dormakaba

Community

Installation Guide

PK3695 2.4.0 - 05/2025
Original document

EN

dormakaba Canada, Inc.
105 Marcel-Laurin Blvd
Montreal, Quebec H4N 2M3
T: +1 866-dormakaba (1-866-367-6252)

www.dormakaba.com

Table of contents

1 About this document

1.1 Validity

This document describes the product:

Product designation:	Community
Version:	2.4

1.2 Target audience

This document is for IT specialists responsible for all tasks related to installing the Community Server and Community Client.

1.3 Purpose and objective

The purpose of this document is to provide information and instructions to support all tasks related to installing Community. The document lists requirements and includes pre-installation checklists.

1.4 Additional documents

Community User Guide 2.4.0 (PK3706-EN)

Community Release Notes 2.4.0 (PK3696)

Community Enhanced Key Security 2.4.0 (PK3776)

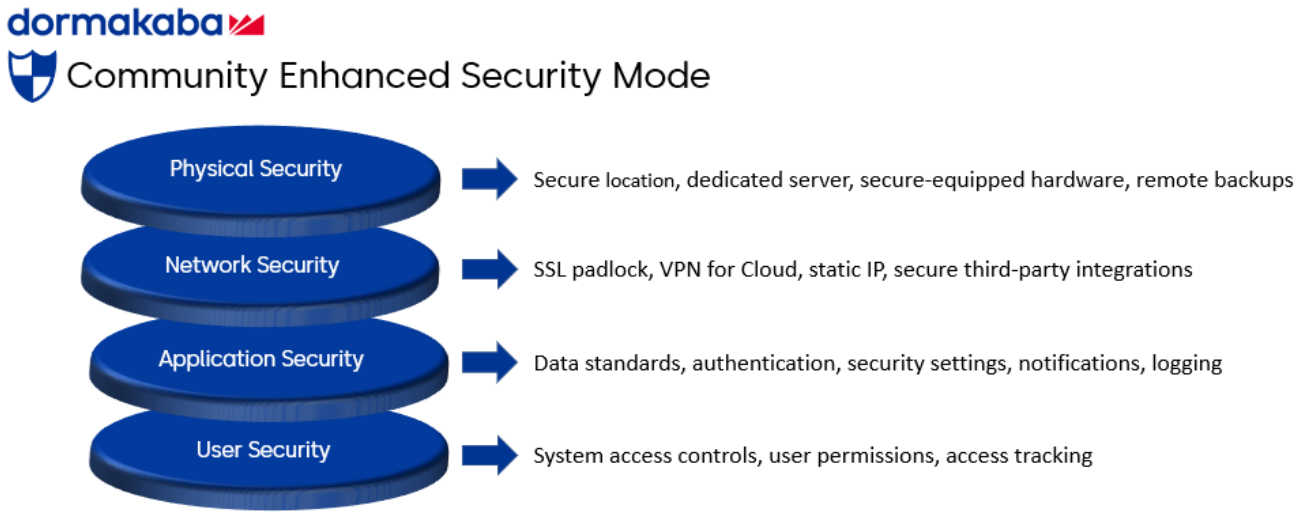
2 Welcome

Community® is flexible and easy-to-use management software for multihousing properties. Developed for security and designed for users, the application streamlines access control management and provides an efficient and user-friendly method to setup and operate apartment buildings, student housing, senior living, and other multi-tenant properties. Flexible configuration and integration options showcase a robust feature set including mobile key access and resident-delegated visitor management. Guided workflows simplify property configuration, staff and vendor management, key issuance, and resident management. Configurable user permissions secure system access. Lock and system data collection supports detailed access point audits and reporting. Remote lock management provides immediate and convenient control of access points. Seamless integration with Keyscan Aurora Access Control extends management to connected perimeter doors and removes the pain of syncing resident and staff data between different systems.

3 Security overview

As a leader in the access control industry, dormakaba recognizes the continuously evolving nature of security technology. We strive to make ongoing improvements in our products, and we encourage our customers to implement enhanced authentication and encryption protocols. Moreover, dormakaba recommends configuring security-related options available in Community and adopting standard best practices.

This chapter presents security-related options and best practices based on the relevant layer of security. Enhanced security mode is prioritized as the principal and strongest recommendation to ensure end-to-end security.



3.1 Enhanced security mode

Enabling enhanced security mode introduces an additional layer of security for protecting data on RFID keys. The technological shift increases the integrity of the entire access management system. With enhanced key security:

- All keys include enhanced security.
- Data encoded on keys is protected using global encryption standards.
- Encoders support advanced encryption standards.
- Lock programming is protected with stronger encryption and authentication.
- Locks are programmed to accept only high-security keys.

Enhanced key security requires devices that are compliant with advanced encryption standards and authentication protocols. Locks, encoders, Maintenance Units, RFID keys and elevator controllers must meet minimum requirements. For details, refer to the relevant sections in Device requirements.

Implementing enhanced key security involves establishing device requirements and enabling enhanced security mode in System Settings. Refer to the document *Community Enhanced Key Security* accessible at the root of the software download folder. The document describes options and provides step-by-step instructions for enabling enhanced security mode. The document also contains important information for sites that upgrade without enhanced key security.

3.2 Physical security

Physical security is the foundation upon which all additional layers of security depend.

3.2.1 Hardware selection

When planning an initial deployment or upgrade, use hardware that supports enhanced security:

- Server–A dedicated server is recommended for Community.
- Locks– All lock profiles in Community support enhanced security except RT and Confidant.
- M-Units–(Maintenance Units) Use only type M-Unit Saflok HH6 NFC. Required for enhanced security mode.
- Encoders–Use only type dormakaba RFID Encoder II, part number 75720. Required for enhanced security mode.
- RFID keys–Please be advised that many access cards utilized in RFID systems have become susceptible to cloning and related attacks over the years. Notably, certain legacy card technology has been the subject of published vulnerability reports. dormakaba recommends using credentials utilizing MIFARE DESFire EV2/EV3 to provide an additional layer of security for the installed version of Community
  - For resident credentials–Select the more secure credentials MIFARE DESFire EV2/EV3 which have security features that offer additional protection against cloning.
  - For staff/vendor credentials–Our recommendation is also to use MIFARE DESFire EV2/EV3. This will offer an additional layer of security for the access management software presently installed at your property. Our implementation of the MIFARE Plus credential was designed to provide compatibility with legacy solutions, specifically MIFARE Classic. As a result, for this particular application MIFARE Plus will not provide the same level of security as Ultralight C.

3.2.2 Installation / upgrades

- Install the Community server in a secure physical location.
- dormakaba strongly recommends scheduling automated backups to a remote server and storing backup and archival data in a secure location off-site. Requirements apply to back up to a remote server. For upgrades, take a backup of the database before performing the upgrade. For online systems, take backups of Community SQL Server and MongoDB databases. See System Settings > Database Backup.

3.3 Network security

Prior to deployment, a dormakaba technician works with site IT to discuss network requirements. Review the following best practices and security-related options.

3.3.1 Installation

- Prior to starting the installation, verify that all Windows updates are installed.
- Configure the Community server with a static IP address.
- dormakaba strongly recommends installing an SSL certificate to enable the HTTPS protocol. The SSL certificate to enable HTTPS mode must be provided by a well-known and trusted certificate authority. If you opt to install an SSL certificate post-installation, use the Service Manager for a streamlined transition.
- If deploying Community on a cloud VM (virtual machine), a VPN (virtual private network) is required to secure the communication between the site and cloud VM.
- Versioning controls dictate that Community workstations are required to be at the same version as the Community server to program locks and encode/read keys.

3.3.2 Configuration

- Communication ports–Default secure ports are listed in product release notes. When necessary, consult a dormakaba technician for customizing ports. See Communication ports.
- HTTPS Browser Certificate–When Community is deployed with an SSL certificate, specify the number of days before the certificate expires to start receiving a daily warning. See System Settings > Security > HTTPS Browser Certificate.
- Secure email notifications–When SSL is enabled and security certificates are valid, all email data sent from the email server to mail clients is private and secure. See System Settings > Email Configuration.
- Integrations–Integrate only with third-party applications that support secure communication. See Communication ports and obtain integration documentation from dormakaba Customer Service.

3.4 Application security

Community supports industry data standards and recommends taking advantage of security-related options. See also Proprietary design decisions.

3.4.1 Data standards

- PCI-DSS–Select whether to enable PCI-DSS (Payment Card Industry Data Security Standard), an information security standard for organizations that handle credit cards. Recommended value: YES. When you enable PCI-DSS, the Enable security questions option in Password Reset is set to YES and cannot be disabled.

3.4.2 Security features

- Enhanced security mode–This setting enables enhanced encryption for encoding data on keys. Default: NO. See System Settings > Security > Enhanced Security Mode.
- RFID key types–dormakaba recommends enabling enhanced security mode which supports MIFARE DESFire EV2/EV3 (recommended), MIFARE Plus and MIFARE Ultralight C. When enhanced security mode is not enabled, dormakaba recommends MIFARE DESFire EV2/EV3 (Standard Security). See System Settings > Advanced > RFID key types.
- M-Unit authentication–Select whether to require M-Unit authentication. When authentication is enabled, M-Unit credentials are required to program and audit locks. When authentication is enabled, M-Unit credentials must be configured in Staff/Vendor Management for at least one operator. Required for enhanced security mode. See System Settings > Security > Maintenance Unit.
- M-Unit security code–When enhanced security mode is enabled, a security code is required to program locks with the M-Unit. See System Settings > Security > Enhanced Security Mode.
- API authentication–Select whether to require authentication for API requests. When authentication is enabled, API credentials must be configured in Staff/Vendor Management for at least one operator. See System Settings > Security > API.
- Lock access–Review settings for Escape return, Quick relatch, and Disability mode to fine-tune lock access after a door opens. See System Settings > Security > Lock Access.
- Data security–dormakaba strongly recommends scheduling automated backups to a remote server and storing backup and archival data in a secure location off-site. Requirements apply to back up to a remote server. See System Settings > Database Backup.
- PPK/SPK–Primary and secondary programming keys can be made in advance in System Keys to prepare for disaster recovery. The PPK is essential to recover from database corruption or total loss.
- Failsafe keys–Failsafe Keys are backups of individual unit keys that are made in advance and maintained in complete sets to be issued in the event of a system or power failure. See System Settings > Failsafe Keys.
- Staff/System keys–Always specify a key holder when making staff and system keys. Although it is not required, identifying the key holder is useful for tracking and accountability. See Staff Keys and System Keys.
- Invalidate access when appropriate:
  - Use the Block and Deactivate functions in Staff/Vendor Management to restrict operator access when necessary. See Staff/Vendor Management.
  - Use the System Keys at locks to invalidate staff and resident access. See System Keys.
  - Use the Erase key function (from Read Key dialog) to invalidate keys. See the Community toolbar.
  - Use the Deactivate resident feature when appropriate. See Resident Management.
- Access tracking–Staff/vendor and resident access tracking reports can be generated from the Read Key dialog.
- Notifications–Configure notification groups, then assign subscriptions for staff members in Staff/Vendor Management. See Notifications and Staff/Vendor Management.
- Logging–Extensive logging is produced to facilitate troubleshooting.
- Firmware upgrades–Establish a schedule to upgrade devices with the latest supported firmware.
- Reports–Establish a schedule to run and review Community reports. See Reports.

3.4.3 Proprietary design decisions

A security-focused approach to site configuration involves detailed planning.

- Property Builder–Thoughtfully plan, create and maintain access points. Establish standards for creating restricted area and foyer door access point types, and when selecting the limited access option for resident and staff common areas. See Property Builder.
- Access Management–Thoughtfully plan, create and maintain access management controls utilizing schedules, credentials, and common area access. See Access Management.

- Credentials–Carefully configure all credentials.
- Emergency Keys–When necessary, obtain a license for Emergency Keys. Only Emergency keys *always* override a projected dead bolt or active privacy switch.

3.5 User security

System access controls include the following options and best practices:

- Password, login, and account settings–Customize global settings to prevent unauthorized operator access. See System Settings > Security.
- Role Management–Operator roles determine the level of access to Community features and functions. Thoughtfully plan and assign operator roles. When necessary, create custom roles. See Role Management.
- Staff/Vendor Management–Staff/vendor profiles are designed to store details about all staff/vendors. Specify all available details on the Staff/Vendor Info tab. For operators, create API login credentials on the Operator Info tab. The credentials are validated when M-Unit and API authentication are enabled. See Staff/Vendor Management.
- Default Admin account–After installation, log in to the default Admin01 account to change the default password. Create strong passwords using at least eight characters that include uppercase and lowercase letters, numbers, and special characters.

4 Requirements

This section lists minimum system, network, device and interface requirements for installing and using Community. Additional resources may be required based on site configuration and usage.

4.1 System Requirements

Minimum requirements for the Community server are based on the number of access points. Additional notes are listed at the end of the table. [1]

A dedicated server is recommended but not required.

	Server		Workstation
	Small ≤ 500 access points	Medium 500-2k access points	not applicable
CPU [2]	2GHz/Intel x64-bit/4 core	2GHz/Intel x64-bit/8 core	2GHz/Intel x64-bit/dual core
RAM	16 GB or more	16 GB or more	8GB
Disk Drive Free Space [3]	30GB	60GB	50MB
Network Controller	Gigabit Ethernet - 1Gb/second	Gigabit Ethernet - 1Gb/second	Gigabit Ethernet - 1Gb/second
USB 2.0 Port	Required to connect encoder	Required to connect encoder	Required to connect encoder
Operating System [4]	▪ Microsoft Windows Server 2025/2022/2019 Standard ▪ Microsoft Windows 10 Pro/Enterprise [5] ▪ Microsoft Windows 11 Pro/Enterprise [5, 6]	▪ Microsoft Windows Server 2025/2022/2019 Standard	▪ Microsoft Windows 10 Pro/Enterprise ▪ Microsoft Windows 11 Pro/Enterprise [4]
.NET Framework	8.0.x	8.0.x	not applicable
Database [7]	▪ SQL Server Express 2022/2019/2017 ▪ SQL Server 2022/2019/2016	▪ SQL Server Express 2022/2019/2017 ▪ SQL Server 2022/2019/2016	not applicable
Web Browser [8]	▪ Google Chrome (latest) ▪ Microsoft Edge (latest)	▪ Google Chrome (latest) ▪ Microsoft Edge (latest)	▪ Google Chrome (latest) ▪ Microsoft Edge (latest)

[1] Additional recommended hardware for the server includes: UPS Backup, Integrated HD Graphics Card, Keyboard/Mouse.

[2] Supported CPUs: Intel and AMD x64.

[3] Additional free space may be required depending on database backup and archiving settings.

[4] Community is localized for all supported operating systems. Languages: English, French. Note that browser language settings may affect on-screen text.

[5] Windows 10 Pro/Enterprise and Windows 11 Pro/Enterprise do not support Online Communication due to MIcrosoft limitations on the number of concurrent network connections.

[6] TPM (Trusted Platform Module) 2.0 is required to run Windows 11.

[7] a) SQL Server Express 2022 is bundled with Community and can be selected to install during installation. b) IMPORTANT: For security reasons, dormakaba strongly recommends SQL Server 2022 (or SQL Server Express 2022). c) IMPORTANT: Due to SQL Server Express limitations, dormakaba recommends SQL Server Standard for medium and large deployments. For details, consult Microsoft documentation. d) For large deployments, dormakaba recommends using a dedicated server for the Community database. e) Microsoft reports issues that prevent SQL Server from installing successfully on a Domain Controller. Avoid installing SQL Server on a Domain Controller.

[8] Recommended Web browser resolution: 1366 x 768 or greater.

4.2 Network Requirements

The Property IT is responsible for establishing and maintaining a secure network (Ethernet or WiFi) environment on which the Community server, workstations, and integrated interfaces are deployed and used.

4.2.1 Deployment on Virtual Machine

If deploying Community on a cloud VM (virtual machine), a VPN (virtual private network) is required to secure the communication between the site and cloud VM.

4.2.2 Communication Ports

The following table lists the default Community Server port settings. If you have a firewall, configuration changes may be required to make ports accessible to the Community Server. Inbound ports require a firewall rule to allow communication with the server.

Inbound Port	Outbound Port	Protocol	Description
80/443		HTTP/S	Community Web User Interface, PMS – LGS SOAP API (80 for HTTP/443 for HTTPS)
8083/443		HTTP/S	Community API
28000/28001		TCP	dormakaba RFID Encoder I (28000)/dormakaba RFID Encoder II (28001, required for Enhanced Security Mode)
27700	27701	TCP	ONLINE – Gateway I, Control 4 (27701 is the listening port on the hardware)
28002		TCP	ONLINE – Gateway II, RAC5-MFC/XT
	23211	TCP	ONLINE – INNCOM (23211 is the listening port on the INNCOM server)
40100		HTTP/S	Community Client and Maintenance Unit. No firewall rule required. This port is not exposed to external computer; it is localhost only.

4.3 Device Requirements

This section lists the embedded devices required to use Community and the **latest** firmware versions.

Community devices are backward compatible with all previous firmware versions.

4.3.1 RFID keys

The following table shows the RFID key types that Community supports.

Key type	Enhanced Key Security	Standard Key Security	Legacy Key Security
MIFARE DESFire EV2/EV3	✓	✓	Not Supported
dormakaba RFID ComID Cards / Fobs (treated as MIFARE DESFire, not listed in user interface)	✓	✓	Not Supported
MIFARE Plus	✓	Not Supported	✓
MIFARE Ultralight C	✓	✓	Not Supported

4.3.2 Encoders

The following table lists the encoders that Community supports and the **latest** firmware version.

Encoder type	Latest FW	Supported key types
dormakaba RFID ENCODER I (part 064-514822 or 74750) (not supported when enhanced security mode enabled)	1.015	MIFARE Plus MIFARE Ultralight C
dormakaba RFID ENCODER II (part 75720) (required when Enhanced Security Mode enabled)	3.002 Applet version: 1.003	MIFARE DESFire EV2/EV3 MIFARE Plus MIFARE Ultralight C

Encoders that shipped before September 2022 may not have the applet version required for enhanced key security. For more information, contact dormakaba Support.

4.3.3 Maintenance Units

The following table lists the M-Units that Community supports and the **latest** firmware versions.

Programmer type	Latest supported FW	Minimum FW for enhanced security
M-Unit SAFLOK HH6	1.53	Not Supported
M-Unit SAFLOK HH6 NFC (required when Enhanced Security Mode enabled)	2.46	2.40

4.3.4 Locks

The following table lists supported locks and the **latest** firmware versions. The BLE version for all locks is 1.3.1.0.

Toggle mode is not currently supported when enhanced security mode is enabled. Toggle mode is supported for standard and legacy security. The latest firmware versions are required when programming units and suite units in multihousing toggle mode.

Lock profile	Boot & Main	Supported readers	Supported key types	Zigbee AVR
Use with Enhanced, Standard and Legacy security				
Confidant NFC	04.29.24.4	Integrated reader	MIFARE DESFire EV2/EV3 MIFARE Plus MIFARE Ultralight C	1.10x/5.13x / 6.05x
MT4 (secure boot)	06.28.24.4	▪ Quantum (secure boot): 06.18.24.5	MIFARE Plus MIFARE Ultralight C	1.10x/5.13x/6.05x
Quantum MT6 (secure boot)	10.03.24.4	LEGIC	MIFARE DESFire EV2/EV3 MIFARE Plus MIFARE Ultralight C	1.10x/5.13x/6.05x
Nova	04.29.24.4	Integrated reader	MIFARE DESFire EV2/EV3 MIFARE Plus MIFARE Ultralight C	5.13x / 6.050
Pixel	06.28.24.4	▪ Quantum (secure boot): 06.18.24.5	MIFARE Plus MIFARE Ultralight C	1.10x/5.13x/6.05x
Quantum (secure boot)	06.28.24.4	▪ Quantum (secure boot): 06.18.24.5	MIFARE Plus MIFARE Ultralight C	1.10x/5.13x/6.05x
RAC5 XT/Lite (hardware for common areas)	08.22.23.4 (Main only)	▪ SRK (NFC Wall) Reader: V_07.04.24.3	MIFARE DESFire EV2/EV3 MIFARE Plus MIFARE Ultralight C	N/A
RCU4	06.28.24.4	▪ Quantum (secure boot): 06.18.24.5	MIFARE Plus MIFARE Ultralight C	1.10x/5.13x/6.05x
RT+	04.29.24.4	Integrated reader	MIFARE DESFire EV2/EV3 MIFARE Plus MIFARE Ultralight C	1.10x/5.13x / 6.05x
Saffire LX	04.29.24.4	Integrated reader	MIFARE DESFire EV2/EV3 MIFARE Plus MIFARE Ultralight C	5.13x / 6.05x

Lock profile	Boot & Main	Supported readers	Supported key types	Zigbee AVR
Saffire LXD	04.29.24.4	Integrated reader	MIFARE DESFire EV2/EV3 MIFARE Plus MIFARE Ultralight C	5.13x / 6.05x
Use with Standard and Legacy security				
Confidant	09.03.19.2	Integrated reader	MIFARE Plus MIFARE Ultralight C	1.10x/5.13x
MT4	08.03.21.4	▪ Quantum (secure boot): 02.06.19.1	MIFARE Plus MIFARE Ultralight C	1.10x/5.13x/6.05x
Quantum	08.03.21.4	▪ Quantum (secure boot): 02.06.19.1	MIFARE Plus MIFARE Ultralight C	1.10x/5.13x/6.05x
RT	06.14.18.2	Integrated reader	MIFARE Plus MIFARE Ultralight C	1.10x/5.13x/6.05x

All lock profiles support all previous firmware versions except RT; the RT lock supports firmware versions since 2015.

The RT and legacy Confidant lock models do not support the extended common areas feature.

4.3.5 Elevator Controllers

The following table lists supported elevator controllers and the **latest** firmware versions. The BLE version for all elevator controllers is 1.3.1.0.

	Boot & Main	Supported readers	Supported key types	Zigbee AVR
Enhanced, Standard and Legacy security				
ECU/RCU4	06.28.24.4	Quantum (secure boot): 06.18.24.5	MIFARE Plus MIFARE Ultralight C	1.10x
RAC5-MFC	08.22.23.4	▪ Integrated reader ▪ SRK (NFC Wall) Reader: V_07.04.24.3	MIFARE DESFire EV2/EV3 MIFARE Plus MIFARE Ultralight C	N/A
Standard and Legacy security				
ECU/RCU4	08.03.21.4	Quantum (secure boot): 02.06.19.1	MIFARE Plus MIFARE Ultralight C	1.10x
Legacy MFC	0.017 (Main only)	Integrated reader	MIFARE Plus MIFARE Ultralight C	N/A
EMCC	20090929 (Main only)	Integrated reader	MIFARE Plus MIFARE Ultralight C	N/A
MCC 8/12	0.031398 (Main only)	Integrated reader	MIFARE Plus MIFARE Ultralight C	N/A

4.3.6 Zigbee Gateways

The following table shows the Zigbee gateways that Community supports and the **latest** firmware versions.

	Boot	BLE	Zigbee
Gateway I	0.221	N/A	1.10x/5.13x

	Boot	BLE	Zigbee
Gateway II	0.022	N/A	6.05x

4.4 Interface Requirements

Community supports the following:

- Aurora SDK—v1.0.19 to v1.0.25
- Aurora software—v1.0.19 to v1.0.25

(Aurora integrations only) In Aurora, the following requirements apply when Community license includes Visitor Management:

- Enable Extended PIN (7-digit), (Application)
- Enable Auto Generate PIN
- Enable Keyscan Credentials for Extended Card Format
- Enable KABA Integrated Mode
- Enable Auto Expiry mode
- Enable Card Count on ACUs
- Per ACU, select reader mode S - KABA Integration

For details, refer to the *Community Aurora Integration Deployment and Support Manual* (PK3769).

4.5 Online Communication Interfaces and Devices

The following table shows the Online Gateway combinations that Community supports. For example, the Gateway I device is compatible with other Gateway I devices, RAC5 and MFC elevator controllers, and one third-party interface.

	Gateway I Device supported with	Gateway II Device supported with	Rx-Link supported with	RAC5-MFC/XT supported with
Gateway I Device	✓	Not Supported	Not Supported	✓
Gateway II Device	Not Supported	✓	✓	✓
Rx-Link	Not Supported	✓	✓	✓
RAC5-MFC	✓	✓	✓	✓
RAC5 XT	✓	✓	✓	✓
Legacy MFC	✓	Not Supported	Not Supported	Not Supported
Third-Party Interfaces (mutually exclusive)				
INNCOM®	✓	✓	✓	✓
INTEREL®	✓	Not Supported	Not Supported	Not Supported
Telkonet®	✓	Not Supported	Not Supported	Not Supported
Control4®	✓	Not Supported	Not Supported	Not Supported

4.6 Online Communication Lock Support

The following table shows the locks supported with remote lock management (online communication).

	Gateway I / Legacy 3rd-Party Interfaces (Zigbee Gen I)	Gateway II / Rx-Link	
		Zigbee Gen II Phase 1	Zigbee Gen II Phase 2
Pixel	✓	✓	✓
MT4	✓	✓	✓
MT6	✓	✓	✓
RCU4	✓	✓	✓
RT	✓	✓	Not Supported
RT+	✓	✓	✓
Saffire LX	✓	✓	✓
Nova	✓	✓	✓
Confidant	✓	✓	Not Supported
Confidant NFC	✓	✓	✓

4.7 No Touring Requirements

The No Touring feature cancels access to common areas when a resident key is canceled prior to the expiration date. To use the feature, the following requirements must be met:

- MT/RCU Series locks must be installed at Resident Common Areas.
- The locks must be updated to the latest firmware.
- The M-Unit (HH6) must be updated to the latest firmware.

For information about the M-Unit, refer to the *Saflok HH6 User Reference Guide*.

5 Pre-installation checklist

The following items apply to initial installations only.

5.1 Requirements

1	☐	Server/Client. Verify that all system requirements are met.
2	☐	Server. Verify that the Date/Time and Time Zone settings are correct. (The Community Server and the locks installed at access points must be configured for the same time zone.)
3	☐	**IMPORTANT!** Server/Client. Verify that all Windows updates are installed.
4	☐	Server. Verify that Windows PowerShell 4.0 is installed.
5	☐	Server. Verify that the following programs are **NOT** installed:
6	☐	SQL Server (only if not connecting to an existing SQL instance)
7	☐	Redis
8	☐	RabbitMQ
9	☐	Web Server IIS
10	☐	Server. Verify that you have an activation key for Community .
11	☐	Disable Windows USB power saving settings (to ensure encoders connected via USB function properly).
12	☐	Server/Client. Verify that the operating system is up and activated.
13	☐	Server/Client. Perform the installation as a **Local Administrator**.
14	☐	If applicable, prepare to connect to an existing SQL Server instance.
15	☐	Server. Make sure antivirus software is disabled before proceeding with server installation.
16	☐	Server. If the language used for the user interface is different from the server operating system language, it is required to install the Microsoft Windows language pack matching the user interface language for Community reports to display the appropriate information.

5.2 Recommendations

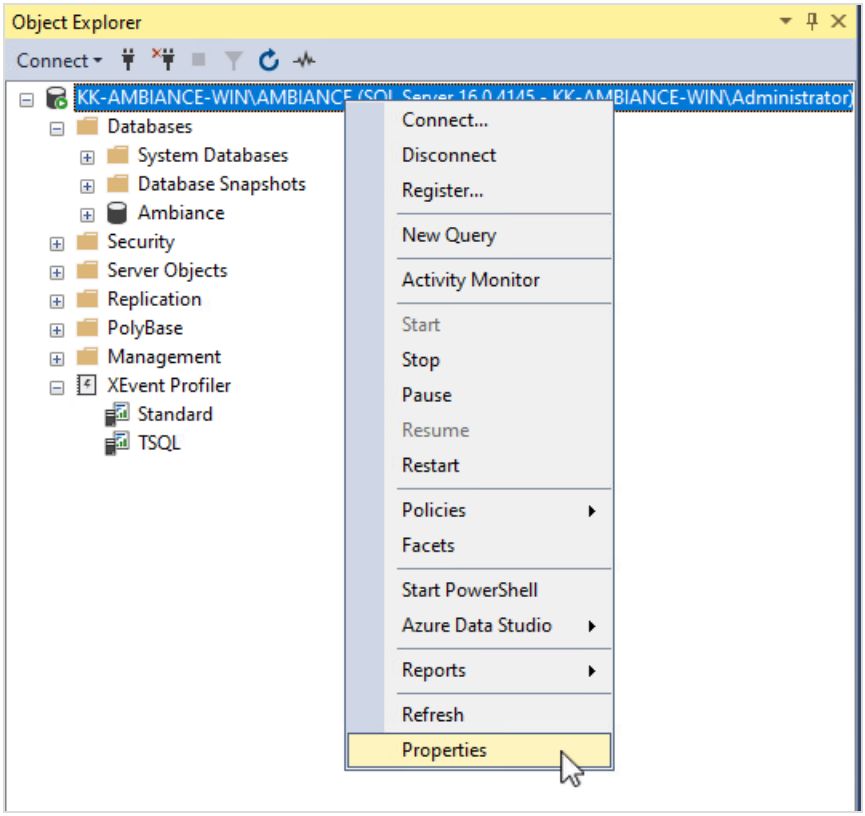
1	☐	**IMPORTANT!** Install the Community Server in a secure physical location.
2	☐	**IMPORTANT!** Ensure that the edition of SQL Server meets organizational requirements.
3	☐	Server. If deploying on a cloud VM, set up a VPN to secure the communication between the site and cloud VM.
4	☐	Server. Verify that the server where SQL Server is installed is not a Domain Controller.
5	☐	Server. If possible, disable Windows Defender for the duration of the installation.
6	☐	Server. Configure the Community Server with a static IP address.
7	☐	Make sure that you have your Windows OS Installer available.

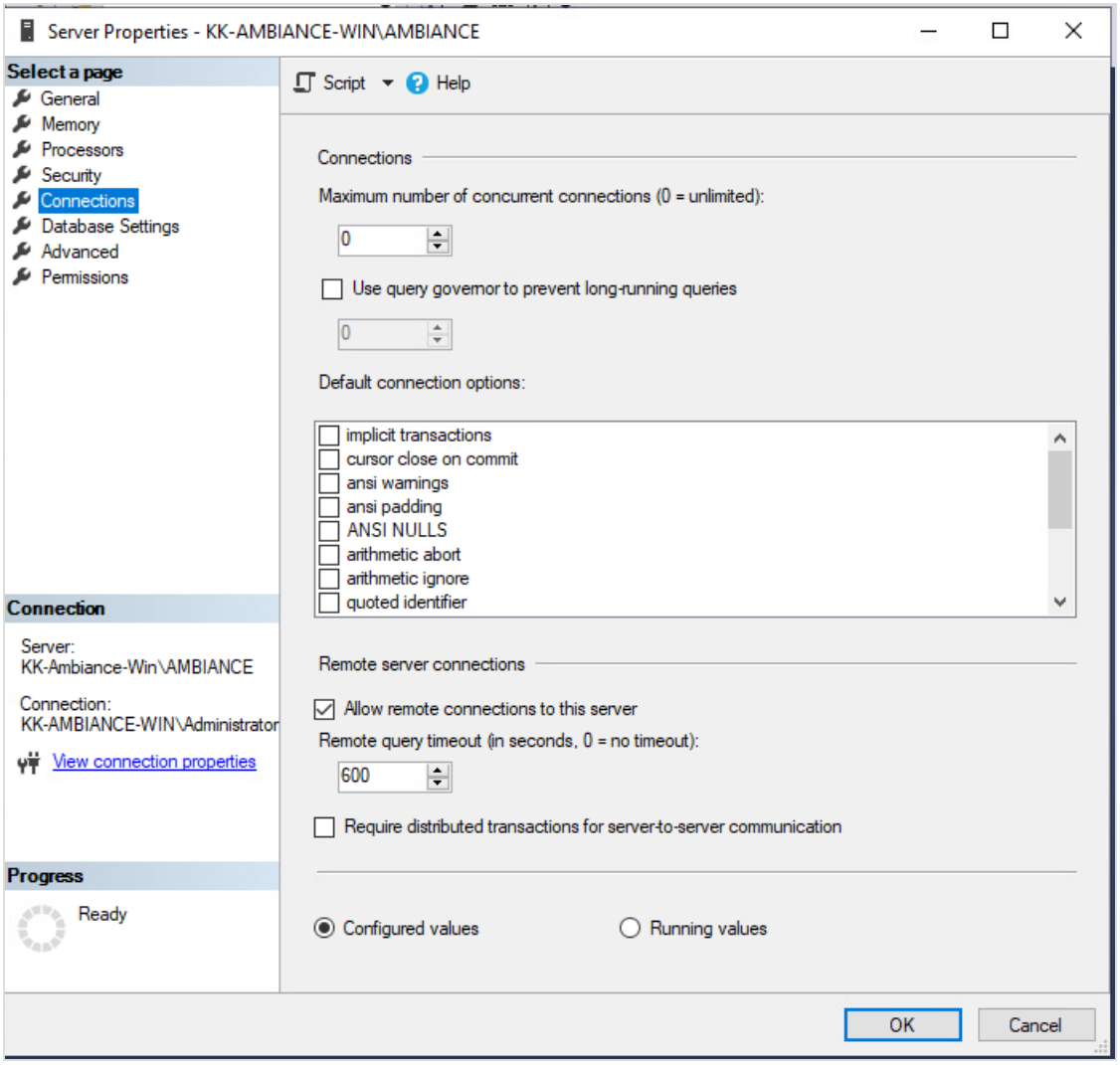
6 Prepare for using an existing SQL Server instance

If you plan to connect to an existing SQL Server database (local or remote), you must prepare before starting the installation.

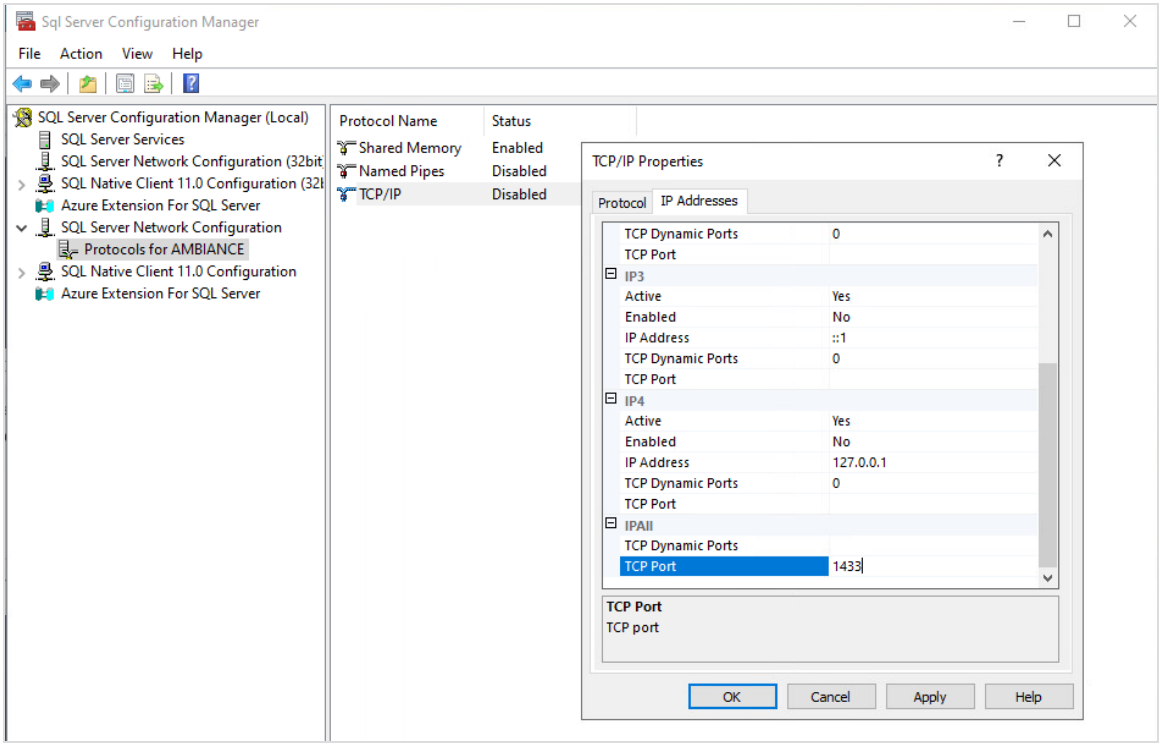
1. In the Community installation package, go to the COMMUNITY_PREREQUIS folder and copy the master database file (Community.mdf) to the remote computer where Microsoft SQL Server is installed. Recommended path: C:\Program Files\Microsoft SQL Server\MSSQL*version.instanceName*\MSSQL\DATA\.
2. Right-click the database file and select **Properties**. Deselect the Read-Only attribute, then click **Apply** > **OK**.
3. Attach the database:
   a. Open SQL Server Management Studio.
   b. Connect to an instance of the SQL Server Database Engine.
   c. In Object Explorer, expand the instance view.
   d. Right-click **Databases** and select **Attach**.
   e. In the Attach Databases dialog box, click **Add.**
   f. In the Locate Database Files dialog box, navigate to and select the .mdf file (previously pasted in step 1).
   g. Click **OK**.

4. Right–click the server and select **Properties**.





5. For **Connections**, select the **Allow remote connections to this server**, then click **OK.**
6. Open the SQL Server Configuration Manager.
7. Navigate to SQL Server Network Configuration > Protocols for instanceName (COMMUNITY).



8. Right-click **TCP/IP** and select **Properties**.
9. In the TCP/IP Properties dialog, select the **IP Addresses** tab and scroll to **IPAll**.
10. Set the **TCP Dynamic Ports** to blank and **TCP Port** to **1433**. (Port 1433 is the default instance that SQL Server uses.)
11. Click **Apply** > **OK**.

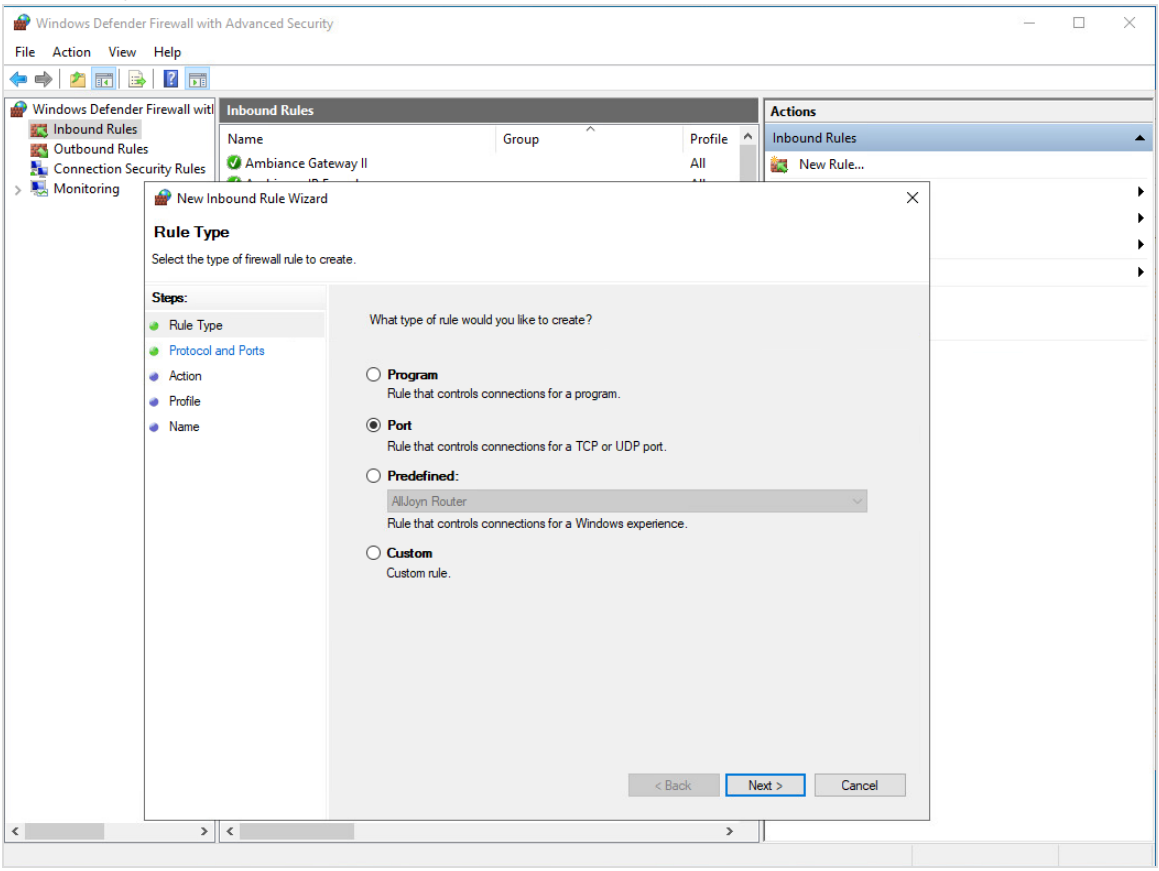
If using a firewall, continue to the next section to open access for the database engine.

6.1 Configure a Windows firewall for database engine access

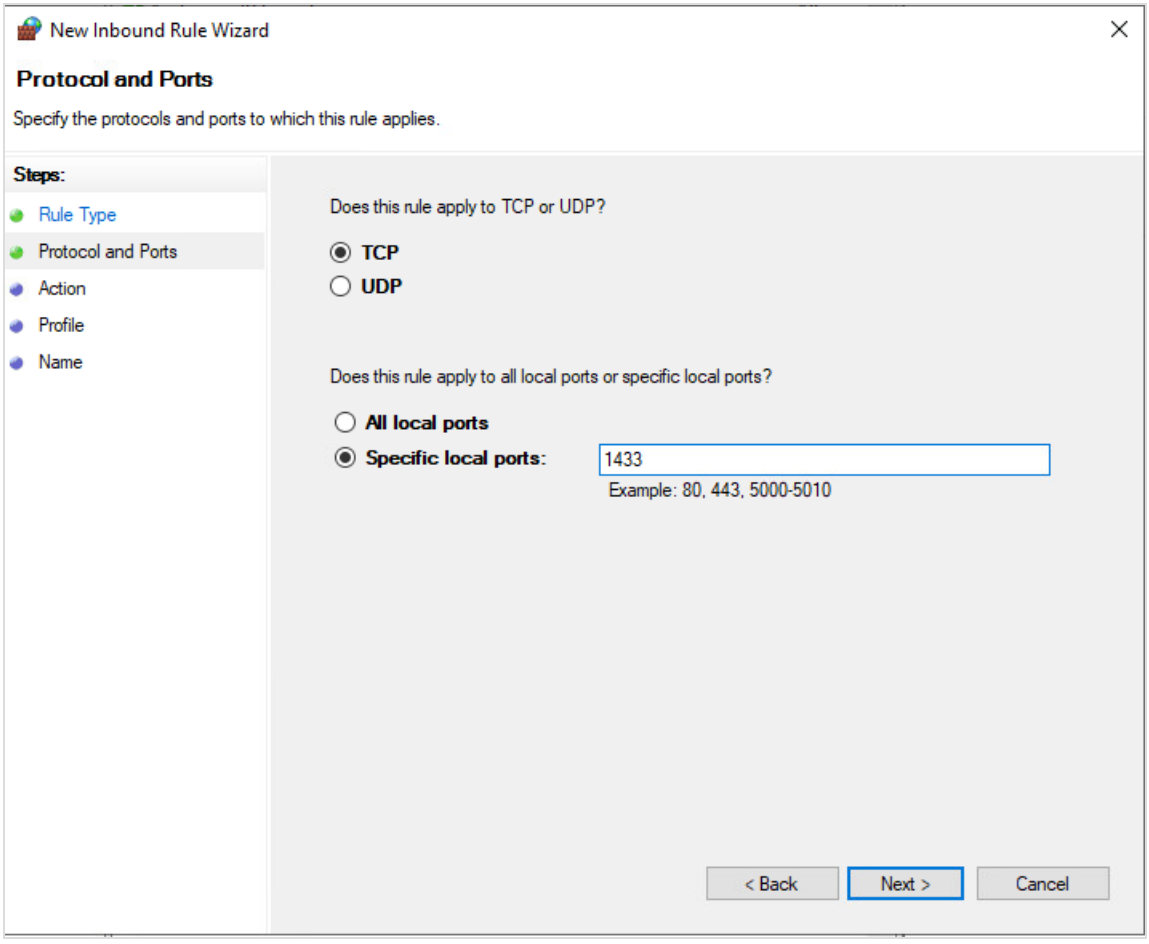
If the firewall is turned on, you need to add an exception for the 1433 port to allow TCP/IP traffic on Port 1433 and UDP traffic on Port 1434.

1. In the Windows Search bar, search for and open Administrative Tools.
2. Open Windows Defender Firewall with Advanced Securty.
3. Select **Inbound Rules**.

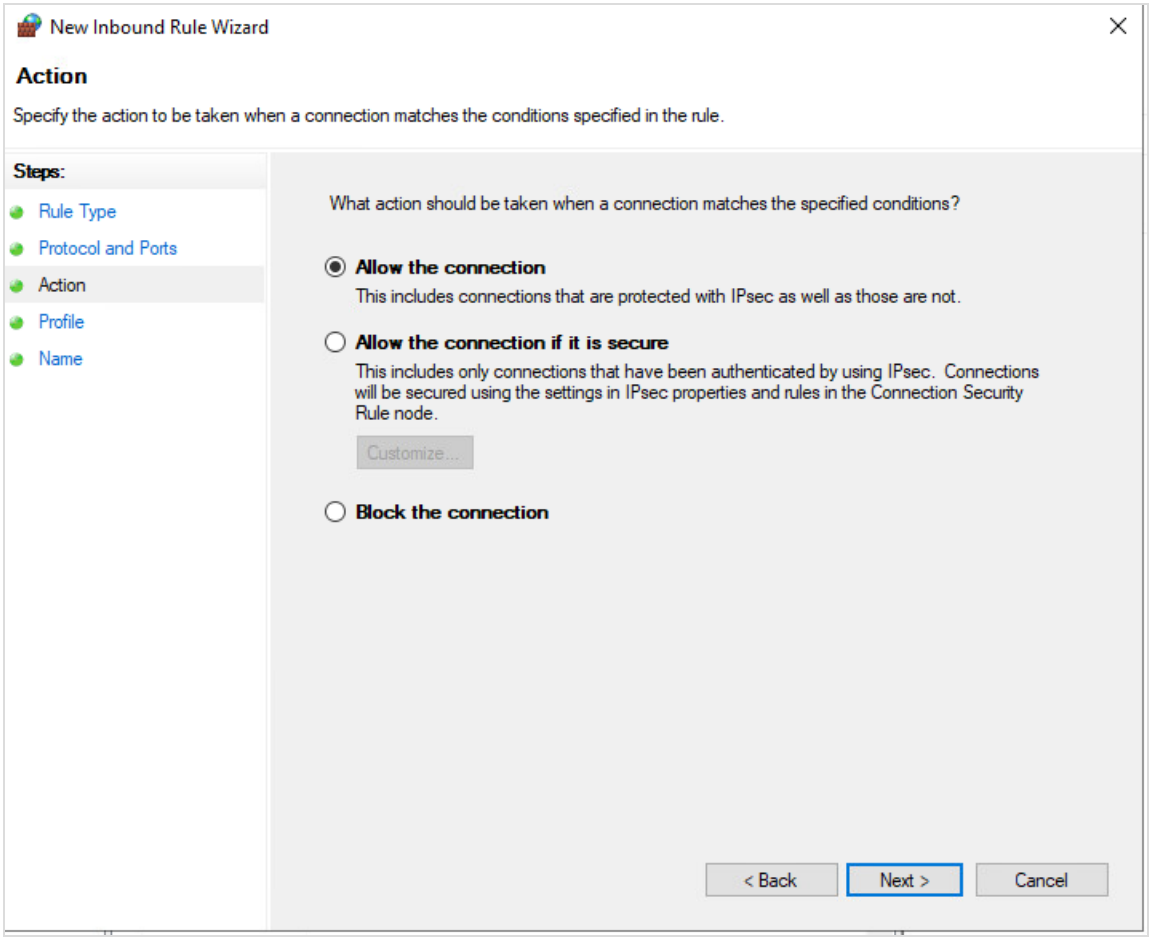
4. Under **Actions**, select **New Rule**.



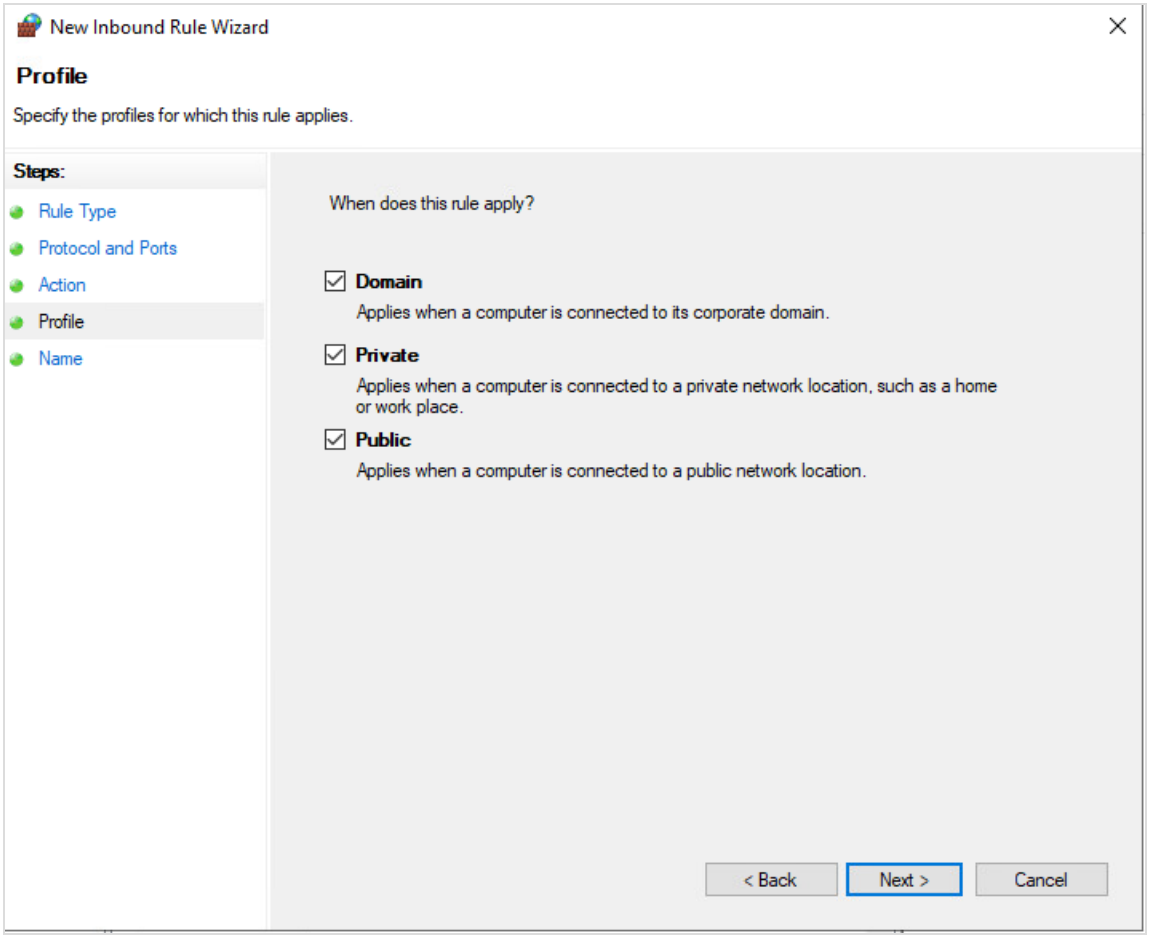
5. For Rule Type, select **Port**, then click **Next**.
6. For Protocols and Ports, select **TCP** and specify **1433** for **Specific local ports**, then click **Next**.



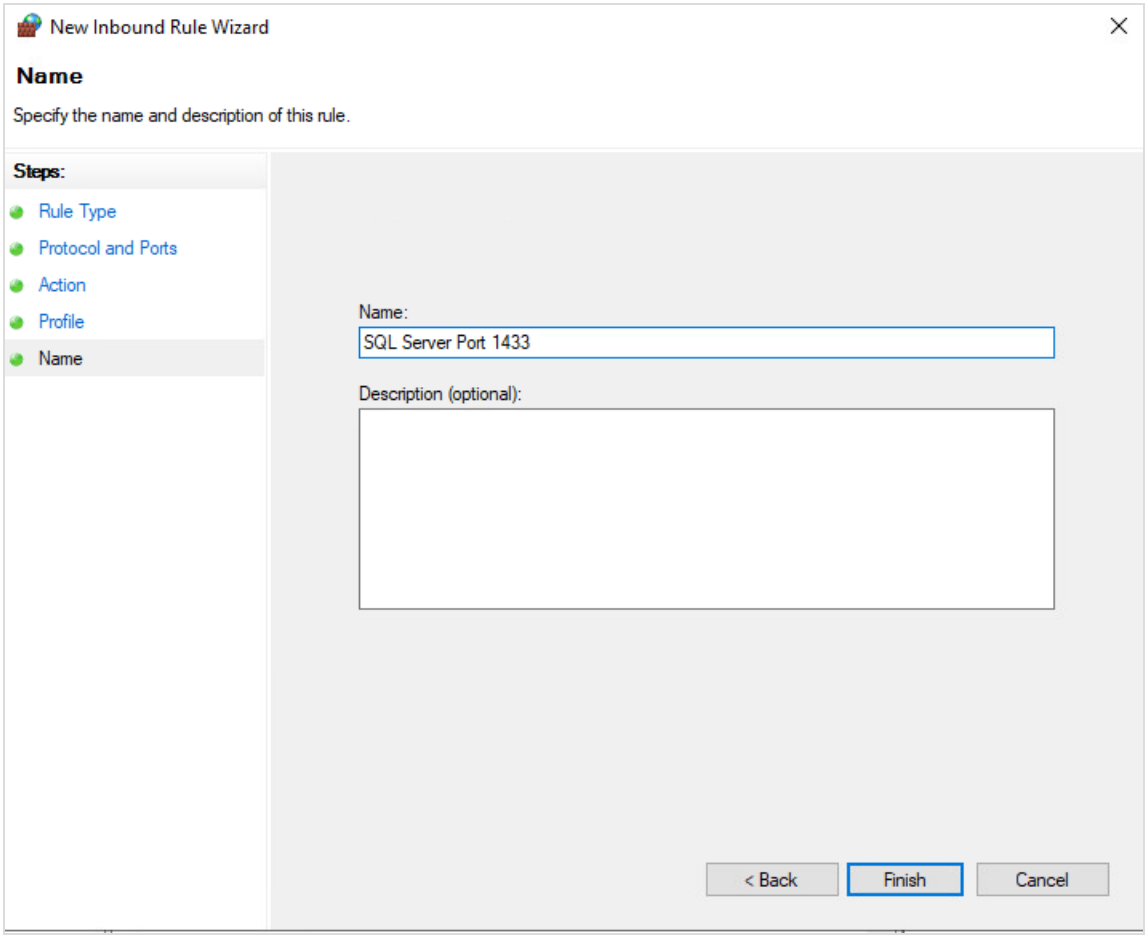
7. For Action, select **Allow the connection** (to specify the action to be taken when a connection matches the conditions specified in the rule).



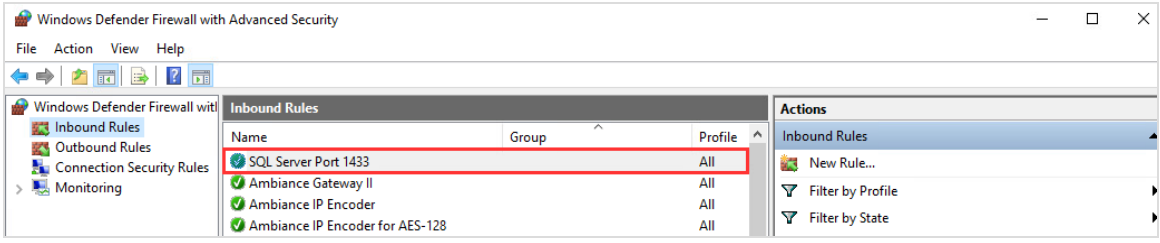
8. For Profiles, select the profiles to which the rule applies, then click **Next**.



9. For Name, specify the name of the new rule, then click **Finish**.



You can now see the created rule in the list of inbound rules.



10. Repeat the same steps to add UDP port 1434.

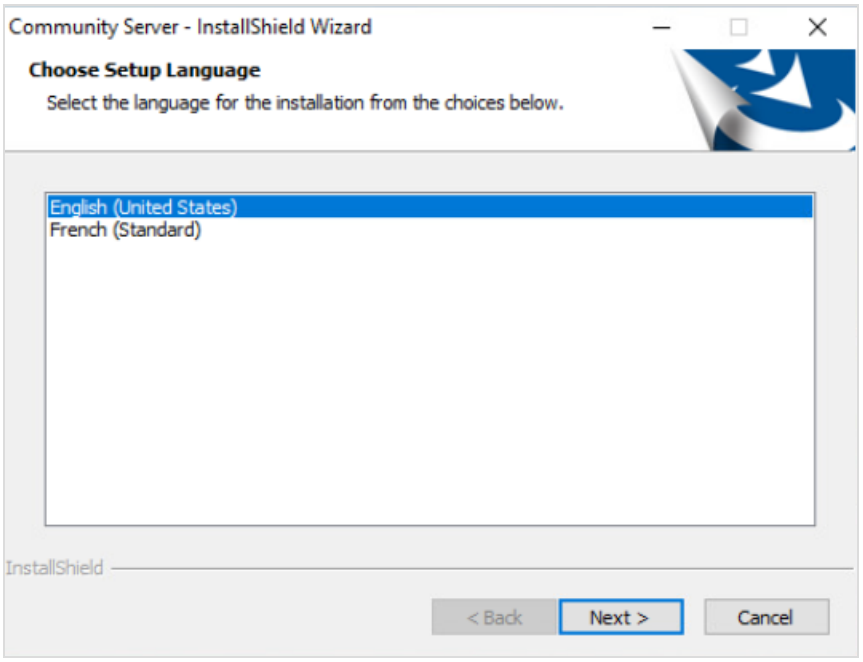
7 Community server installation

This chapter is for first-time installations. If the installation is an upgrade, refer to *Community Upgrades*.

To install the Community Server:

1. In the dormakaba/Community folder, open the SERVER folder.
2. Double-click **CommunityServer.exe**. The installation wizard opens and prepares for setup. Depending on the server, the following steps may occur during installation:
   - If Microsoft .NET 8.0 is not installed, the prompt to allow the program to make changes to the computer displays. Click **YES** to proceed with the installation.
   - If the Microsoft OLE Database Driver for SQL Server is not installed, click **Install** to proceed with the installation.
3. Follow the instructions for each of the following wizard pages. When a restart is required, confirm to proceed with the installation.

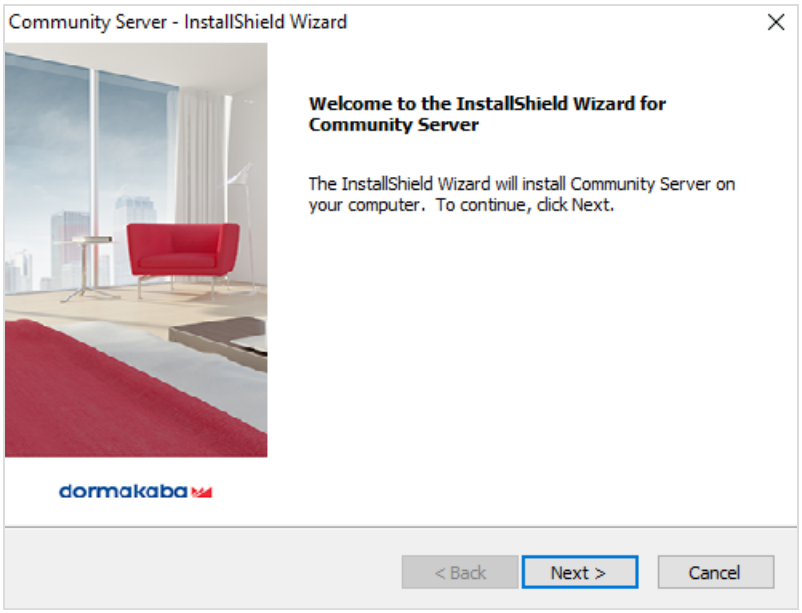
7.1 Choose Setup Language page



On the Choose Setup Language page:

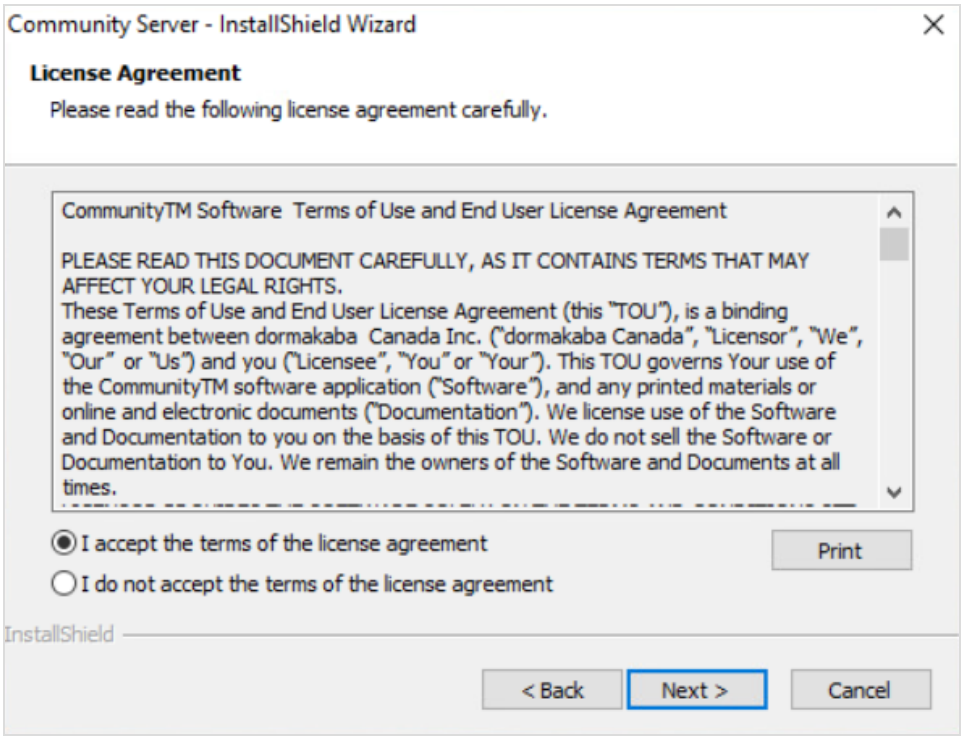
1. Select **English (United States)**.
2. Click **Next**.

7.2 Welcome page



On the Welcome page click **Next**.

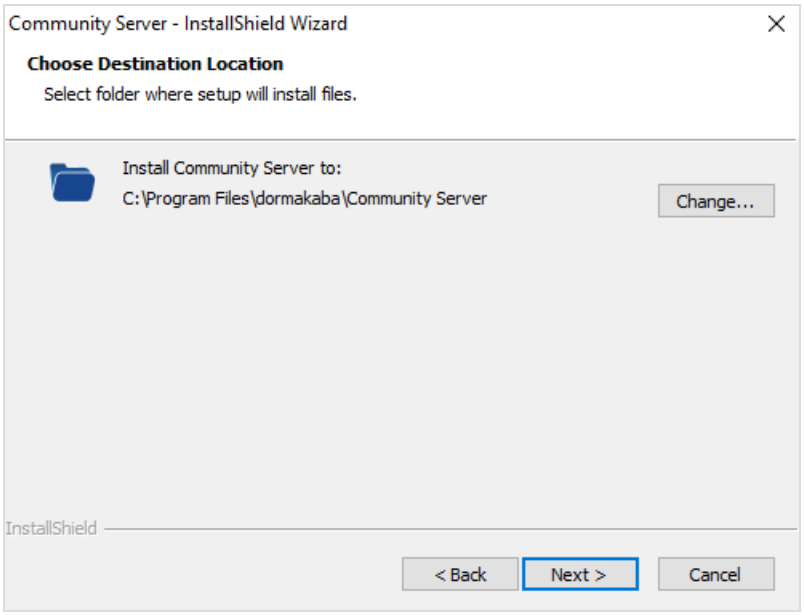
7.3 License Agreement page



On the License Agreement page:

1. Accept the terms of the license agreement.
   You can optionally print the agreement.
2. Click **Next**.

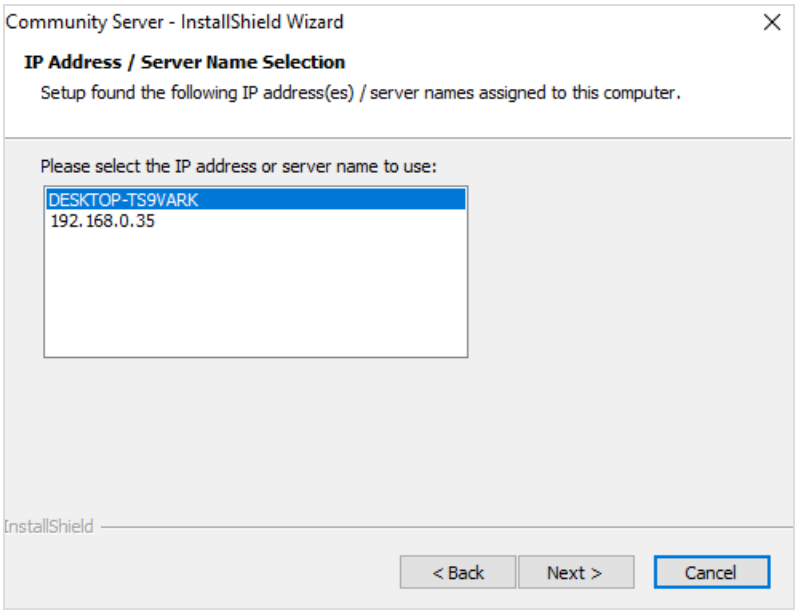
7.4 Choose Destination Location page



On the Choose Destination Location page:

1. Choose where to install Community Server files:
   - Accept the default location (recommended).
   - Click **Change** and navigate to a location on the server.
2. Click **Next**.

7.5 IP Address / Server Name Selection page

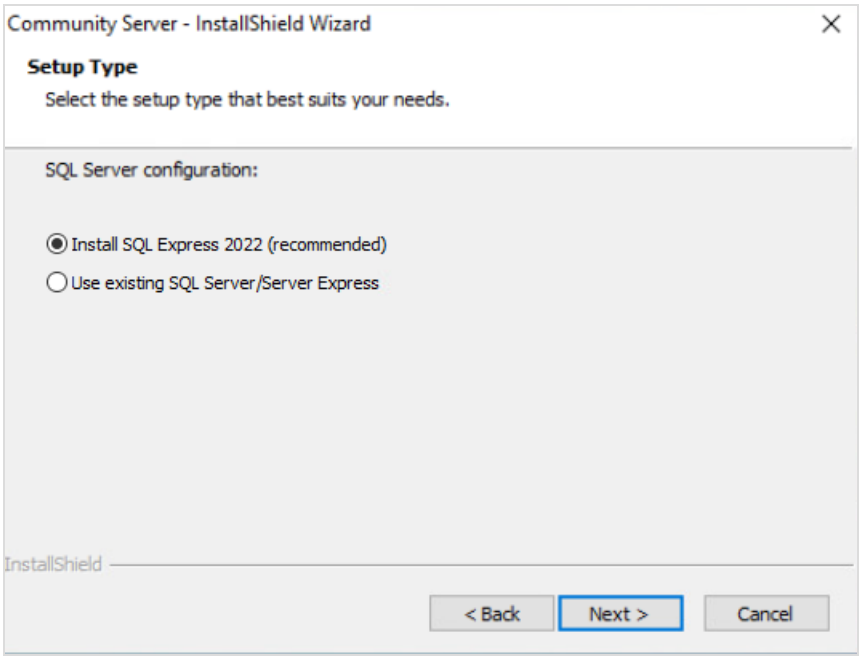


On the IP Address / Server Name Selection page:

1. Select the IP address or host name to use for the installation.
2. Click **Next**.

7.6 Setup Type page

This page only displays if the installer detects an existing instance of SQL Server.

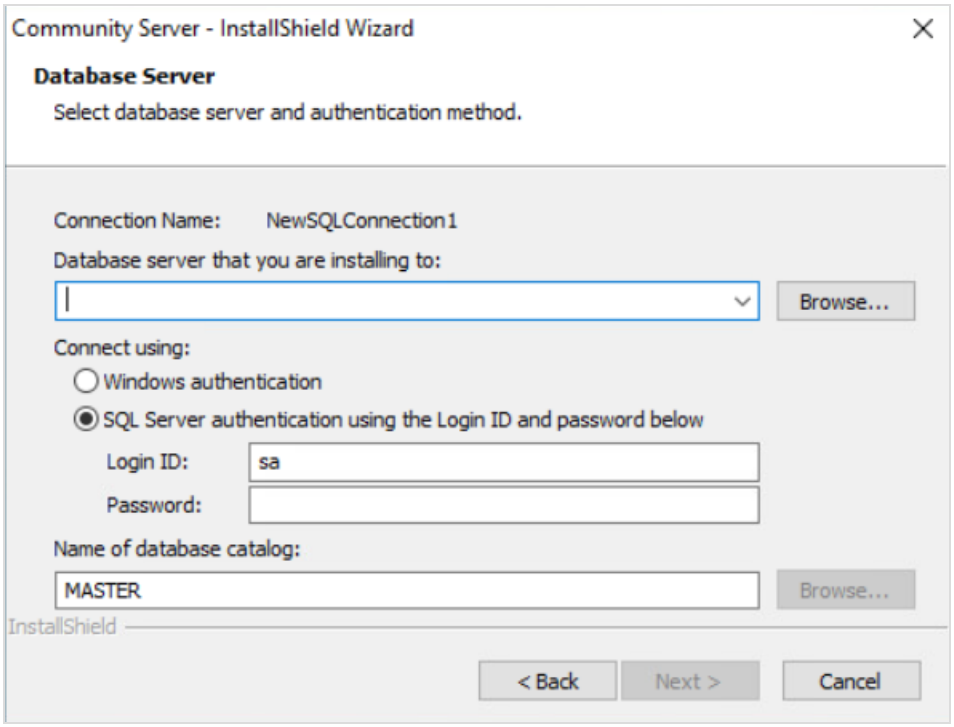


On the Setup Type page:

Select whether to install a new instance of SQL Server or connect to an existing local or remote SQL Server/Server Express database instance. If installing a new instance, SQL Server Express 2022 is installed. Any instance to which you connect must be a supported version (see *Requirements*).

- If installing a new instance, click **Next** and proceed to *Setup Status Page*.
- If connecting to an existing instance, click **Next** and proceed to *SQL Database Server Page*.

7.7 SQL Database Server page

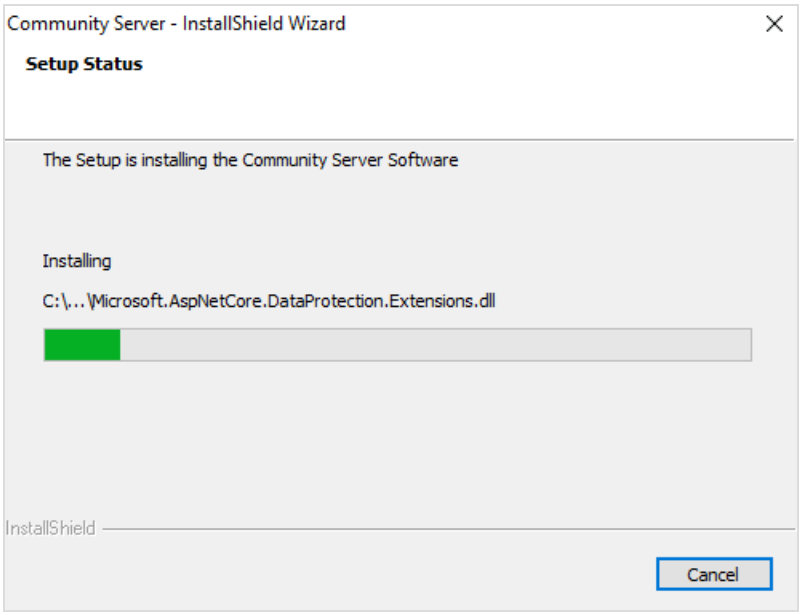


On the SQL Database Server page:

1. Click Browse, navigate to select the correct SQL instance.
2. Specify valid SQL Server credentials
3. Click **Next**.

If there is no database attached to the selected instance, a message informs to prepare for using an existing SQL Server instance. For instructions, see the previous chapter.

7.8 Setup Status page



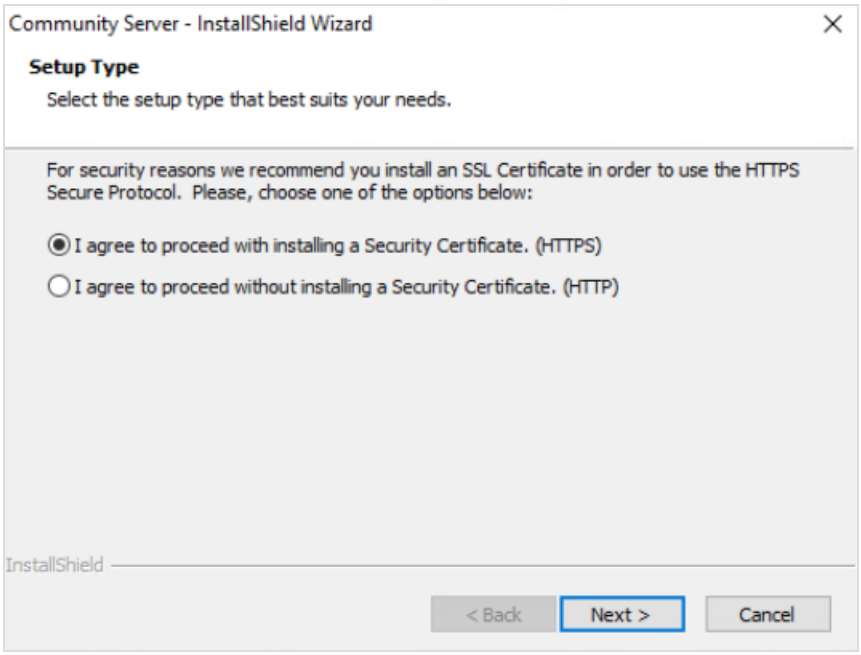
The Setup Status page displays the installation status. When prompted, click **Next**.

The following third-party applications are installed:

- Microsoft .NET 8.0.x
- Microsoft SQL Server Express 2022 (if selected) and hotfix KB5050771
- Redis Server 7.4.0
- Erlang Software 26.2.5
- RabbitMQ 3.13.6
- VC++ Redistributable 2013, 2015-2019
- MongoDB 7.0.x
- Angular 18.1

7.9 Setup Type page

Security is your responsibility. dormakaba strongly recommends installing an SSL certificate to enable the HTTPS protocol. The SSL certificate to enable HTTPS mode must be provided by a well-known and trusted certificate authority.



On the Setup Type page:

1. Select whether to install an SSL certificate.
2. Click **Next**. If you proceed without installing a certificate, a warning displays.

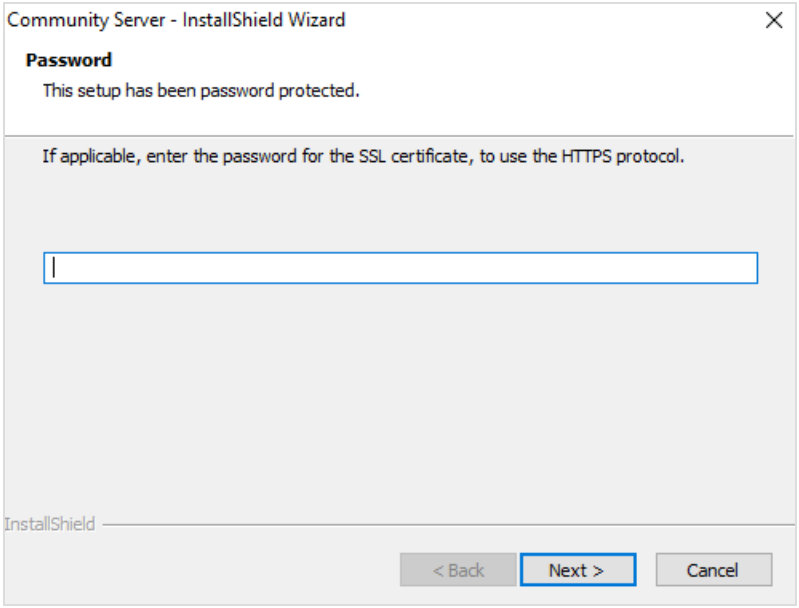
To install an SSL certificate after installation, use the Service Manager (on the server); use the Service Manager (on workstations) to change the server IP/name to https://.

7.9.1 Choose SSL certificate

In File Explorer:

1. Navigate to and select the SSL certificate to install.
2. Click **Open**.

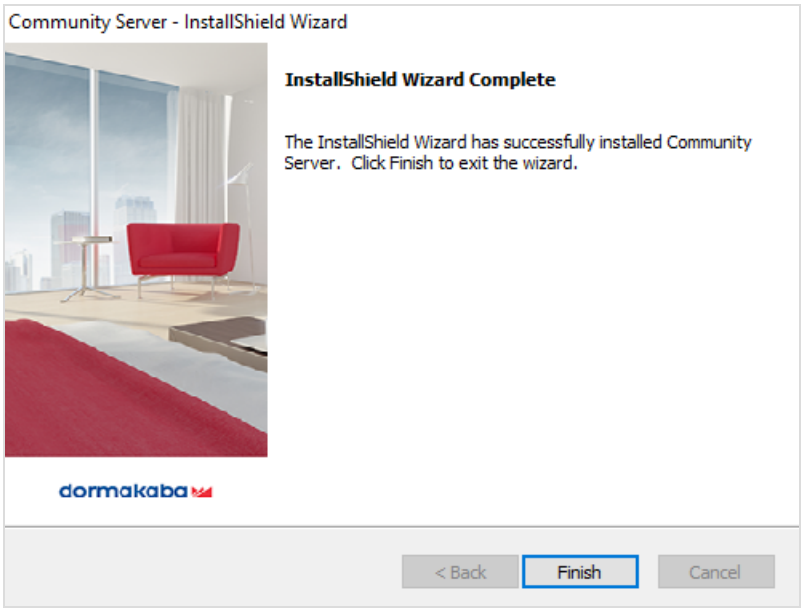
7.9.2 Password page



On the Password page:

1. Specify the password for the SSL certificate that you selected.
2. Click **Next**.

7.10 Installation Complete page



When notified the installation is complete, click **Finish**.

After the Community Server is installed, upgraded or restarted, wait two to three minutes before using Community.

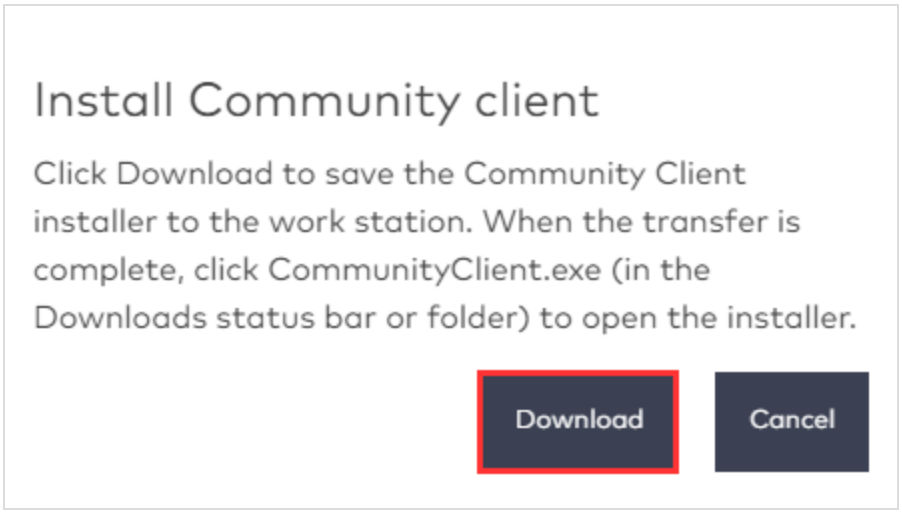
8 Community client installation

This chapter guides you through the Community Client installation. You must install the Client on every workstation where a USB encoder and / or Maintenance Unit is required.

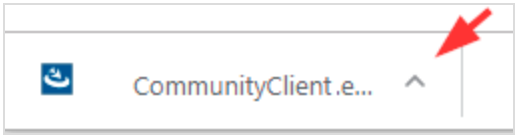
To install the Community Client:

1. In a supported browser, go to the IP address of the Community server.
2. Log in.
3. Go to Device Management.

4. In the toolbar, click to install the Community client.

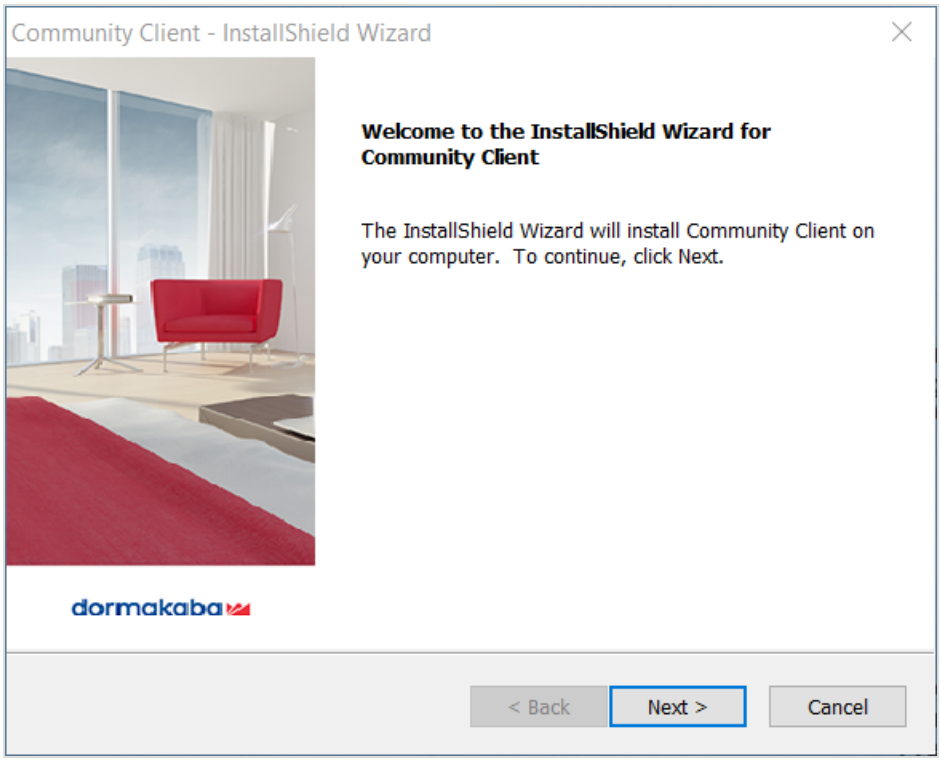


5. Click Download. A total of three files are required Community_Client.exe, serverURL.config, and token.txt.



6. Open **Community.exe**. The installation wizard opens and prepares for setup. Depending on the computer, the following step may occur during installation:
   - The wizard checks for Microsoft .NET 8.0, and installs it if not found.
7. Follow the instructions for each of the following wizard pages.

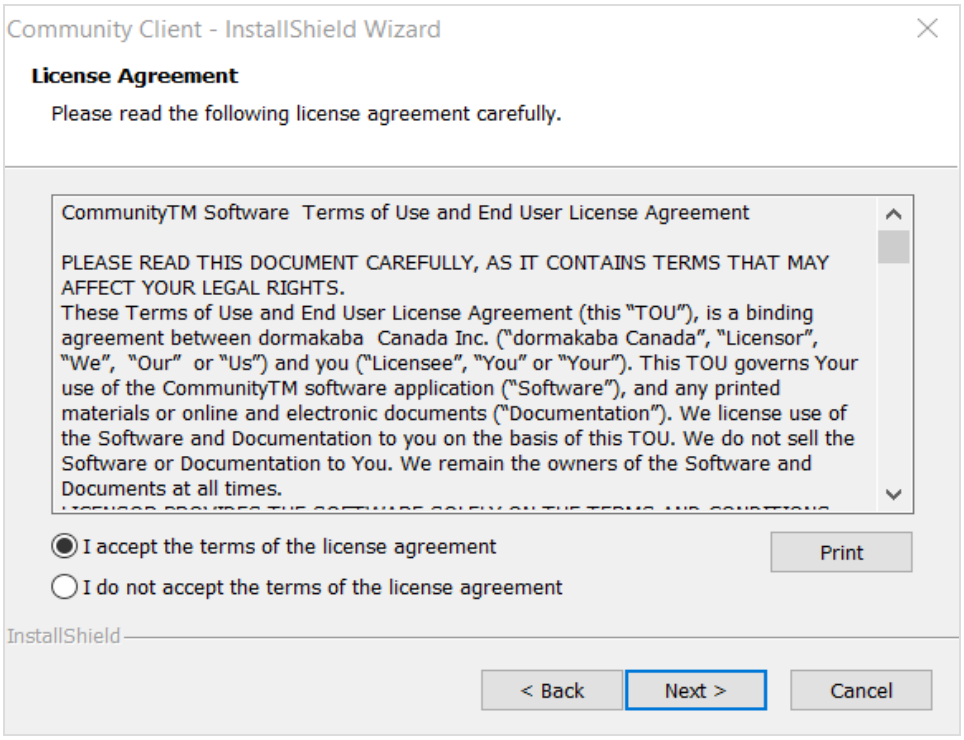
8.1 Welcome page



On the Welcome page:

- Click **Next**.

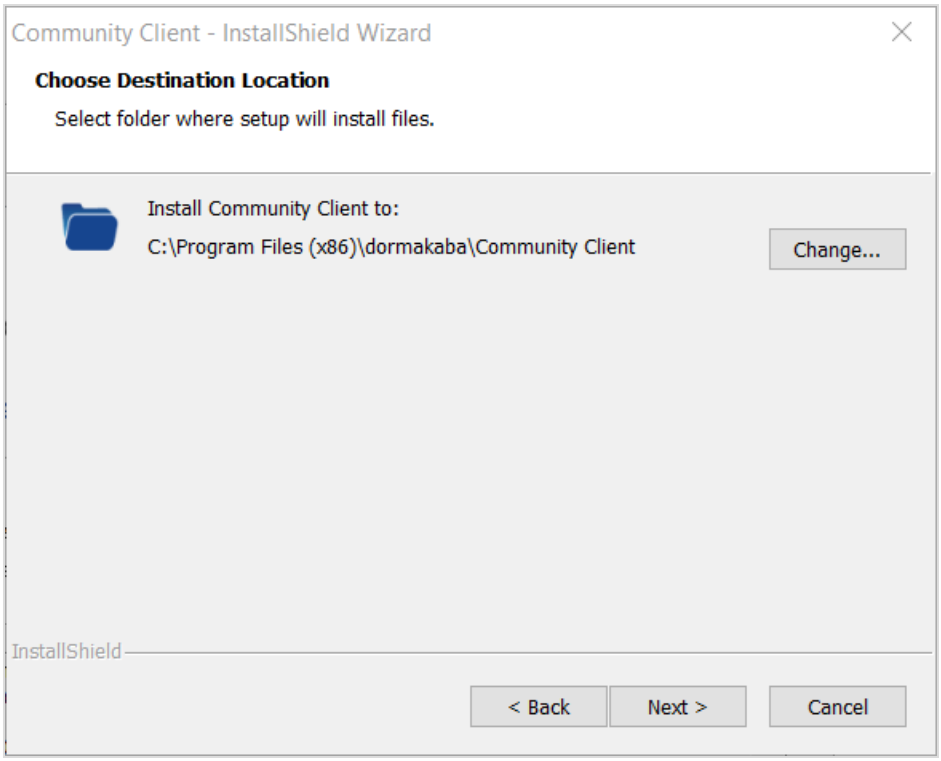
8.2 License Agreement page



On the License Agreement page:

1. Accept the terms of the license agreement.
   You can optionally print the agreement.
2. Click **Next**.

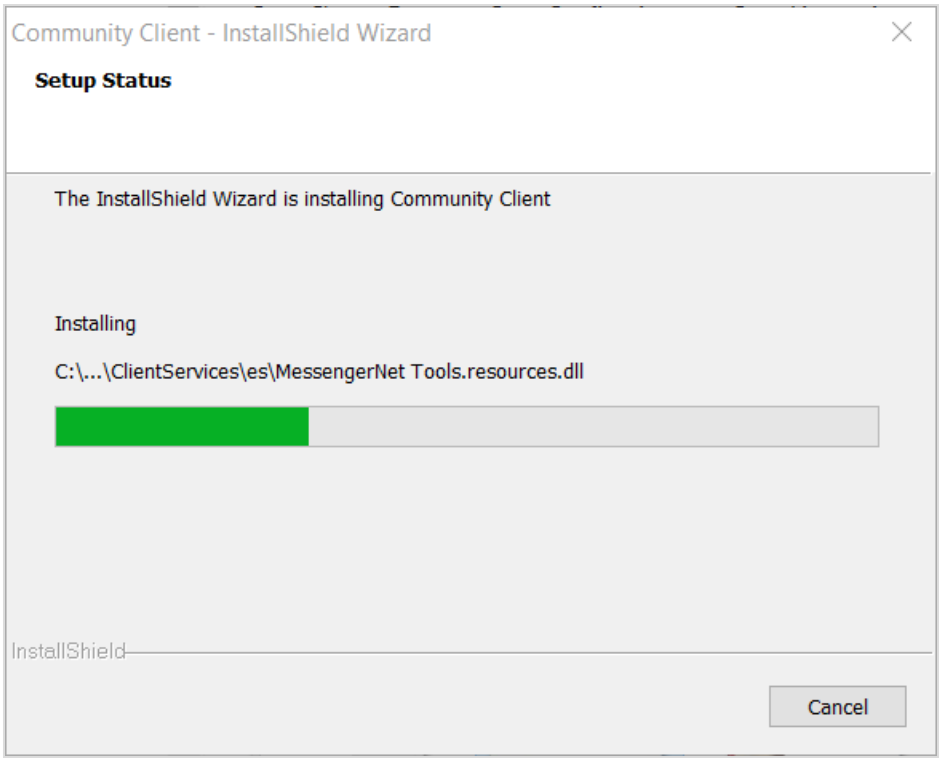
8.3 Choose Destination Location page



On the Choose Destination Location page:

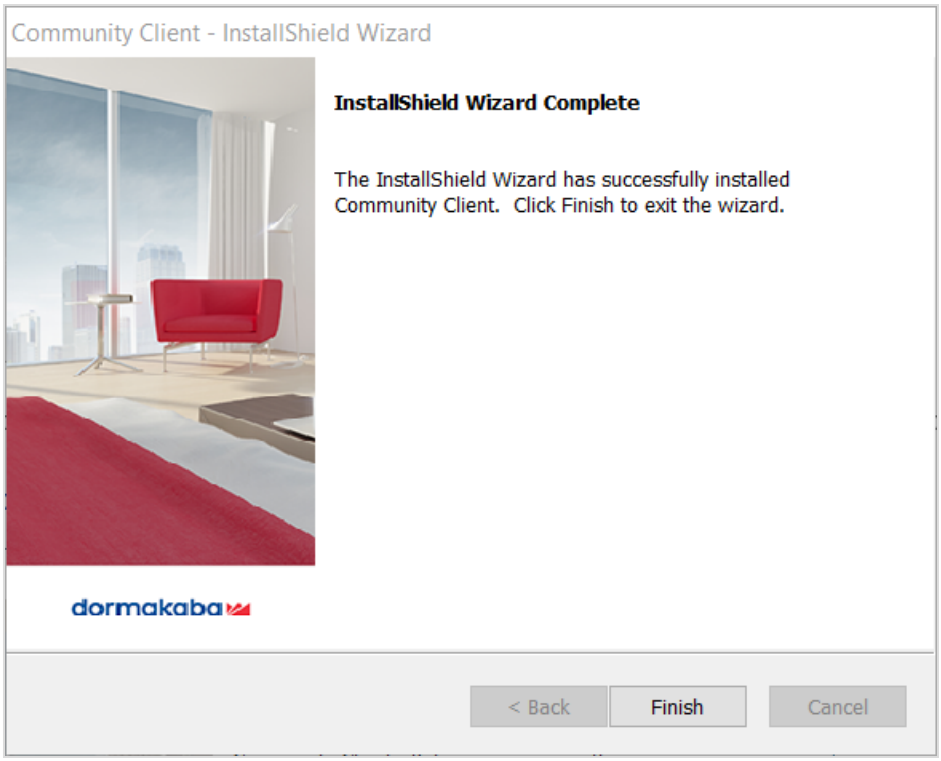
1. Choose where to install Community Client files:
   - Accept the default location (recommended).
   - Click **Change** and navigate to a location on the server.
2. Click **Next**.

8.4 Setup Status page



The Setup Status page displays the installation status. When prompted, click **Next**.

8.5 Installation Complete page



When notified the installation is successful, click Finish.

9 Post-installation checklist

The following items apply to initial installations only.

1	☐	Server. Re-enable antivirus software.
2	☐	Server. If necessary, re-enable Windows Defender.
3	☐	Server. Activate the product. Open Community in a supported browser and specify a valid activation key for Community 2.4.
4	☐	Server or Client. Change the default password.
5	☐	Server (Online Installations only). Make sure gateway and access point firmware versions are updated to the latest versions as per "Device Requirements."
6	☐	Microsoft Edge. A Windows issue prevents the Edge browser from detecting/connecting to the Maintenance Unit. Consequently, access points cannot be programmed or audited without intervention. Open the Command prompt and issue the following command: `C:\windows\system32\CheckNetIsolation.exe LoopbackExempt -a -n=Microsoft.MicrosoftEdge_8wekyb3d8bbwe`
7	☐	Microsoft Edge. Add the Community Server IP address as a trusted site. Go to **Control Panel** > **Network and Internet** > **Internet Options** > **Security** > Trusted Sites. Click **Sites** and add the Community Server IP address.
8	☐	Microsoft Edge. Default Windows 10 Edge browser security blocks access to the local host thus disallowing Maintenance Unit communication for access point programming and auditing operations. Use Chrome or run the following command from the Windows console: ▪ Windows 10 Build 10158 or above: CheckNetIsolationLoopbackExempt-a-n=Microsoft.MicrosoftEdge_8wekyb3d8bbwen ▪ For previous builds: CheckNetIsolationLoopbackExempt-a-n=Microsoft.Windows.Spartan_cw5n1h2txyewy

10 Community upgrades

The following upgrade paths are supported:

- 1.6 and above to 2.4.

Community 2.3 introduced enhanced security mode to provide an additional layer of key security. Although the feature is disabled by default, dormakaba strongly recommends enabling enhanced security mode.

Before upgrading, refer to *Community Enhanced Key Security* to learn about the requirements for enhanced security mode and for important information about upgrading without enabling enhanced security mode. The document is accessible at the root of the software download folder.

10.1 Pre-upgrade checklist

1	☐	**IMPORTANT!** Server/Client. Verify that all Windows updates are installed.
2	☐	Server. Take a backup of the database before performing an upgrade. For online systems, take backups of SQL Server and MongoDB databases.
3	☐	Server/Client. Perform the installation as a **Local Administrator**.
4	☐	Server. Make sure antivirus software is disabled before proceeding with server installation.
5	☐	Server. If possible, disable Windows Defender for the duration of the installation.

10.2 Upgrade process

The upgrade is installed with the same options selected during the initial install.

1. In the dormakaba/Community folder, open the SERVER folder.
2. Double-click **CommunityServer.exe**. The installation wizard opens and prepares for setup.
3. On the Welcome page, click **Next**.
4. On the License Agreement page, accept the terms of the license agreement, then click **Next**. You can optionally print the agreement. The upgrade process starts.
5. When prompted, select whether to restart the server. Restart is required to complete the upgrade.

10.3 Post-upgrade checklist

1	☐	Restart the Community Server.
2	☐	Server. Re-enable antivirus software.
3	☐	Server. If necessary, re-enable Windows Defender.
4	☐	Upgrade the Community Client installed on workstations. The server and client versions must be the same.
5	☐	This step is recommended but not required for sites that do not enable enhanced security mode. Review RFID key type configurations at *System Settings > Advanced Settings > RFID key types*. Any change to settings requires reprogramming access points. Locks accept only those key types that are selected in System Settings.

To enable enhanced key security, refer to *Community Enhanced Key Security* (PK3776). The document lists requirements and provides step-by-step instructions for enabling enhanced key security.

10.4 SQL Server upgrades

dormakaba strongly recommends using SQL Server 2022 (or SQL Server Express 2022).
To upgrade to SQL Server 2022:

1. Back up the Community database.
2. In Service Manager, stop all Community services.
3. Run the following command:
   SQLEXPR_x64_ENU.exe /QS /ACTION=UPGRADE /INSTANCENAME=COMMUNITY/ISSVCAccount="NT Authority\Network Service" /IACCEPTSQLSERVERLICENSETERMS
4. Restore backed up database.
5. Restart all Community services.

SQL Server 2022 (16.x) supports upgrade from the following versions of SQL Server:

- SQL Server 2012 (11.x) SP4 or later
- SQL Server 2014 (12.x) SP3 or later
- SQL Server 2016 (13.x) SP3 or later
- SQL Server 2017 (14.x)
- SQL Server 2019 (15.x)

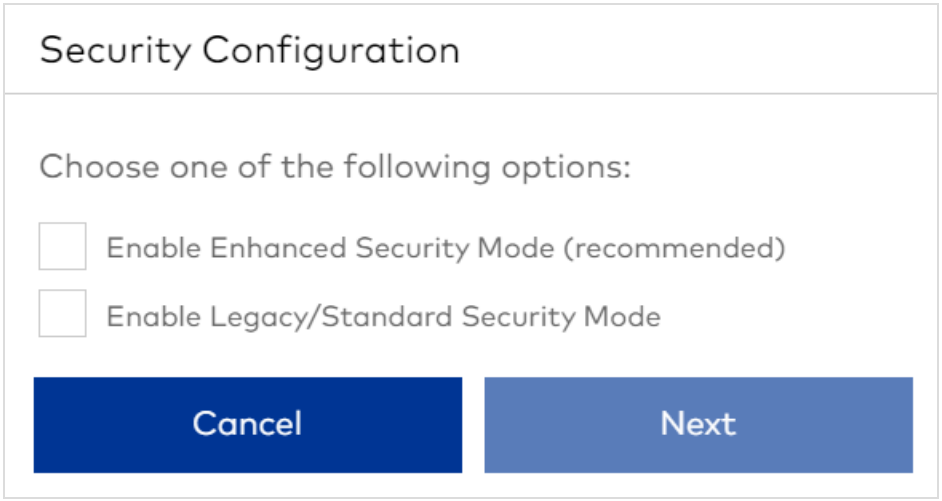
11 Getting started with Community

This chapter provides basic information for getting started with Community.

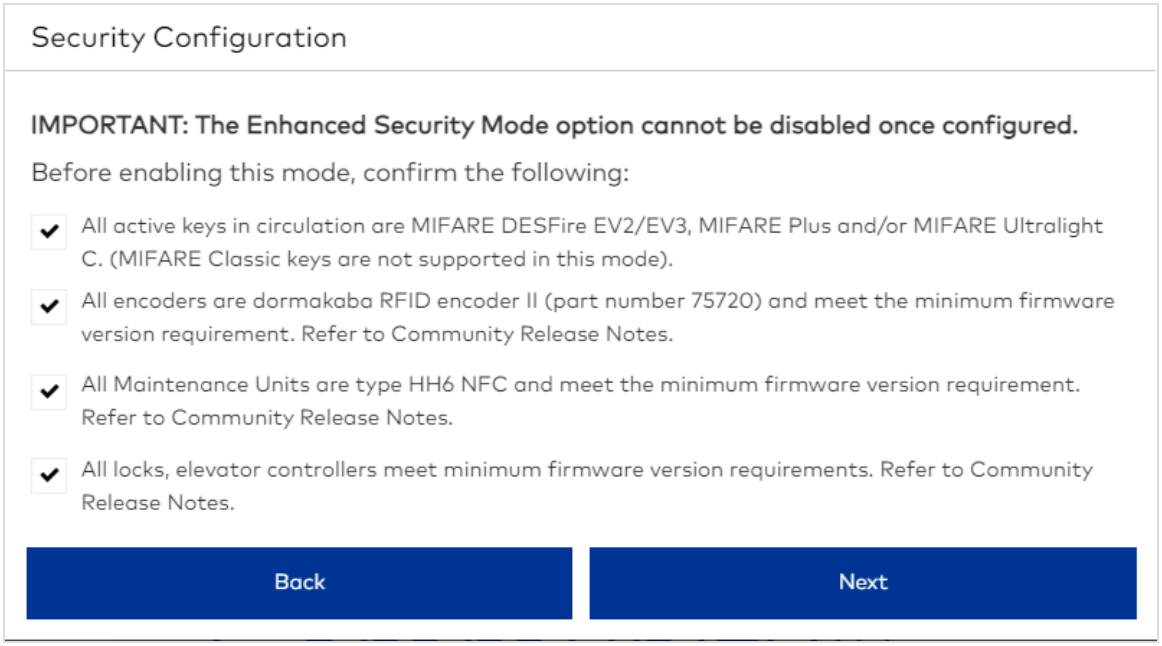
11.1 Product activation

Community must be activated to access, configure and use the product.

1. Go to the IP address of the Community server in the location bar of a supported browser.
2. Specify a valid activation key. dormakaba provides the activation key with the product purchase or upon request when a new activation key is required.
3. Log in using the Admin01 account. The default password is provided with the product purchase. Community prompts require changing the password for the Admin01 account.
   - For new installation initial logins, proceed to the next step.
   - For all other logins, the Home page displays. Proceed to configure the product.
4. Select whether to enable enhanced security mode, then click Next.



   - If the option Enable Enhanced Security Mode was selected, proceed to the next step.
   - If the option Enable Legacy/Standard Security Mode was selected, the Home page displays. Proceed to configure the product.
5. Acknowledge that requirements to enable enhanced security mode are established, then click Next.



The Home page displays. Proceed to configure the product.

11.2 Site configuration workflow

The Community workflow is an excellent resource to guide your deployment. The document provides an overview of the application flow and the first steps to take in each module to set up Community.

The *Community User Guide* is a new resource that provides information and instructions for all Community Operators.

- The "Site Configuration" section provides an easy-to-follow workflow and step-by-step instructions for setting up Community.
- The "Using Community" section provides instructions for day-to-day work after Go Live and includes *Troubleshooting* and *Working with ...* topics that address some of the more complicated situations.

Look for the guide in the software download folder.

11.3 Remember to ...

- Go to **System Settings** > **Database Backup** to configure regularly scheduled backups and data retention for the Community SQL Server database (and MongoDB for online systems). The recommendation is to store backups at a secure external location.
- After completing Site Configuration, go to **System Settings** > **Failsafe Keys** to make backup keys.
- If not licensed for PPK/SPK Storage, go to System Keys and make primary and secondary program keys.

A Appendix A: Service Manager

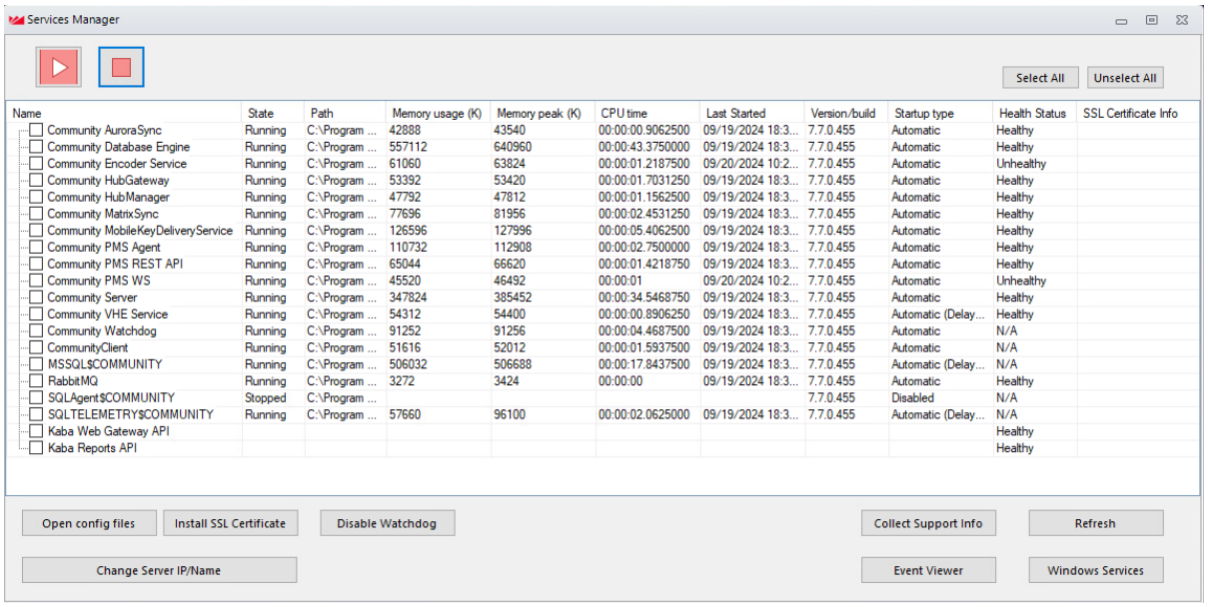
The Service Manager provides convenient access to post-installation configuration options. Access the Service Manager at the following locations:

- On the Community server:

C:\Program Files\dormakaba\Community Server\Services\Service Manager\ServiceManager.exe

- On the Community client:

C:\Program Files (x86)\dormakaba\Community Client\Services\Service Manager\ServiceManager.exe

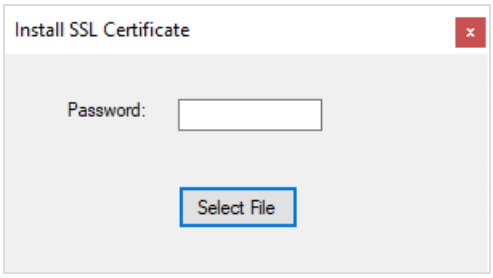


A.1 Installing / renewing SSL certificate after installation

Use the Service Manager to install or renew an SSL certificate on the Community server after installation. Each Community workstation must be updated to use the HTTPS protocol.

A.1.1 Server

1. On the Community server, open the Service Manager.
2. Click Install SSL Certificate.
3. Disregard the warning message and click Yes to proceed.



4. If applicable, specify the password for the certificate.
5. Click Select File.
6. Navigate to and select the certificate (.pfx).
7. When notified the certificate was installed successfully, click OK.

A.1.2 Client

The following steps must be performed on each Community workstation.

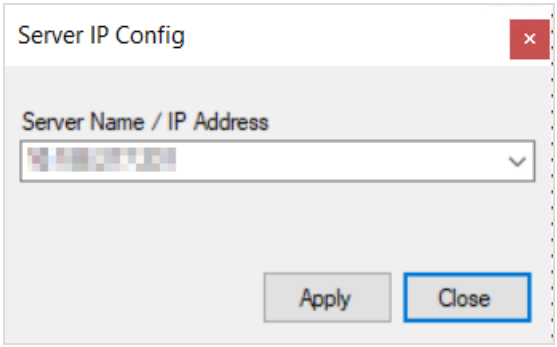
1. Open the Service Manager.
2. Select the CommunityClient service and click  to stop the service.
3. Click Open Config files.
4. Change "WebAPIUrl" and "signalrURL" values to point to **https**:
   - From:
     <add key="WebAPIUrl" value="http://<Community Server IP>/WebAPI/" />
     <add key="signalrURL" value="http://< Community Server IP>/
     WebAPI/signalr/" />
   - To:
     <add key="WebAPIUrl" value="https://< Community Server IP>/WebAPI/" />
     <add key="signalrURL" value="https://< Community Server IP>/
     WebAPI/signalr/"/>
5. Save and close the configuration file.
6. Click  to restart the CommunityClient service.

A.2 Changing server IP address

Use the Service Manager to change the Community server IP address after installation. Changing the IP address requires that the Community client be uninstalled and reinstalled on each workstation.

A.2.1 Server

1. On the Community server, open the Service Manager.
2. Click Server IP Config.
3. Disregard the warning and click Yes to proceed.
4. Specify the new IP address, then click Apply.



5. Restart the Community Server.

A.2.2 Client

The following steps must be performed on each Community workstation.

1. Open the Service Manager.
2. Select the CommunityClient service and click  to stop the service.
3. Click Open Config files.

4. Change “WebAPIUrl” and “signalrURL” values to point to the new IP address.
   - From:
     <add key="WebAPIUrl" value="https://<Community Server IP>/WebAPI/" />
     <add key="signalrURL" value="https://< Community Server IP>/
     WebAPI/signalr/" />
   - To:
     <add key="WebAPIUrl" value="https://< Community NewServer IP>/WebAPI/" />
     <add key="signalrURL" value="https://< Community NewServer IP>/
     WebAPI/signalr/"/>
5. Save and close the configuration file.
6. Click  to restart the CommunityClient service.

A.3 Disable/enabling Watchdog

The Service Manager includes a Watchdog feature that performs regular healthchecks on server. The Watchdog is enabled by default. To disable / enable Watchdog, open Service Manager and click the appropriate button.

PK3695-EN 2.4.0 - 05/2025

www.dormakaba.com

dormakaba Canada
105 Marcel-Laurin Blvd
Montreal, Quebec H4N 2M2
Canada
T: +1 877 468-3555

www.dormakaba.com