



M1FE Installation Guide

Version 4.0



Index

• Requirements	3
Database Server	3
M1FE Server Components.....	4
Additional Requirements	5
Microsoft .Net Framework 4.0 or later	5
• 1. Microsoft SQL Server Installation	6
Login to the SQL Server.....	15
• 2. M1FE Tools.....	16
• 3. M1FE Message Server	24
• 4. M1FE Communication Server.....	31
• 5. M1FE Client	38
Connecting the M1FE Client	44
• 6. M1FE GPRS Server	45
• Server & Network Configuration	52
Communication Server.....	52
GPRS Server	59
Router Configuration	66
Testing Opened Ports.....	67
• M1FE Server Architecture	68
Single Server - Direct Connection.....	68
Single Server With Router.....	69
Multiple Servers	70
Cloud Servers	71



Requirements

Database Server

The Microsoft SQL Database can be installed on systems with the below system specifications for most Editions of SQL Server.

For detailed requirements for a specific version, you can check this [link \(https://docs.microsoft.com/en-us/sql/sql-server/install/hardware-and-software-requirements-for-installing-sql-server?view=sql-server-2014\)](https://docs.microsoft.com/en-us/sql/sql-server/install/hardware-and-software-requirements-for-installing-sql-server?view=sql-server-2014).

Component	Requirement
Processor	Type AMD Opteron, AMD Athlon 64, Intel Xeon with Intel EM64T support Intel Pentium IV with EM64T support, Intel Core Duo, Intel Core 2 Duo Intel i3, Intel i5, Intel i7 or later Speed Minimum: 1.4 Ghz Recommended: 2.5 GHz or faster
Operating System	Minimum: Windows 7 Recommended: Windows Server 2012 or later
Memory	Minimum: 2 GB Recommended: 4 GB
Hard Disk	Size: at least 40 GB



M1FE Server Components

The server components for M1FE, namely, Communication Server, Message Server and GPRS Server can be installed on another instance of server or on the same database server.

Component	Requirement
Processor	Type AMD Opteron, AMD Athlon 64, Intel Xeon with Intel EM64T support Intel Pentium IV with EM64T support, Intel Core Duo, Intel Core 2 Duo Intel i3, Intel i5, Intel i7 or later Speed Minimum: 1.4 Ghz Recommended: 2.5 GHz or faster
Operating System	Minimum: Windows 7 Recommended: Windows Server 2012 or later
Memory	2 GB or more
Hard Disk	Size: at least 50 MB of free disk space



Additional Requirements

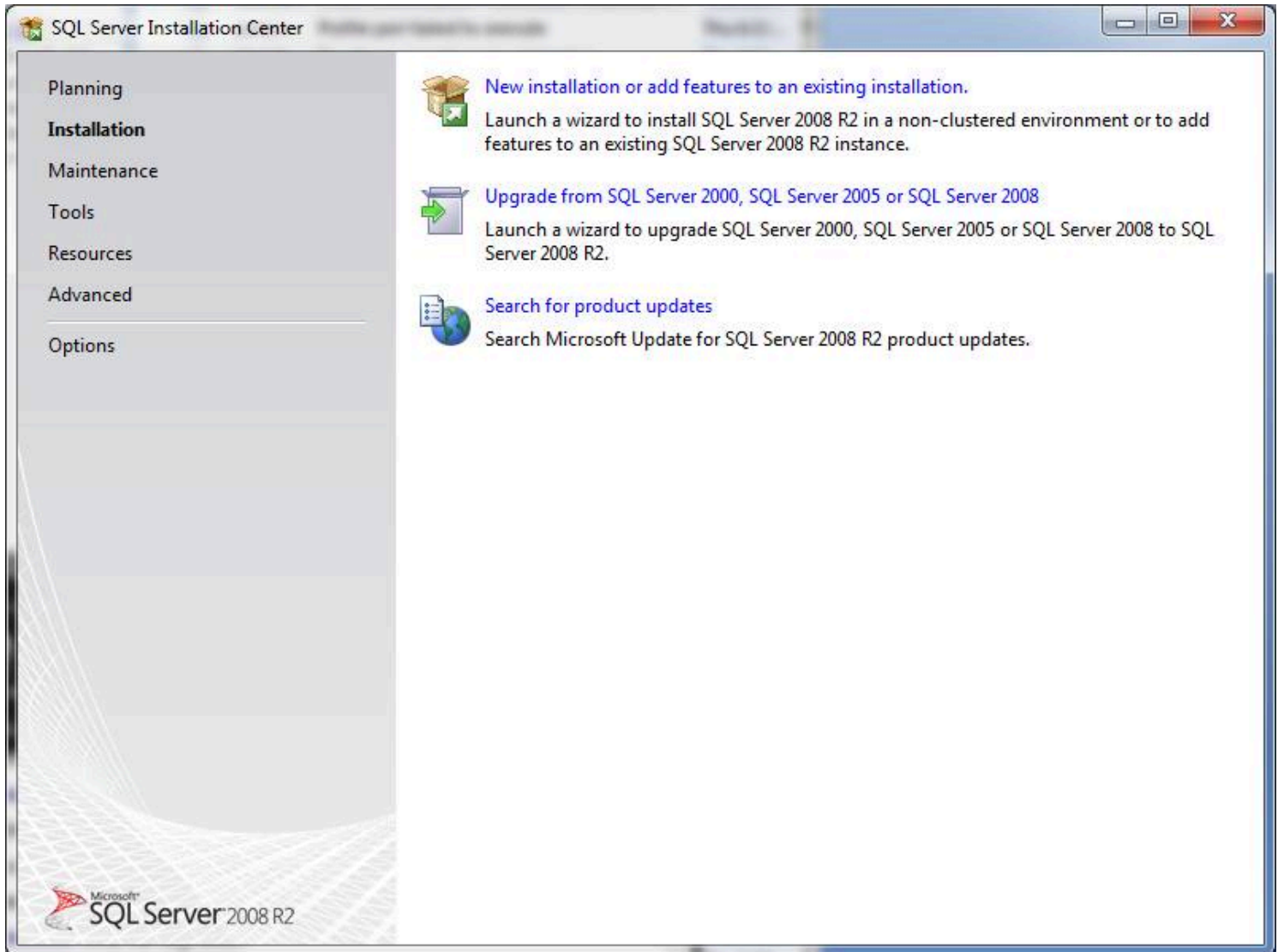
Microsoft .Net Framework 4.0 or later

Microsoft .Net Framework 4.0 or later versions can be downloaded from [Microsoft \(https://www.microsoft.com/en-us/download/search.aspx?q=.net%20framework\)](https://www.microsoft.com/en-us/download/search.aspx?q=.net%20framework).

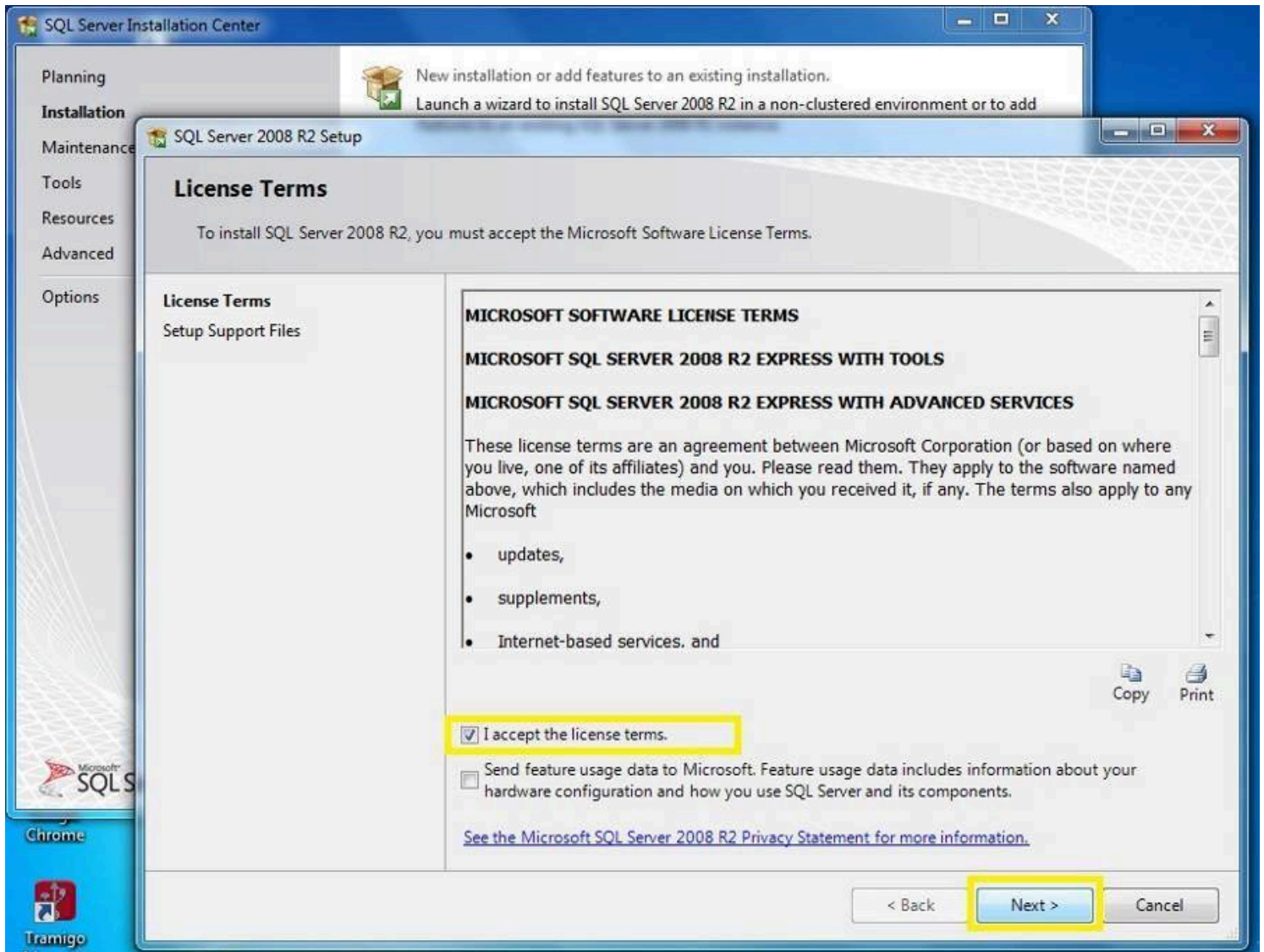


1. Microsoft SQL Server Installation

- Download the [Microsoft SQL Server](https://www.microsoft.com/en-ph/download/details.aspx?id=29062) (<https://www.microsoft.com/en-ph/download/details.aspx?id=29062>) with tools (SQLEXPRT) for your version of Windows.
- When download has finished, run the installer and select New installation or add features to existing installation, and accept the license agreement to proceed



Select New installation or add features to existing installation



Accept the License Agreement



- Microsoft SQL Server scans for Support Rules prior to installation. If all the rules are satisfied, click on Next.

SQL Server 2008 R2 Setup

Setup Support Rules

Setup Support Rules identify problems that might occur when you install SQL Server Setup support files. Failures must be corrected before Setup can continue.

Setup Support Rules

- Feature Selection
- Installation Rules
- Instance Configuration
- Disk Space Requirements
- Server Configuration
- Database Engine Configuration
- Error Reporting
- Installation Configuration Rules
- Installation Progress
- Complete

Rule check in progress...

Hide details << Re-run

Ru	Rule	Status
✓	Fusion Active Template Library (ATL)	Passed
✓	Unsupported SQL Server products	Passed
✓	Performance counter registry hive consistency	Passed
✓	Previous releases of SQL Server 2008 Business Intelligence Devel...	Passed
✓	Previous CTP installation	Passed
	Consistency validation for SQL Server registry keys	
	Computer domain controller	
	Microsoft .NET Application Security	
	Edition WOW64 platform	
	Windows PowerShell	
	Windows Firewall	

< Back Next > Cancel Help

Check each rule is satisfied and click Next

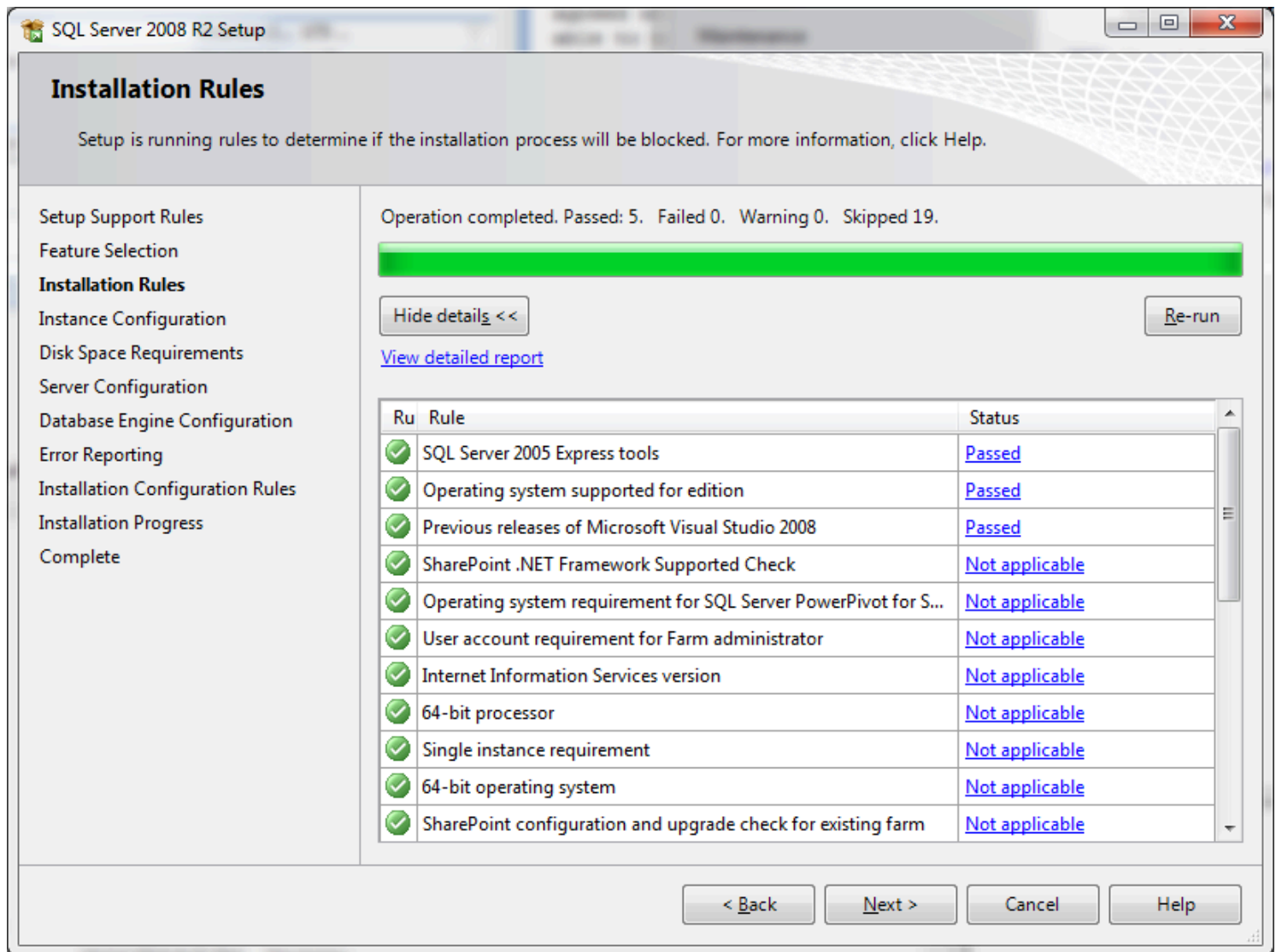


- On the Feature Selection, make sure to check the Database Engine Services, Management Tools and SQL Client Connectivity then click Next.

Put a check on Database Engine Services, Management Tools, and SQL Client Connectivity. Click Next.



- Another set of Installation Rules are scanned. Check that each is satisfied then click Next.



Check all rules are satisfied then click Next.



- On the Instance Configuration, select Default Instance then click Next.

SQL Server 2008 R2 Setup

Instance Configuration

Specify the name and instance ID for the instance of SQL Server. Instance ID becomes part of the installation path.

Setup Support Rules
Feature Selection
Installation Rules
Instance Configuration
Disk Space Requirements
Server Configuration
Database Engine Configuration
Error Reporting
Installation Configuration Rules
Installation Progress
Complete

☒ Default instance
☐ Named instance:

Instance ID:

Instance root directory: ...

SQL Server directory: C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER

Installed instances:

Instance Name	Instance ID	Features	Edition	Version
---------------	-------------	----------	---------	---------

< Back **Next >** Cancel Help

Select Default Instance and click Next



- On the Server Configuration, beside SQL Server Browser, change Startup Type to Automatic.

SQL Server 2008 R2 Setup

Server Configuration

Specify the service accounts and collation configuration.

Setup Support Rules
Feature Selection
Installation Rules
Instance Configuration
Disk Space Requirements
Server Configuration
Database Engine Configuration
Error Reporting
Installation Configuration Rules
Installation Progress
Complete

Service Accounts Collation

Microsoft recommends that you use a separate account for each SQL Server service.

Service	Account Name	Password	Startup Type
SQL Server Database Engine	NT AUTHORITY\NETWORK...		Automatic
SQL Server Browser	NT AUTHORITY\LOCAL S...		Automatic

Use the same account for all SQL Server services

< Back Next > Cancel Help

Beside SQL Server Browser, change Startup Type to Automatic



- On the Database Engine Configuration, choose Mixed Authentication and enter the password for SQL Server system administrator (sa) account. **Remember the password used for SA to be able to login as the system administrator.** Click also on Add Current User to add the current Windows User as administrator, if not yet added. Click Next.

SQL Server 2008 R2 Setup

Database Engine Configuration

Specify Database Engine authentication security mode, administrators and data directories.

Setup Support Rules
Feature Selection
Installation Rules
Instance Configuration
Disk Space Requirements
Server Configuration
Database Engine Configuration
Error Reporting
Installation Configuration Rules
Installation Progress
Complete

Account Provisioning | Data Directories | FILESTREAM

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

☐ Windows authentication mode

☒ **Mixed Mode (SQL Server authentication and Windows authentication)**

Specify the password for the SQL Server system administrator (sa) account.

Enter password:

Confirm password:

Specify SQL Server administrators

Tramigo-PC\Tramigo (Tramigo)

SQL Server administrators have unrestricted access to the Database Engine.

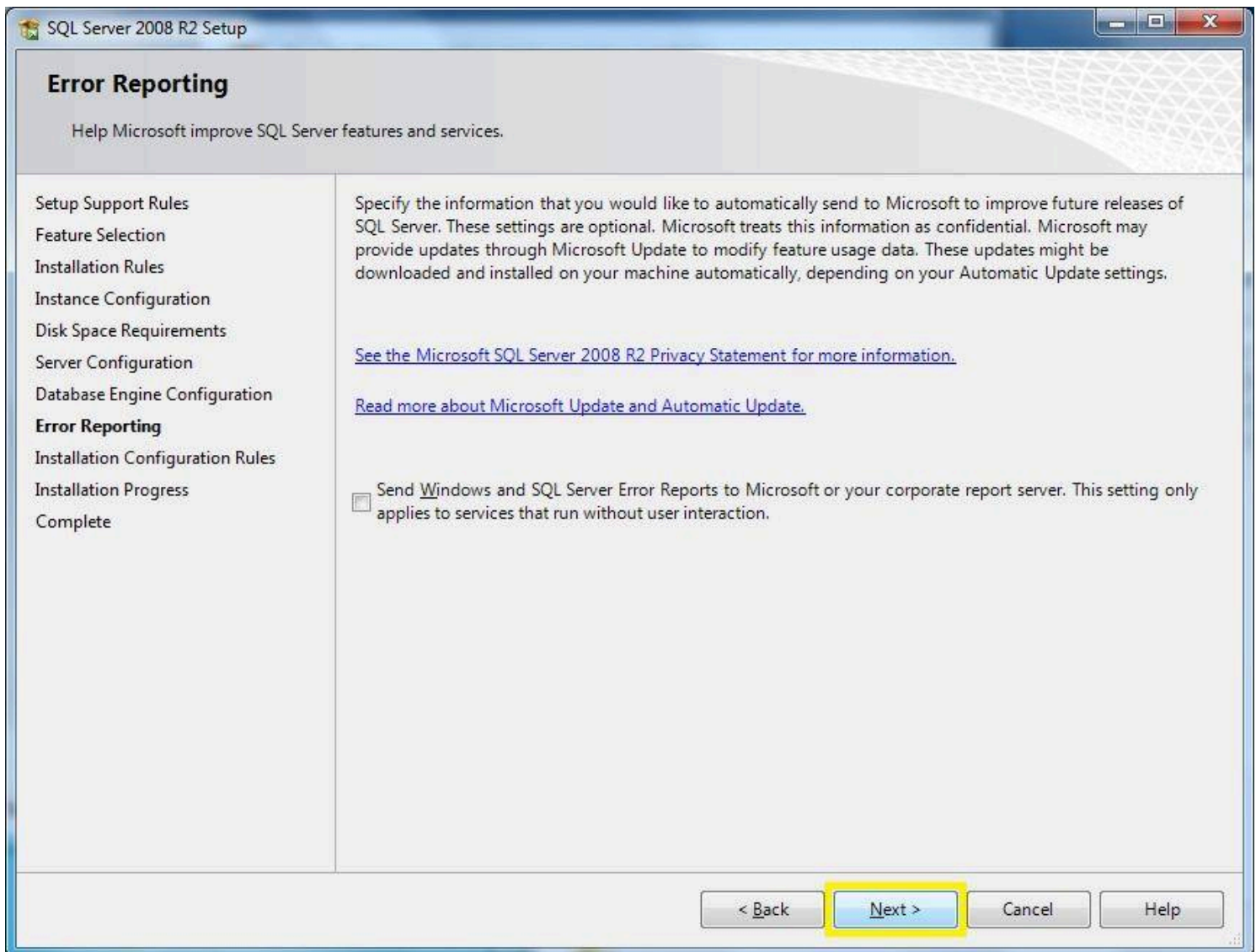
Add Current User | Add... | Remove

< Back | **Next >** | Cancel | Help

Choose Mixed Authentication, enter password for system administrator (sa) account, and click on Add Current User. Click Next.



- On Error Reporting, click Next and SQL Server should begin the installation.



Click Next and wait for installation to finish.



Login to the SQL Server

- You should now be able to login and check the newly installed database engine.
- Open SQL Server Management Studio or SSMS.
- On the login dialog of SSMS, you can use the values on the screenshot. Server name is (local). set Authentication to SQL Server Authentication, under Login, enter sa and on Password, enter the password set for SA during the installation.



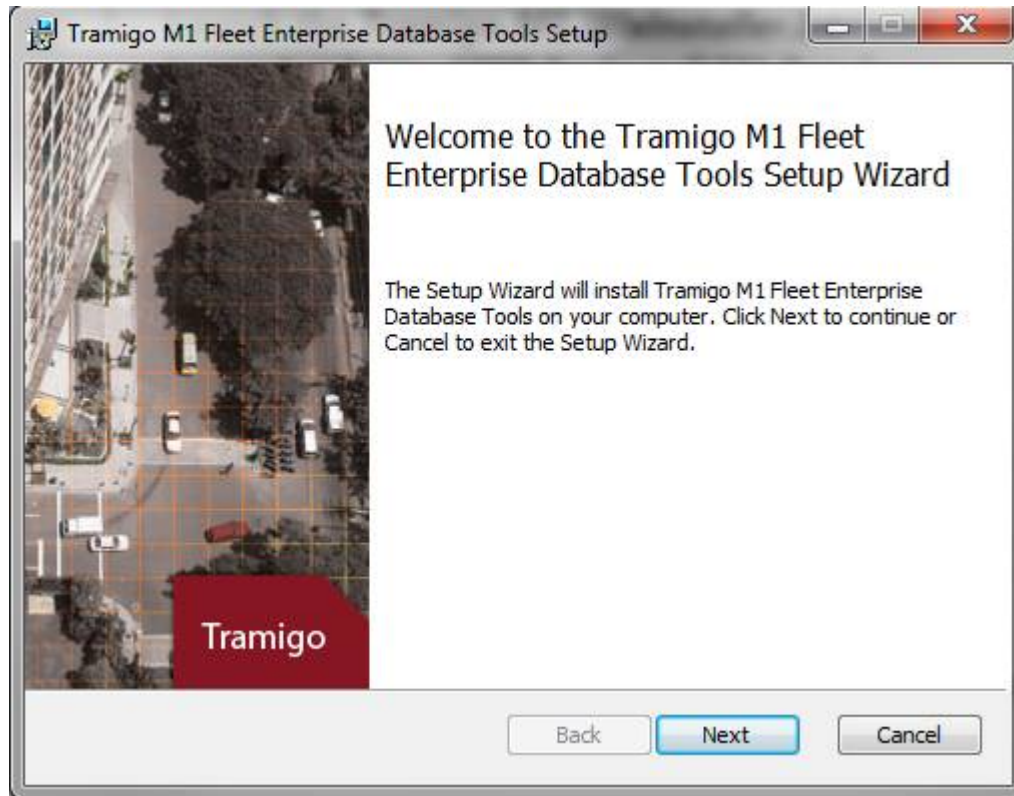
Login to SQL Server to check the installation.

- SQL Server should be working correctly if you are able to login.



2. M1FE Tools

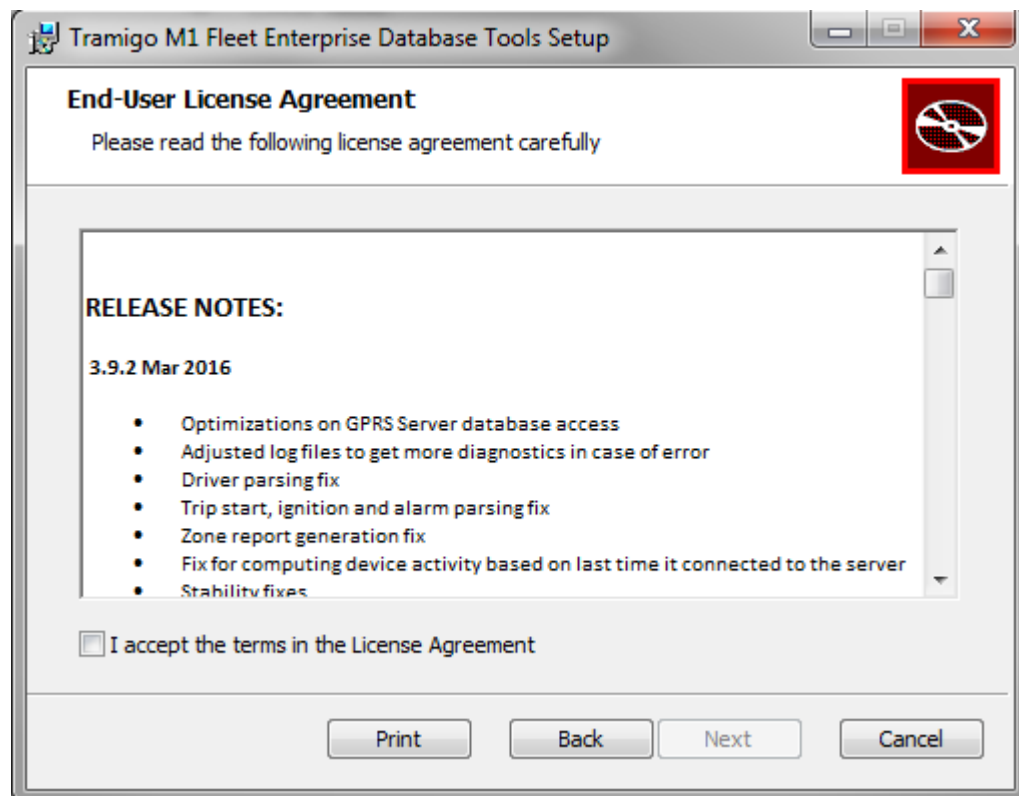
- Launch the M1FE Tools Installer (Tramigo.M1.WixInstaller.DBTools.msi) and run the installation. Click Next.



Open M1FE Tools Installer and click Next.



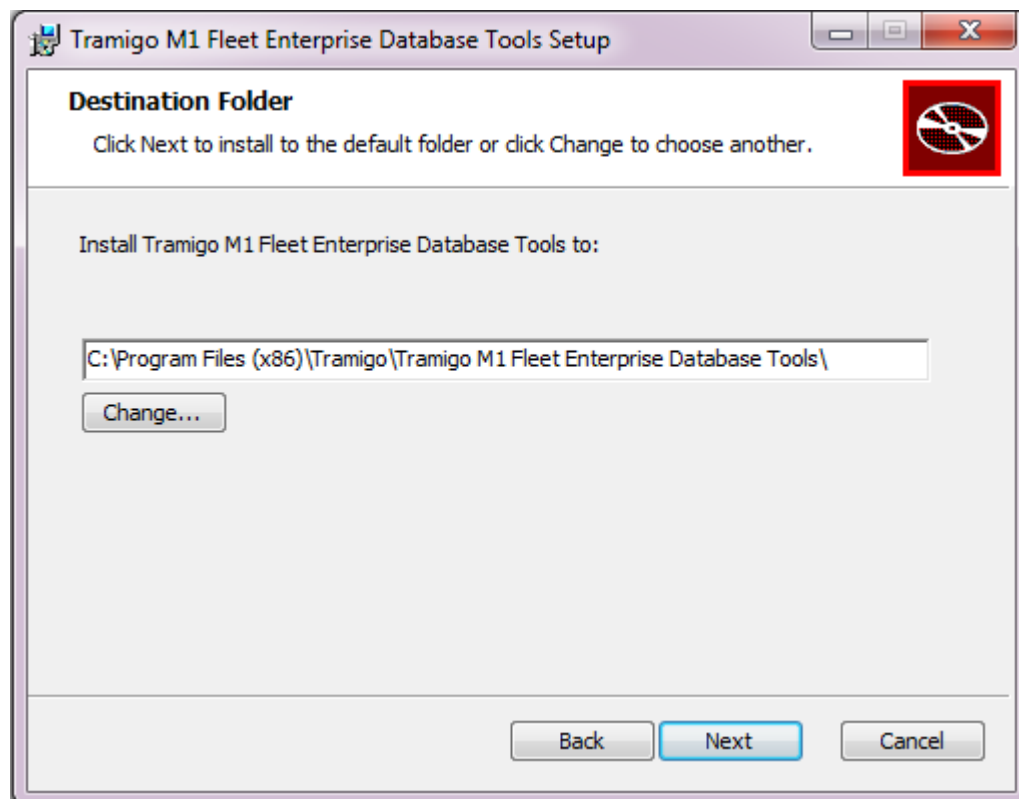
- Accept the End User License Agreement and click Next.



Accept the End User License Agreement and click Next.



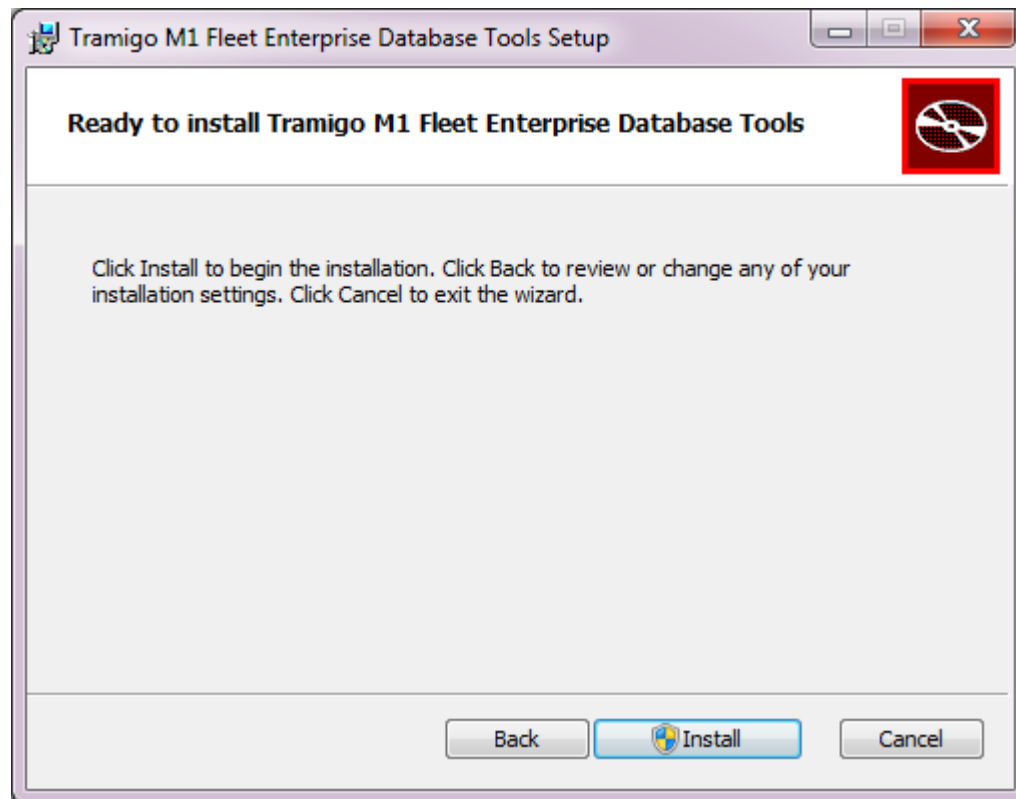
- Select the installation directory and click Next.



Select the installation directory and click Next.



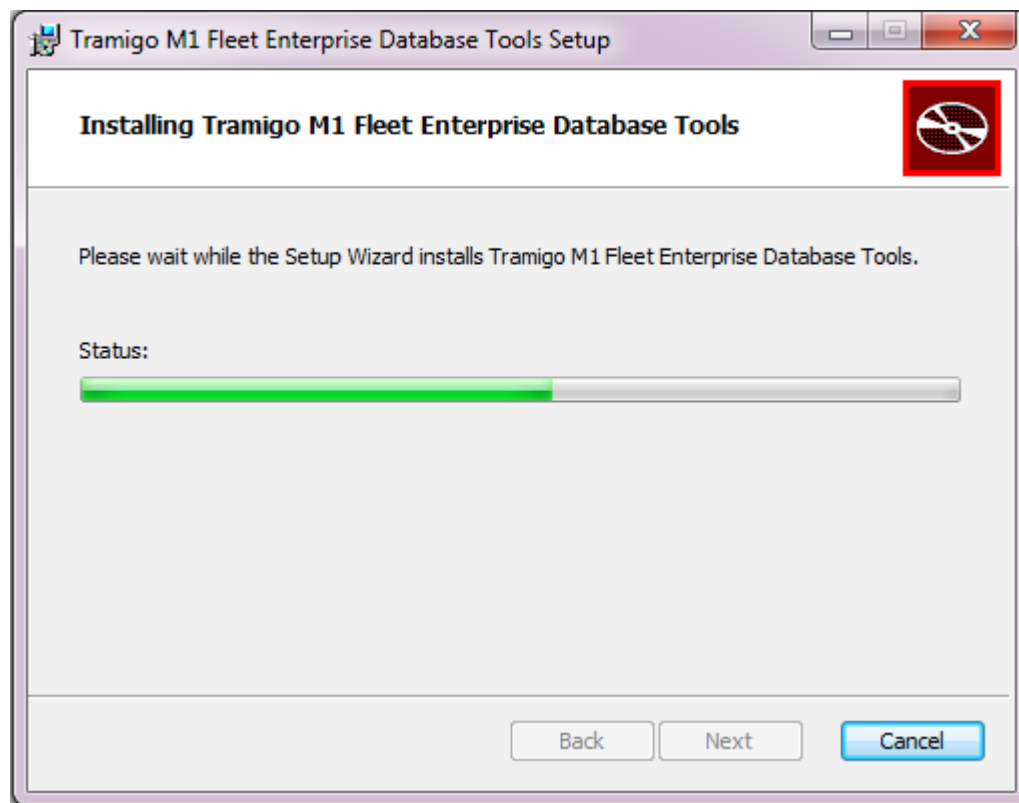
- Click on Install to begin the installation.



Click on Install.



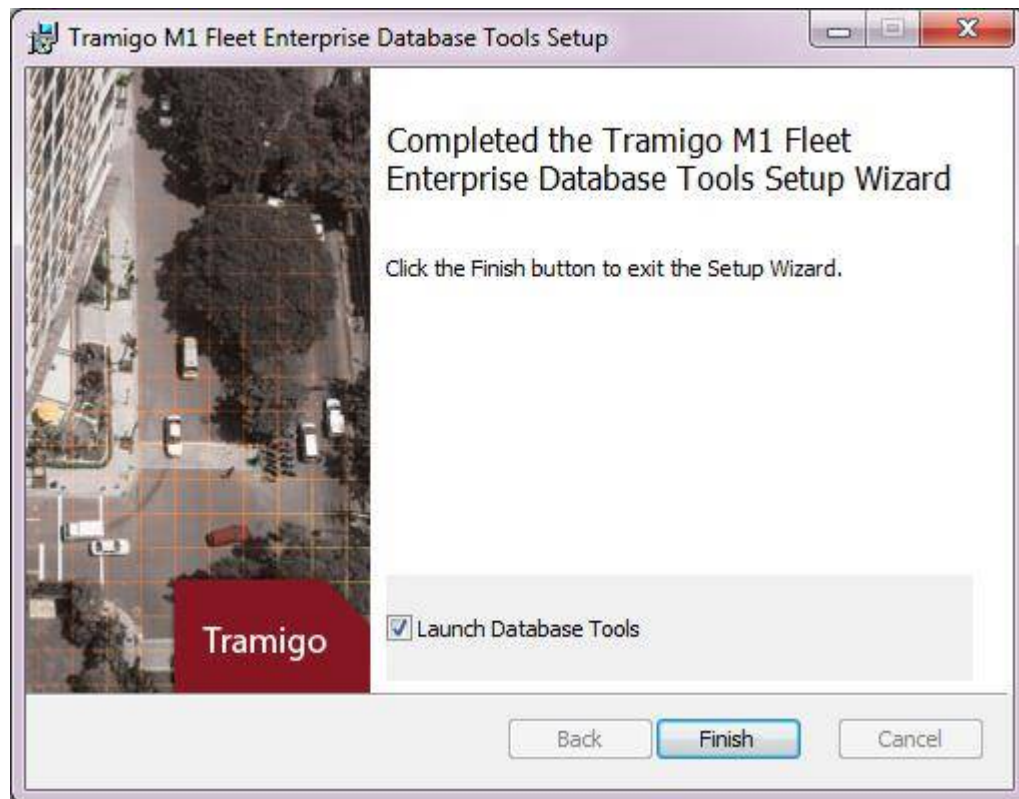
- Wait for the installation to finish.



Wait for the installation to finish.



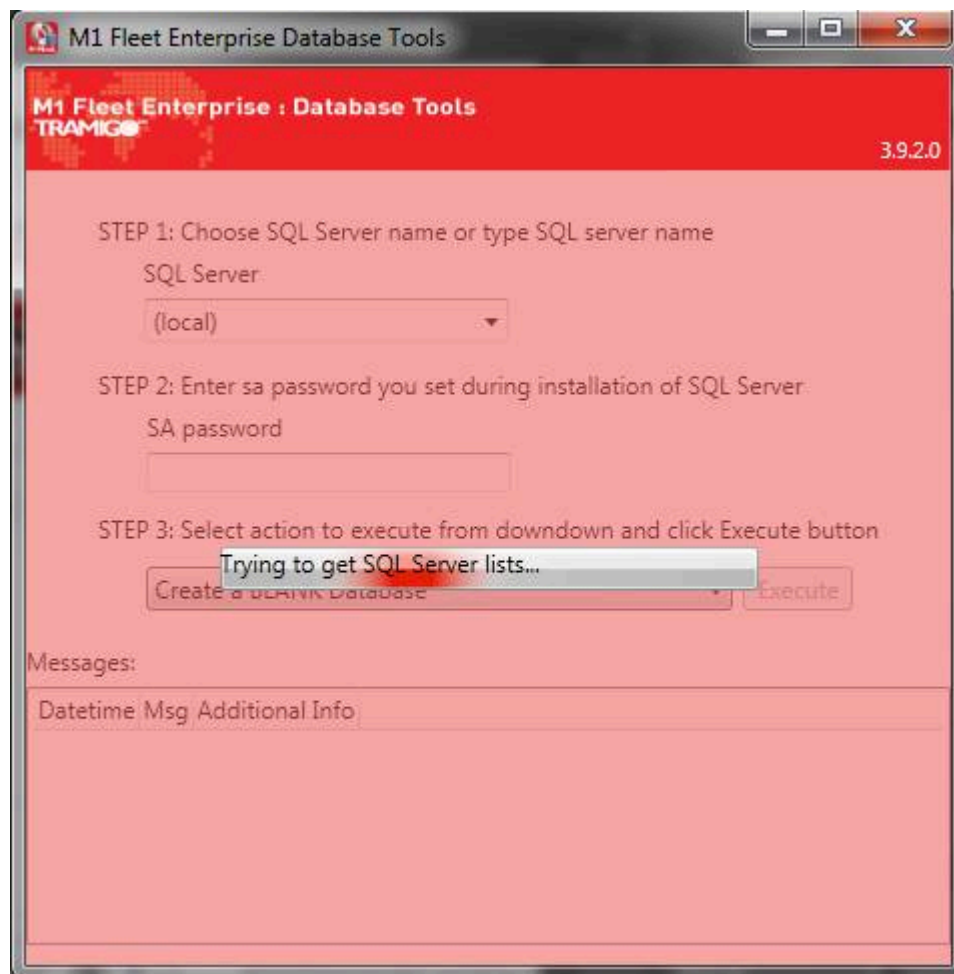
- Click on Finish to exit the installation.



Click on Finish.



- Launch M1FE Tools



Launch M1FE Tools.



- For new installation, make sure to create first the database before proceeding.
 - Set the SQL Server to point to the correct server if located on a different server.
 - Enter the SA password or use Windows Authentication.
 - Make sure Create a BLANK Database is selected on the dropdown box.
 - Click on Execute.

The screenshot shows the 'M1 Fleet Enterprise Database Tools' window. The title bar says 'M1 Fleet Enterprise Database Tools'. The window has a red header with 'M1 Fleet Enterprise : Database Tools' and 'TRAMIGO' logo on the left, and '3.9.2.0' on the right. The main area contains three steps:

STEP 1: Choose SQL Server name or type SQL server name
SQL Server
(local) ▼

STEP 2: Enter sa password you set during installation of SQL Server
SA password

STEP 3: Select action to execute from dropdown and click Execute button
Create a BLANK Database ▼

Messages:

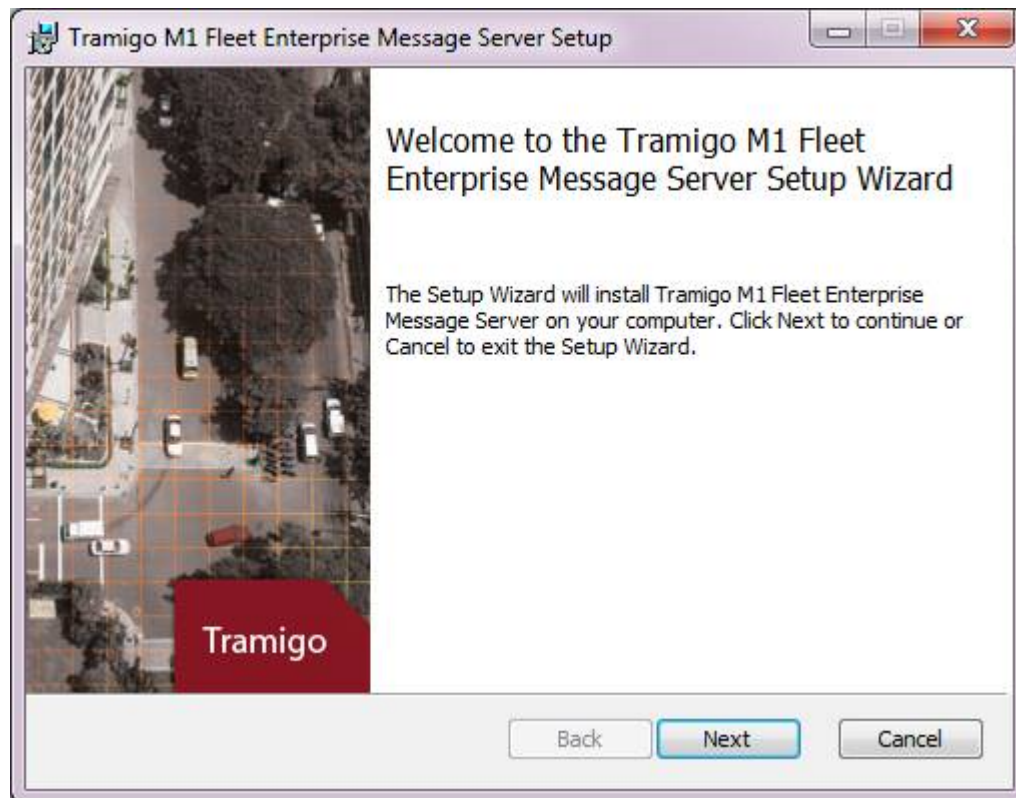
Datetime	Msg	Additional Info
3/22/2013 4:39:16 PM	Create database command started.	
3/22/2013 4:39:16 PM	Trying connection...	
3/22/2013 4:39:16 PM	Connection OK.	
3/22/2013 4:39:16 PM	Start creating database...	
3/22/2013 4:39:20 PM	Newly created database connection testing success.	
3/22/2013 4:39:20 PM	Successfully created M1 Fleet Enterprise Database	

Create the database.



3. M1FE Message Server

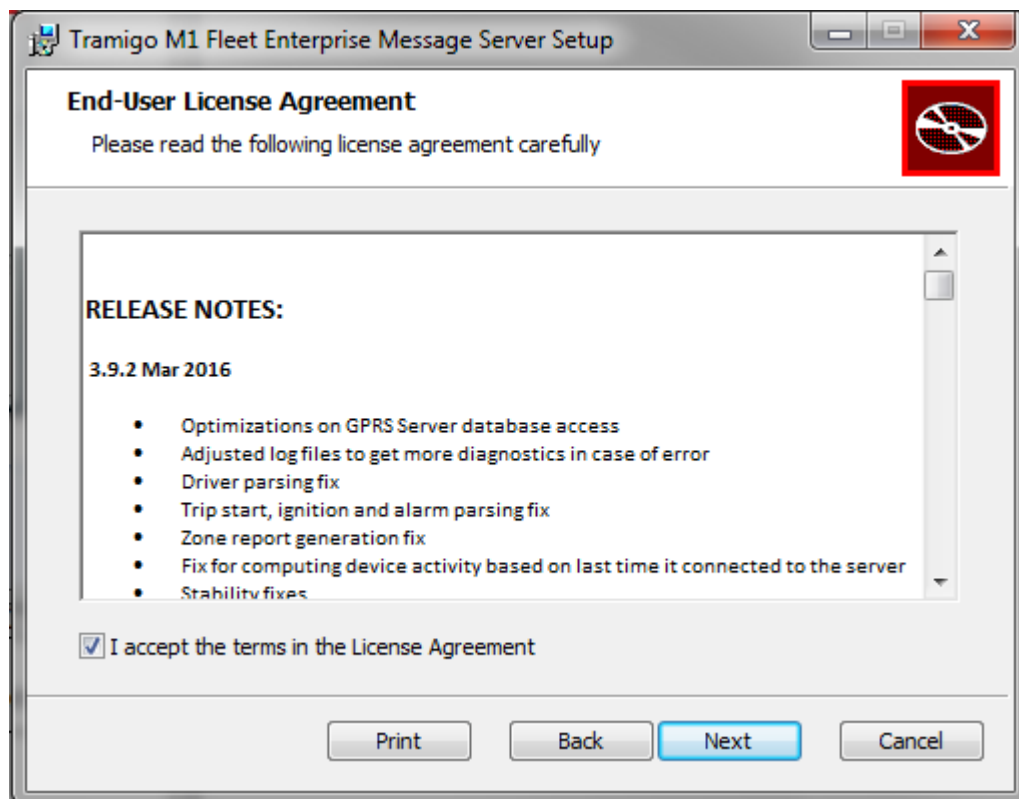
- Install the Message Server Component by launching the installer (Tramigo.M1.Installers.MessageServer.msi)



Open Message Server Installer



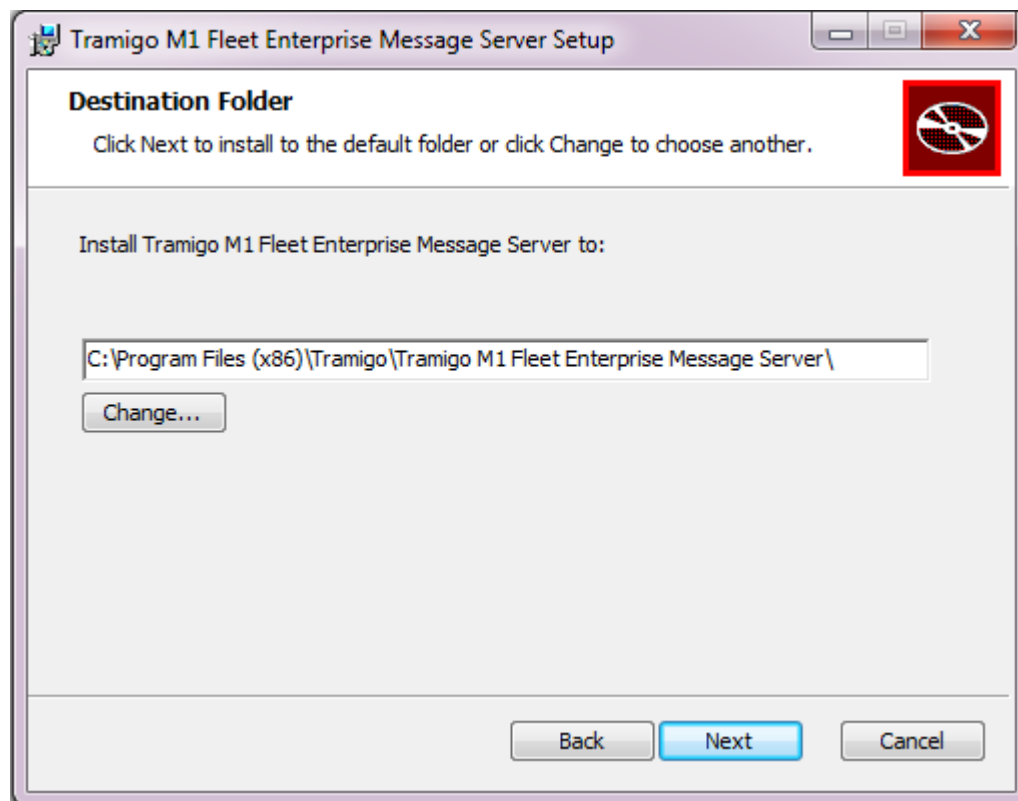
- Accept the End User License Agreement and click Next.



Accept the End User License Agreement and click Next.



- Select the installation directory and click Next.



Select the installation directory and click Next.



- Enter the SQL Server location if it's on a different server.

Database server connection

Configure SQL server connection

Enter SQL Server where GPRS Server will connect to.

SQL Server name

(local)

Note:

Enter (local) if the SQL Server is the same where you are installing Message

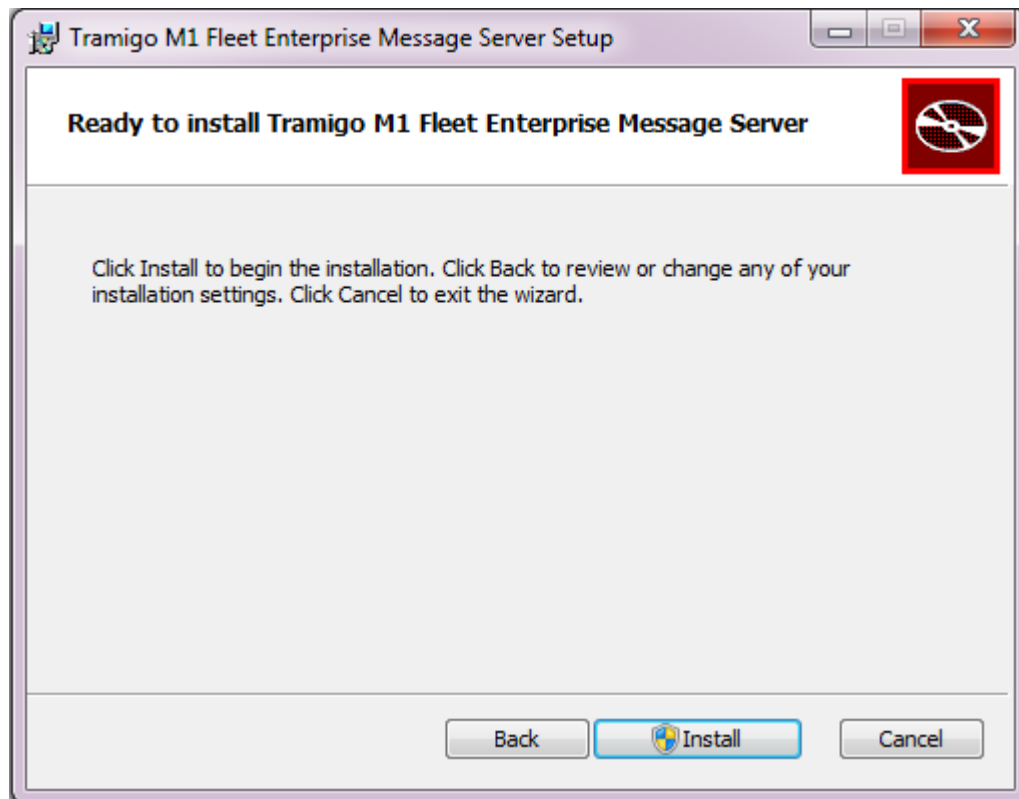
Enter IP Address or SQL Server name of the database server is in a remote machine.

Back Next Cancel

Enter the SQL Server location



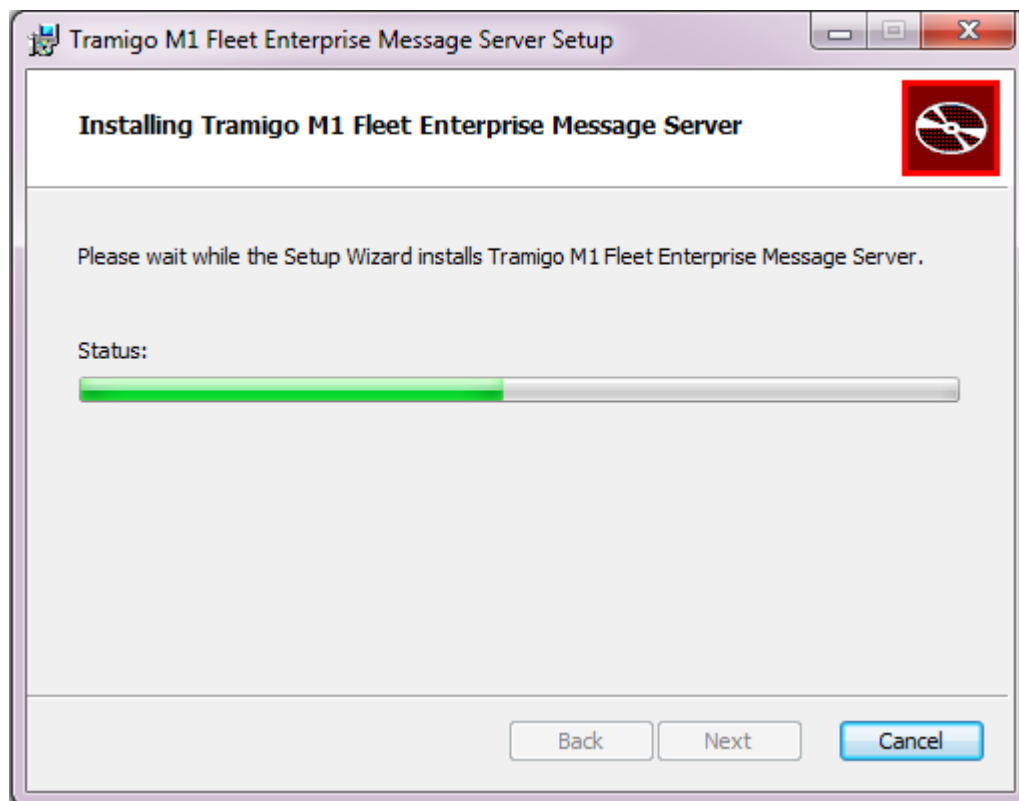
- Click on Install to begin the installation.



Click on Install.



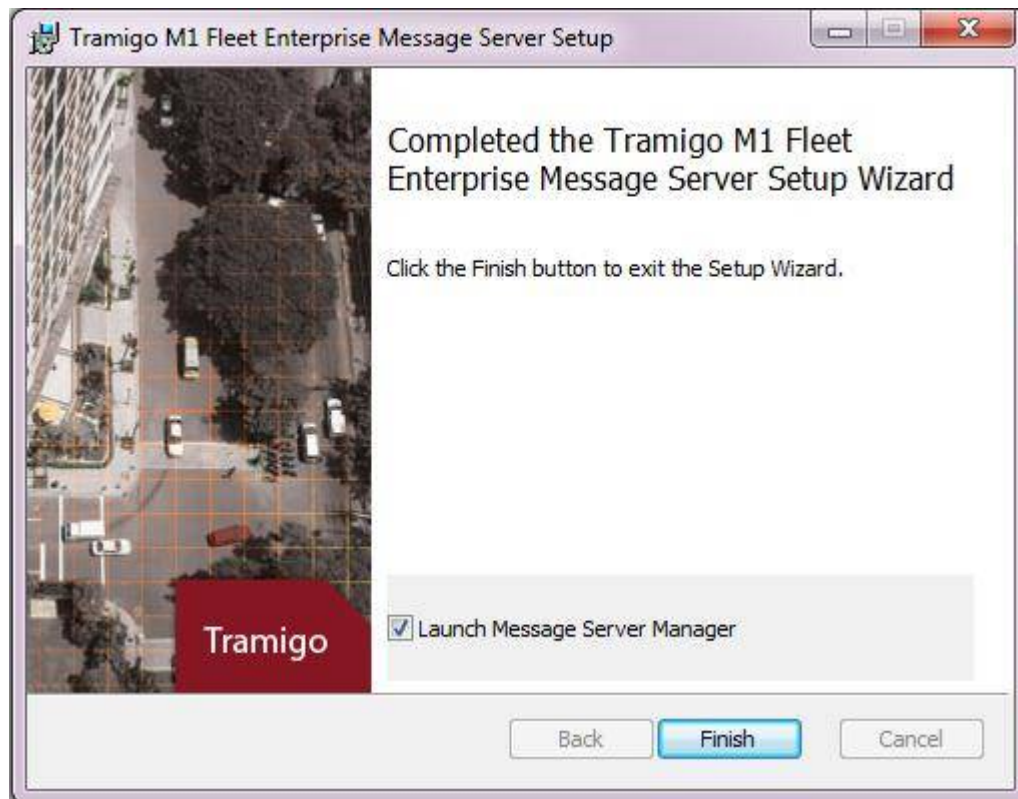
- Wait for the installation to finish.



Wait for the installation to finish.



- Click on **Finish** to exit the installation.

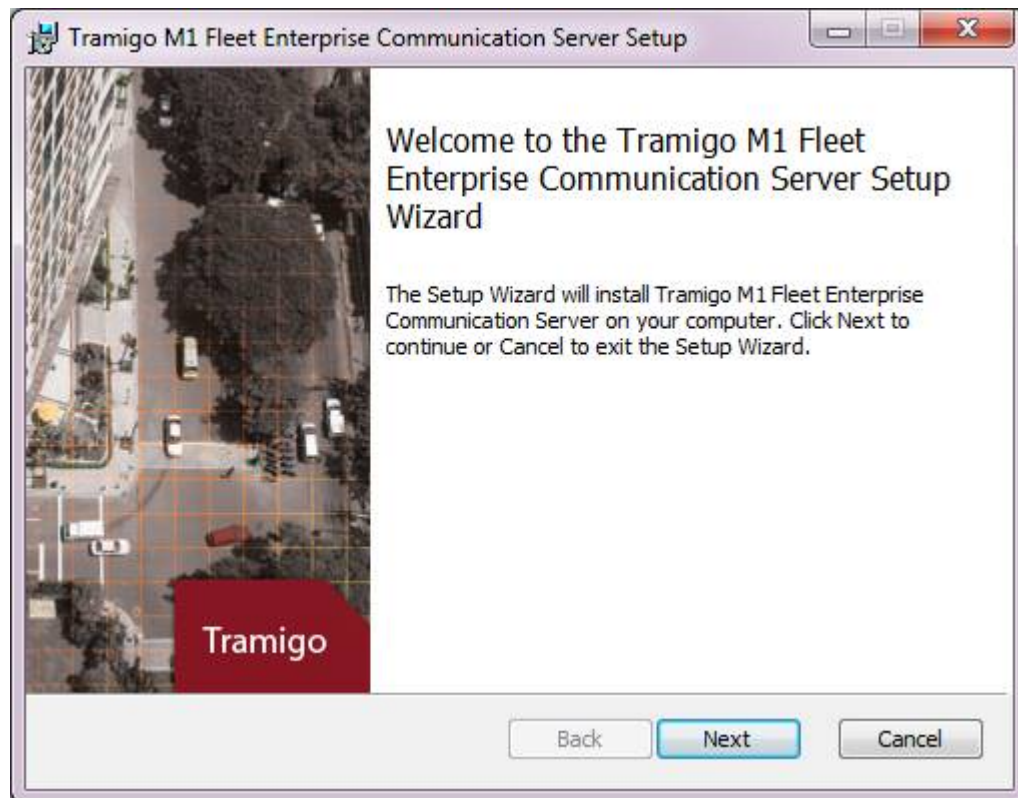


Click on **Finish**.



4. M1FE Communication Server

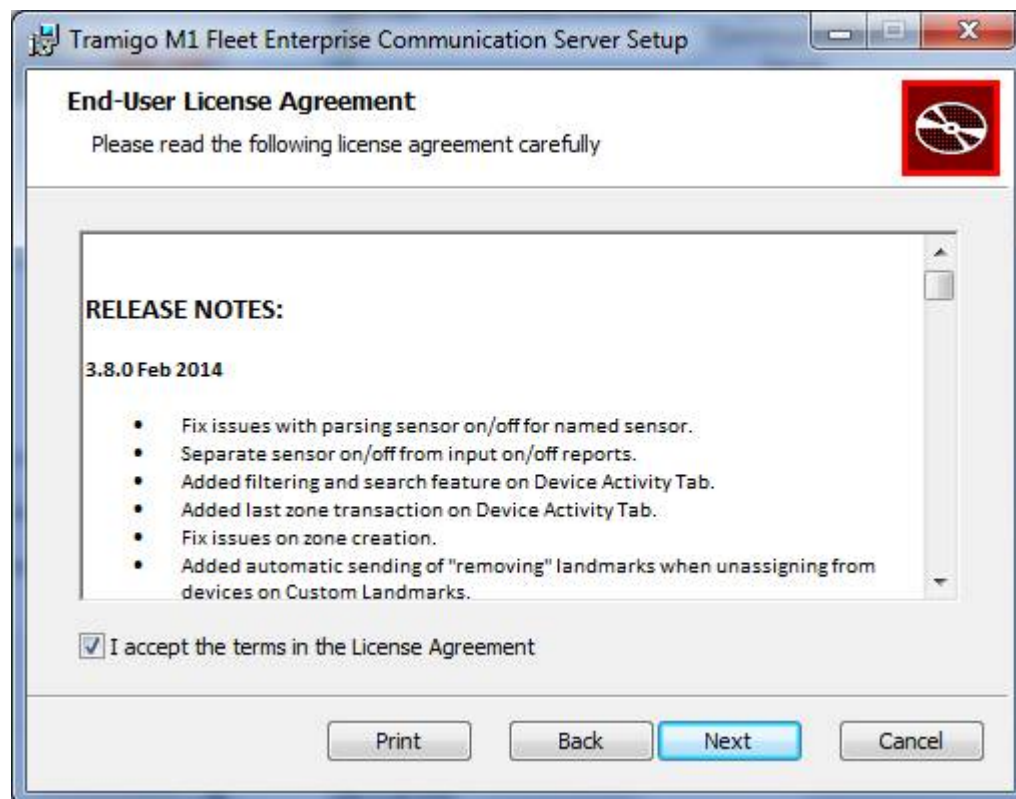
- Install the Communication Server component by launching the installer (Tramigo.M1.Installers.CommunicationServer.msi)



Open Communication Server Installer



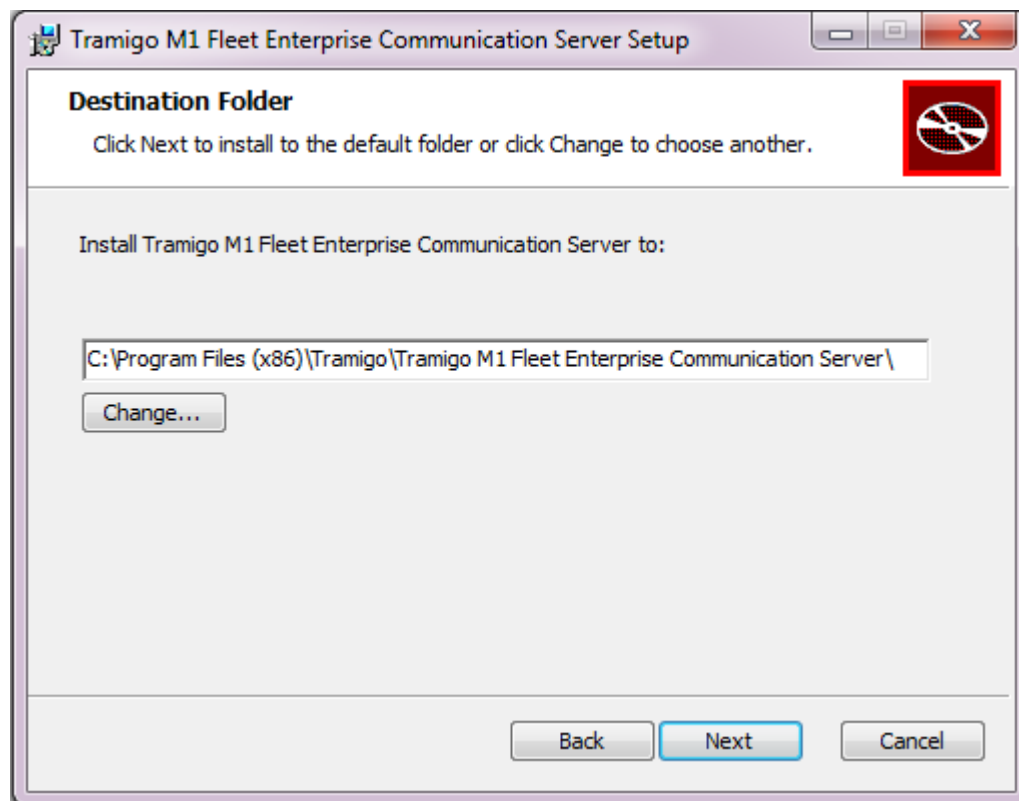
- Accept the End User License Agreement and click Next.



Accept the End User License Agreement and click Next.



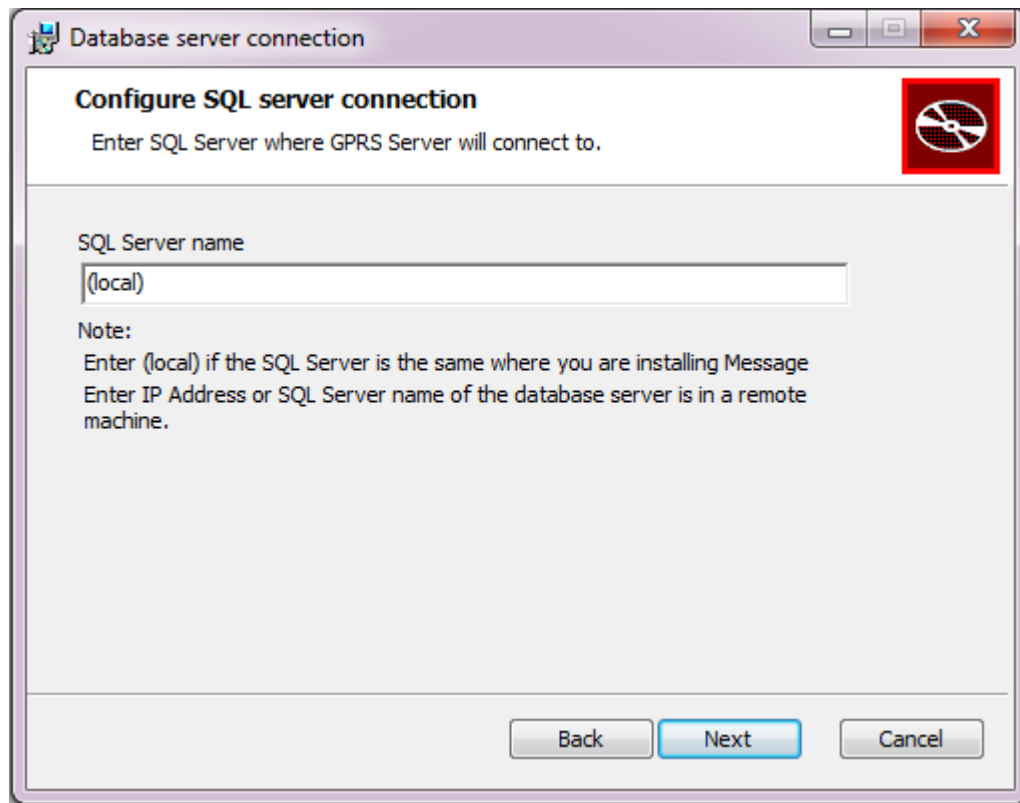
- Select the installation directory and click Next.



Select the installation directory and click Next.



- Enter the SQL Server location if it's on a different server.

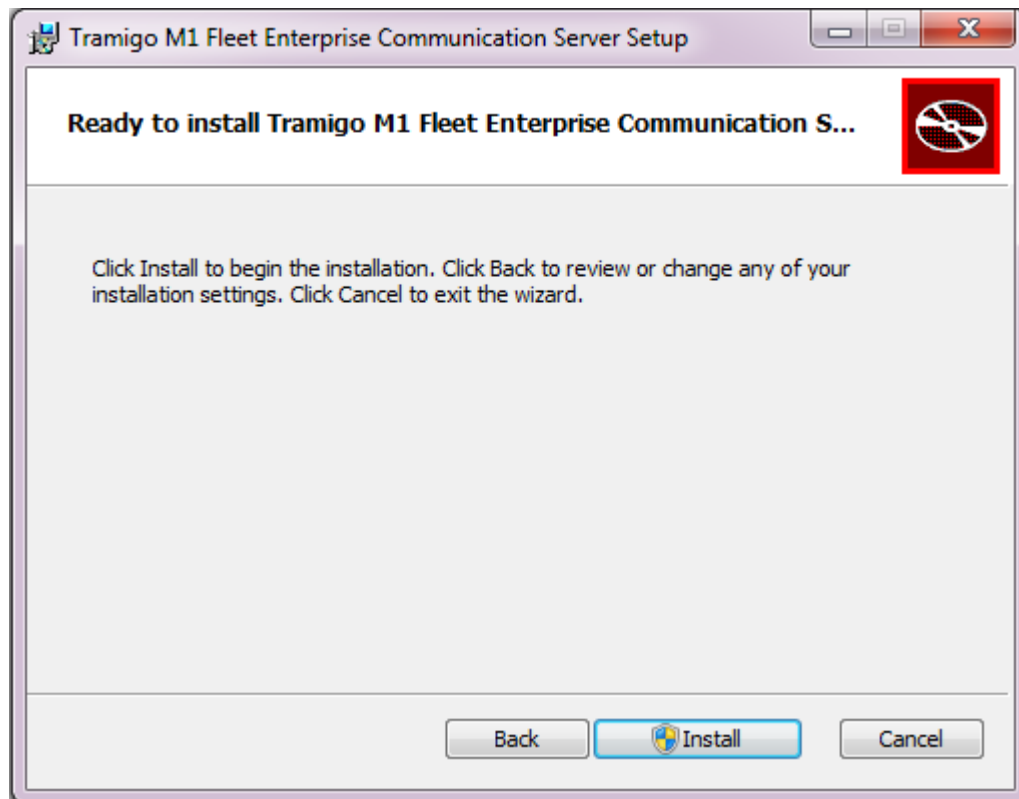


The screenshot shows a Windows-style dialog box titled "Database server connection". Inside, there's a section titled "Configure SQL server connection" with a red icon of a hard drive. Below the title, it says "Enter SQL Server where GPRS Server will connect to.". There is a text input field labeled "SQL Server name" containing the text "(local)". Below the input field, there is a "Note:" section with the following text: "Enter (local) if the SQL Server is the same where you are installing Message" and "Enter IP Address or SQL Server name of the database server is in a remote machine.". At the bottom right, there are three buttons: "Back", "Next" (which is highlighted in blue), and "Cancel".

Enter the SQL Server location



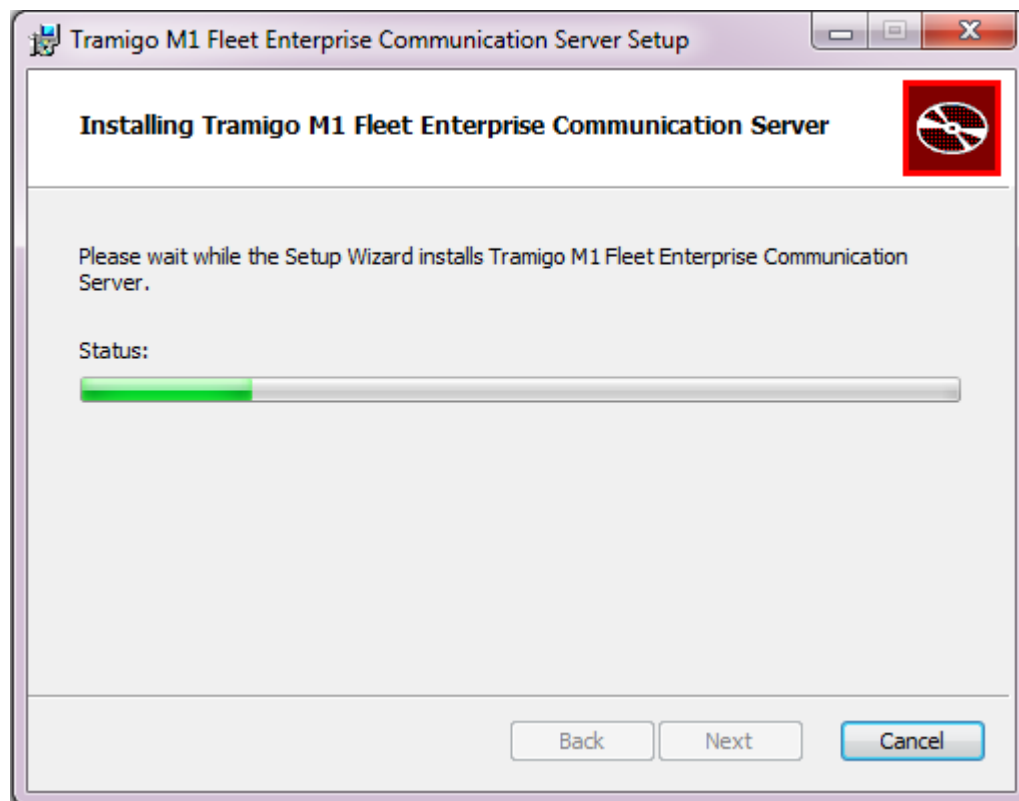
- Click on Install to begin the installation.



Click on Install.



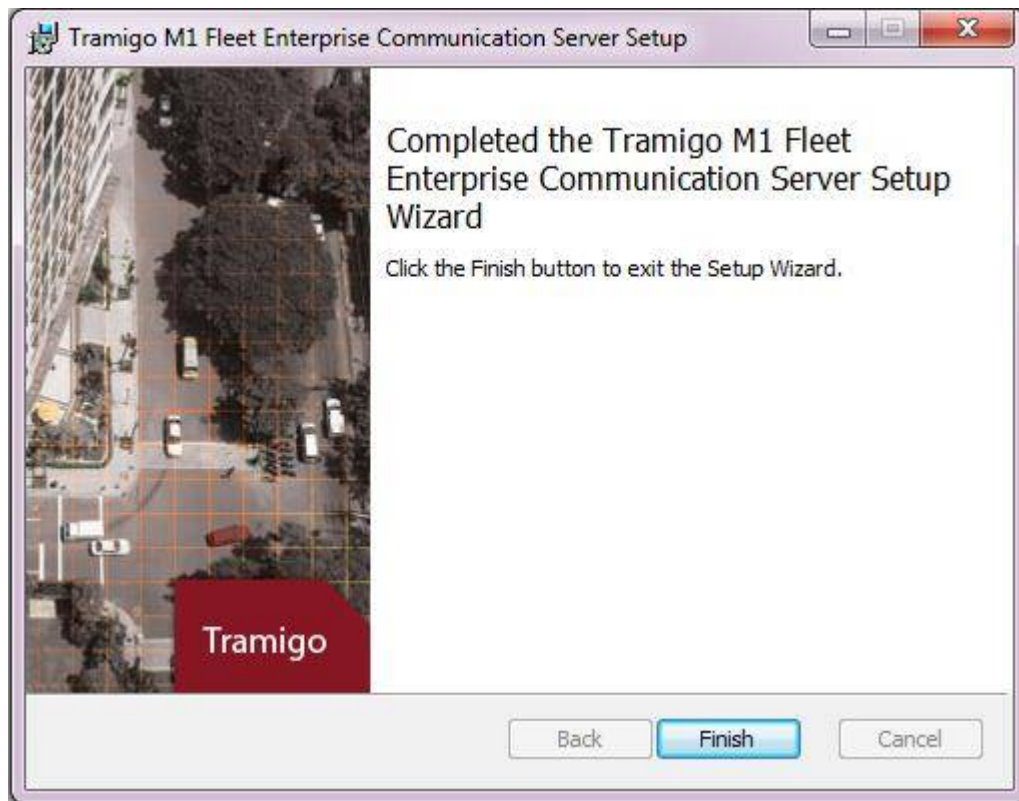
- Wait for the installation to finish.



Wait for the installation to finish.



- Click on **Finish** to exit the installation.



Click on **Finish**.



5. M1FE Client

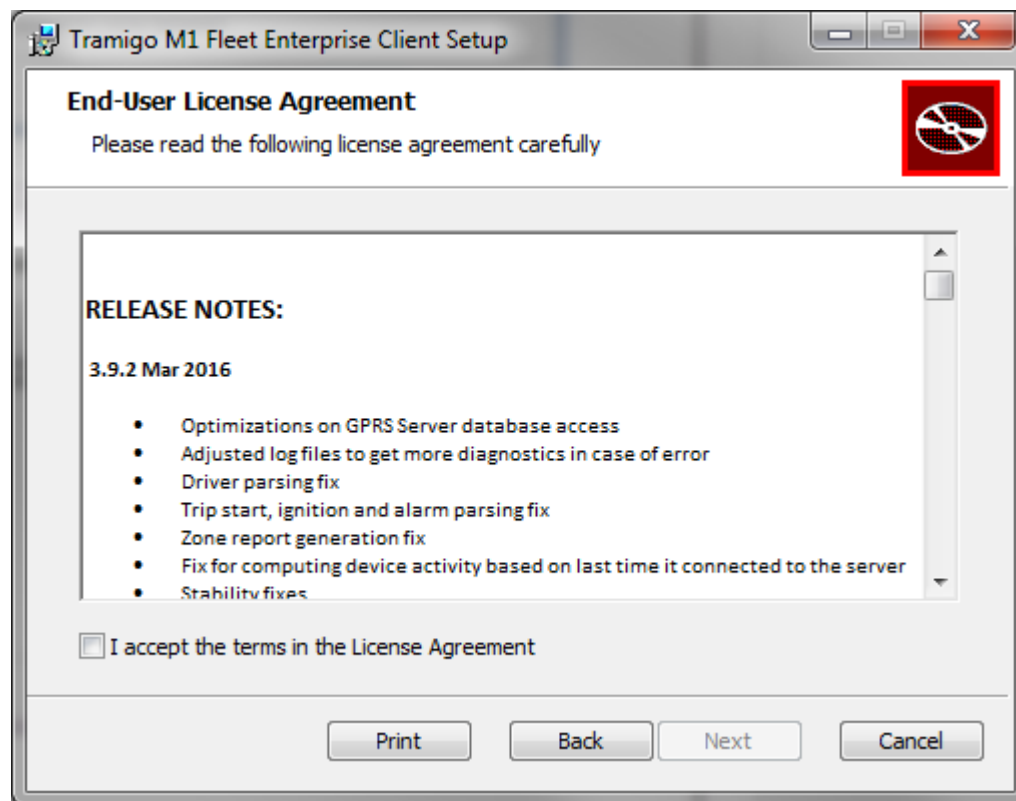
- Install the Client Component by launching the installer (Tramigo.M1.Installers.WinClient.msi)



Open M1FE Client Installer



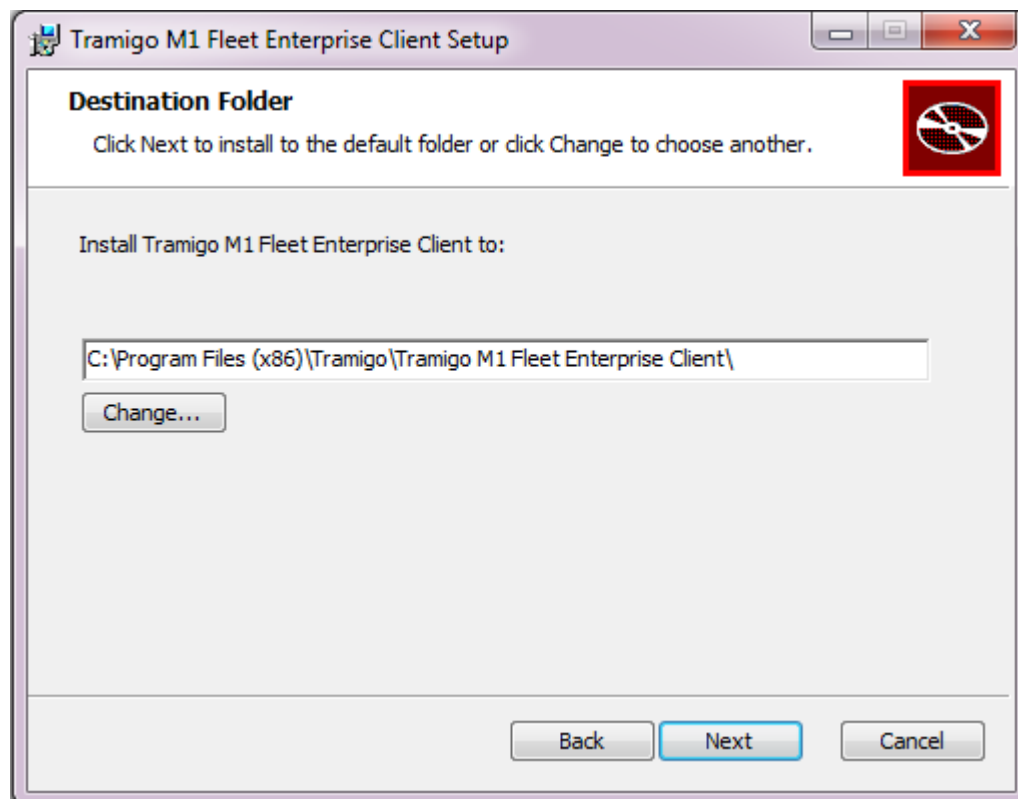
- Accept the End User License Agreement and click Next.



Accept the End User License Agreement and click Next.



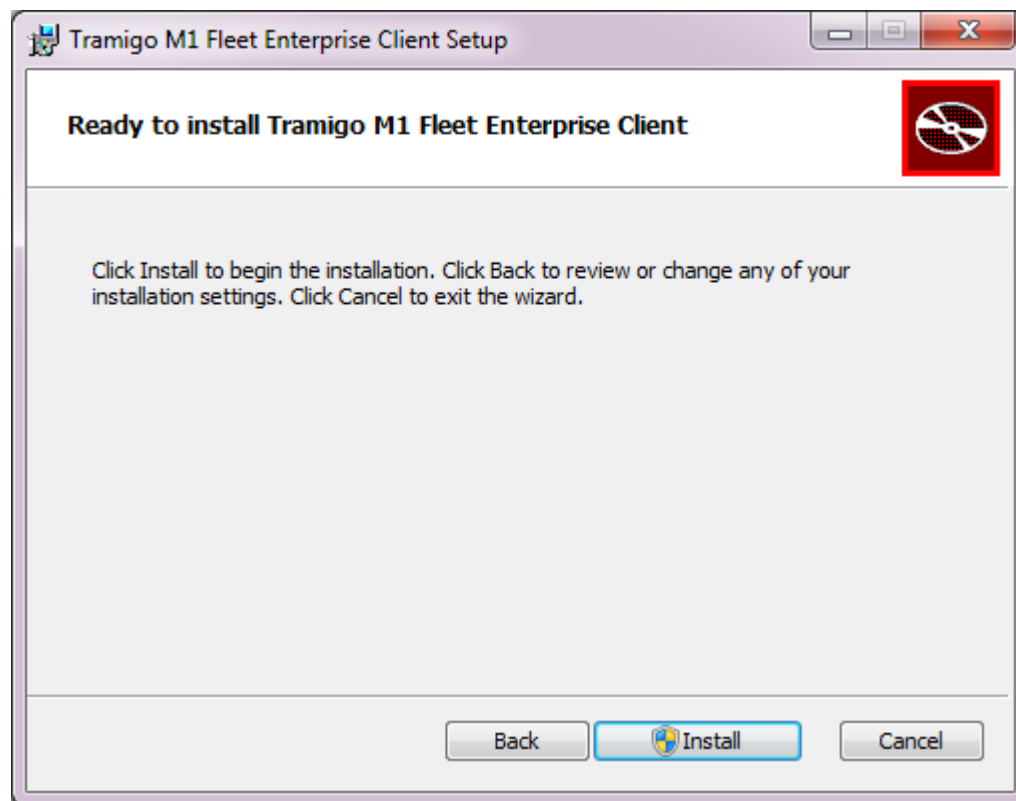
- Select the installation directory and click Next.



Select the installation directory and click Next.



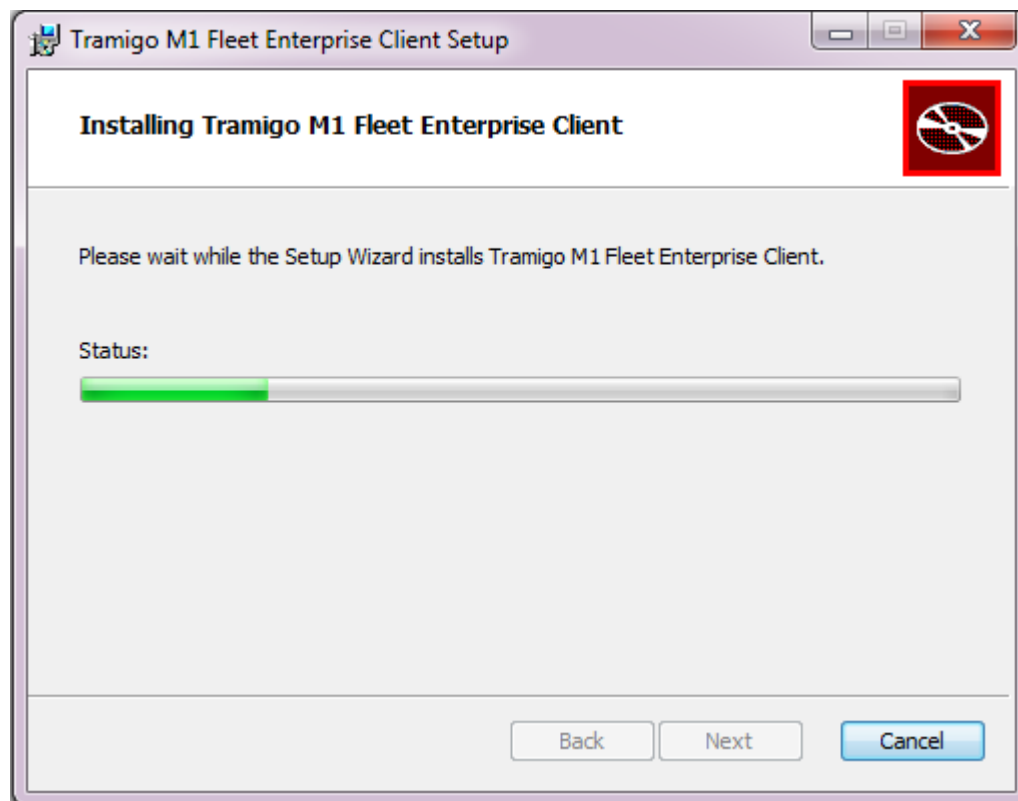
- Click on Install to begin the installation.



Click on Install.



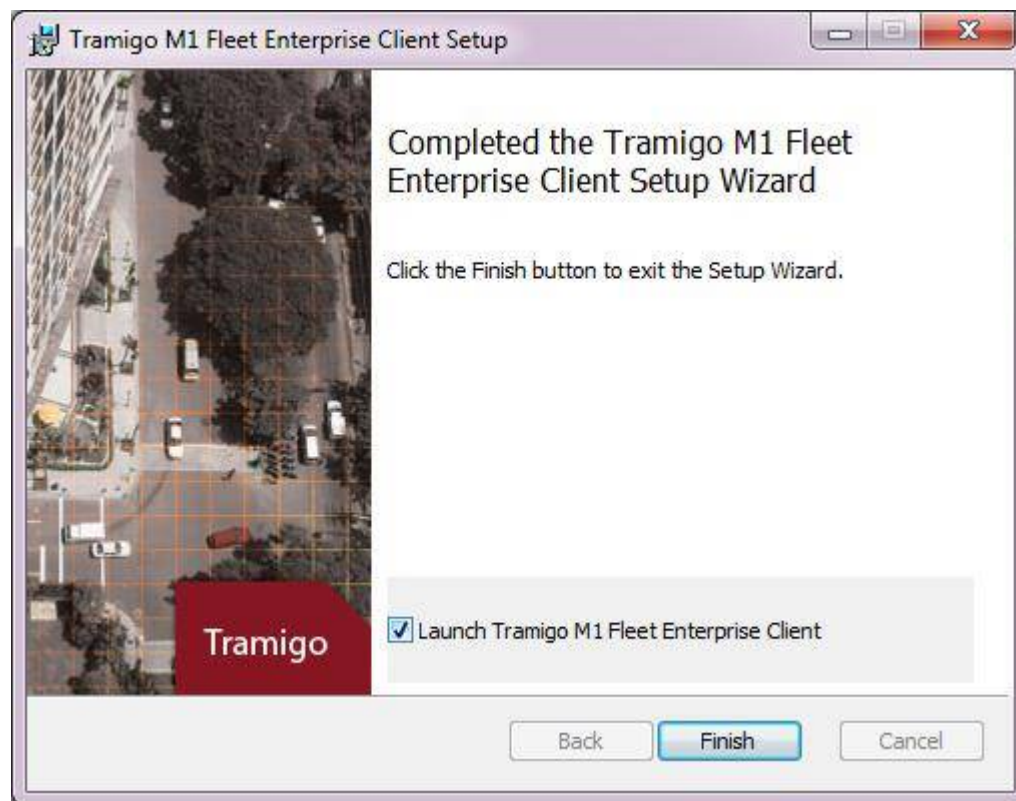
- Wait for the installation to finish.



Wait for the installation to finish.



- Click on **Finish** to exit the installation.



Click on **Finish**.



Connecting the M1FE Client

- You can now open M1FE Client and try logging in.
You can use the default **username: admin** and **password: admin** to login for new installations.

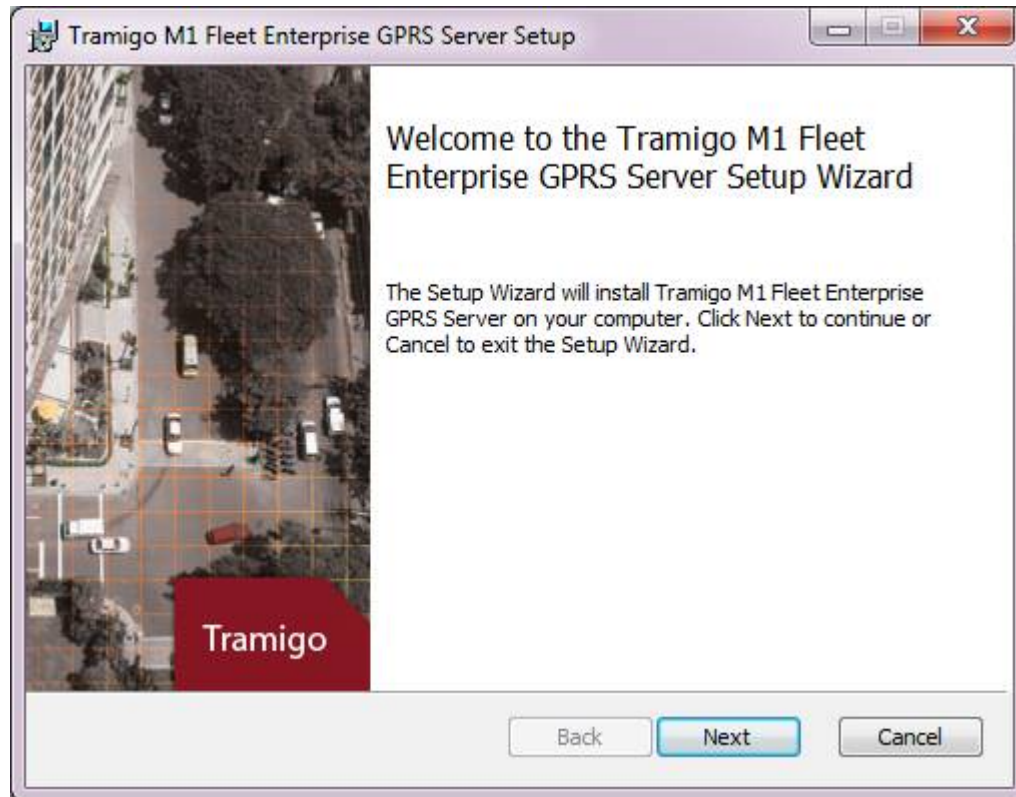


Login to M1FE



6. M1FE GPRS Server

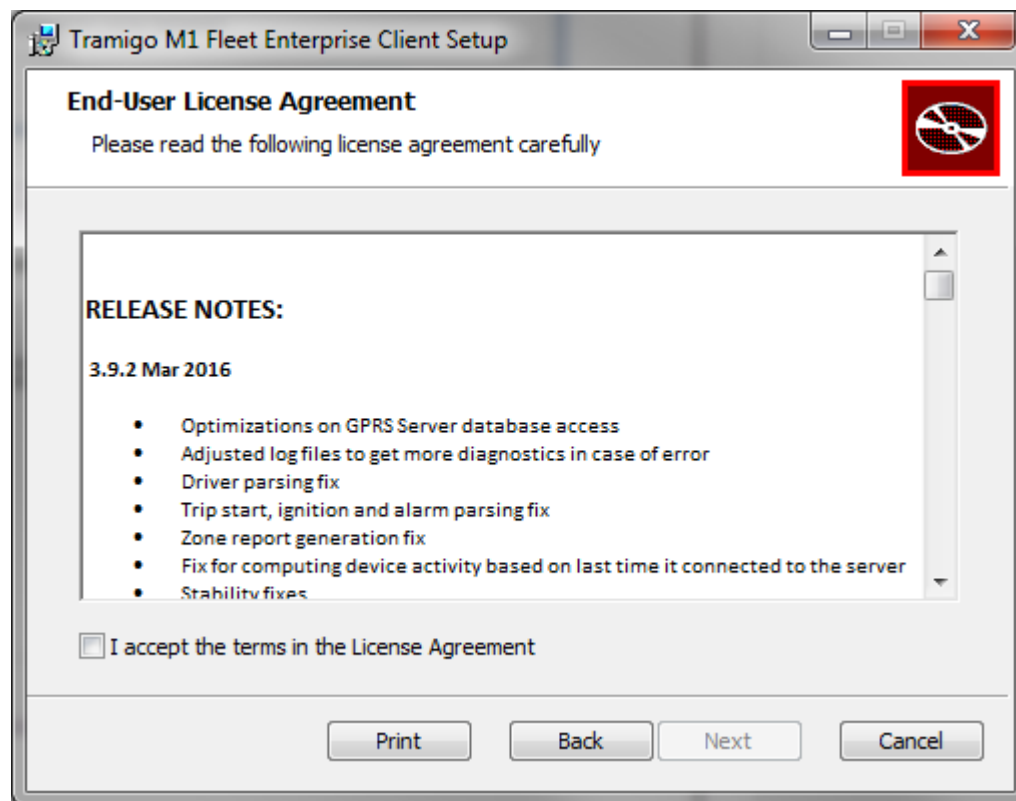
- Install the GPRS Server component by launching the installer (Tramigo.M1.Installer.GPRSServer)



Open GPRS Server Installer



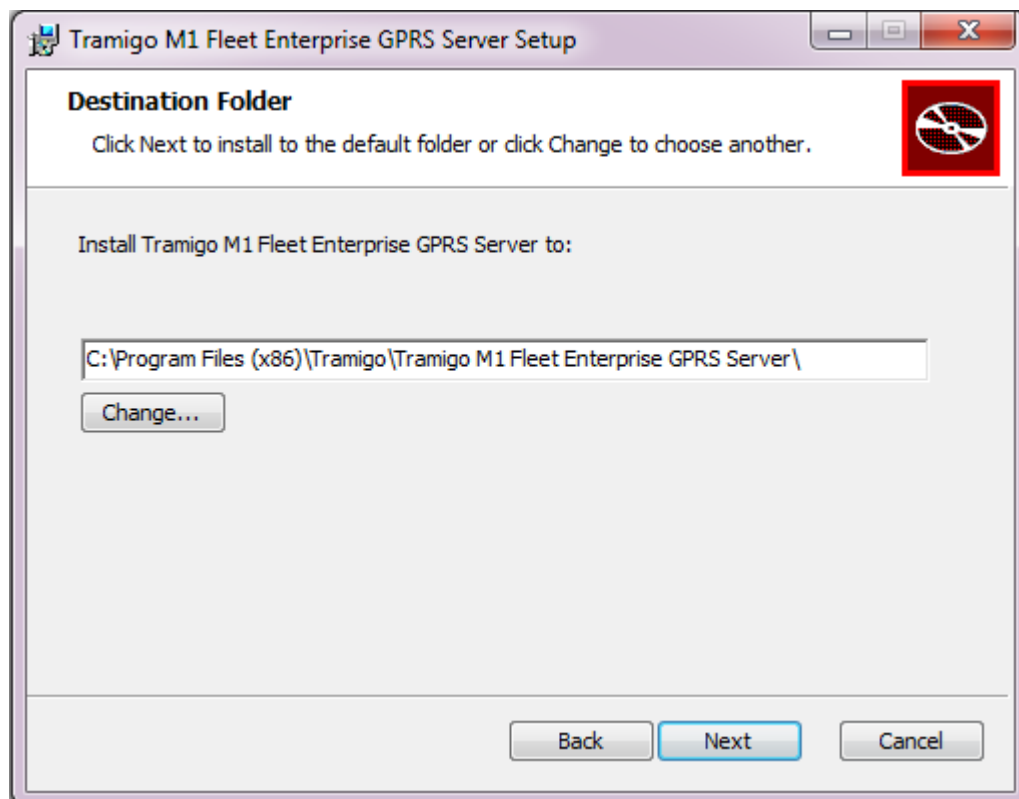
- Accept the End User License Agreement and click Next.



Accept the End User License Agreement and click Next.



- Select the installation directory and click Next.



Select the installation directory and click Next.



- Enter the SQL Server location if it's on a different server.

Database server connection

Configure SQL server connection

Enter SQL Server where GPRS Server will connect to.

SQL Server name

(local)

Note:

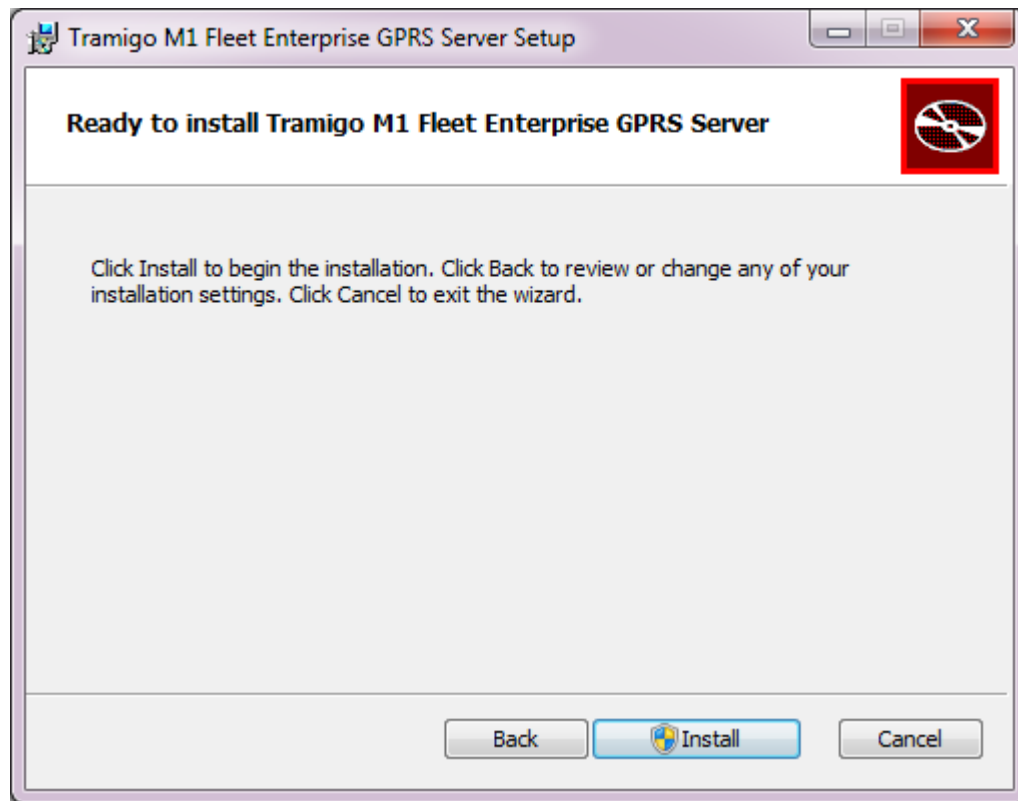
Enter (local) if the SQL Server is the same where you are installing GPRS server.
Enter IP Address or SQL Server name of the database server is in a remote machine.

Back Next Cancel

Enter the SQL Server location



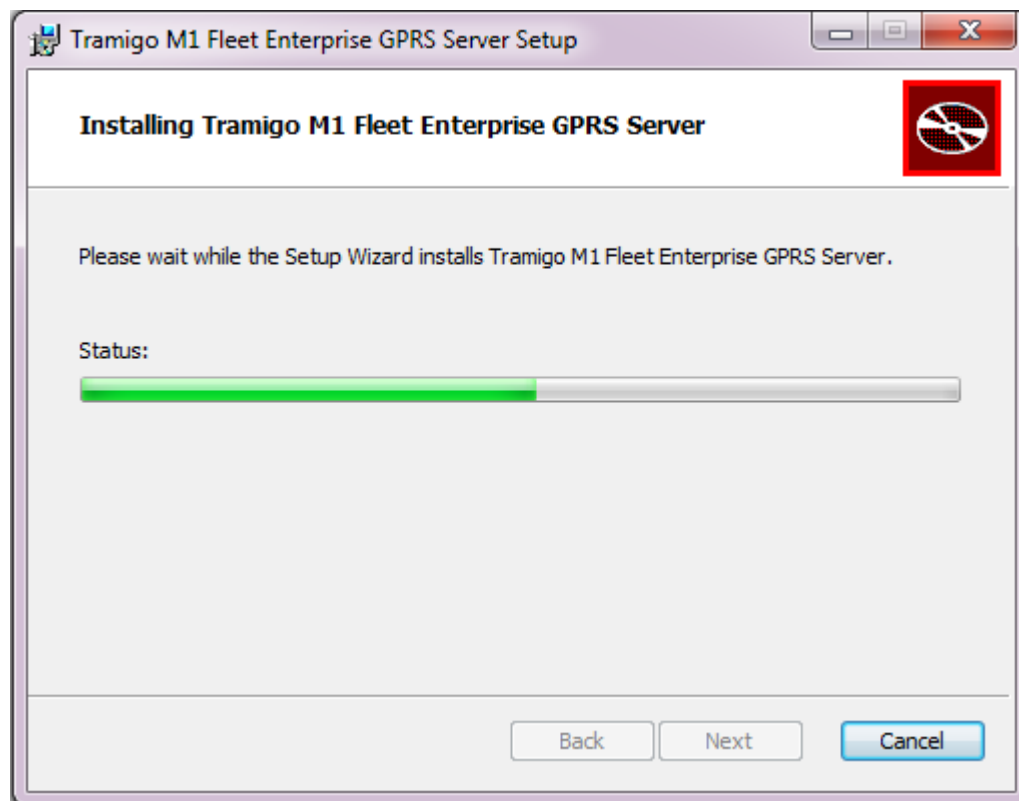
- Click on Install to begin the installation.



Click on Install.



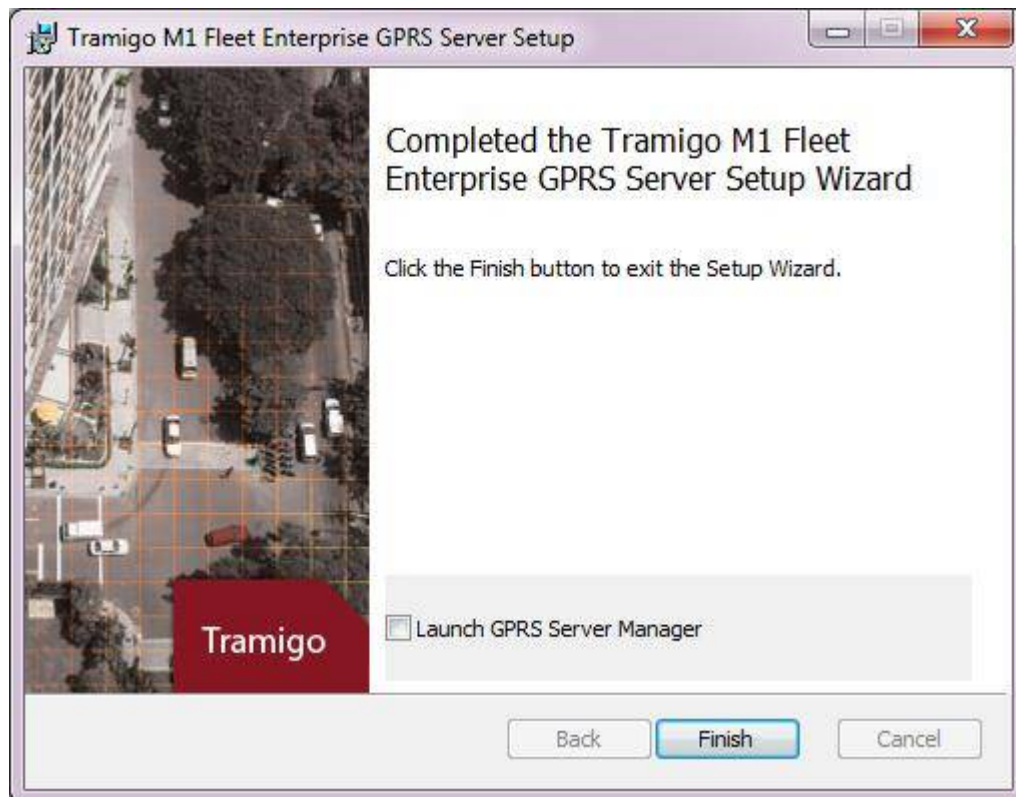
- Wait for the installation to finish.



Wait for the installation to finish.



- Click on Finish to exit the installation.



Click on Finish.



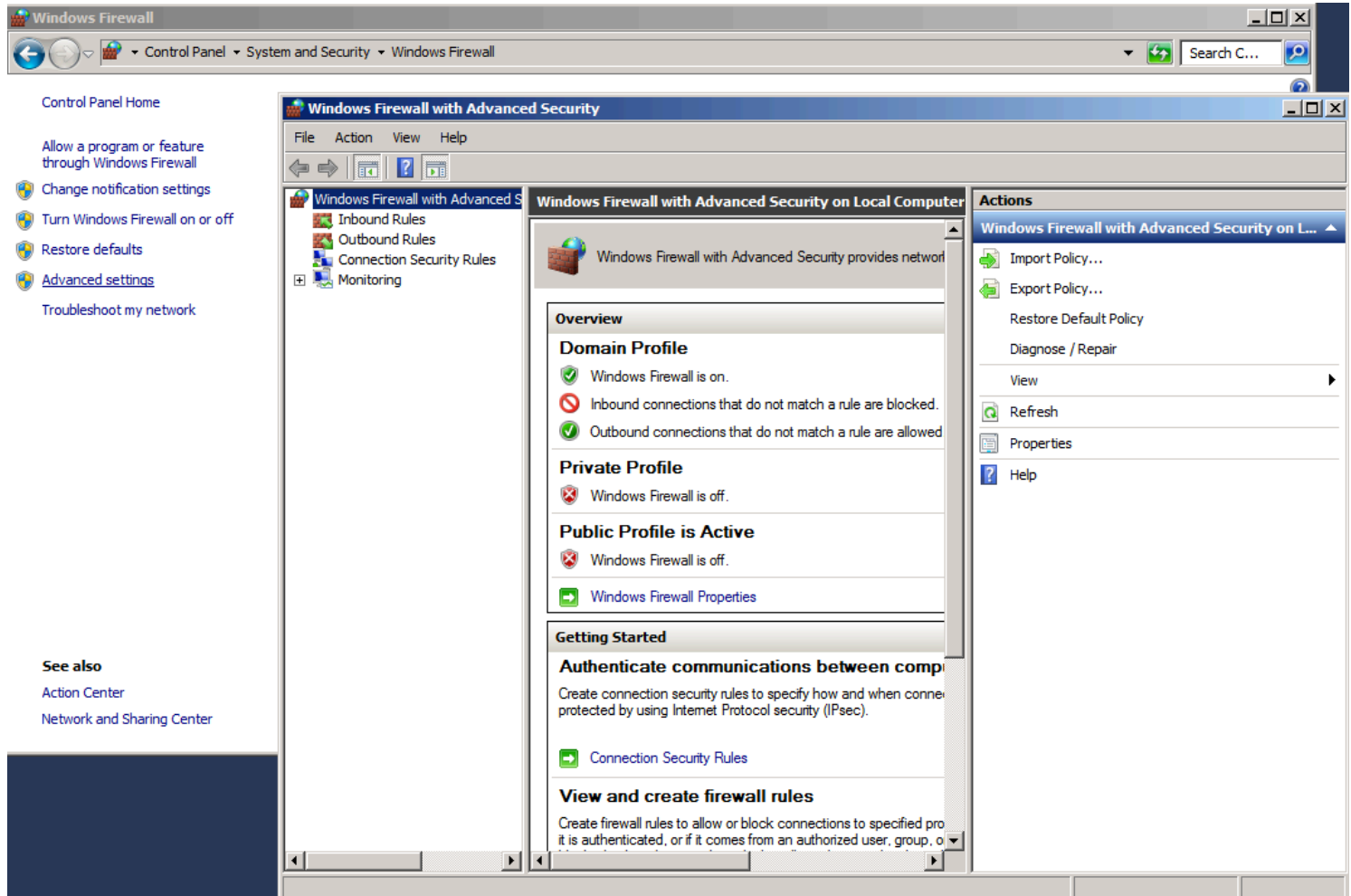
Server & Network Configuration

Communication Server

The Communication Server service is the API used by the M1FE Client. During installation, the default port used by this service is 8080.

If the server has firewall, create rules for port 8080 so it is reachable outside the network.

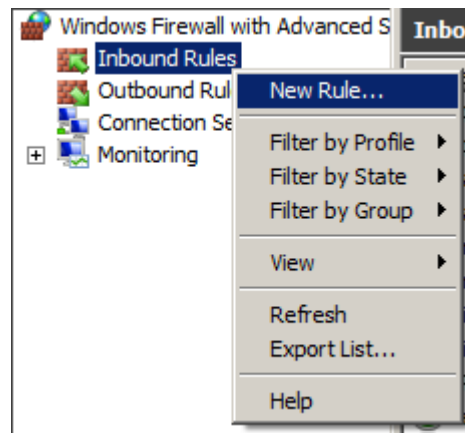
Windows Firewall, usually pre-installed with Windows, needs to be configured to allow port 8080. Open the Windows Firewall with Advanced Security from the Control Panel or from the Windows Applications.



Open Windows Firewall with Advance Security



On the Inbound Rules, create a new rule.



Create a new inbound rule



New Inbound Rule Wizard [X]

Rule Type

Select the type of firewall rule to create.

Steps:

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

What type of rule would you like to create?

☐ **Program**
Rule that controls connections for a program.

☒ **Port**
Rule that controls connections for a TCP or UDP port.

☐ **Predefined:**

Rule that controls connections for a Windows experience.

☐ **Custom**
Custom rule.

[Learn more about rule types](#)

< Back Next > Cancel

Select Port and click Next



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

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

Does this rule apply to TCP or UDP?

☒ **TCP**

☐ **UDP**

Does this rule apply to all local ports or specific local ports?

☐ **All local ports**

☒ **Specific local ports:**

Example: 80, 443, 5000-5010

[Learn more about protocol and ports](#)

< Back Next > Cancel

Leave the selection to TCP and fill-up Specific local ports with 8080. Click Next.



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

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

What action should be taken when a connection matches the specified conditions?

☒ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

☐ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
[Customize...](#)

☐ **Block the connection**

[Learn more about actions](#)

< Back Next > Cancel

Select Allow the connection and click Next



New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

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

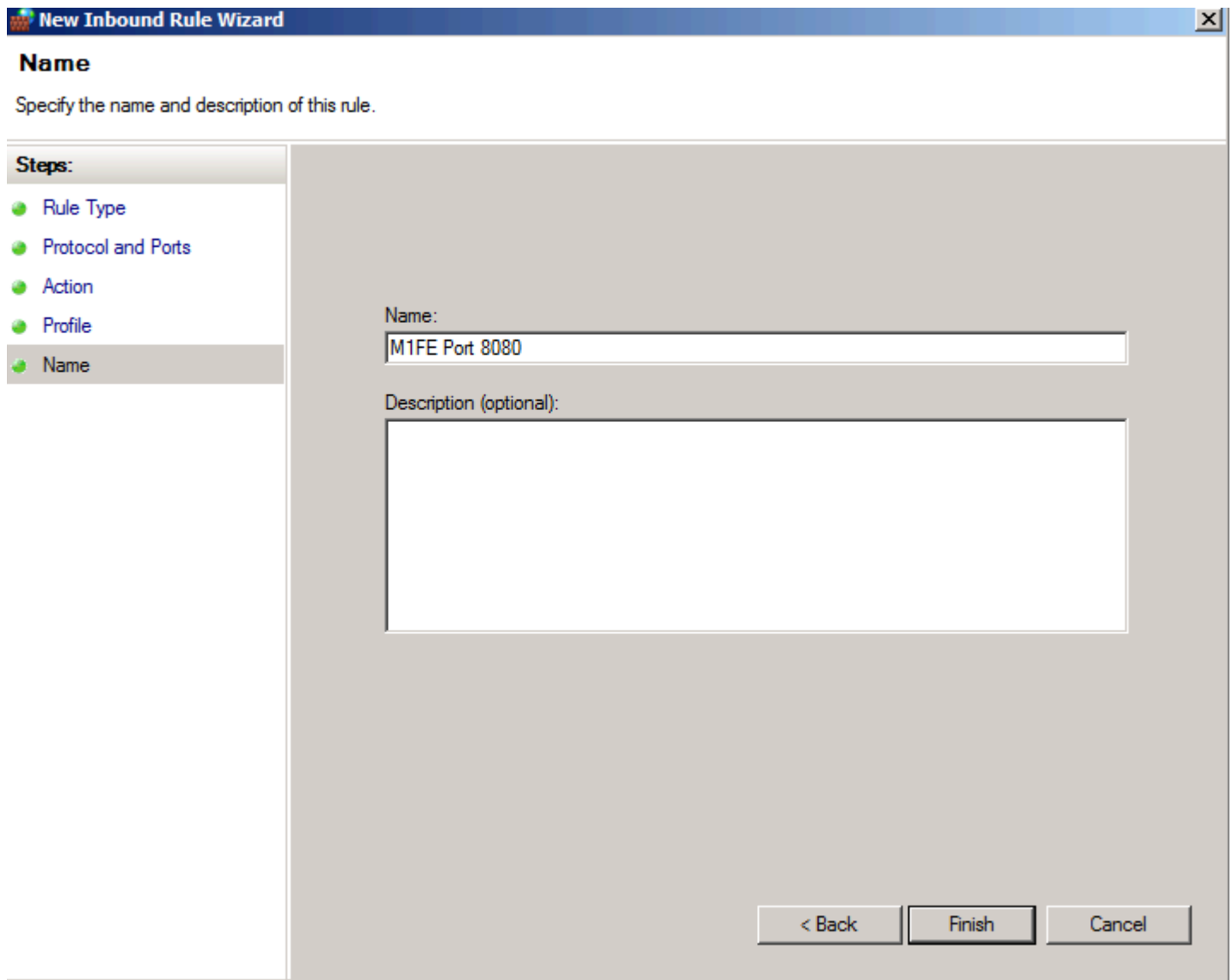
When does this rule apply?

- ☒ **Domain**
Applies when a computer is connected to its corporate domain.
- ☒ **Private**
Applies when a computer is connected to a private network location.
- ☒ **Public**
Applies when a computer is connected to a public network location.

[Learn more about profiles](#)

< Back Next > Cancel

Leave Domain, Private and Public checked. Click Next.



Set the name to M1FE Port 8080. Click Finish

The Windows Firewall should now be configured to allow connections to TCP port 8080 on the server.

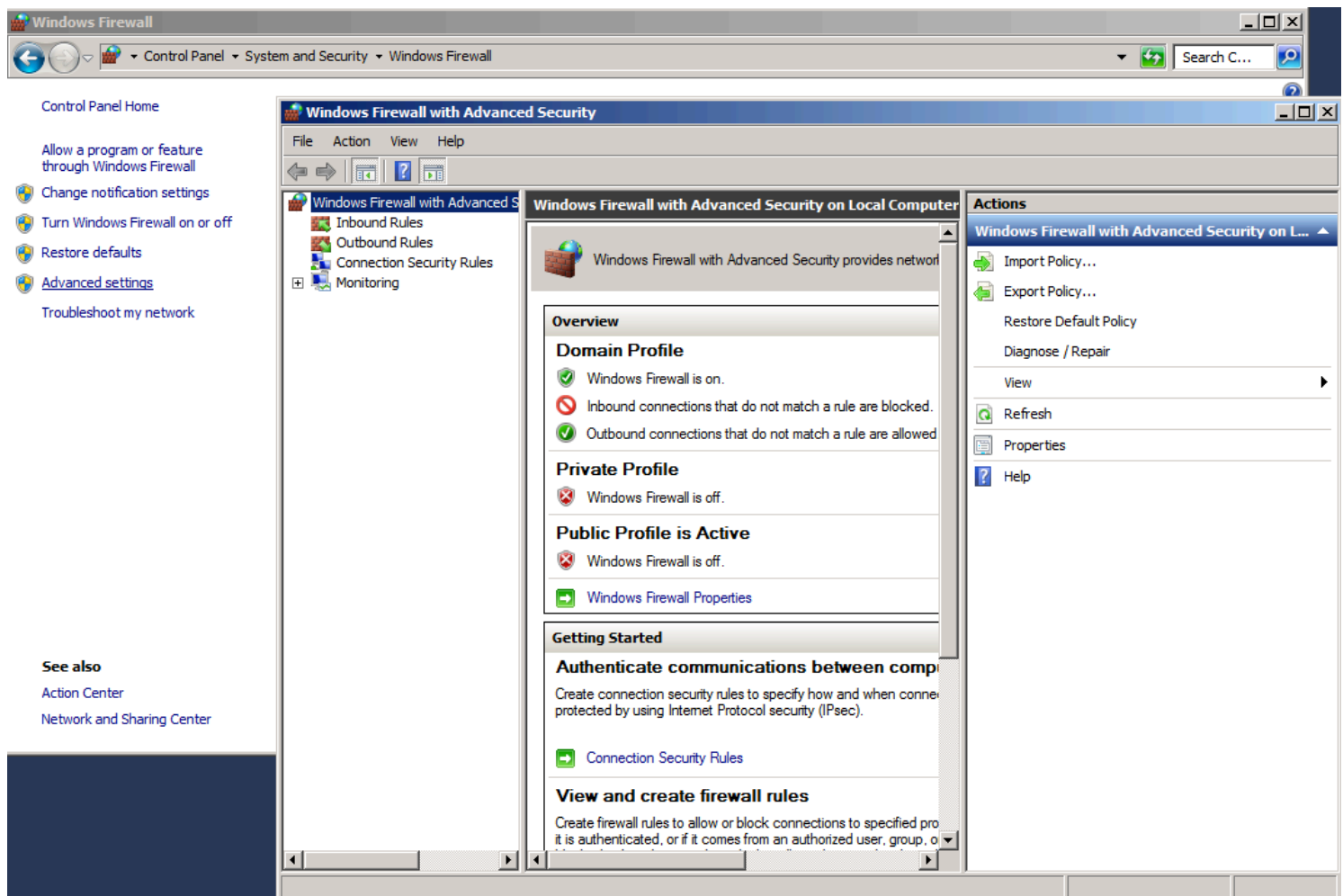


GPRS Server

The GPRS Server is the service listening and processing reports sent by devices to the server. During installation, the default port used by this service is 9566.

If the server has firewall, create rules for port 9566 so it is reachable outside the network.

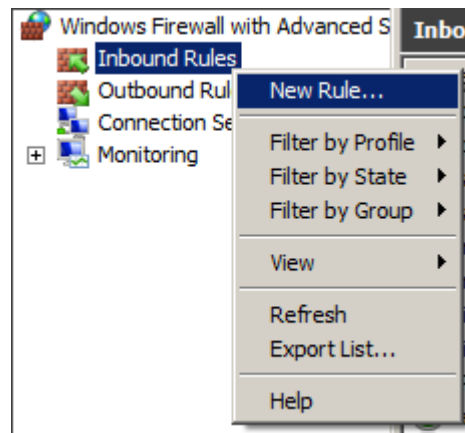
Windows Firewall, usually pre-installed with Windows, needs to be configured to allow port 9566. Open the Windows Firewall with Advanced Security from the Control Panel or from the Windows Applications.



Open Windows Firewall with Advance Security



On the Inbound Rules, create a new rule.



Create a new inbound rule



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

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

What type of rule would you like to create?

☐ **Program**
Rule that controls connections for a program.

☒ **Port**
Rule that controls connections for a TCP or UDP port.

☐ **Predefined:**

Rule that controls connections for a Windows experience.

☐ **Custom**
Custom rule.

[Learn more about rule types](#)

< Back Next > Cancel

Select Port and click Next



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

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

Does this rule apply to TCP or UDP?

☒ **TCP**

☐ **UDP**

Does this rule apply to all local ports or specific local ports?

☐ **All local ports**

☒ **Specific local ports:**

Example: 80, 443, 5000-5010

[Learn more about protocol and ports](#)

< Back Next > Cancel

Leave the selection to TCP and fill-up Specific local ports with 9566. Click Next.



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

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

What action should be taken when a connection matches the specified conditions?

☒ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

☐ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
[Customize...](#)

☐ **Block the connection**

[Learn more about actions](#)

< Back Next > Cancel

Select Allow the connection and click Next



New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

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

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

[Learn more about profiles](#)

< Back Next > Cancel

Leave Domain, Private and Public checked. Click Next.



New Inbound Rule Wizard [X]

Name
Specify the name and description of this rule.

Steps:

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

Name:

Description (optional):

< Back Finish Cancel

Set the name to M1FE Port 9566. Click Finish

The Windows Firewall should now be configured to allow connections to TCP port 9566 on the server.



Router Configuration

If the server is behind a router, you may need to configure the port forwarding on the router to allow ports used by M1FE (8080 for Communication Server and 9566 for GPRS Server) to be forwarded.

You can check your router guide on how to access the dashboard for setting up port forwarding.



Testing Opened Ports

You can check if the port is reachable outside the network by using the Open Port Check Tool available from this [link \(https://www.yougetsignal.com/tools/open-ports/\)](https://www.yougetsignal.com/tools/open-ports/).

Enter the IP Address of the server and the configured port and click Next

open port finder

Remote Address Port Number
[↻ Use Current IP](#)

Check a port's status by entering an address and port number above.

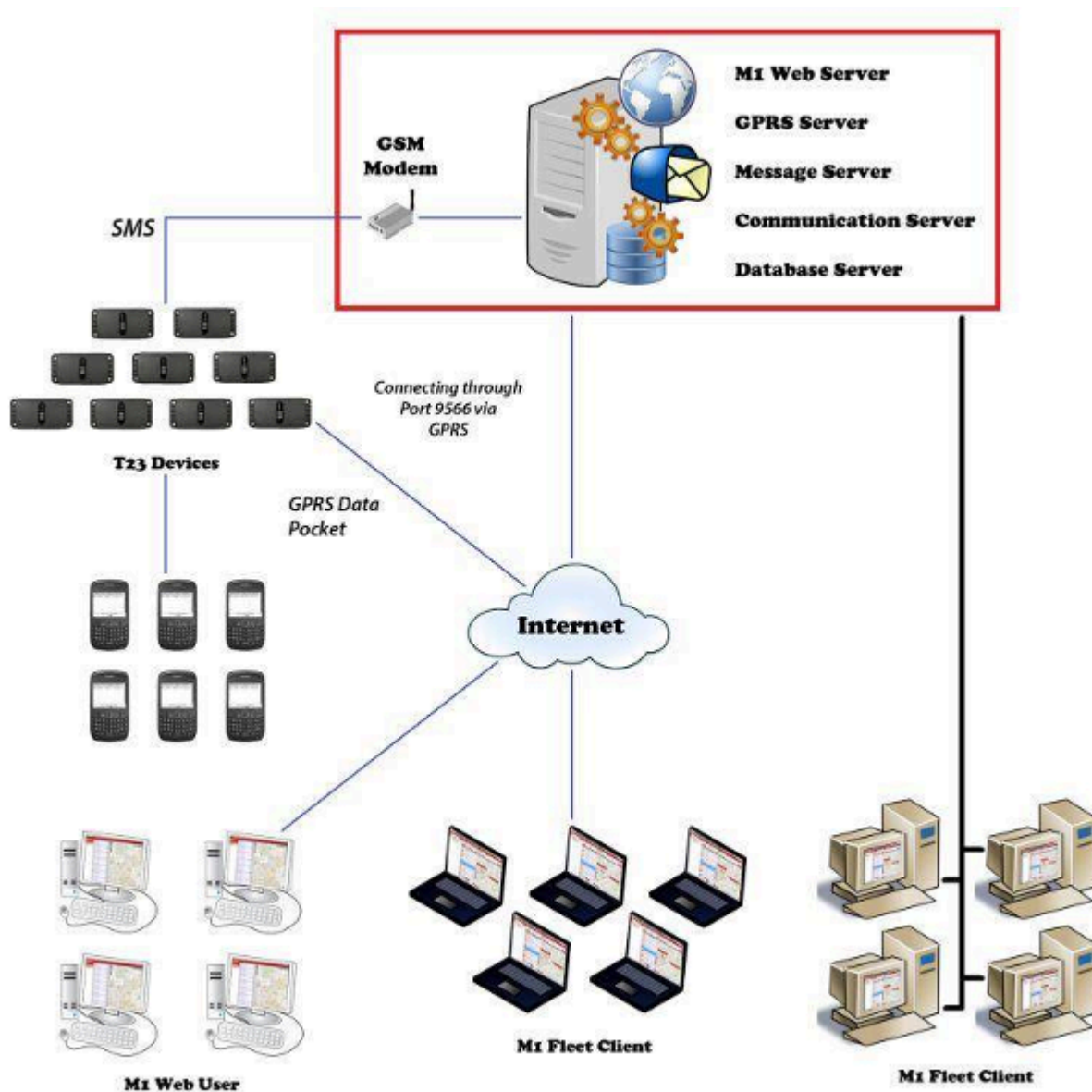
Enter IP Address of server and the port. Click Check



M1FE Server Architecture

Single Server - Direct Connection

The server is connected directly to an ISP with public static IP or fully qualified domain name. Database and M1FE components are installed on a single server.



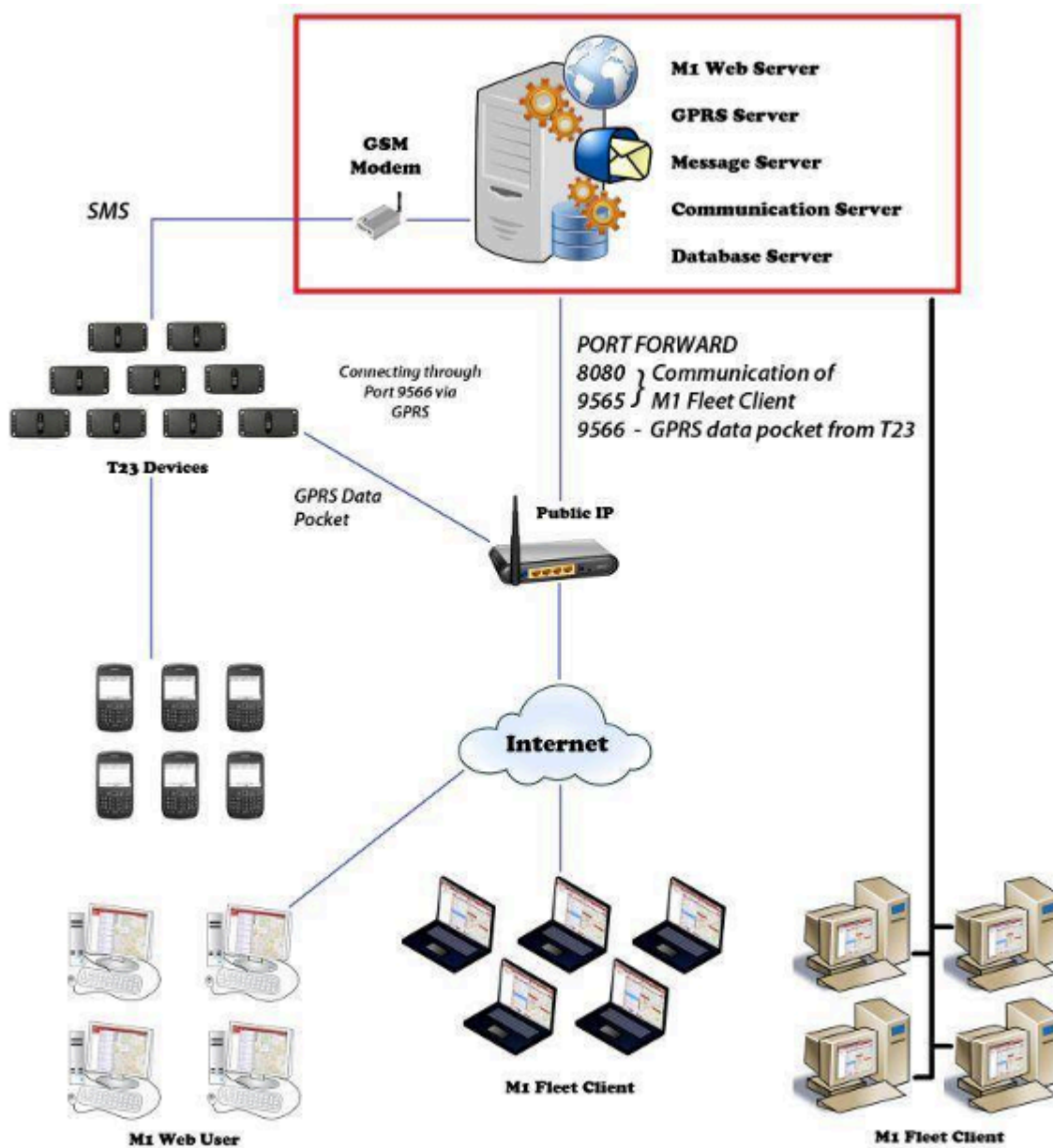
Single Server - Direct Connection



Single Server With Router

The server is connected to a router and, optionally, to a load balancer and external firewall. The router is assigned with a public static IP or binded to a fully qualified domain name.

Database and M1FE components are installed on a single server.



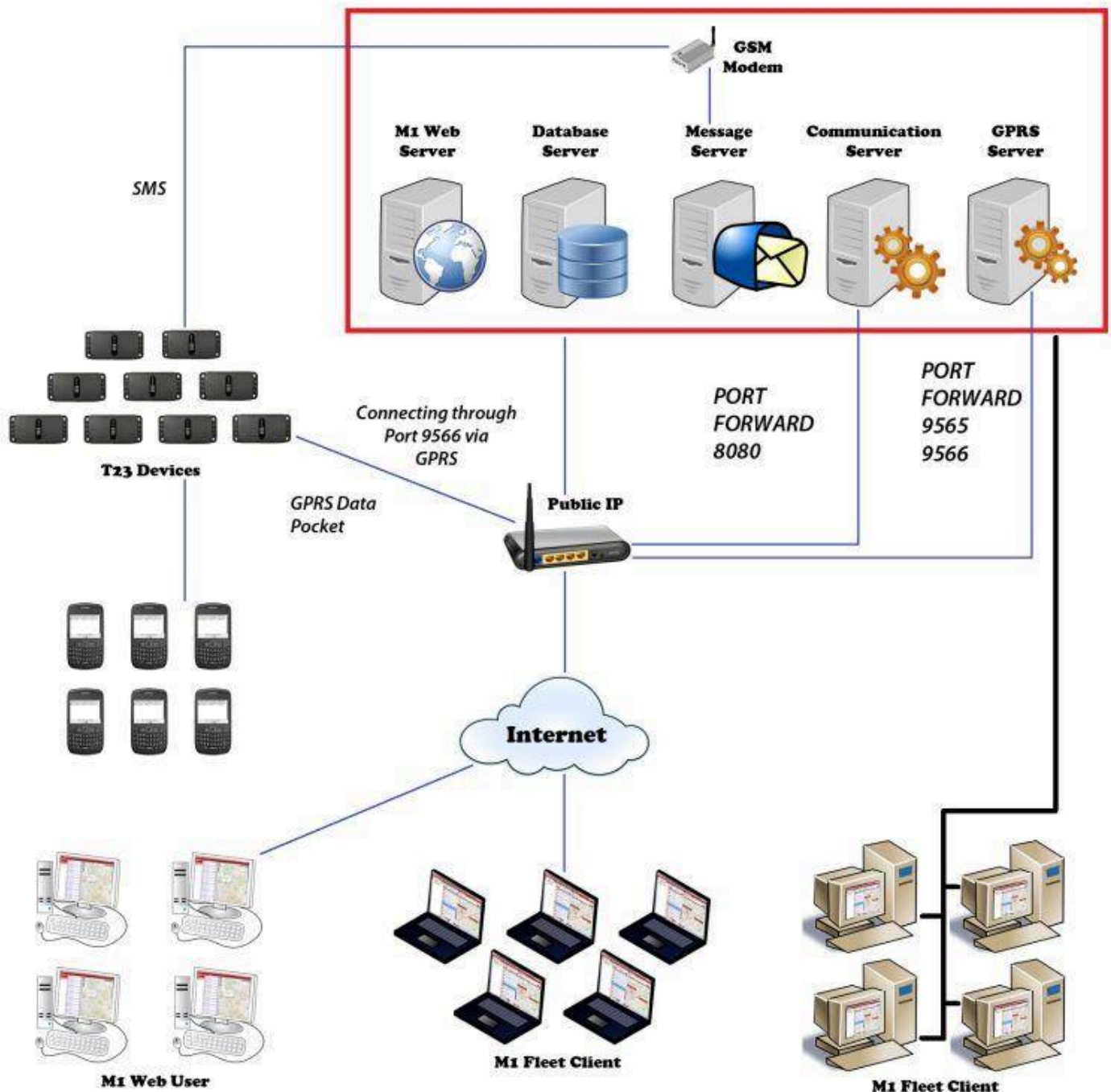
Single Server With Router



Multiple Servers

The server is connected to a router and, optionally, to a load balancer and external firewall. The router is assigned with a public static IP or binded to a fully qualified domain name.

Database and M1FE components are installed on different server instances for maximum scalability.



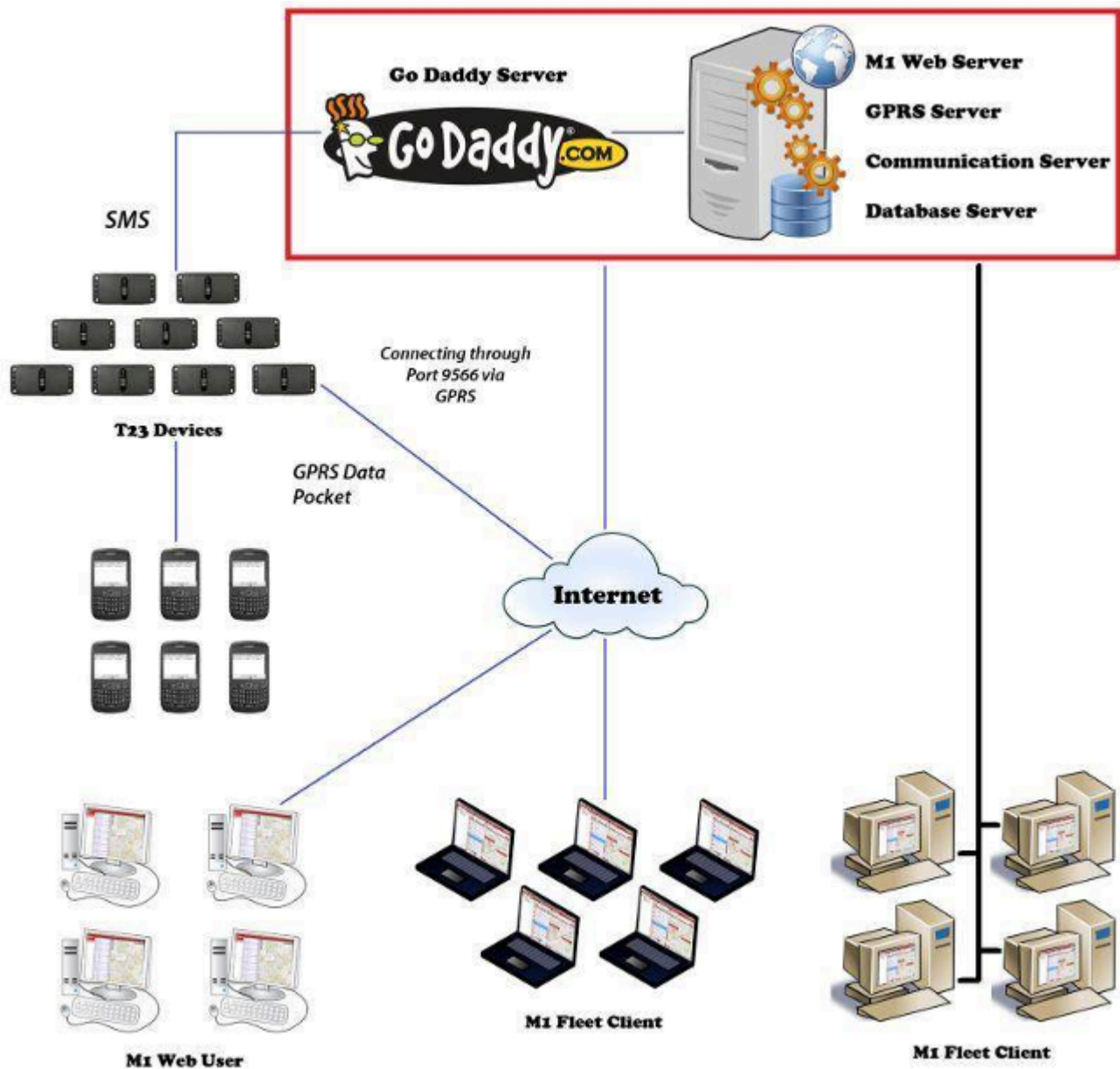
Multiple Servers



Cloud Servers

The server is hosted on the cloud with various scalability and architecture options as supported by the hosting provider. Cloud services offer various networking tools to configure securing, routing and balancing the network. You can check with your hosting provider for the available setup.

The simplest of this architecture is to have database and M1FE components on a single server instance on the cloud.



Cloud Server