StarNet 2™

Security Management System

Installation & Configuration Guide

S2DA0102-001 Rev J
September 20, 2021
S/W V1.15

SENSTAR®

Senstar Corporation
Website: www.senstar.com
Email address: info@senstar.com

S2DA0102-001 Rev J
September 20, 2021
S/W V1.15

The information provided in this guide has been prepared by Senstar Corporation to the best of its ability. Senstar Corporation is not responsible for any damage or accidents that may occur due to errors or omissions in this guide. Senstar Corporation is not liable for any damages, or incidental consequences, arising from the use of, or the inability to use, the software and equipment described in this guide. Senstar Corporation is not responsible for any damage or accidents that may occur due to information about items of equipment or components manufactured by other companies. The figures included in this document are for illustration purposes only, and may differ from the actual equipment. Features and specifications are subject to change without notice.

Any changes or modifications to the software or equipment that are not expressly approved by Senstar Corporation void the manufacturer's warranty, and could void the user's authority to operate the equipment.

Senstar Corporation's Quality Management System is ISO 9001:2015 registered.

Change history

Revision	Changes
July 27, 2021 V1.14-V1.15	StarNet 2 version 1.15 can now issue a csv report without the need of Microsoft Excel to be installed on the workstation. Troubleshooting section added for other database errors.
September 25, 2020 V1.11-V1.14	NMS support for Silver Network FP400 MX Controller and Zone devices FiberPatrol RSU NMS supports fiber cut location and displaying the location on a picture-map Picture engine supports a new navigation feature which can be turned on and off using SN2 setup The new feature enables the user to zoom in and out and scroll the map up/down, right/left using the mouse All exported reports (PDF or CSV) shall be sorted by date Audit reports store information on: Mute Alarm on/off activity Event Automatic Mode on/off action V1.12 Problem with redundancy support has been fixed V1.14 Problem with Network Manager status update following a software restart has been fixed
September 1, 2019 V.110-V.111	Every valid message from the Network Manager is now considered a heartbeat message Problems with the enforcement of permissions related to running reports have been fixed
March 26, 2019 V.109-V.110	Added support for Aimetis Symphony VMS 10 Added an alarm silencer button to silence the alarm sound without acknowledging the alarm Added Auto-delete function to reset an event once it returns to the default state Rules can be placed on maps and triggered by Operator actions (Acknowledge, Reset and select from queue) StarNet supports an unlimited number of Network Managers The administrator can set a default picture map that appears on startup
April 19, 2018 V.108-V.109	Added support for Windows 10 Added support for Airship VMS Added support for Senstar LM100 Added support for Network Manager Faulty status reporting

Revision	Changes
January 4, 2018 V.107-V.108	Added Alarm Escalation functions Added support for Network Manager Alarm Logic Engine Additional information provided for Network Manager faulty status Added Rule Engine ASCII command function capability and Run Simultaneously capability Terminology changes (Accept to Acknowledge; Close to Reset) Added Russian language support
November 22, 2016 V.106-V.107	Updated network configuration information Minor text improvements and fixes New database maintenance and archive procedures Updated troubleshooting information New installation procedures
February 22, 2016	Added new database installation procedures
December 14, 2015	Updated database restore procedure Renamed Watchdog icon to Service Manager icon
November 17, 2015	Added procedure for hidden sensors Added table outline system change/restart requirements
November 10, 2015 build - 7945	Added monitoring icon information Updated upgrade instructions Minor edits and fixes
October 10, 2015	Improved descriptions of Network Manager IP addresses Added multi-site staging procedure

Table of Contents

1 System Overview

The StarNet 2 Security Management System (SMS) provides monitoring, operation, and alarm management of Senstar intrusion detection systems and third-party security products. StarNet 2 runs on Microsoft Windows operating systems and is designed to manage daily routines and activities as well as crisis situations. It enables an organization to reduce its reaction time, improve its efficiency and safeguard its personnel and property.

The user interface is optimized for operator efficiency and ease-of-use. The location and coverage area of each security sensor is displayed visually on a map. When an alarm occurs, the operator can quickly determine its location, type, and severity. If any cameras are associated with the sensor, the specific video feed can be displayed.

The StarNet 2 SMS is optimized to support Senstar sensors. This includes, but is not limited to, the following systems: FlexZone, FP400, FiberPatrol, FlexPS, OmniTrax, UltraLink I/O, UltraWave, X-Field, and Senstar LM100. Third-party security products, connected via supervised dry-contact inputs, are also supported. Third-party security products can also be integrated in software via a Senstar-supported security protocol.

Figure 1: Sample StarNet 2 SMS Screen

Sensor Integration

The StarNet 2 SMS communicates with Senstar security sensors via the Network Manager (NM) software. All Senstar sensors, including MX Controllers and MX Zone devices, that use the Silver, CCC, FiberPatrol, and Crossfire network protocols are supported. StarNet 2 also supports the NM's alarm logic engine (ALE).

The Network Manager collects information about the status of the security sensors and communicates it to the StarNet 2 SMS. Any device managed by the Network Manager automatically appears in the StarNet 2 SMS.

Third-Party Security Devices

The StarNet 2 SMS supports third-party security devices that are connected to the Senstar equipment via auxiliary (dry contact) inputs. The inputs automatically appear in the StarNet 2 SMS under the names given to them by the Network Manager. You can customize the names as they appear on the operator screen during system configuration.

Video Management Systems

The StarNet 2 SMS can send commands to Aimetis, Airship, and other video management systems. Video output from third-party systems appears on a separate monitor, or on a 4-panel video matrix (Airship). Each connected sensor can be configured to send specific event actions to the video management system.

StarNet 2 Architecture

A sample StarNet 2 network is shown in Figure 2.

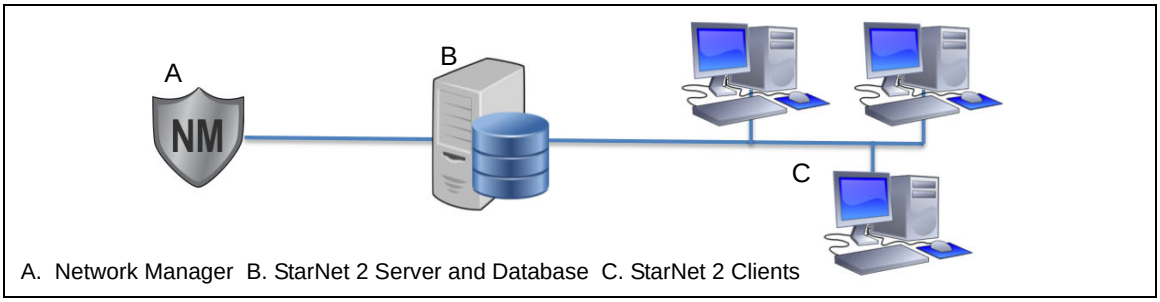


Figure 2: StarNet 2 SMS Network Architecture

Applications and Services

The StarNet 2 SMS consists of a set of software applications and services which interface with each other and with external software systems.

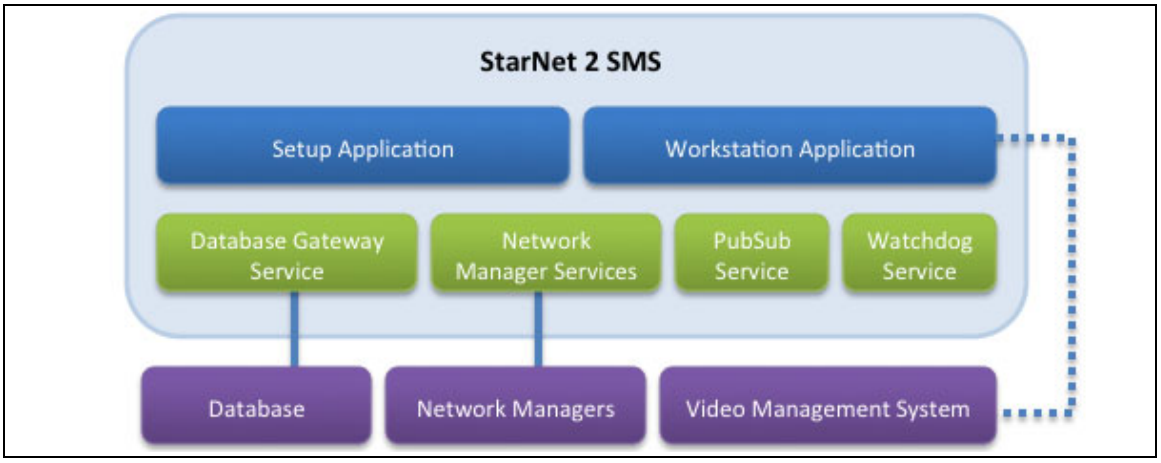


Figure 3: StarNet 2 Applications and Services

Database

An SQL database stores the system configuration as well as alarm and event histories. The StarNet 2 SMS supports SQL Server Standard 2008 and 2014. The database is typically installed on the same system as the StarNet 2 server software.

StarNet 2 Workstations

There are two StarNet 2 applications which provide graphical user interfaces (GUI) that system administrators and operators use to configure and operate the system:

- **Setup** – Used by system administrators to configure the sensors and workstations used by the system. This application does not need to be installed on each workstation.
- **Workstation** – Used by operators to view and respond to alarms.

StarNet 2 Server

The server runs a set of services that enable the StarNet 2 SMS to communicate with the database as well as the security sensors monitored by the Network Manager.

The following applications and services are installed with the StarNet 2 server:

- Setup – A local copy of the client application that is used to configure the sensors and workstations
- Workstation – A local copy of the client application that is used to monitor the status of the sensors and connected devices
- Database Gateway service – Responsible for access to the SQL database
- PubSub service – The communication protocol used by the system
- Network Manager Bridge services – Communicates with the Network Manager; a separate service exists for each Network Manager monitored by StarNet 2
- Watchdog service – Starts and monitors the services running on each workstation or server

- 4G Server service – Placeholder for future services
- Server External Systems service – Manages email and ASCII output functions
- Rule Engine service – Manages rules triggered by sensor and scheduled events
- Msg Dev Manager service – Manages messages

2 Server Installation

This chapter explains how to install the StarNet 2 Security Management System (SMS).

- Review the Installation Requirements on page 15
- Install the database (Install StarNet 2 Server on page 19)
- Install StarNet 2 Server on page 19
- Configure Network Manager on page 23
- Wait for sensor synchronization to finish (Synchronize Sensors on page 27)
- Add application shortcuts to the Windows desktop (Configure StarNet 2 Shortcuts on page 29)

After you have performed the above steps, you can proceed to Sensors and Picture-Maps on page 39. If you are familiar with the system, you may also choose at this time to install the workstation software on other computers (see Workstation Installation on page 31).

Installation Requirements

Before proceeding with the installation, review the following requirements and ensure that each one is met.

Computer (hardware)

The StarNet 2 computer must meet the following minimum requirements:

- processor: Intel Core i5 or equivalent
- hard drive: 320 GB
- memory: 8 GB RAM
- network interface: 10/100 Mbit Ethernet
- display: min. 1440 X 990 resolution; 1920 X 1080 resolution with dual output recommended

Operating Systems

The StarNet 2 SMS (database, server, and client) run on the following operating systems:

- Windows 7 64-bit with Service Pack 1
- Windows 8.1 Pro

- Windows 10 Pro 64-Bit

Note	The procedures described in this user guide are written for users running Windows 10. Before you start the installation, ensure that the latest service packs and security patches have been applied.

Databases

The StarNet 2 SMS uses Microsoft SQL Server to store its configuration data. SQL Server 2014 Standard is included with the StarNet 2 SMS.

Note	Senstar strongly recommends that you install StarNet 2 on a dedicated computer. If you are installing it on a PC with other software (including other SMS or VMS software), check to see if SQL Server is already installed prior to starting the installation. An existing SQL Server installation may cause installation, configuration, or performance issues.

Senstar Network Manager

StarNet 2 works with the following Senstar network types: Silver, FiberPatrol, CCC, and Crossfire. Note the following requirements:

- The StarNet 2 SMS requires at least one actively running Network Manager.
- The Network Manager must be configured with the IP address of the StarNet 2 Server as it blocks connections from unregistered computers.
- The Network Managers may be installed on the same computer as StarNet 2 or on different computers, which have a network connection to the StarNet PC.

See the Network Manager documentation for information about installation and configuration.

Note	If your Network Manager is installed on the same computer as the StarNet 2 server, use 127.0.0.1 as the SMS IP address.

Note	It is strongly recommended that sensors only be added to the Network Manager after they are installed and functional. Adding improperly configured sensors to a StarNet 2 system will generate large volumes of network traffic and false alarms, thus reducing the overall effectiveness of the security management system and site security processes.

Off-Site Configuration and Testing

If you do not have access to your sensor network (for example, you are staging it at another location), you can use the Network Manager Simulator to simulate the Network Manager and the security sensors. The StarNet 2 SMS will function properly with the simulated data. When configuring the simulator, use the loopback IP address (127.0.0.1) for the SMS configuration.

Note	When using the simulator, the node order of the sensors MUST match the node order of the actual equipment exactly. If the ordering differs, the sensors' configuration will not work on the real system.

Universal Configuration Module

The Universal Configuration Module (UCM) is a Windows-based software application that performs the calibration, setup, maintenance and diagnostic functions for Senstar's line of intrusion detection sensors. The UCM connects directly to each device via USB. The UCM can also connect to sensors remotely through the Network Manager.

Note	Senstar recommends that the UCM application be installed on the StarNet 2 server. The system administrator can assign a UCM password to prevent unauthorized access to network based sensors.

Network Configuration

Tip	Windows 10 includes a search feature that enables easy access to the Windows configuration tools. Click the search box and type the name of the item. The item will be displayed in a Best Match search box. Click the name on the list and the item will open. To display the search box, right-click the clock area > Cortana > Show search box.

In a typical configuration, the StarNet 2 server and database are installed on the same computer. The server also includes the Setup and Workstation client applications. Each operator workstation requires its own client software.

- Multiple workstations – If multiple computers are used, each computer, along with the Network Manager, requires a fixed IP address and must be addressable from each other. Typically, each computer is on the same sub-network.
- Single standalone workstation – If the StarNet 2 SMS and the Network Manager are installed on a single computer and that computer is connected to a Senstar Silver Network via a USB connection, network interfaces are not required. In this case, the system will use the 127.0.0.1 loopback address.

Note	In a standalone system, deactivate any unused network interfaces. In the search box type "Settings" **> Network & Internet > Change adapter options**. Right-click on any unused connections, and select Disable.

IP Addresses

If your server or workstation is configured with multiple network interfaces (for example, one for Ethernet and one for WiFi), you may be prompted during installation to select one. If you do not know which IP address is used by which interface, run the **ipconfig** command from a Command Prompt window (in the search box type **"**Command Prompt").

Note	StarNet 2 automatically uses the first active network connection in the system and may not start correctly if the network configuration changes. To check the network adapter status: in the search box type **"**Settings" **> Network & Internet > Change adapter options**. You can prevent potential issues by disabling unused network adapters. Right-click on any unused connections, and select Disable.

PC Name and Workgroup

Each PC on the network must have a unique name and be within the same domain or workgroup. In the search box type "Control Panel" **> System & Security >** under **System** select **See the**

name of this computer in the Computer name, domain, and workgroup settings, select **Change Settings**. Select the **Change** button on the Computer Name tab and enter a unique **Name**, and a shared **Domain** and **Workgroup** name.

Firewalls

The StarNet 2 SMS is intended to be installed within a secure, protected network. During installation, disable any firewall software (including the Windows firewall) for each computer.To disable the built-in Windows firewall:

1. In the search box type “Settings” **> Update & Security > Windows Defender**.
2. Click the **Open Windows Defender Security Center** button then click **Firewall & Network Protection**.
3. Click **Turn Windows Firewall on or off**.
4. Turn off Windows firewall for Private Network settings and Public network settings.
5. Click **OK**.

Note	After installation, you should re-enable the firewall and test the system. See Firewall and Port Settings on page 111 for information about required ports and firewall settings.

Administrator Account

Log in using an administrator account during the installation process to prevent possible access or privilege issues.

To create an administrator user account:

1. In the search box type “Control Panel” > **User Accounts** > **Manage User Accounts**.
2. Click **Add**.
3. Create the required administrator user account (starnet2) and set a password (Senstar recommends the last 4 digits of the PC service tag).

Software Licensing

The use of StarNet 2 requires a software license that is provided on a USB flash drive. The number of licenses on the flash drive is based on the number of operator Workstation applications actively running. Running the Setup application does not count towards this number. The USB flash drive must be installed on a PC that is actively running the Workstation application.

Computer and Operating System Setup

The following lists the requirements for setting up the StarNet 2 computer and operating system.

1. BIOS settings: Enter the computer’s BIOS setup and enable the Power ON after AC power failure; Disable all Sleep and Power Saving settings.
2. Unpin all tiles from the Start menu: Select Start > right click a tile > select Unpin from Start.
3. Turn off notifications: In the search box type “Settings” **> System > Notifications and Actions > Turn OFF all notifications**.

4. Turn OFF Cortana: In the search box type “Settings” > **Cortana** > Turn **OFF** Cortana settings. (This will not affect the search box.)
5. Configure Windows Explorer to show extensions, hidden files and drives, and menus: Open File Explorer > View > Options check or uncheck the desired options.
6. Create a Power Plan “Always ON”: In the search box type “Windows System” **> Control Panel > Power Options > Create a power plan >** In Plan Name type “Always ON” then click **Next** > Disable all power conservation settings (e.g., Turn off display - Never; Disable the sleep settings; etc.).
7. Set User Account Control to Never notify about changes: In the search box type “Control Panel” **> User Accounts > Change User Account Control Settings >** set Choose when to be notified about changes to your computer to Never Notify.
8. Windows Login: In the search box type “run” > type “netplwiz” and uncheck **Users must enter a name and password > select OK**.

Note	To ensure communication between StarNet 2 and the SQL database, the Locale must be set to English (United States).

9. Set Locale to English (United States). In the search box type “Control Panel” **> Region > Administrative > Change System Locale >** select **English (United States)**.
10. Verify Windows 10 Pro is installed and activated then download all Windows updates: In the search box type “System Configuration” **> Tools > System Properties > Launch**.
    In the search box type “Updates” **> Check for Updates**.
11. Disable Windows updates: In the search box type “Administrative Tools” **> Services >** disable **Update Orchestration Service** and **Windows Update**.
12. Right-click the taskbar and uncheck **Show People**.
13. Disable Internet time synchronization: Right-click the clock > select **adjust date/time** > select **add clocks for different time zones > Internet time >** uncheck **Synchronize with Internet time server**.
14. Uninstall undesired applications: In the search box type “Apps & features” scroll through the list to choose and uninstall unwanted programs (e.g., Microsoft Solitaire Collection).

Install StarNet 2 Server

Installation of the StarNet 2 Server consists of three steps:

1. Install the StarNet 2 Server software
2. Start the StarNet 2 services
3. Perform an initial backup

Note	Before installing the StarNet 2 software, check the installation package for any build-specific installation instructions or readme files. If the installation of SQL server fails, check the specified log files for information.

Step 1: Install StarNet 2 Server

1. Run **Setup.x.x.x.xx.exe**.
2. If prompted to allow changes, click **Yes**.
   The installation wizard starts.
3. Click **Next**.
4. Select **Server (Full installation includes Client)**.

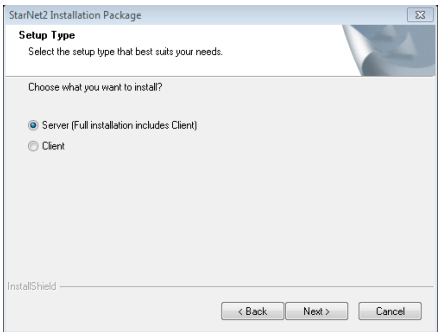


Figure 4: StarNet 2 installation dialog

5. Click **Next**.
6. The next step differs depending if this is a new system or an upgrade:
   - New installation: select **Install Microsoft SQL Server 2014 Standard** and click **Next**.
   - Upgrade: The installer will automatically detect the existing database.
   - Existing database on different computer: select **Using Existing SQL Server Instance** and click **Next**.
7. A message stating which database will be used is displayed. Click **Next**.
8. If you are performing a new installation, you will need to enter a system administrator (sa) password and license key for SQL Server 2014 (included in the readme file). Click **Install SQL Server**.

Note	Use a strong password (minimum 8 characters with at least one capital and one number); otherwise SQL Server may generate warnings and the installation process may fail. Enter the license key EXACTLY as shown in the readme file.

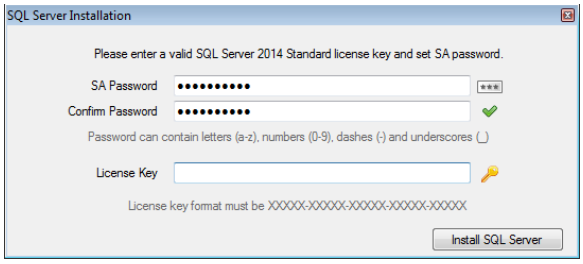


Figure 5: SQL Server installation window

The SQL database will be installed. This may take a few minutes.

9. Enter the database connection settings. Configure authentication to use the system administrator (sa) password.

Note	Normally you can use the default (local) setting. However, if your database is running on a different computer or under a different instance (non-default instance), you must specify the IP address and instance name (for example, 127.0.0.1/SQLSERVER).

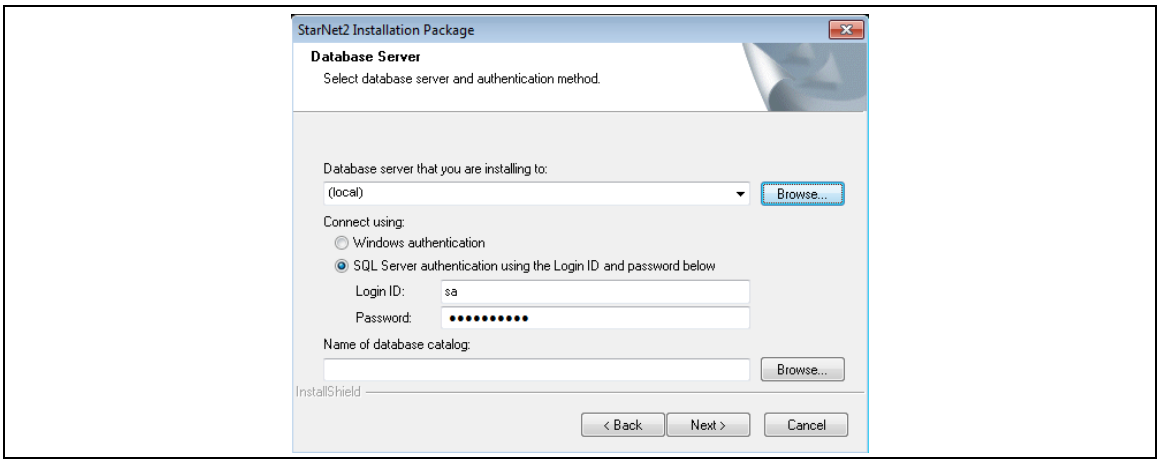


Figure 6: Database Server installation window

10. Click **Next**.
    The installer will create or upgrade the databases as required.
11. Click **Install** to start the installation of the StarNet 2 applications.
12. If your workstation is configured with multiple network interfaces, a pop-up window will appear prompting you to select the IP address to use with StarNet 2.
    Select the IP address from the dropdown and click **OK**.

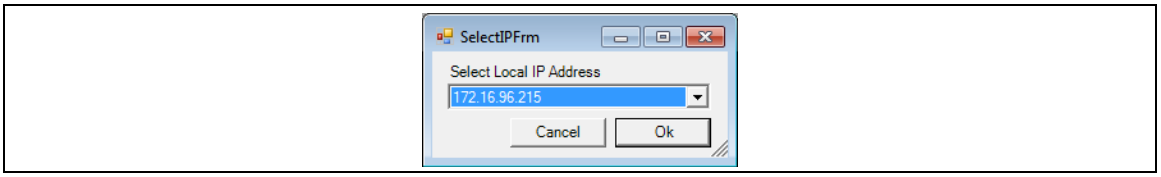


Figure 7: Select IP window

The command window may open several times and run a set of maintenance tasks

13. Click **Finish**.

You are now ready for Step 2, Start StarNet 2 Services.

Step 2: Start StarNet 2 Services

The StarNet 2 SMS Server uses background services to communicate with the Network Manager and manage the database. Before you start the StarNet 2 services, ensure that the Network Manager (or Network Manager simulator) is operational and configured to communicate with the StarNet 2 SMS. If not, the security sensors will not be populated correctly.

1. If there is an icon on your desktop labeled “Watchdog”, rename it as “Service Manager”.
2. Check to see if the Service Manager is running in the Windows taskbar. It should start automatically after installation.

   If you cannot see the Service Manager icon, you may need to adjust the taskbar settings. Right-click in the clock area, select **Taskbar Settings**, under Notification area click **Select which icons appear on the taskbar** and ensure that the Magal.S3.Server.Watchdog is switched ON.

   If it isn't already started, right-click on the Service Manager shortcut on the Windows Desktop and select **Run as Administrator**.
3. Right-click the Service Manager icon .
4. Start all the StarNet 2 services by clicking **Watchdog** (under the Services category). The Watchdog service is responsible for starting and stopping all StarNet 2 services.

The icon indicates the state of the service:

Service is running, click X to stop service

Service is not running, click arrow to start service

5. After the services are started, the following two applications appear in the Service Manager menu under Applications:

StarNet 2 Workstation	Opens the local StarNet 2 Workstation client.
StarNet 2 Setup	Opens the StarNet 2 Setup application. From the Setup application, you can configure security sensors, maps, and workstations.

6. The first time Setup is run the Station Connection Settings dialog box will be presented to select the IP address of the database and the IP address of the video system (if one is present). For the database IP address enter the IP address of the computer where the SQL databases created by StarNet 2 are located. This is normally the same computer that is running the StarNet 2 server components so 127.0.0.1 can be used. The Use Video System field selects the video system in use. Select either Airship, Aimetis (Symphony), or None. Select Automatic event printing to send every event to a line printer. This requires a line printer to be configured in Windows as the default printer (see Line Printers.)

Figure 8: Station Connection Settings

Step 3: Backup Database

Senstar recommends that you make an initial backup of the newly created database. This will let you “start over” a site configuration without having to re-install the software.

1. Perform a backup of the new StarNet 2 databases, as described in Backing Up Database & Site Configuration on page 81.
2. Copy the .bak files to a new, permanent location.

Rename the files such that you will be able to differentiate them from other, post-configuration, backup files.

Configure Network Manager

After installing the StarNet 2 Server, you need to configure the IP address(es) of the Network Manager(s). The Network Manager is responsible for relaying the status of the security sensors to the StarNet 2 SMS. StarNet 2 now supports an unlimited number of network manager connections. This enables StarNet 2 to monitor multiple sites from a central location, or to monitor a site with multiple Network Managers (see Adding Additional Network Managers on page 25).

Note	Any time that you make changes to the Network Manager, you must stop all StarNet 2 services, refresh the database, and restart the services.

Configure Network Manager

1. If necessary, start the StarNet 2 Setup application:
   a. On the StarNet 2 Server, right-click the Service Manager icon on the Windows taskbar and select **StarNet 2 Setup**.
   The StarNet 2 Setup application is started.
   b. If any warning messages are displayed, click **Close** to dismiss them.
2. Expand **Sensors**. If the tree is already populated with sensors, you can skip this procedure. If the Sensors node doesn't appear or is empty, continue with this procedure.
3. Expand **Pub Sub Configuration** > **SystemComponent**.
4. Configure Network Manager Bridge:
   a. Double-click **SenstarNMBridge**.
   The Properties window on the right displays the network settings.
   b. In the Initialize property, click the Initialize button.
   The Initialize window is displayed.

Figure 9: Select the Initialize button

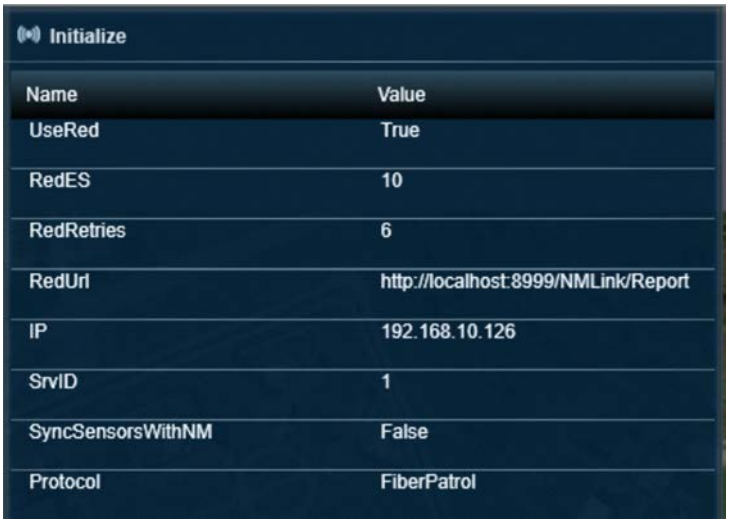


Figure 10 Initialize window

c. In the IP property, configure the following parameters:

IP	The IP address of the Network Manager. Use the loopback IP address (127.0.0.1) if the Network Manager is on the same computer as the server.
SrvID	The Id of the Network Manager (typically "1" if StarNet 2 is only monitoring one Network Manager). If there is more than one Network Manager running, this number will change, as each Network Manager has its own ID value. You MUST use a unique SrvID for each Network Manager, even if they are located on different computers.
SyncSensorsWithNM	True or False. When enabled, StarNet 2 will auto-discover all possible sensor points each time its services start. You must leave this enabled the first time you launch Setup. After your site configuration is complete, change this value to False to speed up startup time.
Protocol	The protocol used by the specified Network Manager. Valid entries are: • **Silver** – For FlexZone, OmniTrax, FlexPS, UltraWave, XField, Senstar LM100, FP400, UltraLink I_O systems and Alarm Logic Engine • **Silver** – For MX Controller and MX Zone devices • **FiberPatrol** – For FiberPatrol Sensor Unit and Redundant Sensor Unit • **CCC** – For CCC-based systems • **Crossfire** – For Crossfire-based systems

d. Click **OK**.

e. Click **Save**.
The IP address of the Network Manager is updated.

5. Exit the StarNet 2 Setup application by clicking **Exit**.
6. Stop the StarNet 2 services: Right-click the Service Manager on the Windows taskbar and stop all the services by clicking **Watchdog**. All the services will stop after a few seconds.
7. Refresh the StarNet 2 settings. Right-click the Service Manager on the Windows taskbar and select **Settings > Refresh**.
8. Start the StarNet 2 services: Right-click the Service Manager on the Windows taskbar and select **Watchdog**.
9. Start the StarNet 2 Workstation application: Right-click the Service Manager on the Windows taskbar and select **StarNet 2 Workstation**. Wait until the StarNet 2 Workstation application is started and confirm that sensor synchronization is completed (see Synchronize Sensors on page 27). Exit the StarNet 2 Workstation application.
10. Start the StarNet 2 Setup application: right-click the Service Manager on the Windows taskbar and select **StarNet 2 Setup**.
The StarNet 2 Setup application is started.
11. Ignore any warning messages by clicking **OK**.
12. Expand **Sensors**.
If the Network Manager is configured correctly, it will be populated with entries from your site's security sensors.

Adding Additional Network Managers

If you are using StarNet 2 to monitor several Network Managers, you will need to add and configure additional Network Manager bridges.

Note	Do not change the Service Name or the Service Display fields of the pre-installed Network Manager.

Note	It it extremely important that you follow these procedures carefully. StarNet 2 will not function properly if the Network Manager bridges are configured incorrectly.

1. Configure the first Network Manager, as described above.
2. Expand **Pub Sub Configuration** > **SystemComponent**.
3. Double-click **SenstarNMBridge**.
   The Properties window on the right displays the Silver Network settings for the first Network Manager.
4. Click **Copy**. A clone of the existing bridge properties is displayed.

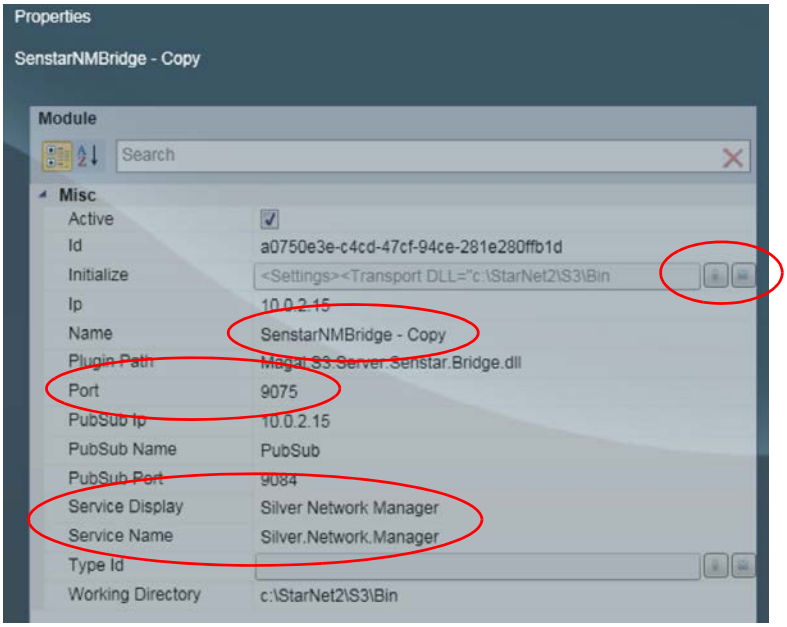


Figure 11: Bridge Properties Copy window

5. In the Initialize property, click the Set button.

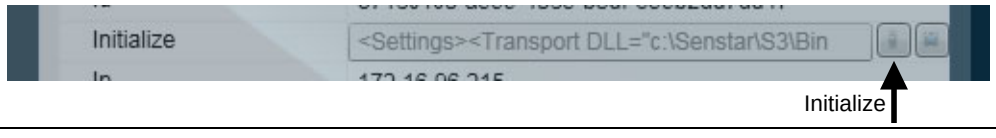


Figure 12: Select the Initialize button

6. Enter the IP address, ID number, and Protocol of the new Network Manager.

Figure 13: Entering the NM ID

7. Click **OK**.
8. In the Name field, enter a descriptive name for the bridge (for example, *NM Bridge 2*).

Note	Do not name the bridge “Network Manager #”, as that name is reserved for use by the Network Manager services.

9. Enter a unique port number (unused by any other services or software on the PC) for the NM bridge service in the Port field (for example, 11001). This port number **MUST** be different than the port number used by the other Network Manager bridge and must not exceed 65535**.**

Note	If you are unsure about which ports are used by your system, run “netstat -an” from a console window and ensure your port number is not in use.

10. Modify the Service Display and Service Name fields so they have different values than the original Network Manager settings (for example, use “Silver Network Manager 2” and “Silver.Network.Manager2”)
11. Click **Save**.
12. Create a StarNet 2 technology instance for the new bridge component:
    a. Select **Misc > Technology**.
    b. Click **New**.
    c. In the Name field, enter a descriptive name (for example, “SN2 Bridge Tech2”).
    d. In the Technology Type field, select **StarNet**.
    e. In the Id field, click the Initialize icon and select the Network Manager bridge component you previously defined. Your new technology component should look similar to the following:

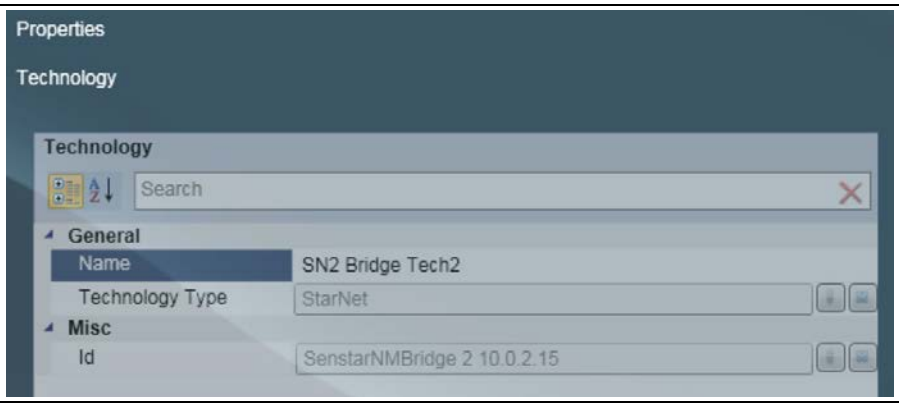


Figure 14: Creating the technology instance

    f. Save the changes.
    g. Repeat this process for any other Network Managers.

13. Exit the StarNet 2 Setup application by clicking **Exit**.
14. Stop the StarNet 2 services: Right-click the Service Manager on the Windows taskbar and stop all the services by clicking **Watchdog**. All the services will stop after a few seconds.
15. Refresh the StarNet 2 settings. Right-click the Service Manager on the Windows taskbar and select **Settings > Refresh**.

CAUTION	The synchronization process can take several minutes to complete. Confirm that synchronization has completed before launching Setup and making any sensor changes. Failure to do so may result in a corrupted sensor database.

16. Start the StarNet 2 services: Right-click the Service Manager on the Windows taskbar and select **Watchdog**.
17. Start the StarNet 2 Setup application: right-click the Service Manager on the Windows taskbar and select **StarNet 2 Setup**.
    The StarNet 2 Setup application is started.
18. Ignore any warning messages by clicking **OK**.
19. Expand **Sensors**.
    If the new Network Manager is configured correctly, it will appear in the Sensors tree and be populated with entries from its sensors.
20. Repeat this procedure for any additional Network Managers.

Note	If all of the Network Managers do not appear in the Setup application, see Network Managers not appearing in Setup on page 98.

Synchronize Sensors

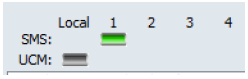
By default, StarNet 2 downloads a list of the available sensor points provided by the Network Manager. This process, sensor synchronization, occurs automatically each time the StarNet 2 services are started.

Depending on the number and type of sensors used in your system, synchronization may take several minutes to perform. Once a system is ready to go live at a site, Senstar recommends that you disable sensor synchronization. See Configure Network Manager on page 23 for additional information about disabling sensor synchronization.

CAUTION	Before performing any map creation or sensor configuration, ensure that the synchronization process has successfully completed. Failure to do so may result in a corrupted sensor database.

To confirm that the sensors have synchronized:

1. Make sure that the Network Manager and StarNet 2 Network Manager bridge services are configured and running. The SMS light in the Network Manager should be green.



2. Launch the StarNet 2 Workstation application.
3. If prompted, enter the IP address of the database:

- In a typical installation, where the database is installed on the same computer and is running as the default instance, type in “127.0.0.1”.
- If you are running the database on a different computer or with a named instance, enter the IP address and instance name, if required (e.g., 10.0.0.1/SQLINSTANCENAME).

4. If the Workstation application does not start, launch the Workstation application again and, if prompted, terminate the existing process.
5. Ignore any error messages that may appear.
6. The Workstation application will start. Observe the network status icon:

   During synchronization, the icon will display a caution symbol. 

   The caution symbol changes to a green checkmark when synchronization is complete. 

7. After synchronization is completed, exit the Workstation application.
8. Launch the Setup application.
9. Inspect the sensor points in the System Control tree. The sensors must appear in the following order:

   Sensors > *network_manager_name* > *sensor_name* > *sensor_point_name*

Figure 15: System Control tree

If any sensor points are missing, or if the sensor tree is incorrect (e.g., sensor points appear directly under the network manager rather than the sensor name), sensor synchronization is not complete. If this occurs, you MUST exit the Setup application, restart all StarNet 2 services, and wait for sensor synchronization to finish.

CAUTION	DO NOT proceed to edit picture-maps and sensors if the sensor tree is incorrect. This could potentially cause the sensors to stop working and force you to recreate the maps.

10. If the sensor tree is correct and all your sensors are present, you may begin configuring the picture-maps (see Sensors and Picture-Maps on page 39).

Configure StarNet 2 Shortcuts

System administrators and operators can access the StarNet 2 applications in three ways:

- By right-clicking the Service Manager tray icon and selecting StarNet 2 Workstation or StarNet 2 Setup (default)
- By double-clicking a desktop icon
- By configuring the Workstation application to start automatically after boot-up

Configuring desktop icons:

1. Right-click the Service Manager on the Windows taskbar and select **Applications > Create Shortcuts**.

   The Shortcuts utility is displayed.

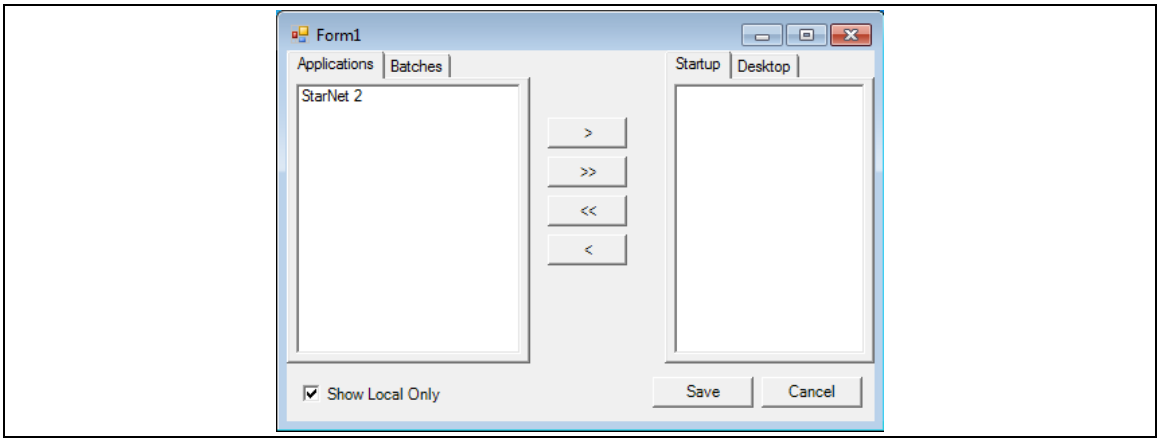


Figure 16: Shortcuts utility

2. Click the Applications tab
3. Click the Desktop tab.
4. Select **StarNet 2**.
5. Click the **>** (add) arrow.
6. Click **Save**.
   Shortcuts for the Setup and Workstation applications appear on the desktop. You can now double-click a shortcut icon to start the application.

Adding StarNet 2 to the Startup folder

The StarNet 2 installation package includes a Windows batch file that will automatically start the StarNet 2 Service Manager and the StarNet 2 operator application when the computer boots up.

Note	The Network Manager Service must also be configured to autostart.

1. Using Windows file explorer, copy autostart.bat which is located on the StarNet 2 USB key in a folder named Batch Files.
2. Paste autostart.bat into the Windows Startup folder: C:\Users\"*username*"\App Data\Roaming\Microsoft\Windows\Start Menu\Programs\Startup.
3. Restart the computer.

Following bootup the StarNet 2 operator application will be running. If the Network Manager Service was configured to autostart on this computer, it will also be running.

Note	If the Workstation application does not automatically start upon reboot/ user login, you may need to adjust the Windows UAC settings.

Note	Do not delete the Service Manager (or Watchdog) shortcut; this is required to start the Service Manager in the task tray.

The following is the content of autostart.bat (which can be edited in Notepad or another text editor):

```
start C:\StarNet2\S3\Bin\Magal.S3.Server.WatchDog.exe /t
start C:\StarNet2\S3\Bin\Magal.S3.Server.WatchDog.exe /r /n="StarNet 2" /o="Workstation"
```

3 Workstation Installation

This chapter explains how to install a StarNet 2 workstation. Workstation installation is similar to that of installing the server, only you don't install the database.

During the workstation installation, you will perform the following procedures:

- Review the Installation Requirements on page 31
- Install Workstation Software on page 33
- Copying Map and Sound Files on page 36

This chapter also explains Modifying Workstations After Installation on page 37

Note	Before proceeding with a workstation installation, you must have the workstation connected to the network and have SQL Server running on the server.

Installation Requirements

Before proceeding with the installation, review the following requirements and ensure that each one is met.

Operating Systems

The StarNet 2 client workstation runs on the following operating systems:

- Windows 7 (32/64 bit) with Service Pack 1
- Windows 8.1 Pro
- Windows 10

Note	The procedures described in this user guide are written for users running Windows 10. Before you start the installation, ensure that the latest service packs .NET libraries, graphics drivers, and security patches have been applied. Also, disable the screen saver, power saving modes, and Windows time synchronization (if applicable).

Network Configuration

If your server or workstation is configured with multiple network interfaces (for example, one for Ethernet and one for WiFi), you may be prompted during installation to select one. If you do not know which IP address is used by which interface, run the ipconfig command from a Command Prompt window (in the search box type "**Command Prompt**" **> ipconfig**).

Before installing the software, ensure the workstation can access the server over the network (in the search box type "**Command Prompt**" **> ping <server_ip>**)

Note	StarNet 2 automatically uses the first active network connection in the system and may not start correctly if the network configuration changes. To check the network adapter status in the search box type "Settings" > **Network & Internet > Change adapter options**. You can prevent potential issues by disabling unused network adapters. Right-click on any unused connections, and select Disable.

PC Name and Workgroup

Each PC on the network must have a unique name and be within the same domain or workgroup. Go to **Control Panel > System & Security >** under **System** select **See the name of this computer** in the Computer name, domain, and workgroup settings, select **Change Settings**. Select the **Change** button on the Computer Name tab and enter a unique **Name**, and a shared **Domain** and **Workgroup** name.

Firewalls

The StarNet 2 SMS is intended to be installed within a secure, protected network. During installation, disable any firewall software (including the Windows firewall) for each computer. To disable the built-in Windows firewall:

1. In the search box type "Settings" > **Update & Security > Windows Defender**.
2. Click the **Open Windows Defender Security Center** button then click **Firewall & Network Protection**.
3. Click **Turn Windows Firewall on or off**.
4. Turn off Windows firewall for Private Network settings and Public network settings.
5. Click **OK**.

Note	After installation, you should re-enable the firewall and test the system. See Firewall and Port Settings on page 111 for information about required ports and firewall settings.

Administrator Account

Log in using an administrator account during the installation process to prevent possible access or privilege issues.

To create an administrator user account:

1. In the search box type **"**Control Panel" **> User Accounts > Manage User Accounts**.
2. Click **Add**.
3. Create the required administrator user account and set a password.

Licensing

The use of StarNet 2 requires a valid software license that is provided on a USB flash drive. The number of licenses on the flash drive is based on the number of operator Workstation applications actively running. Running the Setup application does not count towards this number. The USB flash drive (one per site) must be installed on a PC actively running the Workstation application.

Install Workstation Software

Installation of the StarNet 2 Workstation consists of two steps:

Step 1: Install the StarNet 2 client software on page 33.

Step 2: Start StarNet 2 Services on page 35.

Note	Before installing the StarNet 2 software, check the installation package for any build-specific installation instructions or readme files.

Step 1: Install the StarNet 2 client software

1. Confirm that SQL Server is running on the server and that the workstation PC has network connectivity with the server.
2. Log in as an administrator to the workstation.
3. Open the folder or drive containing the StarNet 2 installation files.
4. Run **Setup.x.x.x.xxxxxx.exe**.
5. If prompted by User Account Control to allow changes, click **Yes**.
   The installation wizard starts.

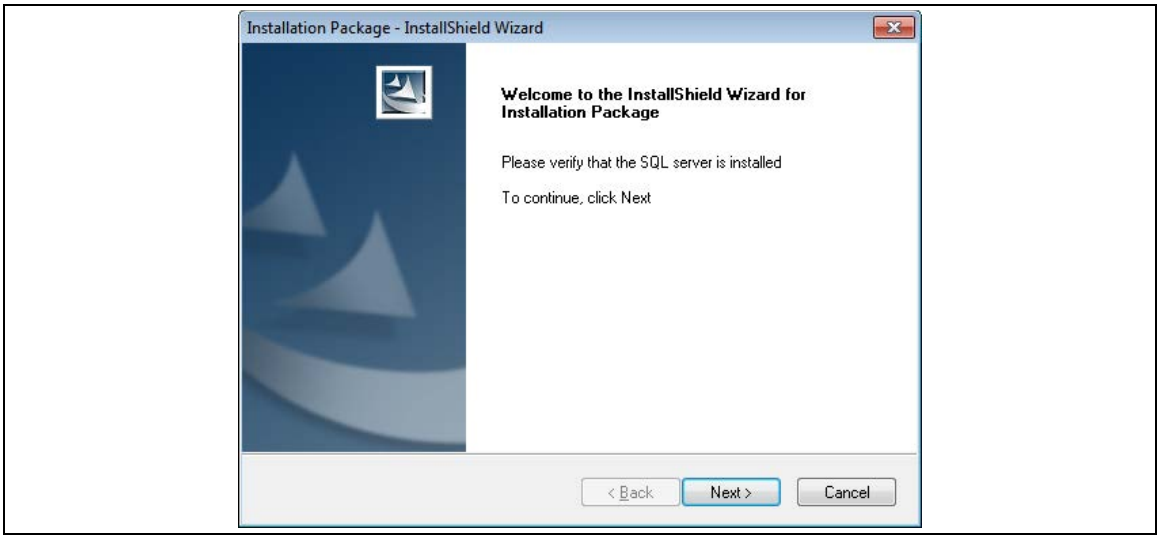


Figure 17: Installshield Wizard dialog

6. Click **Next**.
   The Setup Type dialog is displayed.
7. Select **Client**.

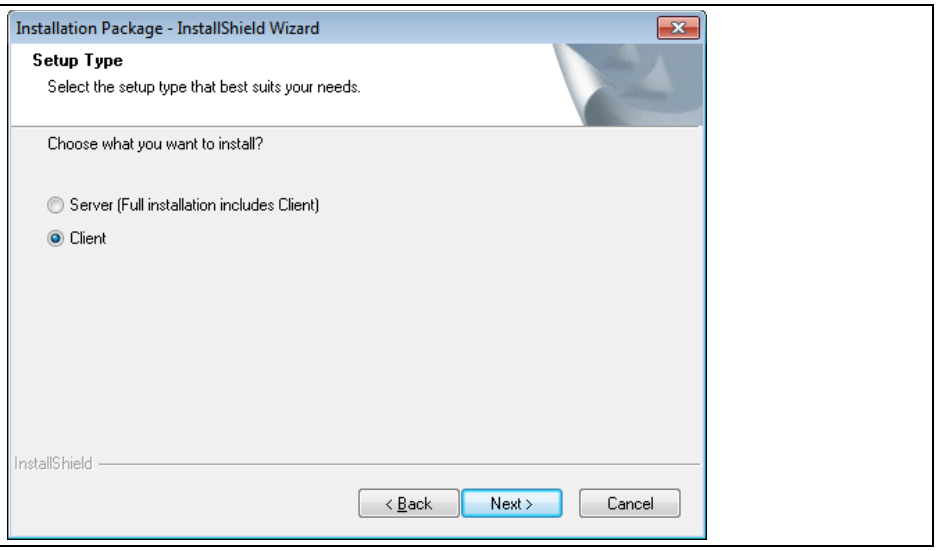


Figure 18: Select Client

8. Click **Next**.
   The Database Server screen is displayed.
9. Click **Browse** and select the server running the SQL database.

Note	If the database cannot be found, you can enter its IP address manually. However, you should confirm network connectivity to the server (e.g. ping the server). If you encounter any errors during installation, database connectivity was likely not established and you will need to re-install the client software.

10. Enter the Login ID (sa) and Password for the SQL databases. These are the same authentication values you used when installing SQL Server (see Install StarNet 2 Server on page 19).

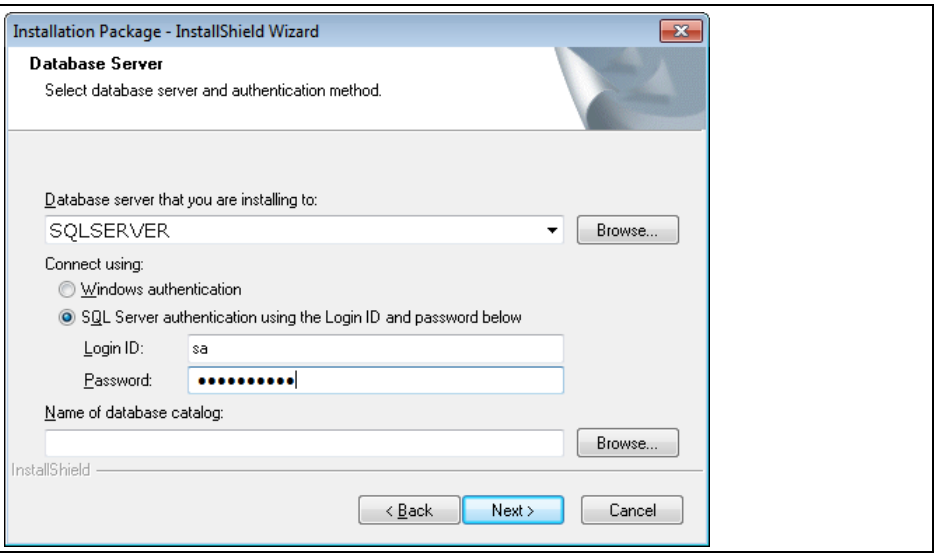


Figure 19: Select Database server dialog

11. Click **Next**.
    The Ready to Install the Program dialog is displayed.

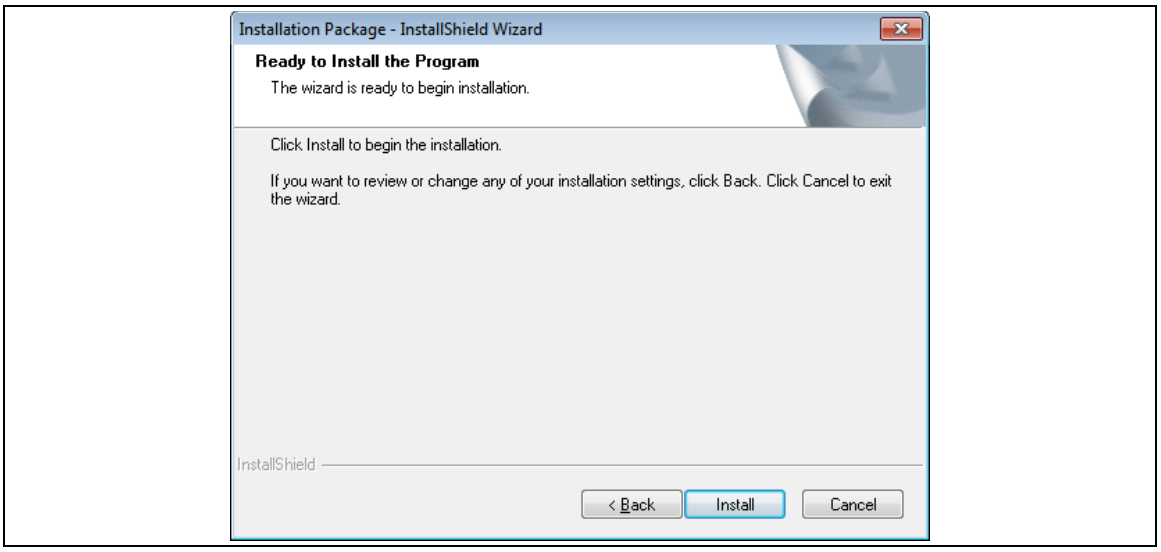


Figure 20: InstallShield Wizard dialog

12. Click **Install**.
13. If your PC is configured with multiple network interfaces, a pop-up window will appear prompting you to select the IP address to use with StarNet 2. Select the IP address from the dropdown and click **OK**.

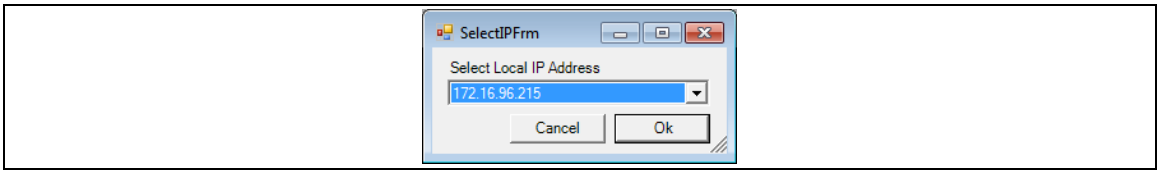


Figure 21: Select IP dialog

The command window opens and a set of maintenance tasks are run.

14. When prompted, enter a name for this new workstation. This name will appear in the StarNet 2 operator interface and be used when acknowledging and transferring events.

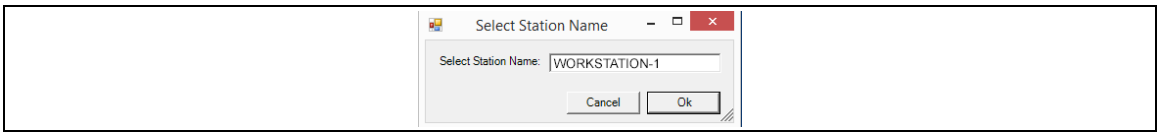


Figure 22: Select Station Name dialog

15. Follow onscreen instructions.
16. Click **Finish**.

You are now ready for Step 2, Start StarNet 2 Services.

Step 2: Start StarNet 2 Services

The StarNet 2 client uses background services that communicate with the StarNet 2 server:

1. On the server, exit any open StarNet 2 application, stop all services, perform a refresh, and restart the services.
2. On the workstation, If there is an icon on your desktop labeled “Watchdog”, rename it to “Service Manager”.

3. Check to see if the Service Manager is running in the Windows taskbar. It should start automatically after installation.
   If you cannot see the Service Manager icon, you may need to adjust the taskbar settings. Right-click in the clock area, select **Customize notification icons**, and ensure that the Watchdog behavior is set to **Show icon and notifications**.
   If it isn't already started, right-click on the Service Manager shortcut on the Windows Desktop and select **Run as Administrator**.
4. Right-click the Service Manager icon and select **Settings > Refresh.**
5. Right-click the Service Manager icon and start the StarNet 2 services by clicking **Watchdog** (under the Services category). The Watchdog service is responsible for starting and stopping all StarNet 2 services in the current computer.
   The icon indicates the state of the service:

   Service is running

   Service is not running.
6. After the services are started, the StarNet 2 applications appear in the Watchdog menu:

<*Name*> Workstation	Opens the local StarNet 2 Workstation application.
<*Name*> Setup	Opens the StarNet 2 Setup application. From the Setup application, you can configure security sensors, maps, and workstations

7. Test the installation by launching StarNet 2 Workstation.
8. If prompted, enter the IP address of the database:
   - In a typical installation, where the database is installed on the same computer and is running as the default instance, type in “127.0.0.1”.
   - If you are running the database on a different computer or with a named instance, enter the IP address and instance name, if required (e.g. 10.0.0.1/SQLINSTANCENAME).
9. If the Workstation application does not start, launch the Workstation application a second time and, if prompted, terminate the existing process.

Copying Map and Sound Files

Whenever you add a workstation, or a new map, sound, or icon, you need to manually copy the new files to each workstation:

- Maps: Copy the .JPG files to c:\StarNet2\fortis4g_data\sensor_images
- Sounds: Copy the .WAV files to c:\StarNet2\fortis4g_data\sounds
- Icons: Copy the .PNG files to c:\StarNet2\fortis4g_data\icons

Modifying Workstations After Installation

Workstations are automatically added and configured in the system during installation. However, you may need to adjust a workstation's configuration post-installation as a result of changes to the system (e.g., to limit access only to the operator application, to change IP addresses, to change a workstation's name).

There are two system components that contain each workstation's configuration:

- A StarNet 2 component, located in **PubSub Configuration > SystemComponent**.
- A Station component, located in **Stations**.

To modify an existing workstation configuration

1. Exit the workstation whose configuration you intend to change.
2. In the StarNet 2 Setup application (located on the server), expand **Pub Sub Configuration** > **SystemComponent**.
3. Double-click the name of the station.
4. If required, enter a new name for the station.
5. If required, configure the applications for the new workstation by clicking the Initialize icon.
   - Select **[Workstation: STARNET2]** if the workstation will only run the operator application and then click **OK**.
   - Select **[Workstation: STARNET2|Setup:SETUP_STARNET2]** if the workstation will run both the operator and setup applications and then click **OK**.
6. If required, configure the IP address parameter.
7. Click **Save**.
8. Expand **Stations**.
9. Select **Station**.
10. Double-click on the station number.
11. Click the Component initialize icon.
12. Select the workstation name from the list (e.g. "Workstation 2").
13. Click **OK**.
14. Enter a unique number for the Station Number parameter (e.g. 2). Note that 99 is typically used by the workstation instance running on the server.
15. Click **Save**.

4 Sensors and Picture-Maps

Each sensor managed by StarNet 2 appears under the Sensor node in the System Control tree. Sensors are organized as follows: Network Manager > Sensor Name > Individual sensor node.

The available sensor control nodes are dependent on the type of sensor. For example, a FlexZone sensor has individual nodes for each zone as well as auxiliary inputs and relay outputs, whereas a an UltraLink I/O sensor only has input and output control nodes.

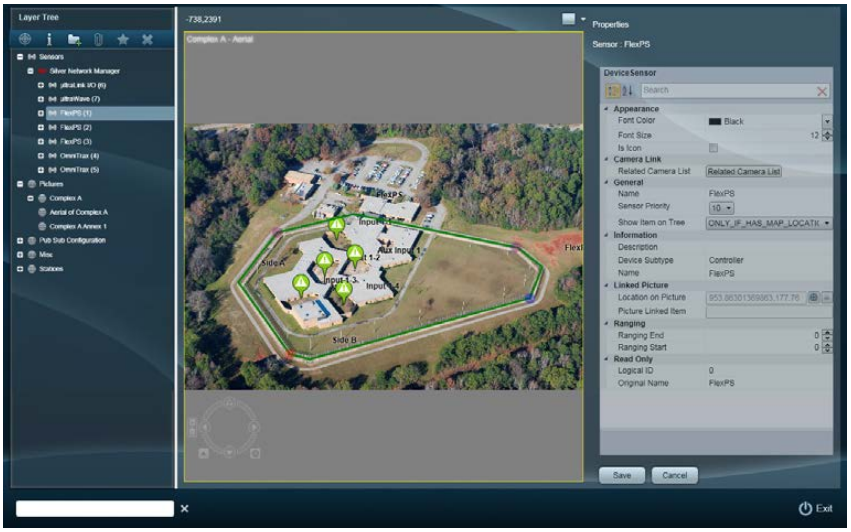


Figure 23: StarNet 2 Setup Application

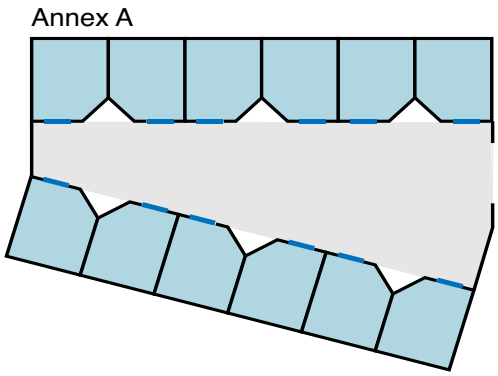
In this chapter

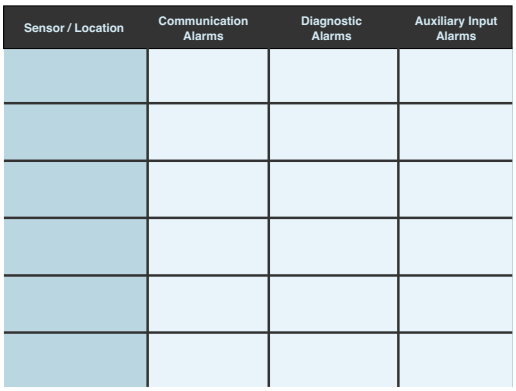
Picture-Maps

A key feature of StarNet 2 is the ability to display the location and coverage area of security sensors over your own custom images (called picture-maps). You can add as many picture-maps as you require. For example, you can add an overview map that shows the entire site and several detailed maps that show specific areas. Each map must be in .jpeg format.

Choosing Images

When choosing an image, note the following recommendations.

	Aerial photos may be obtained from map web sites, mapping software, or survey companies. When selecting an aerial photo, use one that: • shows the necessary coverage area • uses a perspective that doesn't hide or obscure key locations • has sufficient resolution to clearly indicate key building details • ensure the jpeg image doesn't have any visible compression artifacts
	Drawings of building layouts or floor plans can be used. These are useful for indoor areas or areas where there are too many sensors to fit on a photo. When selecting a layout or floor plan: • add titles or text to ensure maps are distinguishable • avoid complicated line patterns that may be difficult to view on smaller computer screens • use solid colors or gradients to indicate different areas • use neutral colors to ensure security sensors are clearly visible • ensure the jpeg image doesn't have any visible compression artifacts
	Drawings that provide a background over which the security sensors can be organized. Like with layouts or floor plans: • avoid complicated line patterns that may be difficult to view on smaller computer screens • use solid colors or gradients to indicate different areas • use neutral colors to ensure security sensors are clearly visible • ensure the jpeg image doesn't have any visible compression artifacts



Drawings that provide a grid on which equipment status alarms can be organized.

- avoid using small text that may be difficult to read on smaller computer screens
- use solid colors or gradients to indicate different functional areas
- use neutral colors to ensure sensors are clearly visible
- ensure the jpeg image doesn't have any visible compression artifacts

Preparing Images

After you have chosen your images, open them in an image editor (e.g. Microsoft Paint) and ensure that they are cropped, sized correctly, and saved as jpegs. The dimensions of the image should be set to display correctly on the workstation's screen when zoomed to a 100% (actual size). All images must be saved in JPEG (.jpg) format. On a dual-display system using 1920 x 1080 monitors (standard size), the images should be 1873 x 959.

Map Groups

Images are organized into groups. Groups can be organized in any manner; typically by area, site, or building. Use descriptive names to ensure maps are easily identifiable.

Add Picture-Maps

Note	Before adding picture-maps to your system, verify that a folder named sensor_images is in the fortis4g_data folder: C:\StarNet2\fortis4g_data\sensor_images If the sensor_images folder is not there, create one.

1. If required, start the StarNet 2 Setup application.
2. Select **Picture-Map**.
3. Add a picture group (you need at least one picture group):
   a. Click **New**.
   The Properties window is displayed for the new picture group.
   b. Enter a Name.

Note	The name you enter will affect where in the list the map appears. Maps are organized alpha-numerically in both the lists and thumbnail images.

   c. Click **Save**.
   The picture group is added to the system.
   d. Add any additional picture groups as required.
4. Add a new site picture-map:
   a. Select the picture group that will contain your site maps.
   b. Click **New**.

The Properties window is displayed for the new site map.

c. In the File Name property, click the Find File icon.

Figure 24: Creating the technology instance

The Select a file window is displayed.

d. Select the file to use as a picture-map and click **Open**.

e. In the Name property, enter the name of the map as you want it to appear in the Pictures list.

f. Click **Save**.
The picture-map is added to the system.

g. Add any additional image maps as required.

5. Review the images by double-clicking on each one in the Pictures list. Once you are satisfied, you can proceed to Security Sensors on page 42.

Note	Anytime you add a picture-map to the system, you need to manually copy the JPEG files to each workstation (see Copying Map and Sound Files on page 36).

Setting the Default Picture-Map

A picture can be set as the default picture-map for when the StarNet 2 software starts up.

1. While in the Setup application, go to Picture map.
2. Select the desired picture and mark it as default.

SrarNet 2 picture-maps can be panned and zoomed. This feature is enabled via the General Configuration Properties window.

Security Sensors

The StarNet 2 SMS makes it easy to place your security sensors and their coverage area on your custom maps. Configuring a sensor consists of two steps:

1. Select the sensor and place it on the map
2. Configure the sensor's properties.

Note	In order for a sensor to appear in the lists used by rules and procedures, it must be added to a picture-map (or have its properties changed to always appear in the lists). Sensors, for which location is not important, can be added to a dashboard or status screen picture-map.

Sensor Representation on a Map

There are three ways to represent a sensor on a map:

- Polylines,
- Sensor icons, and
- Monitor icons.

Type	Graphic	Description	Examples
Polyline		You can draw lines to represent the area of coverage. Lines consist of multiple straight segments. Each point can be positioned independently. Lines are typically used to represent perimeter intrusion sensors or sensors that have a coverage area. If the sensor supports ranging, the location of the intrusion can be displayed as a dot on the sensor line. The red circle indicates the start of the sensor range (e.g. 1 m); the blue circle indicates the end of the sensor range (e.g. 300 m).	Omnitrax, UltraWave, FlexZone, FiberPatrol, Senstar LM100
Sensor icon		You can represent sensors that have a specific position with an icon. The icon changes color and image depending on the type of alarm.	Auxiliary inputs such as gate contacts
Monitor icon		You can use monitor icons to indicate the status of an input. Monitor icons do not generate alarms. The icon changes color depending on its state: • Green: Input asserted • Red: Input de-asserted • White: Input supervision state	Auxiliary inputs that indicate the result of other systems (e.g. a door closed indicator)

Figure 24 shows the Setup application. In this example, there are both polyline and discrete sensors added to an aerial view map.

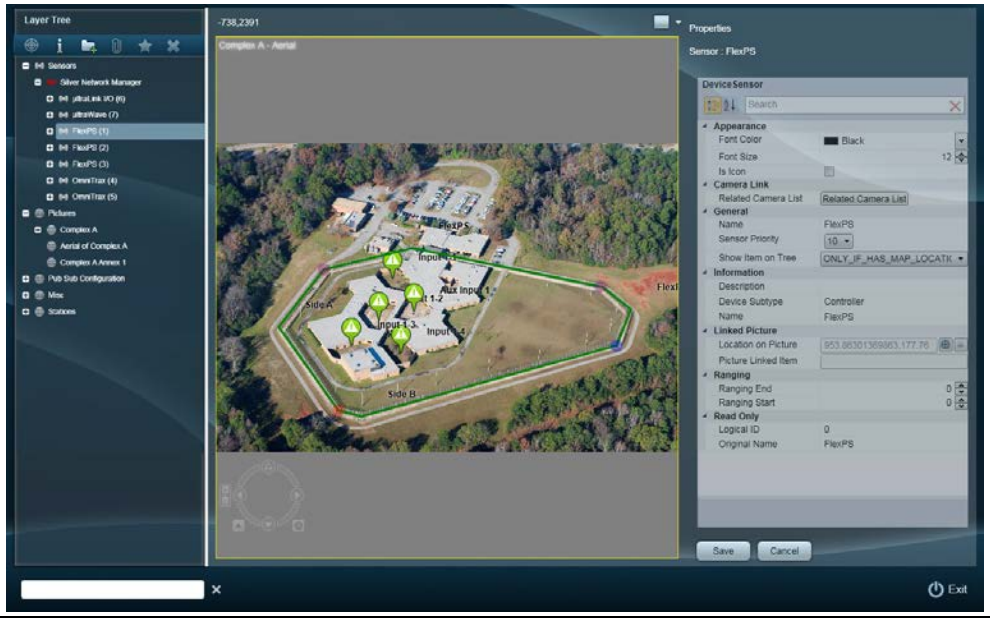


Figure 25: Sample Security Sensor Configuration

Sensor Names

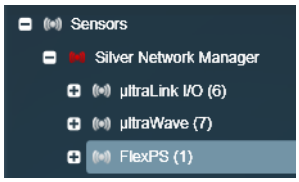
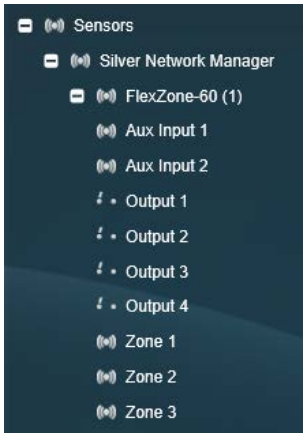
In the Sensor tree, the number beside the sensor name indicates the Silver Network node number, as configured in the Network Manager. Use this number to identity which entry corresponds to the actual sensor.

You can change the name of a sensor by editing the Name field in the Properties pane. The Original Name field is read-only and indicates the sensor name as it appears in the Network Manager.

Sensors appear in the System Control tree in alpha-numeric order.

Intrusion vs Equipment Alarms

When placing a sensor indicator on a map, you can select the sensor name, which indicates general equipment status, or an individual alarm output from that sensor:

Equipment control alarm		If you pick the entire sensor, the sensor indicator displays an alarm on the map as a result of an abnormal condition. This can include a diagnostic fault, network disconnect, or test event.
Sensor output		If you pick a specific output, the sensor indicator only displays an alarm on the map for that specific condition. This can include, for example, a specific perimeter zone or an auxiliary input.

Map Controls

When placing sensors on the map, use the following controls to move the map around and zoom in/out.

Function	Icon	Mouse Equivalent
Zoom in/out		Wheel up/down
Zoom to select	–	Shift + click and drag
Move		Click and drag
Rotate		–
Reset rotation		–
Display entire image		–

Sensor Properties

Each sensor has the following properties that affect its appearance on the maps.

Category	Parameter	Description
Appearance	Event Font Color	–
	Event Font Size	–
	Font Color	Sets the color of the sensor's label. Labels are black by default.
	Font Size	Sets the text size of the sensor's label. Labels are set to 12 pt by default.
Information	Description	Custom description of sensor or event. This text appears in the More Info tab of the sensor’s Properties window.
	Device Subtype	Displays the type of device: controller, control point, or sensor point
	Name	The text shown in the sensor's label. If you have multiple processors and each reports a similar sensor name (e.g. “zone 1”), change this to something more description, like “North side, P1-Zone 1)”.
General	Is Monitoring Sensor	Configures the sensor as a monitor. Monitor sensors do not generate alarms.
	Non Disable	Disables the ability for an operator to mask the sensor, even if they have permission. Note that this setting does not affect any sensor masking by the rules engine.
	Sensor Priority	Configures where sensor alarms appear in the list of events. Priority 10 makes the sensor appear at the top; priority 1 makes it appear at the bottom.
	Show Item on Tree	Configures how the sensor appears in the Sensor tree on each client workstation. From the sensor tree, the operator can view details about the sensor, and see or mask any current alarms: Note: If you want to use a sensor to trigger an event or display a procedure, the sensor must appear in the tree, otherwise you will not be able to select it for your rules. • ONLY IF HAS MAP LOCATION – Only appears in the sensor tree if it is included on a map. • ALWAYS – Always appears, even if it doesn't have a map location. • NEVER – Never appears, even if it is on a map. • NO_VALUE – Keep existing value.

Category	Parameter	Description
Linked Picture	Is Icon	Toggles the sensor type between discrete and line.
	Location on Picture	Click the target icon to link the sensor to the picture-map (by default, it will place a point icon).
	Picture Linked Item	The name of the picture-map to which the sensor is linked.
Polyline	Picture Polyline	Click the target icon to place a polyline on the picture-map.
	Polyline Width	Width of the polyline as it appears on the picture-map. Increasing the line width can help improve visibility.
Ranging	Ranging Start	Configures the start of sensor cable distance values so that intrusion locations are displayed as moving dot.
	Ranging End	Configures the end of sensor cable distance values so that intrusion locations are displayed as moving dot.
Read Only	Original Name	Sensor name as reported by the Network Manager

Placing a Polyline Sensor

Note Ensure that you are on the correct picture-map.

1. Select the picture-map on which the sensor will be displayed.
2. Expand **Sensors** > ***<Network_Manager_Name>***.
3. Double-click on either the sensor, or expand the sensor and double-click the zone.
   The Properties window for the selected sensor is displayed.
4. In the Linked Picture field check (enable) the Is Icon checkbox.
5. Left-click the Location on Picture button .
6. Left-click the location of the sensor on the picture-map.
   An icon appears indicating the location of the sensor label on the picture-map (displayed during an alarm condition).
7. Uncheck the Is Icon checkbox.
8. In the Polyline field, left-click the Polyline on Picture button .
9. Left-click the location of the first point of the polyline on the picture-map (the beginning of the area covered by the zone).
10. Continue left-clicking to add each subsequent point until the zone's coverage is complete. Double-click or right-click when you are done. (Clicking the scroll wheel will undo the previous point or segment.)
11. Edit the polyline as required by left-clicking the Polyline on Picture button and making the necessary changes:

- Edit a point by dragging it to a new location.
- Add a point by clicking the segment between two points.

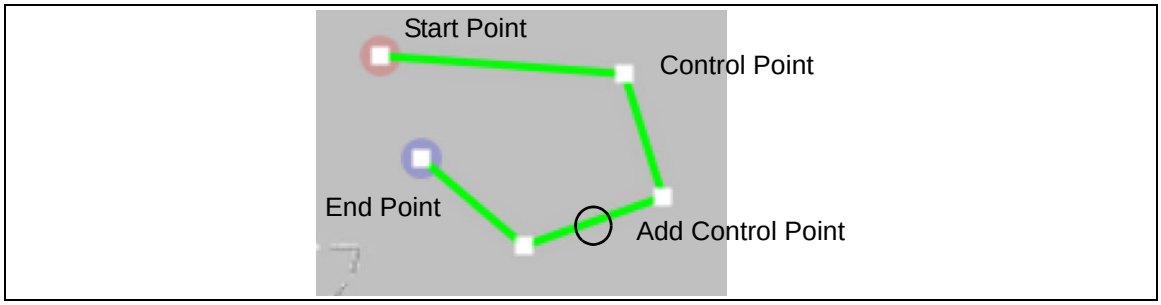


Figure 26: Creating a Polyline Sensor

12. In the Name property, enter the text that will be displayed on the operator map during an alarm.
13. Click **Save**.

The sensor is placed on the map. The next step is to configure its other properties. See Configuring and Editing Sensor Properties on page 49.

Placing a Discrete Sensor

Note	Ensure that you are on the correct picture-map.

1. Select the picture-map on which the sensor will be displayed.
2. Expand **Sensors** > **Silver Network**.
3. Double-click on either the sensor, or expand it and double-click the specific sensor point. The Properties window for the selected sensor is displayed.
4. In the Linked Picture field check (enable) the Is Icon checkbox.
5. Left-click the Location on Picture button .
6. Left-click the location of the sensor on the picture-map. An icon appears indicating the sensor's location.
7. In the Name property, enter the text that will be displayed on the operator map during an alarm.
8. Click **Save**. The sensor is placed on the map. The next step is to configure its other properties (see Configuring and Editing Sensor Properties on page 49).

Placing a Monitoring Sensor

Note	Ensure that you are on the correct picture-map.

1. Select the picture-map on which the sensor will be displayed.
2. Expand **Sensors** > **Silver Network**.
3. Double-click on either the sensor, or expand it and double-click the specific point. The Properties window for the selected sensor is displayed.
4. In the Linked Picture field check (enable) the Is Icon checkbox.
5. Left-click the Location on Picture button .

6. Left-click the location of the sensor on the picture-map.
   An icon appears indicating the sensor's location.
7. Check (enable) the **Is Monitoring Sensor** checkbox.
8. In the Name property, enter the text that will be displayed on the operator map during an alarm.
9. Click **Save**.
   The monitor sensor is placed on the map. You can configure its label in General Configuration Properties (see Monitor Labels on page 58).

Configuring and Editing Sensor Properties

You can configure and edit a sensor after you have placed it on a picture-map:

1. Expand **Sensors** > ***<Network Manager>***.
2. Double-click on either the sensor, or expand it and double-click the specific point.
   The Properties window for the selected sensor is displayed.
3. Configure the properties, as required:
   - polyline location
   - polyline width
   - label location, font, color, size
   - sensor name
   - ranging start and end
   - sensor priority
   - disable/non-disable
4. Click **Save**.

Deleting a Sensor

1. Select the sensor on the picture-map:
   - If the sensor is a polyline, click the delete icon in the Polyline.
   - If the sensor is an icon, click the delete icon in Linked Picture.
2. Click Save.
   The sensor is removed from the picture-map.

Hiding a Sensor

You can configure a sensor so that it is hidden from workstations during non-alarm (secure) conditions and only appears when it enters an alarm state.

Note	If you use this procedure, you must ensure that any new workstations added to the system are also configured to view sensors by group instead of all. If a workstation in the network is configured to view all sensors, alarms from the hidden sensors will only appear on the workstations configured to view all. Before following this procedure, ensure that you are familiar with StarNet 2's alarm routing feature (see Alarm Routing on page 62).

1. In the Setup application, configure the hidden sensors to always appear on the system tree.
2. In the Workstation application, create a group that contains all the sensors EXCEPT for the ones you want hidden:
   a. From the Workstation's **Tools** menu, select **Sensor Management**.
   b. Select the Groups tab.
   c. Create a new group by clicking **Add**.
   d. Enter a name and description for the new group.
   e. Select the new group.
   f. In the Sensors section, click **Add**.
   g. Select all the sensors you want VISIBLE in the group and click **OK**.
   h. In the Backup Handling Station box, select the stations that will see the sensors.
   i. Click **OK**.
3. From the Workstation's **Tools** menu, select **Sensor Management**.
4. Select the Stations tab.
5. Select the Station from the Stations list.
6. Select **View sensors by group**.
7. Click **OK**.
8. Configure any other workstations present in the system to also view sensors by the same group.

   At this point, any sensor not in the group will not be visible on the workstation when in a non-alarm (secure) state. However, as there are no workstations in the system configured to view the hidden sensors, alarms from those sensors will be routed to ALL workstations in the system.

5 User Management

Access to StarNet 2 and its functions is controlled through user accounts, groups, and permissions.

- Users require a user name and password in order to access the system.
- Each user account belongs to a specific user group
- Each user group has a set of permissions that provide access to specific functions.

Note	By default, the system is configured without any user accounts.

In this chapter

Authentication Method

By default, StarNet 2 authenticates users against its own local database. Depending on your site's security policies and requirements, you can configure StarNet 2 with the following authentication methods:

- NONE – Users are not authenticated
- LOCAL – Users are authenticated against local password information stored in the StarNet 2 database.

Note	If NONE is selected, the audit and event logs will only report the workstation that performed the action, not an individual user.

To configure user authentication:

1. Open the StarNet 2 Setup application.
2. Expand **Misc** > **General Configuration**.
3. Select **General Configuration**.
4. Click the User Login Type initialization icon.

5. Select NONE or LOCAL.
6. Click **OK**.
7. Click **Save**.

Group Permissions

StarNet 2 divides users into four possible groups:

- Administrators: By default, provides full access to the system. Intended for system administrators who configure the system.
- Operators: Limits access to functions required by those who monitor the system and respond to alarms and other events.
- Supervisors: Limits access to functions required by those who supervise or manage the operators.
- Viewer: Intended for the read-only display of system. By default, disables access to all configuration and alarm processing functions.

Permissions are managed by enabling or disabling functions for each group.

Figure 27: Users & Permissions Management Window

To manage user group permissions:

1. Open the StarNet 2 Workstation application.
2. From the **Tools** menu, select **Edit > Users & Permissions Management**.
   The Permissions window is displayed.
3. Expand **User Group**.
   A list of the available user groups is displayed.

4. Select the user group whose permissions you want to edit.
5. Enable or disable the group's permissions as required.
6. Save the changes by clicking **Update**.

Adding a User

CAUTION	When adding accounts, you MUST first add an administrator account. Failure to do so may lock you out of the system.

Add a user account:

1. From the Workstation's **Tools** menu, select **Edit > Users & Permissions Management**.
   The Permissions window is displayed.
2. Confirm that there is an existing administrator account. If there is not an existing administrator account, create one.
3. Click the **Add User** icon.
4. Enter the following information.

First Name	Given name of user
Last name	Surname of user
User Group	The user's role (Administrator, Operator, Supervisor, or Viewer)
Login	The username for the user (entered during the login process)
Password	User account password (entered during the login process)

5. Save the changes by clicking **Update**.

Deleting a User

1. From the Workstation's **Tools** menu, select **Edit > Users & Permissions Management**.
   A list of the available user groups and their associated permissions is displayed.
2. Expand **User Group**.
   A list of the available user groups is displayed.
3. Expand the user group containing the user account you want to remove.
4. Select the user account.
5. Click the **Delete** icon.

6 Workflows

This chapter explains how to modify the settings in StarNet 2 to better fit the needs and workflows of your site.

Automatic Picture-Map Switching

The StarNet 2 application can automatically display the relevant picture-map whenever a sensor located on it reports an alarm or event.

To configure automatic picture-map switching:

1. In Workstation application, click **Event Automatic Mode**  . Automatic picture-map switching is now enabled.
2. To cancel automatic picture-map switching, repeat step 1.

Alarm Properties

The General Configuration properties control how alarms appear and sound at operator workstations.

Property	Description
Alarm Sound	Configures the sound used to indicate an alarm event. To change alarm sound, click the Find File icon and select the new audio file (.wav).
Bypass Sensor Terminology	The term used by your organization when temporarily overriding an event. The default terms are Disable, Mask, Access, or Bypass.
Require Closing Reason	When enabled, this property forces the operator to enter a reason when resetting (closing) an event. The resetting reasons are configurable. See Alarm Resetting Reasons on page 57.
System Failure Sound	Configures the sound used to indicate a system failure event. System failures are conditions that effect the operation of the StarNet 2 application, such as network connectivity. To change alarm sound, click the Find File icon and select the new audio file (.wav).
Alarm Sound Repeat Interval	The number of seconds after which an event will be repeated if there is still an open event. Click the arrows to change the number of seconds. A zero (0) value means no repeat.
System Failure Sound Repeat Interval	The number of seconds after which the siren sounds again to indicate there is a problem with a critical system. Click the arrows to change the number of seconds. A zero (0) value means no repeat.
Enable map zoom	Enables operators to pan and zoom the currently selected map.

Configure general properties:

1. Open the StarNet 2 Setup application.
2. Expand **Misc** > **General Configuration**.
3. Select **General Configuration**.
4. Configure the properties as required.
5. Click **Save**.

Alarm Silencer

The alarm silencer button gives the operator the ability to silence the alarm sound once an event is received without acknowledging the alarm.

Figure 28 Alarm silencer button

Auto-delete

The Auto-delete functionality will reset an event automatically, if it returns to the secure state. Auto-delete can be enabled separately for normal events (typically zone alarms) and for technician/diagnostic events. For each option there is a separate permission that can be set in the Users & Permissions Management properties. To enable this feature:

1. In the Workstation application, click on Tools > Edit and select the Auto-delete function.

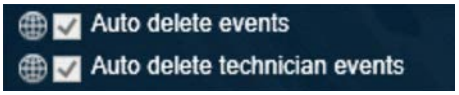


Figure 29 Setting up Auto-delete

Alarm Resetting Reasons

By default, when an operator acknowledges and resets an alarm event, the operator must provide a reason. You can customize the list of available reasons to be specific for your site.

Note	You can disable the requirement for operator's to provide a closing reason (see Alarm Properties on page 55).

Configure alarm resetting reasons:

1. Open the StarNet 2 Setup application.
2. Expand **Misc**.
3. Expand **Event Resetting Reason**.
4. Configure the reason:
   - To edit an existing reason, double-click the reason.
   - To create a new reason, select **Event Resetting Reason** and click **New**. The Property window is displayed.
5. Enter the reason in the Name property.
6. Click **Save**.
   The resetting reason is updated.

Exit Password

To prevent accidental or unauthorized closing of the StarNet 2 operator application, you can configure an exit password that is required whenever the Exit button is clicked. The exit password is shared for all users of the system and is not linked to a specific account.

Note	While the exit password reduces the risk of accidentally closing the operator screen, the application can still be terminated by authorized users, like other Windows applications, via the Taskbar or Task Manager. See Windows Security on page 106 for information on preventing application exits.

To configure an exit password:

1. Open the StarNet 2 Setup application.
2. Select **Misc** > **General Configuration** (see Figure 30:).
3. Enter the text for the Exit Password parameter.
4. Click **Save**.

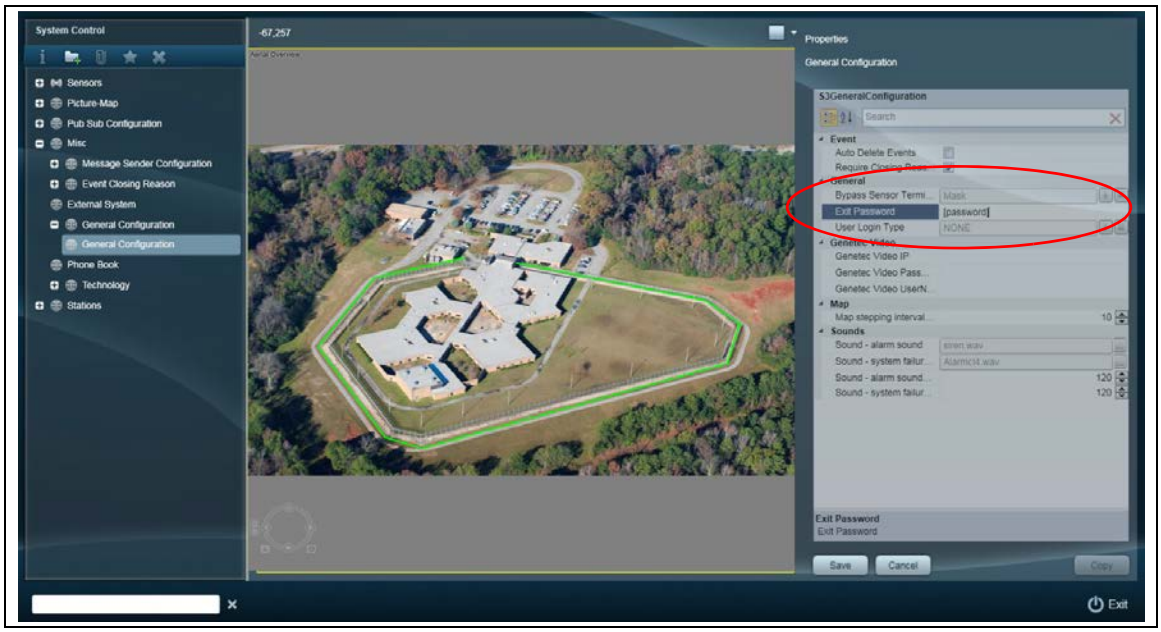


Figure 30: Configure the Exit Password

Monitor Labels

You can configure the text that appears beside monitoring labels.

Note	All monitoring sensors use the same labels. If you require different labels per monitor icon, add them to the background of the picture-map.

To configure monitor labels:

1. Open the StarNet 2 Setup application.
2. Select **Misc** > **General Configuration**.
3. Enter the text to display when the monitored inputs are asserted or de-asserted.
4. Click **Save**.

Operator Procedures

StarNet 2 can display operator procedures on-screen whenever a specific sensor and/or calendar event occurs. For example, if a disturbance is detected in a zone along the perimeter, the operator can be instructed to record the incident and dispatch security personnel. Procedures can also be invoked according to a schedule (e.g. to instruct security personnel to perform a perimeter inspection).

A procedure can also incorporate the triggering of rules. A rule can be triggered by any or all of the following conditions:

- when the procedure is invoked
- when an alarm is not acknowledged in a specified period (see Alarm Escalation on page 61)
- when an alarm is not reset in a specified period (see Alarm Escalation on page 61)

After the procedure tasks are displayed, the operator clicks the **Done** button beside each step, thus providing a record that the task was acknowledged.

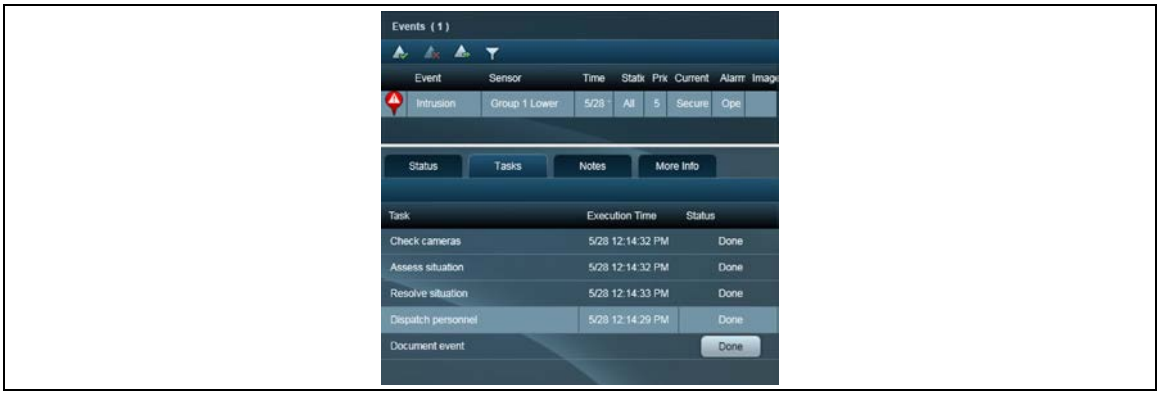


Figure 31: Configure the Operator Events

To add a procedure:

1. Open the StarNet 2 Workstation application.
2. Select **Tools > Edit > Procedure Editor**.
3. Create a new procedures category or select an existing one.

4. Click **Add Procedure**.

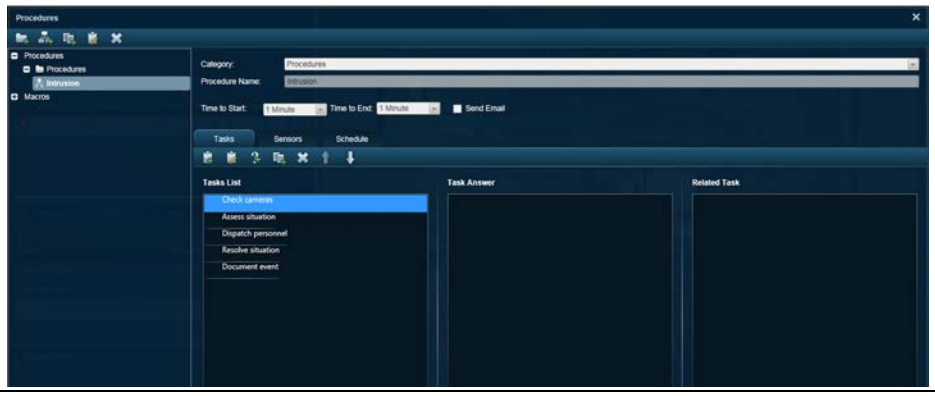


Figure 32: Procedure Editor Screen

5. Add tasks to display on the screen:
   a. Click **Tasks**.
   b. Click **Add Task** and enter the text.
   c. Configure the procedure's options:
      - **Send Email –** Enable if you want an email generated whenever this procedure occurs (see E-Mail Generation on page 74 for information about configuring emails).
   d. Click **Add** to save the text.
   e. Repeat this procedure for additional tasks.
   f. Click the Up and Down arrows to adjust the list order, if required.
6. Select any sensors that will trigger this procedure:
   a. Click **Sensors**.
   b. Select the sensors and their status states that will invoke the procedure.
7. Configure any schedule-based triggers to invoke the procedure:
   a. Click **Schedule**.
   b. Click **Add**.
   c. Select the Station on which the procedure will appear, its schedule, and add a note describing it for reference.
   d. Click **OK**.
8. Once you have completed adding the tasks, sensors, and/or schedule, click **Close**.

Defining Macros

Macros are generic procedures that you can re-use to help speed up the creation of many procedures. To define a macro:

1. Open the StarNet 2 Workstation application.
2. Select **Tools > Edit > Procedure Editor**.
3. Click **Add Macro**.
4. Enter a name for the macro.
5. Select the new macro from the list.
6. Click **Edit**.

7. Add tasks as required. See page 59 for information on adding tasks.
8. Click **Update** to save your changes.

To use a macro in a procedure:

1. Edit the procedure as required.
2. Open the StarNet 2 Workstation application.
3. Select **Tools > Edit > Procedure Editor**.
4. Create a new procedures category or select an existing one.
5. Click **Add Macro** to add the macro steps.
6. Select the macro from the list.
7. Click **Add**.

The tasks from the macro appear in the procedure's Tasks List.

Defining Conditional Tasks

Conditional tasks are like regular procedures, only that instead of the operator clicking Done after performing each task, they select the outcome from a list.

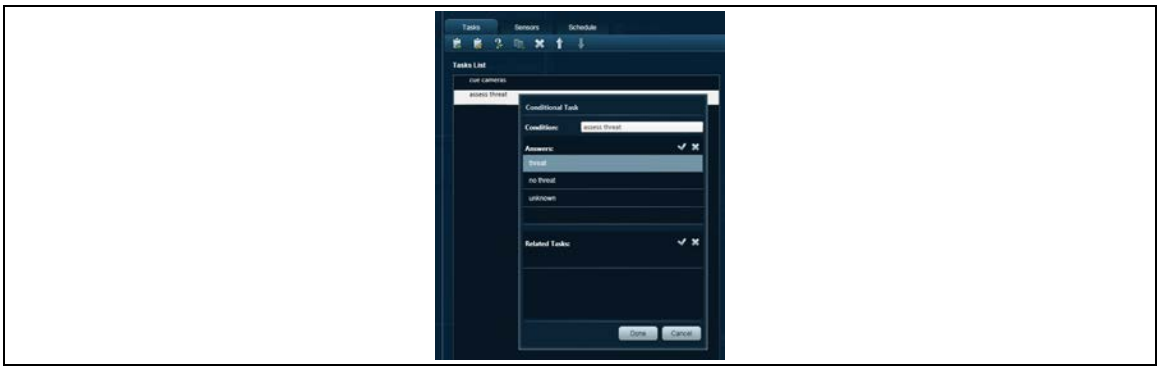


Figure 33: Conditional Tasks Screen

1. Create procedure with tasks, as described in Operator Procedures on page 59.
2. Select the task and click the Conditional task button  .
3. Enter the possible outcomes and click **Done**.

Alarm Escalation

It is possible to configure StarNet 2 to escalate an alarm that has not been acknowledged within a specified period and/or has not been reset within a specified period after being acknowledged.

Alarm escalation for unacknowledged alarms is activated by selecting a time from the **Time to acknowledge** drop-down menu. Leaving the default setting of None disables unacknowledged alarm escalation. When alarm escalation for unacknowledged alarms is activated the following occurs if an alarm has not been acknowledged by the selected time:

- If the alarm sound is set to non-repeat, the alarm sound or equipment failure sound is played. This will repeat at an interval equal to the alarm escalation time setting (e.g. if the Time to acknowledge is set to 30 seconds, the alarm sound will play every 30 seconds).
- A symbol is added to the event information line in the Events table indicating that an escalation has occurred.
- If the **First Escalation Time** column heading is added to the event information line the time of the first escalation will be shown.
- If a rule is selected in the **Select Rule** selector box the selected rule is activated.
- If the **Forward to all Stations** box is checked the alarm is forwarded to all stations, any one of which can acknowledge the alarm.

Alarm Routing

You can configure which sensors appear on each monitoring station as well as which workstations are responsible for handling a set of sensors. First, you create a group that contains a specific set of sensors. Next, you assign that group to a specific monitoring station.

To configure a workstation to handle a group of sensors:

1. From the Workstation's **Tools** menu, select **Edit > Sensor Management**.
2. Select the Groups tab.
3. Create a new group by clicking **Add**.
4. Enter a name and description for the new group.
5. Select the new group.
6. In the Sensors section, click **Add**.
7. Select the sensors you want in the group and click **OK**.
8. In the Backup Handling Station box, select the stations that will receive (and subsequently process) the alarms from the dropdown list.
9. If you want other stations to also receive the alarms, select them from the dropbox list in the Watching Stations box.
10. Click **OK**.
    The sensor group is now defined.

To configure which sensors are displayed on a specific station:

In some situations, you may want to limit a workstation to only display a group of sensors. This differs from handling sensors, in that this feature is only about making the sensors visible on the workstation. Sensors will still appear on the map when they enter an alarm state.

1. From the Workstation's **Tools** menu, select **Edit > Sensor Management**.
2. Select the Stations tab.
3. Select the Station from the Stations list.
4. Select which sensors to display on that station:
   - View all sensors – Display all the sensor events on that station.
   - View sensors by group – Display only those sensors displayed in the following group lists.
5. Click **OK**.
   Your changes are saved.

7 Rules Engine

This chapter explains how to create rules that perform specific actions when certain conditions occur.

Overview

StarNet 2 can perform actions whenever a sensor event or specific time occurs. These actions are managed via user-configurable rules.

A rule consists of a set of triggers and actions. When one of the triggers occurs (a sensor event or a scheduled time) a set of actions is performed. Actions can include sending a command to a sensor or sending a custom ASCII text string to another system.

When creating or using rules, it is important to understand some key concepts:

- Sensor triggers occur when a sensor changes from one state to another. Therefore, if a rule sets a sensor to a particular state (e.g. mask) but the sensor is already in that state, then no other rules that have a trigger based on that particular state will be invoked because the sensor did not change states.
- Subsequent invocations of a rule cancel any still-running previous invocations unless the “Run Simultaneously” checkbox is selected. Rules can also be canceled manually by the Operator via the system control tree.
- The Rules Engine includes a Run Simultaneously checkbox that allows more than one instance of a rule to run at the same time.
  This function is used primarily for rules which trigger ASCII commands or send emails.
- If the Run Simultaneously checkbox is not selected, only one instance of the rule can run at any given time. If a rule is invoked again (before it has a chance to finish), the first instance will be stopped (wherever it is in its set of actions) and the new instance will run.

Note	Previously, in versions up to and including V.106, rules always ran to completion and you could have multiple instances of each rule running at the same time. For example, if a relay switch was used to trigger a rule, then toggling the switch multiple times would result in multiple instances of the rule being run.

Manually Invoke/Cancel Rules

A rule can be manually invoked and/or canceled from the StarNet 2 Workstation application if the rule is configured for manual activation. To manually invoke a rule, the operator expands the System Control tree, right-clicks the rule and selects Activate Rule. Alternatively, if the Rule is on a map, the Operator can select and run the Rule from the map. The flag icon will turn green. To stop the rule, right-click on the rule and select Cancel.

Configuring Rules

Rules are configured in the Rules Engine window.

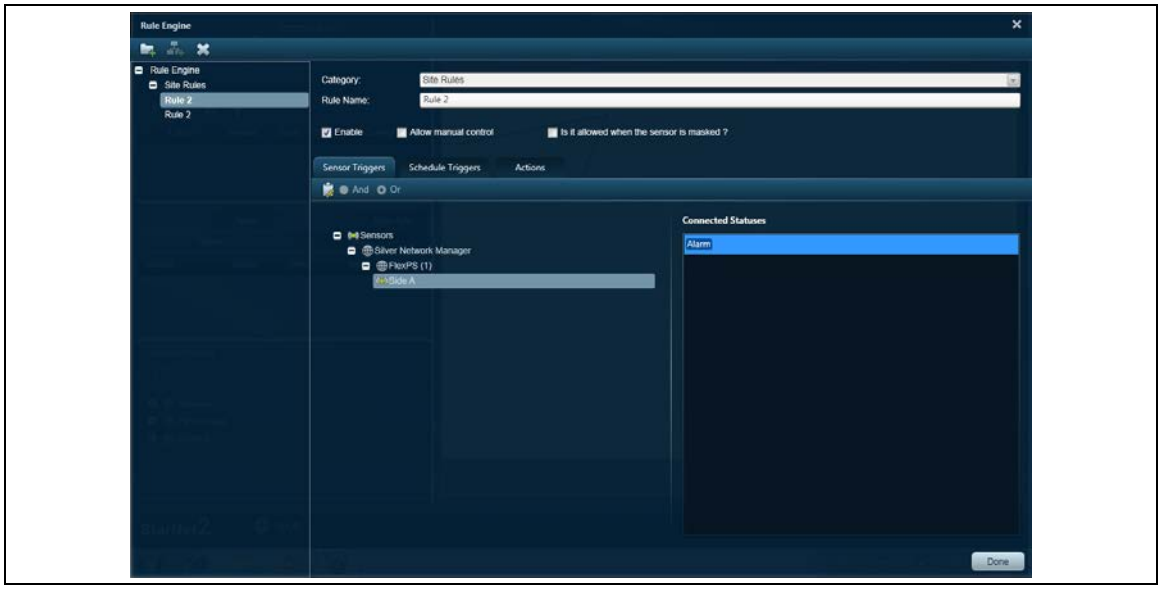


Figure 34: Rules Engine Window

Defining Rules

To define a rule, perform the following steps:

1. Select a rule category or create a new rule category (see Categories on page 65).
2. Create a new rule or edit an existing rule (see Rules on page 66).
3. Configure sensor triggers (see Sensor Triggers on page 66) and/or schedule triggers (see Schedule Triggers on page 68).
   It is possible to have multiple triggers for one rule.
4. Configure actions to perform whenever the trigger(s) occur (see Actions on page 70).

Categories

Rules are organized into categories (left pane), which are similar to folders. There must be at least one rule category.

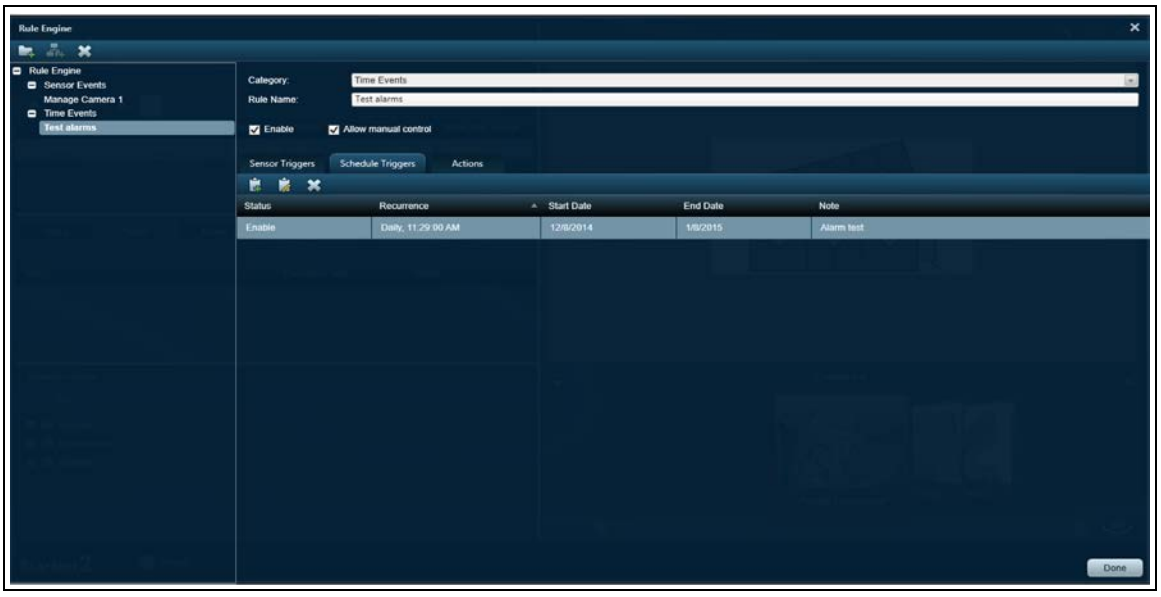


Figure 35: Adding the Rule Category

To add a category:

1. Open the StarNet 2 Workstation application.
2. Select **Tools > Edit > Rule Engine Editor**.
3. Click **New Category**.
4. Enter a name.
5. Click **Add**.

To rename a category:

1. Open the StarNet 2 Workstation application.
2. Select **Tools > Edit > Rule Engine Editor**.
3. Select the category.
4. Enter a new name.
5. Click **Add**.

To delete a category:

1. Open the StarNet 2 Workstation application.
2. Select **Tools > Edit > Rule Engine Editor**.
3. Select the category.
4. Click **Delete**.
5. Confirm the deletion by clicking **Yes**.

Rules

After creating a category, you create a rule that contains triggers and actions.

Add a rule:

1. Open the StarNet 2 Workstation application.
2. Select **Tools > Edit > Rule Engine Editor**.
3. Select the category.
4. Click **Add rule**.

Figure 36: Adding a Rule

5. Select the category.
6. Enter the Rule Name.
7. To make the rule active, ensure **Enable** is checked.
8. To make it possible for an operator to manually invoke the rule, select **Allow manual control**.
9. If you want the rule to activate when the sensors that trigger the rule are masked, select **Is it allowed when the sensor is masked?**
10. Click **Add**.

The placeholder for the rule is added. To configure the rule's specific functions:

- Sensor Triggers on page 66
- Schedule Triggers on page 68
- Operator triggers on page 69
- Actions on page 70

Sensor Triggers

Sensor triggers consist of one or more sensor control points that activate a rule when the control points status changes to a specified state (e.g. alarm, supervision, disconnected, etc). The trigger is activated when any (OR) or all (AND) of the sensor triggers statuses become true. When a rule is placed on a map, the operator can select and run the rule by right-clicking the rule on the map and selecting Activate Rule.

Note	Sensor control points must be added to a map before the control points can be used to trigger rules.

Note	Only manually triggered rules can be allocated on a map.

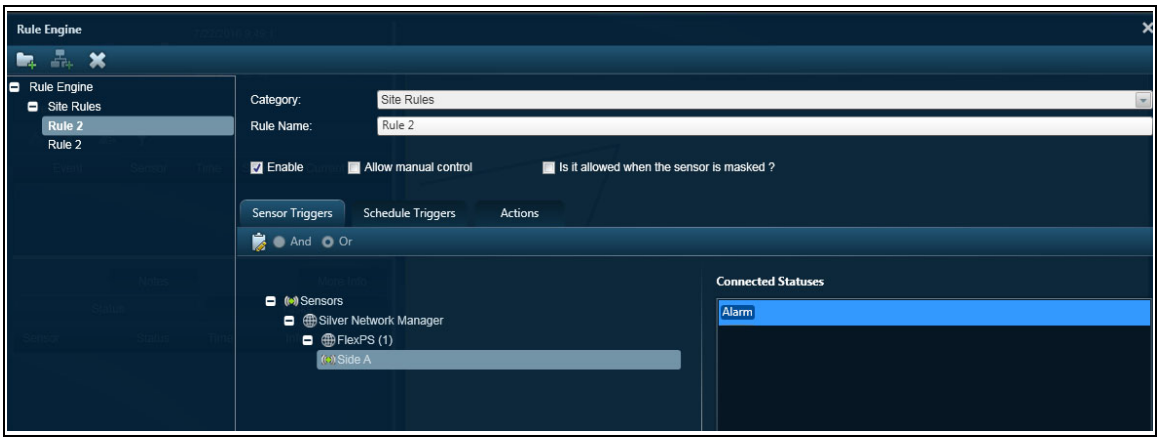


Figure 37: Sensor Triggers

To define or edit a sensor trigger:

1. Create a new rule, or display an existing rule.
2. Select **Sensor Triggers**.
3. Click **Edit Rule**.
   A list of selectable control points is displayed:

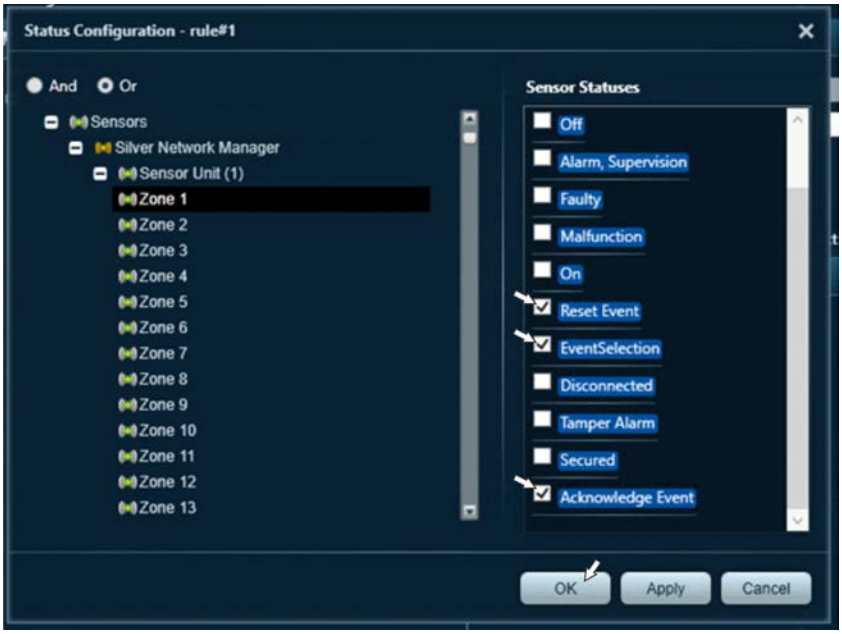


Figure 38: Selectable Control Points

4. Select the sensor control point(s) for the trigger.
5. Select the operator (AND or OR) that determines how multiple sensor control points are to be handled.
6. Enable or disable the sensor status states that activate the trigger.
7. Click **OK** when done, or click **Apply** to add additional control points.
   The triggers are now displayed in the sensor list. Select a sensor control point to see the configured trigger status states.

Schedule Triggers

Schedule triggers occur according to a schedule: daily, weekly, monthly, yearly, or once. You can also define optional start and end dates during which the schedule trigger occurs. Schedule triggers can be used for a variety of purposes, such as:

- Activation of sensors at specific times (i.e. sensors that are disabled during working hours)
- Notifications to perform periodic maintenance
- Notifications to perform security checks
- Drills and system tests

Note	Often, when using schedule triggers, you must define two rules: one rule to activate a sensor at a specific time and another rule to mask the sensor at a later time (or vice versa).

Figure 39: Schedule Triggers

To define or edit a schedule trigger:

1. Create a new rule, or display an existing rule.
2. Select **Schedule Triggers**.
3. Click **Add** to add a new schedule trigger, or select an existing schedule trigger and click **Edit**.

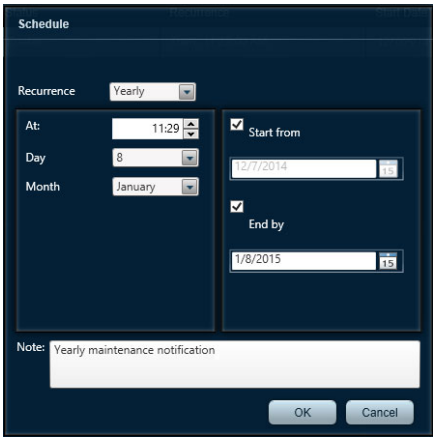


Figure 40: Editing Schedule Triggers

4. Select the **Recurrence** period: Daily, Weekly, Monthly, Yearly, or Once.
5. Enter the time at which the trigger occurs.
6. If applicable, select the Day and/or Month at which the trigger occurs.
7. Set the start and end dates, if the trigger has a fixed time period.
8. Enter a note describing the trigger.
9. Click **OK**.

10. Repeat this procedure to add any additional schedule triggers that will activate this rule.
    The schedule triggers for the rule are displayed.

Figure 41: Adding Schedule Triggers

11. Click **Done**.

To delete a schedule trigger:

1. Select the trigger from the list.
2. Click **Delete**.
   The schedule trigger is deleted.

Operator triggers

Rules Engine (Operator Action Triggering)

The Rules engine can also be triggered by operator actions associated with a sensor point, to do so, configure a rule and on the trigger tab use the following (see Figure 38:):

- Acknowledge event
- Reset event
- EventSelection (double-click an Event in the Event queue)

Rule Allocation on a Picture Map

Once a rule is defined, the user can log in to StarNet setup and allocate the rule on a map.

1. Click on S3RuleLocationData.

Figure 42 Opening the Station Connection Settings dialog

2. Click on the desired rule, and then click on the picture map to set the rule's location.

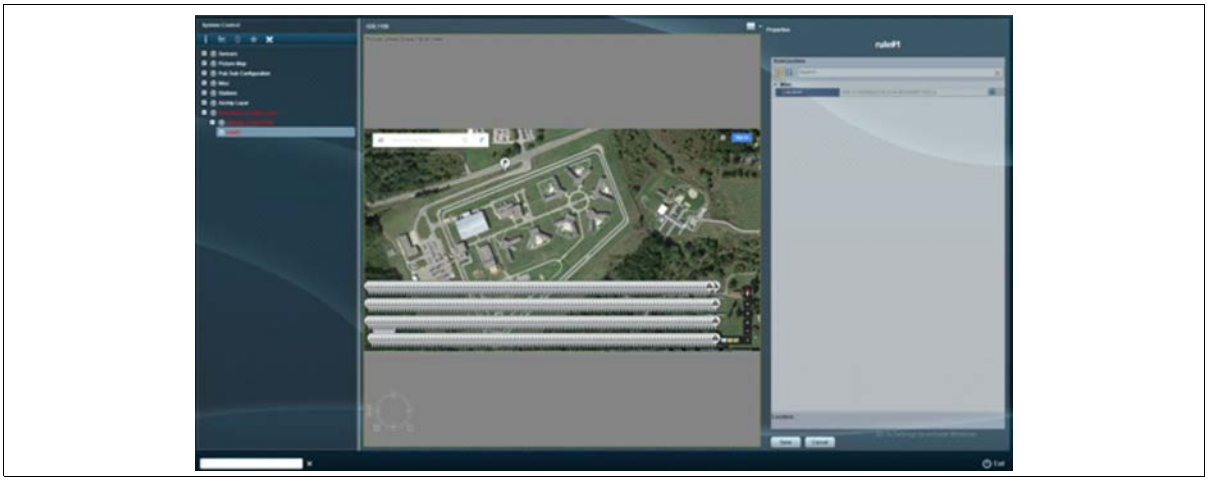


Figure 43 Allocating a rule on a picture map

3. Click Save.

Actions

Actions are the commands that will be performed when the trigger(s) occurs. There are three types of actions: sensor commands, ASCII text commands, and delays. When configuring actions, the following general parameters can also be set:

- Enable or disable the rule
- Allow the operator to manually run the rule
- Allow the rule to run when the trigger sensors are masked

- Allow multiple instances of the rule to run at the same time

Figure 44: Setting Actions

Send Command to Sensor

Actions can be used to send a command to any sensor control point in the system (if the control point appears on a picture-map). Depending on the control point, different options will be available:

- If the control point is an output managed by the Network Manager, you can turn it ON or OFF.
- If the control point is an input or sensor, you can enable it or mask it.

Note	Monitor sensor points do not respond to commands.

To send a command to a sensor:

1. Display the rule.
2. Click the Actions tab.
3. Click the Send Command icon  .
4. Select the sensor's control point.
5. Select the command to issue to the selected control point.
6. Click **OK**.
7. Repeat this procedure for any additional sensor control points managed by this rule.
8. Click **Done**.

Figure 45: Sending Commands to Sensors

Send ASCII command

You can send a custom ASCII text string to external systems. For information on configuring the external system to receive the commands, see ASCII Text Output on page 76.

To send an ASCII command, click the Send ASCII Command icon  . Enter the text string, and the name of the external system, then click **OK**.

ASCII commands can be sent using ASCII code special notes by adding the back-slash character \ to the ASCII code e.g. \000 equals NUL

Delay

The Delay command  inserts a pause (in seconds) in the list of commands. A delay can be used to delay a command from executing in order for something else to occur (e.g. an operator action).

8 System Integration

The StarNet 2 SMS can be integrated into an environment with other security management systems, including video management systems. The following integration options are explained:

Line Printers

StarNet 2 can be configured to send every event to a line printer. A line printer provides a physical record of each event and can be installed in a remote, secure location. StarNet 2 uses the default printer configured on the workstation.

Note	The line printer function requires a printer that is capable of single line printing, such as a dot matrix printer fed with continuous form paper.

To configure a line printer for a specific workstation:

1. In the workstation's Windows operating system, configure the line printer as the default printer.
2. From the Workstation **Tools** menu, select **Station Connection Settings**.
   The Station Connection Settings dialog box is displayed.

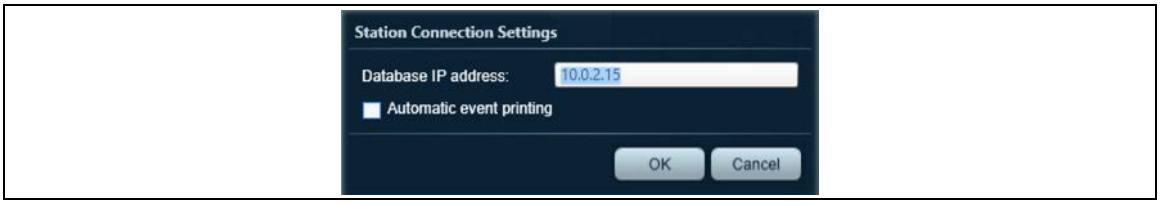


Figure 46: Conditional Tasks Screen

3. Enable the **Automatic event printing** check box.
4. Click **OK**.
   The changes are saved, and will become active after the server is restarted.

Video Systems

StarNet 2 supports integration with Aimetis and Airship video management systems. When a sensor generates an alarm or event, StarNet 2 can instruct a camera to perform a specific action and display the video in a window (see Sensor Properties on page 46).

Note	StarNet 2 can also send ASCII text string commands to third-party video management systems. See ASCII Text Output on page 76.

Note	See StarNet 2 application note #1 Airship VMS integration (S2DA0109) or #2 Aimetis Symphony VMS integration (S2DA0209) for installation, setup and configuration information.

Configure video server:

1. Expand **Misc** > **General Configuration**.
2. Double-click **General Configuration**.
3. Configure the video server parameters.
4. Click **Save**.

Property	Description
Video IP	The IP address of the video server
Video Password	The password used by the video server account
Video UserName	The username used to access the video server

E-Mail Generation

StarNet 2 can generate an email message whenever an alarm or event occurs. To send emails, StarNet 2 requires access to a Simple Mail Transport Protocol (SMTP) server.

Property	Description
Email Password	The password of the SMTP account used by StarNet 2 to generate emails; note that this is not the email recipient's account
Email Sender Name	The name used in the From fields of the generated emails (e.g. StarNet2)
Email Server Port	The port used by the SMTP server (typically 110)
Email Service On	Enable or disable email generation
Email SMTP Client	The IP address or domain name of the SMTP server (e.g. smtp.example.com)
Email User	The user name of the SMTP account used by StarNet 2 to generate the emails (often an email address) note that this is not the recipient's account

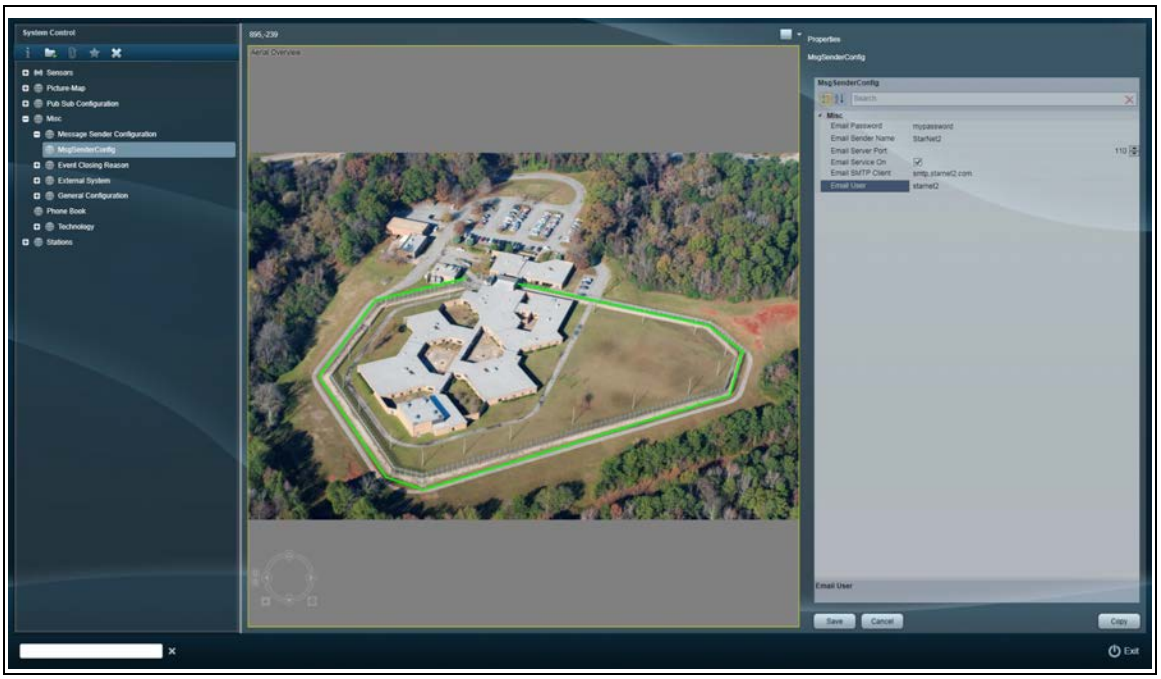


Figure 47: Email Server (SMTP) Parameters

To configure e-mail:

1. In the Setup application, expand **Misc > Message Sender Configuration**.
2. Select **MsgSenderConfig**.
   The Properties pane is displayed.
3. Enter the parameters for the StarNet 2 SMTP account.
4. Click **Save**.
5. Under Misc, select **Phone Book**.

Figure 48: Email Configuration

6. Click **New**.
7. Enter the parameters for the email recipient: email address, first name, last name, and telephone number.
8. Click **Save**.
9. Enter other email recipients as required (StarNet 2 will send emails to all of the addresses).
10. Restart the StarNet 2 services (see Step 2: Start StarNet 2 Services on page 21) to make the email changes active.
11. At this point, you can configure operator procedures to automatically generate emails when the procedures are run (see Operator Procedures on page 59).

ASCII Text Output

StarNet 2 can generate ASCII text strings to communicate with external systems. StarNet 2 can send text strings via serial, TCP, or UDP connections to any system that is capable of receiving them (e.g. a video management system). After adding external systems in the StarNet 2 Setup, you can select the external systems when defining rules in the Rules engine.

Note	You can configure more than one external system to receive text messages.

Property	Description
Name	Name of the external system.
Communication Type	TCP, UDP, or serial
IP	IP address of the external system if TCP or UDP is used.
Create Connection On Every Message	Enable this property if the external server cannot maintain an active system while StarNet 2 is running; if the external device can maintain a session (for example, if it can act as a telnet-style server), leave this property blank
Port	Port number of the external system if TCP or UDP is used.

To configure an external system

1. In the StarNet 2 Setup application, select **Pub Sub Configuration > System Component > External System**
2. Enter a unique PubSub Port value.
3. Click **Save**.
4. In the StarNet 2 Setup application, select **Misc > External Systems**.
5. Click **New**.
6. Enter the external system parameters, as required.
7. Click **Save**.
   Now that the external system is configured, you can define rules that generate ASCII text based on events. See Send ASCII command on page 72.

9 Audits and Reports

StarNet 2 keeps detailed records on the following activities:

- Events (alarm occurrences)
- Sensors (status of sensors over time)
- Audits (operator activities)
- System reports (StarNet 2 and network status)

You can export the results to PDF or to an Excel-compatible .CSV file.

Note	StarNet 2 includes PDF software for viewing the report files. To view a CSV-formatted report, you can either open the file in a text editor, install a CSV viewer on the StarNet 2 computer, or open the files on a separate computer with Excel or other CSV-compatible software. Consult with your Senstar technical representative for information.

Events Report

StarNet 2 can generate reports that describe when specific events occur (e.g. alarm, equipment fault, or user event).

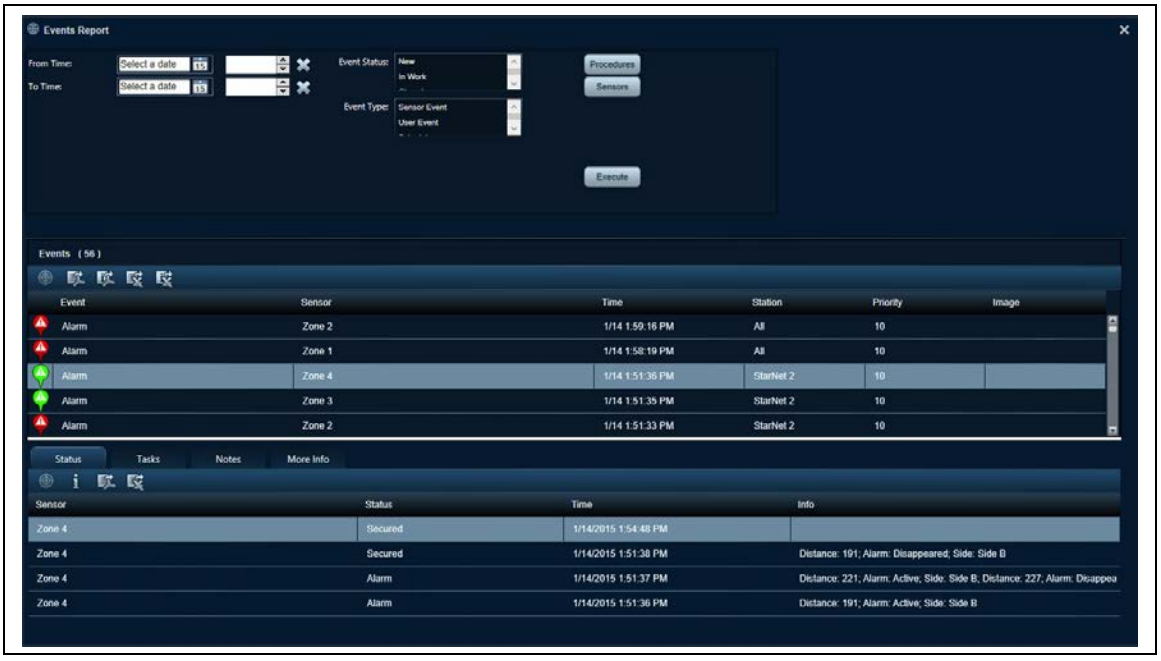
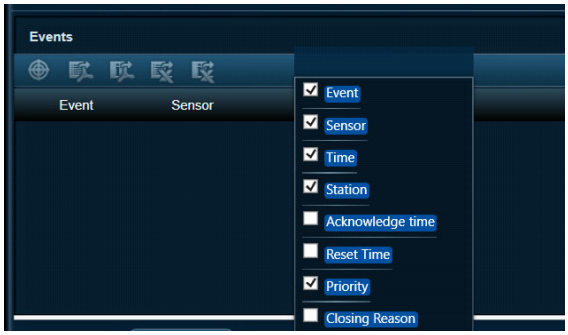


Figure 49: Events Report Window

To generate an event report:

1. Open the StarNet 2 Workstation application.
2. Select **Tools > Event Report**.
3. Select the From and To dates and times. To select the entire range, click **X** beside the field.
4. Select criteria:
   a. Select the Event Status criteria (hold down Control to select multiple items). Leave it blank to select all.
   b. If required, select the Event Type folders (hold down Control to select multiple items). Leave it blank to select all.
5. Select filters:
   a. Click **Procedures** to filter the results by which operator procedures were invoked.
   b. Click **Sensors** to filter the results by specific sensors.
6. Right-click on the column headings and select which fields you want in your report.
7. Pick **Execute**.
   A list of all events is displayed.
8. To review more information about a specific event, select it and additional information is displayed below.
9. To export the results, click the PDF or CSV export buttons on the toolbar.
10. Click the **X** to close the window and return to the Operator application.



Sensors Report

StarNet 2 can generate reports on the state of each sensor over a time period.

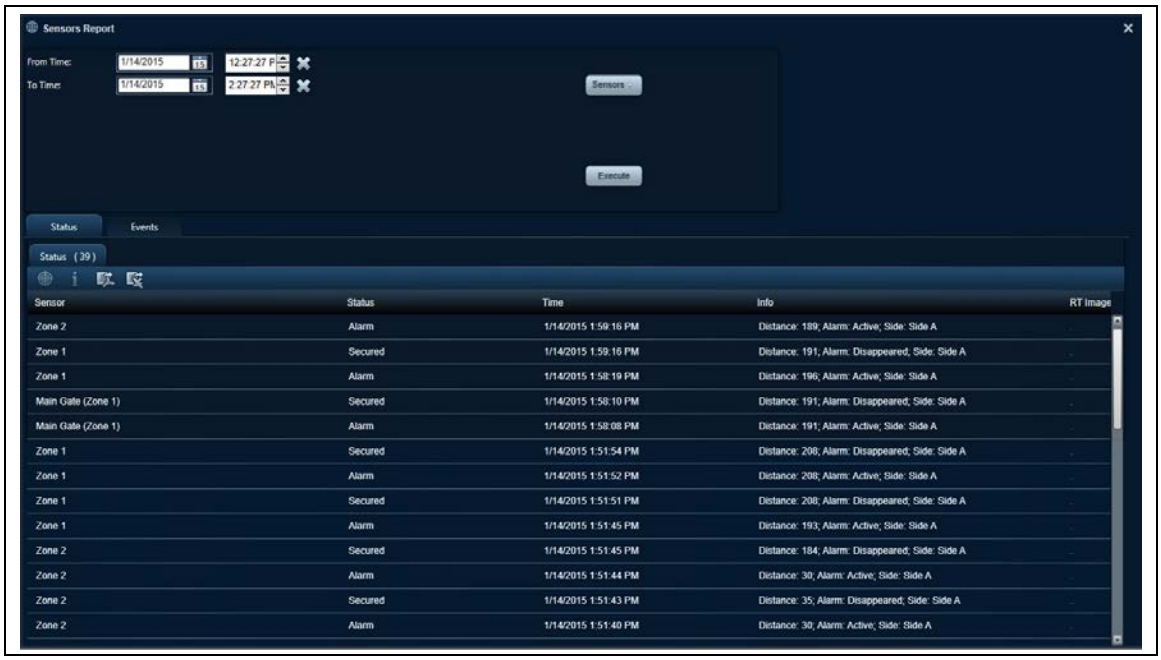


Figure 50: Events Report Window

To generate a sensor report:

1. Open the StarNet 2 Workstation application.
2. Select **Tools > Sensors Report**.
3. Select the From and To dates and times. To select the entire range, click **X** beside the field.
4. Select filters:
   a. Click **Sensors** to filter the results by specific sensors.
5. Pick **Execute**.
   A list of all events is displayed.
6. To review more information about a specific event, select the event and click information.
7. To export the results, click the PDF or CSV export buttons on the toolbar.
8. Click the **X** to close window and return to the Operator application.

Audit Reports

StarNet 2 can generate reports that describe the actions performed by operators when responding to events.

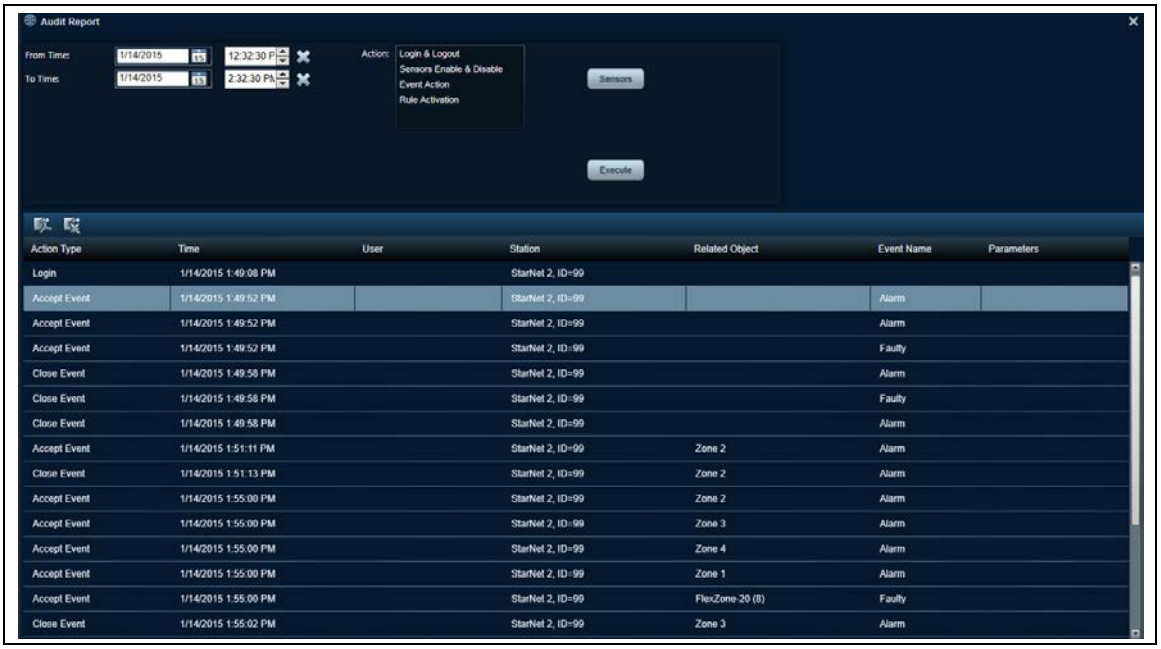


Figure 51: Audit Reports Window

To generate an audit report:

1. Open the StarNet 2 Workstation application.
2. Select **Tools > Audit Report**.
3. Select the From and To dates and times. To select the entire range, click **X** beside the field.
4. Select criteria:
   a. Select the Action criteria (hold down Control to select multiple items). Leave it blank to select all.

5. Select filters:
   a. Click **Sensors** to filter the results by which sensors were affected.
6. Pick **Execute**.
   A list of all operator activities is displayed.
7. To export the results, click the PDF or CSV export buttons on the toolbar.
   Click the **X** to close the window and return to the Operator application.

System Report

StarNet 2 can generate reports that provide a log of the network connection status between the Network Managers, individual workstations, and StarNet 2 server.

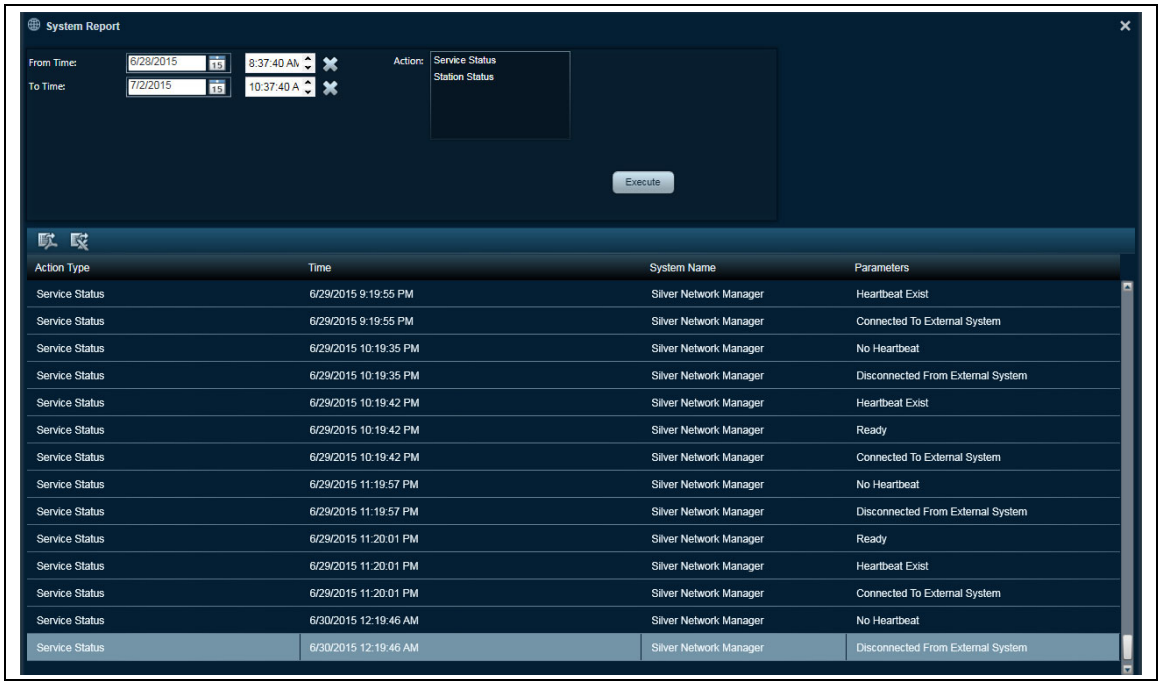


Figure 52: System Reports Window

To generate a system report:

1. Open the StarNet 2 Workstation application.
2. Select **Tools > System Report**.
3. Select the From and To dates and times. To select the entire range, click **X** beside the field.
4. Select criteria:
   a. Select the Action criteria (hold down Control to select multiple items). Leave it blank to select all.
5. Pick **Execute**.
   A list of all operational activities is displayed.
6. To export the results, click the PDF or CSV export buttons on the toolbar.
7. Click the **X** to close the window and return to the Operator application.

10 Database Management

Senstar recommends that you make periodic backups of the StarNet 2 databases. Database backups are handled via Microsoft's SQL Server Management Studio, an application installed as part of SQL Server. The backup files can be used to restore a StarNet 2 system to a previous state, or to copy a StarNet 2 configuration from one computer to another.

This chapter covers:

Backing Up Database & Site Configuration

1. Exit or switch out of the StarNet 2 Operator or Setup application, if currently active. You do not need to stop the StarNet 2 services.
2. From the Windows desktop, select **Start** > **All Programs** > **Microsoft SQL Server 2008 R2** > **SQL Server Management Studio**.
3. Select SQL Server Authentication.
4. In Login, type **sa** and enter the Password.
5. Click **Connect**.
6. Expand the Databases node and select the database to backup:
   - KeyStone – Contains all events.
   - SensorsServerConfiguration – Contains sensor and picture-map configuration information.
7. Right-click on the database and select **Tasks** > **Back Up**.
   The Back Up Database window is displayed.

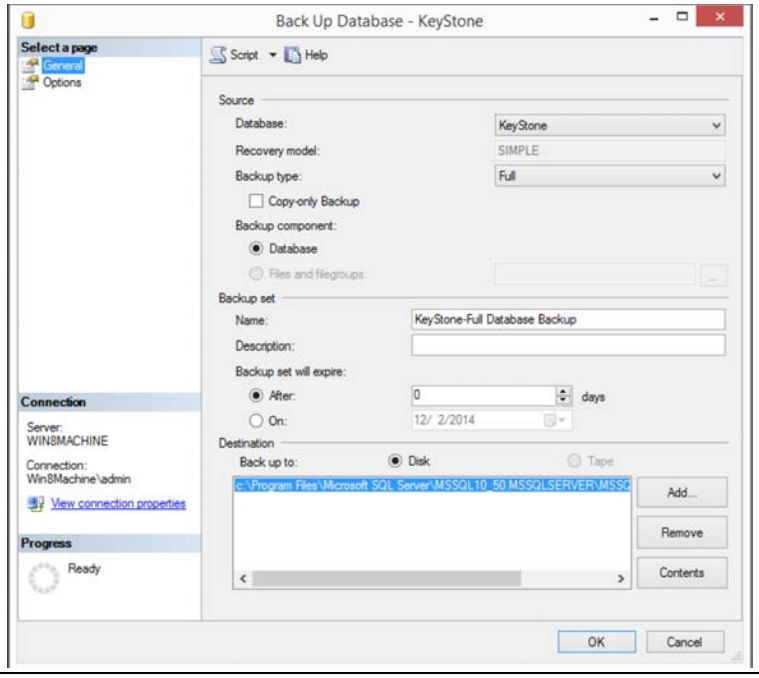


Figure 53: Backup Database Window

Note	The location of the backup files is shown in the Destination box. You may use the existing location, or specify another. The location must be on the same drive as the database (e.g. C).

Note	Make sure that **only one backup location is listed.** If multiple backup locations are used, the backup becomes split between the locations and you will need to obtain each file to perform a restore.

1. Keep the default backup values.
2. Click **OK**.
3. If the backup was successful, a confirmation message is displayed. Click **OK**.
4. Repeat this procedure with the other database.

Backing Up Additional Configuration Data

While most of a site's configuration is stored in the database, there are a few files you may also want to backup. The following files are located on each workstation:

- Picture-map files: c:\StarNet2\fortis4g_data\sensor_images
- Custom sound files: c:\StarNet2\fortis4g_data\sounds
- Language setting: C:\Users\<account>\AppData\Local\Senstar\KeyStoneWS.exe_<value>\<release>\user.config (optional, language can be set by workstation application)
- Workstation layout: C:\Users\<account>AppData\Local\StationSettings.xml

Copying Databases

After you perform a backup, you can copy the files to another location (e.g. a USB flash drive):

1. Display the folder where the backups were made (typically C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Backup).
2. Copy the KeyStone.bak and SensorsServerConfiguration.bak files to the new location.

Restoring Databases

This procedure explains how to revert the StarNet 2 databases to a previous state, or replace the existing databases with ones from a different computer (e.g. from a system configured off-site).

1. Copy the backup databases to a temporary folder on the C:\ drive.
2. If running, stop the StarNet 2 services: Right-click the Service Manager on the Windows taskbar and stop all the services by clicking **Watchdog**. All the services will stop after a few seconds.
3. Right-click the Service Manager icon and select **Exit**.
4. If your system includes additional workstations:
   a. Exit the Operator or Setup application, if active.
   b. Stop the Watchdog service in the Service Manager.
   c. Right-click the Service Manager and select **Exit**.
5. From the Windows desktop, select **Start** > **All Programs** > **Microsoft SQL Server 2008 R2** > **SQL Server Management Studio**.
6. Select SQL Server Authentication.
7. To Login, type **sa** and enter the Password.
8. Click **Connect**.
9. Expand the Databases node and select the database you want to restore:
   - KeyStone – Contains all events.
   - SensorsServerConfiguration – Contains sensor and picture-map configuration information.
10. Right-click the database and select **Tasks** > **Restore** > **Database**.

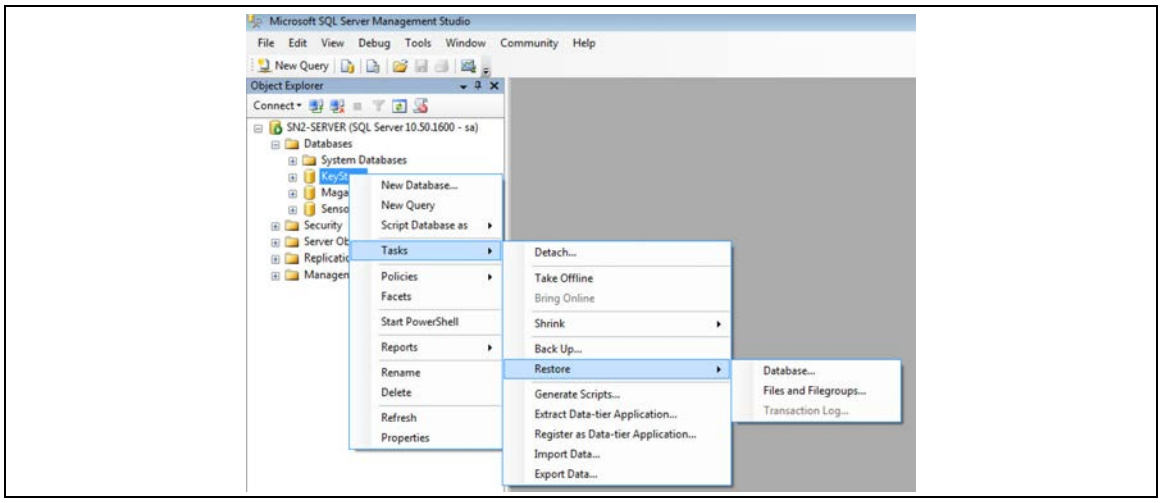


Figure 54: Accessing the Restore Database Window

The Restore Database window is displayed.

11. Select **From device** and click the **...** icon.

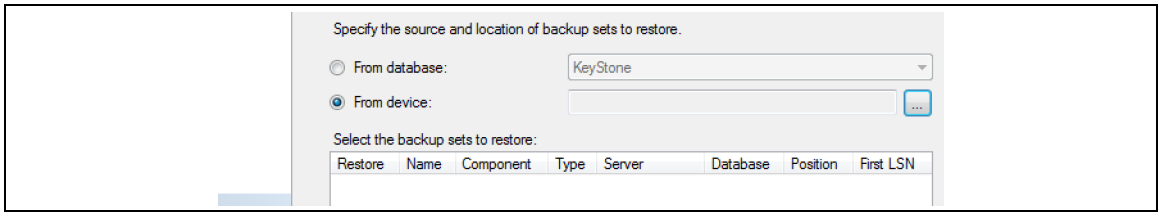


Figure 55: Restore Database setup

12. Click **Add**.
13. Select the backup file and click **OK**.

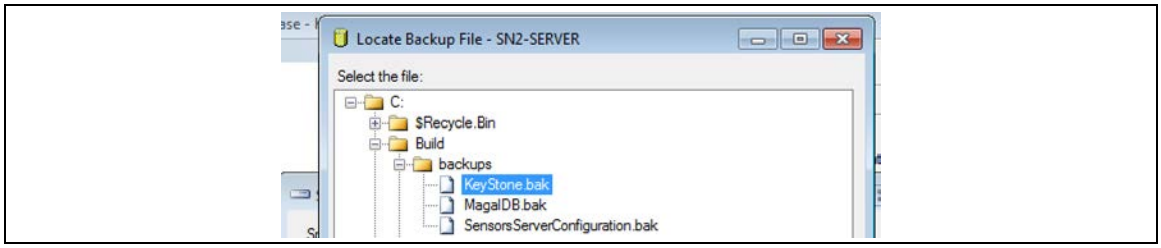


Figure 56: Selecting the Backup File

14. Click the **Restore** box. If there are multiple backup sets, select the one from the time period you wish to restore.

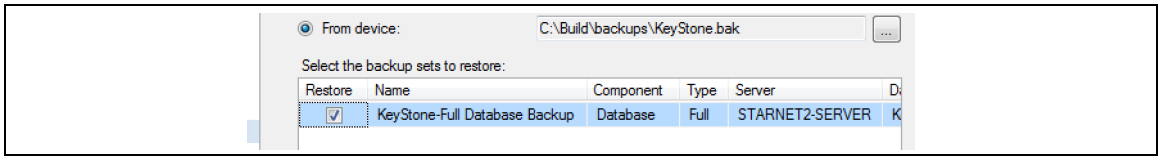


Figure 57: Restoring the Backup File

15. Click the **Options** page and select **Overwrite the existing database (WITH REPLACE)**.

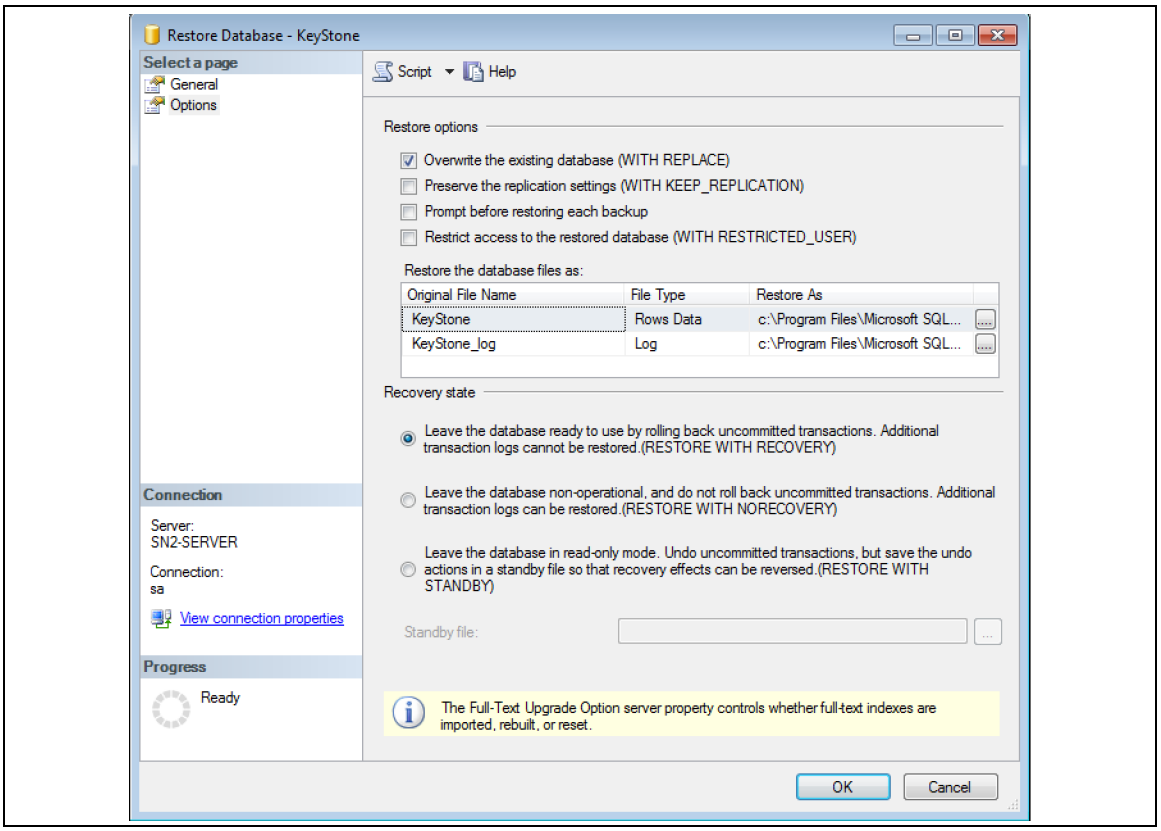


Figure 58: Finalizing the Database Restoration

16. Click **OK**.
    The database is restored. A message indicating a successful restore is displayed.

Note	If the restore fails, it is likely because one or more of the StarNet 2 services, or the Server Manager tray application, is still running. If necessary, relaunch the Service Manager, stop the Watchdog, confirm that the services have stopped, and then exit the Service Manager.

17. Click **OK**.
18. Repeat this procedure for the other databases.

Note	If the IP address of the current computer is different from the one used to create the backups, you will need to fix the IP address of the StarNet 2 services as well as the Network Manager configuration. See Using A Single PC to Stage Multiple Sites on page 86.

19. Restart the StarNet 2 services: right-click on the Service Manager and select **Watchdog**.
20. Launch the StarNet 2 application and confirm that the updated system is functional.

Using A Single PC to Stage Multiple Sites

If you are using a single PC to prepare StarNet 2 databases for multiple sites/servers, use the following guidelines to ensure an efficient and problem-free workflow.

Note	If the sites will not be on a network, stage the systems on a non-networked PC. If you use a networked PC, you will have to fix the IP addresses at the sites (see Changing IP Addresses on page 91).
OR	
Note	If the sites will be networked, stage each system on a networked PC using the correct IP address. If this isn't possible, you will have to fix the IP addresses at the site (see Changing IP Addresses on page 91).

1. Install and configure the Network Manager simulator to match your site, but leave it off at this time.
2. Install StarNet 2.
3. Make a backup copy of the databases (see Backing Up Database & Site Configuration on page 81).
4. Copy the resulting .bak files to a new location on the same drive (e.g. c:\db_template). Use this blank database as the template for subsequent sites.
5. Copy the picture-map files and any custom sounds (c:\StarNet2\fortis4g_data).
6. Run the Network Manager Simulator and configure the nodes to match the site.
7. Run StarNet 2 and configure your site.
8. Once done, make a backup copy of the new site databases (see Backing Up Database & Site Configuration on page 81).
9. Copy these files to a new location, separate from the blank database. Copy the image files from c:\StarNet2\fortis4g_data\sensor-images to the same location.
10. Stop the StarNet 2 services.
11. Confirm that the backup files are valid by performing a test restore (see Backing Up Database & Site Configuration on page 81) and restarting StarNet 2.
    Make sure the sensors are displayed correctly.
12. After confirming that your database backup files are valid, stop the StarNet 2 services and restore the original blank database to the system.
13. Run the Network Manager Simulator and configure the nodes to match the next site.
14. Start the StarNet 2 services and run Setup.
15. Repeat this process until all StarNet 2 sites/servers are done.
16. At each site/server, install StarNet 2 and then restore the specific database files for that site.

Deleting a Database

This procedure explains how to delete a StarNet 2 site configuration.

CAUTION	Use this procedure only to replace an existing installation with a new one. To keep the existing data, use the upgrade procedure.

To delete the StarNet 2 databases:

1. Remove the StarNet 2 database:
   a. Launch SQL Server Management Studio: select **Start** > **All Programs** > **Microsoft SQL Server 2008 R2** > **SQL Server Management Studio**.
   b. Enter the database authentication details (sa/password) and click **Connect**.
   c. In the Object Explorer, Select **Databases** > **KeyStone**.
   d. Right-click on KeyStone and select **Delete**.
   e. Select **Close existing connections**.
   f. Click **OK**.

      The database is deleted.
   g. Repeat this step for the SensorsServerConfiguration and MagalDB databases.
2. Delete the KeystoneUser and MagalDBUser user accounts (Security > Login).
3. In Windows Explorer, open the folder C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA.
4. Confirm that the KeyStone and SensorsServer databases are deleted. If they still exist, delete them.

   The database and sensor configuration is fully removed from the system.

Archiving Operational Data

Depending on your organization's storage and archival procedures, you may be required to periodically collect and archive operational data. Also, depending on the volume of activity at the site, the archiving of operational data may be required to maintain free disk space on the primary drive of the StarNet 2 server.

Raw Sensor Data

Consult the online help included with the UCM software about capturing and saving the raw data from Senstar sensors for troubleshooting or optimization purposes. Under normal operation, Senstar sensors report all events to the Network Manager and the raw sensor data is not required.

Network Manager Logs

The Network Manager software stores the following information:

- Debug logs: C:\Senstar\Network Manager\LogFiles
- Configuration: C:\Senstar\Network Manager\Network #\NM.xml
- Sensor events: C:\Senstar\Network Manager\Network #\events\
  - <*date*>.txt: Alarm and diagnostic events (one file per day).
  - EvAD <*date*>.txt: Detailed alarm and diagnostic events (one file per day).

Network Manager logs consist of plain-text files and are stored indefinitely, with a new file being created each day. For most sites, these files may be left as-is. For extremely high-volume sites, you may need to move these files periodically to a secondary storage device. Consult your Senstar technical representative for information specific your to site.

StarNet 2 Log Files

StarNet 2 stores all its event and user activity data in the SQL database. It also maintains a set of log files for troubleshooting purposes. These files do not contain event or user activity data and may be archived or deleted periodically to free up disk space:

- Network Manager Bridge log files: C:\StarNet2/S3/Bin/Logs/
- StarNet 2 server logs: C:\StarNet2/S3/Bin/LocalLog.xml, C:StarNet2/S3/Bin/LocalLog.xml##
- StarNet 2 application logs: C:\Users\<username>\AppData\Local\Temp\Keystone\logfileKeyStone.txt##

Note	Do not delete these files if you are currently experiencing issues and require technical support.

Note	The Windows Disk Cleanup utility can be used to quickly and safely remove the StarNet 2 application logs. When running the utility, make sure you include Temporary files.

StarNet 2 Configuration Database

The SensorsServerConfiguration database stores the configuration of the server, sensors, workstations, and rules. As this data remains relatively unchanged once a system is operational, it does not need to be periodically archived.

Note	Always maintain a current backup copy of your site's configuration (see Backing Up Database & Site Configuration on page 81).

StarNet 2 Event Database

The Keystone database stores all the alarms, diagnostic events, and user activity. This database will grow in size, with the rate dependent on the volume of activity.

Event Archival Period

The event archival period is controlled by a value set in the SQL database.

Note	Reducing the event archival period from the previously set value results in the data older than the new value being permanently deleted from the database. Ensure that this is desired before reducing the event archival period. Contact your Senstar technical representative for guidance when changing this value.

1. Exit or switch out of the StarNet 2 Operator or setup application, if currently active. You don't need to stop the StarNet 2 services.
2. From the Windows desktop select Start > All Programs > Microsoft SQL Server 2014 > SQL Server 2014 Management Studio.
3. Select SQL Server Authentication.
4. In Login, type sa and enter the Password.
5. Click connect.
6. Expand the Database's node and select the Keystone database.
7. Expand the Keystone database node.
8. Expand the Tables node.
9. Scroll to find the table dbo.GeneralConfiguration.
10. Right-click table dbo.GeneralConfiguration and select Edit Top 200 Rows.
11. Find the table row with ParamKey "DeleteEventsOlderThanInMonth". Change the value field to the number of months to retain the StarNet 2 activity. The default value is 3 months. The change takes effect immediately.

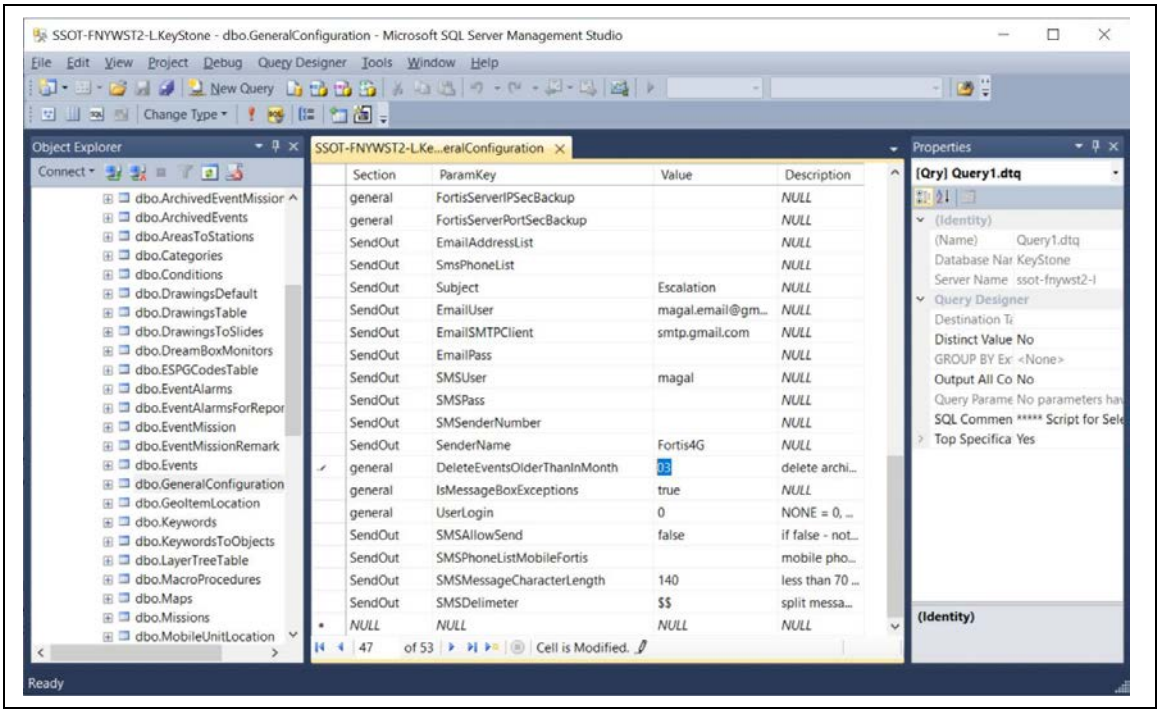


Figure 59: Keystone database

12. Save the changes.
13. Restart the PC.

Archiving Events

There are several ways to archive the record of all events that occurred in the StarNet 2 system:

- Report creation: You may generate PDF or CSV-formatted reports from within the StarNet 2 operation application (see Audits and Reports on page 77).
- Database backup: Periodically backing up the entire Keystone database will ensure that all events are saved (see Backing Up Database & Site Configuration on page 81). If you choose this method, you will need to restore the backup files on a different StarNet 2 system in order to generate reports with the data.
- Custom SQL reports: Users familiar with SQL reporting tools can use the Reporting Services to design custom-reports.

Optimizing SQL Server

CAUTION	This section describes changes to the system that should be performed only by a qualified StarNet 2 technician. Incorrectly adjusting these settings may cause instability in the system. Contact your Senstar technical representative for additional information.

Limit SQL Server Memory Allocation

This procedure adjusts how memory is allocated to the SQL Server services. Under normal conditions, you can use the default values.

1. In SQL Management Studio, right-click on the server name in the Object Explorer and select **Properties**.
2. Select the Memory page.
3. Set the Minimum server memory (in MB) to 1024.
4. Use the following formulas to set the maximum server memory values (in MB):
   - When server and client run on the same computer:
     TOTAL MEMORY (GB) – 4GB * 1024
   - When server and client run on separate computers:
     TOTAL MEMORY (GB) – 2GB * 1024

   For example, if your computer has 8 GB of RAM and runs both server and client:
   (8 – 4) * 1024 = 4096 MB
5. Click **OK**.
6. Restart the PC.

11 Troubleshooting

This chapter explains how to troubleshoot common problems, see:

Changing IP Addresses

StarNet 2 consists of a set of software components that communicate with each other. Therefore, it is important to follow the correct procedures when making changes to the sensors or network. If you change the IP address used by the StarNet 2 server, StarNet 2 will not work until you update the IP address in the software. To update StarNet 2 to work with new IP addresses, use the Fix IP(s) tool.

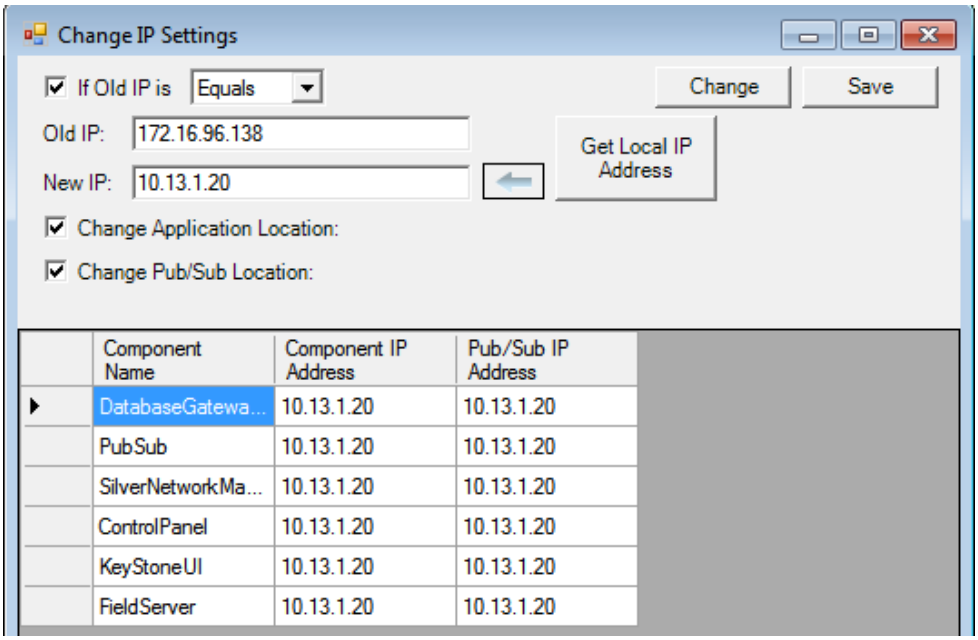


Figure 60: Change IP Settings Window

To change IP addresses:

Item	Description
Component Name	The name of each StarNet 2 service.
Component IP Address	The IP address where each StarNet 2 service runs (typically this is the server's IP address).
PubSub IP Address	The PubSub service is responsible for direct messages between StarNet 2 services. The IP address of the PubSub service should be the same for all components.
Old IP	The existing IP address in the system.
New IP	The new IP address that will be used.

1. Stop the StarNet 2 services: Right-click the Service Manager on the Windows taskbar and stop all services by clicking **Watchdog**. The services will stop after a few seconds.
2. Right-click the Service Manager and select **Tools** > **Fix IP(s)**.
   The Change IP Settings utility is displayed.
3. Adjust the IP addresses as required.

   To change from a previous IP address to your PC's current address:

   a. Enable **If Old IP is Equals**
   b. Under Old IP, enter the previously used IP address.
   c. Click **Get Local IP Address** to use the current PC IP address.
   d. Enable **Change Application Location** and **Change Pub/Sub Location**.
   e. Click **Change**.
   f. Click **Save**.
4. Close the Change IP Settings utility.

5. Right-click the Service Manager and select **Settings** > **Refresh**.
6. Restart all services: right-click the Service Manager and select **Watchdog**.
7. Update the Network Manager (or NM simulator) to use the new IP address of the StarNet 2 SMS and restart StarNet 2.
8. Configure the Network Manager Bridge in the Setup application to use the new IP address (see Configure Network Manager on page 23).

Note	If the Network Manager is running on the same PC as the StarNet 2 server and you used the loopback IP address (127.0.0.1), you do not need to update it.

9. Review the addresses of each Station in the Setup application to ensure they are using the correct IP address (see Step 1: Install the StarNet 2 client software on page 33.)
10. Launch the StarNet 2 workstation. The system will enable the sensors after a few minutes. If the sensors remain disabled, restart the StarNet 2 services.

Uninstalling StarNet 2 Software

Note	This procedure uninstalls the StarNet 2 application from the server and deletes the StarNet 2 database. The SQL Server application, however, is left as-is.

Note	To upgrade a StarNet 2 site to a new version while keeping the existing database (see Upgrading StarNet 2 on page 94).

To uninstall StarNet 2 from a server or workstation:

1. If StarNet 2 is currently running, stop the Watchdog service:
   a. Right-click the  Service Manager in the taskbar.
   b. Click the  icon next to WatchDog under the category.
   c. If you are uninstalling the server, ensure that the other services are not active. Stop them if necessary, by clicking their respective icons (if a service does not stop, close the Watchdog application, restart it via the Run as administrator command, and repeat this procedure).
   d. On the Watchdog menu, click **Exit**.

      The Watchdog service is stopped.
2. Remove the StarNet 2 application:
   a. Open the Windows Control Panel: in the search box type **Control Panel**.
   b. Select **Programs** > **Uninstall a program**.
   c. Select **StarNet 2** and click **Uninstall**.
   d. If prompted to close any applications, select the automatic option and click **OK**.
   e. If prompted, confirm the uninstallation by clicking **Yes**. Depending on your system, this may occur several times.
   f. If prompted to restart your system, you will need to restart your computer to complete the uninstallation process.

3. Remove the Senstar Installation Package:
   a. Open the Windows Control Panel in the search box type **Control Panel**.
   b. Select **Uninstall a program**.
   c. Select **Senstar Installation Package** and click **Uninstall**.
   d. If prompted to close any applications, select the automatic option and click **OK**.
   e. If prompted, confirm the uninstallation by clicking **Yes**.
   f. Click **OK** to complete the uninstallation and restart your computer.

   The Starnet 2 SMS is removed from your system.
4. Remove leftover files in the user account folder:
   a. Delete C:\Users\<name>\AppData\Local\Senstar.
   b. Delete C:\Users\<name>\AppData\Local\Temp\Keystone.
   c. Delete C:\Users\<name>\AppData\Local\StationSettings.xml
5. Delete C:\StarNet2 and C:\ComponentTypes.xml
6. Delete any StarNet 2 shortcuts located on the desktop.

Upgrading StarNet 2

Note	Before upgrading to a new version of StarNet 2, review the readme file and ensure that any build-specific procedures are followed. This procedure has been verified to work as-is for upgrading StarNet 2 from build 106 to 107, 107 to 108, 108 to 109, 109 to 110, and 110 to 111. This procedure keeps the existing database and site configuration.

To upgrade StarNet 2 server to a newer version:

1. Log in to Windows using an administrator account.
2. Stop the Watchdog service:
   a. Right-click on the Service Manager in the taskbar.
   b. Click the icon next to WatchDog under the category.
   c. Ensure that the other services are not active. Stop them if necessary by clicking their respective icons.
   d. On the Watchdog menu, click **Exit**.
   The Watchdog service is stopped.
3. Make a backup copy of the database (see Changing IP Addresses on page 91).
4. Uninstall the current version of StarNet 2 (see Uninstalling StarNet 2 Software on page 93).
5. Install the new version of StarNet 2 (see Server Installation on page 15).

To upgrade a StarNet 2 workstation to a newer version:

1. Log in to Windows using an administrator account.
2. Stop the Watchdog service:
   a. Right-click on the Service Manager in the taskbar.
   b. Click the icon next to WatchDog under the category (if service does not stop, close the Watchdog application, restart it via the “Run as administrator” command and repeat this procedure).

c. On the Watchdog menu, click **Exit**.

The Watchdog service is stopped.

3. Uninstall the current version of StarNet 2 (see Uninstalling StarNet 2 Software on page 93).
4. Install the new version of StarNet 2 (see Workstation Installation on page 31).

Troubleshooting

StarNet 2 application won't start

If the StarNet 2 application won't start:

- Check to see if the Service Manager is in the windows taskbar.
  - If it is not, right-click on the Service Manager (or Watchdog) on the Windows Desktop and select **Run as administrator**.
  - If the Service Manager won't start, check to see if there are multiple network connections on your workstation (e.g. Ethernet, WiFi). Only the configured network interface should be active.
- Ensure that the Watchdog service is running.
- Check to see if the Network Manager service or Network Manager Simulator is running (and that both are not running at the same time).
- Check to see if SQL Server is running and that there is network connectivity between the workstation and the database.
- If you have not run StarNet 2 previously or have recently changed your network's configuration, check the IP addresses and network setting.
- Ensure that the user account that runs StarNet 2 has Administrator privileges.

StarNet 2 application doesn't start automatically

If you want StarNet 2 to start automatically after bootup and Windows login:

1. Make sure that the Watchdog shortcut is in the Windows Startup folder.
2. Right-click on the shortcut and select Properties. Make sure that "Run this program as an administrator" is enabled in the Compatibility tab.
3. Add the workstation shortcut to the Windows Startup folder (see Configure StarNet 2 Shortcuts on page 29). Select Startup instead of Desktop. After perform the procedure, delete the Setup shortcut so that the Startup folder only contains Watchdog and Workstation.

If the application doesn't automatically start after a reboot, lower the Windows User Account Control (UAC) options to a lower value (in the search box type **UAC**).

Sensors are temporarily disconnected in StarNet 2 after a reboot

By default, the Network Manager service is configured to use a delayed start. StarNet 2 will function after the service has started.

By default, the workstation polls the network to determine which sensors are present in the network. It is possible, once a system is fully tested, to disable the sensor synchronization process. Contact Senstar technical support for details.

Setup or Workstation application not in Watchdog menu

If the StarNet 2 Setup or Workstation application does not appear in the tasktray menu (under Applications):

- Ensure that the Watchdog service is running.
- Check the IP addresses and network status of the PC. The network adapter used by StarNet 2 must be active.
- Ensure the Network Manager is running.
- If the applications are not appearing on a workstation, check the IP address configured on the server.

Client workstation cannot connect to database during installation

If a client workstation cannot connect to the server's database during the initial software installation process:

- Confirm that the firewall is disabled on the server.
- Check the database service log on credentials. If the system was previously working, check if the Windows account password is expired.

Error Messages

If any of the following error messages occur, follow the recommended solution to prevent them from appearing in the future.

Error Message	Solution
No user is defined.	You need to add users to the system (see User Management on page 51). If you don't want StarNet 2 to use user accounts, change the authentication to NONE in **Misc > General Configuration**.
PubSub is not connected yet.	You need to start the PubSub service. Make sure that all the StarNet 2 services are running.
No station is defined.	You need to add a local client workstation (99) to the server.
No system component defined with this station ip <*ip_address*>	One of: • The IP address of the computer has changed. In this case, run the Fix IP(s) utility and change it to the IP address currently in the database. • The client computer that you are using is not added to the system yet. In this case, add the station information in setup.
Picture layer was not found.	Make sure that the folder c:\senstar\fortis4g_data\sensor-images exists.

Sensors disabled in Workstation

If the sensors are disabled in the workstation application, check to see if the Network Manager is running and is actively communicating with the StarNet 2 server.

Click the System Status icon to display the state of the services and Network Manager. The services should have a checkmark beside them and the Network Manager should be white.

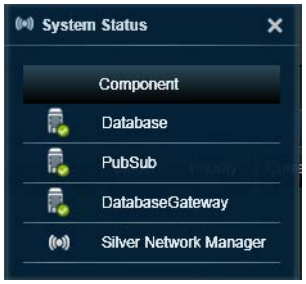


Figure 61: System Status

A red icon (or X) indicates that the service is not running, is temporarily disconnected, or is incorrectly configured. An orange Network Manager indicates that the system is still downloading sensor data from the Network Manager, or that no sensors have been added in the Network Manager.

Ranging locations are reversed

If the ranging sensors display the location opposite to the physical sensors, go to the Setup application and reverse the position of the line sensor's end points.

Ranging locations appear off sensor

If the ranging sensors display the location off the physical sensors, adjust the ranges in Setup so they accurate reflect the distances reported by the Network Manager.

Missing Maps or Sounds

You need to manually copy all map and sound files to each computer running StarNet 2. For example, if you added a map on the server, copy the JPEG files to the c:\StarNet2\fortis4g_data folder on each workstation.

Labels for Polyline Sensors are located incorrectly

The label appears where the initial icon location is defined. To change the position of a label, select the sensor location as if it was an icon, then define the polyline.

The label starts approximately 30 units above and to the right of where you click. The unit coordinates are shown in the top-left corner of the sensor placement window.

Network Managers not appearing in Setup

Perform the following:

- Ensure the Network Manager(s) are running and configured to use StarNet 2 as their SMS.
- Make sure you have defined an NM bridge component for each NMS.
- Make sure each NM bridge is configured with a unique service name, port number, and NM service ID number.
- Make sure a StarNet technology component is configured and initialized for each NM bridge component.

Sensors configured in Simulator not working on real equipment

When configuring systems off-site using the Simulator, the device nodes must match that of the Network Managers exactly. If the Network Manager nodes are different (e.g. a FlexZone processor is in node 2 instead of node 1), StarNet 2 will not recognize the configuration.

Picture-maps not filling up available space

If you have displayed a thumbnail view and then hidden the thumbnail view, the picture-map may not resize correctly. Switch to a different map and then back to refresh the image.

Make sure your images are cropped to the correct size (typically 1873 x 959 when used in a dual-monitor setup).

Renaming a Windows account used by StarNet 2

Make sure the watchdog service and SQL Server services are running under an administrator account. Restart the system to confirm the new settings.

Workstation is running in Demo Mode

If you receive a license error, make sure a valid license USB key is inserted into a PC running an active instance of the workstation (typically the server workstation) before starting another instance of the workstation application.

Procedures Not Appearing

If you assign tasks to a set of sensor events and it doesn't appear when those events occur:

- Exit from all currently running workstation applications
- In the Watchdog menu, refresh the settings (Settings > Refresh)
- Restart the workstations

Unused Sensor Points Stuck in Alarm

If there are some sensor points in the system that are not used and are generating alarms that cannot be cleared, you can mask the sensor points until the equipment is fixed:

1. In Setup, set the sensor point's Show Item on Tree property to ALWAYS.
2. Launch the operator application. and mask the sensor.
3. Return to Setup.
4. Set the sensor point's Show Item on Tree property to NEVER.

Remove Left-Over Services

If you created a system with several Network Managers, some StarNet 2 entries may remain in the Windows services list if StarNet 2 is uninstalled. To manually remove service entries, launch regedit and remove the service(s) in HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services.

Database Errors During Installation

If you encounter database errors during the installation process:

- If you are installing a workstation, make sure the workstation can see the server over the network.
- Ensure that the SQL Server service is running
- Ensure that you are using the correct login (sa/password)
- Ensure that SQL Server is configured to run as the Default Instance.
- Ensure that there are no previous instances running.

Missing Status, Tasks, and Notes More Info Tabs

If the tabs disappear (typically when switching back and forth between single and dual-monitors), delete C:\Users\<username>\AppData\Local\StationSettings.xml.

Note	The AppData folder is typically hidden in Windows.

Splash screen freezes on “Initializing Map Engine” or “Message Service” error

Make sure that:

- The workstation can see the server over the network.
- The workstation (stations) is added to the server configuration (this occurs automatically during workstation install).
- All services on the server were restarted AFTER the workstation was added and that the services are currently running.

Missing Sensors in Workstation

If some of the sensors are missing on a workstation but appear on other computers, check the alarm routing configuration for that station (see Alarm Routing on page 62).

Low Resource or Low Memory Windows Error

If a Windows error message indicating that the system is running low on resources, you should:

1. Reboot the system.
2. Check the Network Manager logs to see if the system is being flooded with invalid events generated by malfunctioning equipment.
3. Ensure that the workstation’s graphics driver and the Windows .Net libraries are fully up to date.
4. Ensure that you are using only an external graphics card, if present. Do not use both an internal and external graphics device.
5. Contact Senstar technical support.

Network Manager Bridge Icon Stays Orange in Workstation

Normally, the bridge icons (Network Status window) in the Workstation application stay orange while they are initially downloading sensor data. The icon should turn white when done. If the icon stays orange, the Network Manager bridge is not configured correctly:

1. Make sure the bridge component has a valid IP address, valid port, and valid NM properties (svr number, IP address, and protocol).
2. Make sure the bridge has a technology component correctly linked to it.
3. Make sure you stop, refresh, and restart the services.

Other Database Errors

If after installation StarNet 2 cannot communicate with the SQL database, verify that the “Collation” property set within Microsoft SQL Server is set to SQL_Latin1_General_CP1_CI_AS. If the collation property is not set this way, the most effective way to set it to SQL_Latin1_General_CP1_CI_AS is to perform a Reset on the Windows installation (Reset this PC) and in the subsequent setup process make sure the Windows Language and Locale is set to English and United States respectively. Setting the Language and Locale in this way will ensure that SQL will select the SQL_Latin1_General_CP1_CI_AS collation when SQL is installed.

Collecting Data for Troubleshooting

If you encounter an issue, Senstar technical support may request that you collect additional information from your PC.

Software Versions

Collect the version numbers of the following software applications installed on your system:

- StarNet 2 – In the Workstation application, go to Tools > About
- Network Manager Front Panel – From the main menu, select Help > About NM

StarNet 2 Server Logs

StarNet 2 server debug and logging files are located at the following locations:

- C:\StarNet2/S3/Bin/Logs/ (NM bridge log files)
- C:\StarNet2/S3/Bin/LocalLog.xml (plus rolled-over versions)
- C:\Users\<username>\AppData\Local\Temp\Keystone\logfileKeyStone.txt##

Note	Enter %temp% in the Run box to quickly display the AppData folder. There will be multiple logfileKeyStone.txt files, organized by timeframe.

StarNet 2 Workstation Logs

StarNet 2 workstation debug and logging files are located at the following locations:

- C:\StarNet2/S3/Bin/Logs/ (NM bridge log files)
- C:\StarNet2/S3/Bin/LocalLog.xml (plus rolled-over versions)
- C:\Users\<username>\AppData\Local\Temp\Keystone\logfileKeyStone.txt##

Note	Enter %temp% in the Run box to quickly display the AppData folder. There will be multiple logfileKeyStone.txt files, organized by timeframe.

Network Manager Logs

Network Manager log files maintain a record of every event recorded by the Network Manager as well as configuration and network data.

- C:\Senstar\Network Manager\LogFiles (NM communications)
- C:\Senstar\Network Manager\Network #\NM.xml (Network Manager configuration)
- C:\Senstar\Network Manager\Network #\events\ (sensor events collected by NM)

MS SQL Logs

- C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Log
- In SQL Management Studio, collect the server logs from Database > Management > SQL Server Logs

Windows Event Logs

From the Windows Event Viewer, export Windows Logs for both Application and System (expand Event Viewer > Windows Logs, right-click on Application or System, and select Save All Events As).

StarNet 2 Databases

Obtain the disk usage of the two StarNet 2 databases:
(KeyStone and SensorsServerConfiguration)
located in:
C:\Program Files\Microsoft SQL SERVER\MSSQL10_50.MSSQLSERVER\MSSQL\DATA.

Windows Performance Data

Collect data from the Windows Performance Monitor (Task Manager > Performance > Resource Monitor).

Making Changes to Deployed Systems

The following table lists the steps required after making changes on actively running systems.

Application	Change	Required Action
Setup	Changes to PubSub or any system component properties	Stop services, refresh settings, and restart services
Network Manager	Changes to sensor nodes	Restart Network Manager service and launch setup after new configuration has finished downloading
Setup	Sensor line or icon moved	Restart other active workstations
Setup	Rename a sensor	Restart other active workstations
Setup	Add new sensor	Restart other active workstations
Setup	Change to General configuration properties	Restart other active workstations
Setup	Add or delete a picture-map	Restart other active workstations
Setup	Add new station	Restart other active workstations
Workstation	Add or edit a procedure or any other procedure settings	Restart other active workstations
Workstation	Add or edit a user	None
Workstation	Any change using Sensor management tool	Restart all workstations
Workstation	Any change using Rule engine tool	Restart all workstations

Startup Time and Processes

The time required for StarNet 2 to start operation depends on the number and configuration of sensors. However, the following process occurs in all systems. If a step does not start, there may be a configuration issue.

Note Senstar recommends that you record and observe the start of each software component during setup and testing so that you can use them as a reference when observing the booting of a production system.

1. Windows bootup.
2. Network Manager(s) Services.
3. Operator login to Windows (if required).

4. StarNet 2 Service Manager tray application.
5. StarNet 2 operator application (depending on system configuration, some systems may be configured for it to start manually).
6. Sensor synchronization. The time required depends on sensor configuration. This time can be measured during setup and kept as a reference.
   The Network Manager bridge icon (in the Network Status box) is orange when the sensor information is being polled and turns white (fully functional) when the sensor synchronization is complete. See Configure Network Manager on page 23 for information about enabling or disabling sensor auto-synchronization.
   On a finished, tested system, you can disable auto-synchronization to improve start times. Contact your Senstar technical representative for information.
7. Network Manager bridge icon(s) turns white, indicating that the system is operational.

12 Server and Workstation Security

This chapter explains how to lock down the StarNet 2 server and workstations to prevent unauthorized access:

SQL Server Security

This section explains the security considerations involving SQL Server configurations.

SQL Server Account

By default, SQL Server runs using the Network Service built-in account. To run SQL Server under a centrally managed domain-authenticated account, edit the SQL Server Services properties in SQL Server Configuration Manager and select a custom account.

SQL Server Browser

By default, SQL Server Browser runs under the Local Service account and enables all administrator users access to the database. To limit access to the database:

- Configure SQL Server Browser to run under a centrally managed domain-authenticated account (SQL Server Browser properties).
- Block unnecessary user accounts from accessing the database. In SQL Server Management Studio, remove the users from the Security > Logins tree.

Windows Security

This section explains how to lock down the StarNet 2 environment to prevent operators from accessing other applications or operating system functions.

User Accounts

The StarNet 2 Server must run under a Windows administrator account as the Watchdog must be able to start and stop services. StartNet 2 workstations, however, can use non-administrator accounts when running the Operator application.

Password Requirements

If you want StarNet 2 to start automatically without requiring a Windows user login:

1. Click **Start**, type **netplwiz** and press Enter.
2. In the User Accounts dialog box, click the account you want to automatically log on as.
3. Make sure that the box for Users Must Enter a User Name and Password is left unchecked.
4. Click **OK**.
5. If prompted, enter the password the account twice and click **OK**.

Windows 7 Lock Down Activities

You can prevent user access to the operating system via a combination of StarNet 2 configurations, Windows policy settings, and third-party keyboard intercept scripting.

Step 1: Configure StarNet 2 Exit Password

Configure StarNet 2 to require a password to exit the application (see To configure an exit password: on page 58).

Step 2: Configure StarNet 2 Workstation to Start Automatically

Add the Workstation application to the Windows Startup folder (see Configure StarNet 2 Shortcuts on page 29).

Step 3: Disable Popup Window on USB device insertion

In Control Panel, Select Hardware and Sound > AutoPlay and disable Use AutoPlay for all media and devices.

Step 4: Prevent Access to User Account Switching and Task Manager

1. Launch the Local Group Policy Editor: Click **Start**, type **edit group** in Search bar, and select **Edit Group Policy**.
2. Under Computer Configuration, disable user switching:
   a. Select **Administrative Templates > System > Logon**.
   b. Enable **Hide Entry Points for Fast User Switching**.
3. Under User Configuration Options, disable Ctrl-Alt-Delete settings:
   a. Select **Administrative Templates > System > Ctrl+Alt+Delete Options**.
   b. Enable all options.

Step 5: Block Task Switching Keys

1. Download and install the utility “Autohotkey” from http://autohotkey.com.
2. Create a script (starnet2_keyboard.ahk) with the following content:

```
; Disable Alt+Tab
!Tab::Return
; Disable Alt+Windows Key + Tab
*LAlt::LCtrl
LCtrl::Return
; Disable Windows Key + Tab
#Tab::Return
; Disable Left Windows Key
LWin::Return
; Disable Right Windows Key
RWin::Return

; disable escape key sequencess
!Esc::Return
^Esc::Return
```

3. If you want to enable access to the Network Manager Front Panel (or Simulator) add the following line to the script:

```
RunOrActivate(Target, WinTitle = "")
{
	; Get the filename without a path
	SplitPath, Target, TargetNameOnly

	Process, Exist, %TargetNameOnly%
	If ErrorLevel > 0
		PID = %ErrorLevel%
	Else
		Run, %Target%, , , PID

	; Activate by title if given, otherwise use PID.
	If WinTitle <>
	{
	SetTitleMatchMode, 2
	WinWait, %WinTitle%, , 3
	TrayTip, , Activating Window Title "%WinTitle%" (%TargetNameOnly%)
	WinActivate, %WinTitle%
}
	Else
{
	WinWait, ahk_pid %PID%, , 3
		WinActivate, ahk_pid %PID%
}
}

; launch diagnostics
^n::RunOrActivate("C:\Senstar\Network Manager\NMS Front Panel.exe")
return
```

   where ^ is the control key, ! is the alt key, and n is the letter.

4. Copy the script to the Windows StartUp folder.

Windows 10 Lock Down Activities

New Windows 10 security permissions do not allow programs that require administrative privileges to be placed in the startup folder. This affects AutoHotKey (AHK) from preforming as intended with StarNet 2. This section provides instructions to get the AutoHotKey program working correctly with Windows 10. Please refer to Windows 7 Lock Down Activities on page 106 to configure the AHK files and StarNet 2 for auto start up. This procedure must be done from the Administrator account.

Note	Make sure that you have the current version of AutoHotKey (Version 1.1.30.03 as of the date of this manual).

1. Create the starnet2_keyboard.ahk file and then copy it to the desktop (see Windows 7 Lock Down Activities on page 106).
2. Right-click and “Compile Script” (1) as seen in Figure 62: . It should output an exe File (2).

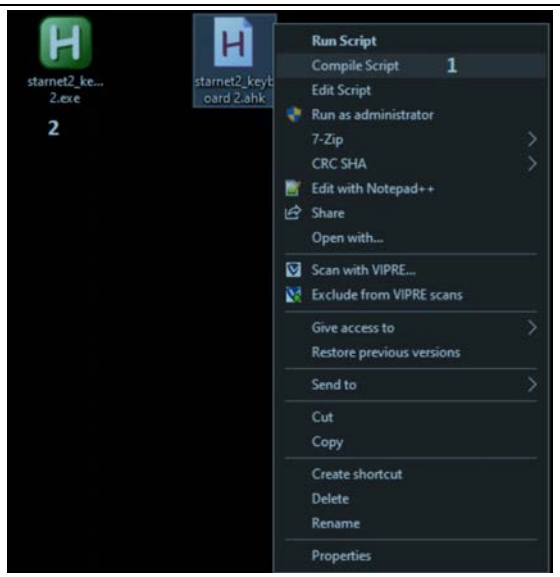


Figure 62: Compile Script

3. Click the Windows key on the keyboard and type “task scheduler”. Open the application.

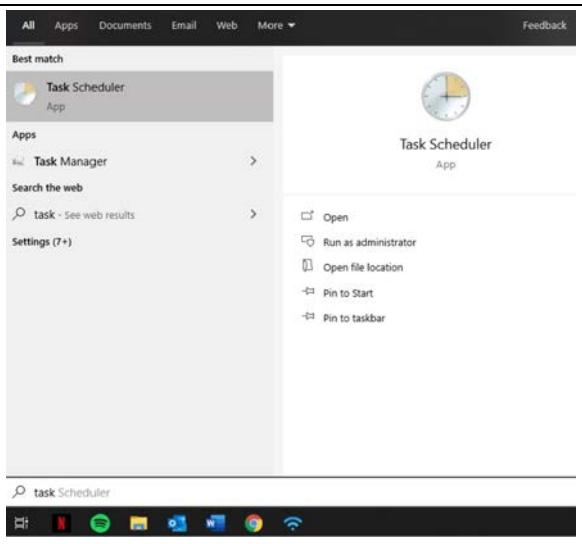


Figure 63: SQL Task Scheduler

4. With task scheduler open. Go to “Action” > “Create task”.

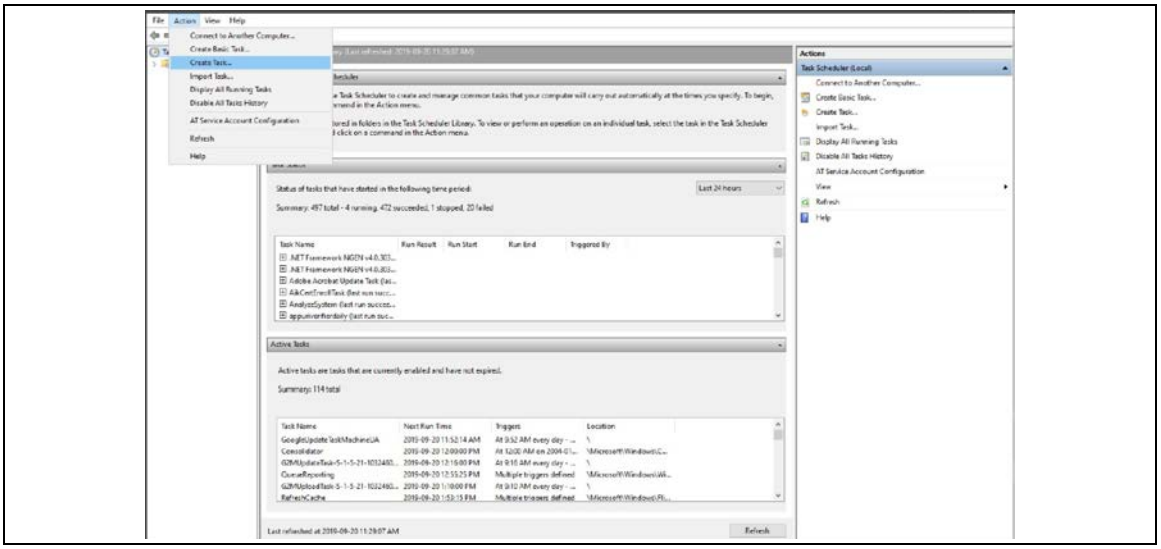


Figure 64: SQL Create Task

5. In the name field type AutoHotKey SN2 or any relevant name (1). Make sure that “Run with highest privileges” is checked (2). Select “Configure for Windows 10” (3) from the dropdown.

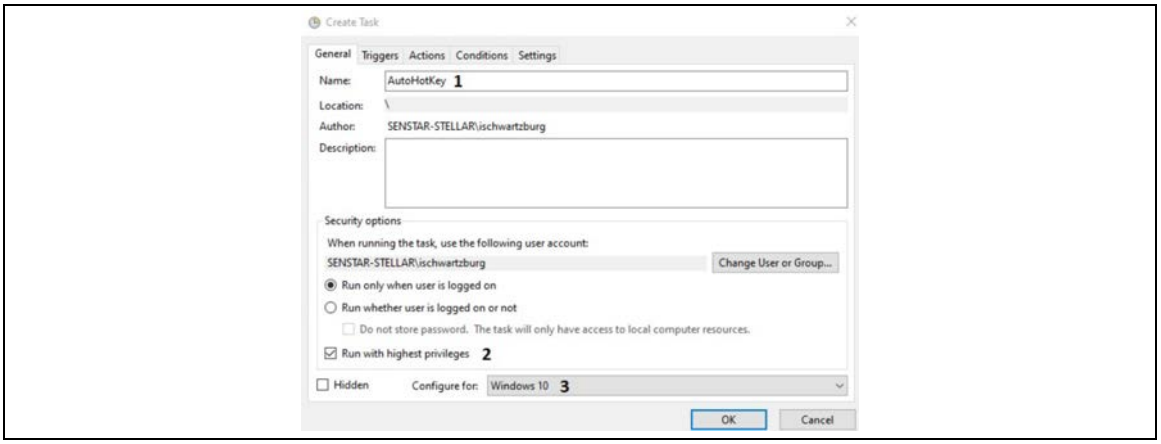


Figure 65: Creating a Task

6. Next, configure the trigger (this is when the action will happen). Choose the “Trigger” tab and click “New” at the bottom. In the “Begin the task” drop down choose “At log on”. Make sure “any user” is selected (see Figure 66:).
7. Click OK.

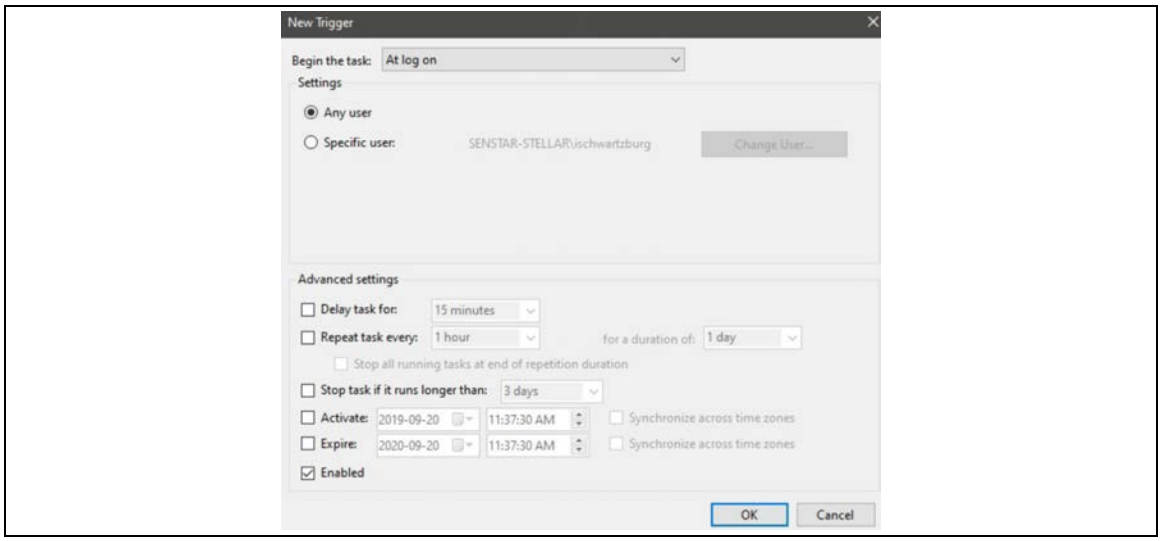


Figure 66: Configuring the Trigger

8. Next click the “Actions” tab (this is where you define what will happen). Click “New” at the bottom. By default the action should be “Start a program” (1). If not select “Start a program” from the dropdown. In the “Program/script” field click “Browse” (2).

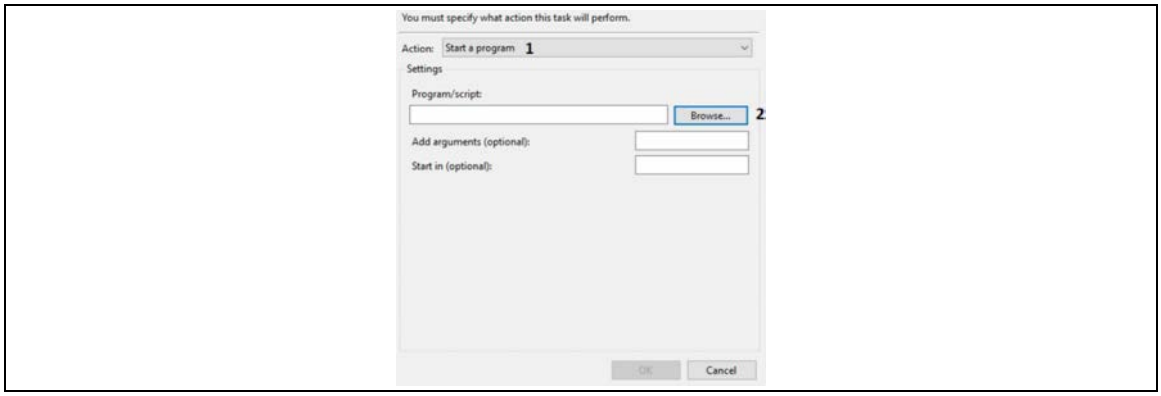


Figure 67: SQL Server installation window

9. In the file browser choose the .exe file that was created in Step 1 of this procedure.

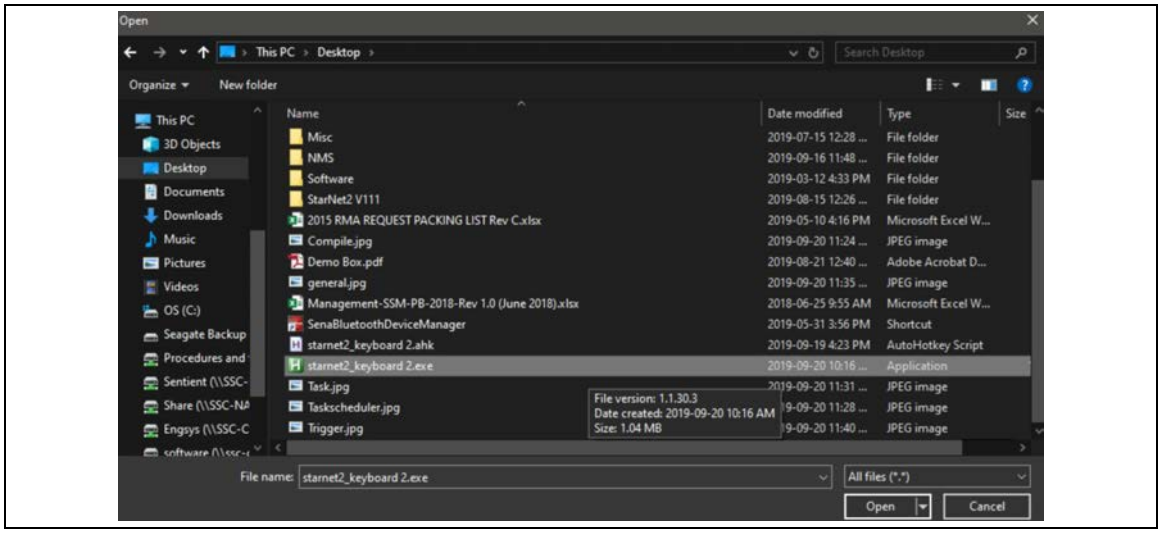


Figure 68: Selecting the .exe file

10. Click “Open”. On the next window, click “OK”. On the next window, click “OK”. This will create the auto start up task. To test the task, reboot the computer.

Firewall and Port Settings

You can determine which ports are required by StarNet 2 to communicate with other StarNet 2 workstations by running **Tools > Set Active** from the Watchdog menu.

Anytime that you get the error message **server not responding** on a workstation, it means there is a communications problem with one of the StarNet 2 services on the server. If the Fix IPs utility still works, then the database connection is OK but something else is wrong. To prevent these communication problems Senstar recommends testing the ports with telnet before installing the workstation.

StarNet 2 should be run within a secured environment and isolated from the Internet. For additional security, a host-based firewall like Windows Firewall can be used, if TCP traffic is enabled for key ports. By default, the following ports are used:

- 4G Server – 9107
- Database Gateway Service – 9080
- PubSub – 9084
- Server ExternalSystems – 9100
- SenstarNMBridge – 9075
- StarNet 2 (and other workstations) – 9083
- MsgDevManager – 9094
- RuleEngine – 9099

Note	Each subsequent Network Manager bridge added to the system will require its own unique port number (i.e. 10001).

The following is a summary of how to get StarNet 2 running on PCs that use firewalls:

- run the StarNet 2 Set Active utility to obtain a list of the ports being used
- in Windows Firewall/Advanced Firewall Settings on the server:
  - add StarNet 2 as an allowed program in outgoing connections
  - create a new incoming rule that opens up the required StarNet 2 ports
- from the workstation, test the settings by running telnet <ip_address> <port> on each port:
  - enable telnet client (Programs > Add Features)
  - if the port is open, telnet will go to a blank screen
  - if the port is closed or the network is down, the connection is refused
- add StarNet 2 as an allowed program on the workstation

13 Commissioning Checklists

When installing StarNet 2 at a site, review the following checklists to ensure all necessary tasks are completed and the system is fully operational.

Before You Go To Site

The following checklist lists all the activities that can be done off-site.

Done	Task	Value/Options
	Ensure that Windows is fully updated and patched, especially the graphics drivers and the .NET libraries	
	Set correct time zone on PC	
	Copy StarNet 2, Network Manager (if required), and UCM (if required) builds to folder on C drive	
	Install SN2 software	# of workstations:_____
	Install Network Manager (if required)	
	Install UCM (if required)	# of workstations: _____
	Ensure Windows taskbar shows all icons by default	
	Configure Windows notification/AV/update settings	
	Configure BIOS to boot after power loss	
	Configure StarNet 2 workstation application to auto start	
	Configure Windows to show extensions, hidden files	
	Disable screen-saver, power saving modes	
	Disable Windows screen animations, transparency, etc.	
	Password-protect UCM, if installed	
	Create user accounts (i.e. administrator account, operator accounts)	
	Create maps with editable labels (i.e. PPT), determine output monitor (1 or 2) and resolution requirements	
	In Network Manager (or simulator) confirm Node order and add sensors	Sensors (in order):

	Configure Windows auto-login	
	Configure Windows password never expire (if required)	
	Lock down PC	
	Create Contact Technical Support label for PCs	
	Use UCM config files for StarNet 2 ranging configuration, if required	
	Configure NM alarm hold time	0 seconds (v1.0 only)
	Create SN2 desktop shortcuts: watchdog, setup, workstation	
	Remove all desktop but SN2 and NM Front Panel	
	Remove simulator, if present	
	Configure SN2 exit password	
	Configure alarm repeat time	
	Configure alarm sound	
	Configure equipment alarm repeat time	
	Configure equipment alarm sound	
	Configure alarm close reasons	For example: Fence test Intrusion attempt Maintenance Staff Traffic Unknown Wildlife Weather
	Review role permissions	
	Perform pre-site backup of db	
	Test power fail recover	

At the Site

The following activities are typically performed at the site. Completing the tasks will result in a fully functional, and tested system.

Done	Task	Options
	Connect PCs to sensor network	Connection type: _____
	Configure NM, UCM, SN2 as required	
	Confirm communication (NM, UCM, SN2)	
	Adjust sensors on picture maps as required	
	Configure ranging info for each sensor	Z1: Z2: Z3: etc.
	Configure sensor disable option (mask) for each sensor	Sensor 1: Yes/No Sensor 2: Yes/No etc.
	Permanently mask and hide any unused sensor points that generate equipment error alarms (show in tree, mask, hide in tree)	List sensor points (use blank page)
	Add procedure text (i.e. Call up camera 12)	
	Create initial operator accounts	
	Perform zone tests	
	Adjust as required	
	Stop system, perform database backup	
	Restart system	
	Perform training with real fence data	