

WIN-911 2025 Security Best Practices

Before You Begin the Installation - SQL Recommendations

The WIN-911 2025 installer will offer to install a new instance of SQL Server 2022 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 2017-2022. 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 WIN911 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 windows service, to host its configuration GUI and application services. For security purposes, it is advisable to separate WIN-911 services and databases servers. If WIN-911 installed machine 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.

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](https://msdn.microsoft.com/en-us/library/ms144228(v=sql.120).aspx).

Performance

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

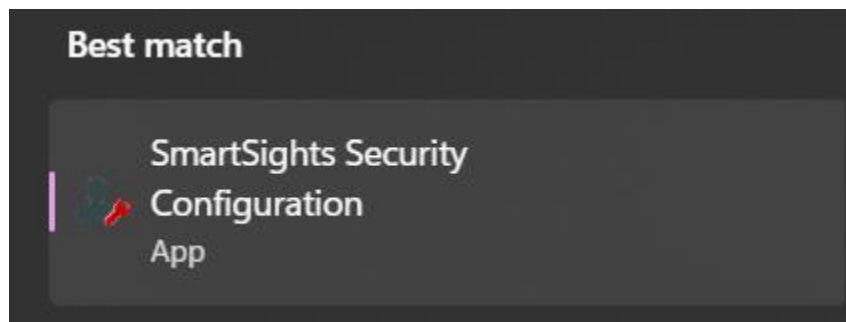
Meaning SQL Server will attempt to reserve all RAM and utilize as many CPU cycles as possible. If you must install SQL and WIN-911 on the same machine, it may be worth the effort to use CPU affinity masks for SQL and configure SQL to reserve less RAM.

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)

Keeping Your WIN-911 2025 Secure

WIN-911 uses certificates to secure communication between the modules that make up the WIN-911 system. When your certificate becomes expired, you can run the SmartSights Security Configuration utility to generate a new certificate. You can find this utility under the Start menu just search for SmartSights.



When the SmartSights Security Configuration utility runs, it will present a screen like this:

Machine Certificate ^

Subject CN=DESKTOP-RUV1D2U, C=US, O=WIN-911 Software
Valid to 10/9/2033 7:53:19 AM
Thumbprint AE1C7DEB4F669CAC16C5B595443F2A9B0EBE4162

Reset Certificate

Remote Certificates ^

Service to accept trust certificate requests is listening on port 4018.

WIN-911 Remote Machine/IP Address

Port

4018

Test Connection

☐

Subject ▼ Is Trusted Valid to ▼ Thumbprint ▼

Reload Certificates

Trust Certificates

Service Execution v

Generating New Certificate

Under the “Machine Certificate” section, you can see the information about the current certificate and “Reset Certificate” button to generate new certificate.

WIN-911 Security Configuration

WIN-911

Machine Certificate

Subject CN=DESKTOP-RUV1D2U, C=US, O=WIN-911 Software
Valid to 10/9/2033 7:53:19 AM
Thumbprint AE1C7DEB4F669CAC16C5B595443F2A980EBE4162

Reset Certificate

Remote Certificates

Service to accept trust certificate requests is listening on port 4018.

WIN-911 Remote Machine/IP Address

Port

4018

Test Connection

☐

Subject

Is Trusted

Valid to

Thumbprint

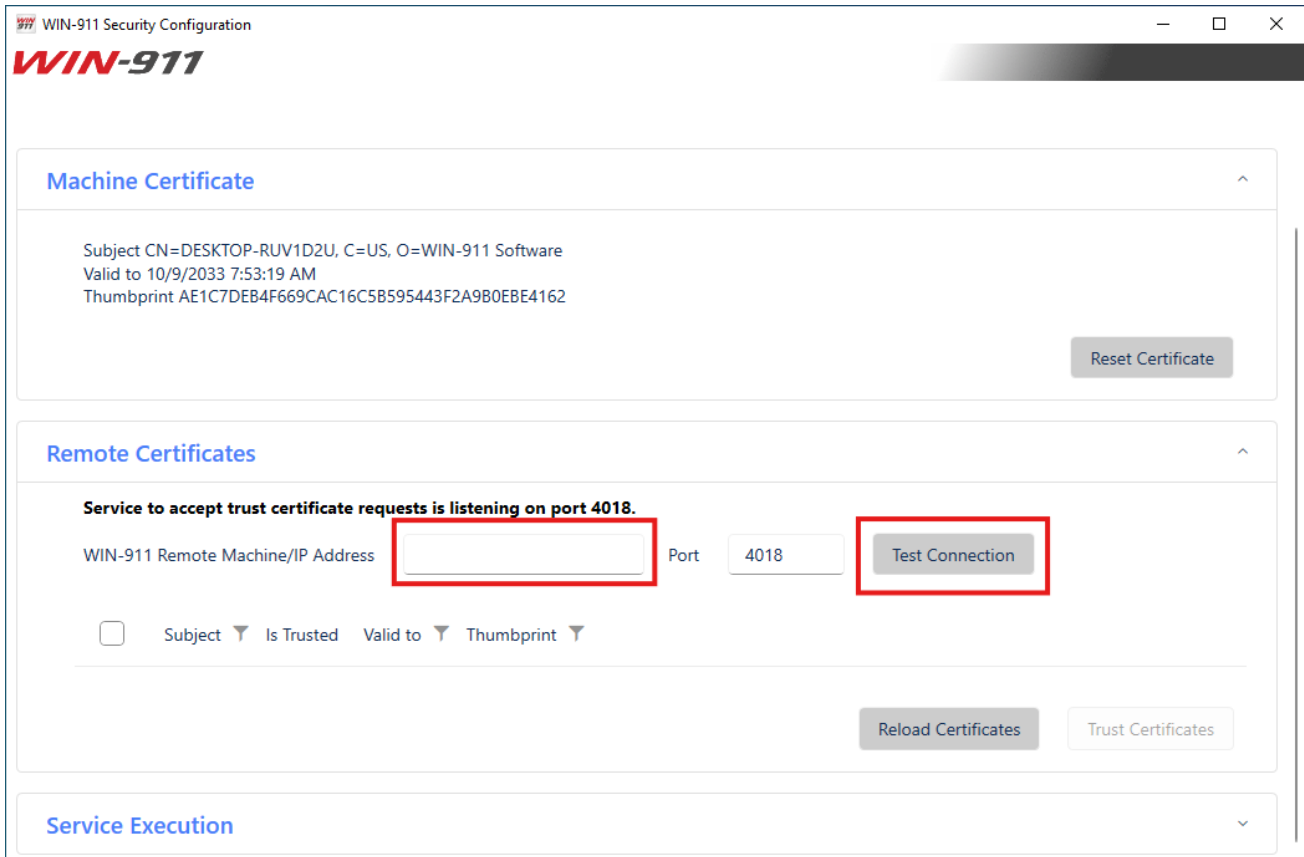
Reload Certificates

Trust Certificates

Service Execution

Establishing Trust (Distributed Environment)

If you have a distributed install and have generated a new certificate for a module, it is important that you run the SmartSights Security Configuration utility on every computer on which SmartSights components are installed and perform the certificate trust process. To perform the certificate trust process on the “Remote Certificate” section of the utility, Enter the remote machine/IP address where another WIN-911 module is running and click the “Test Connection” button. The Default Port for communication is 4018.



The screenshot shows the 'WIN-911 Security Configuration' window. The 'Machine Certificate' section displays the local certificate details: Subject CN=DESKTOP-RUV1D2U, C=US, O=WIN-911 Software; Valid to 10/9/2033 7:53:19 AM; and Thumbprint AE1C7DEB4F669CAC16C5B595443F2A9B0EBE4162. A 'Reset Certificate' button is present. The 'Remote Certificates' section shows a message: 'Service to accept trust certificate requests is listening on port 4018.' Below this, there is a text input field for 'WIN-911 Remote Machine/IP Address', a 'Port' dropdown set to '4018', and a 'Test Connection' button. A table with headers 'Subject', 'Is Trusted', 'Valid to', and 'Thumbprint' is visible but empty. At the bottom of the 'Remote Certificates' section are 'Reload Certificates' and 'Trust Certificates' buttons. The 'Service Execution' section is partially visible at the bottom.

WIN-911 Security Configuration

Machine Certificate

Subject CN=DESKTOP-RUV1D2U, C=US, O=WIN-911 Software
Valid to 10/9/2033 7:53:19 AM
Thumbprint AE1C7DEB4F669CAC16C5B595443F2A9B0EBE4162

Reset Certificate

Remote Certificates

Service to accept trust certificate requests is listening on port 4018.

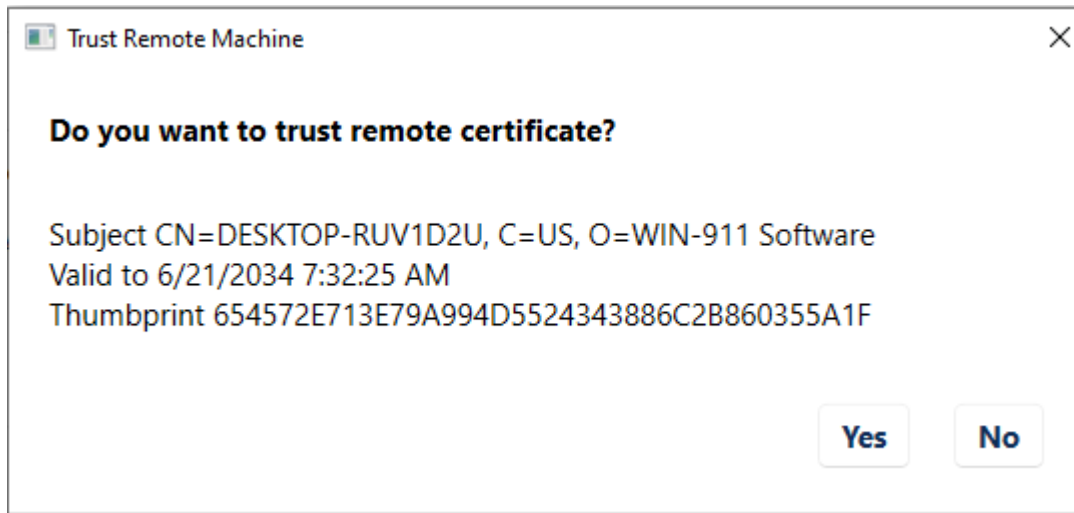
WIN-911 Remote Machine/IP Address Port 4018 Test Connection

☐ Subject Is Trusted Valid to Thumbprint

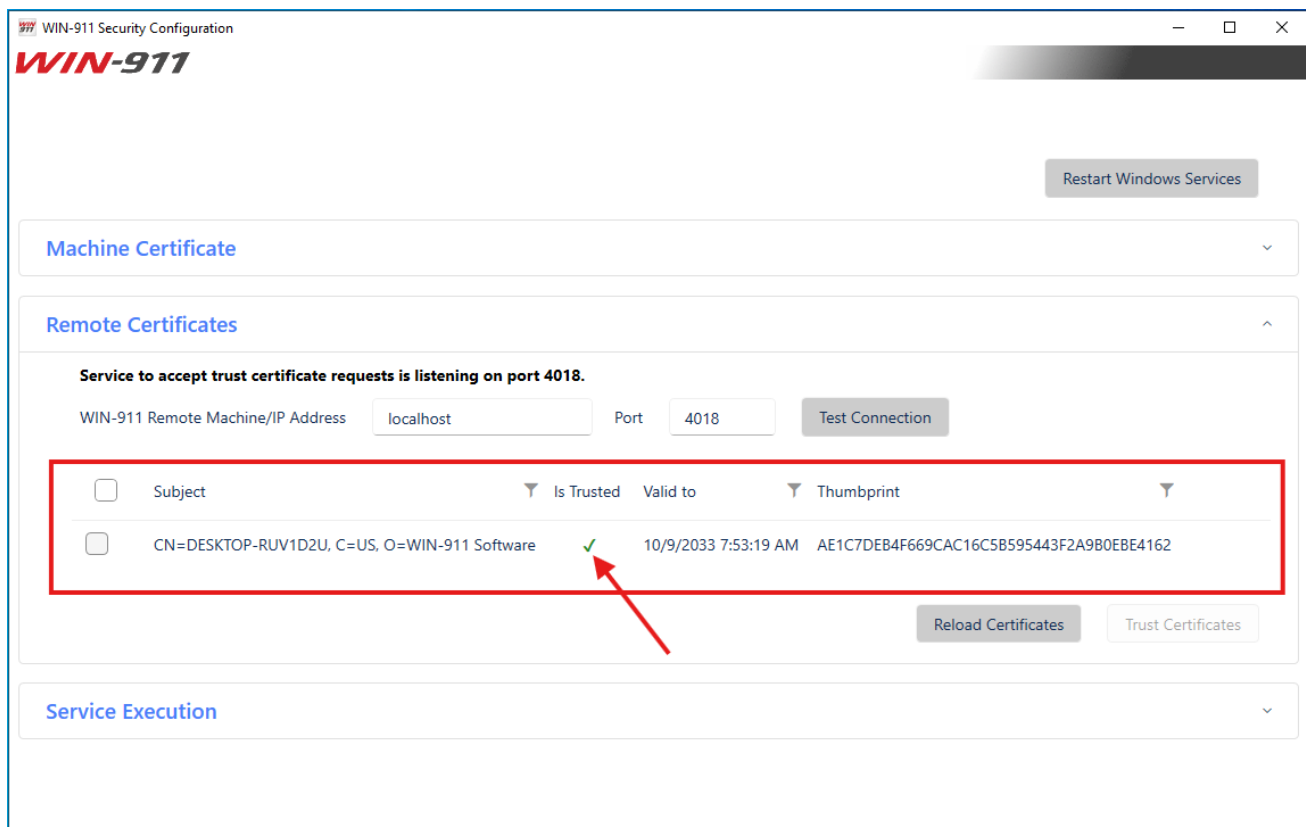
Reload Certificates Trust Certificates

Service Execution

SmartSights Security Configuration utility on both computers will see a popup dialog with an option to trust Yes or No.



Once the remote host is trusted you will see it on the list of certificates with a green check mark icon on "Is Trusted" column.



The SmartSights Security Configuration utility is typically installed automatically with all WIN-911 components. The setup for the SmartSights Security Configuration utility can be found in the Setup folder of your WIN-911 2025 Installation media (SS_SCU.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. When using a different service account, it's important that the account has permissions to host windows services and have a non-expiring password.

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.

The screenshot shows the 'WIN-911 Security Configuration' window. The title bar includes the text 'WIN-911 Security Configuration' and standard window controls. The main window features the 'WIN-911' logo in the top left. On the right side, there is a 'Restart Windows Services' button. Below this, there are three expandable sections: 'Machine Certificate', 'Remote Certificates', and 'Service Execution'. The 'Service Execution' section is currently expanded, revealing a form with two input fields: 'Username' (containing 'DESKTOP-RUV1D2U\yzzone') and 'Password' (with a placeholder 'Enter password'). A 'Browse' button is located to the right of the Username field. At the bottom right of the 'Service Execution' section, there is an 'Apply' button. Red rectangular boxes are drawn around the Username and Password input fields, and the 'Apply' button.

WIN-911 2024 File Permissions

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

- Workspace
- Operator Workspace
- iFIX Runtime
- InTouch Runtime
- Control Center
- Security Configuration
- Failover Utility
- Backup Restore
- Mobile Hub

This will prevent people with only Users rights to access WIN-911 2024. 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 gRPC, over ports 4020-4100 through HTTPS endpoints. If WIN-911 is installed across multiple computers, you will 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 or WIN-911 modules are distributed, a firewall exception must be created to allow traffic and modules will communicate to MS SQL server using TCP port 1434.

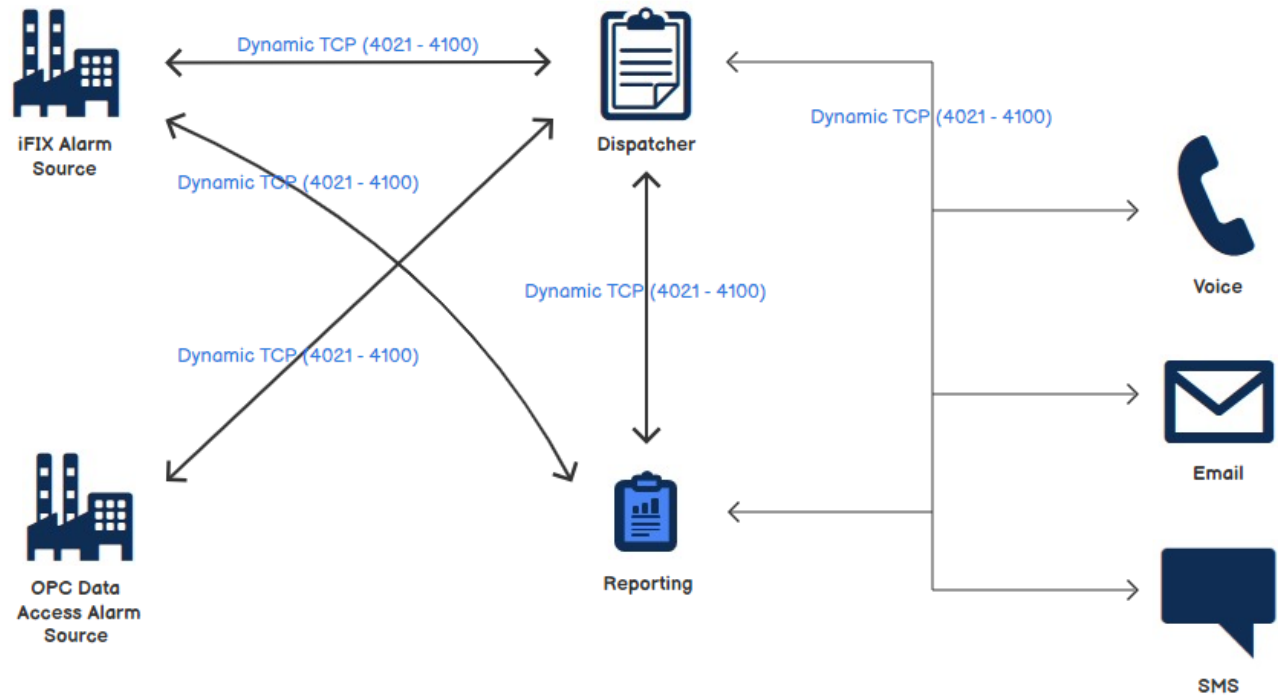
Notification modules each have their own network requirements, for example, the Email module will need to connect to an email server and the Voice module will need to connect to a VoIP server.

Ports Summary

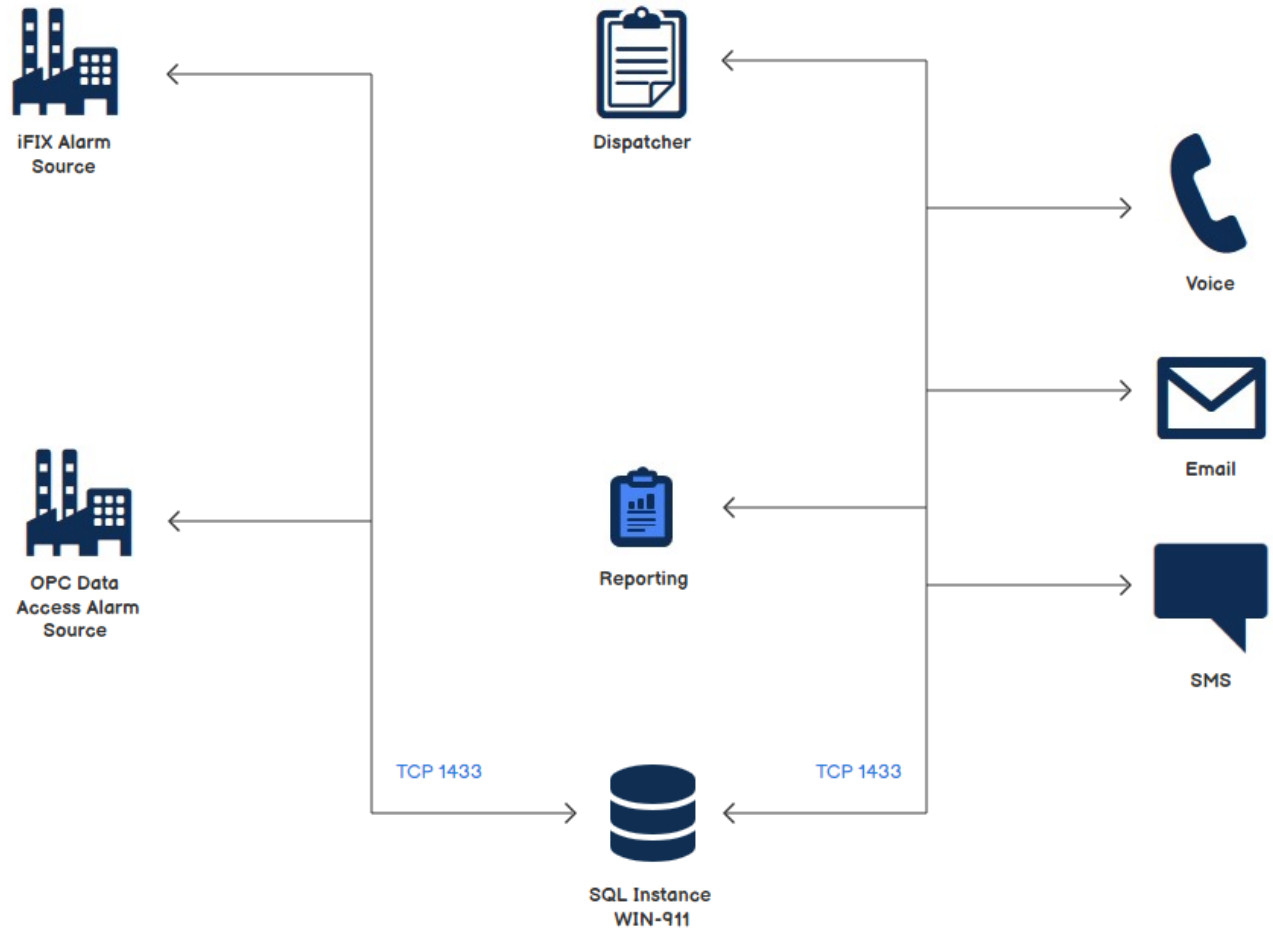
| Ports | Descriptions |
|-------------------------|---|
| TCP 25, 465, 587 | Ports might be used by WIN-911 Email module for SMTP Traffic. |
| TCP 110, 995 | Ports might be used by WIN-911 Email module for POP Traffic. |
| TCP 143, 993 | Ports might be used by WIN-911 Email module for IMAP Traffic. |

| | |
|--------------------------|---|
| TCP 135 | Used for connection between WIN-911 OPC and OPC Server. |
| TCP 443 | Used by SmartSights Edge Gateway for authentication and use SmartSights Cloud resources. Email module may used for Office 365. |
| TCP 4017 | Default port for WIN-911 Failover Utility. |
| TCP 4018 | Default port for SmartSights Security Configurator Utility, Used for all certificate traffic between SmartSights systems. Used during WIN-911 installation. |
| TCP 4019 | Used by SmartSights Edge Gateway Configurator to inform configuration changes. (local only) |
| TCP 4020 | Default port for WIN-911 Navigation, this is used by all WIN-911 Modules. |
| TCP 4021 - 4100 | WIN-911 Modules get port dynamically within this range. |
| TCP 1433 | MS SQL server, WIN-911 module will access the SQL server over this port when on same network. Not needed when SQL is Locally installed. |
| TCP 1434 | MS SQL server, WIN-911 module will access the SQL server over this port when on different networks. See Remote SQL Access KB for configuring remote SQL access. |
| TCP 5000 | SMS modem connects with WIN-911 installed system using this COM port. (if connected via network and not via plug and play) |
| TCP/UDP 5060-5700 | Different VoIP servers might use different ports within this range |
| TCP 59111 | Used by WIN-911 Mobile to communicate SmartSights Edge Gateway. |

Module to Module Communication



Module Communication to SQL Server



Notification Module Communication

