

dormakaba Canada, Inc.

# Community™

## Installation Guide

Version 1.9

**CONFIDENTIAL:** This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of dormakaba.

© dormakaba Canada, 2020, All rights reserved. dormakaba and Community are trademarks of dormakaba Canada. All other trademarks are property of their respective owners.

PK#: 3695 Rev 20200504

# TOC

Welcome .....	3
Requirements .....	3
Pre-Installation Checklist .....	8
Prepare for Using an Existing SQL Server Instance .....	9
Community Server Installation .....	17
Community Client Installation .....	29
Post-Installation Checklist .....	35
Community Server Upgrades .....	36
Getting Started with Community .....	37

# Welcome

Community is web-based access management software for our multihousing property employees to easily configure resident, vendor and staff access. Community empowers property managers to intuitively authenticate and manage authorization throughout the entire property providing security, convenience and operational efficiency.

Community offers web-based access from a desktop computer, laptop or mobile device while on the property's network. Property configuration and access management of residents, staff and vendors can be programmed remotely at any time 24/7.

## 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.

### System Requirements

The following table lists minimum requirements for the Community Server and Community workstation. Ancillary recommendations are listed at the end of the table.<sup>1</sup>

Requirement	Community Server	Community Workstation
CPU	<ul style="list-style-type: none"> <li>■ 2GHz/64-bit/quad core</li> <li>■ Dedicated server (recommended)</li> </ul>	2GHz/64-bit/dual core
RAM	16 GB or more	8GB
Disk Drive Free Space	30GB <sup>2</sup>	50MB
Network Controller	Gigabit Ethernet - 1Gb/second	Gigabit Ethernet - 1Gb/second
USB 2.0 Port	Required to connect encoder	Required to connect encoder
Operating System	<ul style="list-style-type: none"> <li>■ Microsoft Windows Server 2019/2016/2012 R2 Standard</li> </ul>	<ul style="list-style-type: none"> <li>■ Microsoft Windows 10 Pro/Enterprise (English/French)</li> </ul>

Requirement	Community Server	Community Workstation
	(English/French)—Suitable for large and small-scale implementations and Online functionality. ■ Windows 10 Pro/Enterprise (English/French)—Use for small-scale implementations only (recommended maximum of 1,000 access points and two encoders). <sup>3</sup>	
Database <sup>4</sup>	■ SQL Server Express 2014/2017 ■ SQL Server 2014/2016	N/A
Web Browser <sup>5</sup>	■ Google Chrome (latest) ■ Microsoft Edge (latest)	■ Google Chrome (latest) ■ Microsoft Edge (latest)

<sup>1</sup>Additional recommended hardware for the Community Server includes: UPS Backup, Integrated HD Graphics Card, Keyboard/Mouse.

<sup>2</sup>Additional free space may be required depending on database backup and archiving settings.

<sup>3</sup> Windows 10 Pro/Enterprise does not support Online Communication, the online functionality implemented by deploying gateways.

<sup>4</sup>The Microsoft OLE Database Driver for SQL Server is also required. Community prompts to install the driver if it is not detected. Microsoft reports issues that prevent SQL Server from installing successfully on a Domain Controller. Avoid installing SQL Server on a Domain Controller.

<sup>5</sup>Recommended Web browser resolution: 1366 x 768 or greater.

## Network Requirements



If you have a firewall, configuration changes may be required to make ports accessible to the Community Server.

The following table lists the default Community Server port settings.

Port	Protocol	Description
80	HTTP	Community Web User Interface
443	HTTPS	Community Web User Interface
28000	TCP	KABA RFID IP encoder

## Device Requirements

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



Community is backward compatible with all previous firmware versions.

### Encoders

The following table shows the encoders that Community supports and the latest supported firmware version.

KABA RFID	1.012

### Maintenance Units

The following table shows the M-Units that Community supports and the latest supported firmware version.

HH6	2.21



The latest supported firmware versions are required when using the Community No Touring feature and when programming units and suite units in Multi-Housing Toggle Mode.

### Locks

The following table shows the locks that Community supports and the latest supported firmware versions.

	Boot	Main	Quantum	BLE	ZigBee
MT4, Pixel	11.20.19.2	11.20.19.2	02.06.19.1	1.1.1.0	1.10x
RCU4	11.20.19.2	11.20.19.2	02.06.19.1	1.1.1.0	1.10x
RT+	07.26.19.4	07.26.19.4	N/A	1.1.1.0	5.12
Saffire LX (M,E & C, D & I), Nova	07.26.19.4	07.26.19.4	N/A	1.1.1.0	5.12
Confidant	09.03.19.2	09.03.19.2	N/A	1.1.1.0	1.10x
RT	06.14.18.2	06.14.18.2	N/A	1.1.1.0	1.10x



The latest supported firmware versions are required when using the Community No Touring feature and when programming units and suite units in Multi-Housing Toggle Mode.

## Elevator Controllers

The following table shows the elevator controllers that Community supports and the latest supported firmware versions.

	Boot	Main	Quantum	BLE	ZigBee
MFC	N/A	0.017	N/A	N/A	N/A
EMCC	N/A	20090929	N/A	N/A	N/A
MCC 8/12	N/A	0.031398	N/A	N/A	N/A
ECU/RCU4	11.20.19.2	11.20.19.2	02.06.19.1	1.1.1.0	1.10x

## ZigBee Gateways

The following table shows the ZigBee gateways that Community supports and the latest supported firmware versions.

	Boot	Main	Quantum	BLE	ZigBee
GWY I		0.221			
GWY II		0.01			

## Interface Requirements

Community supports the following:

- **Aurora SDK**—v1.0.19
- **Aurora software**—v1.0.19 or higher

## No Touring Requirements

To use the Community No Touring 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*.

# Pre-Installation Checklist

## Requirements

1	<input type="checkbox"/>	Server/Client. Verify that all <a href="#">system requirements</a> are met.
2	<input type="checkbox"/>	Server. Verify that the <b>Date/Time</b> and <b>Time Zone</b> settings are correct. (The Community Server and the locks installed at access points must be configured for the same time zone.)
3	<input type="checkbox"/>	<b>IMPORTANT!</b> Server/Client. Verify that all Windows updates are installed.
4	<input type="checkbox"/>	Server. Verify that Windows PowerShell 4.0 is installed.
5	<input type="checkbox"/>	Server. Verify that the following programs are <b>NOT</b> installed:
6	<input type="checkbox"/>	SQL Server (only if not connecting to an existing SQL instance)
7	<input type="checkbox"/>	Redis
8	<input type="checkbox"/>	RabbitMQ
9	<input type="checkbox"/>	Web Server IIS
10	<input type="checkbox"/>	Server. Verify that you have a new activation key for Community .
11	<input type="checkbox"/>	Server/Client. Verify that the operating system is up and activated.
12	<input type="checkbox"/>	Server/Client. Perform the installation as a <b>Local Administrator</b> .
13	<input type="checkbox"/>	If applicable, <a href="#">prepare to connect to an existing SQL Server instance</a> .

## Recommendations

1	<input type="checkbox"/>	<b>IMPORTANT!</b> Install the Community Server in a secure physical location.
2	<input type="checkbox"/>	Make sure that you have your Windows OS Installer available.
3	<input type="checkbox"/>	Server. If possible, disable Windows Defender for the duration of the installation.

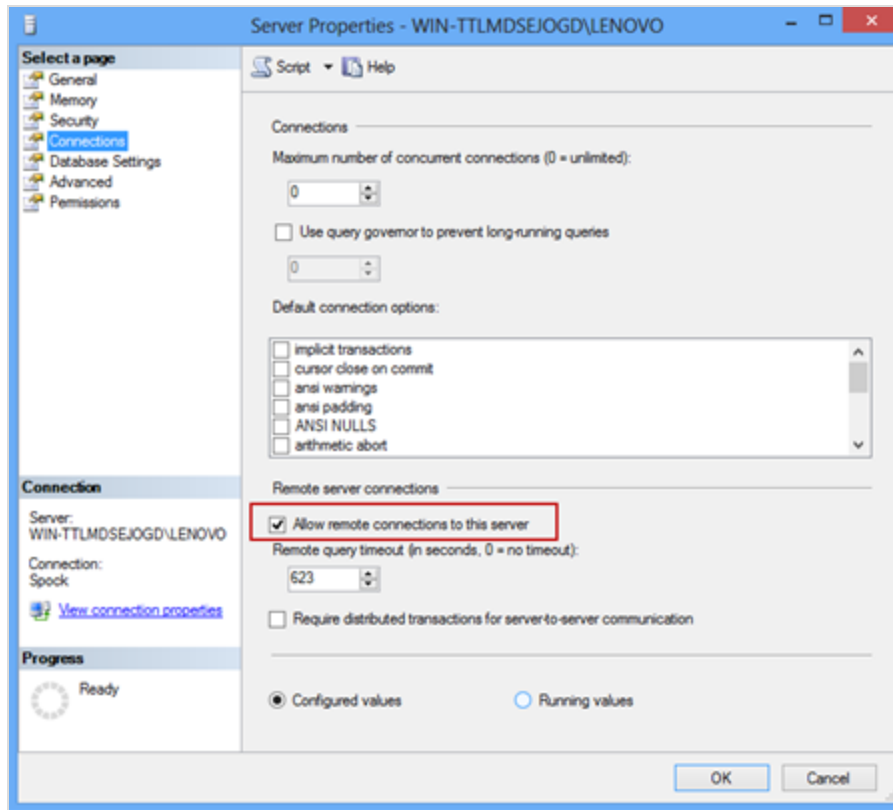


# Prepare for Using an Existing SQL Server Instance

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

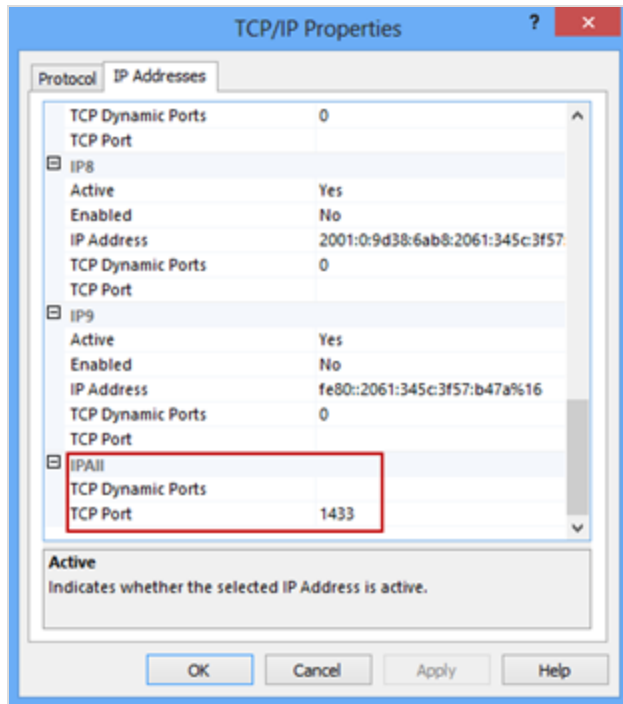
1. In the Community installation package, go to the **AMBIANCE\_PREREQUIS** folder and copy the master database file (Community.mdf) to the remote computer where Microsoft SQL Server is installed. Recommended path: C:\Program Files\Microsoft SQL Server\MSSQLX.SQLEXPRESS\MSSQL\DATA\ -> X is the SQL instance name.
2. Attach the database:
  - a. In SQL Server Management Studio Object Explorer, connect to an instance of the SQL Server Database Engine, then click to expand that instance view.
  - b. Right-click **Databases** and select **Attach**.
  - c. In the Attach Databases dialog box, click **Add**.
  - d. In the Locate Database Files dialog box, select the location where the "Community.mdf" file was previously copied and select Community.mdf.
  - e. Click **OK**.

3. Right-click on the server and select **Properties**.



4. For **Connections**, select the **Allow remote connections to this server**, then click **OK**.
5. Open the SQL Server Configuration Manager.
6. Right-click **TCP/IP** and select **Properties**.

7. In the TCP/IP Properties dialog, select the **IP Addresses** tab and scroll to **IPv4**.
8. Set the **TCP Dynamic Ports** to blank and **TCP Port** to **1433**. (Port 1433 is the default instance that SQL Server uses.)



5. Click **Apply** > **OK**.

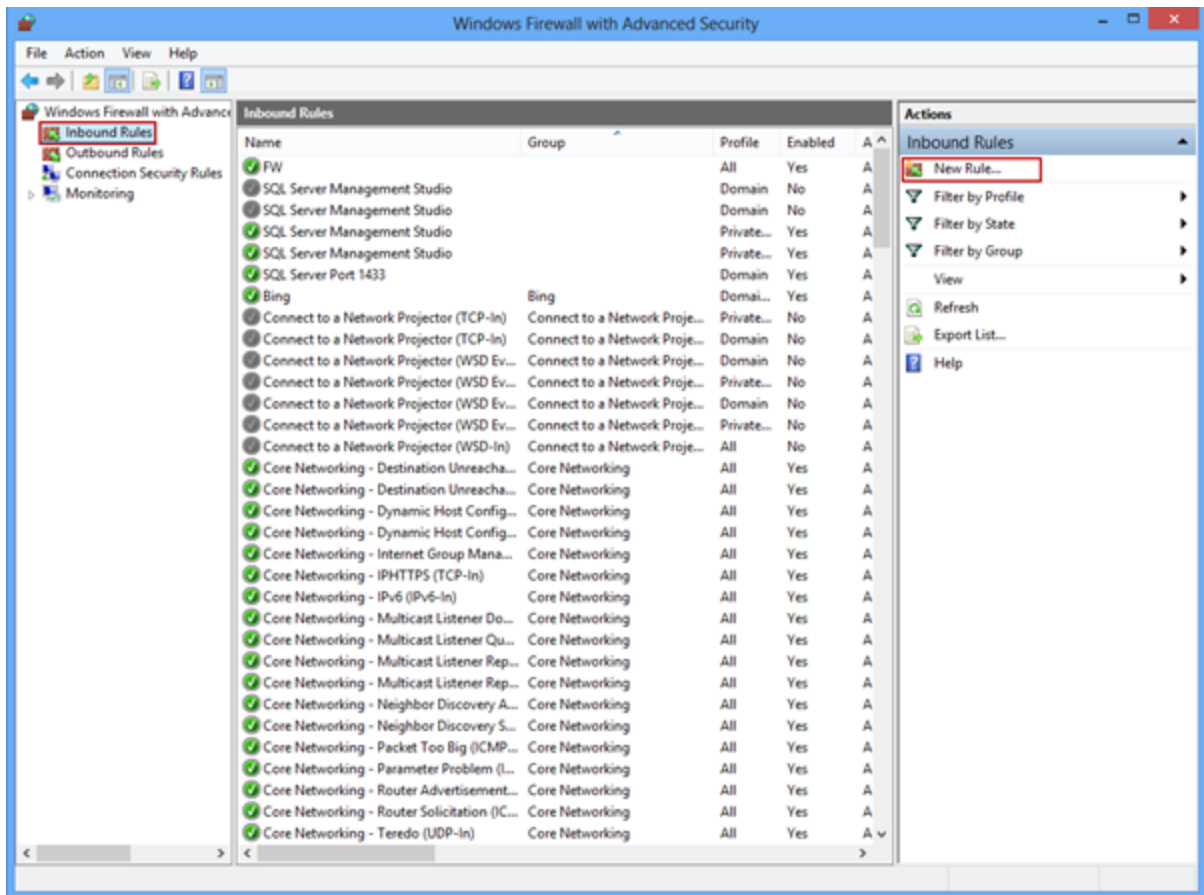
If using a firewall, continue to the next section to open access for the database engine.

## Configure a Windows Firewall for Database Engine Access

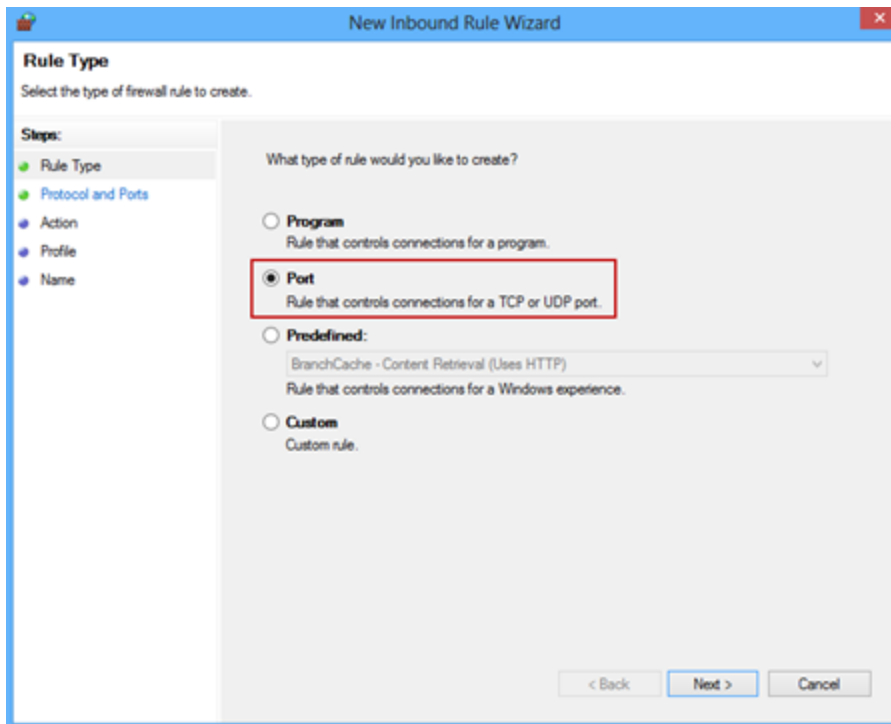
If the firewall is turned on, you need to add an exception for the 1433 port to allow TCP/IP traffic on Port 1433 and UDP traffic on Port 1434.

1. Go to **Programs > Administrative Tools** and select **Windows Firewall with Advanced Security**.
2. Select **Inbound Rules**.

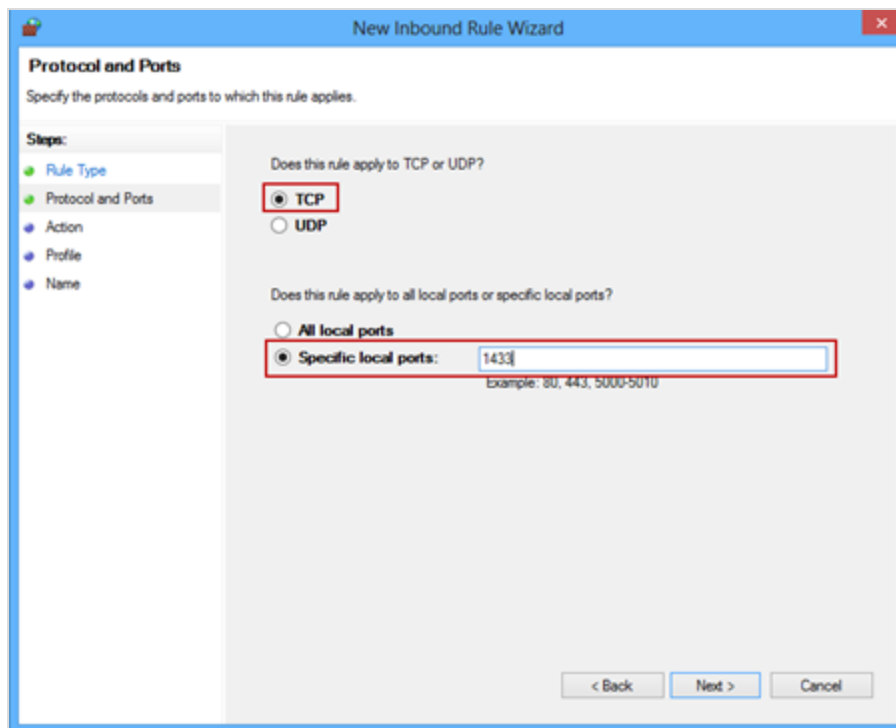
- Under **Actions**, select **New Rule**.



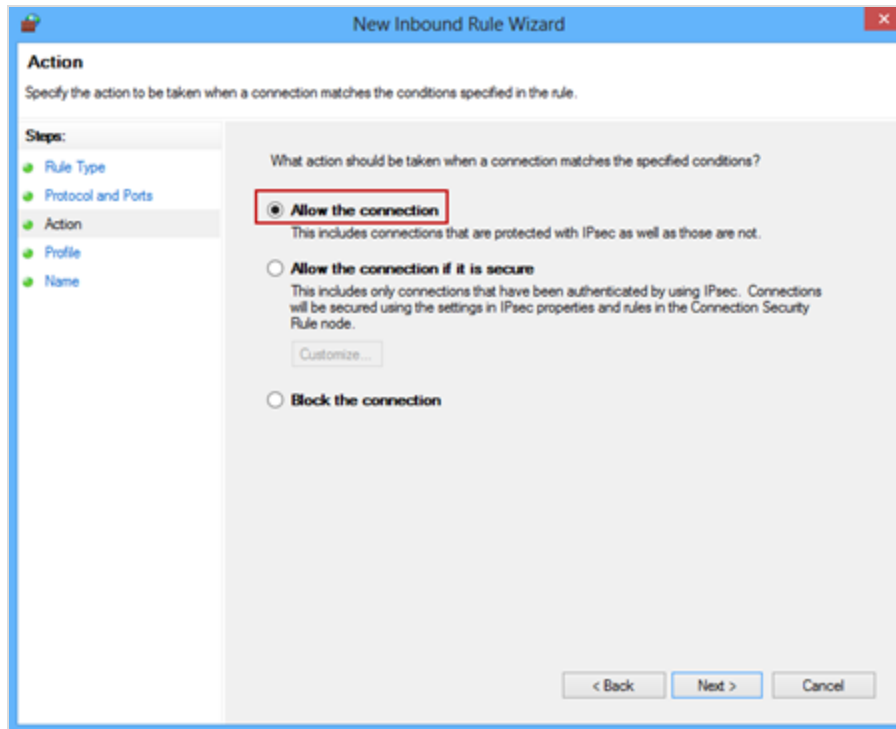
- For Rule Type, select **Port**, then click **Next**.



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



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



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

When does this rule apply?

☒ **Domain**  
Applies when a computer is connected to its corporate domain.

☒ **Private**  
Applies when a computer is connected to a private network location, such as a home or work place.

☒ **Public**  
Applies when a computer is connected to a public network location.

< Back   **Next >**   Cancel

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

**New Inbound Rule Wizard**

**Name**  
Specify the name and description of this rule.

**Steps:**

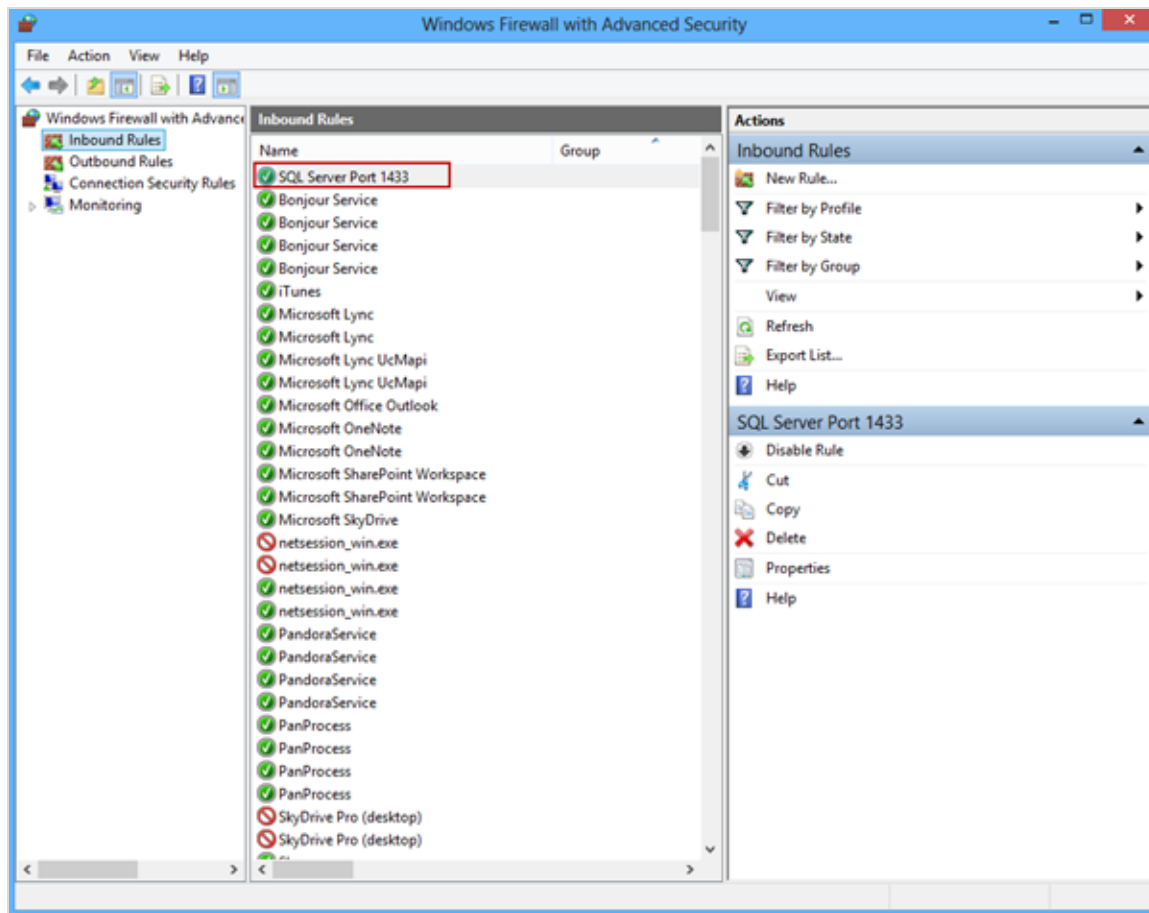
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name**

Name:  
SQL Server Port 1433

Description (optional):

< Back   **Finish**   Cancel

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



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



# Community Server Installation

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

To install the Community Server:

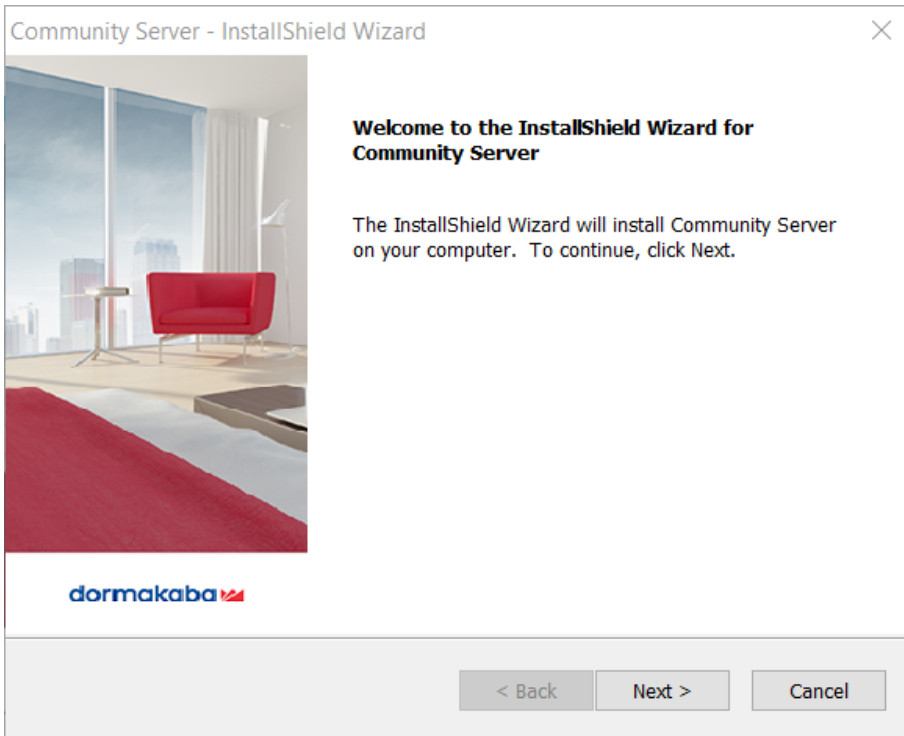
1. In the dormakaba/Community folder, open the SERVER folder.
2. Double-click **CommunityServer.exe**.

The installation wizard opens and prepares for setup. The wizard checks for Microsoft .NET Framework 4.6.2, and installs it if not found. The following screen is displayed after launching setup when using the latest signing certificate. Click **Yes** to continue.



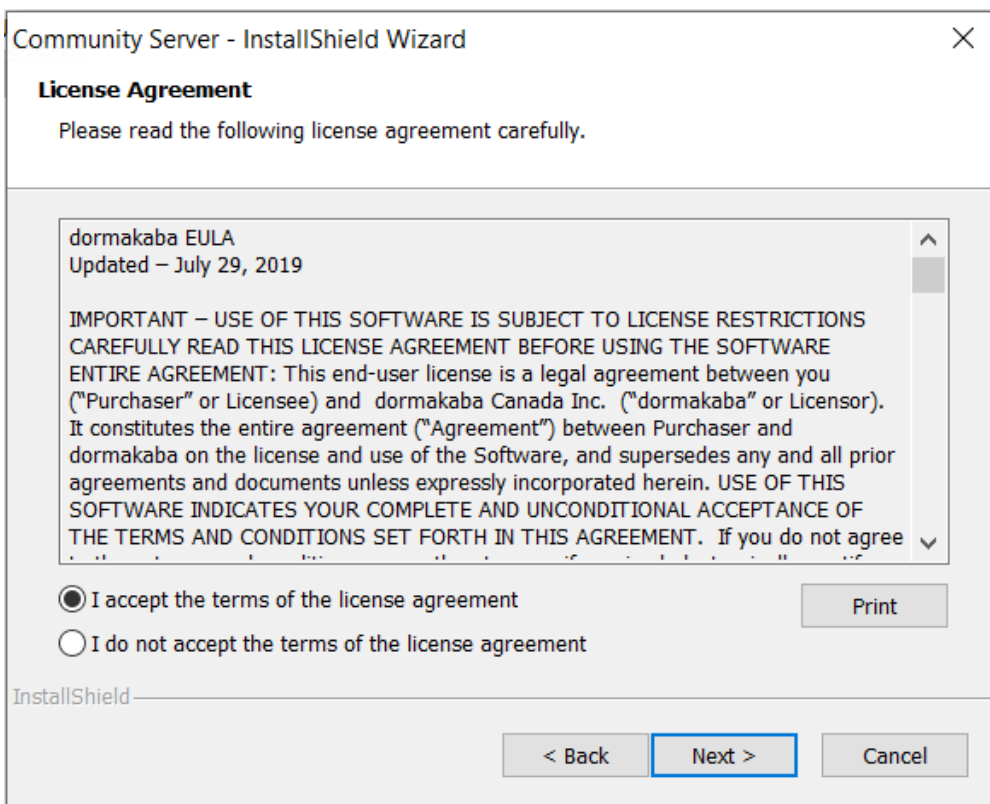
3. (conditional) If the Microsoft OLE Database Driver for SQL Server is not installed, click **Install** to proceed with the installation.
4. Follow the instructions for each of the following wizard pages. When a restart is required, confirm to proceed with the installation.

## Welcome Page



On the Welcome page click **Next**.

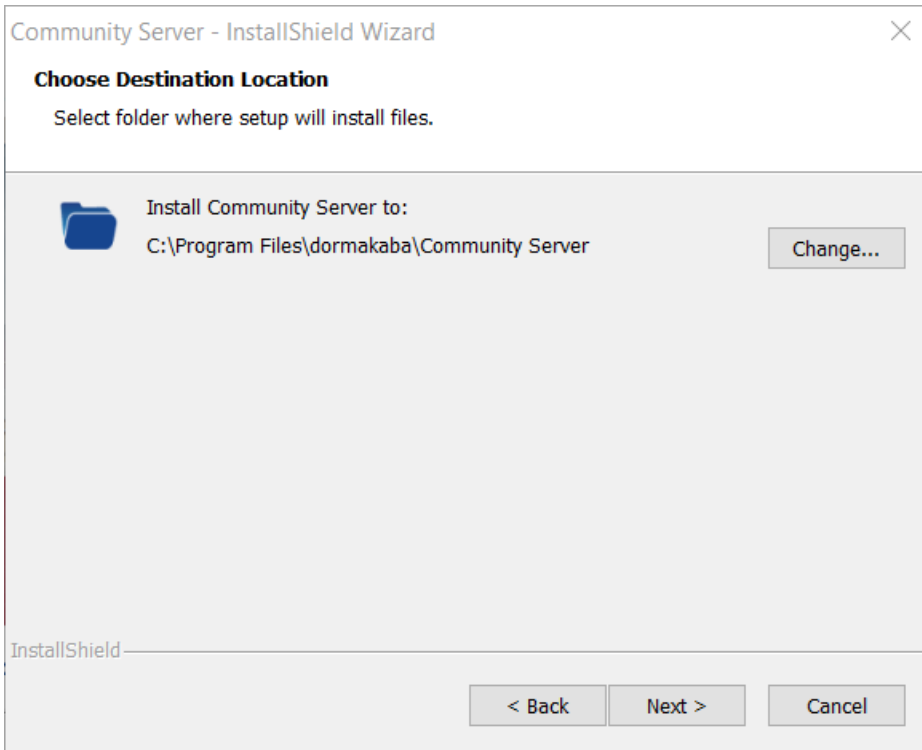
## License Agreement Page



On the License Agreement page:

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

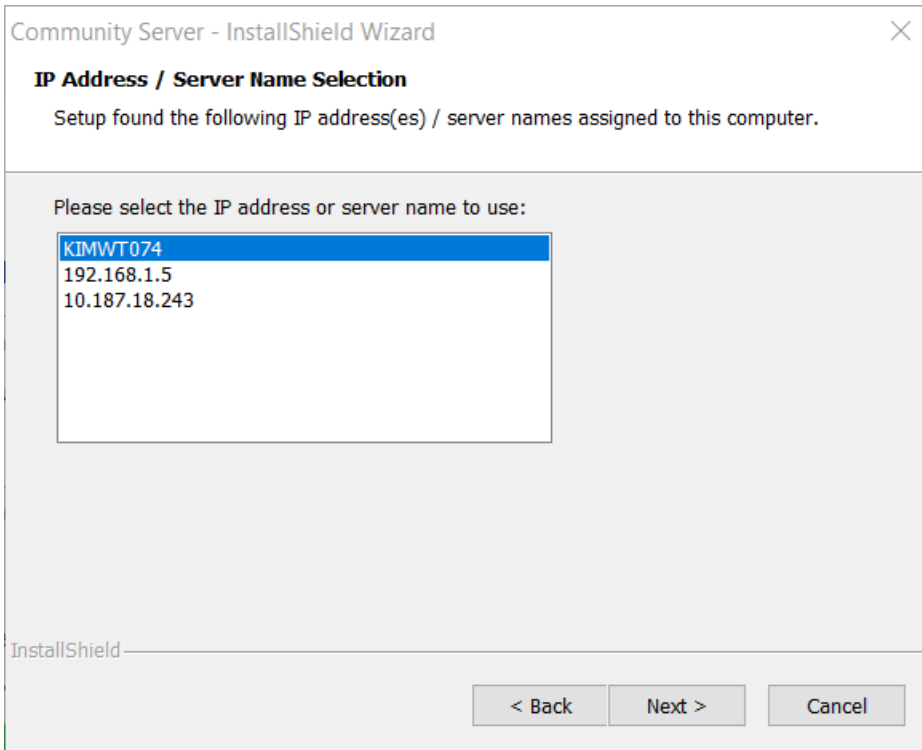
## Choose Destination Location Page



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**.

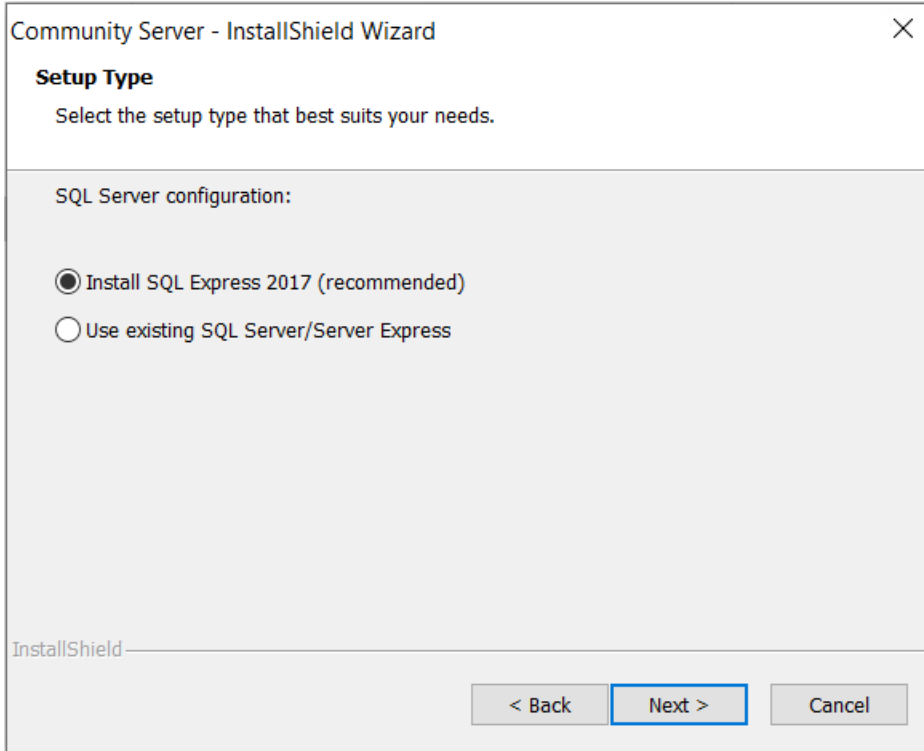
## IP Address / Server Name Selection Page



On the IP Address / Server Name Selection page:

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

## Setup Type Page



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 2017 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*.

## SQL Database Server Page

Community Server - InstallShield Wizard

**SQL Database Server**  
Select SQL database server.

SQL Database server that you are installing to:  
(local)\COMMUNITY Browse...

Connect using:

☒ SQL Server authentication using the Login ID and password below

Login ID:

Password:

InstallShield

< Back Next > Cancel

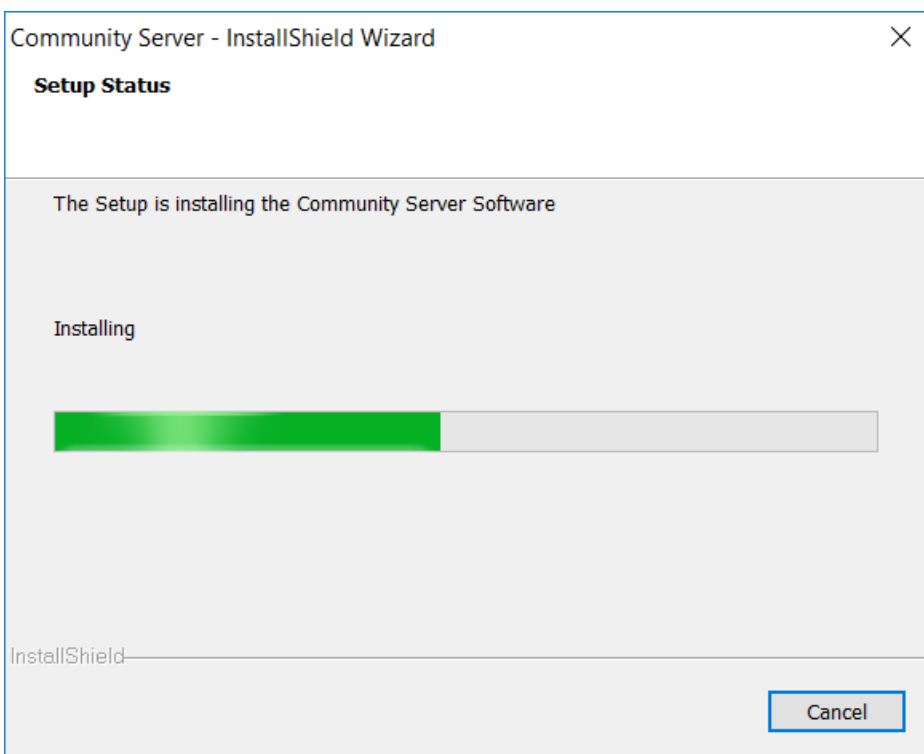
On the SQL Database Server page:

1. Click **Browse**, navigate to and select the .mdf (or .ndf) database file.
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.

## Setup Status Page



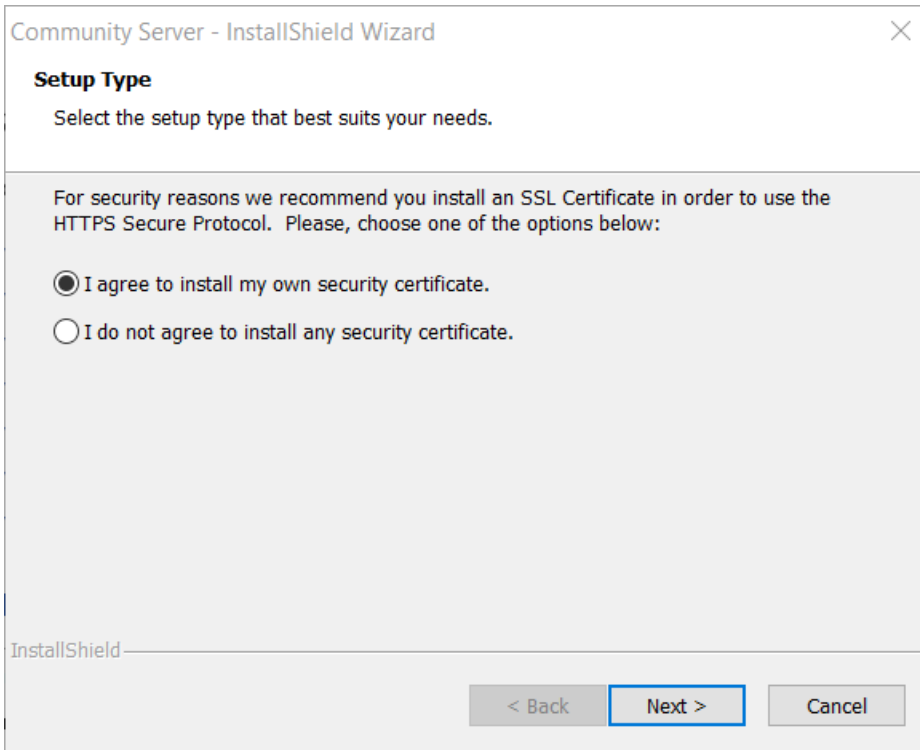
The Setup Status page displays the installation status. When prompted, click **Next**.

The following third-party applications are installed:

- Microsoft .NET Framework 4.6.2
- Microsoft SQL Server Express 2017 (if selected)
- Redis Server
- Redis Desktop
- Erlang Software
- RabbitMQ
- VC++ Redistributable



## Setup Type Page



On the Setup Type page:

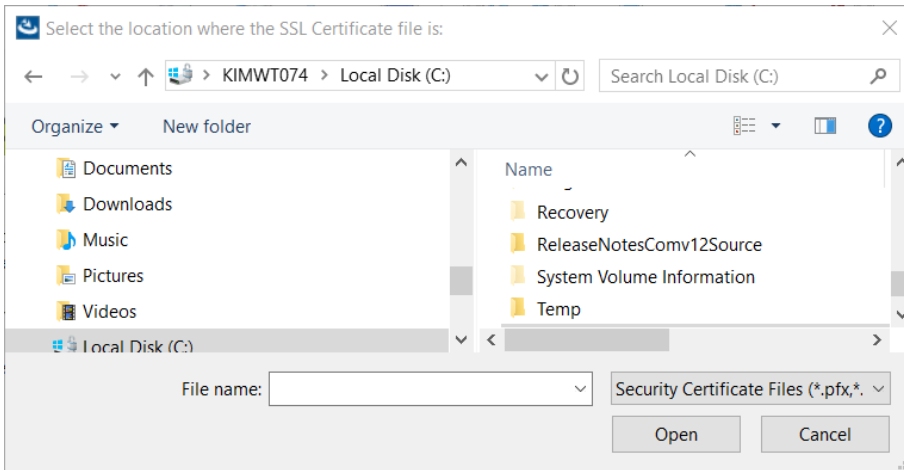
1. Select whether to install an SSL (Secure Sockets Layer) certificate.

 dormakaba strongly recommends installing an SSL certificate to enable the HTTPS protocol. Security is your responsibility. If you opt to install an SSL certificate post-installation, you must also uninstall and reinstall the Community Server in Secure Mode. The process does not affect the Community database; however, dormakaba recommends backing up the database prior to un-installing Community as a precaution. The server path must be changed from HTTP:// to HTTPS://.

2. Click **Next**.

If you did not agree to install an SSL certificate, a warning displays. If you continue with the installation, proceed to Restart Message.

## Choose SSL Certificate



In File Explorer:

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

## Password Page

Community Server - InstallShield Wizard

**Password**

This setup has been password protected.

If applicable, enter the password for the SSL certificate, to use the HTTPS protocol.

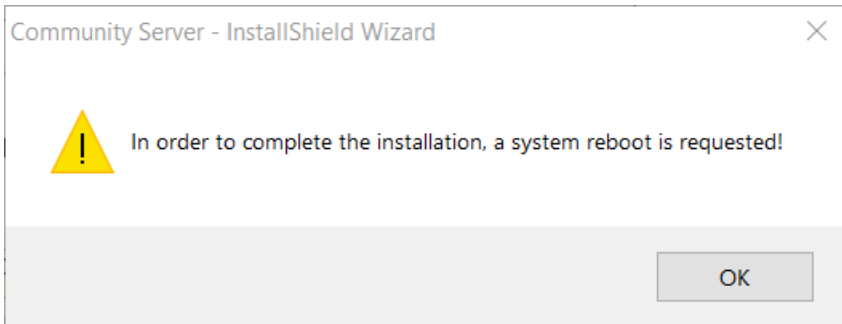
InstallShield

< Back   Next >   Cancel

On the Password page:

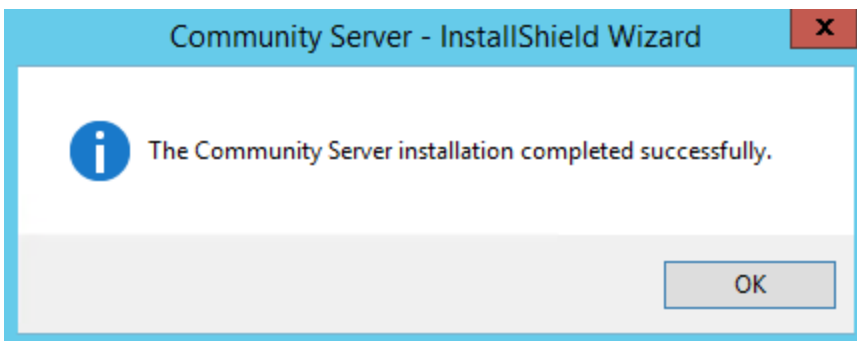
1. Specify the password for the SSL certificate that you selected.
2. Click **Next**.

## Restart Message



When prompted to restart the server, click **OK**.

## Installation Complete



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

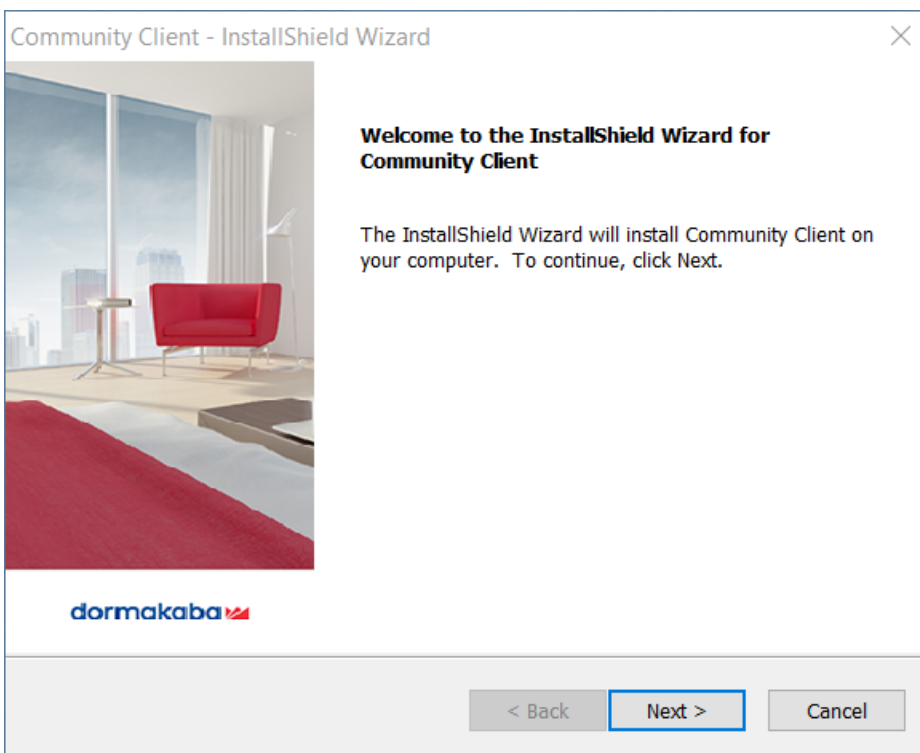
# Community Client Installation

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 the dormakaba/Community folder, open the CLIENT folder.
2. Double-click **CommunityClient.exe**.  
The installation wizard opens and prepares for setup. The wizard checks for Microsoft .NET Framework 4.6.2, and installs it if not found.
3. Follow the instructions for each of the following wizard pages.

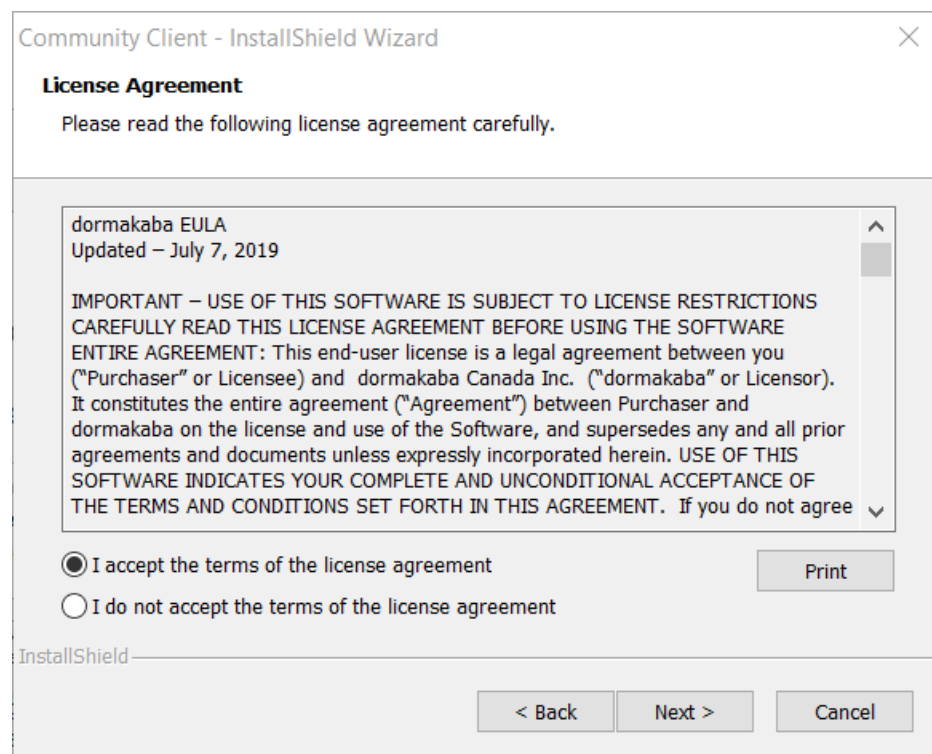
## Welcome Page



On the Welcome page:

- Click **Next**.

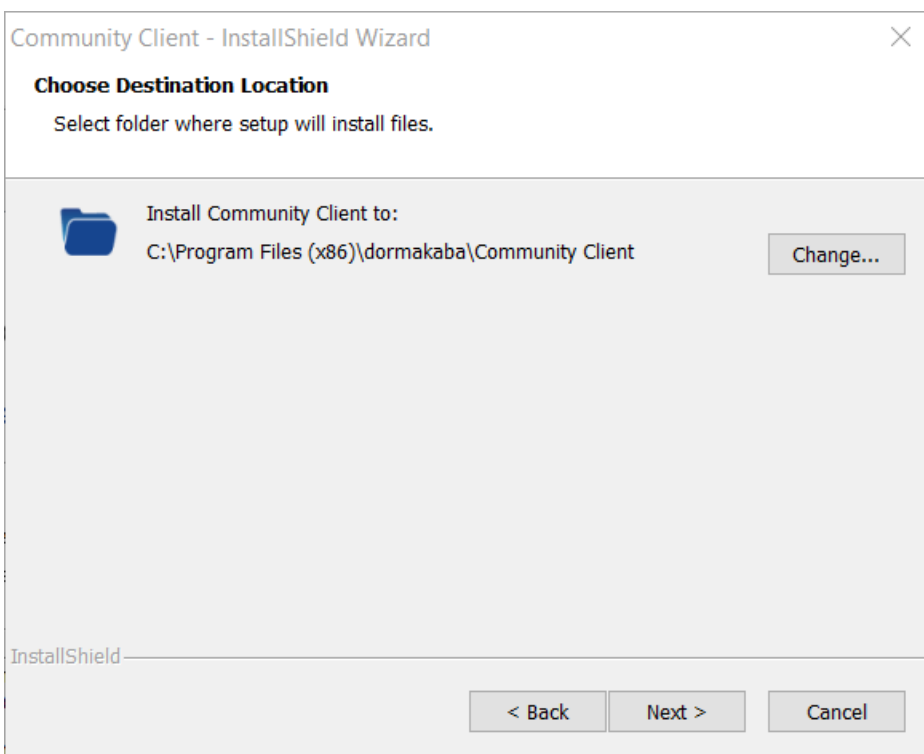
## License Agreement Page



On the License Agreement page:

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


## Choose Destination Location Page

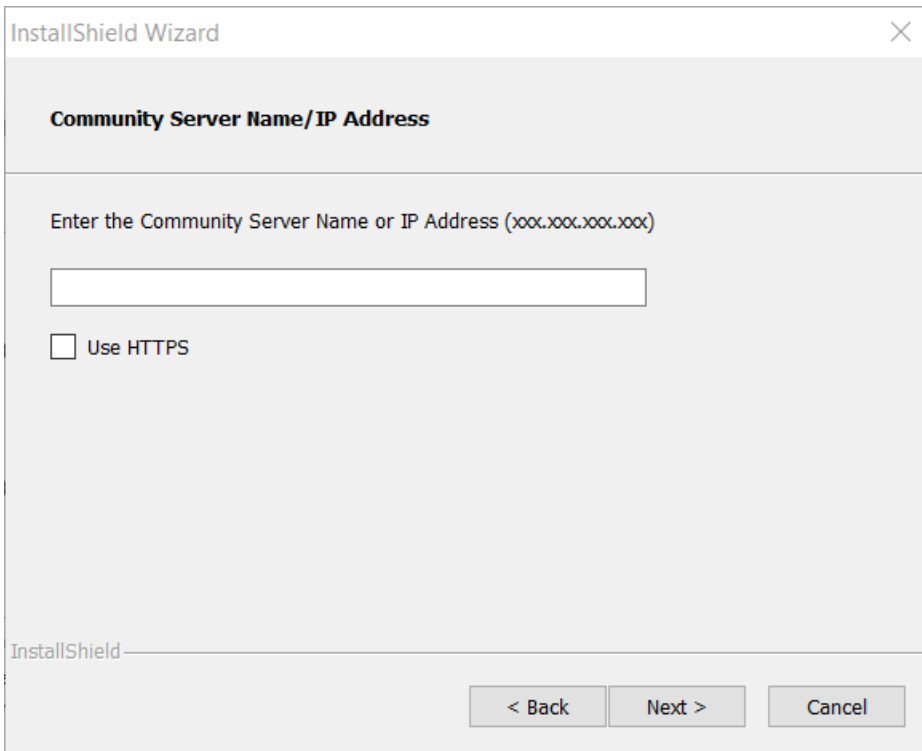


On the Choose Destination Location page:

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**.

## Community Server Name/IP Address Page

 This page does not display when the Community Client is downloaded and installed from the Community user interface. Instead, the installation process automatically detects the IP address or host name.



InstallShield Wizard

**Community Server Name/IP Address**

Enter the Community Server Name or IP Address (xxx.xxx.xxx.xxx)


☐ Use HTTPS

InstallShield

< Back   Next >   Cancel

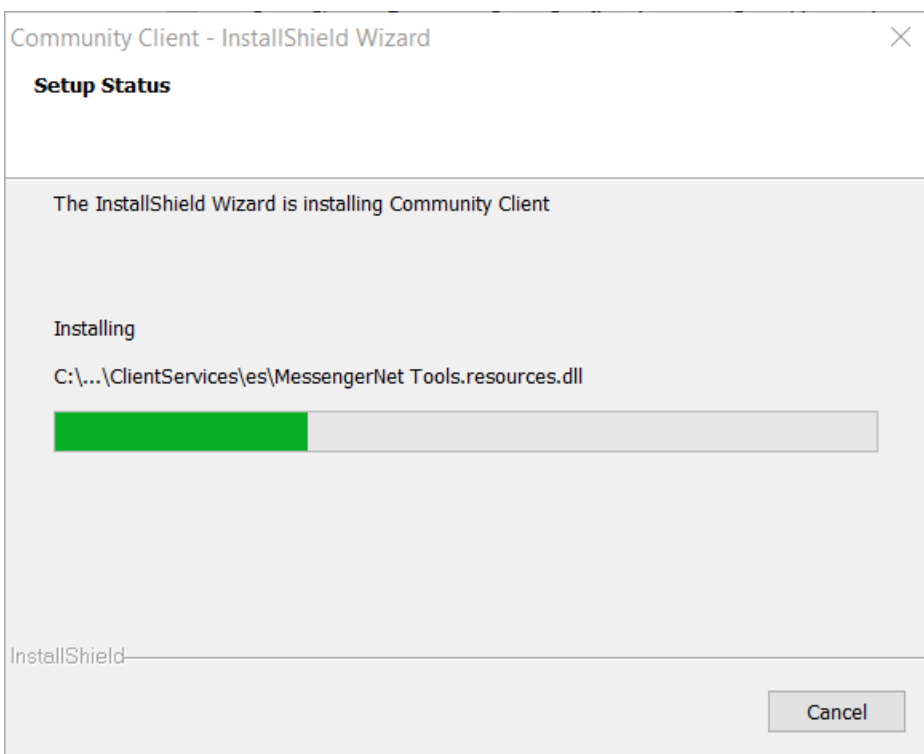
On the **Community Server Name/IP Address** page:

1. Specify the IP address or host name of the Community Server.
2. Select the **Use HTTPS** checkbox if the Community Server is SSL-enabled.
3. Click **Next**.

 If an SSL certificate is installed on the Community Server post-installation, the client must be uninstalled and reinstalled or reconfigured on all workstations to communicate with the Server.

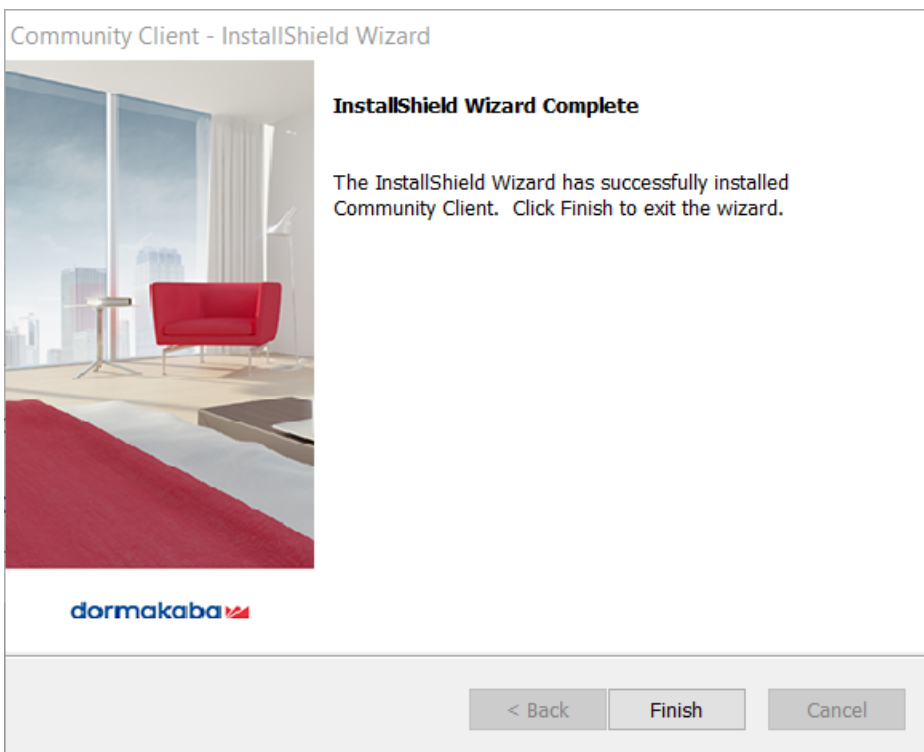


## Setup Status Page



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

## Installation Complete Page



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

# Post-Installation Checklist

1	<input type="checkbox"/>	Server. If necessary, re-enable Windows Defender.
2	<input type="checkbox"/>	Server. Activate the product. Open Community in a supported browser and specify a valid activation key for Community1.9.
3	<input type="checkbox"/>	Server or Client. Change the default passwords. Log in to Community using the following account: username= <b>admin01</b> , password= <b>Admin@01</b> . Change the default password. Repeat the steps for account: username= <b>admin02</b> , password= <b>Admin@02</b> .
4	<input type="checkbox"/>	Microsoft Edge. Add the Community Server IP address as a trusted site. Go to <b>Control Panel &gt; Network and Internet &gt; Internet Options &gt; Security &gt; Trusted Sites</b> . Click <b>Sites</b> and add the Community Server IP address.
5	<input type="checkbox"/>	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:  <code>C:\windows\system32\CheckNetIsolation.exe LoopbackExempt -a -n=Microsoft.MicrosoftEdge_8wekyb3d8bbwe</code>

# Community Server Upgrades

The following upgrade paths are supported:

- 1.6 and above to 1.9

After the upgrade, you must restart the Community Server.

Because the Community Client installed on workstations must be the same version as the Community Server, you must also upgrade the Client. The recommended method is to uninstall the previous version of the Client and then reinstall the current version.

 The upgrade process preserves the Community database.

# Getting Started with 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 your installation folder.

## Remember to ...



Go to **System Settings > Database Backup & Archiving** to configure regularly scheduled backups and archiving for the Community SQL Server database. The recommendation is to store backups at a secure external location.



If Online Communication will be enabled, you must also establish a means to regularly back up the Mongo database (for online communication data) located in the *C:\Program Files\MongoDB* folder. The settings in **System Settings > Database Backup & Archiving** apply to the SQL Server database only.



After completing Site Configuration, go to **System Settings > Failsafe Keys** to make backup resident keys.