

WIN-911 Best Practices for SQL Server and IIS

Microsoft SQL Server Requirements

Hardware and Software Requirements for SQL Server 2017

<https://docs.microsoft.com/en-us/sql/sql-server/install/hardware-and-software-requirements-for-installing-sql-server?view=sql-server-2017>

WIN-911 ships with Microsoft SQL 2017 Express which should be sufficient for most if not all installations of WIN-911. However, if additional performance is required, it may be necessary to upgrade to SQL Server Standard or Enterprise. You will find a matrix of features supported by all editions of SQL Server 2017 here, <https://docs.microsoft.com/en-us/sql/sql-server/editions-and-components-of-sql-server-2017?view=sql-server-ver15>

Other versions of SQL Server are also supported, the following have been tested for compatibility, Microsoft SQL Server 2008 R2 through 2019 (Express, Standard and Enterprise Editions)

WIN-911 Installation Requirements

WIN-911 requires access to a Microsoft SQL Server instance as it is used to store configuration data. During the installation process, the WIN-911 installer will search for a local or remote SQL instance named "WIN911". If no instances are found, the installing user shall be prompted to install a local SQL instance using SQL Server 2017 Express. If the user intends to use another instance not named "WIN911", they should decline this option.

SQL Server Permissions

While installing WIN-911, the logged-on user performing the installation must have the 'sysadmin' role assigned on the SQL instance the installer is targeting. If a user allows the WIN-911 installer to install Microsoft SQL Server 2017 Express for them, the correct permissions will automatically be applied to the instance.

SQL Deployment Considerations

Security

WIN-911 utilizes a web server, Internet Information Services (IIS), to host its configuration GUI so it must be installed on a Windows system running IIS. For security purposes, it is advisable to separate web and databases servers. In the event that IIS is compromised, all software running on the machine is now vulnerable, including SQL Server. If SQL Server is installed on a separate machine, the server can only be accessed through its remote interface. If a user does install WIN-911 and Microsoft SQL Server on the same machine, we highly recommend the use of Firewalls to restrict access to IIS.

For more information, please reference Microsoft's Security Considerations for a SQL Server Installation, <https://docs.microsoft.com/en-us/sql/sql-server/install/security-considerations-for-a-server-installation?view=sql-server-2017>.

Performance

Depending on the size of your WIN-911 configuration, it may be advisable to install SQL Server on a separate server. Without initial performance tuning, SQL Server is designed to run at peak performance and assumes it is the only server running on the OS. Meaning SQL Server will attempt to reserve all RAM and utilize as many CPU cycles as possible. If you must install SQL and IIS/WIN-911 on the same machine, it may be worth the effort to use CPU affinity masks for SQL and IIS to isolate the two on separate cores and configure SQL to reserve less RAM.

For information, please reference Microsoft's TechNet articles regarding SQL Server monitoring and Performance Tuning, [https://technet.microsoft.com/en-us/library/ms189081\(v=sql.120\).aspx](https://technet.microsoft.com/en-us/library/ms189081(v=sql.120).aspx).

Internet Information Systems (IIS) Requirements

WIN-911 utilizes IIS to host application servers which provide access to WIN-911's configuration GUI so it must be installed before you can install WIN-911. Once installed, IIS requires access to SQL Server and the locally running WIN-911 Runtime Services. All other traffic should be blocked unless you require remote access to the WIN-911 GUI. We suggest reviewing Microsoft's Security Best Practices of IIS 8, [https://technet.microsoft.com/en-us/library/jj635855\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/jj635855(v=ws.11).aspx).

When installing IIS, only the modules required by WIN-911 should be installed. Needlessly installing modules which are not used will increase your vulnerability to outside attacks. Below you will find a list of the modules required by WIN-911 in a Server 2012 R2 environment.

(Bolded items are the modules you must install)

- Features
 - .NET Framework 4.5 Features
 - WCF Services
 - **HTTP Activation**
- Server Roles
 - Common HTTP Features
 - **Default Document**
 - **Static Content**
 - **HTTP Redirection**
 - Security
 - **Request Filtering**
 - **Basic Authentication**

- **Windows Authentication**
- Application Development
 - **.NET Extensibility 4.5**
 - **Application Initialization**
 - **ASP.NET 4.5**
 - **ISAPI Extensions**
 - **ISAPI Filters**
- Management Tools
 - **IIS Management Console**

System Architecture

WIN-911 is modular in design, meaning that each feature (iFIX Data Source / Email Notifier / Dispatcher), are all self-contained applications which when combined form one logical system. The modules communicate with each other using Microsoft's Windows Communication Foundation, WCF, over ports 80 and 4020 through http endpoints. Since this communication is local, you will not need to create firewall exceptions for these ports. The modules must also communicate with SQL Server and this is done over the standard TCP port 1433. If your SQL Server is remote from the WIN-911 installation, a firewall exception must be created to allow traffic.

Notification modules each have their own network requirements, for example, the Email module will need to connect to an email server and the Voice module will need to connect to a VoIP server. Below you will find all the modules with the standard communication ports listed.

Dispatcher

Ports Used

TCP 80, 4020, 1433

Communicates with all WIN-911 modules using TCP ports 80 and 4020 and SQL Server over port 1433.

Reporting

Ports Used

TCP 80, 4020, 1433

Communicates with all WIN-911 modules using TCP ports 80 and 4020 and SQL Server over port 1433.

iFIX Data Source

Ports Used

TCP 80, 4020, 1433

Communicates with the Dispatcher and Reporting modules using TCP ports 80 and 4020 and SQL Server over port 1433.

OPC Data Source

Ports Used

TCP 80, 4020, 1433, 135

Communicates with the Dispatcher and Reporting modules using TCP ports 80 and 4020 and SQL Server over port 1433. Communicates to OPC servers using TCP 135.

OPC Data Source

Ports Used

TCP 80, 4020, 1433, 135

Communicates with Dispatcher and Reporting modules using TCP ports 80 and 4020, SQL Server over port 1433, and OPC servers using TCP 135.

Voice Module

Ports Used

TCP 80, 4020, 1433

TCP/UDP 5060 - 5700

Communicates with Dispatcher and Reporting modules using TCP ports 80 and 4020, SQL Server over port 1433, and VoIP servers using TCP/UDP ports 5060 – 5700. VoIP ports will vary with VoIP providers.

SMS Module

Ports Used

TCP 80, 4020, 1433, 5000

Communicates with Dispatcher and Reporting modules using TCP ports 80 and 4020, SQL Server over port 1433. The SMS module uses a cellular modem to send text messages. The modem connects to the PC either directly through a COM port or indirectly over the network over port TCP port 5000.

Email Module

Ports Used

TCP 80, 4020, 1433

SMTP – TCP 25, 465, 587

POP - TCP 110, 995

IMAP – TCP 143, 993

Communicates with Dispatcher and Reporting modules using TCP ports 80 and 4020, SQL Server over port 1433. The Email module supports SMTP, POP, and IMAP protocols. The

Mobile-911 Module

Ports Used

TCP 80, 4020, 1433, 59109, 59111

Communicates with Dispatcher and Reporting modules using TCP ports 80 and 4020 and SQL Server over port 1433. The Mobile-911 Module sends alarm information to the Mobile-911 Server over TCP ports 59109 and 59111.

Mobile-911 Server

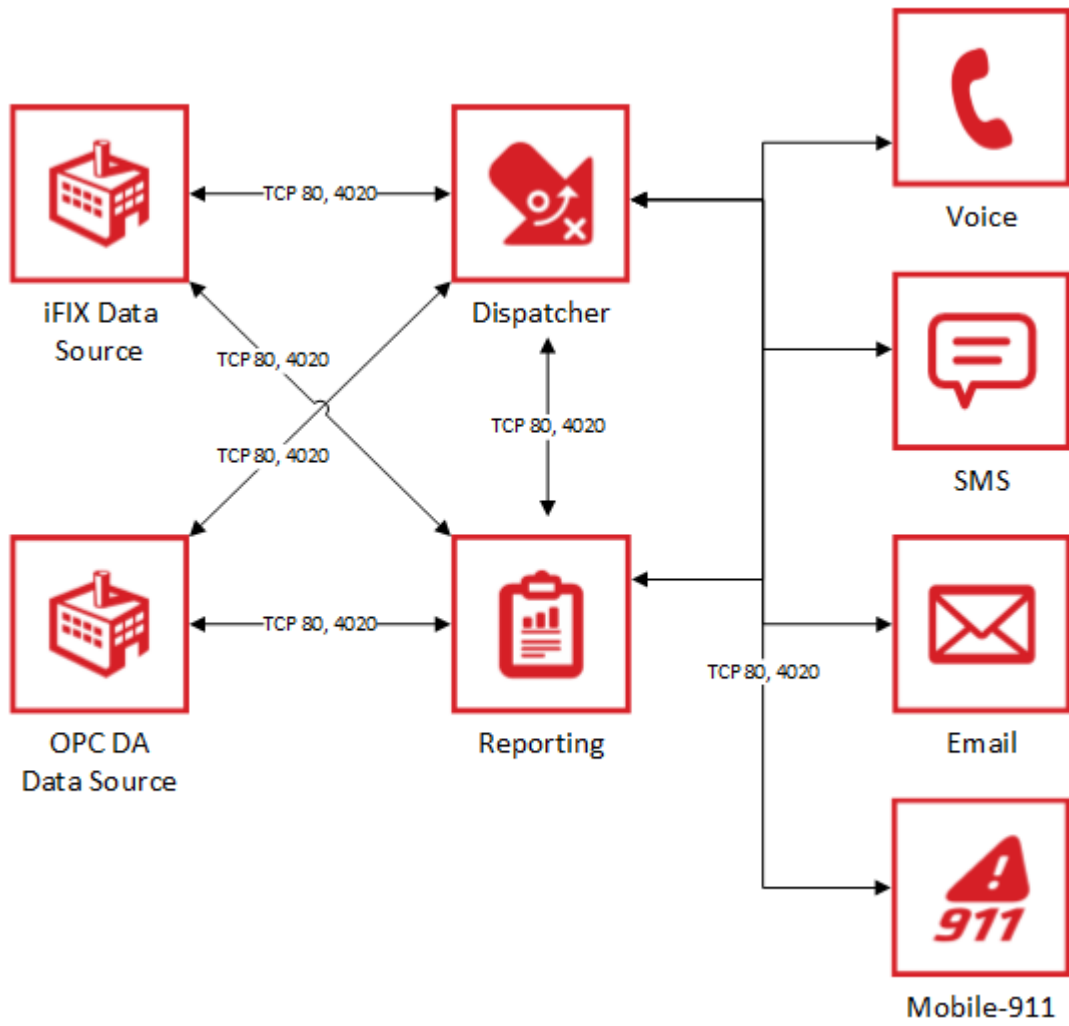
Ports Used

TCP 59109, 59111, 59112, and 11171

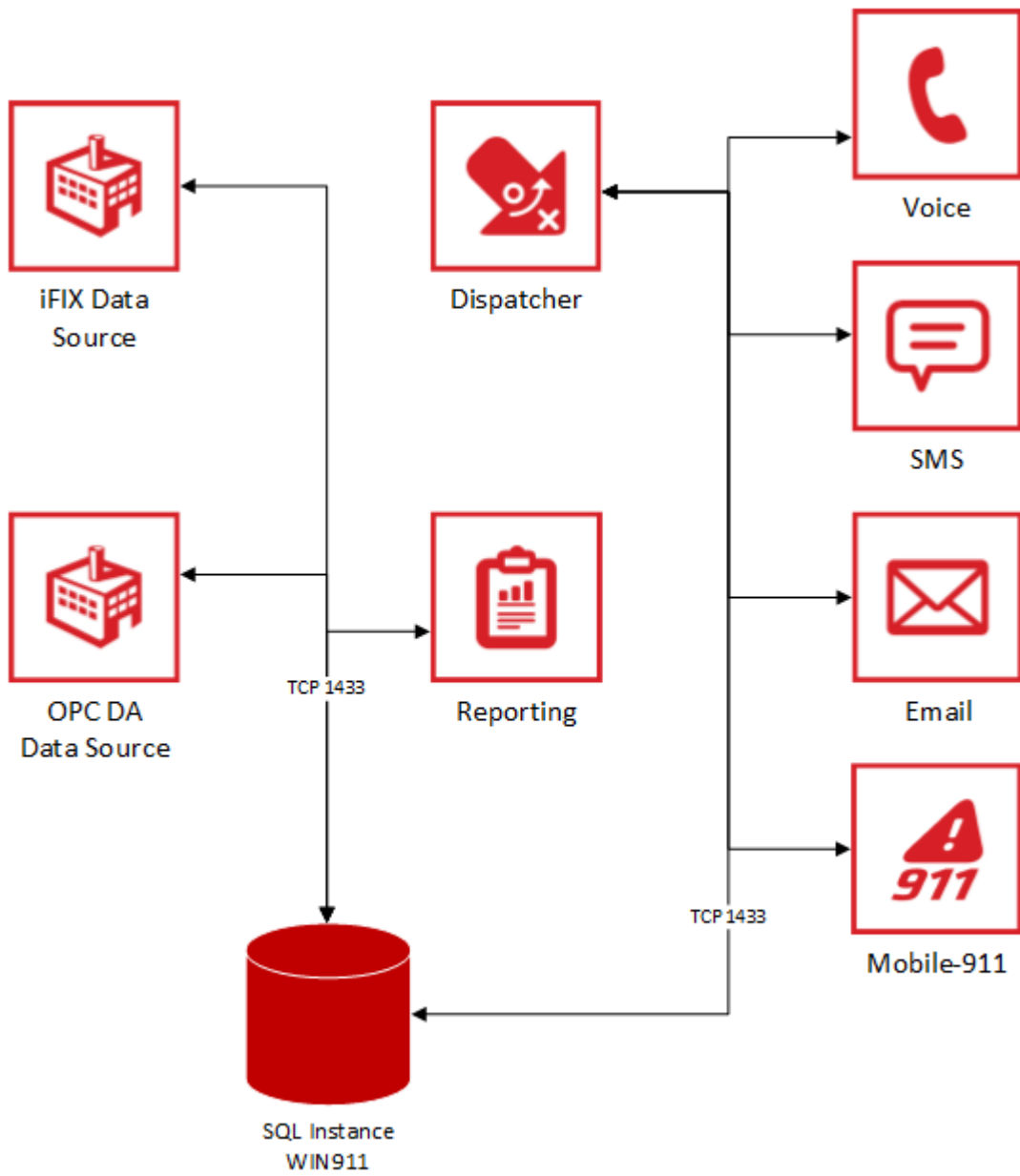
The Mobile-911 Server communicates to the Mobile-911 Module over TCP ports 59109 and 59111, Mobile-911 devices over TCP port 59112, and WIN-911's push notification server over TCP port 11171.

Network Diagrams

Module to Module Communication



Module Communication to SQL Server



Notification Module Communication

