WIN-911 2021 Security Best Practices

Before You Begin The Installation - SQL Recommendations

The WIN-911 2021 installer will offer to install a new instance of SQL Server 2019 Express. If this option is selected, then appropriate SQL permissions will be applied automatically.

You are welcome to use your own existing SQL Server instance 2014-2019. In that case, the account used to install must have either dbcreator or sysadmin rights in SQL. However, it is recommended to use dbcreator. Just ensure that you always have at least one user who does have sysadmin rights. The WIN-911 service account specified during installation (under which WIN-911 processes will run) should have a 'public' role in SQL Server and will be granted db_datareader and db_datawriter permissions on module databases during installation.

When targeting a remote SQL instance, it is necessary to create a local account on the SQL machine with the same credentials (username and password) as the account selected during the WIN-911 install under which WIN-911 services will execute. Since the WIN-911 services account must be local, there is no way for the SQL instance to validate a security token from that account unless it exactly matches a local account on the SQL host.

SQL Deployment Considerations

Security

WIN-911 utilizes a web server, Internet Information Services (IIS), to host its configuration GUI and application services. 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://msdn.microsoft.com/en-us/library/ms144228(v=sql.120).aspx.

Performance

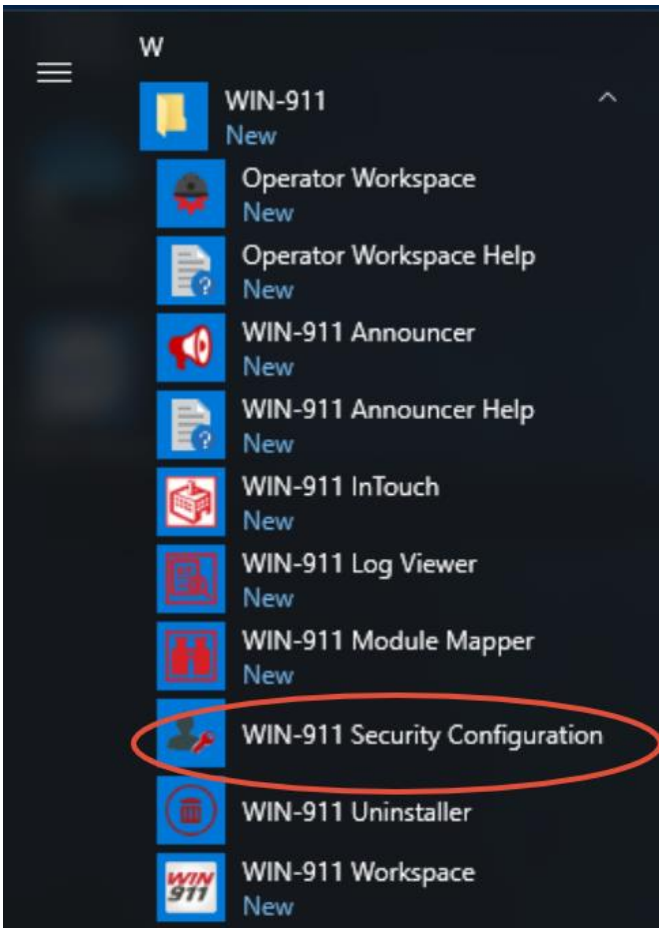
Depending on the size of your WIN-911 configuration, it may be advisable to install SQL Server on a separate server. Without initial performance tuning, SQL Server is designed to run at peak performance and assumes it is the only server running on the OS.

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.

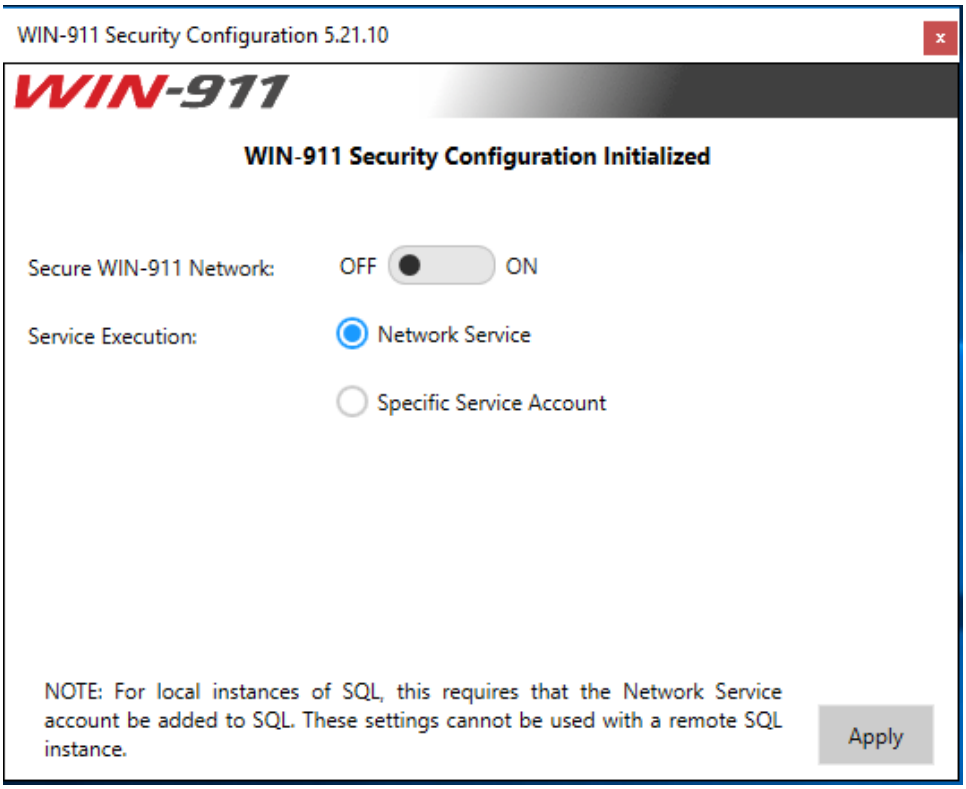
For information, please reference Microsoft's TechNet articles regarding SQL Server monitoring and Performance Tuning, https://technet.microsoft.com/en-us/library/ms189081(v=sql.120).aspx.

Securing Your WIN-911 2021 Installation

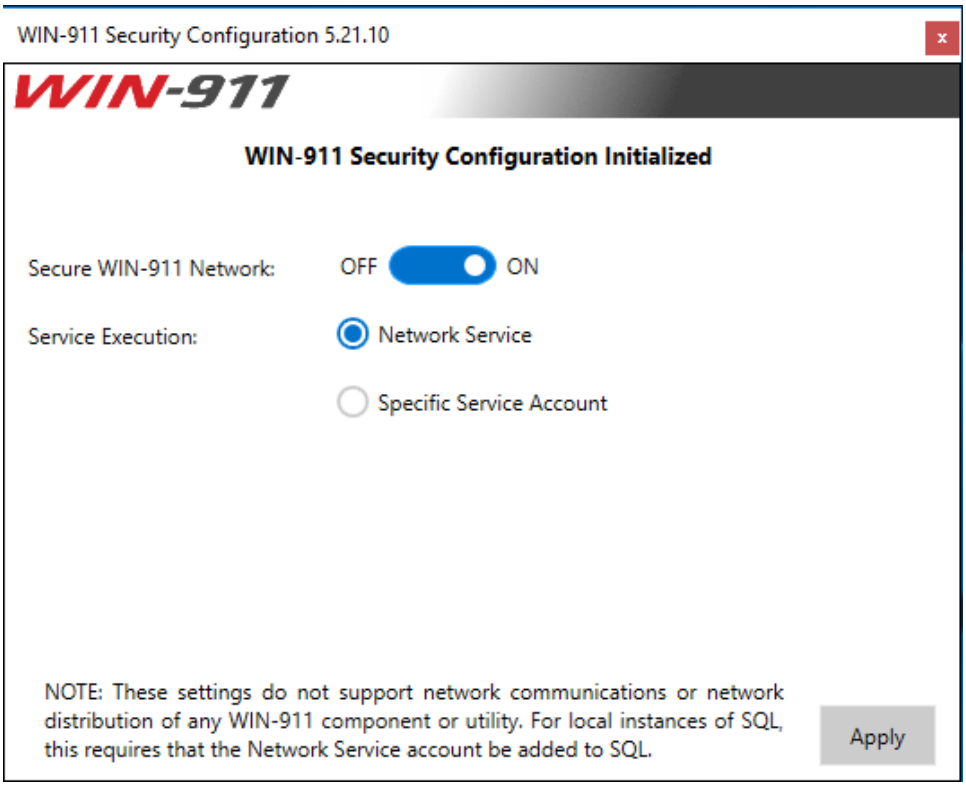
After installing WIN-911 2021, especially in a distributed install, you can run the WIN-911 Security Configuration utility to create a secure connection between the modules that make up the WIN-911 system. You can find this utility under the Start menu in the WIN-911 section.



When the WIN-911 Security Configuration utility runs, it will present a screen like this:



Flipping the switch to "ON" will secure the connections between the installed modules.



If you have a distributed install, it is important that you run the WIN-911 Security Configuration utility on every computer on which WIN-911 components are installed. Moreover, all components should be restarted after applying changes. This includes Workspace, Operator Workspace, iFIX, InTouch, Mobile Hub, and Announcer.

Finally, while the WIN-911 Security Configuration utility is installed automatically with any module install, it will not be installed automatically with the Mobile Hub. The installer for the WIN-911 Security Configuration utility can be found in the Tools folder of your WIN-911 2021 Installation media (WIN911_SC.exe).

WIN-911 Service Account

The utility can also be used to modify the WIN-911 Service account under which WIN-911 processes will execute. Note that NETWORK SERVICE does not support network communication or network distribution. If WIN-911 is deployed as a standalone system, we recommend running under NETWORK SERVICE. When using a different service account it's important that the account have permissions to host windows services and have a non-expiring password. If distributed on a domain, we recommend creating a NT SERVICE account under which processes will run.

The WIN-911 service account specified should have a 'public' role in SQL Server and will be granted db_datareader and db_datawriter permissions on module databases assuming the utility is run as a sysadmin; otherwise those database roles should be added manually.

WIN-911 2021 File Permissions

To further enhance security, you can have your system administrator remove the Users group from file permissions for:

- WIN-911 2021 Workspace
- Operator Workspace
- iFIX Runtime
- InTouch Runtime
- Announcer Utility
- Security Configuration utility
- Mobile Hub

This will prevent people with only Users rights to access WIN-911 2021. Specific users can then be added to the permissions for fine grained control.

Network Communications

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 port 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

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

Reporting

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

iFIX Data Source

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

OPC Data Source

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

OPC Data Source

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

Voice Module

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

SMS Module

Communicates with Dispatcher and Reporting modules using TCP port 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 4020, 1433

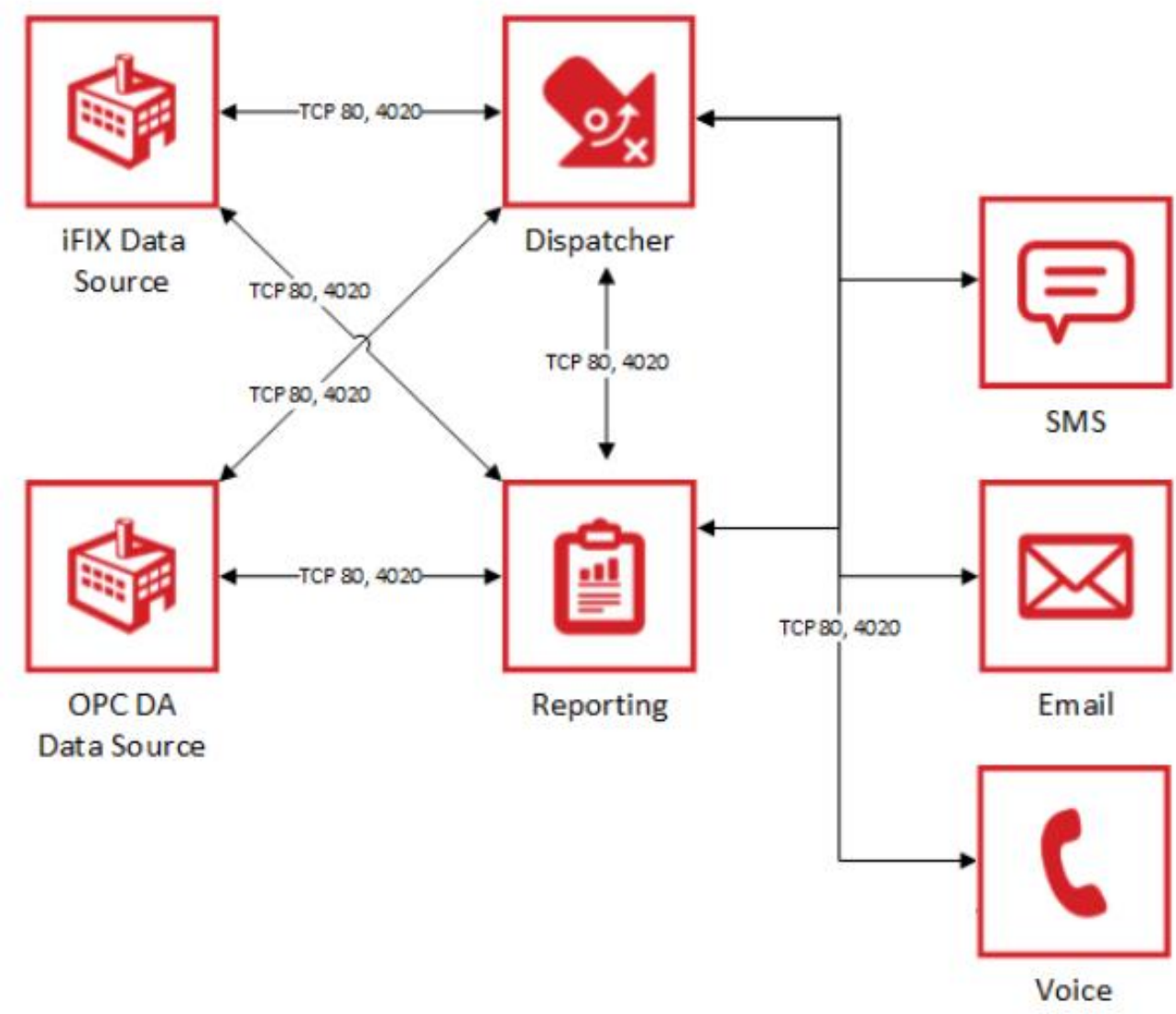
SMTP – TCP 25, 465, 587

POP - TCP 110, 995

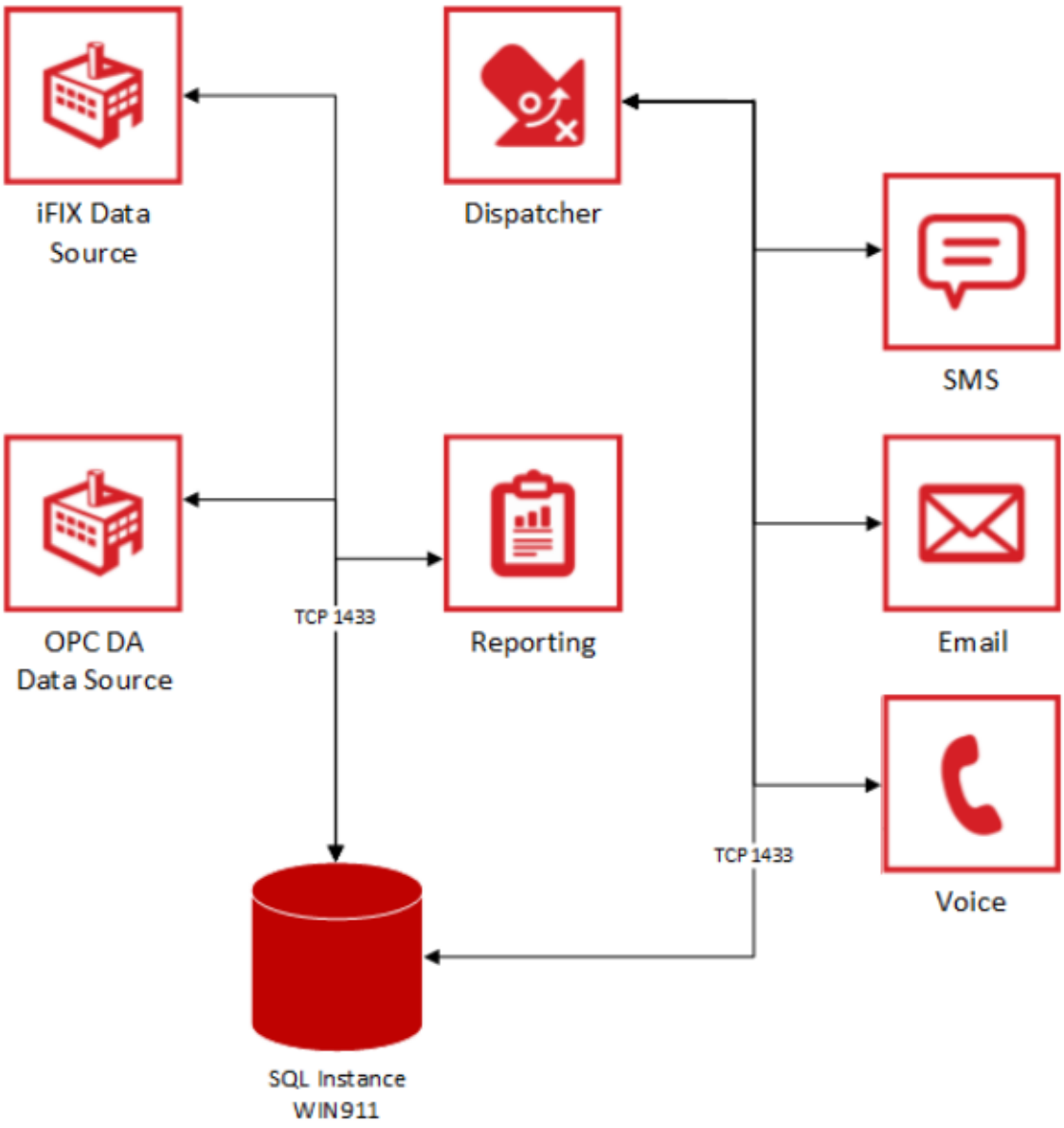
IMAP – TCP 143, 993

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

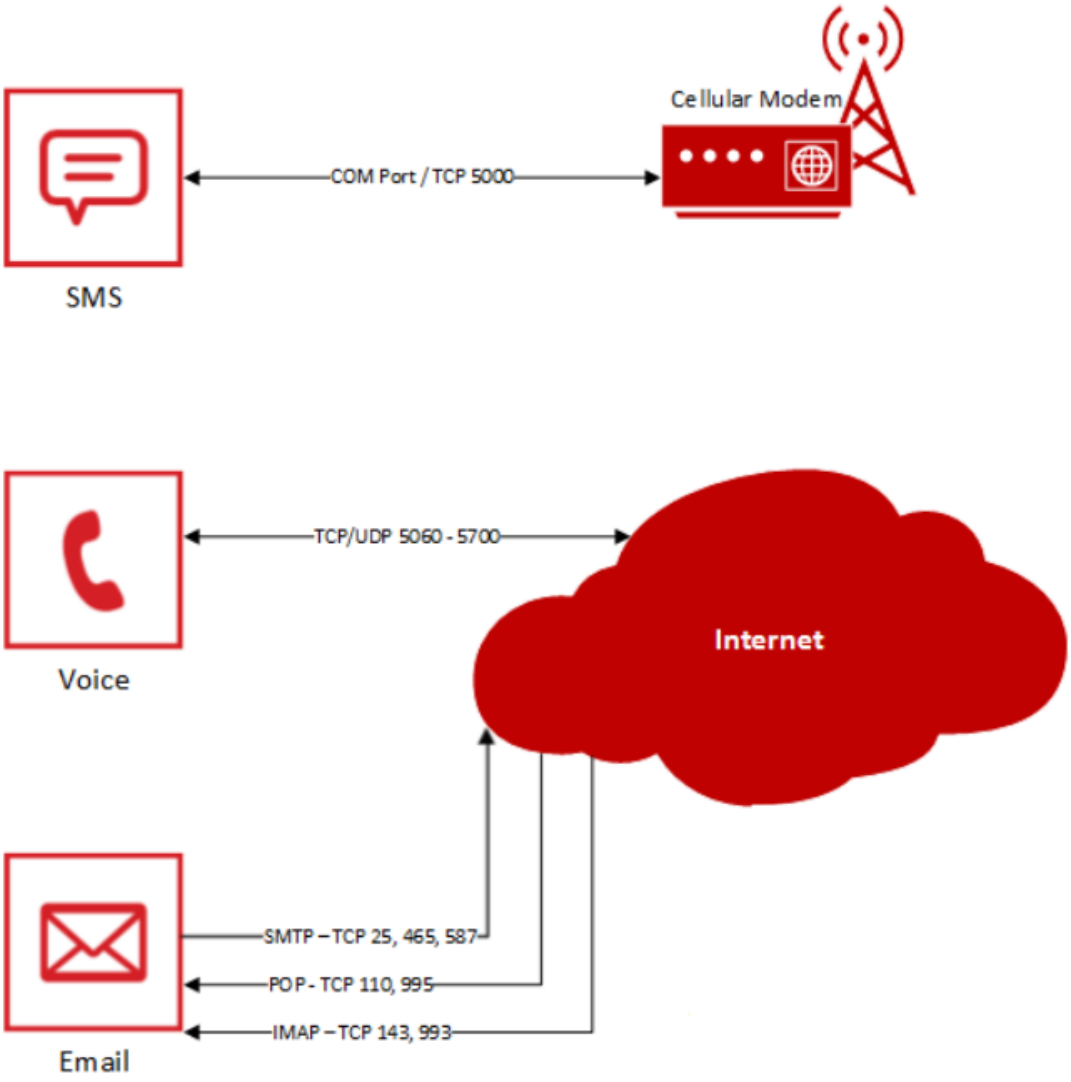
Module to Module Communication



Module Communication to SQL Server



Notification Module Communication


Cellular Modem
COM Port / TCP 5000
SMS
TCP/UDP 5060 - 5700
Internet
Voice
SMTP – TCP 25, 465, 587
POP - TCP 110, 995
IMAP – TCP 143, 993
Email