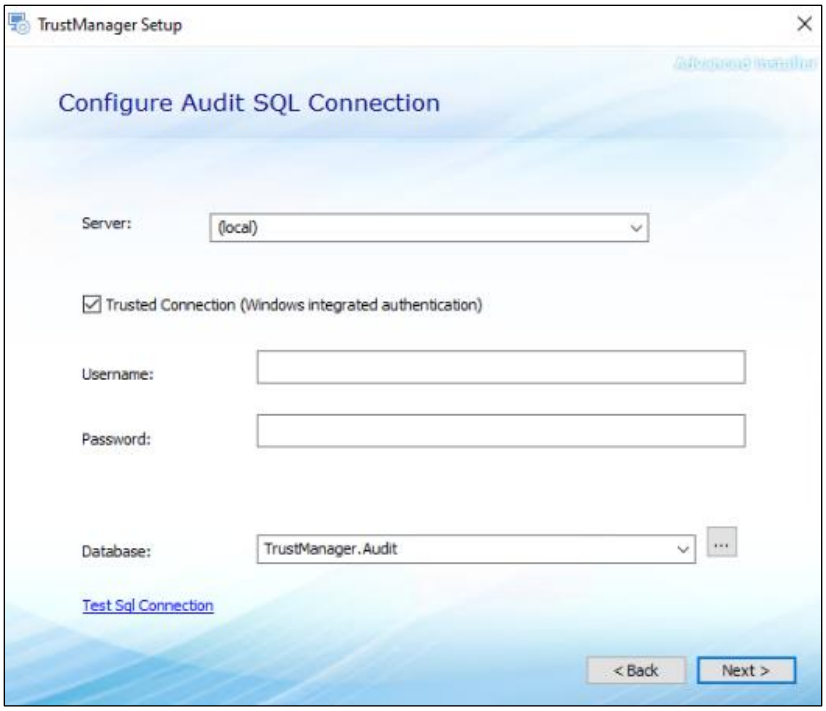
8. In the Server field, select **(local)**. Check the **Trusted Connection** box.
9. Click the **Test SQL Connection** link and ensure that a “Connection Successful” message displays.
10. Click **Next**.



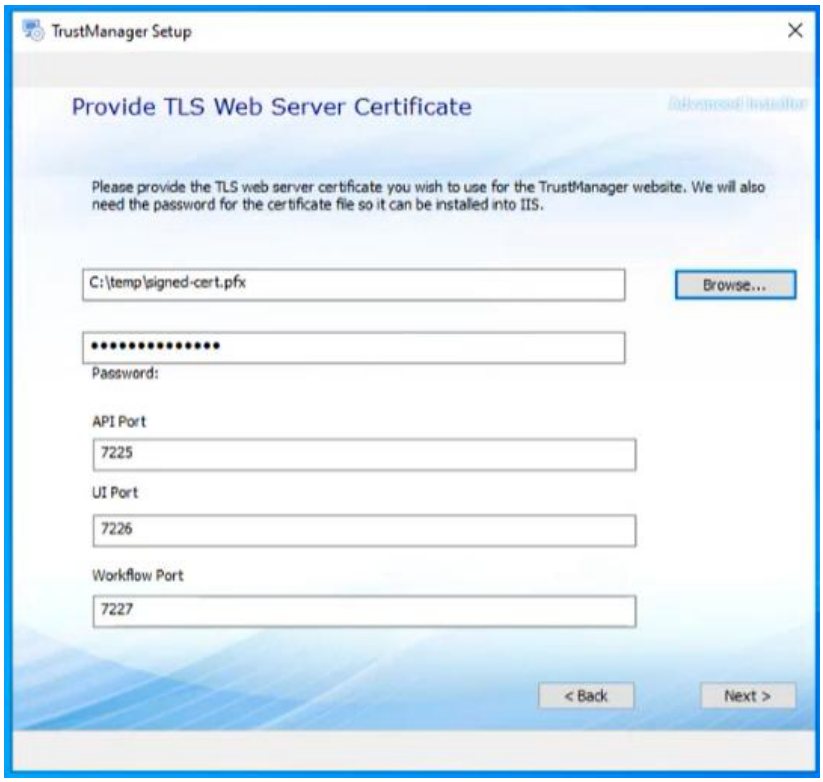
11. In the Server field, select **(local)**. Check the **Trusted Connection** box.

> **Note:** If the SQL server is not local, the server name will need to be entered manually.
>
> **Note:** If SQL exists on a different server, the Application Pool needs to be configured from the network service and connected using the domain account or the server needs to be allowed to connect to SQL.

12. Click the **Test SQL Connection** link and ensure that a “Connection Successful” message displays.
13. Click **Next**.



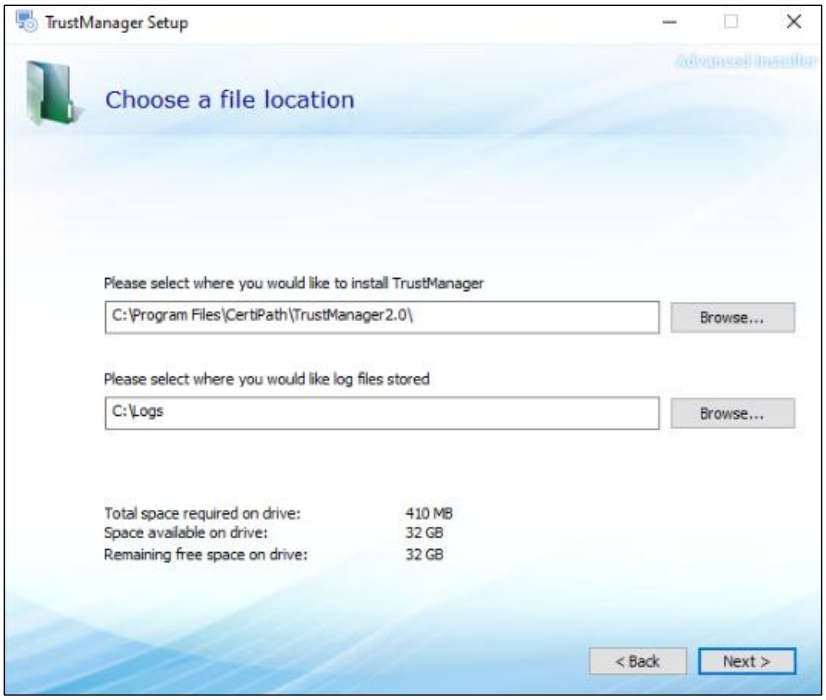
14. In the Provide TLS Web Server Certificate window, browse to the location where the TLS Certificate is stored.
15. In the Password field, enter the password for the certificate file.
16. In the Port fields, enter the following:
    a. API Port: **7225**
    b. UI Port: **7226**
    c. Workflow Port: **7227**
17. Click **Next**.



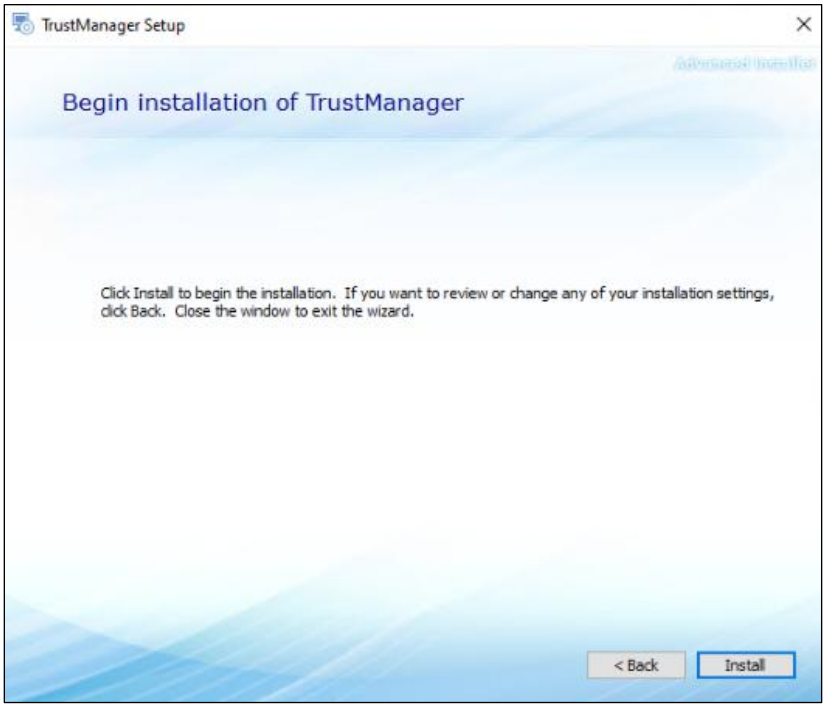
18. Select the file location where you would like to install TrustManager and select the location where you would like to store log files.

> **Note:** TrustManager audit logging is written directly to the application database. The location selected in Step 17 for storing log files should be applicable for runtime production use.

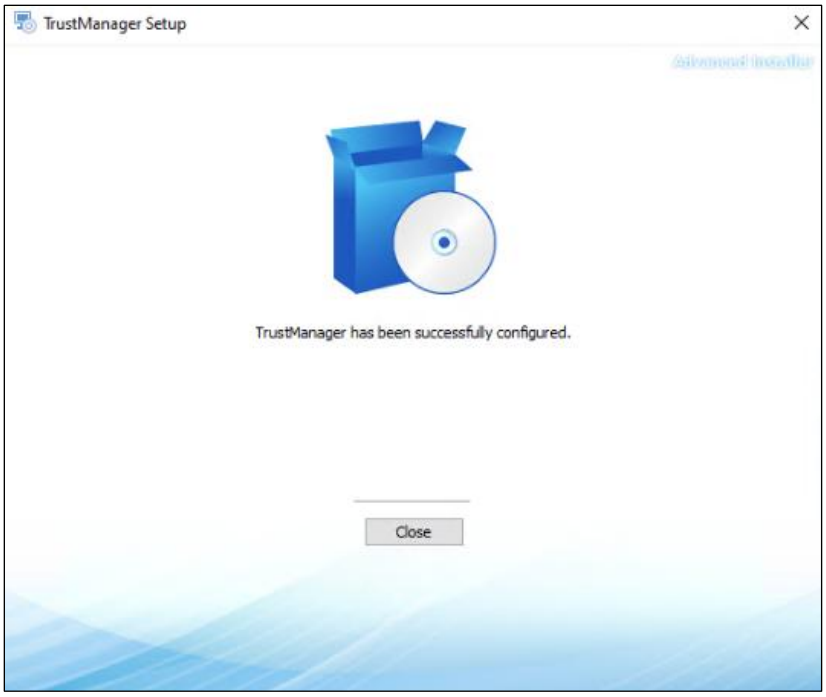
19. Click **Next**.



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



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



22. Use the procedures in the Accessing the TrustManager Administrator UI section of the TrustManager 2.2.2 Administrator and User Guide to access the TrustManager Administrator UI web application.

Initial Post-Installation Configuration

After successfully installing TrustManager, Installer workflow, the TrustManager web application and database components may require additional configuration.

These post-installation configuration steps include:

- Microsoft IIS Web Server Configuration
- Smart Card Login Configuration via Microsoft IIS
- Confirmation of Database Encryption Settings
- Change TrustManager JWT Signing Key in Database
- TrustManager Application Endpoint and Client Certificates
- Confirm TrustManager Integration Retry Intervals

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 13).
- 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 TrustManager Admin UI access using Smart Card Login as described in the following section.

Smart Card Login (SCL) Configuration via Microsoft IIS

The TrustManager 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 TrustManager operation:

- Configure the database connection to use both TLS and an enterprise-trusted web server certificate (if not set directly during installation Step 13).
- 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.

Change TrustManager JWT Signing Key in Database

- Generate a new TrustManager JWT signing key.
- In the following script, replace the value on Line 2 with the new JWT signing key.
- Then, in the SQL Server where TrustManager is installed, execute the script to update the JWT Signing Key for this instance of TrustManager.

```
UPDATE AppConfig
SET Value = '6641AE51-2D58-4020-BAAF-0FF78E0B321E'
WHERE Environment='prod' and [key]='JwtSigningKey'
```

TrustManager Application Endpoint and Client Certificates

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

- Configure the deployed TrustManager service to use an enterprise-trusted web server certificate.
- Configure the deployed TrustManager 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 TrustManager 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.