

Sensor Management in Genetec Security Center

The NMS-GSC software provides complete, bi-directional integration between Senstar perimeter intrusion detection systems and the Genetec™ Security Center (GSC) software.

Senstar's Network Manager software provides a common interface for monitoring and controlling Senstar sensors from VMS, SMS, and PSIM systems.

The Network Manager Service to Genetec Security Center Gateway (NMS-GSC Gateway) integrates the Network Manager service (NMS) with a Genetec Directory service or pair of redundant Directory servers.

OPERATOR FEATURES

From Security Center, operators can:

- Graphically view sensor status on a map
- View video associated with alarms
- Acknowledge alarms
- Arm/disarm zones
- Activate sensor output points (relays)
- Monitor equipment fault alarms

Features and Benefits

- Display zone alarms and equipment status information from Senstar sensors with Security Center
- Supported sensor events include:
 - Sensor/zone alarms (including precise location for ranging sensors)
 - Enclosure tamper events
 - Diagnostic and connectivity faults
- All changes in sensor status are monitored and available as input conditions for event-to-action programming
- Arm/Disarm alarm reporting per sensor zone through on-screen control or event-to-action
- Control sensor output relays by event-to-action programming or by on-screen controls
- Custom icon for zone alarm and status reporting
- Custom icons for output (relay) control and input point status
- Support for redundant Network Managers and Genetec Directory servers
- Support for current Senstar perimeter intrusion detections sensors, including FlexZone®, FiberPatrol®, Senstar LM100, OmniTrax®, UltraWave™, UltraLink™ I/O and XField®
- Alarm Logic Engine support
- Compatibility:
 - Security Center 5.7, 5.8 and 5.9 (certified on 5.7 SR5)
 - Network Manager 2.38 and newer

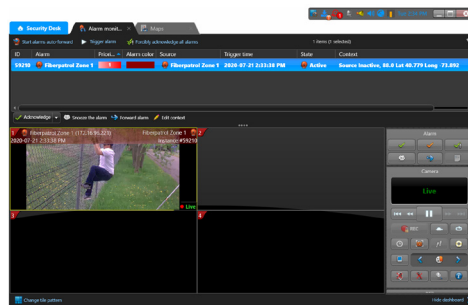
DISPLAY ZONE ALARMS AND SENSOR STATUS

For display of zone alarm status, the NMS-GSC Gateway includes a custom NMS Zone entity. The NMS Zone entity includes custom icons to display detailed status of the alarm zone on the Security Center map and controls to acknowledge and arm/disarm the zone alarm. The zone alarm status conditions that can be displayed are: OK, Alarm, Pre-Alarm, Trouble, Supervision, and Disarmed. For sensors that report a precise intrusion location, the last reported location will be displayed in the Context field.

For display of sensor status, the NMS-GSC Gateway includes a custom NMS Node entity. The NMS Node entity includes custom icons to display the detailed status of a sensor (node) on the Security Center map and controls to acknowledge sensor faults. The sensor status conditions that can be displayed are: OK, Comm Fault, Comm Fail, Enclosure Tamper, Warning diagnostic, and Critical diagnostic.

EVENT-TO-ACTION TRIGGERS

Alarm entities can also be used as trigger events for event-to-action sequences (camera call-up, activation of a siren, turning on lighting, etc). To support event-to-action programming for all sensor conditions monitored by the Network Manager, the NMS-GSC Gateway adds two custom entities to Security Center: NMS Input and Output.



Senstar alarm in Alarm Monitoring screen

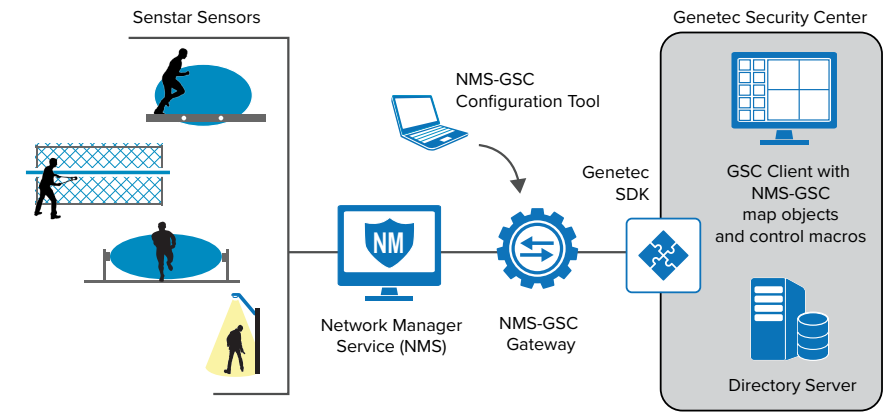
Dry-contact inputs on sensors can be linked to NMS Input entities and used as triggers for event-to-action programming. In this way, non-alarm generation events can still trigger event-to-action sequences. Another example use is a sensor pre-alarm condition used to initiate the move of a PTZ camera before an alarm actual occurs.

Output relays on sensors can be linked to NMS Output entities and controlled by event-to-action macro programming or on-screen controls. Any Security Center event can be used control a Network Manager output point. The NMS Output entity also reports the status of an output point, so that Security Center can detect when another system has commanded a state change.

SYSTEM INTEGRATION

The Network Manager, NMS-GSC Gateway, and Genetec Directory server may be installed on the same server or on separate networked servers.

- NMS-GSC Gateway communicates with the Directory server via SDK and includes files which are installed on each Security Center client.
- The NMS-GSC Gateway Configuration Tool configures the gateway.



NMS-GSC system integration

ORDERING INFORMATION

Senstar part number	00SW0261
Genetec SDK connection license	GSC-1SDK-SENSTAR-NMS Three (3) required per standard Gateway, five (5) required per redundant pair of Gateways Plan Manager Standard license required to display alarms on maps

SOFTWARE COMPATIBILITY

Operating System	Microsoft Windows 10 Pro 64-bit, Windows Server 2016, 2019
Senstar Network Manager	2.38 or newer
Genetec Security Center	5.7 SR5, 5.8, 5.9

DOCUMENTATION

The NMS-GSC Gateway includes comprehensive installation and configuration documentation. Contact your Senstar representative for information.