midmark

Midmark Connect for Epic

Version 11.0

Operation Manual

003-10511-00 Rev. AA1

Notice

The information in this manual is subject to change without notice.

Midmark Corporation shall not be liable for technical or editorial omissions made herein, nor for incidental or consequential damages resulting from the furnishing, performance, or use of this guide.

IQecg, IQmanager, and IQvitals® Zone are trademarks of Midmark Corporation.

Epic, EpicCare, EpicCare Link, App Orchard, Hyperspace, and Hyperdrive are trademarks of Epic Systems Corporation.

Windows and Microsoft are registered trademarks of Microsoft Corporation in the United States and other countries.

Intel and Intel Core are trademarks of Intel Corporation in the United States and other countries.

Citrix, ICA, and XenApp are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

VMware Horizon is a registered trademark of VMware, Inc.

Part Number for this Operation Manual – English: 003-10511-00 Revision AA1

Table of Contents

Important Information

Safety Symbols

	**Warning** *Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.*
	**Caution** *Indicates a potentially hazardous situation that may result in minor or moderate injury. It may also be used to alert against unsafe practices.*
NOTICE	**NOTICE** *Indicates practices not related to physical injury.*

Physician's Responsibility

When enabled, instruments that run through the Midmark Connect software can provide interpretations; these interpretations are for the exclusive use of licensed Physicians or personnel under their direct supervision. The suggested interpretation and the numerical and graphical results should be examined with respect to the patient's overall clinical condition.

Final analysis should always be determined and verified by a Physician. Proper administration of the test is the Physician's responsibility, as is making a diagnosis, obtaining expert opinions on the results, and implementing the correct treatment, if indicated.

RxOnly	Caution: Federal law (U.S.A.) restricts this device to sale by or on the order of a physician.

Related Documents

The following documents may be needed in order to operate Midmark diagnostic devices and software products:

- Midmark Digital Vital Signs Device Operation Manual (Part Number: 21-78-0001)
- Midmark IQvitals® Zone Operation Manual (Part Number: 22-78-0002)
- Midmark Digital Spirometer Operation Manual (Part Number: 56-78-0001)
- Midmark IQecg Operation Manual (Part Number: 48-78-0002)
- Setup Manual: Midmark Products over Thin Client using IQpath™ (Part Number: 61-78-0001)
- Midmark IQiE Operation Manual

All product Operation Manuals can also be downloaded from midmark.com. Contact Midmark Technical Service for additional information.

Overview

Introduction

Midmark Connect for Epic is a connectivity solution that allows for the usage of the following Midmark digital diagnostic devices: Midmark Digital Vital Signs Device, IQvitals® Zone, Midmark Digital Spirometer, IQecg, and electronic weight scales. Midmark Connect interfaces with Epic EHR utilizing the FHIR medical data protocol and custom APIs. Midmark Connect provides a simple, powerful, and seamless user experience.

The Midmark Connect for Epic Software will enable the user to:

- Create new Vitals, Spirometer, and ECG tests using Epic.
- Edit Midmark Spirometer and ECG tests using Epic.
- Support performing tests when there is no access to Epic.
- Support Thin Client environments such as Citrix and VMware.

This Operation Manual is designed as a comprehensive guide to educate the user on the operation and functions of Midmark Connect for Epic Software.

IMPORTANT NOTE
The Installation process detailed below is specific to ECG and Spiro. For Vitals Installation, please refer to the IQiE Operation Manual found under the Manuals folder.

Features

- Use Epic Hyperdrive or Hyperspace to perform acquisition, editing, and comparison of supported Midmark devices
- Create PDFs to be used in Epic ROI and ECLink workflows

Updates and Enhancements

Midmark regularly makes updates and/or enhancements to its software products in a continual effort to provide healthcare providers with products that promote efficient and effective patient care.

For details regarding enhancements to Midmark Connect, contact Midmark Technical Service.

Computer Date Information

Midmark Connect calculates the patient's age by using the current date from the computer and the patient's birth date as entered by the operator. Since the patient's age is vital to producing appropriate diagnostic statements, it is important that the computer's date is accurate. Contact the system administrator for assistance with this function.

Necessary Computer Skills

The installation portion of this manual is written for an IT professional who is capable of managing and setting up a Windows server, IIS, Microsoft SQL, and is familiar with Epic EHR.

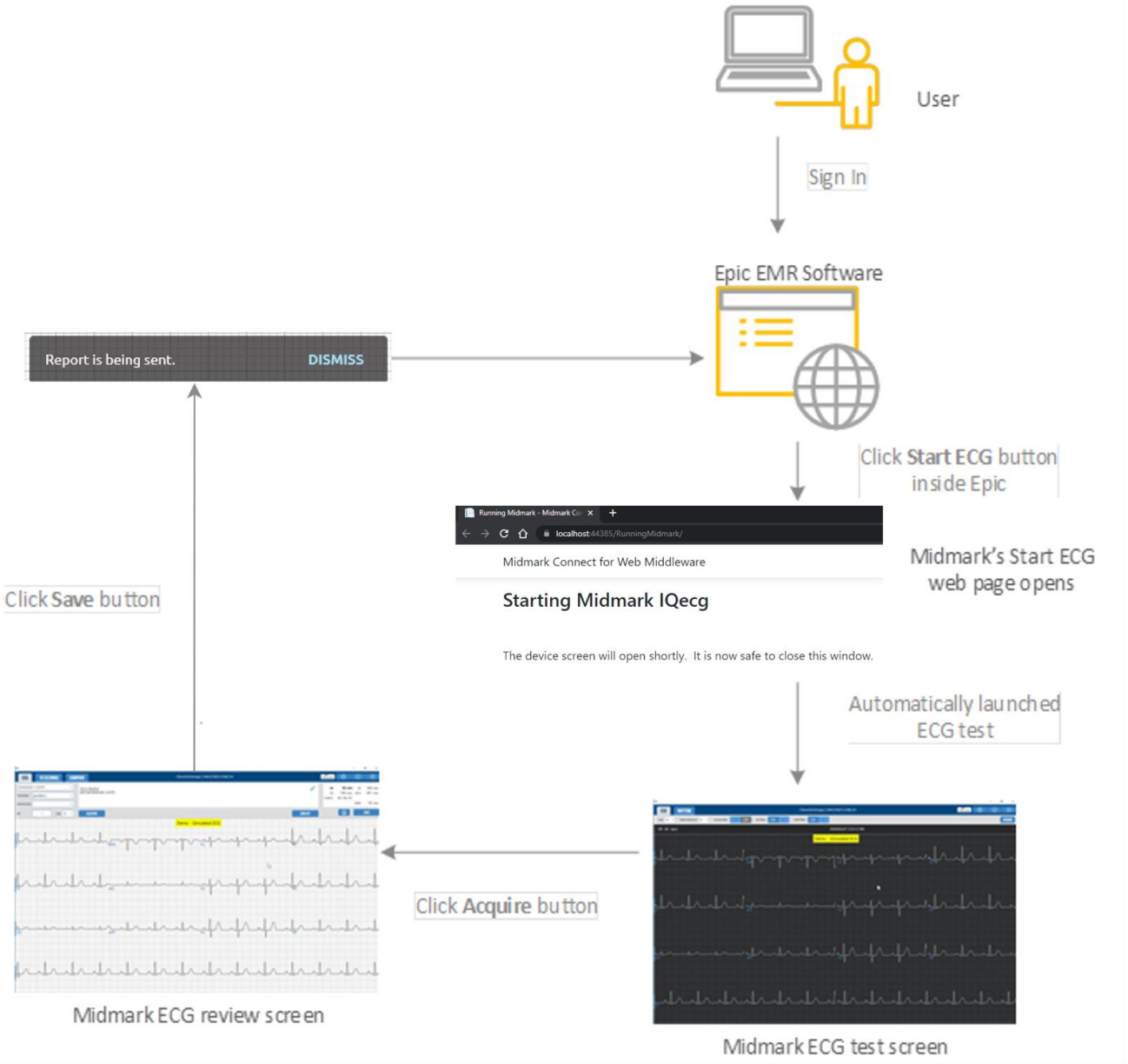
The operation portion of this manual is written for a user capable of using Microsoft® Windows®-based applications, has some understanding of PC operations, and is familiar with the basic operations of Windows®.

For technical questions, please contact Midmark Technical Service.

Technical Overview

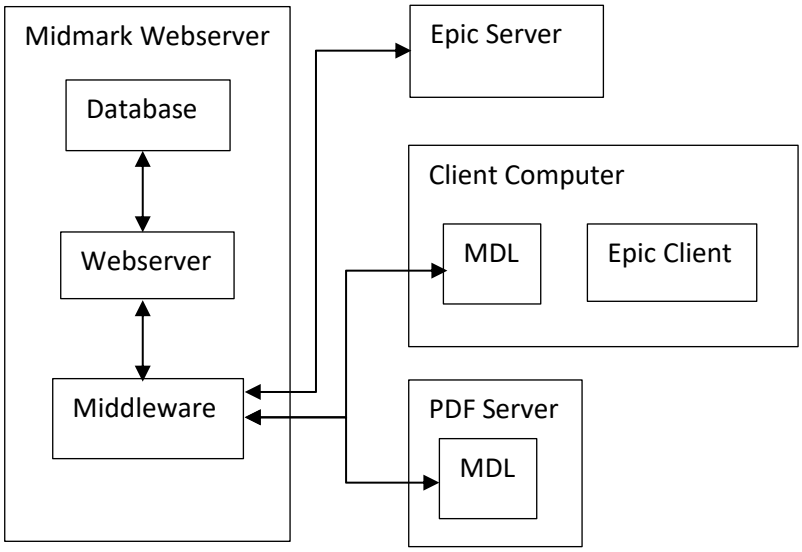
Midmark Connect for Epic User Workflow

The following diagram illustrates the Midmark Connect for Epic Software workflow when the user is interacting with the Midmark device software, in this case, the IQecg plugin.



Midmark Connect for Epic Technical Diagram

The following diagram illustrates the technical architecture of the Midmark Connect for Epic software.



Midmark Webserver

This is the Midmark server which hosts the two MCF web components (**Webserver** and **Middleware**) as described in the Server Software Installation section. This server may be separate from the database server, or the same. In all cases, it must have access to the database and to the computers on which plugins and a Midmark Device Launcher (MDL) are installed.

Database Server

This server hosts MCF's SQL Server database. This server may be a distinct machine from the web server, or it may be the same, the diagram above shows it as the same. The MCF database stores data about the Midmark Device Launchers (MDLs) in use, and nothing else.

MDL (Midmark Device Launcher)

This software is required to be installed and actively running in the system tray of each client computer and PDF server that is interacting with the Midmark reports or devices.

Client Computer

This computer is typically a Citrix or VMware server, but can also be a compatible local Windows machine. It is the computer the staff uses to interact with the Epic client (Hyperspace or Hyperdrive) and will utilize the locally running MDL software to acquire, edit, or compare Midmark's diagnostic test data.

PDF Server

This server hosts a running MDL, typically loaded on a service account to auto login, that has been configured to act as a PDF Server during installation. This server is responsible for generating PDF reports to support Epic's ROI and ECLink workflows.

Epic Server

This is the Epic endpoint that supports the Epic on FHIR APIs and custom APIs to allow for the Midmark Connect for Epic software to interact with the Epic software.

Installation

> ***Note***
> *Contact Midmark Technical Service before installing and setting up Midmark Connect. Computers today are more complex, with more software and hardware options than before, making each computer almost unique. Midmark wants to make sure that Midmark Connect is installed and configured as quickly and easily as possible.*

> ***Note***
> *Before installing the software, note if a screen saver or any energy saving feature is enabled on the computer to make sure that it does not activate and interfere with data acquisition during patient testing. Refer to the computer or software manuals for information on this setting.*

> ***Note***
> *Close all programs before running this software installation; it should not be interrupted once it is initiated.*

Hardware and Software Requirements

Refer to the Minimum Computer Requirements document at midmark.com or contact Midmark Technical Service.

The Minimum Computer Requirements document describes the minimum computer resources and hardware components needed when using new Midmark devices and software. As it is the nature of technology to change often, these requirements will be evaluated and modified periodically. We suggest always referring to the most recent Minimum Computer Requirements document for your version of Midmark software. This information can be found at midmark.com or by contacting Midmark Technical Service.

> ***Note***
> *If updating existing computer systems that are currently being used with older Midmark devices and software, please contact Midmark Technical Service before installing the new software.*

Server Software Installation

1. Log in as the Administrator.

⚠	***Caution*** *The user MUST log in as the Administrator before proceeding. If the user does not have this authority, contact the Network Administrator.*

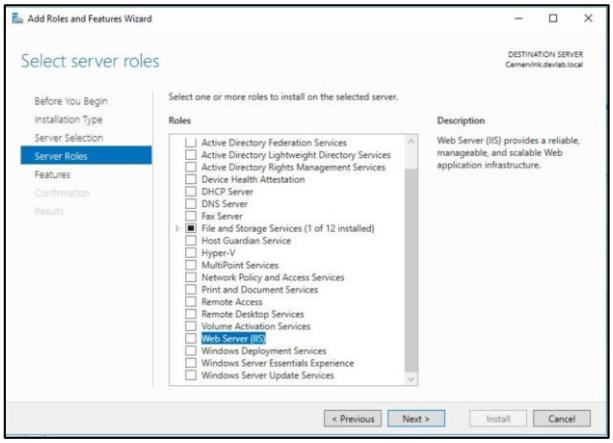
2. Verify that the IIS Server role is installed. If it is not installed, complete the following steps:

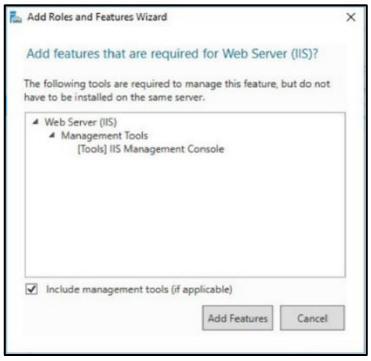
   2.1. Launch the Server Manager.

   2.2. Click on **Manage.**

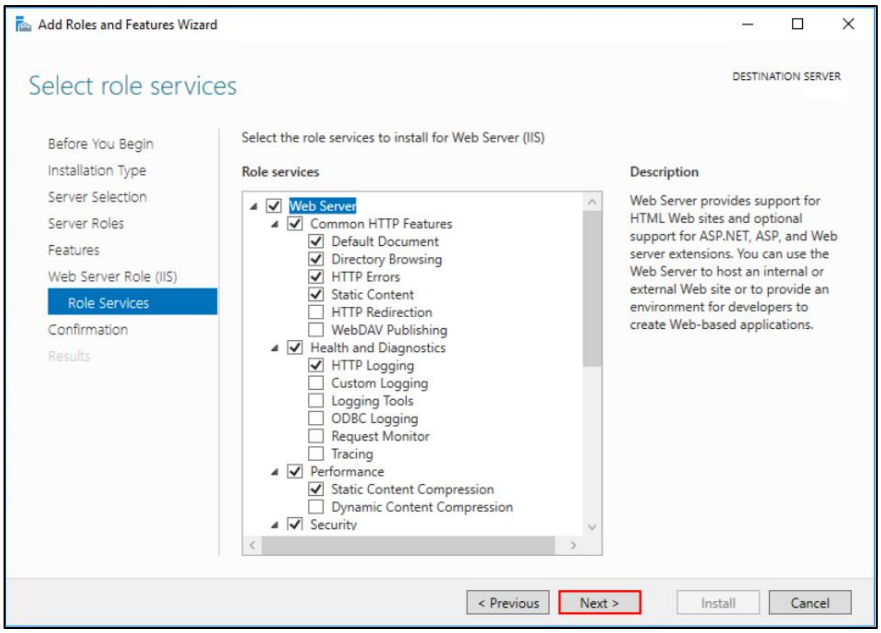
   2.3. Click on **Add Roles and Features.**

   2.4. Check the **Web Server (IIS)** Role. A new window may appear for installing additional required features. Click on **Add Features**. Click **Next** back on the Select server roles.





   2.5. Accept the default role services provided and click on **Next.**



2.6. Proceed to finish installing the web server role and services.

3. Download the Midmark Connect for Epic setup files from the link provided by the Midmark Consulting Team.
4. Un-Zip all the files.
5. Navigate to the following Server folder.
6. The three components of the Server Installation are:
   6.1. DotNetCoreHosting
   6.2. MidmarkConnectForWebMiddleware
   6.3. MIdmarkConnectForWebServer (which hosts the Web Services and generates the required database on the SQL Server)

.NET Core Hosting Installation

1. Locate and open the DotNetCoreHosting folder in the Server folder.
2. Right click on the **dotnet-hosting-3.1.13-win.exe** file and select the **Run as administrator** option.
3. Select **Yes** on the **User Account Control** prompt to allow Windows to run the file.
4. On the Microsoft .NET Core 3.1.13 Windows Server Hosting prompt, click on the checkbox to agree with the license terms and conditions. Then click on Install.
5. Confirm the installation was successful. An installation message reading "Installation Successfully Completed" will appear once the installation is complete.

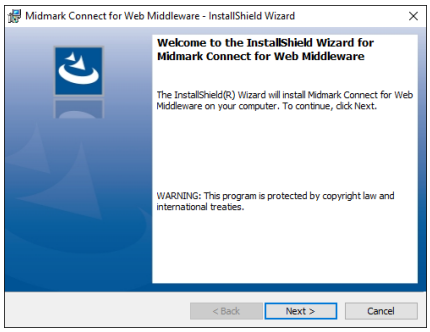
MidmarkConnect For Web Middleware Installation

1. Locate and open the M**idmark Connect For Web Middleware** folder in the Server folder:

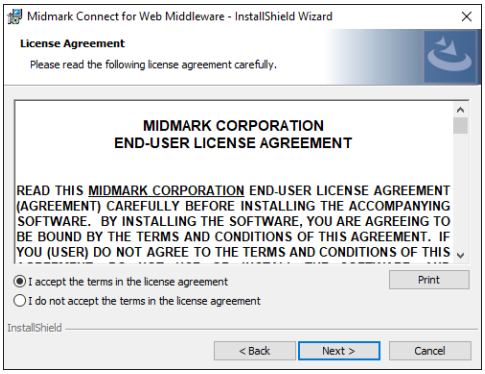
2. Right click on the **WebMiddleware_setup.exe** file and select the **Run as administrator** option. Allow Windows to run the file as Administrator if prompted.

3. Select **Yes** on the **User Account Control** prompt to allow Windows to run the file.

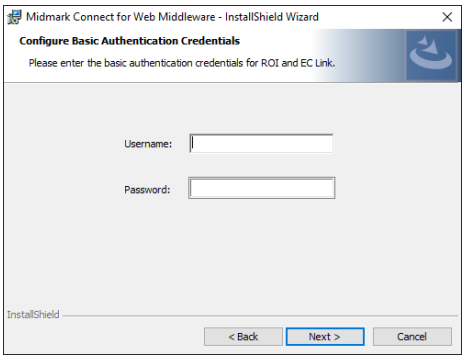
4. Click on **Next** in the **Midmark Connect For Web Middleware** InstallShield Wizard dialog:



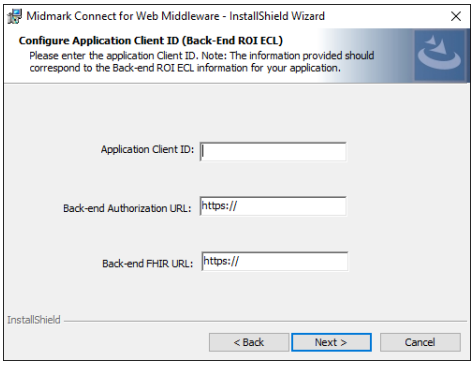
5. Check the **I accept the terms in the license agreement** option, and click on **Next**:



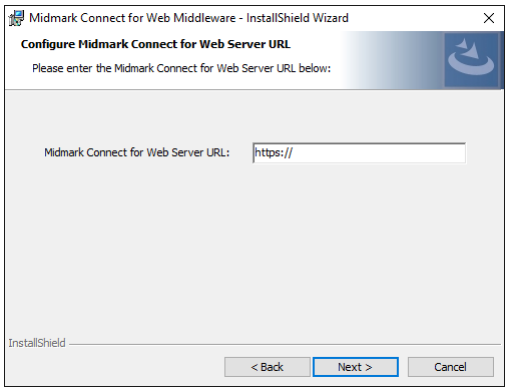
6. Enter the **Username** and **Password** that corresponds to the user's **Basic Authentication Credentials** for the ROI and EC Link feature, and click on **Next**. Note: review the Epic AppOrchard documentation on how to create this credential.



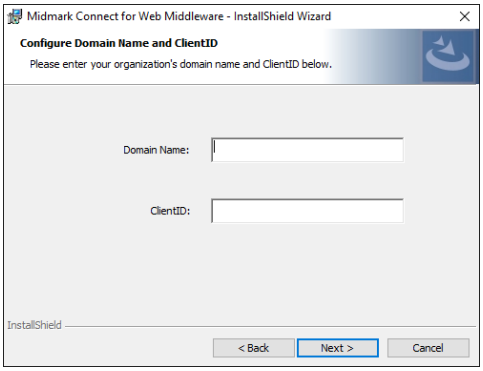
7. Enter the **Application Client ID**, **Back-end Authorization URL**, and **Back-end FHIR URL**, then click on Next. Please note, the Client ID on this dialog corresponds to the application's Back-end Client ID. Your Midmark Implementation Specialist can provide the Application Client ID. These two URLs are customer specific and should be known by the organization's IT or can be found by an Epic Technical Service representative.



8. Enter the **Midmark Connect for Web Server URL** and click on Next:

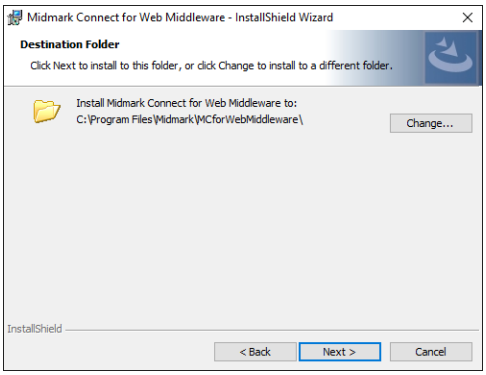


9. Enter the organization's **Domain Name** and front-end **Client ID**:

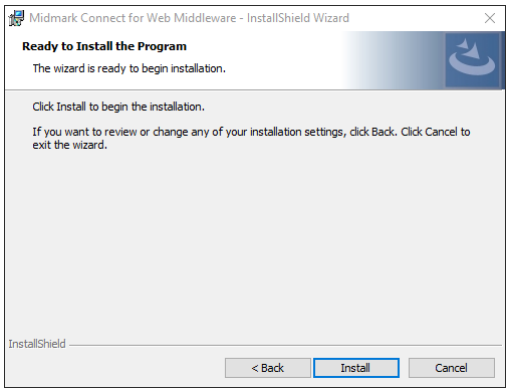


Note
During Installation Domain Name should remain constant. Please use the same Domain Name whenever this variable is presented.

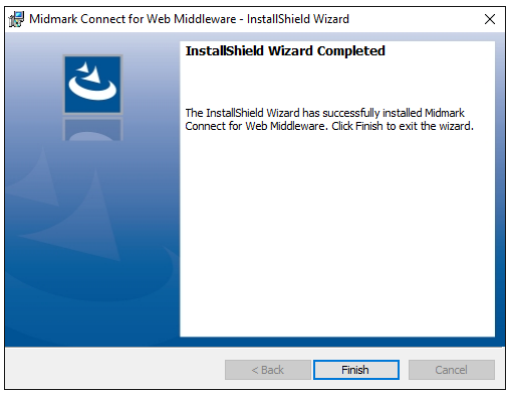
10. Select the installation directory and click on **Next**::



11. Click on **Install** to proceed with the installation:

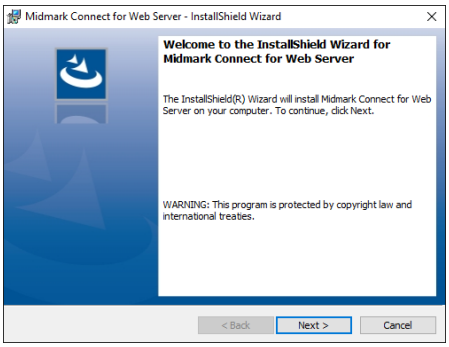


12. Click on **Finish** to complete the installation:

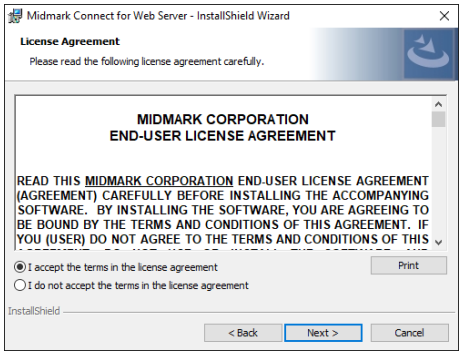


Midmark Connect for Web Server Installation

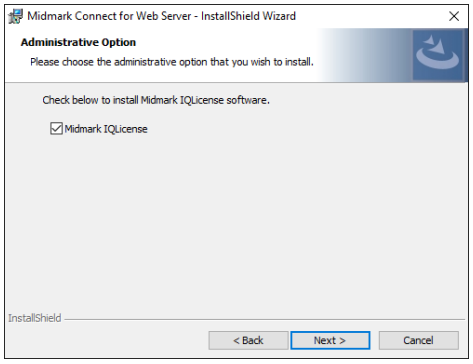
1. Locate and open the **Midmark Connect for Web Server** folder in the Server folder:
2. Right click on the **WebServer_setup.exe** file and select the **Run as administrator** option. Allow Windows to run the file as Administrator if prompted.
3. Select **Yes** on the **User Account Control** prompt to allow Windows to run the file.
4. Click on **Next** on the **Midmark Connect for Web Server** InstallShield Wizard dialog:



5. Check the **I accept the terms in the license agreement** option and click on **Next:**

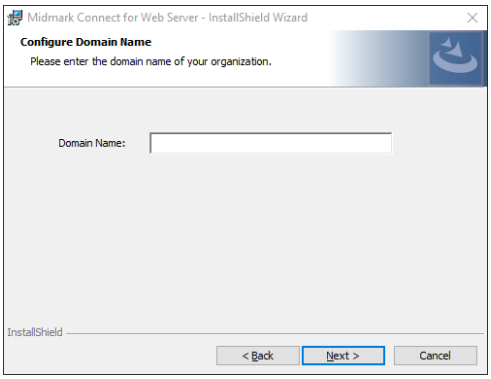


6. Check that the **Midmark IQLicense** box is checked if this will be the computer the licensing software will be deployed on and click on **Next**.

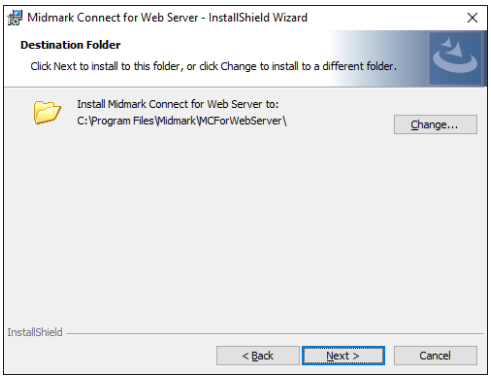


Note
Additional installation steps will be required if the Midmark IQLicense box is checked. See the *Midmark IQLicense and Configuration Appendix* for additional information.

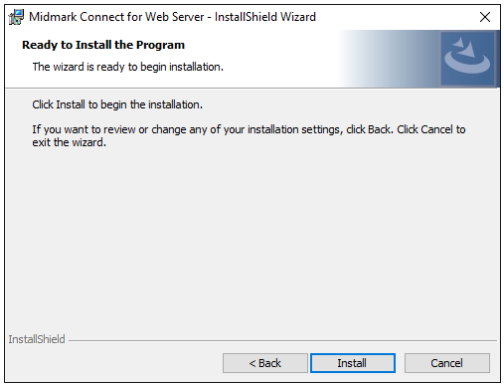
7. Enter the organization's **Domain Name** and click on **Next.**



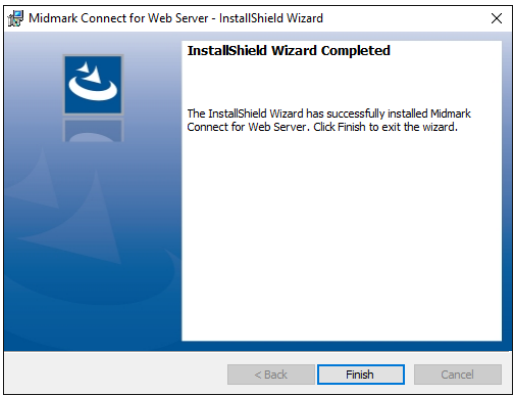
8. Select the installation directory and click on Next.



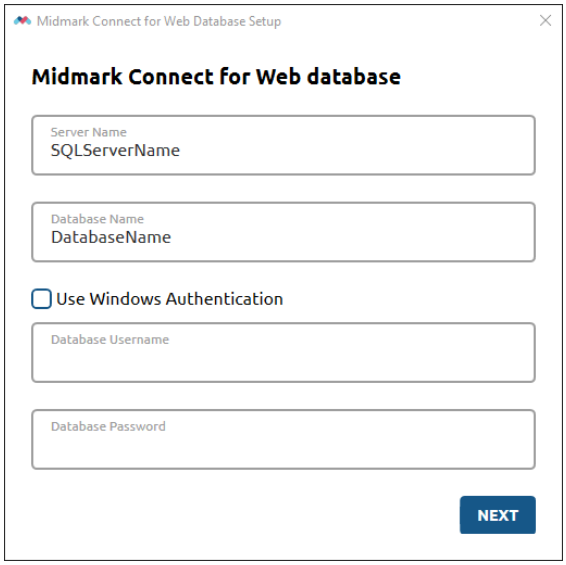
9. Click on **Install** to proceed with the installation.



10. Click on **Finish** to complete the installation.



11. Add the **Server Name and Database Name** for the SQL database server. If you are connecting to a named instance, enter the **Server Name** as the {server name}\{instance name}. For example, *MidmarkSQLServer\SQLExpress.* Also specify a **Username** and **Password** for SQL authentication. Select **Next** to proceed. See **Appendix G Using SQL Server with Windows Authentication** for more details.



Network Configuration

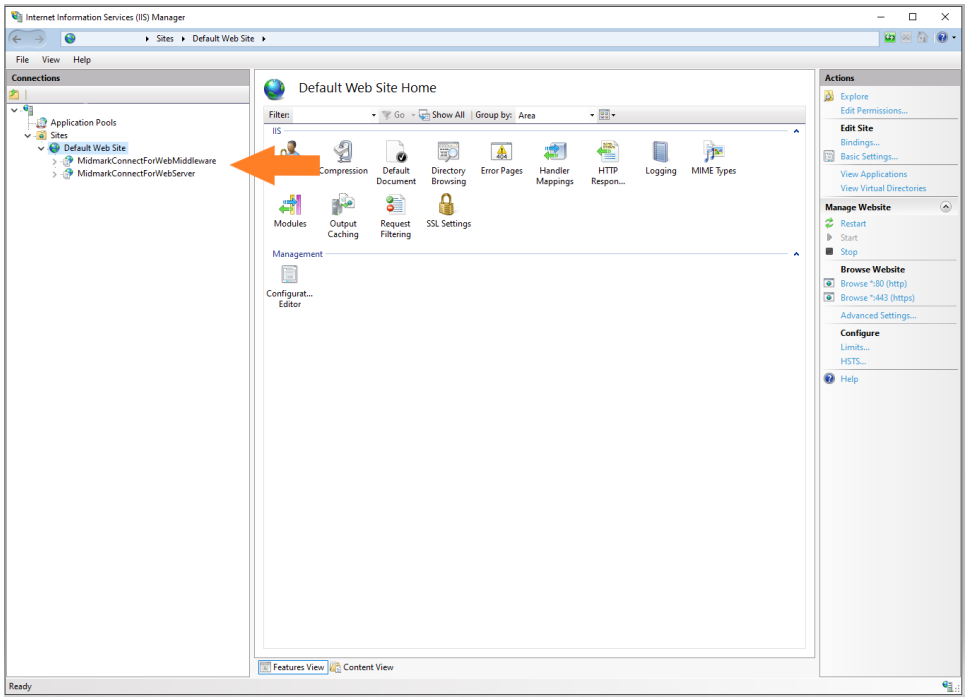
The Midmark Connect for Epic Interface requires a limited number of ports to be open for client/server or server/server communication. The following table lists the port, protocols, and Midmark Connect for Epic components/software that will communicate across those ports.

Server/Item	Protocol	Port	Comments
Midmark Connect Web Service	HTTPS	6436	• Protocol used is dependent on customer requirements.
Midmark Licensing Server	TCP	27500	• Typically installed on the same server as Midmark Connect Web Service. • Software needs to reference this server to check out/check in licenses. • For additional information on Port and Firewall adjustments see Appendix I – Configuring Windows Firewall for Midmark IQlicense.

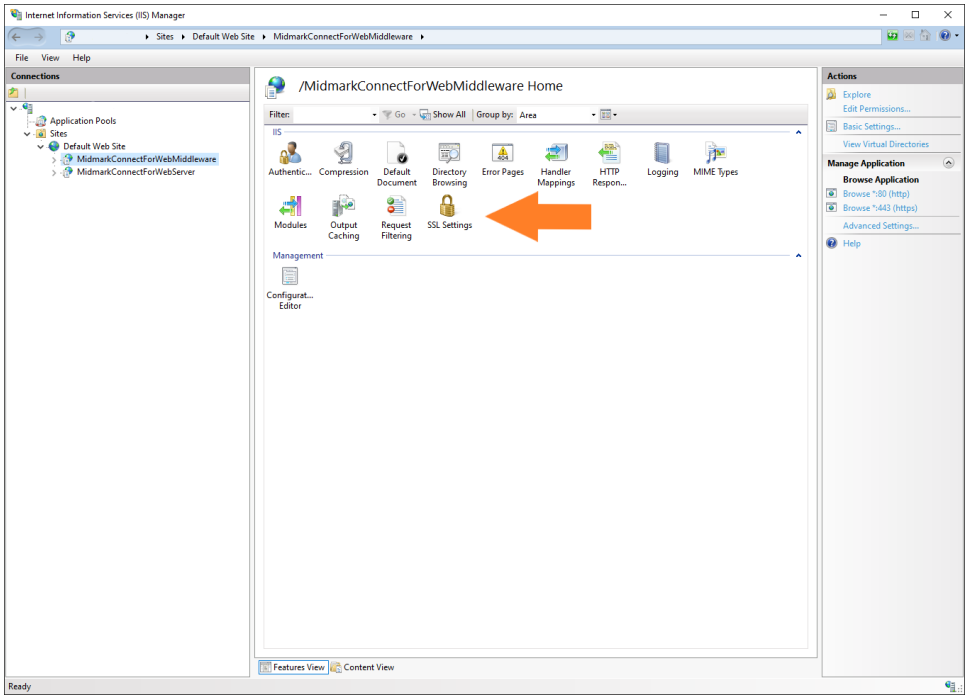
Midmark Application Pool

Please see **Appendix A - Using Midmark Connect with a Secure Connection (HTTPS)** for details on the initial setup with IIS. Then proceed with the steps below to set up IIS with Midmark Connect for Epic.

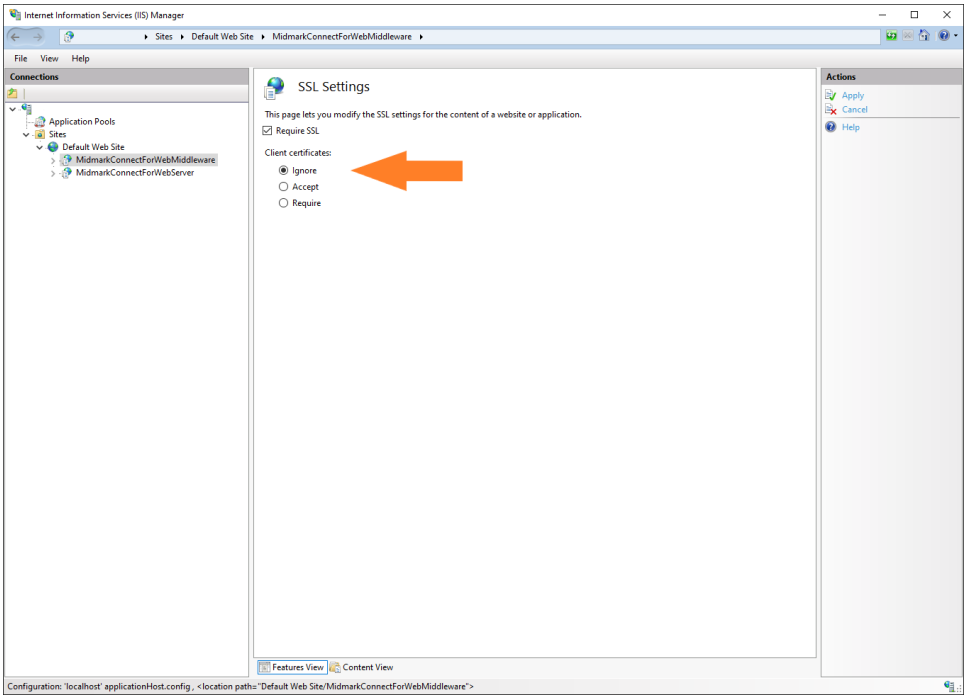
1. After installing the **Midmark Connect for Web Middleware** installer and **Midmark Connect for Web Server,** navigate to IIS Manager. Expand the Default Web Site Section until the **MidmarkConnectForWebMiddleware** and **MidmarkConnectForWebServer** nodes appear.



2. Click on the **MidmarkConnectForWebMiddleware** node. Click on **SSL Settings.**



3. Navigate to the **Action** section on the right hand side of the window and click on **Open Feature**. Check the **Require SSL** checkbox and select the **Ignore** radio button. Repeat Steps 2 and 3 for the **MidmarkConnectForWebServer** node.



Note
Midmark Connect for Web Middleware only supports HTTPS.

4. Reset the IIS to restart the Web Server.
5. Get data from the installation environment and apply it back to the back-end app.
    a. Go to the folder C:\ProgramData\Midmark\CertFiles and find the public key there.
        i. Public key is called “uploadToEpicPubkey.cer”.
    b. If more than one key is present due to past install attempts, be sure to use the one that has the same date and time as the privateKey.pfx.
    c. In your Back end app in AppOrchard, find the Upload public key button, click it, and choose the public key found in the cert files folder.
    d. Click Save at the bottom of the app screen in AppOrchard.
    e. Once the public key has been stored and recognized by Epic’s systems, you should you see a long number / text above the button, instead of a file name.
    f. Epic may take 24 hours or longer to recognize the key.

Note
The Epic environment may take 24 hours or longer to recognize the key. Please check with your Epic Technical Support for steps on potentially speeding up the process.

Note *If you navigate back to the Back end app, please note that the file name will have been converted to a long number / text above the button.*
Note *Microsoft web components are constantly maintained and secured. Please keep the Windows Server OS and SQL Server software up to date with security patches from Microsoft.*

Client Software Installation

Midmark Connect for Epic - Midmark Device Launcher (MDL) Software Installation

Note ***Close all programs before running this software installation.*** *Once the installation initiates, it should not be interrupted until it has completed.*

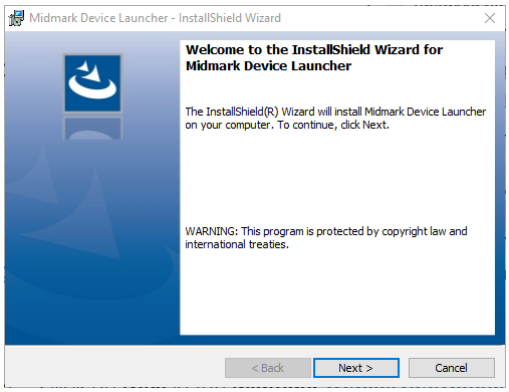
Note *This manual does not describe how to use the Midmark digital diagnostic devices in detail, nor does it describe how to use Epic. Please refer to the relevant documents under Related Documents for additional information.*

The Midmark Connect for Epic – Midmark Device Launcher (MDL) setup file will install the MDL on the client computers. The Server Installation is recommended to be finished before attempting to install MDL.

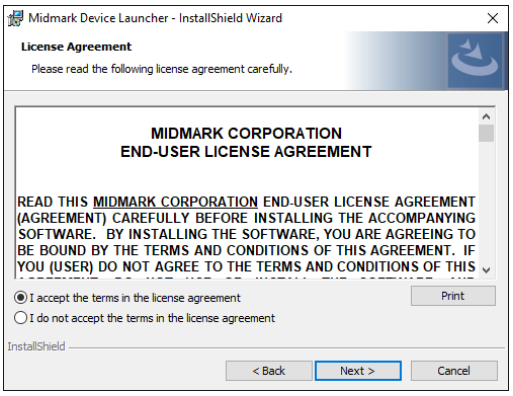
Note that when running on Windows® 10, log in as the administrator before proceeding. Contact the system administrator if this permission has not been granted.

1. Locate and open the **MidmarkDeviceLauncher** folder inside the **Client** folder. Right click on the MDL_setup.exe file and select the **Run as administrator** option.

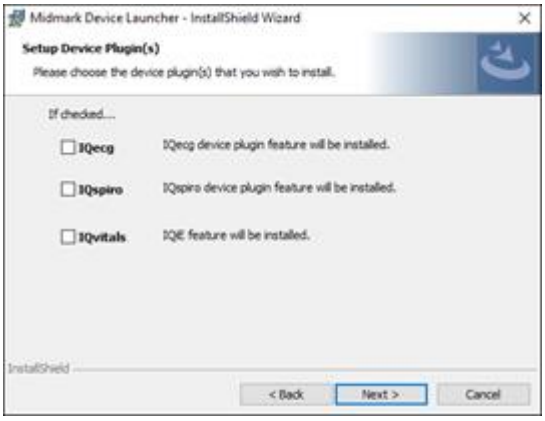
2. Select **Yes** on the **User Account Control** prompt to allow Windows to run the file.
3. Click on **Next** on the *Midmark Device Launcher- InstallShield Wizard* window:



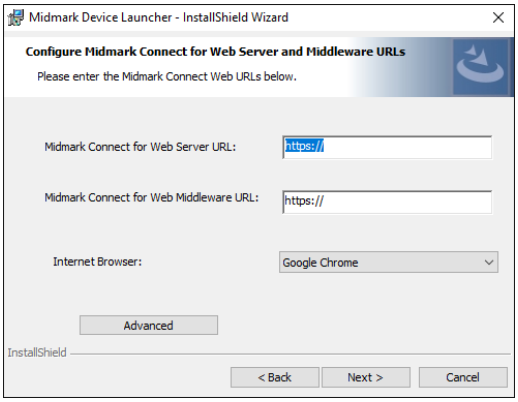
4. Select the **I accept the terms in the license agreement** option and click on **Next**:



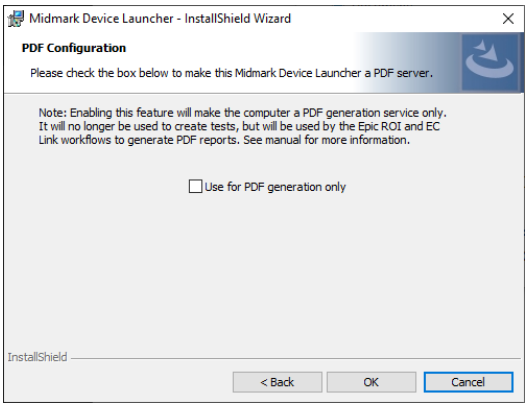
5. Check the Midmark devices plugin options, and click on **Next**:



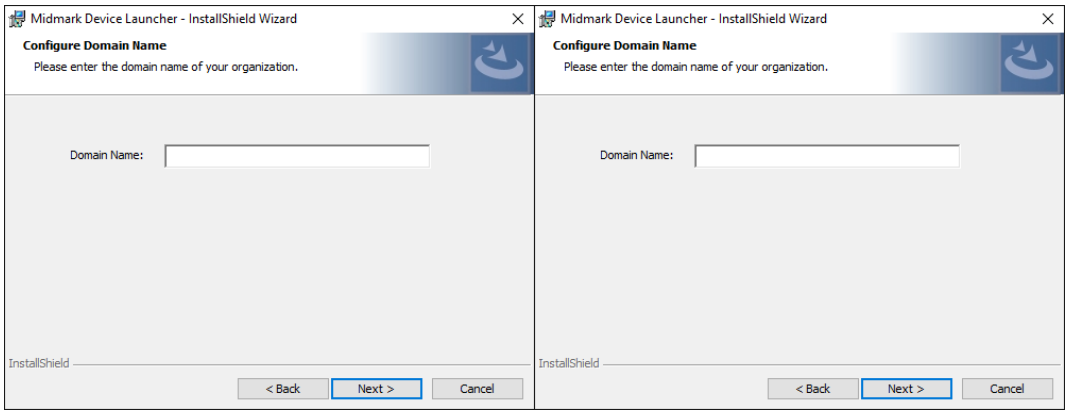
6. Enter the **Midmark Connect for Web Server** and **Web Middleware URLs.** Select the **Internet Browser** that will be used when running the Midmark Connect for Epic software.



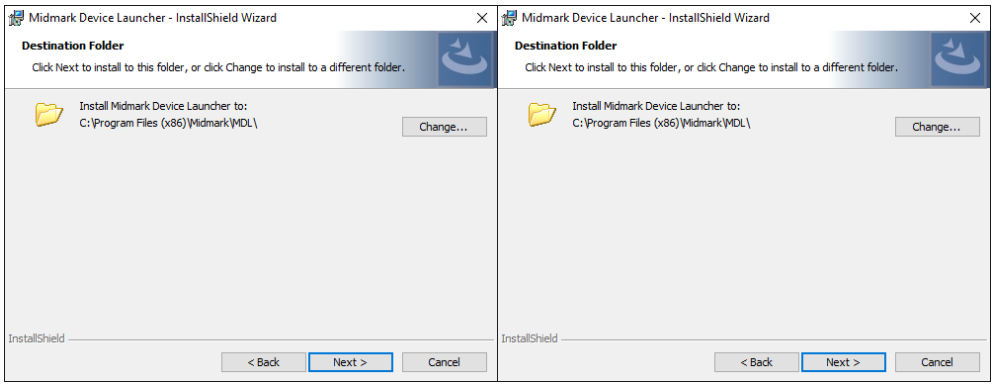
7. If this Midmark Device Launcher will only be used as a PDF server, click on the **Advanced** button and check the **Use for PDF generation only** checkbox then, click on **Next.**



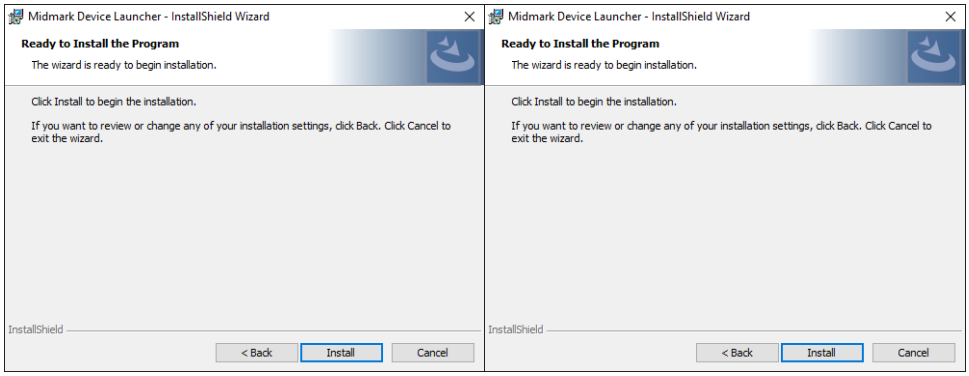
8. Enter the organizations **Domain Name** and click on **Next**.



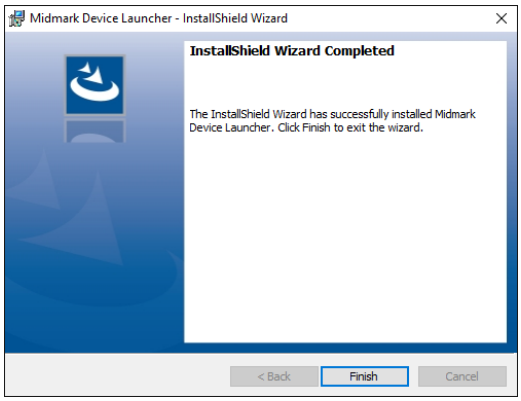
9. Select the installation directory and click on **Next**.



10. Click on **Install** to begin the installation:



11. Click on **Finish** to end the installation:



12. Each device that was selected to be installed will display an installation wizard sequentially. For instructions on installing each device, refer to the appropriate device manual's Installation section, manuals listed under Related Documents.
13. Note the Midmark Connect shortcut on the desktop after all software is installed successfully:

14. The MDL software runs in the system tray after successful installation. If you hover over the icon in the system tray, it should display a ‘connected’ status to indicate it found the appropriate Midmark server.

15. Installation is done and ready to begin performing tests.

Note
The MidmarkMDL.exe located in ‘C:\Program Files (x86)\Midmark\MDL’ will need to be running by the time the end user needs to access Midmark in Epic. If using Midmark in a published application environment, this can be accomplished by publishing a script file that launches Hyperspace/Hyperdrive and the MidmarkMDL.exe or by another preferred method.

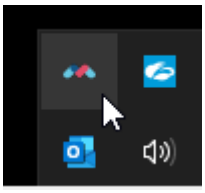
Configuration

Please see Understanding and Editing appsettings.json File Settings appendix to configure and manage the application settings.

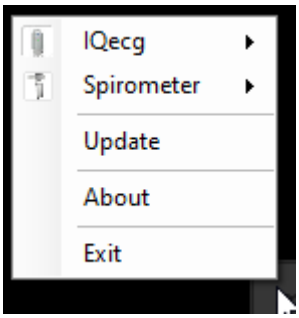
Software Update Screen

The Pending ***Updates*** screen allows the user to view pending updates for installed devices.

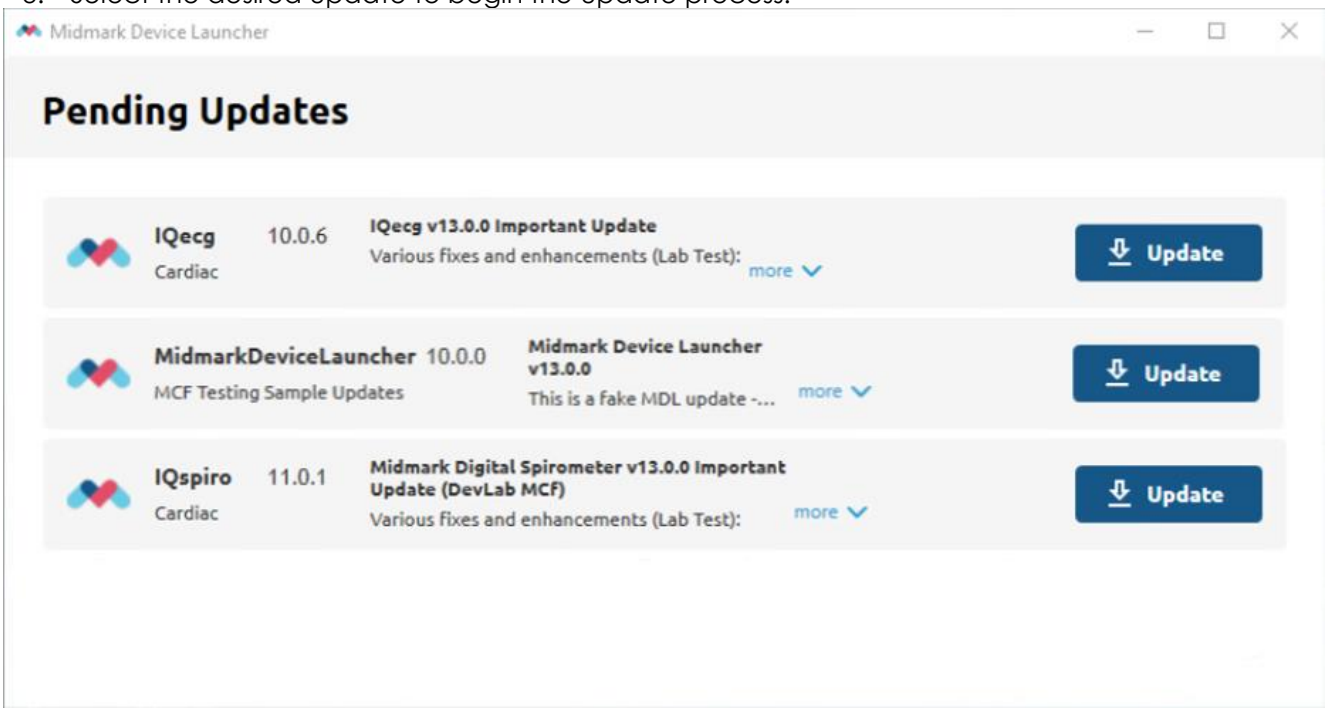
1. Right click on the MDL icon in the System tray.



2. Select the **Update** button to view the pending updates



3. Select the desired update to begin the update process.



Operation

Midmark Connection for Epic Operation

Starting Midmark Connect

The application should be running in the system tray and say 'connected'. If it is in the system tray, but says it is 'disconnected', please see <troubleshooting portion>. If it is not present in the system tray, start the application by double clicking on the shortcut created on the desktop after the application is installed successfully.

Patient Search Screen

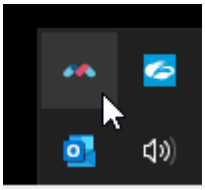
Please see Epic's documentation for details on how to search for and select patients using Epic Hyperdrive or Hyperspace.

Offline Mode

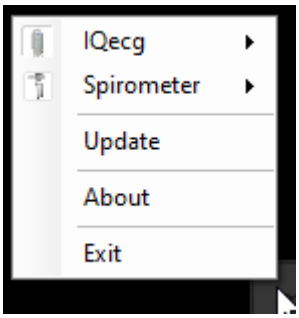
Midmark Connect for Epic can be used to start plugins in Offline mode. Access this feature by following the steps below:

NOTICE	Offline tests are NOT saved to Epic. Instead, they are saved locally on the computer performing the test.

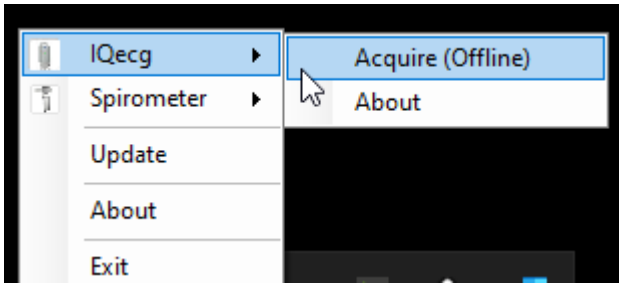
1. Find the MDL icon in the System Tray



2. Right click on the MDL icon and select the desired plugin.



3. Hover over the desired plugin, then click on **Acquire (Offline Mode)** to start the plugin in offline mode.



Device Operation

The software allows for tests acquisition using supported Midmark devices. Refer to the Related Documents section to view a list of Operation Manuals which contain instructions on how to use each applicable Midmark device.

Start Test

There are two ways to start a device test using Midmark Connect, directly from Epic or directly from the app in Offline Mode, see **Offline Mode** above and note Offline Mode will NOT save to Epic. Please review Epic's documentation for details on how to start a test directly from Epic.

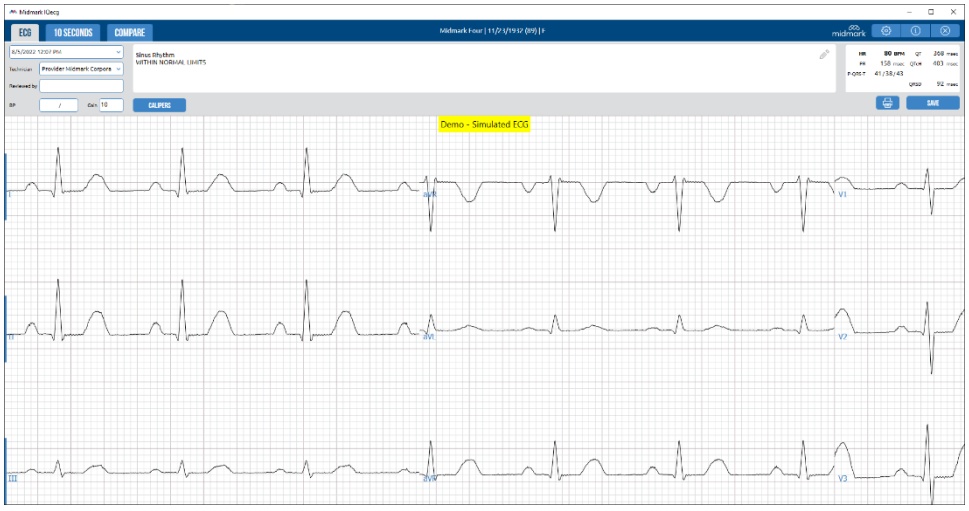
ECG Acquisition

The Midmark IQecg software can be used to generate resting 12-lead ECGs along with R-R Variability (Rhythm) reports.

> ***Note***
> *Refer to the Midmark IQecg Operation Manual for instructions on how to operate this device.*

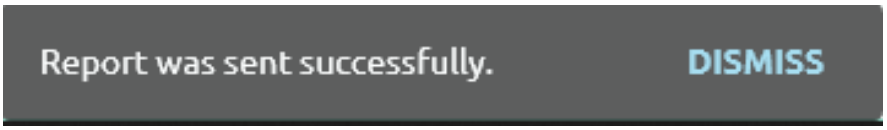
1. Follow the steps in the Start Test section to acquire device data.
2. Perform the test when the plugin opens by selecting **Acquire** on the plugin.

3. After the test is complete, click **SAVE** on the review screen to store the test data in the patient's records.

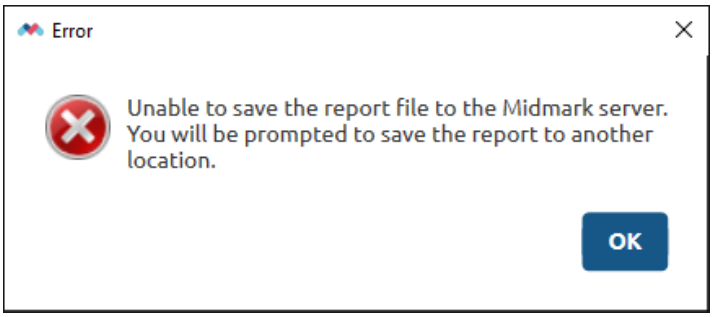


4. A pop-up window will display a message indicating that the report is being sent to Epic.

5. A message will display in the following window indicating that the report was saved successfully.



6. If the report fails to send to Epic, the following message will appear, and the report will be saved at the chosen location. This report will not be sent back to Epic.



Please refer to the **Review Report** section below for details on how to review saved reports.

Vital Signs Acquisition

The vital signs device will acquire blood pressure, pulse, temperature, weight, height, SpO_2, respiratory rate, and pain score. Vital Signs can be acquired from within the Epic workflow using the IQiE EMR software. Please refer to the IQiE operation manual for details on how to configure and run IQvitals through IQiE.

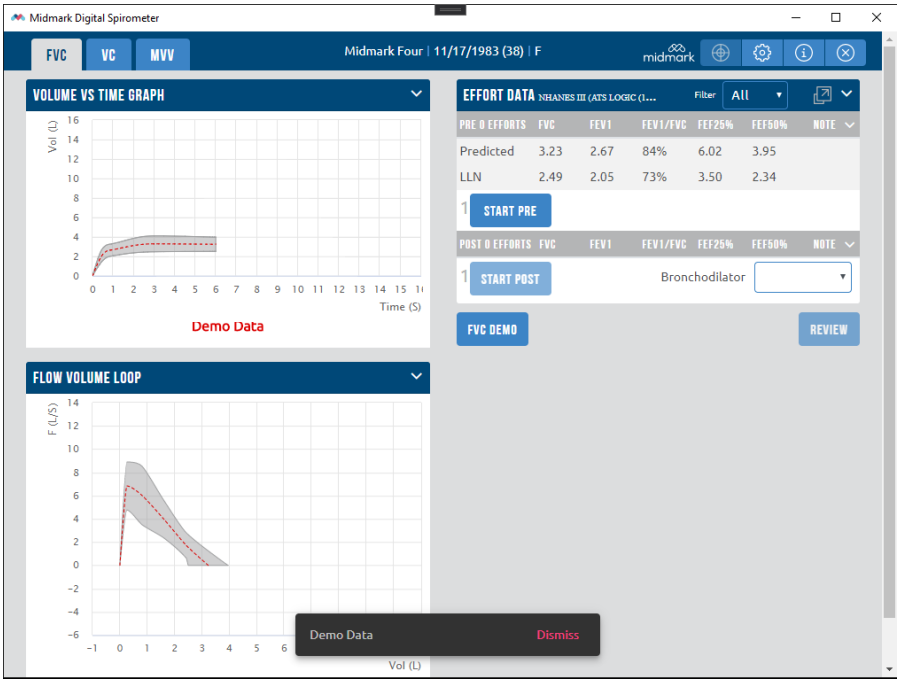
> ***Note***
> *Refer to the Midmark Digital Vital Signs Device or IQvitals® Zone Operation Manuals for instructions on how to operate these devices.*

Spirometry Acquisition

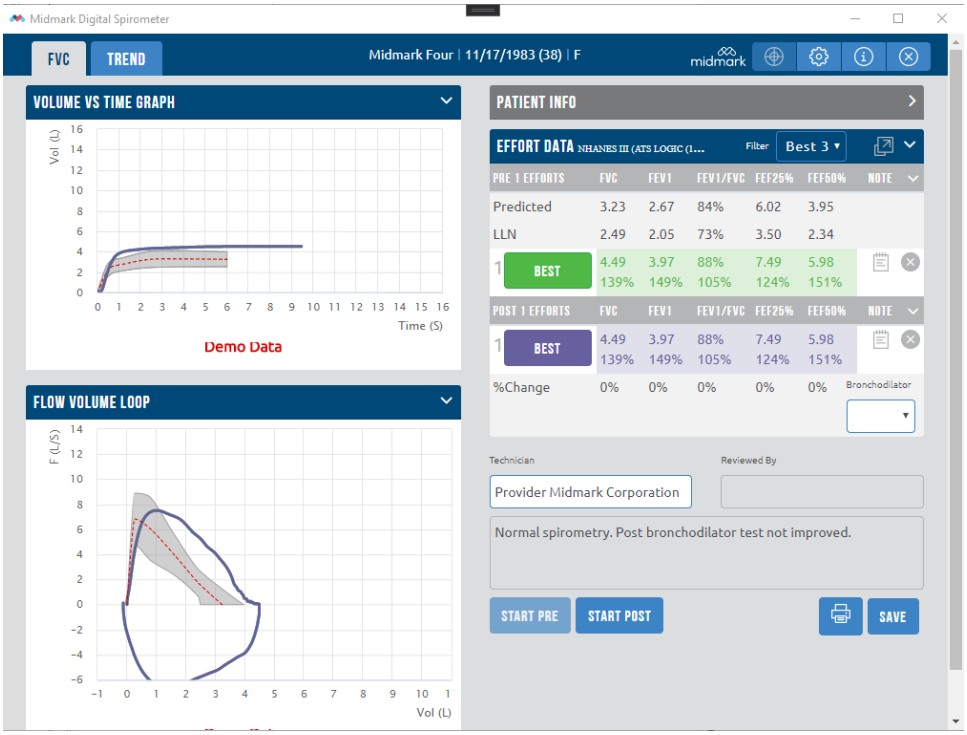
The Midmark Digital Spirometer software can be used to generate FVC, VC, and MVV reports, supporting Pre and Post Bronchodilator efforts.

> ***Note***
> *Refer to the Midmark Digital Spirometer Operation Manual for instructions on how to operate this device.*

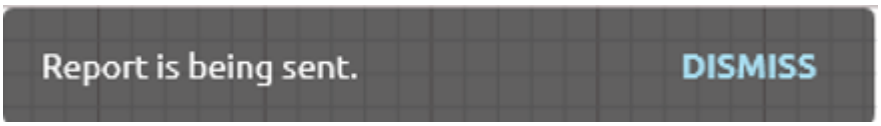
1. Follow the steps in the Start Test section to acquire device data.
2. Perform the test when the plugin opens by selecting **START PRE** on the plugin.



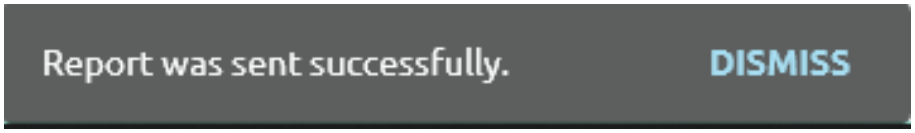
3. After the test is complete, click **SAVE** on the review screen to store the test data in the patient's records.



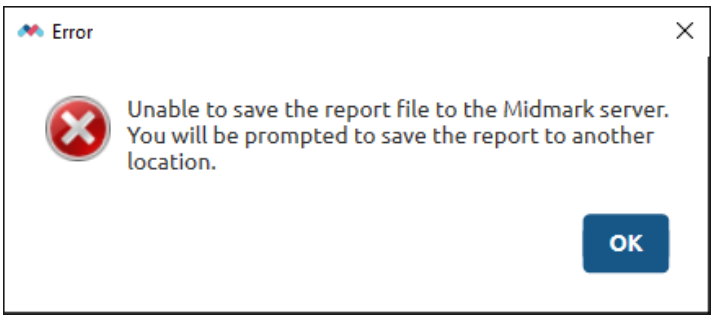
4. A pop-up window will display a message indicating that the report is being sent to Epic.



5. A message will display in the following window indicating if the report was saved successfully.



6. If the report fails to send to Epic, the following message will appear, and the report will be saved at the chosen location. This report will not be sent back to Epic.



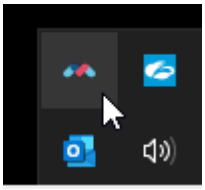
Please refer to the **Review Report** section below for details on how to review saved reports.

Calibration

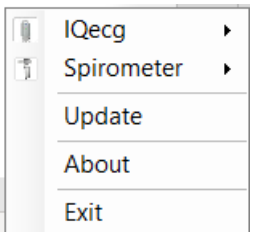
The Calibration can be started in a Spirometer acquisition by selecting the Calibrate icon at the top.

The Calibration can also be started directly from the MDL application

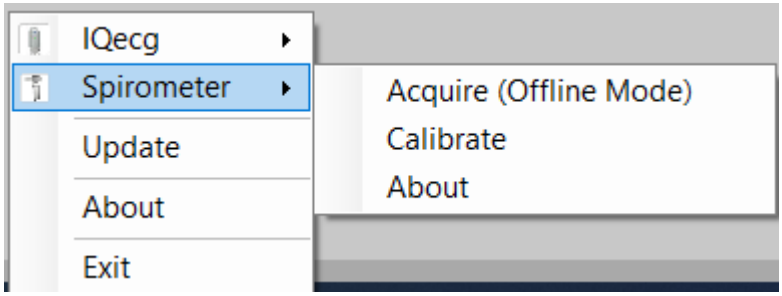
1. Find the MDL icon in the System Tray



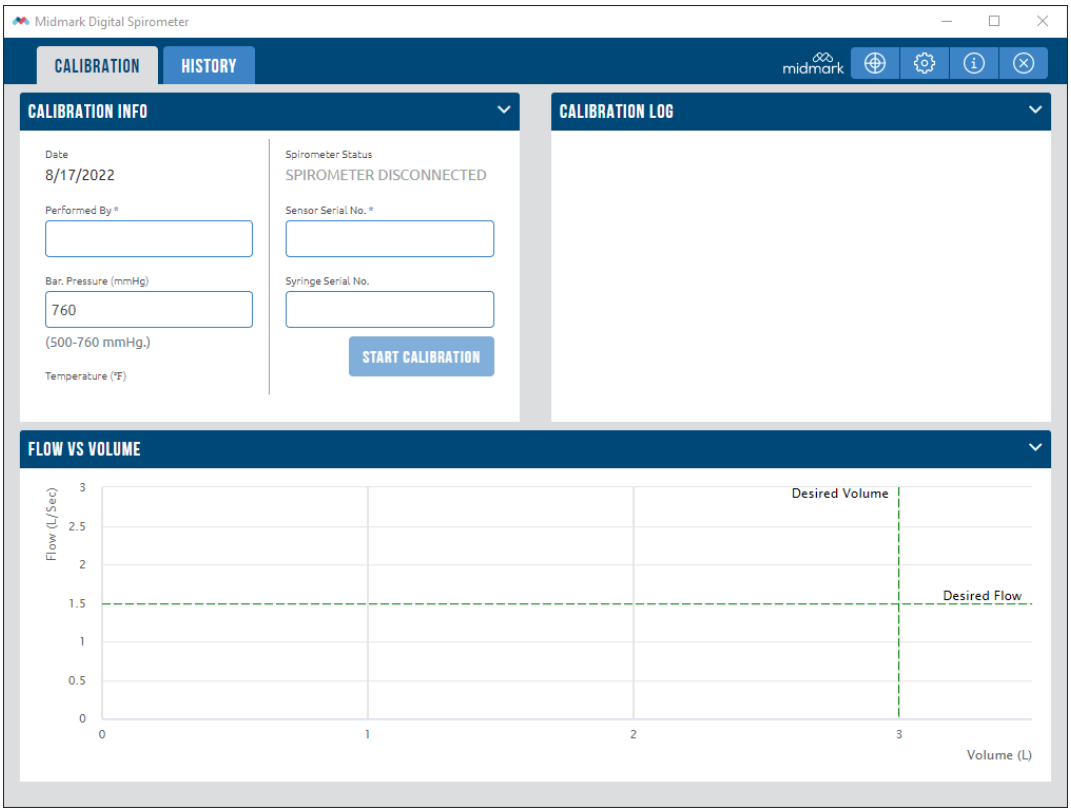
2. Right click on the MDL icon and hover over the **Spirometer** plugin.



3. Click on **Calibrate** to start the calibration procedure. The calibration screen will then be displayed.



> ***Note***
> *Refer to the Midmark Digital Spirometer Operation Manual for instructions on how to operate this device, including calibration*



Report Review

Reviewing reports is performed from within Epic. Please refer to Epic's documentation for more information on how to review a Midmark report.

> ***Note***
> *Please refer to the relevant documents under Related Documents for additional information on how to review Midmark devices' reports.*

Report Review (Offline Mode)

Reviewing reports saved while in Offline Mode is accomplished by double clicking on the saved CAR file. The report will open in the appropriate plugin software but will not be saved back to Epic. Any edits which are saved in review mode will be saved back to the CAR file.

> ***Note***
> *Please refer to the relevant documents under Related Documents for additional information on how to review Midmark devices' reports.*

Appendices

Appendix A – Using Midmark Connect with a Secure Connection (HTTPS)

HTTPS is a secure communications channel that is used to exchange information between a client computer and a server. It uses Secure Sockets Layer (SSL). The information listed below will discuss setting up an HTTPS environment.

SSL Certificate

SSL must be enabled to use HTTPS. To enable SSL in IIS, one must first obtain an SSL certificate. This certificate is used to encrypt and decrypt the information that is transferred over the network.

For more details on requesting and installing an SSL certificate please refer to the following Microsoft article, http://support.microsoft.com/kb/299875.

> ***Note***
> *If the SSL certificate is referencing the server by the fully qualified domain name (FQDN) then all the references to the server must be referenced by the FQDN also. See sections II.B.7 and II.C.4.*

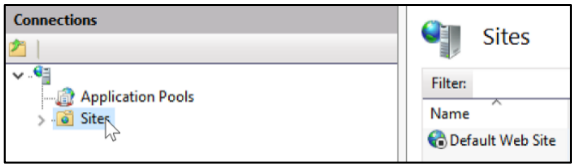
> ***Note***
> *The SSL certificate must be trusted on the client computer. Any certificate error must be resolved before using the interface.*

Configuring Midmark WebService to use HTTPS in IIS

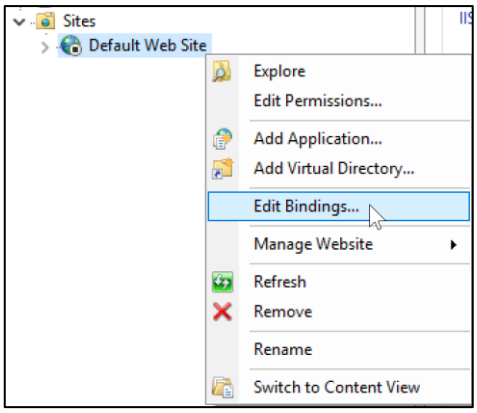
1. Log on to the Midmark server that hosts the WebService.
2. Click **Start**, click **Settings**, and then click **Control Panel**.
3. Double-click **Administrative Tools**, and then double-click **Internet Information Services (IIS) Manager**.

Using IIS 7.0

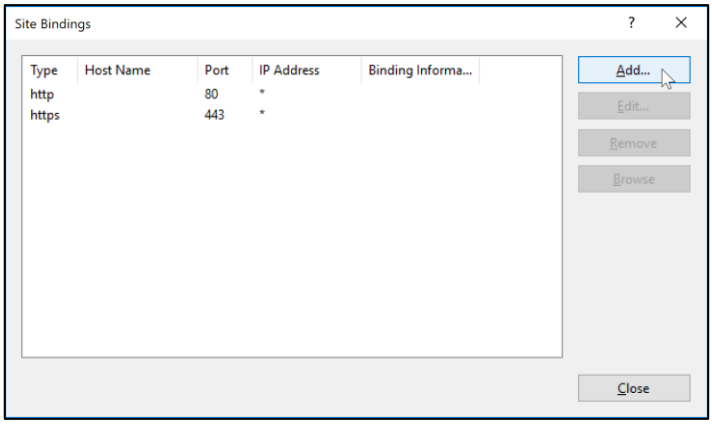
1. Click on the **Sites** folder to expand it.



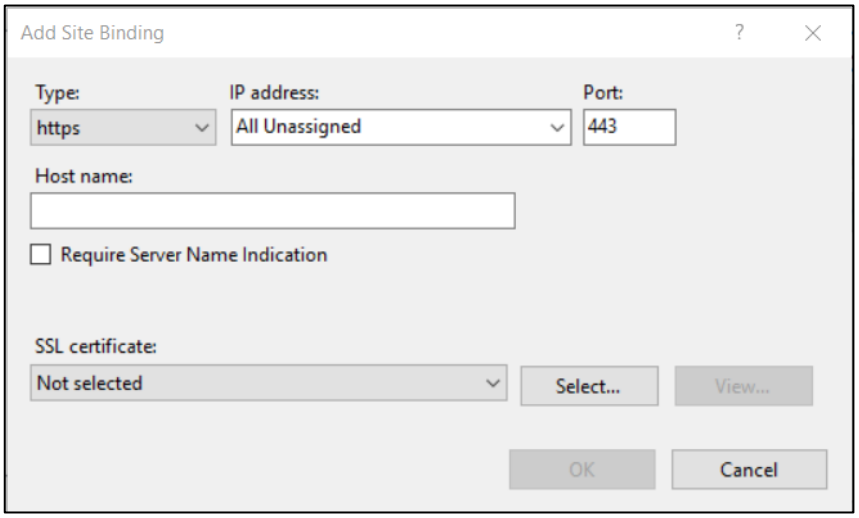
2. Right click on **Default Web Site** and choose the **Edit Bindings** option.



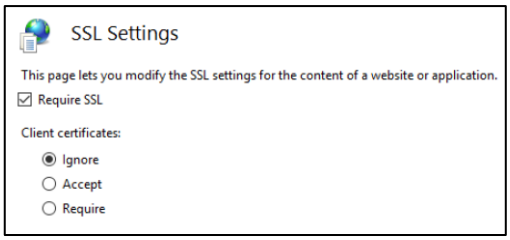
3. Click on **Add**.



4. Choose **HTTPS** as the SSL certificate from the *Type* drop-down list.



5. Select the certificate from **SSL certificate** drop down.
6. Click **OK** and then click **Close** to return to the IIS Manager.
7. Double-click **SSL Settings** in the middle panel. Place a checkmark in **Require SSL** and choose **Ignore** Client certificates. Click on **Apply.**



8. Restart IIS by running the command **iisreset** on the Windows **Run** application.

Appendix B – Understanding and Editing MidmarkMDL.exe.config File Settings

Understanding the MidmarkMDL.exe.config File Settings

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <!-- For more information on Entity Framework configuration, visit http://go.microsoft.com/fwlink/?LinkID=237468 -->
    <section name="entityFramework"
      type="System.Data.Entity.Internal.ConfigFile.EntityFrameworkSection, EntityFramework, Version=6.0.0.0,
      Culture=neutral, PublicKeyToken=b77a5c561934e089"
      requirePermission="false"/>
  </configSections>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.6.2"/>
  </startup>
  <appSettings>
    <add key="ConfigurationRootFolder" value=""/>
    <add key="SettingsRootFolder" value=""/>
    <add key="CommonSettingsSite" value=""/>
    <add key="MCFWebServerURL" value="localhost:44360/" />
    <add key="MCFMiddlewareURL" value="localhost:44385/" />
    <add key="UseSharedSettings" value="false"/>
    <add key="PluginsFolder" value=".\Plugins"/>
    <add key="ReportManagersFolder" value=".\ReportManagers"/>
    <add key="CARFileFolder" value="C:\CARFiles"/>
    <add key="ClientSettingsProvider.ServiceUri" value=""/>
    <add key="DemoMode" value="false"/>
    <add key="HttpListenerPort" value="6436"/>
    <add key="MCFDomainName" value="sample.domain.net" />
    <add key="IsPdfServer" value="false"/>
      <add key="BrowserProcess" value="chrome"/>
    <add key="DoHideBrowser" value="true"/>
    <add key="BrowserWaitInMsec" value="10000"/>
    <add key="BrowserExtraOpenArgs" value=""/>
```

The following settings should be customized for each organization.

Configuration Setting	Description
ConfigurationRootFolder	The root configuration folder in which the configuration file exists. Not currently used.
SettingsRootFolder	The root directory inside which the site folder that will contain the settings file is created.
CommonSettingsSite	The name of the site folder inside which the settings file is created and saved.
MCFWebServerURL	The URL that the MDL will use to connect to the Midmark Connect for Epic Web Server.
MCFMiddlewareURL	The URL that the MDL will use to connect to the Midmark Connect for Epic Middleware.
UseSharedSettings	The parameter that determines whether the MDL will use a shared location to access the settings file.
PluginsFolder	The Plugins folder directory that contains the plugin files.
ReportManagersFolder	The directory that contains the ReportManager files.
CARFileFolder	The directory that will contain the CAR files. Not currently used.
ClientSettingsProvider.ServiceUri	The URL used to get all machine client settings from a RESTful API call. Not currently used.
DemoMode	Determines if the Midmark Device Launcher will run in Demo mode or not.
HttpListenerPort	The HTTP Listener Port assigned to the Midmark Device Launcher.

MCFDomainName	The network domain to be used by the Midmark Device launcher.
IsPdfServer	Determines if the Midmark Device Launcher will be used as a PDF server.
BrowserProcess	Determines which browser the MDL uses to identify itself to the MCF server end. Must match the default browser used in Windows.
DoHideBrowser	Determines if the browser window opened for the MDL to identify itself will be hidden after launching Midmark Connect for Epic.
BrowserWaitInMsec	Determines the time to wait before closing the browser after starting Midmark Connect for Epic.
BrowserExtraOpenArgs	Used for advanced use cases when the MDL identifies itself.

Appendix C – Understanding Client Side MidmarkMDL.exe.config File Settings

Settings File Path

Every component of Midmark Connect stores settings files in a subdirectory of a root settings folder. This root settings folder could look similar to this: *<settingsrootfolder>\<site>\<user>, depending on your setup.*

The *<settingsrootfolder>* is specified in the application config file. It is set at installation time and can be modified by editing the .config file directly. By default, *<settingsrootfolder>* is **C:\Program Data\Midmark\IQconnect**.

The *<site>* is a text string representing a site and also contained in the .config file. By default, *<site>* is just the word **Site**, where all sites share this **Site** directory and if each site is looking at the same *<settingsrootfolder>* then they are sharing settings.

The *<user>* is the Windows authenticated username. By default, the settings will be under **C:\Program Data\Midmark\IQconnect\Site\jdoe**, assuming **jdoe** is the username of the currently logged in user.

Each component of the application creates a subdirectory underneath *<settingsrootfolder>\<site>\<user>* to save settings specific to that component. For instance, directories created for Midmark Connect for Epic, IQecg, Midmark Digital Spirometer, etc.

To change the settings inheritance, locate the **MidmarkMDL.exe.config** file which is located in the Midmark MDL directory by default. In the *<appsettings>* section of the **MidmarkMDL.exe.config** file, there are three keys that can be manually edited to control the settings inheritance.

SettingsRootFolder <settingsrootfolder>

The *<SettingsRootFolder>* key under the *<appsettings>* section can be edited.

<add key="SettingsRootFolder" value=""/>

If left blank, the default of **C:\ProgramData\Midmark\IQconnect** is used.

The most common reason for changing this value is to put it in a network shared folder if this was not specified during installation. If all the computers are configured to use the same network resource, then the user's settings will follow them from computer to computer.

CommonSettingsSite <site>

The *<CommonSettingsSite>* key under the <appsettings> section can be edited.

<add key="CommonSettingsSite" value=""/>

If left blank, the default of **Site** is used and all sites share this path, resulting in a common setting for all sites.

Setting the value will allow all users of this computer to share the same site. If the computers in Site A all used **SiteA** as the *<CommonSettingsSite>* key, and the computers in Site B all used **SiteB** as the *<CommonSettingsSite>* key, then each site would have their own settings.

UseSharedSettings <user>

The *<UseSharedSettings>* key under the *<appsettings>* section can be edited.

<add key="UseSharedSettings" value="false"/>

Setting the value to true will force the software to no longer save setting by user, instead the settings will be shared among all users who have access to that same *<settingsrootfolder>*. The *<user>* portion of the path

will not be used and all settings will be stored in the root of the settings folder, <settingsrootfolder>.

Setting the value to false will force the software to use each user's individual settings. The *<user>* portion of the path will be the users Windows authenticated username.

Common Uses

Scenario - all users have their own settings that follow them throughout the organization.

To configure this scenario,

<SettingsRootFolder> is set to a common location (*//SharedServer/Midmark/Settings*).

<CommonSettingsSite> is set to a common site (left as default value, "").

<UseSharedSettings> is set to "false".

Scenario – all users share the same settings throughout the organization.

To configure this scenario,

<SettingsRootFolder> is set to a common location (*//SharedServer/Midmark/Settings*).

<CommonSettingsSite> is set to a common site (left as default value, "").

<UseSharedSettings> is set to "true".

Appendix D – Using Midmark Devices in Thin Client

Thin Client Configuration

Midmark Connect for Epic supports the IQpath™ Software Solution for thin client configurations.

The IQpath software allows for real time tests ran with Midmark devices to be used in a thin client environment. In this Software environment, Midmark Connect must be installed on the Terminal Server and Midmark devices operated through a thin client terminal.

> ***Note***
> *Setting up any application in a network environment typically requires special access rights and knowledge of the network. Please have the system administrator install and configure the application to the office environment.*

1. Load Midmark Connect on the terminal server.
2. Install one of the following software components on each client computer intended to be used for data acquisition:
   - **IQpath™ for Microsoft Terminal Services:** if using Microsoft Terminal Services (Microsoft RDP). **Not currently supported for Midmark Connect for Epic.**
   - **IQpath™ for Citrix ICA:** if using Citrix® software on the clients and servers.
   - **IQpath™ for VMware:** if using VMware VDI software on the clients and servers.

   These software products are provided separately and may be obtained by contacting Midmark Technical Service.
3. Once the software is installed on the client server network and computers, configure the application for thin client operation as described in Using Midmark Devices with IQpath.

Thin Client Using IQpath™ Software

The IQpath™ Software works with the Midmark devices in high-latency, limited bandwidth, network configurations with Windows-based PC clients.

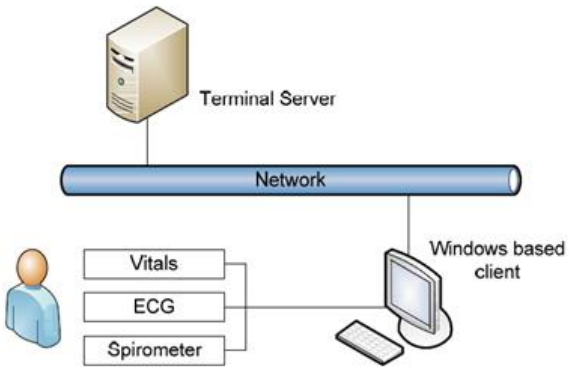
IQpath™ utilizes a dedicated flow control scheme to provide the following advantages over COM port mapping:

- Improved operation over high-latency, low bandwidth, high-loss networks:
  - Microsoft Terminal Services: Improvement is approximately 10 to 1 in latency tolerance.
  - VMware VDI: Improvement is approximately 10 to 1 in latency tolerance.
  - Citrix® ICA® protocol: Improvement is approximately 40 to 1 in latency tolerance.
- No COM port mapping is required.
- The USB versions of IQecg®, Midmark Digital Spirometer, IQvitals®, and IQvitals® Zone™ devices are compatible.
- The BLE versions of IQvitals® Zone™ devices are compatible.
- Improved device auto-configuration and diagnostics.

Note
IQpath™ has specific requirements for computer hardware, software, and network performance. System administrators should read the ***Setup Manual: Midmark Products over Thin Client using IQpath™ or COM port mapping*** *before installing, configuring, and using this software in a thin client environment. See the Related Documents section for additional information.*

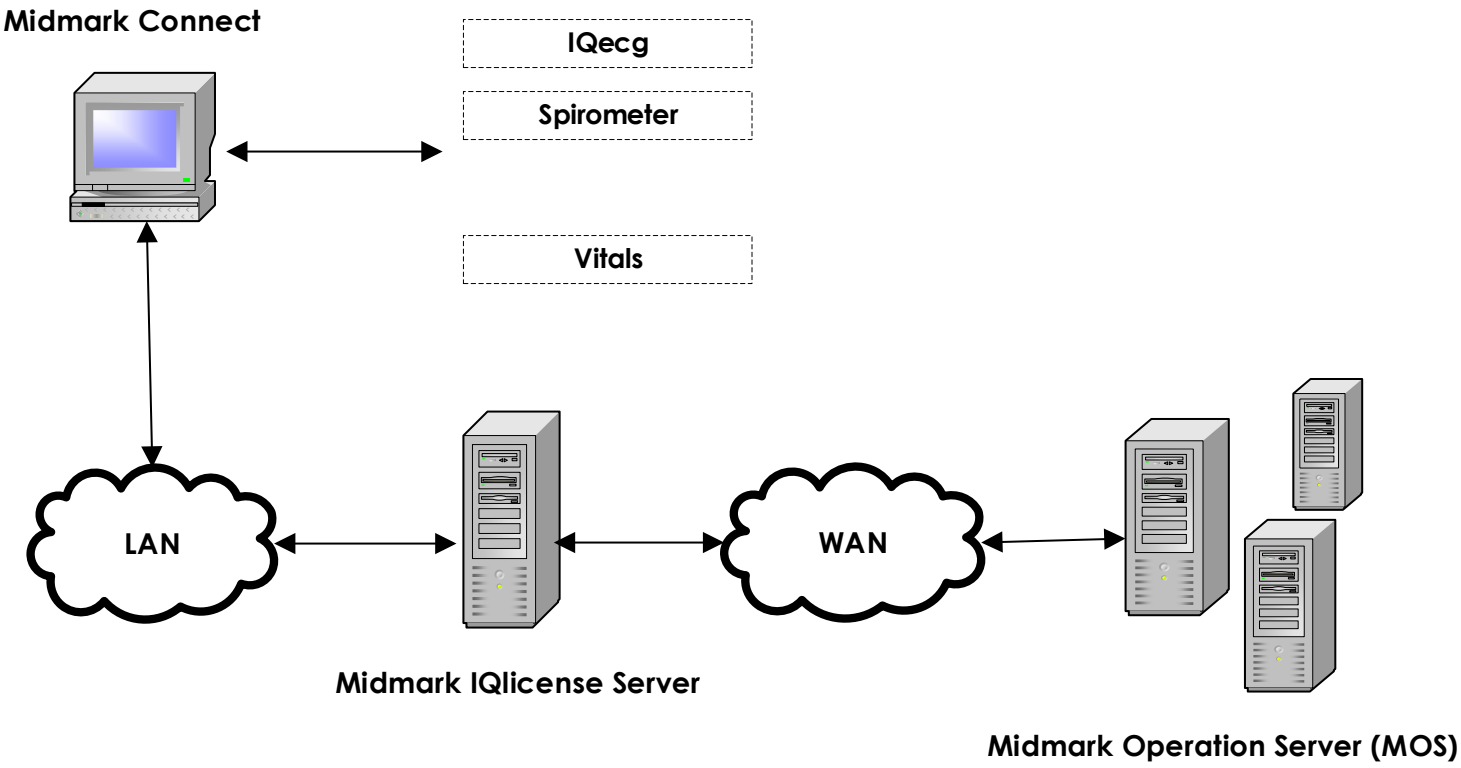
Using Midmark Devices with IQpath

The figure below illustrates IQpath™. In this thin client environment, the client computers must be running a compatible version of Windows®:



1. Depending on the version of Midmark device controls, the IQpath software will be automatically detected and does not need to be configured. If using a version that does not support this workflow, there will be an option to choose the IQpath setting from the device settings screen.
2. Click the **Settings** Icon on the top bar of the appropriate device software.
3. Under the **Common Settings** group, select the **Thin Client Settings** drop down and choose the appropriate thin client option corresponding to the IQpath software installed. Note that Midmark devices inherit these **Common Settings**, but they can be overridden selecting a different option from the drop-down menu.
4. Click **SAVE** on top to accept changes.

Appendix E – Midmark IQLicense and Configuration

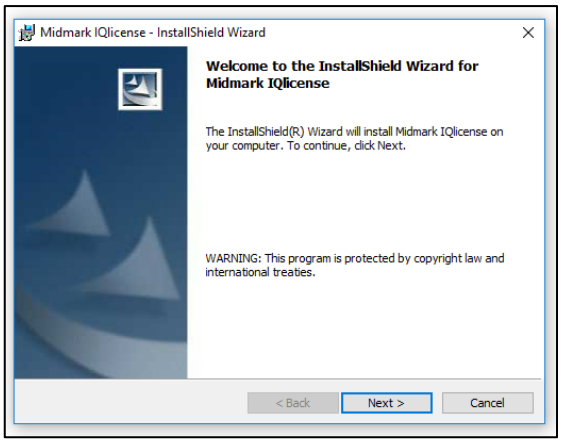


Installing Midmark IQlicense Server Software

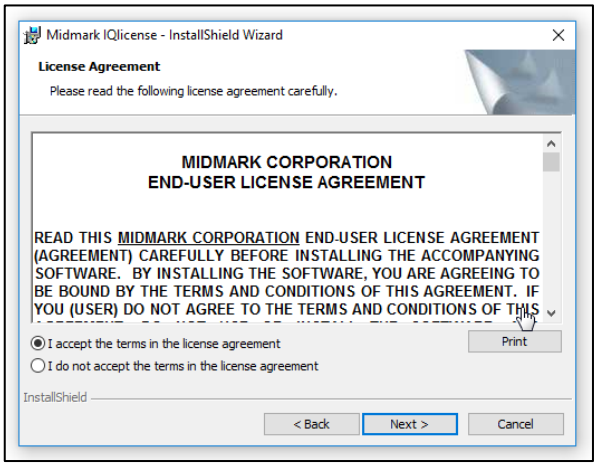
> ***Note***
> *Midmark IQLicense Server Software requires VC++ 2013 (x86) runtime and runtime v12.0.30501 is distributed with the software. If issues are encountered when installing the runtime or require a later version of the runtime, download, and reinstall the runtime from https://www.microsoft.com/en-us/download/details.aspx?id=40784.*

The Midmark IQlicense server must have access to the Internet in order to activate the license file from MOS (Midmark Operation Server), and the server must be reachable from the workstation/server where the Midmark Connect software is installed (it may also be the same computer).

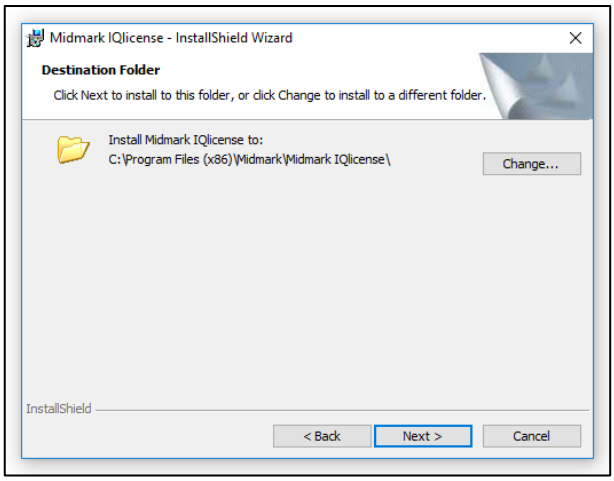
1. Identify where to install the Midmark IQlicense server software (workstation or server).
2. Open the Server Software folder in the Midmark Connect for Epic Installation package.
3. Open the IQlicense folder.
4. Launch the setup file and follow the prompts on the screen.
   4.1. Click **Next** to begin the installation of the IQlicense® software.



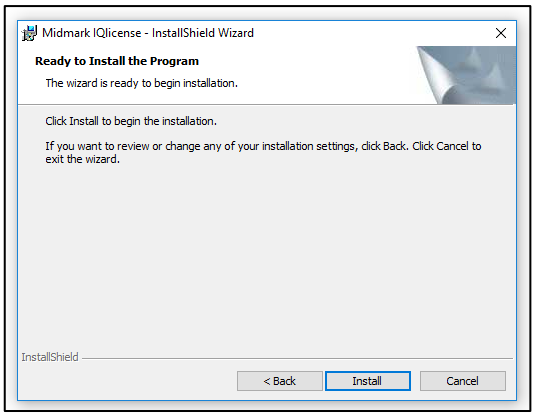
4.2. At the license agreement window, select **I accept the terms in the license agreement** and click **Next** to continue with the installation.



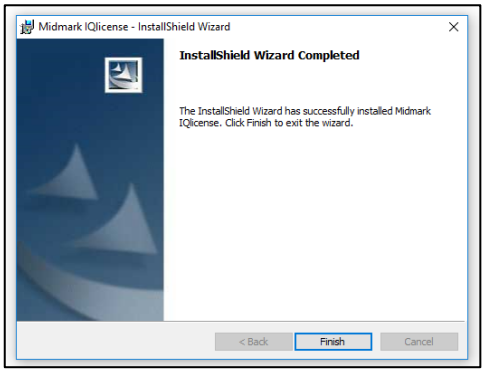
4.3. If desired, click **Change** to change installation directory and then click **Next** to continue with installation.



4.4. Click **Install** to begin the IQlicense® software installation.



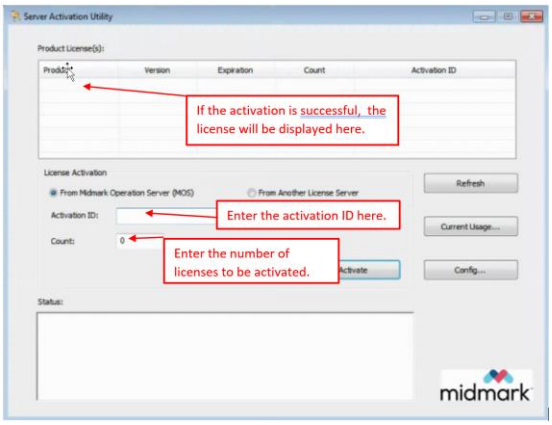
4.5. The following window will appear indicating that the IQlicense® software has been successfully installed. Click **Finish** to complete installation.



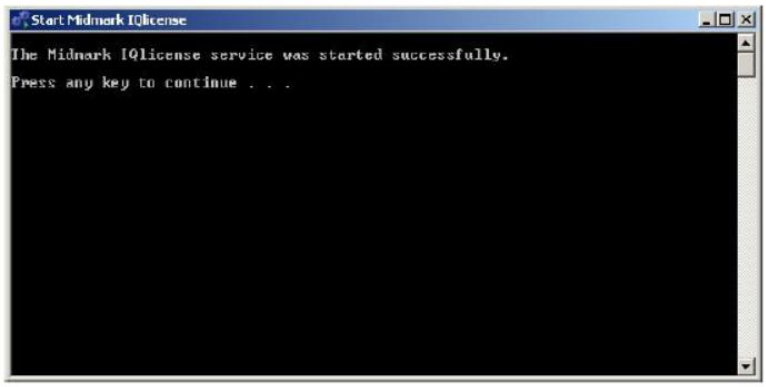
License Activation and configuration

1. To activate the license, launch the **Server Activation Utility** from the Windows® **Start Menu** > **Programs** > **Midmark IQlicense** program group.

2. Once the **Server Activation Utility** is displayed, enter the **Activation ID**. Under "**Count**," enter the **number of licenses** that have been purchased, and then click the **Activate** button.



3. Navigate to **Programs** > Click **Midmark IQlicense**, then **right click Start Midmark IQlicense**, then click on **Run as Administrator**. The DOS prompt will state that the service has started successfully. **Press any key** to close the screen.

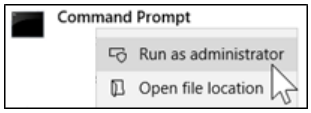


Appendix F – Silent Software Installation and Uninstall

The following information pertains to the silent install and uninstall of Midmark Connect for Epic. Please see the devices manuals for information on silent install and uninstall of the same.

Silent Installation

1. Run the Command Prompt as administrator by right clicking on the application and selecting the **Run as administrator** option:



2. Click on **Yes** on the **User Account Control** window.
3. Locate the directory where the application setup files have been downloaded and change the directory to that folder.
4. Type the following command at the prompt, editing the seven (3) parameters in bold with the correct information and press **Enter**:
5. After the silent installation, navigate to the Window system tray, the MDL application shall be visible

   MDL_setup.exe /s /v"/qn ACCEPT_EULA=Yes DOMAIN_NAME=enter_domain_name MCF_WEB_SERVER_URL=enter_web_server_url MCF_MIDDLEWARE_URL =enter_web_middleware_url"

   Here's the explanation of each parameter:

   1) ACCEPT_EULA

      Accepts End User License Agreement. Must be set to YES to install

   2) DOMAIN_NAME

      Organization's domain name

   3) MCF_WEB_SERVER_URL

      The Midmark Connect for Web Server URL

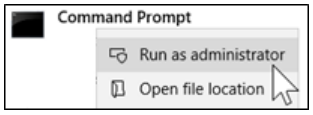
   4) MCF_MIDDLEWARE_URL

      The Midmark Connect for Web Middleware URL

6. Refer to the required device type's operation manual for steps on silently installing the required device software as these steps mentioned above only install the MDL software. To verify successful installation, open Programs and Features, under Control Panel, to verify the appropriate device plugins were installed.

Silent Uninstall

1. Run the Command Prompt as administrator by right clicking on the application and selecting the **Run as administrator** option:



2. Click on **Yes** on the **User Account Control** window.
3. Type the following command at the prompt and press **Enter**:

   msiexec /x {861849F1-6D53-4929-853F-93ABF09C8352**} /passive**

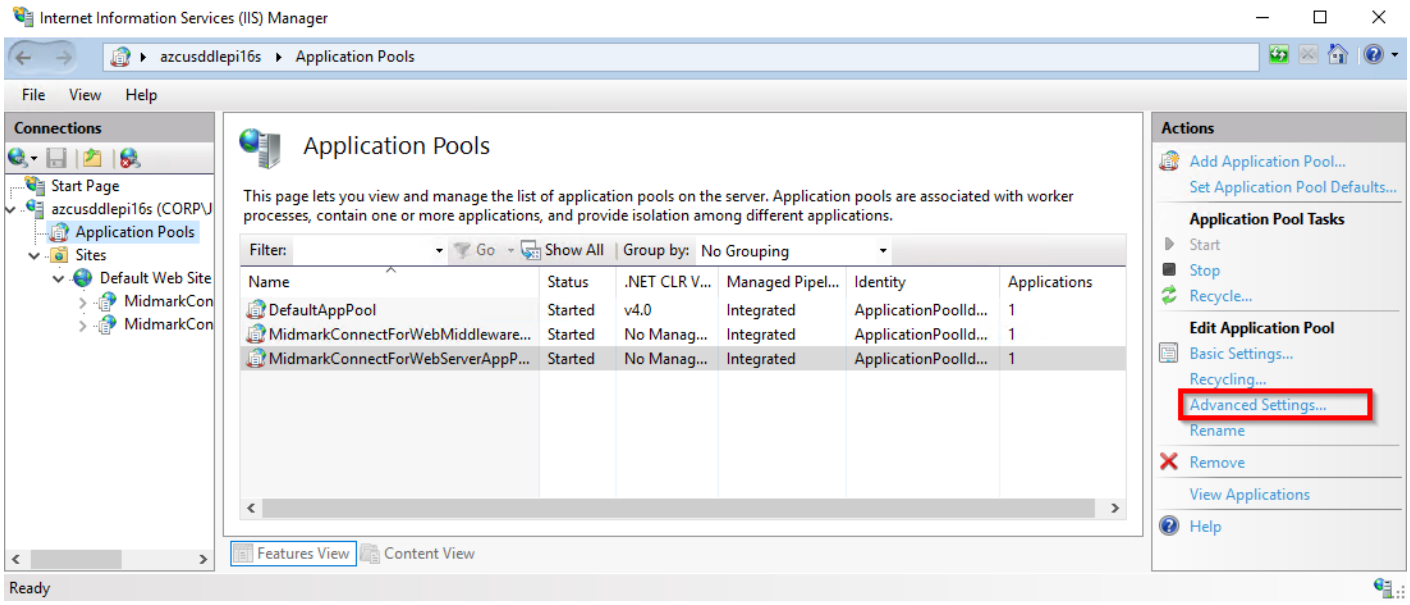
4. Open Programs and Features, under Control Panel, to verify that the appropriate device plugins were uninstalled.

Appendix G – Using SQL Server with Windows Authentication

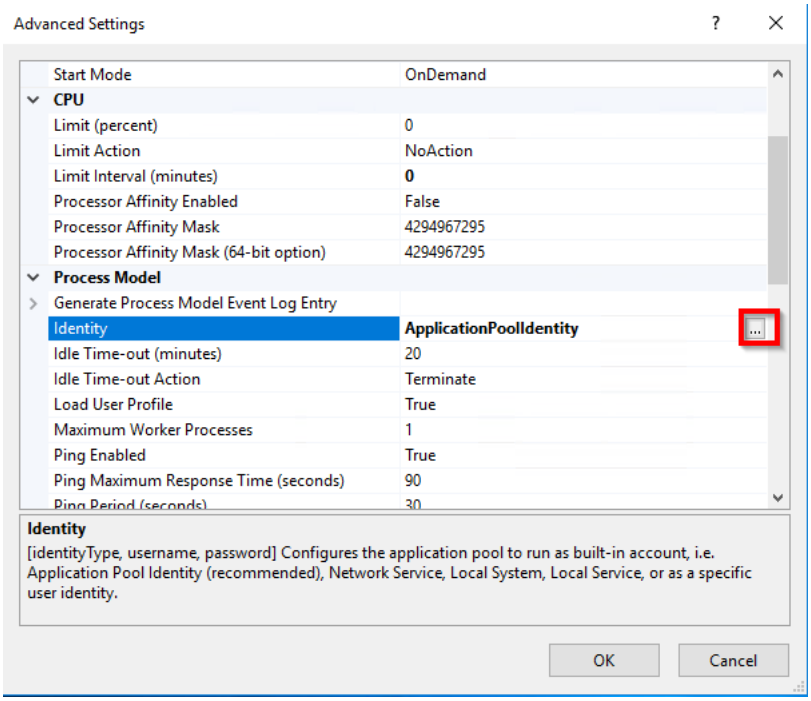
SQL Server with Windows Authentication should be possible to work out of the box. However, due to some previous SQL Server configurations. it could not. Please follow the steps below if there are any issues.

Change the **Identity** of **MidmarkConnectForWebMiddlewareAppPool and MidmarkConnectForWebServerAppPool** from the default "***ApplicationPoolIdentity***" to a service account that is a valid user of the ***MidmarkConnect_Epic*** database, as follows:

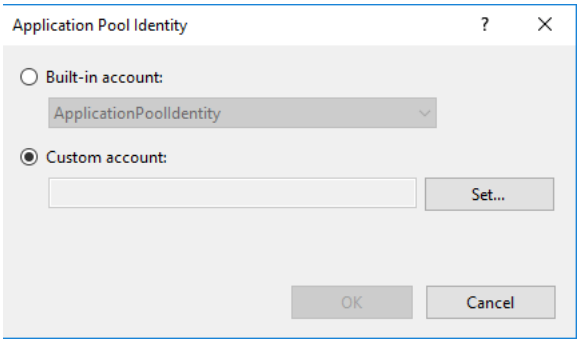
1. Select **MidmarkAppPool** and click **Advanced Settings**.



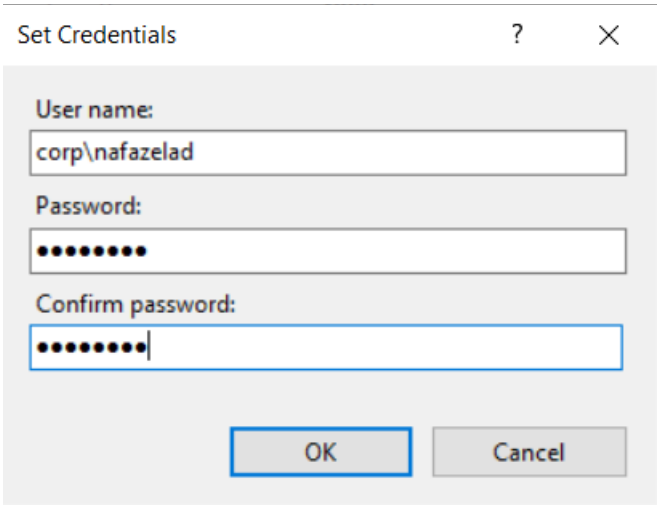
2. On the **Advanced Settings** dialog, click **Identity**, then click on the **…** button to open the **Application Pool Identity** dialog:



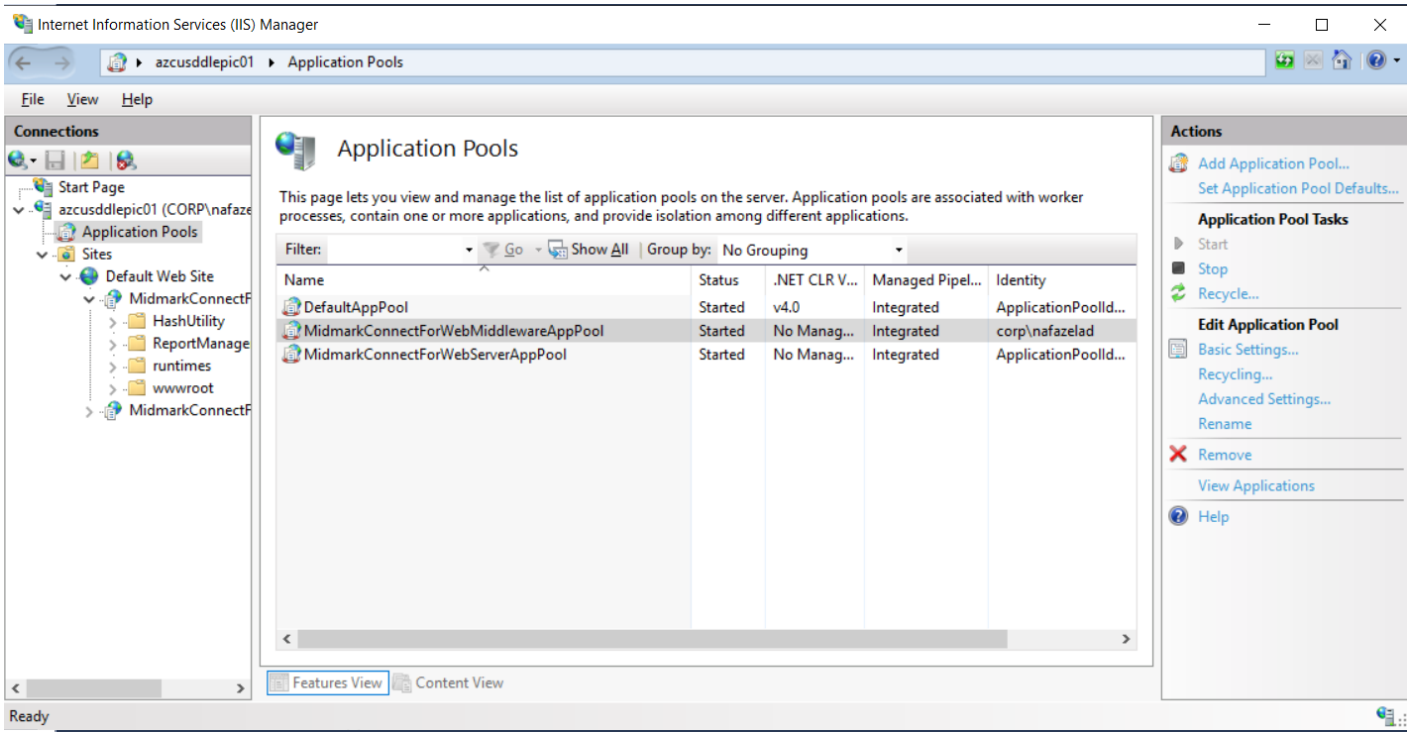
3. On the **Application Pool Identity** dialog, select **Custom account**, and then click the **Set…** button.



4. The **Set Credentials** dialog opens. Enter the user name and password of the service account that is a valid user of the *MidmarkConnect_Epic* database. Click OK to close the **Set Credentials** dialog.



5. Click **OK** again to close the **Application Pool Identity** dialog and then **OK** again to close the **Advanced Settings** dialog. Verify that the Identity of **MidmarkConnectForWebMiddlewareAppPool** has been changed to the service account:

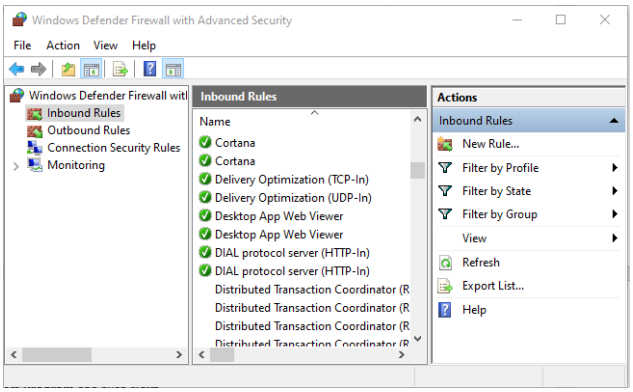


Reset IIS and apply same steps for MidmarkConnectForWebServerAppPool.

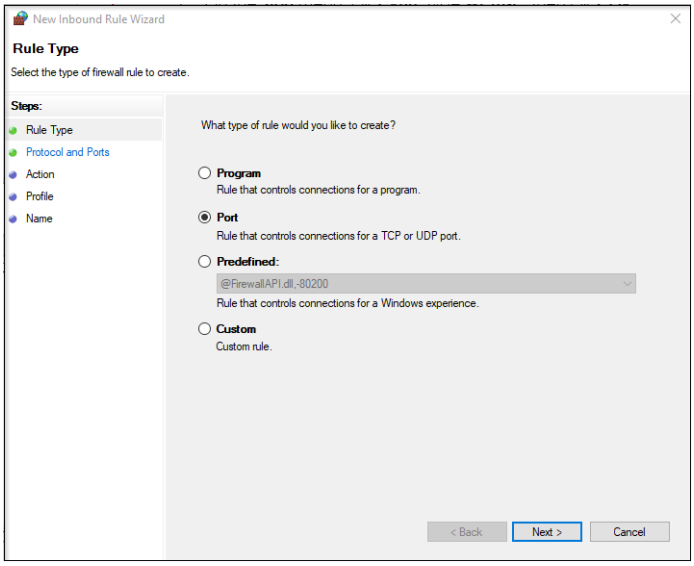
Appendix H – Configuring Windows Firewall for Midmark IQlicense

Please follow these steps to configure Windows firewall for IQlicense access:

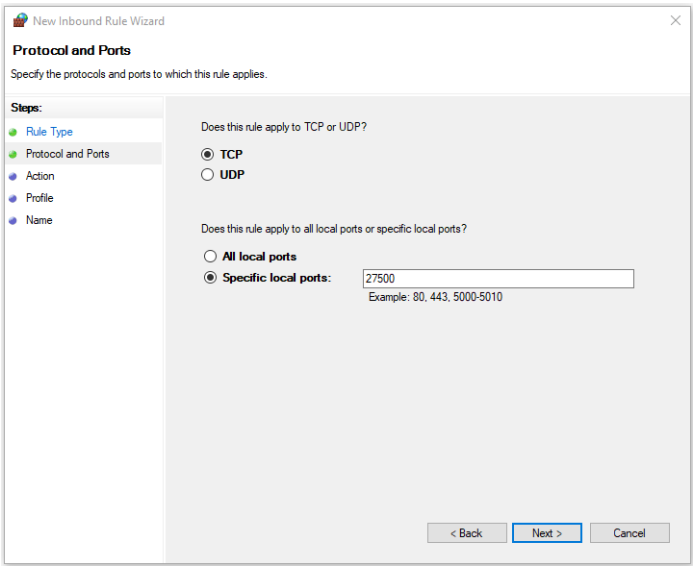
1. On the **Start** menu, click **Run**, type **WF.msc**, then click **OK.**
2. Click **Inbound Rules** in the left pane, then click **New Rule** in the right pane.



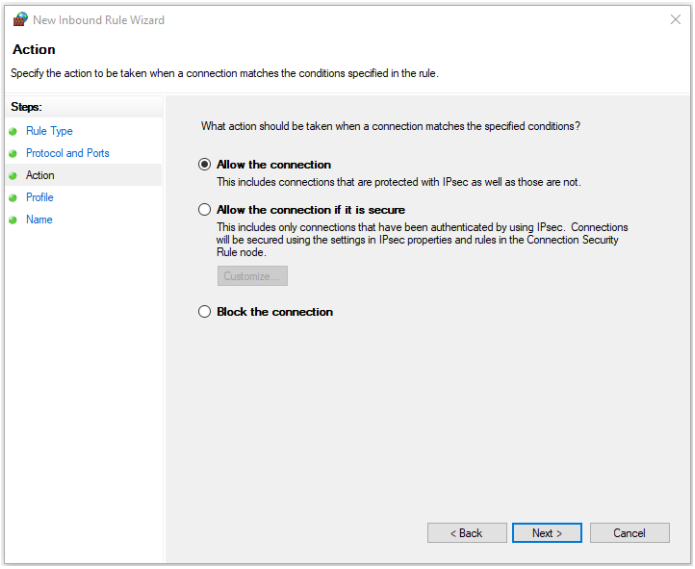
3. Select **Port** and click **Next.**



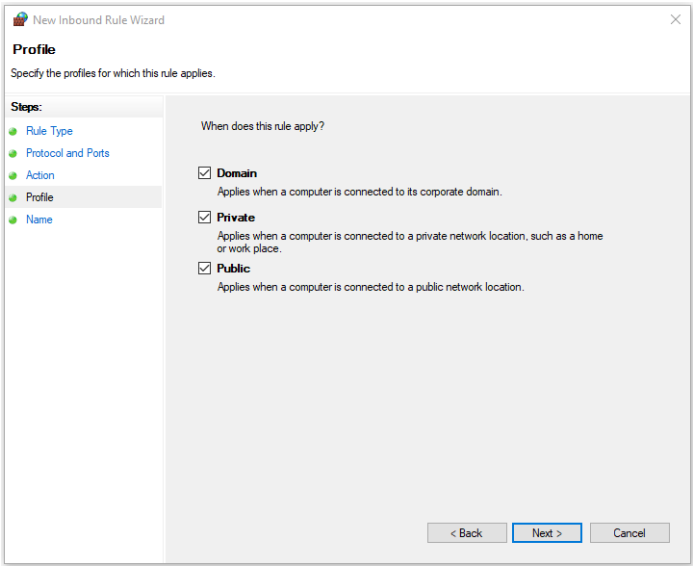
4. For **Specific Local Ports**, enter the port number **27500**, then click **Next.**



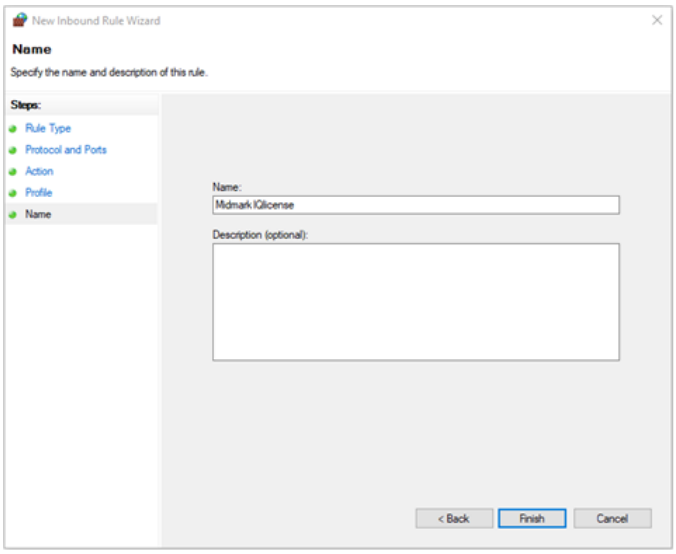
5. Select **Allow the connection**, and then click **Next.**



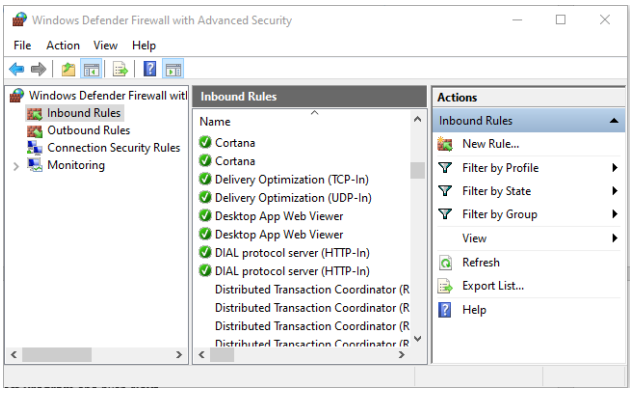
6. Select the profile(s) that matches your connection environment, and then click **Next.**



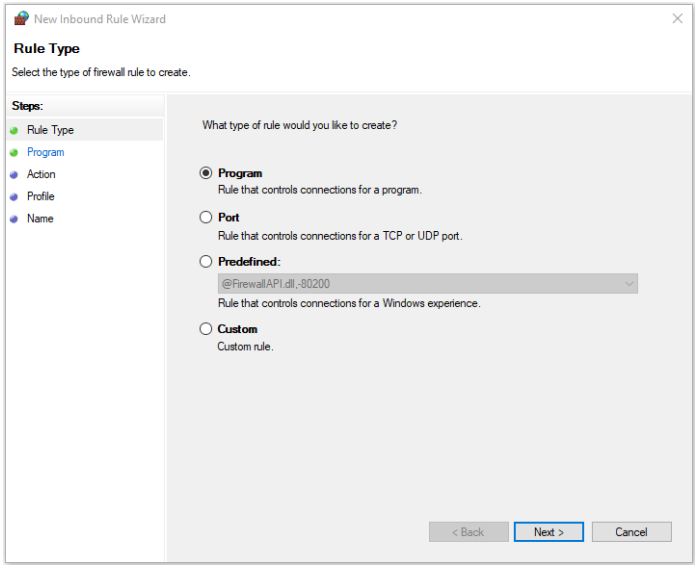
7. Enter the name **Midmark IQlicense**, and then click **Finish.**



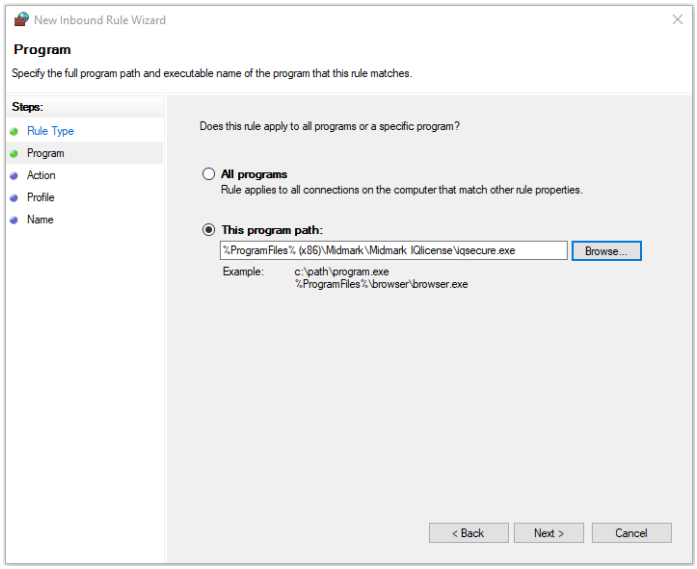
8. Click **Inbound Rules** in the left pane, then click **New Rule** in the right pane again.



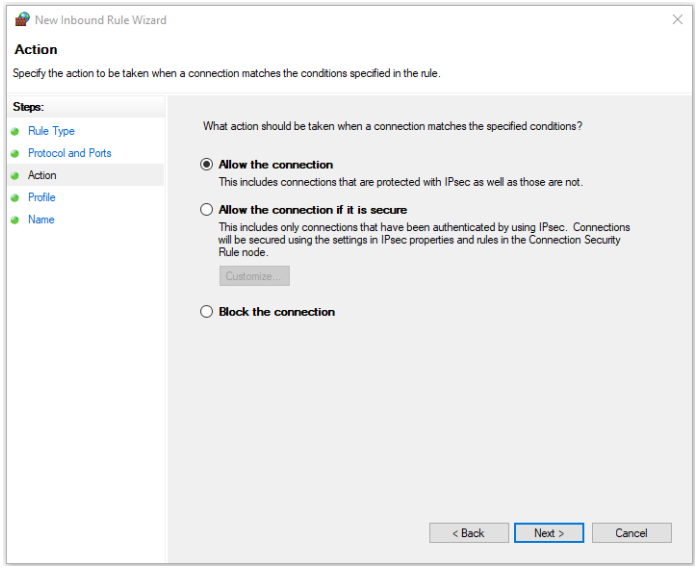
9. Select **Program** and click **Next.**



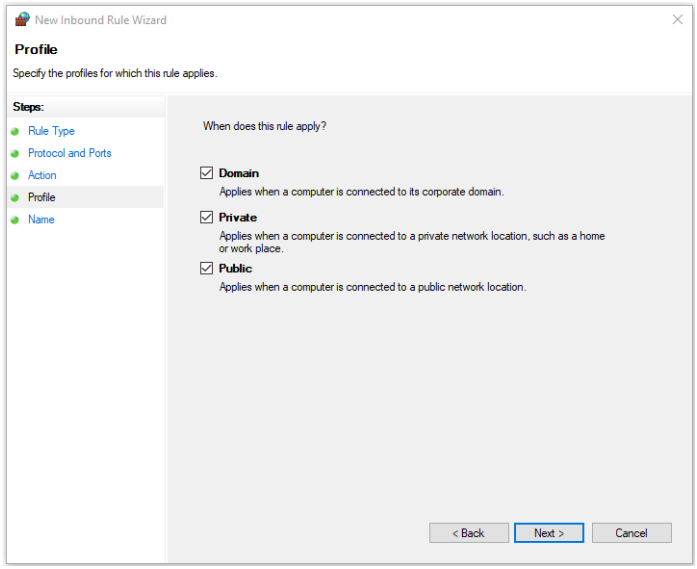
10. Browse to **C:\Program Files (x86)\Midmark\Midmark\IQlicense** and select **IQsecure.exe**, and then click **Next**.



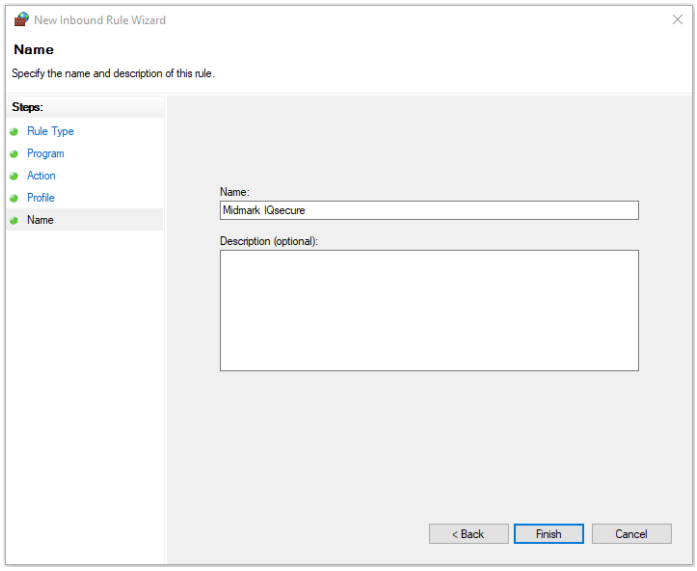
11. Select **Allow the connection**, and then click **Next.**



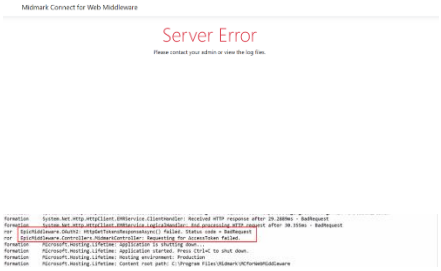
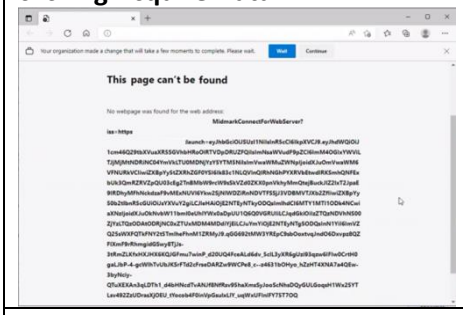
12. Select the profile(s) that matches your connection environment, and then click **Next.**

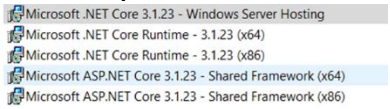
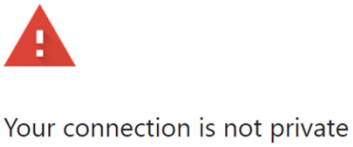
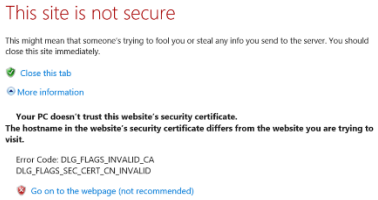
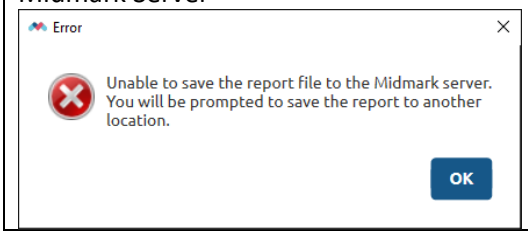


13. Enter the name **Midmark IQsecure**, and then click **Finish.**



Appendix I – Troubleshooting Guide

Problem	Possible Cause	Possible Solution
Server Error on Web Browser 	MDL Session was not created Incorrect Configuration CLIENT ID can be incorrect	Ensure Client IDs are correct. If not, update on Midmark Web Server in C:\Program Files\Midmark\Middleware\appsettings.json Review Client Midmark Logs located in C:\ProgramData\Midmark\IQconnect Review Midmark Server Logs located in C:\ProgramData\Midmark\IQconnect Review Epic Interconnect Trace Log files for any Midmark client ID requests Epic must setup Midmark apps on the Epic side. Ensure that MDL.exe.config file has the correct URLs Verify with Epic that front end Client ID is valid.
Page cannot be found Error after clicking Acquire Data 	Incorrect Configuration	Incorrect URL in the Epic FDI configuration. Ensure URLs are correct. For Example: https://ServerNameFQDN/MidmarkConnectForWebServer instead of https://ServerNameFQDN/MidmarkConnectforWebMiddleware
Welcome page when launching Midmark acquisition	URL that Epic is calling can be missing part of the URL	Ensure that /midmark is added to the end of the URL on the Epic side. https://ServerNameFQDN/MidmarkConnectForWebServer/midmark

Problem	Possible Cause	Possible Solution
Windows cannot find URL error when clicking acquire ECG. 	Incorrect URL configuration in Epic	Ensure the correct URL is being called in Epic.
Error 500.19 (ASP.Net Core runtime not found) 	ASP.NET Core not installed	Make sure you have installed the ASP.NET Core Runtime Hosting Bundle.
Error 500.31 (Failed to load ASP.NET Core runtime)	ASP.NET Core not installed	Make sure you installed the right Hosting Bundle Remove and Reinstall .NET Core Hosting Bundle
Your connection is not private. Certificate not trusted Error. 	Incorrect SSL Configuration	Ensure certificate being used is fully trusted by client system.
The hostname in the website's security certificate differs from the website you are trying to visit Error 	Certificate website does not match actual website name.	Ensure that your certificate matches the computer network name and the server apps' web addresses.
Unable to save the report file to the Midmark Server 	Session information is corrupted on MIdmark SQL DB	Delete Midmark SQL DB and reinstall using MidmarkConnectForWebServer Installer Epic Public Key has not been uploaded to Epic or 24 hours have not elapsed since upload.

Customer Support and Warranty Information

Warranty

Midmark warrants to the original retail purchaser that it will repair or replace software contained within products manufactured by Midmark for a period of 12 months. Midmark does not warrant that the software: (1) is error free; (2) can be used without problems or interruptions; or (3) is free from vulnerability to intrusion or attach by viruses or other methods.

Please refer to midmark.com for the full and current Warranty Terms and Conditions.

Return Materials Authorization

To return any product for repair, a Return Materials Authorization (RMA) number must be obtained from Midmark Technical Service. This RMA number should be referenced on the package(s) containing the items to be returned and in any correspondence regarding the return.

Shipping

Before shipping any unit to Midmark, be certain that an RMA number has been issued and that all guidelines regarding this authorization are followed. We highly recommend following all guidelines for the shipment of medical products set forth by the shipping company used. If a question should arise regarding the appropriate method of shipment, please feel free to ask when calling for an RMA number. It is ultimately the responsibility of the customer when shipping a product to ensure that all packages and their contents get to Midmark safely. Midmark will not assume responsibility for damage due to improper packaging, shipment, or product use. Such actions will void all applicable warranties.

Contact Information

Technical Support is available Monday through Friday (except holidays), 5:00 am to 5:00 pm Pacific Standard Time.

Midmark Corporation
1001 Asbury Drive
Buffalo Grove, IL 60089 USA
Email: techsupport@midmark.com
T: 844.856.1230, option 2
Fax: 310.516.6517
midmark.com

Midmark Corporation
1001 Asbury Drive
Buffalo Grove, IL 60089 USA
T: 844.856.1230, option 2
Fax: 310.516.6050