UL Configuration and Alarm Handling

Revision Date	Version
2021-06-24	1 - “V2” web interface

400 N Tampa St, Suite #1750
Tampa,
FL 33602
(888) 387-2860

www.SureViewSystems.com

Contents

General

SureView® is a UL Classified automation software platform which receives alarm events from multiple industry standard receivers. SureView associates these events with on-site video and other security devices/systems displaying them to the operator in a way that is highly automated and easy to use. Combining the ability to receive events from UL certified burglar and fire alarm systems with video and audio confirmation; SureView® delivers a powerful and unique product to today's security center. SureView® is an open architecture software product which integrates a wide range of security systems providing security centers with a single point of control and enhanced situational awareness for coordinating the rapid response to security events.

In order to meet the UL 1981 3rd edition this document must be followed when installing, operating, and maintaining SureView®

To obtain the 1981 standard and for additional information on it refer to UL's website at www.ul.com

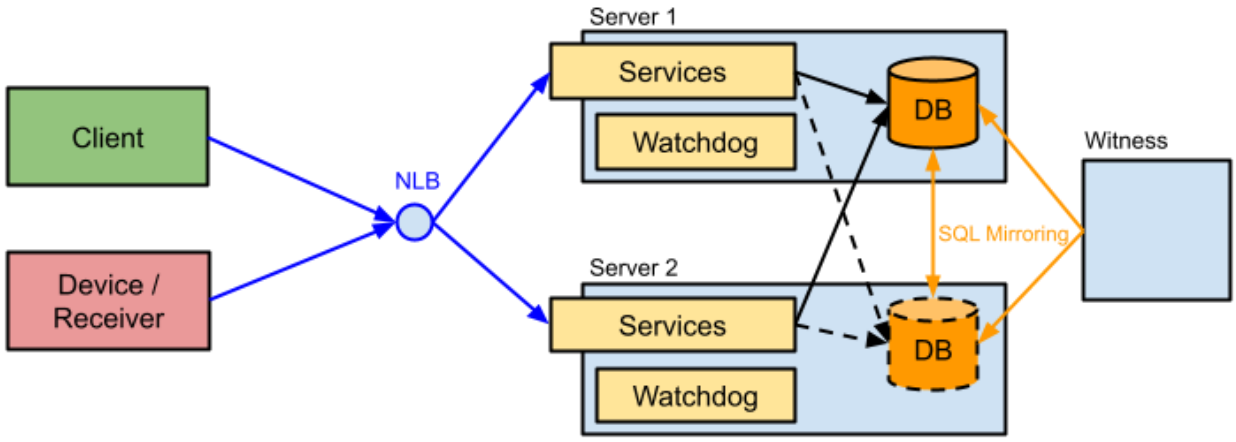
For additional support and troubleshooting information including our support portal refer to our website at www.sureviewsystems.com

Components

A UL-certified SureView deployment is fully redundant to be compliant with all the UL Monitoring Equivalent Weight (MEW) factors and consists of the following components:

- 2x SureView servers configured with SQL Mirroring and Network Load Balancing plus a Witness server which all work together to provide a fully redundant solution.
- Workstations used by operators to process alarms
- Receivers getting the alarms from panels on site and passing them to the SureView servers.
- Ethernet network connecting the above items together

Components of a failover SureView deployment:



Minimum Specifications

Servers

SureView can be installed on physical servers or virtual machines and requires a total of three servers:

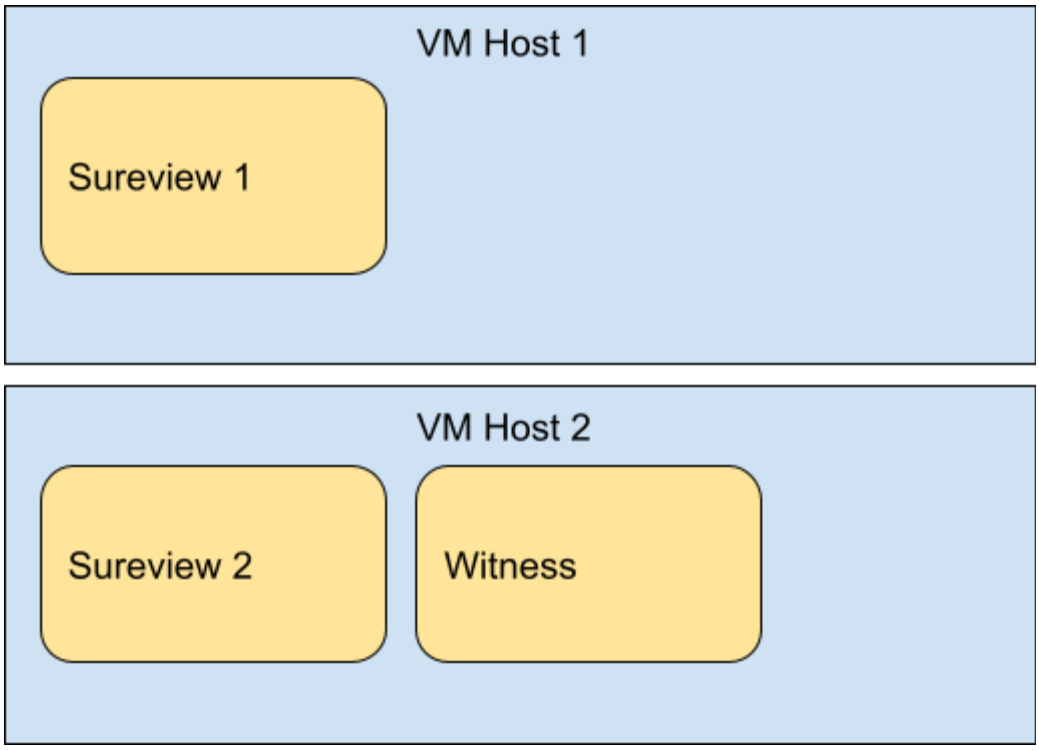
- two identical SureView servers
- a Witness server which performs automatic failover of the database to the ‘mirror’ server in the event the current ‘principal’ server fails.

Virtualization

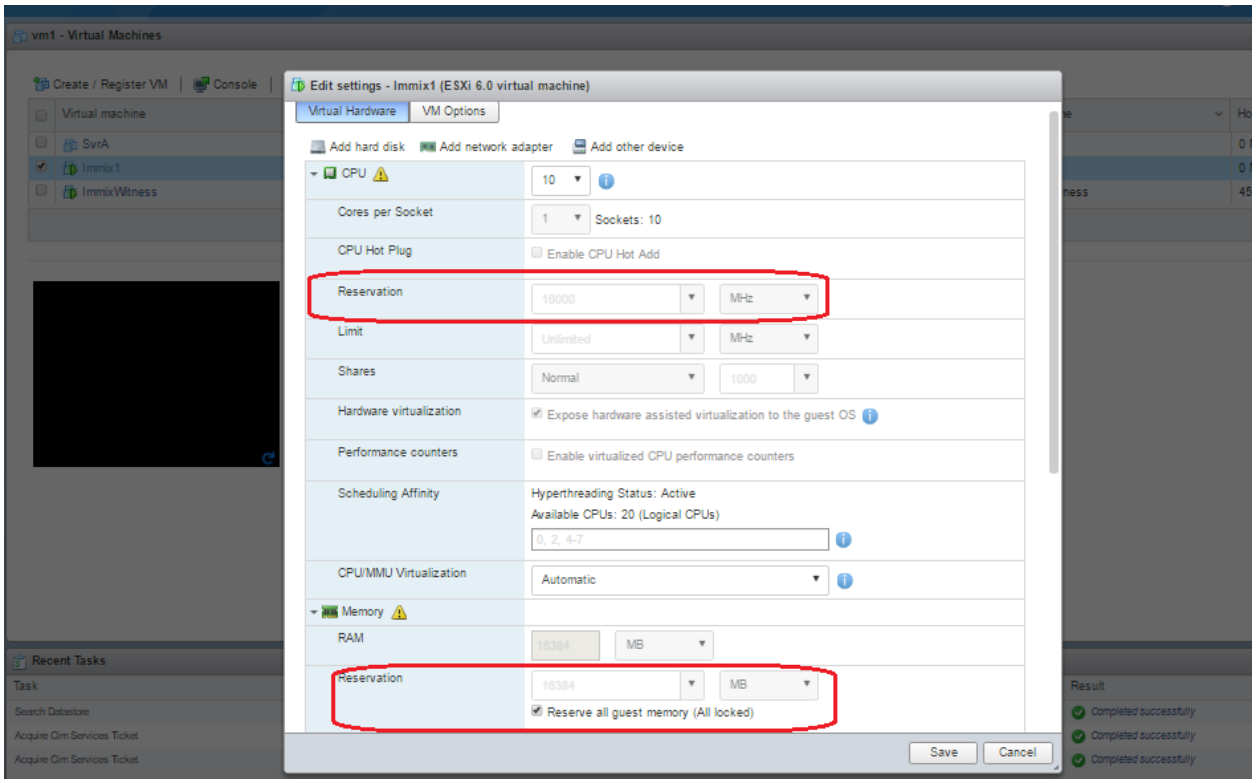
If virtualization is being used then the following additional requirements exist in order to meet UL 1981:

1. At least two physical VM hosts are required for redundancy, with the two main server VMs each existing on a different host (see diagram below - note the Witness can be on either host)
2. The three VMs must be given dedicated (or “reserved”) CPU and RAM resources so that they are not shared with other VMs. Refer to the manufacturer’s documentation of your virtualization hypervisor software on how to configure this.

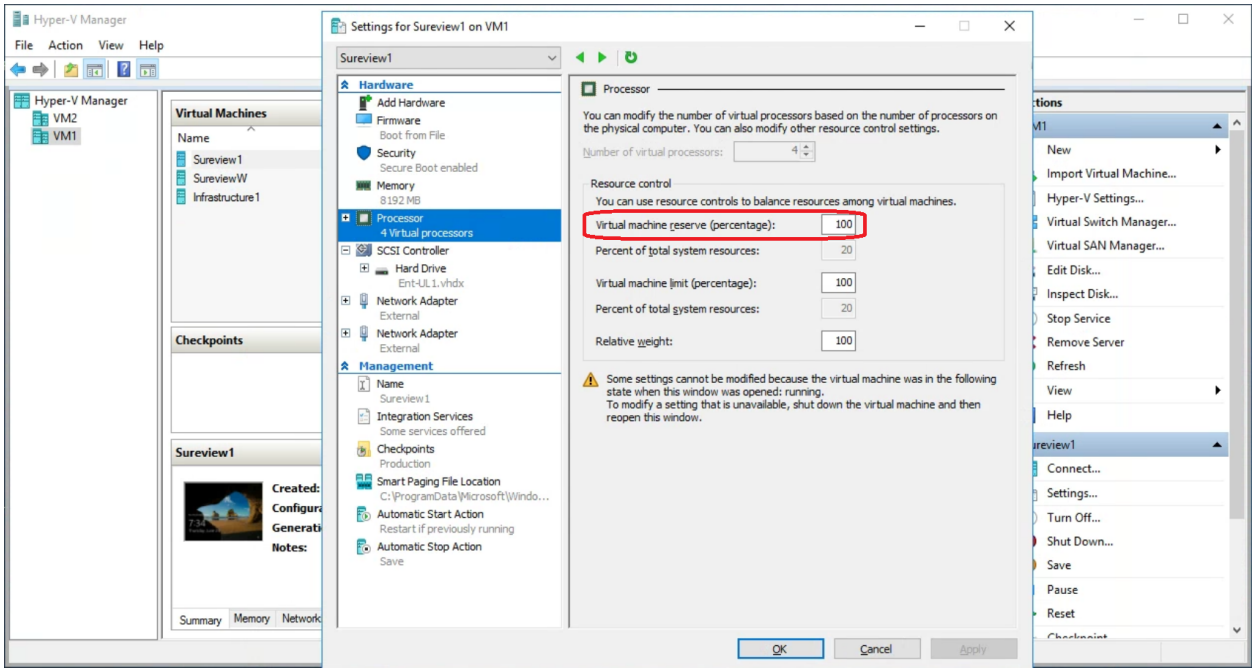
VM deployment with the minimum of two physical hosts:



Setting CPU and RAM resources for a VM to be reserved in VMware:



Setting CPU resources for a VM to be reserved in Hyper-V:



Minimum Specifications

All physical servers

All physical servers (whether hosting VMs or SureView directly) must meet UL 1981 including the minimum hardware specifications of:

- A Nationally Recognized Testing Laboratory (NRTL) certification, such as being listed for UL 60950-1 Information Technology Equipment safety (contact your server manufacturer to confirm this)
- 2x PSUs in redundant configuration (also called “1:1” or “active/active”)
- 2x Cooling fans
- 2x HDDs in RAID1
- 2x Network Adapters
- If hosting VMs:
    - Any Type-1 native hypervisor such as VMWare ESXi v6.0 or higher, or Hyper-V Server 2016 or newer
    - Enough CPU, RAM, and HDD resources to host 1x SureView server and the Witness (see specifications below)
- If hosting SureView directly:
    - Enough CPU, RAM, and HDD resources for the particular server role (see specifications below)

SureView servers (physical or virtual)

Minimum specification for the 2x SureView servers (physical or virtual):

- Microsoft Windows Server 2012 Standard edition or higher
- 8GHz CPU (reserved if virtual)
- 8GB RAM (reserved if virtual)
- 100GB HDD
- 2x Network Adapters
- Microsoft SQL 2012 (“v11”) Standard edition or higher

Witness server (physical or virtual)

Minimum specification for the 1x Witness server (physical or virtual):

- Microsoft Windows Server 2012 Standard edition or higher
- 4GHz CPU (reserved if virtual)
- 4GB RAM (reserved if virtual)
- 100GB HDD
- 1x Network Adapter
- Microsoft SQL 2012 (“v11”) Express edition or higher

Workstations

The workstations access the SureView interface via a compatible web browser (no SureView components are deployed to the workstation) using the NLB address shared by the servers which means no action is needed by the operator in the event of a server failover to continue

working.

The following requirements exist in order to meet UL 1981:

1. There must be at least two operator workstations
2. All workstations must have speakers connected so audible alerts can be heard
3. Saving of passwords must be disabled in the browser (refer to your browser manufacturer's documentation for instructions on disabling this)

Minimum Specifications

- Pentium (or similar) 1.3GHz and higher
- Microsoft Windows 8 or newer
- Chrome or Firefox browser
- 4GHz CPU
- 4GB RAM
- 100GB HDD
- Soundcard with speakers for audible alerts

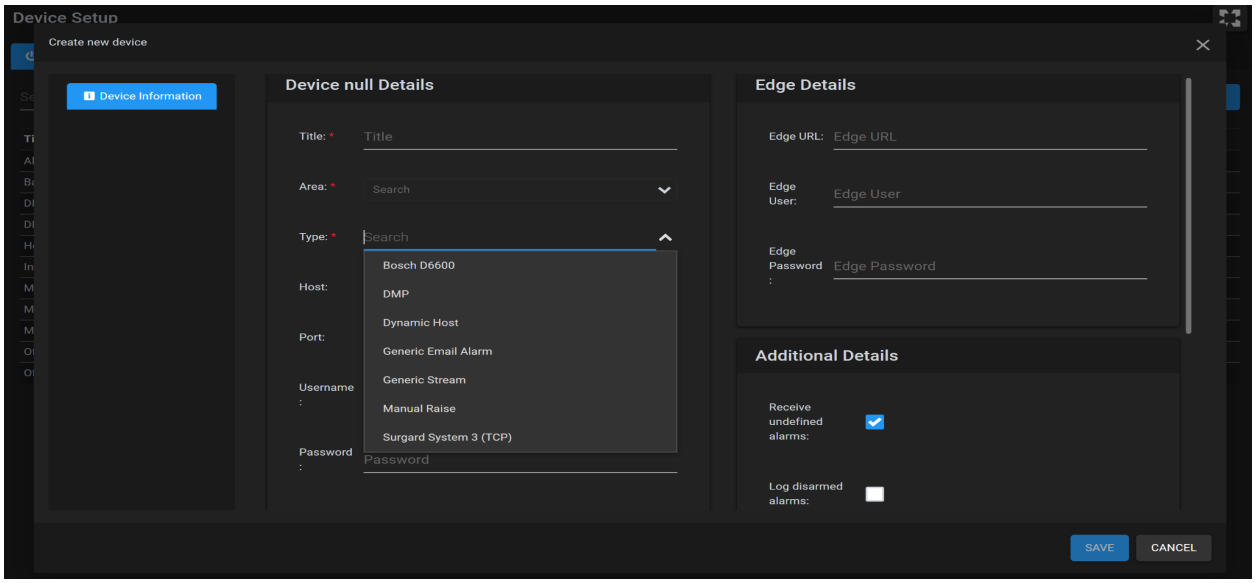
Receivers

The receivers that are compatible with the SureView platform are:

- **DMP SCS-1R, SCS-1, SCS-VR v1.3.5**
    - Failover note: the DMP receivers connect to the shared NLB IP of the SureView servers so no manual changes are required in the event of a failover.
- **DSC Sur-Gard System 3**
    - Failover note: the Surgard receiver is connected to by the current primary SureView server so no manual changes are required in the event of a failover.
- **Bosch D6600 (with D6680 terminal server)**
    - Failover note: the Bosch receiver connects to the primary server only so must be changed over manually in the event of a failover.

The list of installed integrations can be seen in the "Device Setup" screen of the UI

Installed integration list:



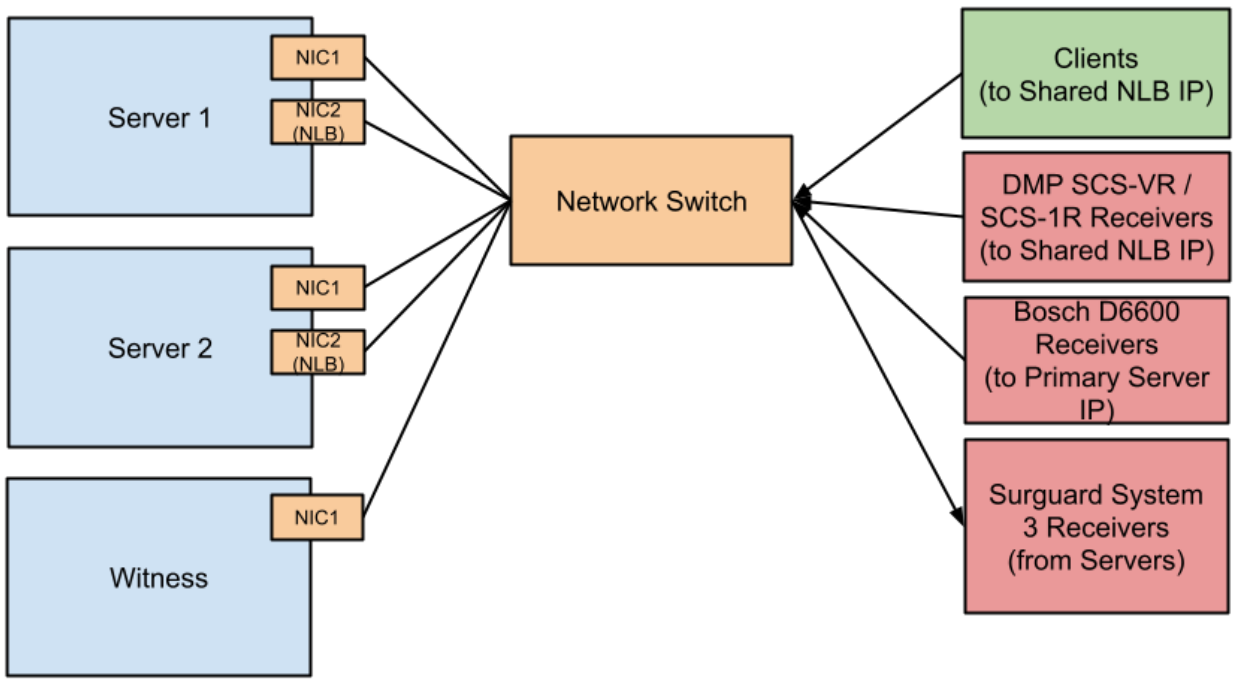
Network

The servers, receivers, and workstations must be connected together by UL certified network switches.

Tested specification:

- Linksys SD2008 v3.0 8 Port 10/100/1000 Switch (for servers)
- Netgear JFS524 24 Port 10/100 Mb (for Receivers and Panels)

Network Diagram:

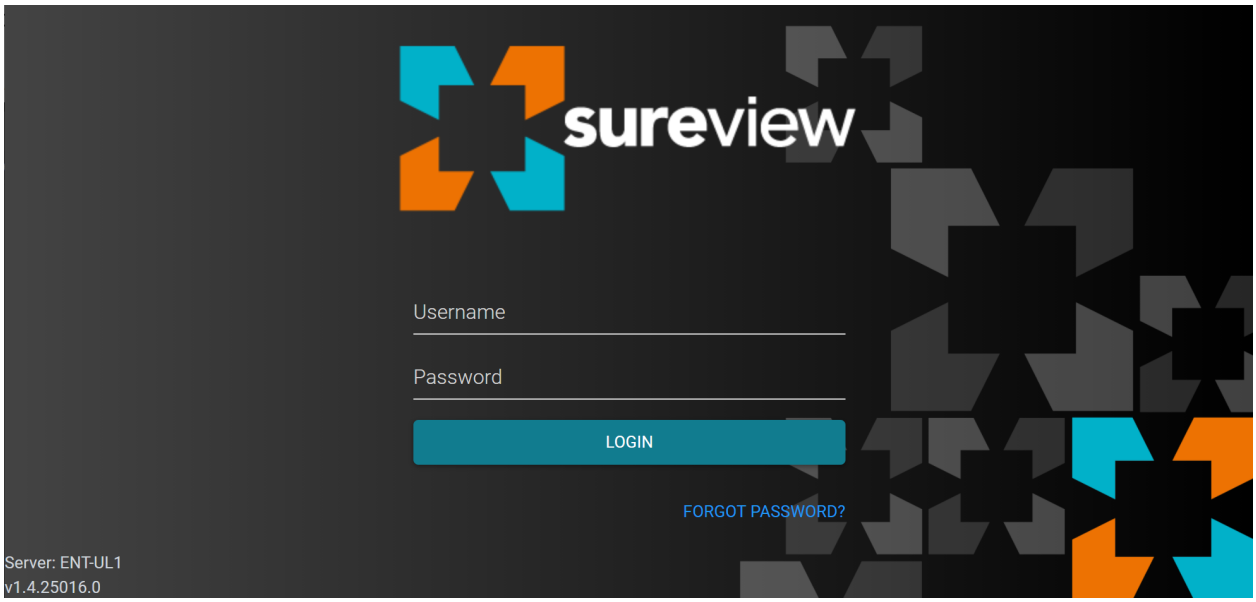


Software Version

Versions covered by certification: v1.x.x.x
Tested version: 1.4.25016.0

The version is shown bottom-left of the Login screen and also in the menu when logged in.

Login screen with version:



System Configuration

Pre-Requisites

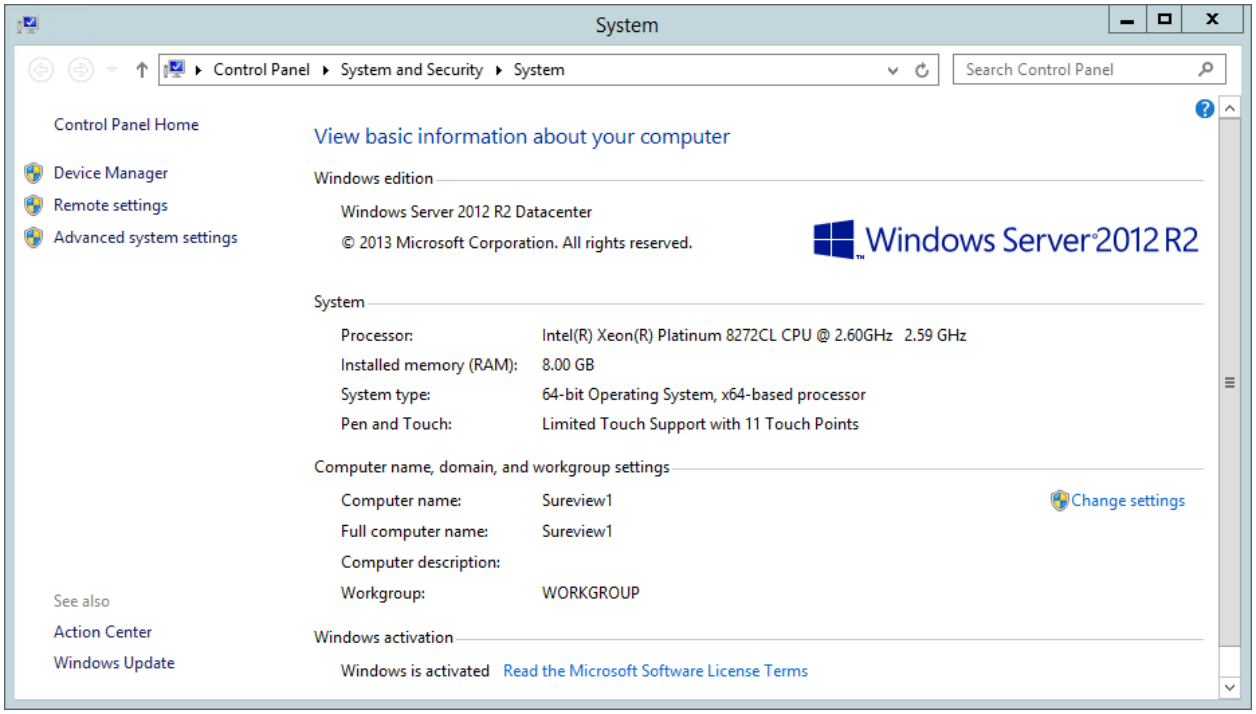
Operating System Installation

See Microsoft documentation for installing the Windows Server operating system on the three SureView servers.
Each server should be named appropriately such as "`SureViewWitness`", "`SureView1`", and "`SureView2`". Note: use numbers rather than words like "Primary" and "Backup" because the database automatically moves back and forth upon server failure so there is no "Primary" server.

On the two main SureView servers there must be the following components installed:

1. "IIS" role with:
    a. "ASP.NET v4"
2. ".NET Framework v4" feature with:
    a. "HTTP Activation" of "WCF Services"
3. .NET Core 2.1 Hosting Bundle installed (note: must be installed after IIS and an "iisreset" must be performed afterwards to apply the changes)
4. "Network Load Balancing" feature

Windows version information:



Network Configuration

Across the 3 servers there will be a total of 5 network interfaces: one for the Witness and two in each main server (one for normal LAN access to the server and one for NLB).

Each of the interfaces must be set with a static IP address so they do not change. For example:

- LAN interface on witness = 192.168.2.60
- LAN interface on server 1 = 192.168.2.61
- LAN interface on server 2 = 192.168.2.62
- NLB interface on server 1 = 192.168.2.71
- NLB interface on server 2 = 192.168.2.72

The “hosts” file (C:\Windows\System32\drivers\etc\hosts) on all 3 servers must be configured with short and fully qualified name entries for all of the LAN interfaces so that external DNS is not a point of failure for name resolution. For example the entries on one server:

- `192.168.2.60    SureViewW`
- `192.168.2.60    SureViewW.mydomain.local`
- `192.168.2.61    SureView1`
- `192.168.2.61    SureView1.mydomain.local`
- `192.168.2.62    SureView2`
- `192.168.2.62    SureView2.mydomain.local`

Network Load Balancing must then be set up on the NLB interfaces of the two main SureView servers to give a sixth IP address, for example 192.168.2.70, which is “shared” between the two, sending data to either (if they are both online) or just the online one (if one is offline).
See Microsoft documentation for configuring Network Load Balancing with the overview of the steps being:

1. Create a new cluster in the Network Load Balancing Manager
    a. Add one server as the first host, choosing the NLB interface
    b. Provide the shared “cluster” IP address that will be used
2. Add the other server to the cluster, choosing the NLB interface
3. Test by:
    a. Telnet from the witness to port 80/443 on the shared IP address (port 80/443 being used by IIS installed with the OS)
    b. Shutdown one server and telnet again.
    c. Restart the server and shut the other one down and telnet again.

The SureView web clients connect to the shared NLB IP address so they always have a connection in the event of a server failure.
Depending on the Receiver model it may connect to the shared NLB address, each server individually, or be connected to by the SureView servers (refer to the “Receivers” section)

Hosts file:

hosts - Notepad

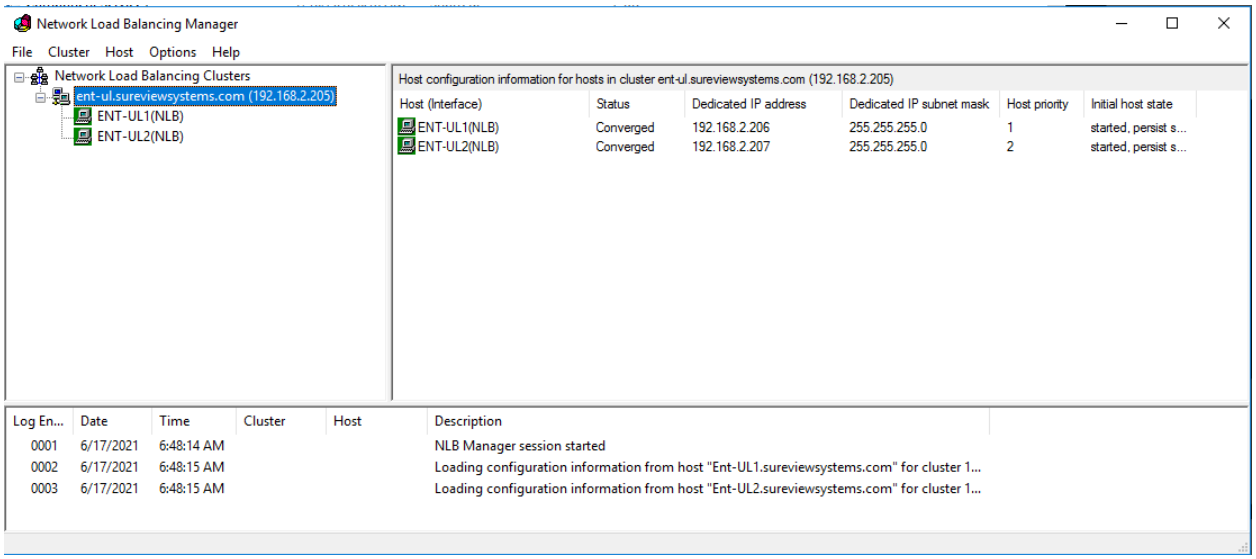
File Edit Format View Help

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
192.168.2.60    SureViewW
192.168.2.60    SureViewW.mydomain.local
192.168.2.61    SureView1
192.168.2.61    SureView1.mydomain.local
192.168.2.62    SureView2
192.168.2.62    SureView2.mydomain.local
```

Ln 27, Col 38 | 100% | Windows (CRLF) | UTF-8

Network Load Balancing setup:



SQL Server Installation

As per the minimum specifications, Microsoft SQL Server Standard edition or higher must be installed on the two main SureView servers and the Witness can use the free Express edition. See Microsoft installation documents for installing SQL Server.

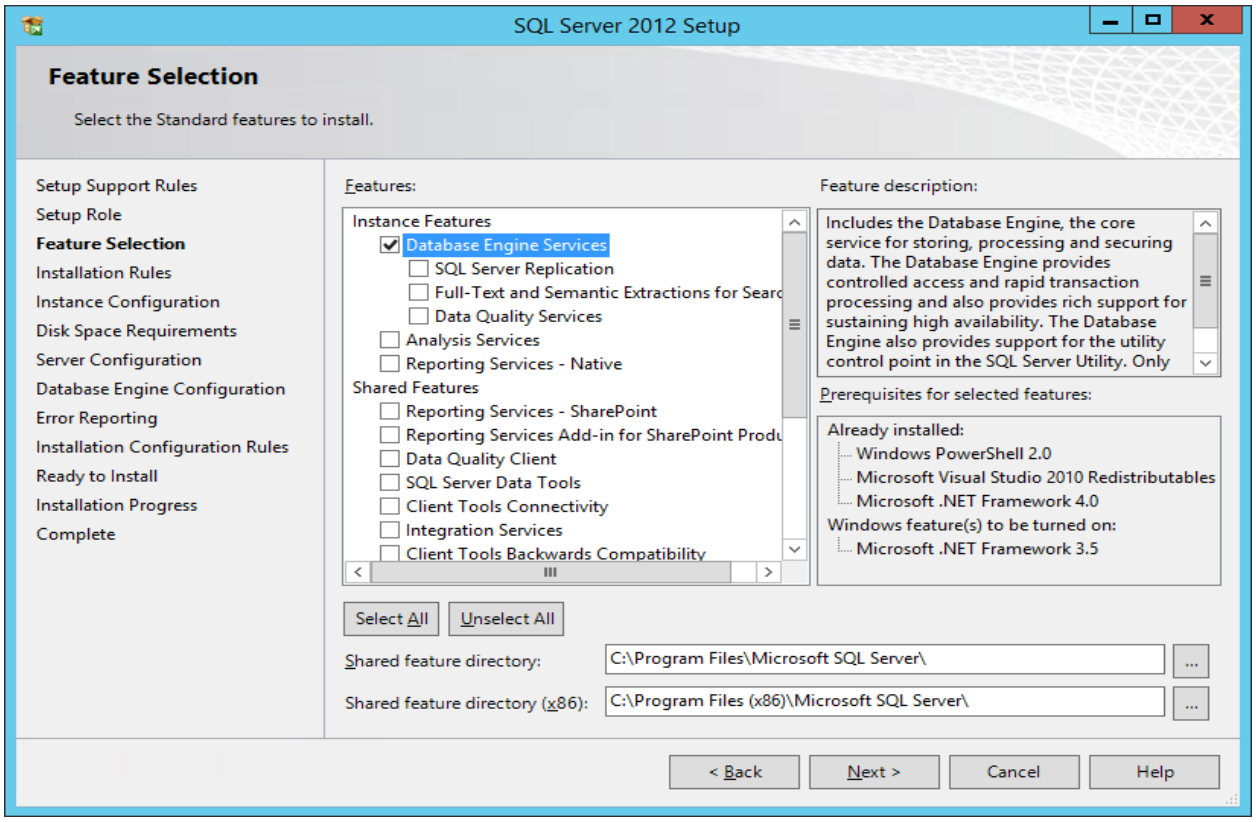
Note it must have at least the following components installed:

- “Database Engine Services”
- “Management Tools” (note this is now provided as a separate download by Microsoft)

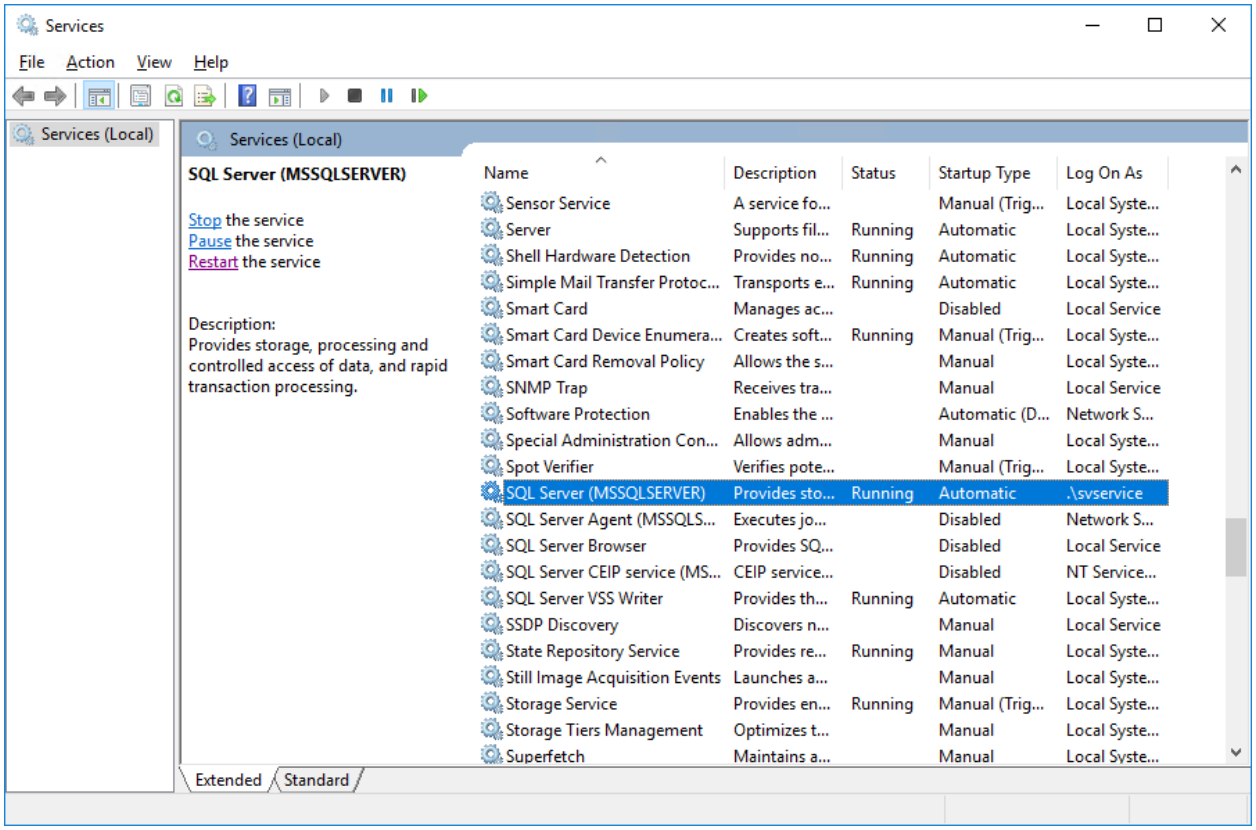
Either during or after installation, the “SQL Server” (database engine) service must be set to run as the same user account on all three servers in order for Mirroring to work. Ideally this should be a domain username but if the servers are not joined to a domain then it can be a user that exists on all three servers with the same username and password (restart the service after changing the login).

After installation, the TCP protocol on port 1443 must be enabled using SQL Server Configuration Manager inside Computer Management as the servers will be connecting to each other over the network (restart the service after changing the setting).
This port 1433 and the port for mirroring 5022 must also be allowed in the firewall from each server to each server. Ports should be locked down using the firewall scope to only accept connections from the other Sureview Servers.

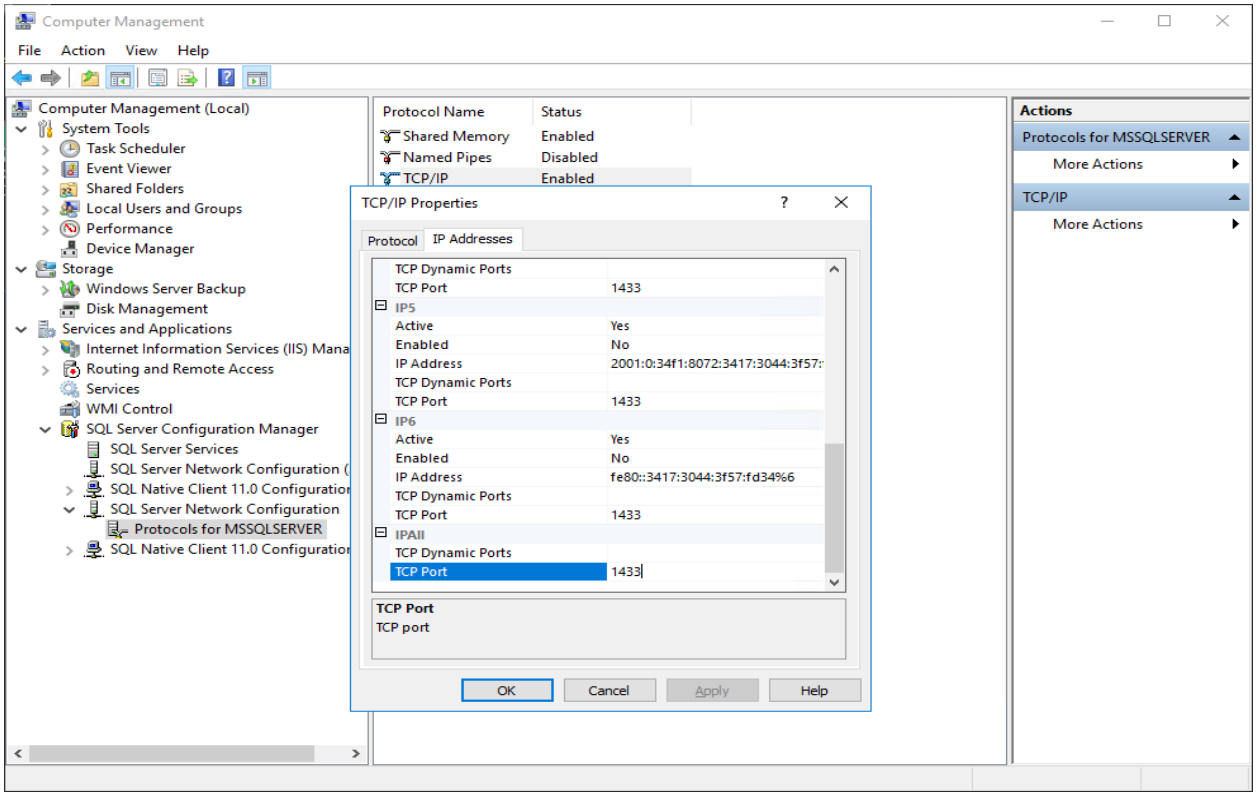
SQL Server feature installation:



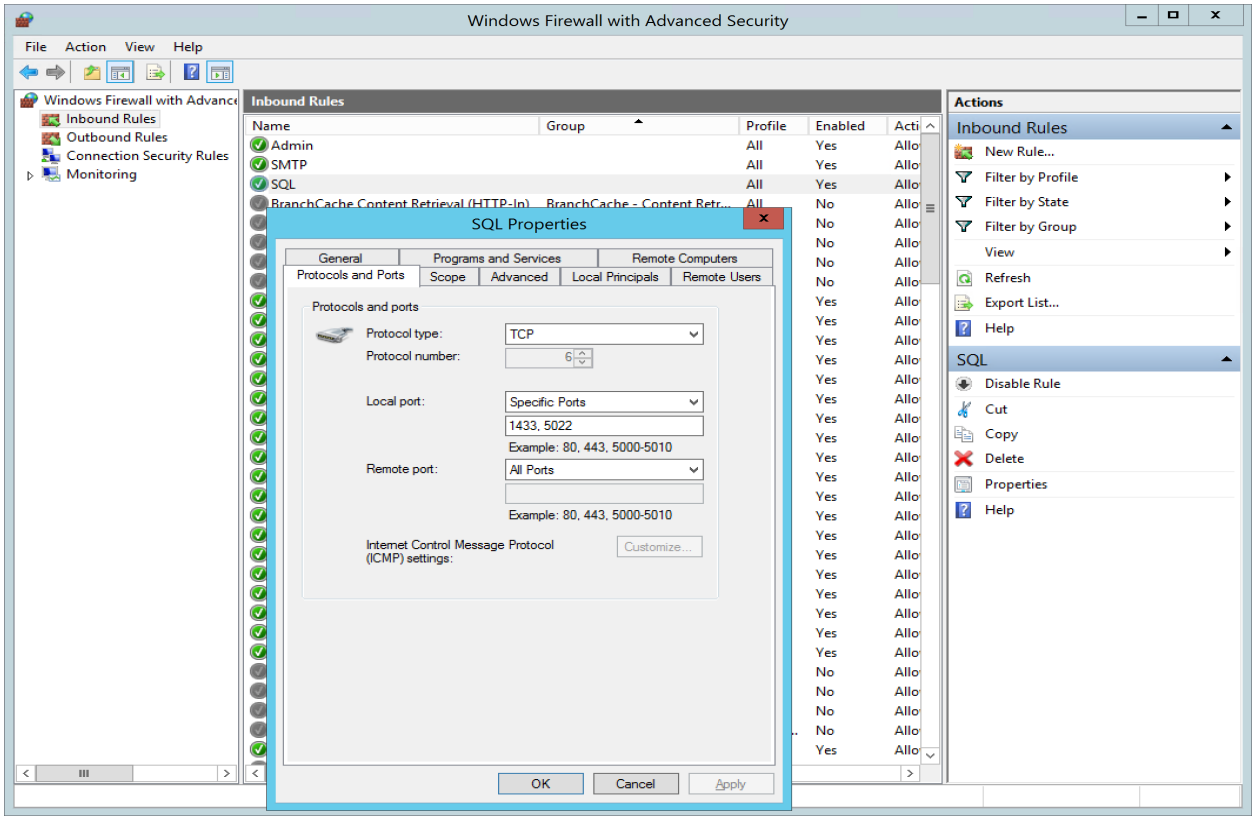
SQL Server service account same on all servers:



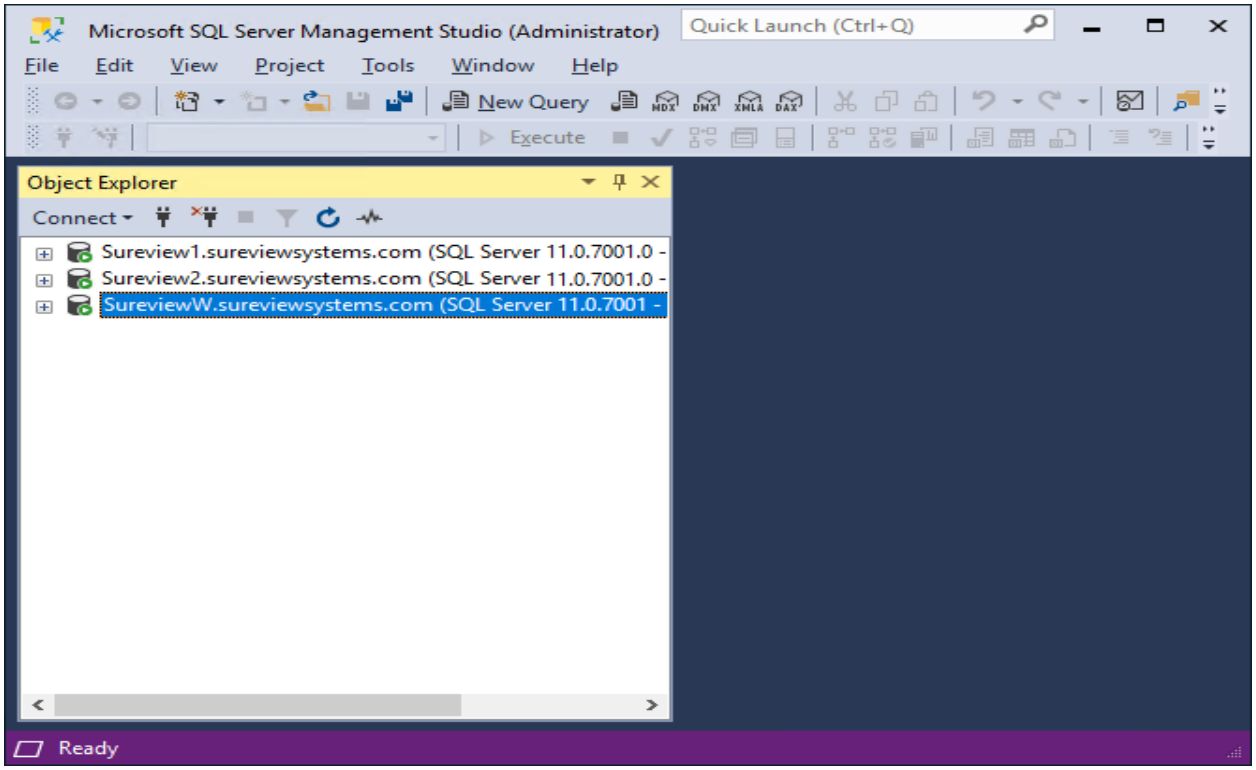
SQL Configuration to enable TCP on port 1433:



SQL Ports allowed in Firewall:



SQL Version information:



Software Installation

Use the SureView installer obtained from SureView to install at least the following packages (note: provide the details of both servers for the database connection, using the current server first and then the other server second):

On the 2x SureView servers:

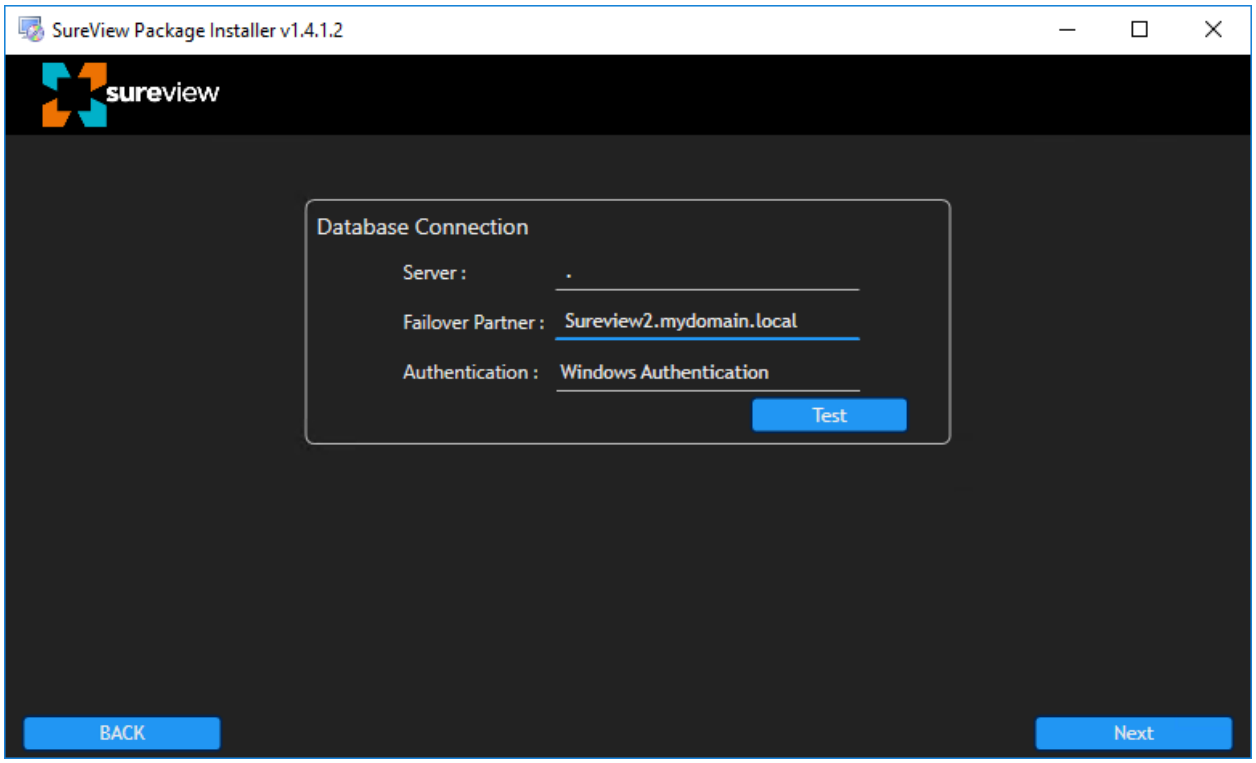
- SureView-DB (Database)
- SureView-DS (Data Service)
- SureView-UI (UI)
- Insight UL Reports
- Scheduler
- Watchdog
- Admin
- SMTP Receiver
- V1 components
    - Cloud Web
    - Data Service
- Optional integrations depending on receivers used:
    - Bosch D6600 Receiver
    - DMP Receiver
    - Surgard Receiver

On the 1x SureView witness:

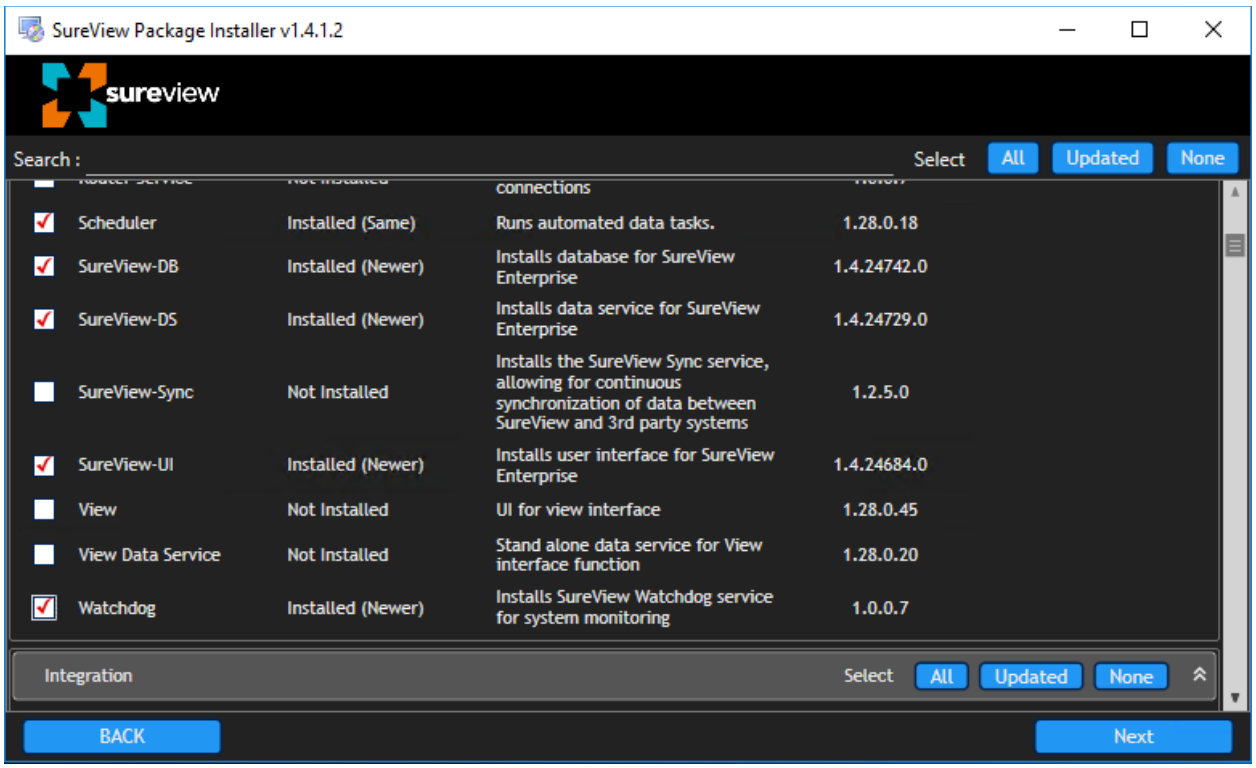
- Admin

Note: the video and non-Receiver integration components of SureView are not covered by UL and may be installed on these servers or separated out onto other servers too.

Installer database connection (using localhost and the other server):



Installer component packages:



Post-Install

Mirroring Configuration

The SureView database must be mirrored using SQL Management Studio to give you a “Principal” and “Mirror” being monitored by the “Witness” which monitors the state of the current Principal and in the event of a failure perform an “automatic failover” causing the current Mirror to become the Principal.

See Microsoft documentation for performing database mirroring, with the overview of the steps being:

1. On server 1:
    a. Set the database to use the “Full” recovery model
    b. Backup the database and transaction log
    c. Copy the backup file to server 2
2. On server 2:
    a. Restore the database and transaction log from the backup using the “With No Recovery” setting (so it is not a live database)
3. On server 1:
    a. Run the “Mirror” task and “Configure Security” to configure the endpoints of all three servers on port 5022
    b. Start mirroring (note: fully qualified domain names must be used)
4. Test:
    a. Stop the SQL service on server 1 to ensure that it automatically fails over to server 2
    b. Then repeat stopping the SQL service on server 2 to ensure it fails back to server 1

Manual Failover

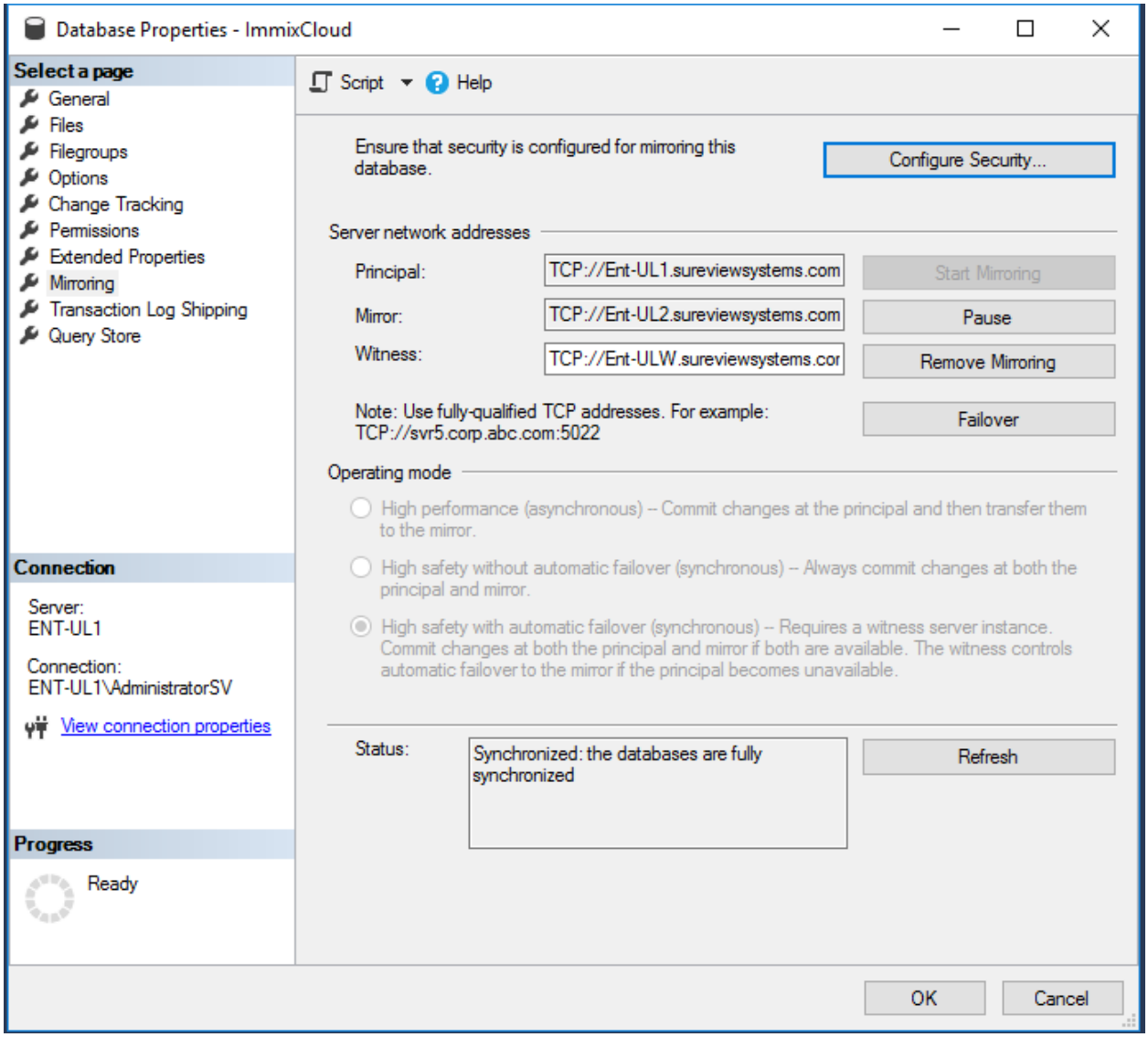
A manual failover can be performed to switch which server is the “Principal” in order to perform maintenance. This may be done via SQL Management Studio using the “Failover” button in the Mirroring page. You may also simulate a harder failure by stopping the SQL Server service on the current principal or even shutting down the server or unplugging the network cables.

It is recommended that a manual failover be performed at least once a year in order to test the functionality of the redundant system.

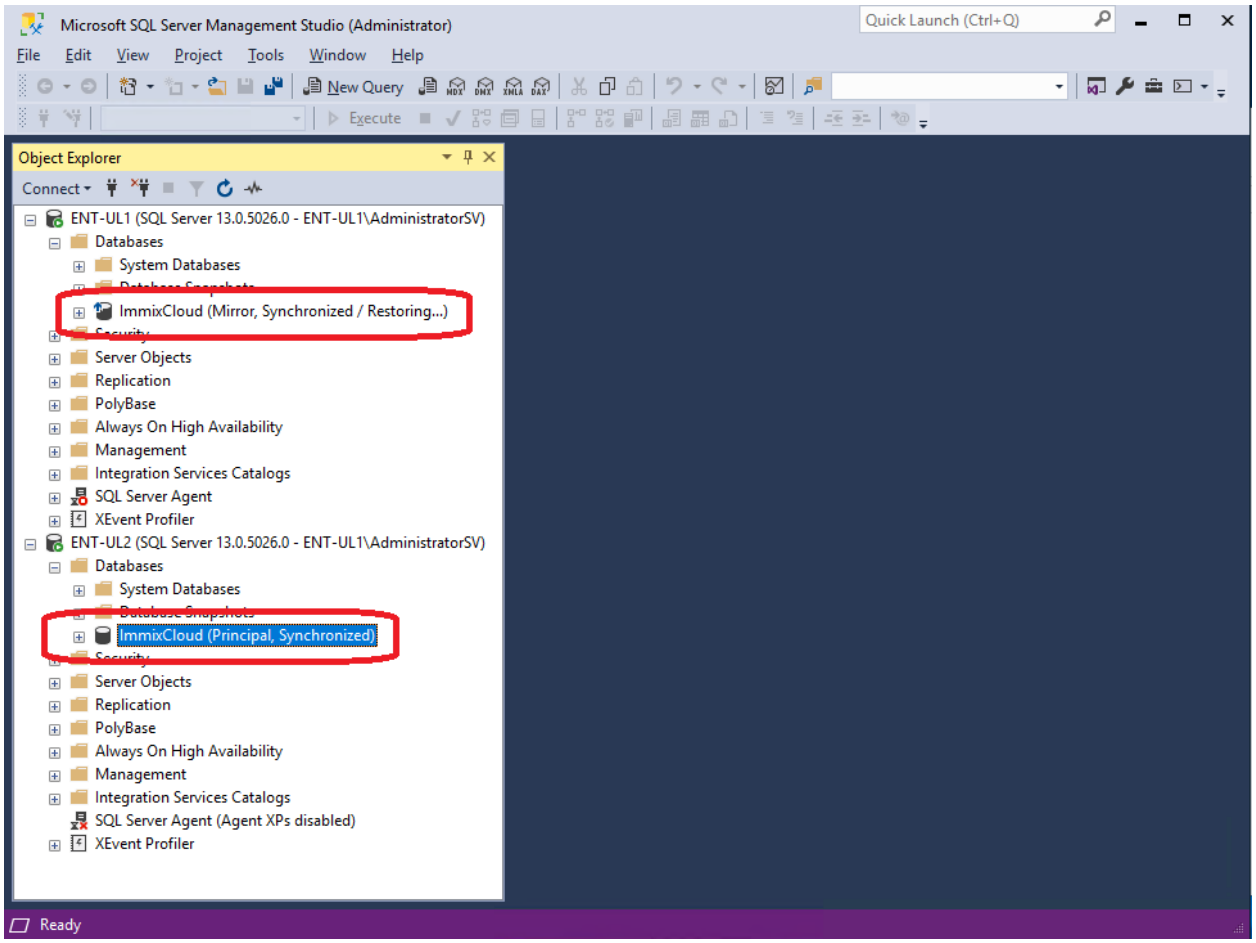
Forced Service

In a disaster scenario where multiple failures have occurred you can force the Mirror into service by running a SQL command (see Microsoft documentation for “Force Service in Database Mirroring”).

Mirroring using SQL mirroring interface:



Database mirrored:



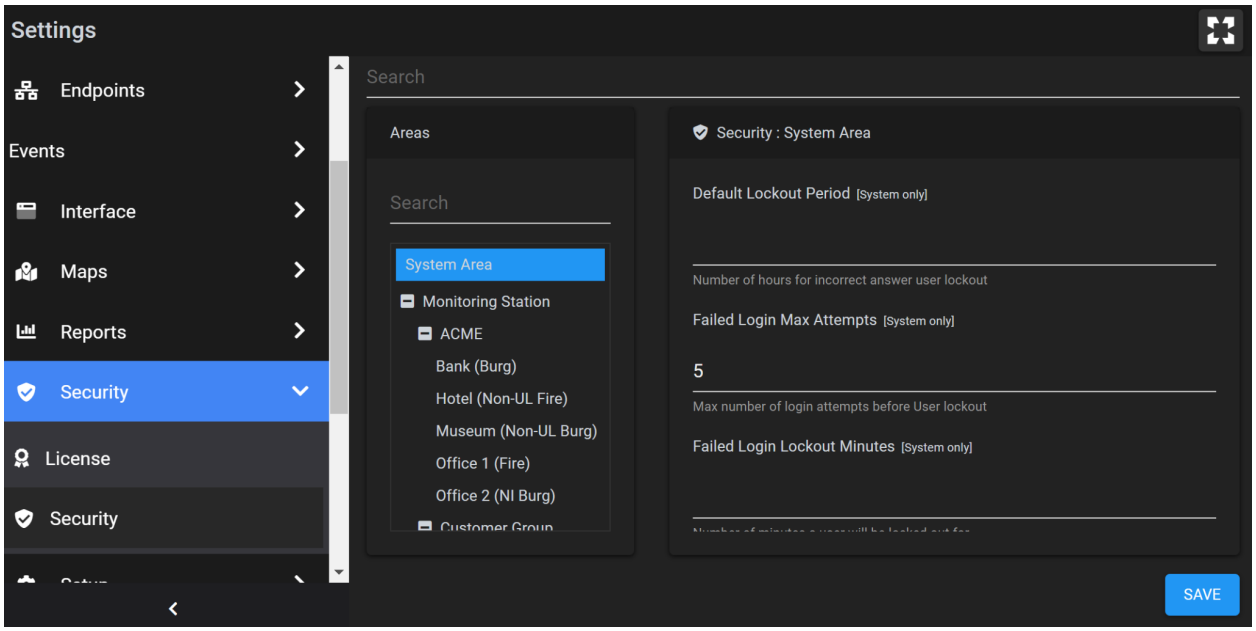
System Settings

The following System Settings must be configured by the system administrator in the “System Settings” screen in order to be UL 1981 compliant (refer to the sections below for instructions on logging into SureView):

- Alarms -> Admin
  - Warn the last user logging out = enabled
- Alarms -> Alarms
  - Alarm priority grouping (separate by priority) = 1000
  - Alarm age warning = 90s
  - Suppress flashing on new alarm = disabled
  - Suppress audio on new alarm = disabled
- Security -> Security
  - Number of days before password change = 90 days
  - Time period for incorrect login counting = 10 mins
  - Enforce password complexity = enabled
  - Prohibit the use of last passwords = 6 last
  - Max consecutive username characters allowed in password = 3 characters
  - Min username length = 6 characters
  - Disable password complexity for new users = disabled

    - Inactivity time for alarm screen = 00:15 (15 mins)
    - Inactivity time for session = 00:15 (15 mins)
- Endpoints -> Email
    - SMTP server details of your company SMTP server to enable SureView to send emails (note: the built-in Windows SMTP service may be used if you do not have a company one available - refer to Microsoft documentation for instructions on configuring this)
- System -> Health Check
    - CPU, RAM, HDD, and Network usage alert thresholds set to 80% use / 20% free as described in the “Performance Monitoring” section

System settings:



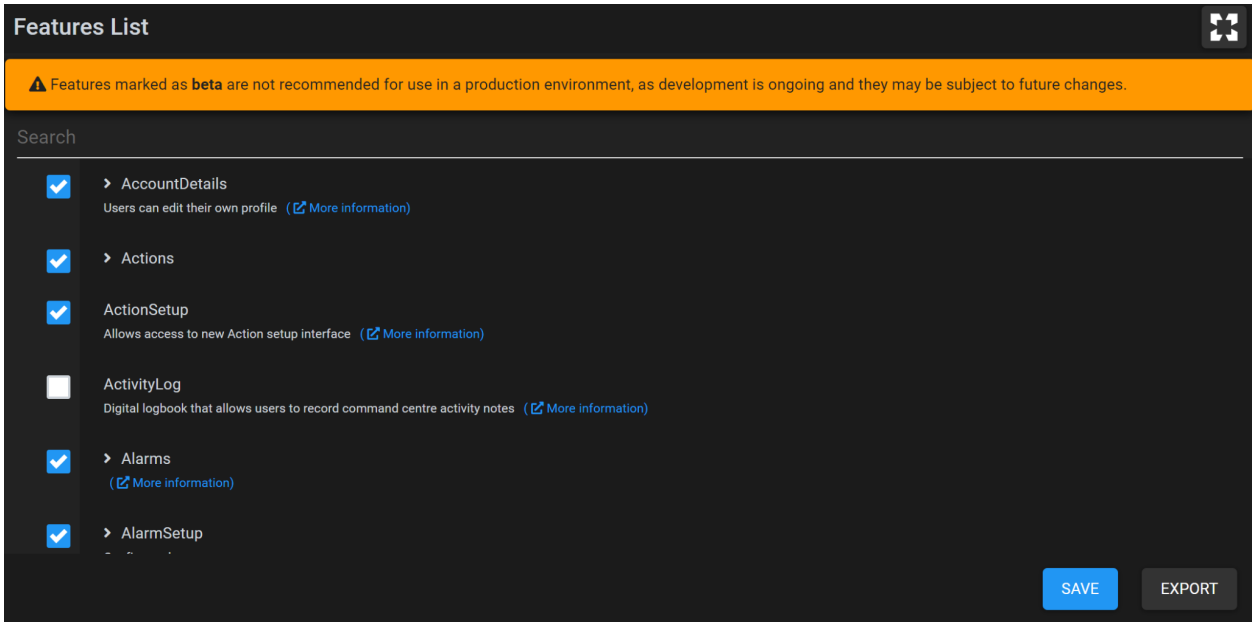
Features

The following Features must be enabled by the system administrator in the “Feature Setup” screen in order to be UL 1981 compliant (refer to the sections below for instructions on logging into SureView):

- Actions
    - Call Contacts
- Alarms
    - Alarm points
        - Audit Mode
        - On Test
        - Masking
    - Dispatch
        - Multi-Dispatch
    - Event Queue

        - In Processing
        - Parked
        - System Events
    - Event Search
        - Download Event
    - Missed Target Response Time Icon
    - Site Monitor
        - Alarm Queue Status
        - Restored Icon
        - Park
        - Site Details
        - SitRep
    - Warn Last Operator
- Area Notes
- Areas
    - UL Area Settings
- Contacts
- Event Category Setup
- Insights
- Settings
- User Groups
- Users

Features:



Performance Monitoring

In order to meet UL 1981 all three SureView servers must be set to continuously log the following performance counters once a minute using the Performance Monitor logging and reporting tool built in to Windows (refer to Microsoft documentation for setting this up):

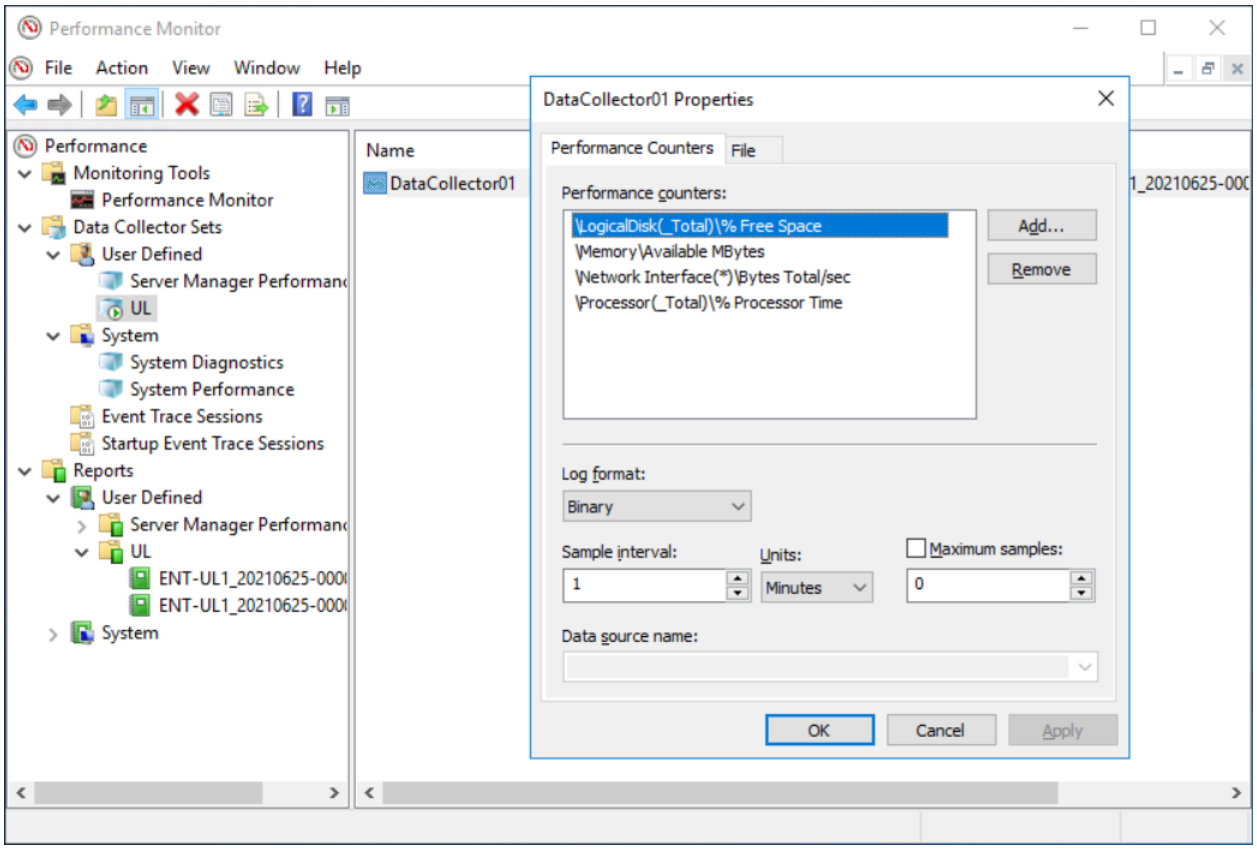
1. CPU use (Counter: Processor -> % Processor Time -> _Total)
2. RAM use (Counter: Memory -> Available M Bytes)
3. Disk use (Counter: Logical Disk -> % Free Space -> _Total)
4. Network use (Counter: Network Adapter -> Bytes Total/sec -> <All Instances>)

NOTE: these logs will grow continuously so it is recommended to implement a regular maintenance schedule (for example once a year) to restart the logging and move the old data off the server to an archive so the hard drive does not fill up.

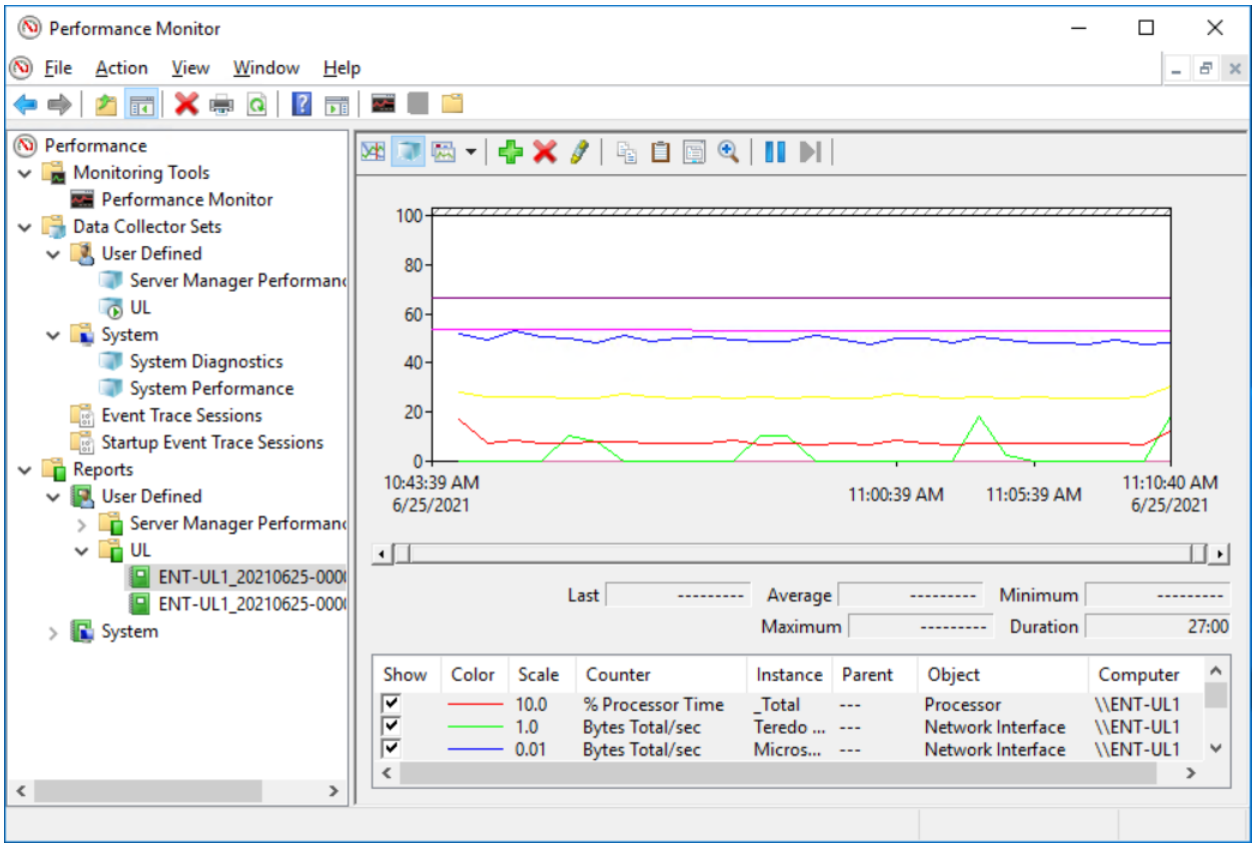
Additionally, the SureView system settings must be set to send alerts at the following maximum values:

1. CPU use: 80%
2. RAM use: 80%
3. Drive free: 20%
4. Network free: 20%

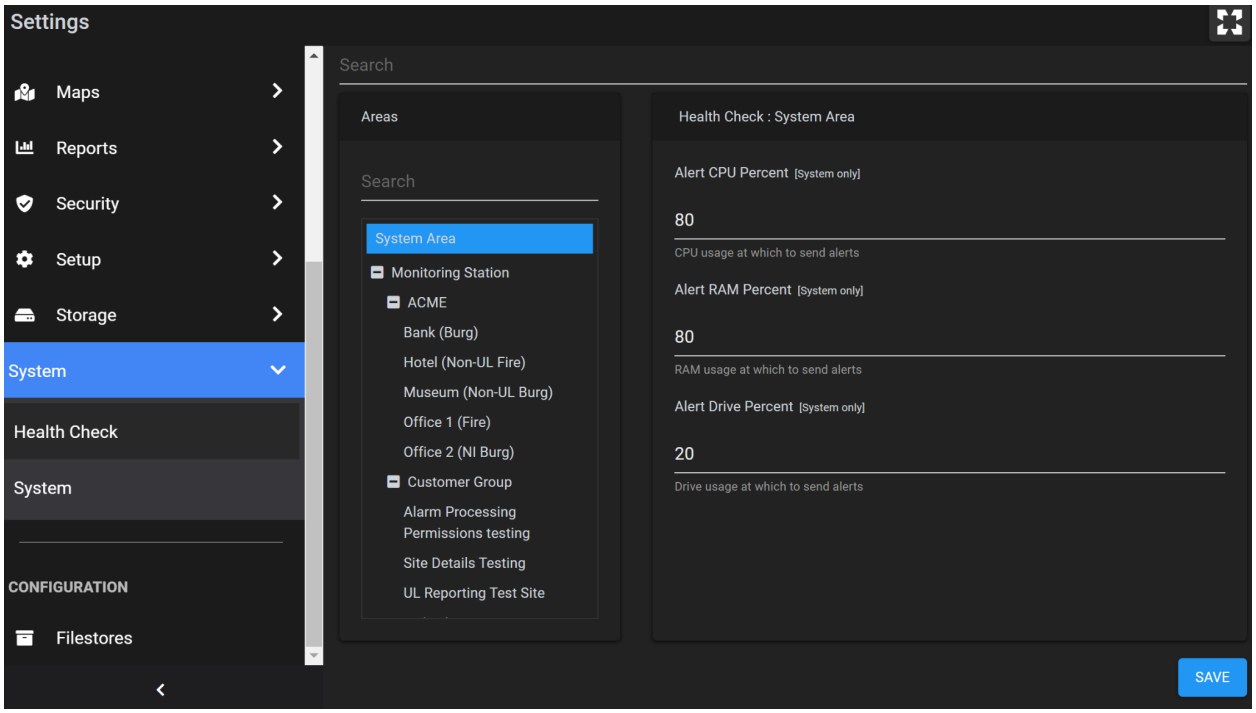
Windows Performance Monitor - data collector setup:



Windows Performance Monitor - data collector report:



SureView performance alert settings:



Hardware Monitoring

Whether using physical or virtual SureView servers, hardware failures must be sent into

SureView as alarms in order to meet UL 1981.

This can be achieved by having the SNMP alerts sent from the servers to SureView as SMTP alarms by the following process:

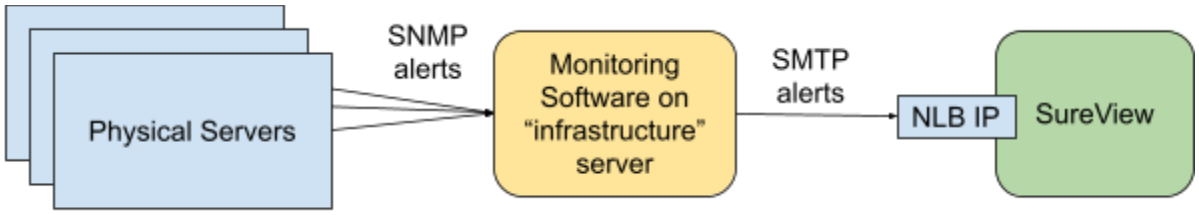
1. Add an “Infrastructure” site to SureView along with a dummy device to get an “S# email address” which when emails are sent to the SureView system with that address will come into that site as alarms.
2. Set your server monitoring system to send an SMTP message to the SureView servers using the S# email address when any Warning and Critical severity messages are received from servers. This is dependent on your particular servers but examples are:
    a. An out-of-band server management module built in to the servers (such as the “DRAC” for Dell servers) sending SMTP alerts on hardware failure
    b. Server monitoring software (such as Dell’s OpenManage or VMWare’s vCenter Server) running in your network on an “Infrastructure” server and monitoring the servers via SNMP, sending SMTP alerts on hardware failure.

Please refer to your hardware manufacturer’s documentation for setting this up and contact the SureView team with any questions.

Ideally all hardware issues should be reported, but the following are required in order to be compliant:

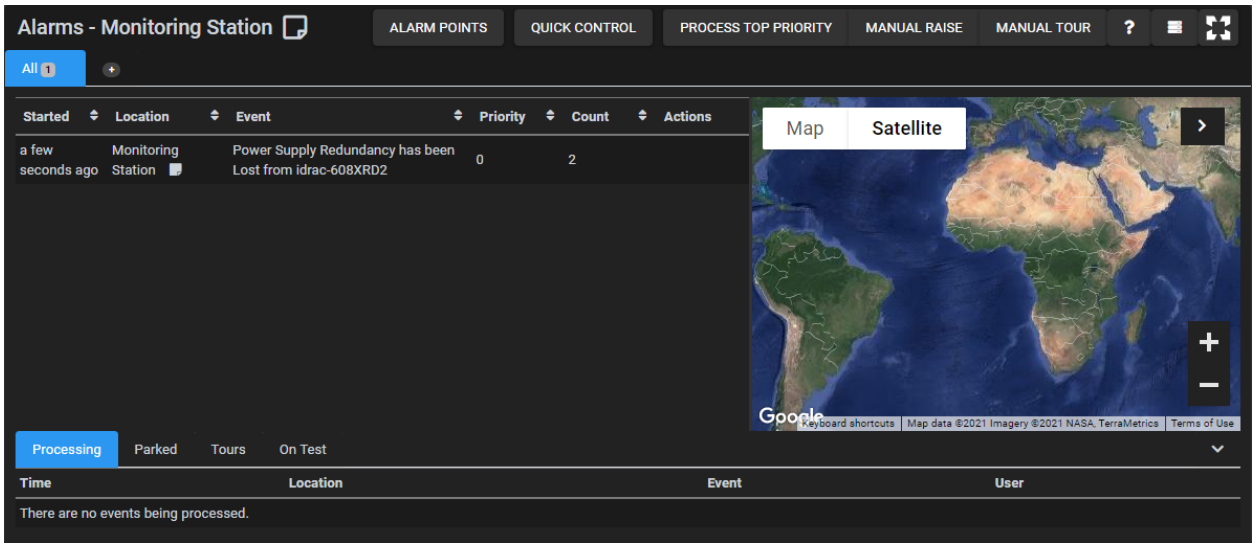
1. Power supply failure / loss of redundancy
2. Hard drive failure / loss of redundancy
3. Network interface failure / loss of connection
4. Cooling fan failure / loss of redundancy

SNMP hardware alerts sent to SureView as SMTP alerts via server monitoring software:



*1 i.e. Dell OpenManage or VMWare vCenter Server (note: may be a VM)

Example of hardware issue alarms (power supply redundancy lost):



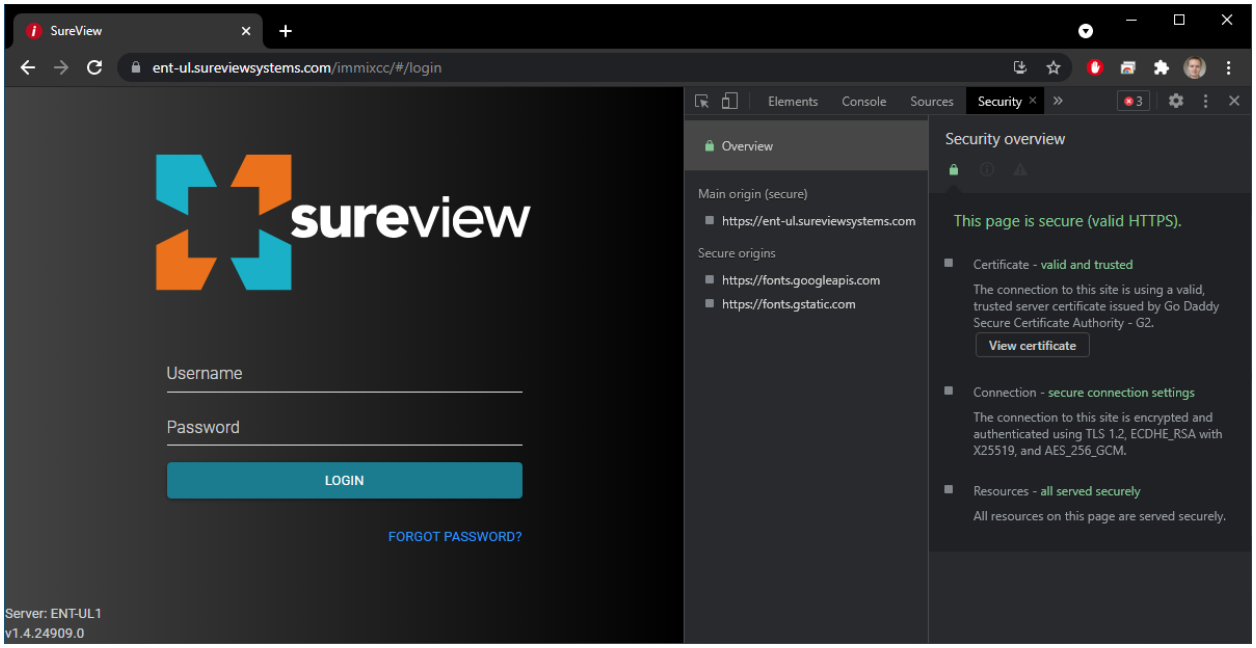
Remote Access

If the SureView system is to be exposed outside of the Central Station for remote access then the following additional steps must be taken in order to safely encrypt all data and meet UL 1981:

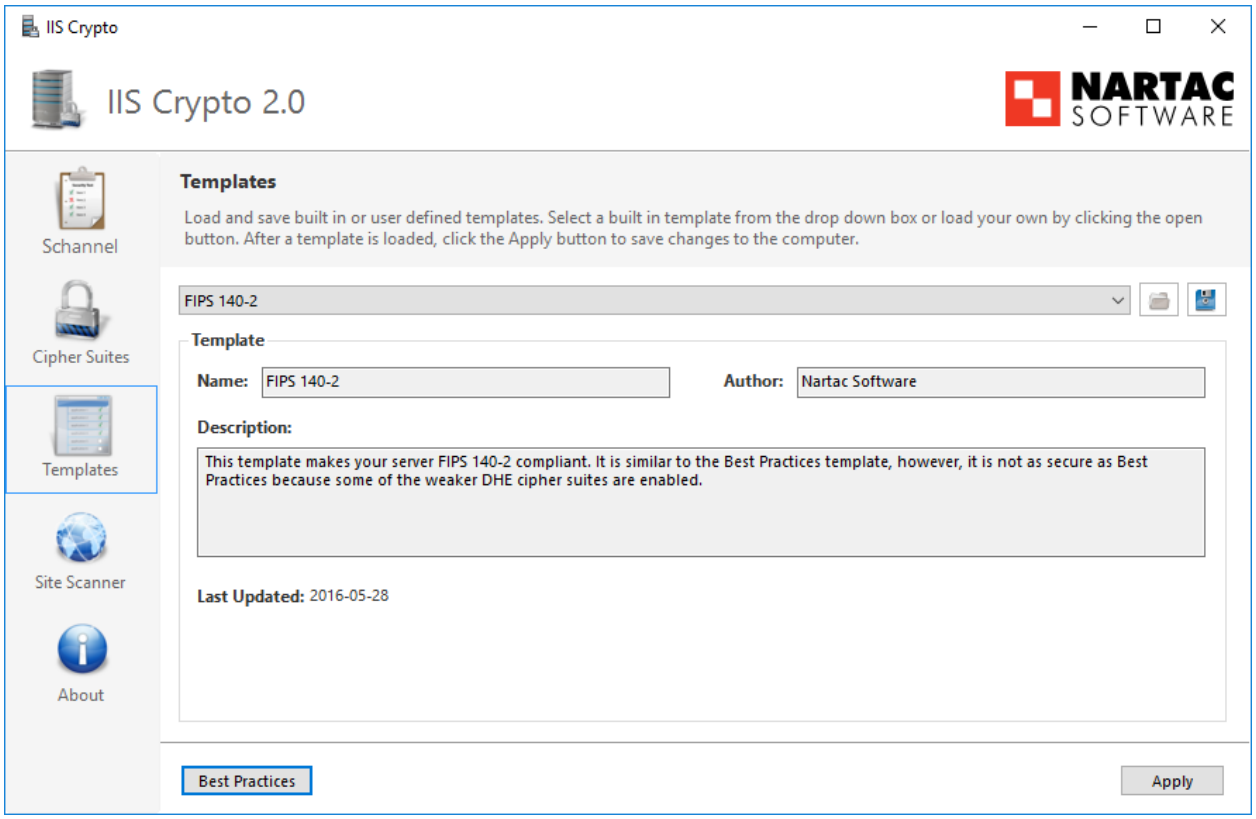
1. HTTPS must be used with a certificate
2. The SSL protocols on the servers must be configured to meet at least FIPS 140-2 compliance (using IIS Crypto).

Please contact the SureView team for assistance in setting this up on your SureView system.

SSL Certificate in use for external connections:



IIS Crypto changing SSL settings for FIPS 140-2 compliance:



Tertiary System

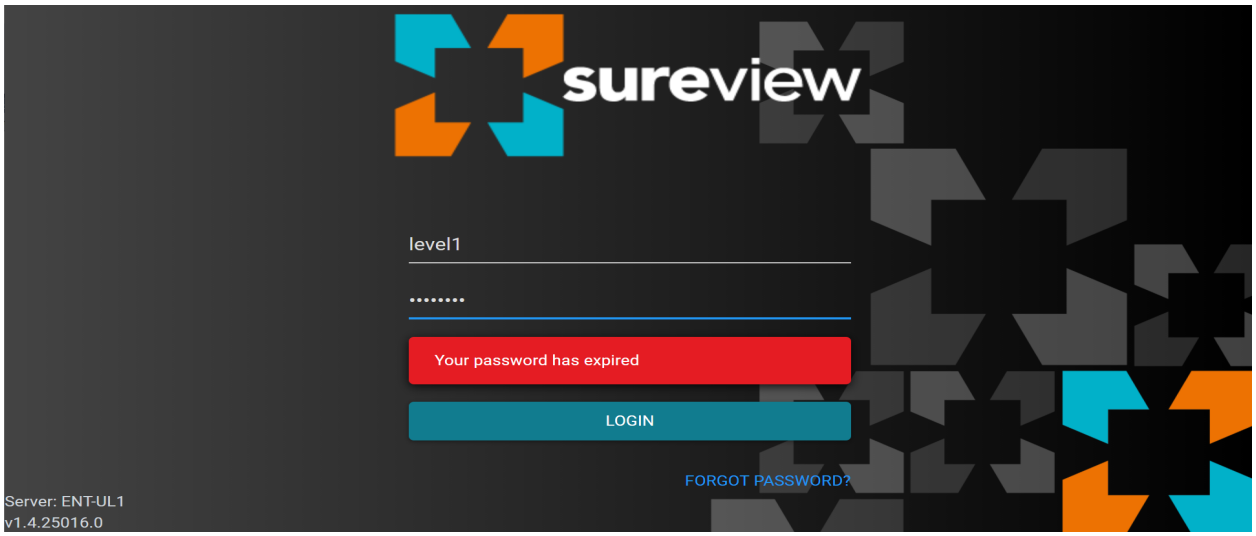
If using a Tertiary system (a completely separate SureView system for disaster recovery), the server must be of identical specifications to one of the SureView servers and must have a regular schedule set up to keep the Tertiary system's data up to date whereby the database from the main SureView system is backed up then copied and restored to the tertiary system using a combination of SQL Scheduled Jobs and Windows Scheduled Tasks (for example once a day). Please contact the SureView team for assistance in setting this up.

Logging in and out

Open the browser on your workstation and go to the URL for the Network Load Balancer (NLB) address.
A number of login-related features are provided to meet UL 1981 and are explained below.

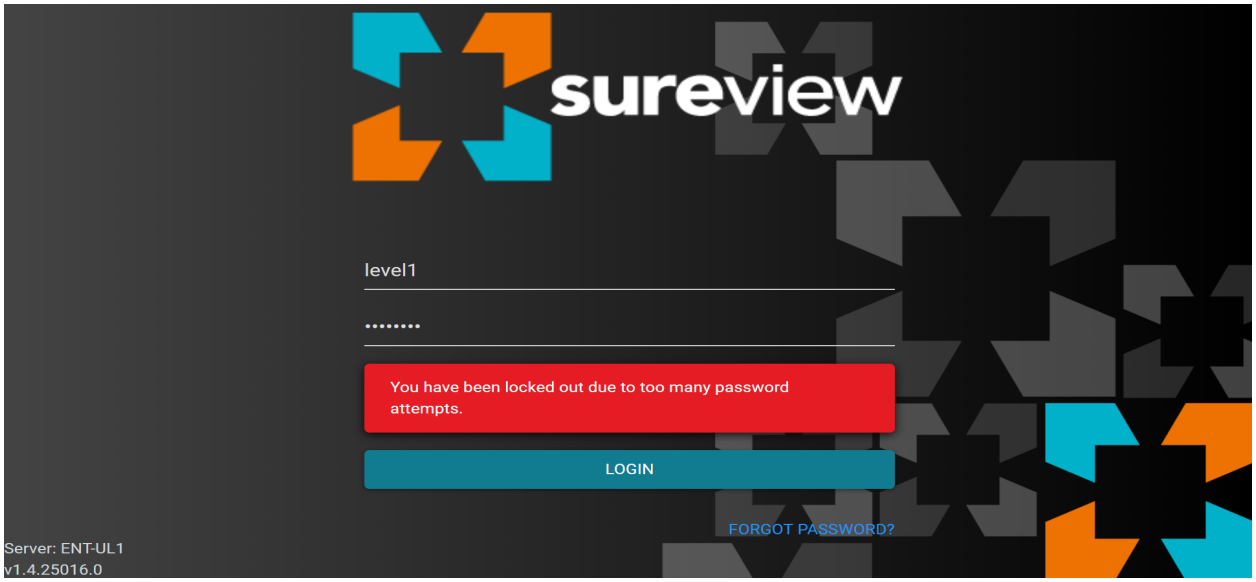
Password Expiry & Requirements

If your password expires you will be forced to change it to a new value that meets the complexity requirements (being a certain length, containing certain characters etc).



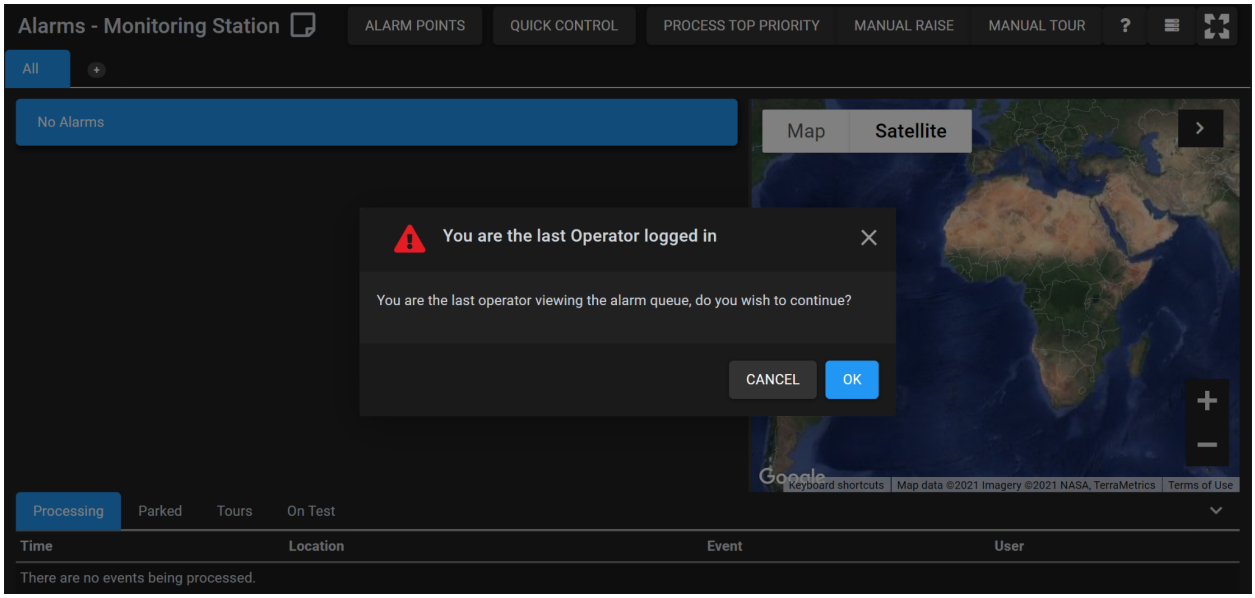
Failed Login Lockout

Too many invalid logins will cause your login to be locked - contact your system administrator to unlock your account.



Last User Logout

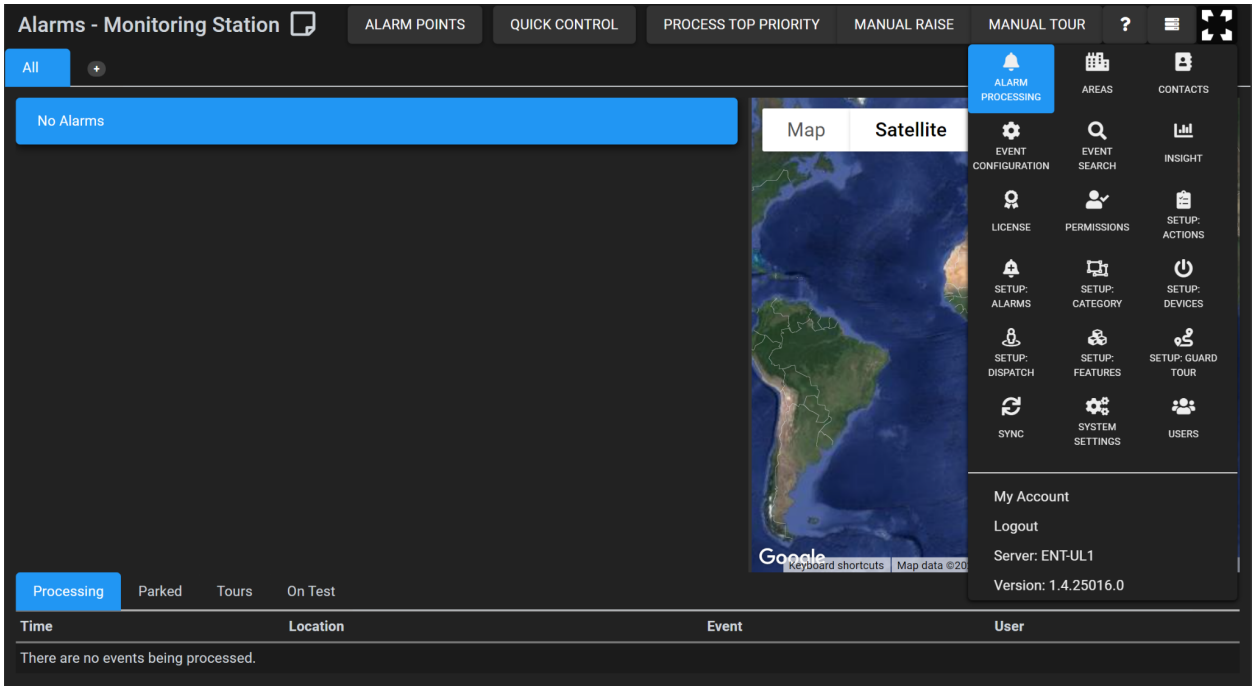
If the last user of the Alarm processing section attempts to log out, move to another section, or close the browser they are shown a warning message stating that you are the last operator and asking whether they wish to continue.



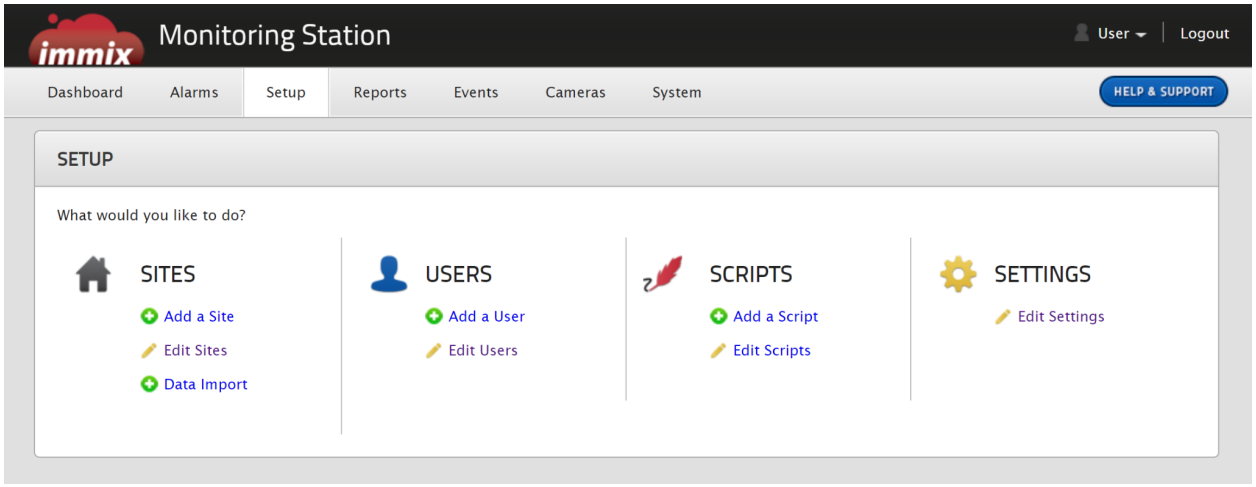
Software Configuration

Configuration is performed via the items available in the menu which is opened from the top-right button (note: some items are currently configured in the old “V1” setup interface which is noted where appropriate - these will be moved over in future)

Menu opened:



Old “V1” setup interface:



User Permissions

User permissions are set up in the “Permissions” menu item, with User Roles that are a group of

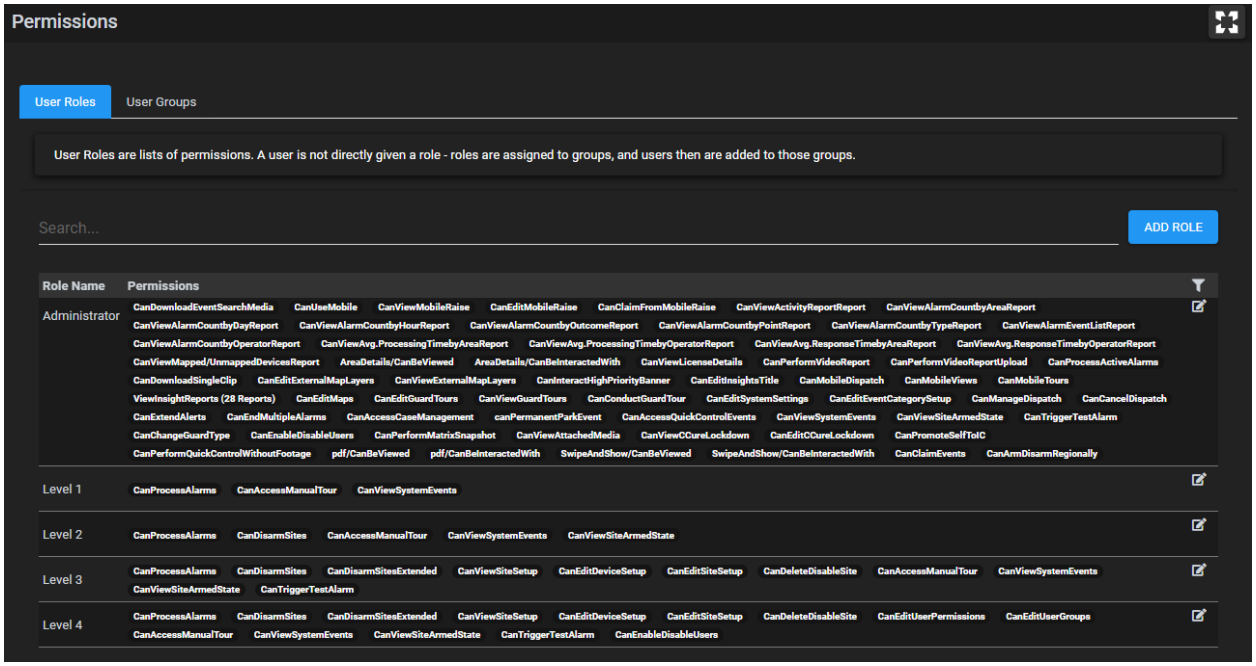
permissions and User Groups which apply those roles to the areas of the system for users.

User Permissions must fall into the following levels in accordance with UL 1981:

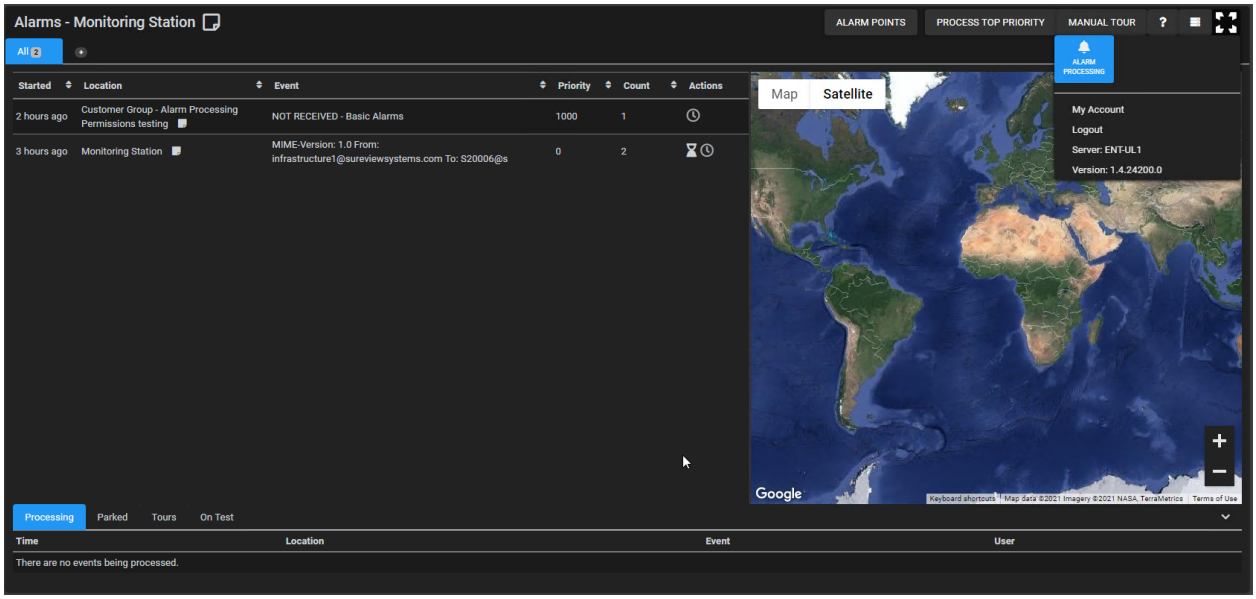
- Level 1: processing alarms and performing manual tours (*"CanProcessAlarms", "CanViewSystemEvents", "CanAccessManualTour"*)
- Level 2: level 1 plus the ability to disarm up to 24 hours (*"CanViewSiteArmedState", "CanDisarmSites"*)
- Level 3: level 2 plus the ability to disarm longer than 24 hours and edit sites (*"CanDisarmSitesExtended", "CanViewSiteSetup", "CanEditSiteSetup", "CanEditDeviceSetup", "CanTriggerTestAlarm", "CanDeleteDisableSite"*)
- Level 4: level 3 plus the ability to edit users (*"CanEditUsersPermissions", "CanEditUserGroups", "CanEnableDisableUsers"*)
- Level 5: change system settings (*"CanEditSettings", "CanEditSystemSettings"*)

NOTE: in accordance with UL 1981 external users outside of the Monitoring Center may only go as high as level 3 (must not be able to edit users or system settings)

User Roles:



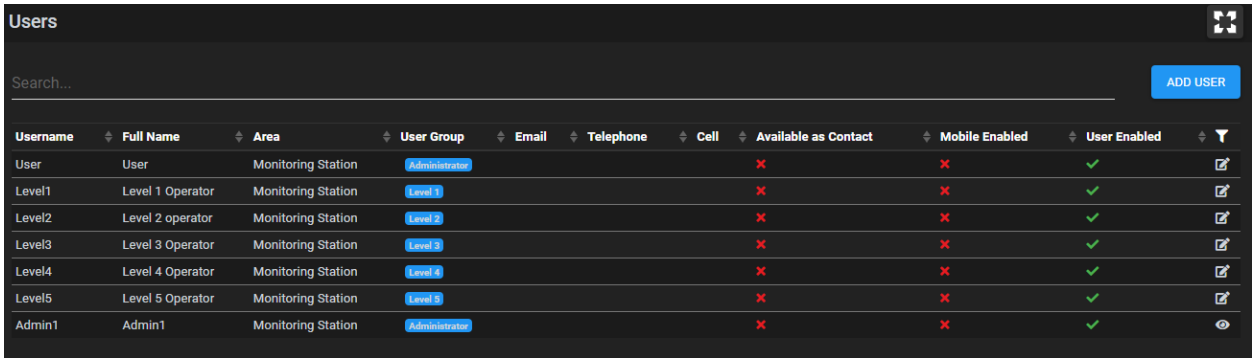
Example of a level user 1 logged in showing the menu items available to them:



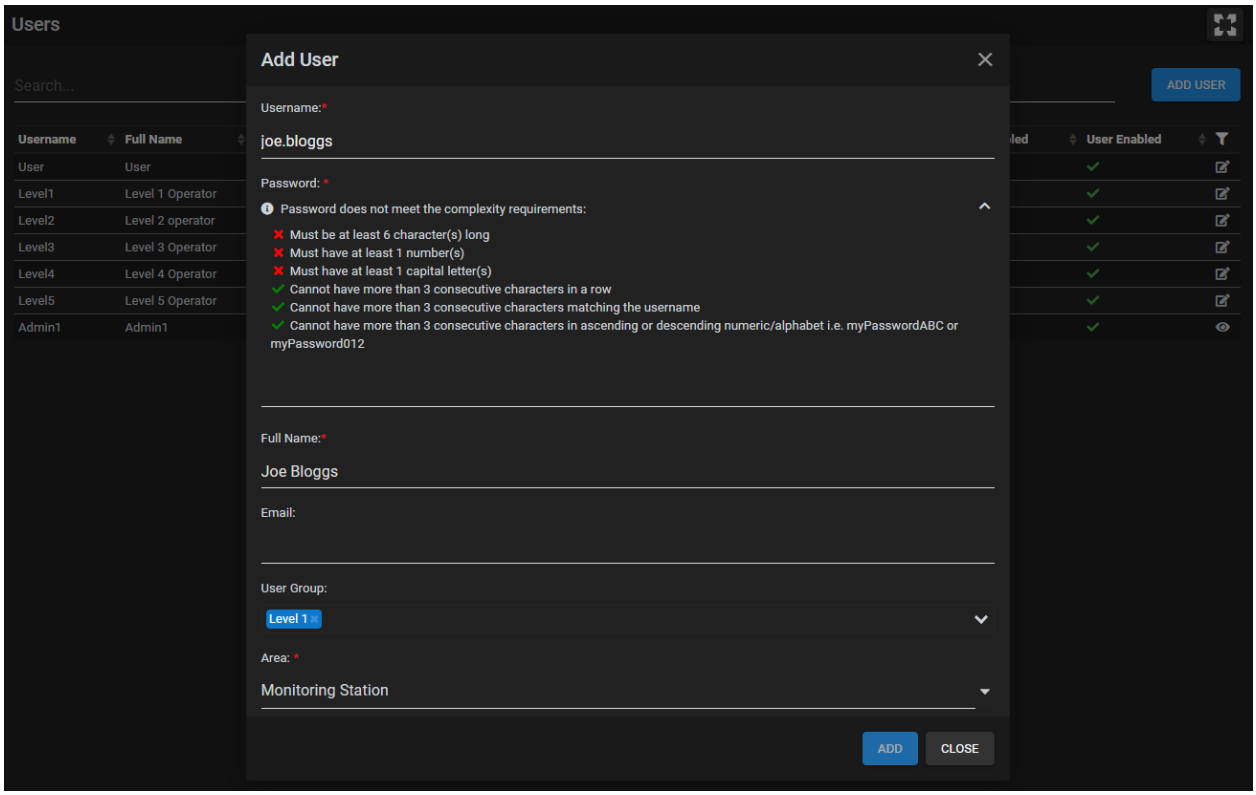
Users

Users of the SureView software are configured in the “Users” menu item and are assigned a username, password, and user group to allow them to log in and perform the actions you have permitted them to do - these might be for monitoring users or external customer users who you are providing access to see the event history of their sites.
Note: the username and password are subject to the complexity requirements mandated by UL 1981 and an error will be shown if they do not match.

Users:



Creating a user including the password complexity:



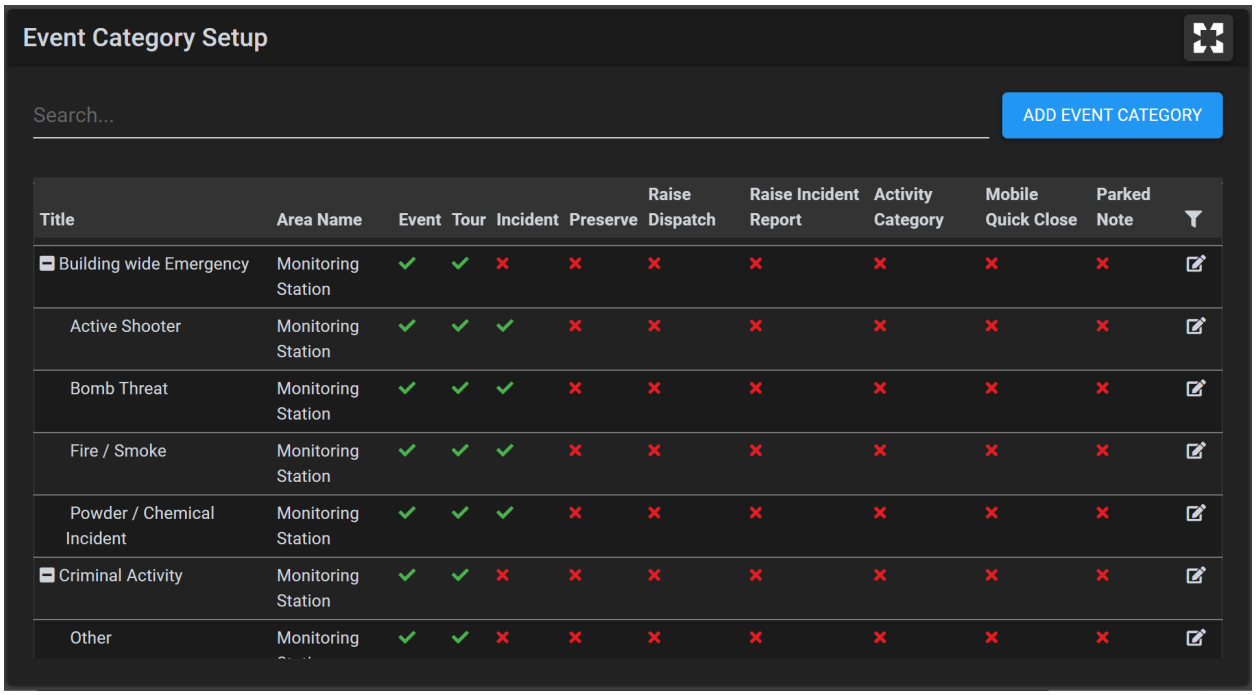
Event Outcomes

When closing an event an operator must provide an outcome (disposition) from a list of preconfigured choices and depending on the chosen outcome certain post-event actions can be taken such as the audit trail being emailed to users belonging to the site.
These are configured in the “Event Category Setup” screen, and while usually being configured at the global level they can also be configured at any level of the site tree to make them site or customer specific.

Ticking the “Incident” setting results in an email being sent to any contacts at the site or customer level that have the “receive incident emails” option ticked and an email address set (see the “Contacts” section below).

Ticking the “Preserve” setting results in the event being marked as preserved so it is never removed by housekeeping.

Event Outcomes:

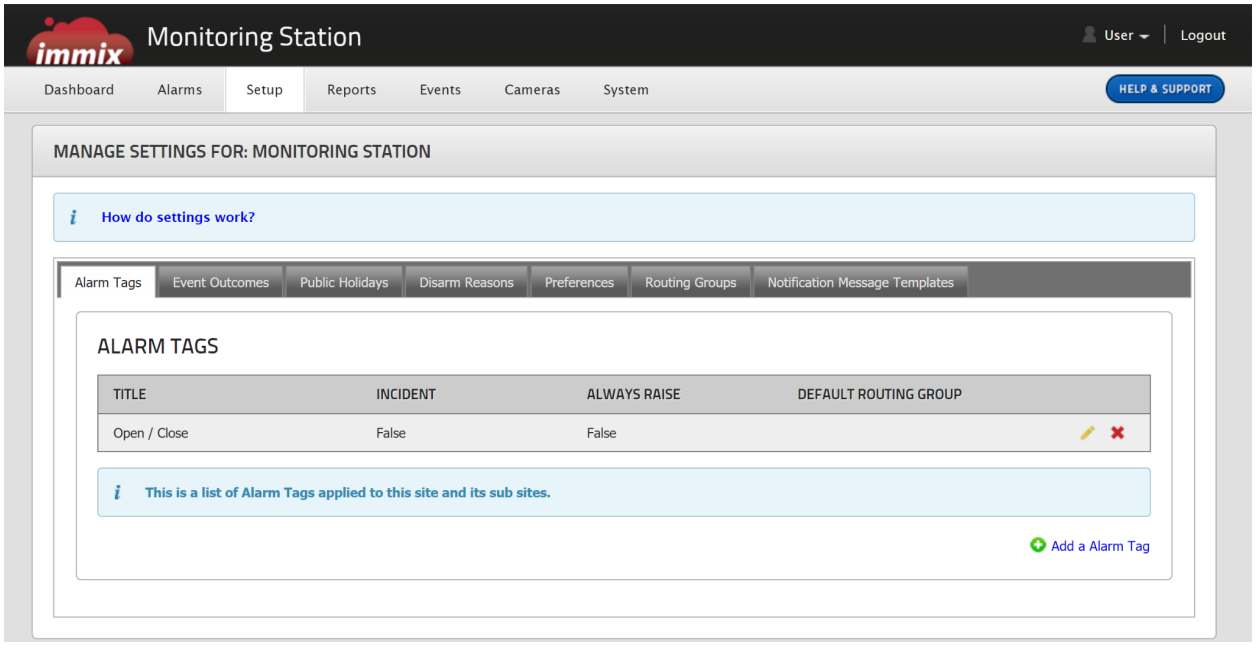


Alarm Tags

Alarm Tags are a way of providing additional classification to alarms and are currently added in the V1 setup interface by going to the Setup->Edit Settings screen.

UL 1981 requires the ability to report specifically on Open/Close alarms so a tag must be made for this and applied to the Open/Close alarms in each UL site (see alarm setup below)

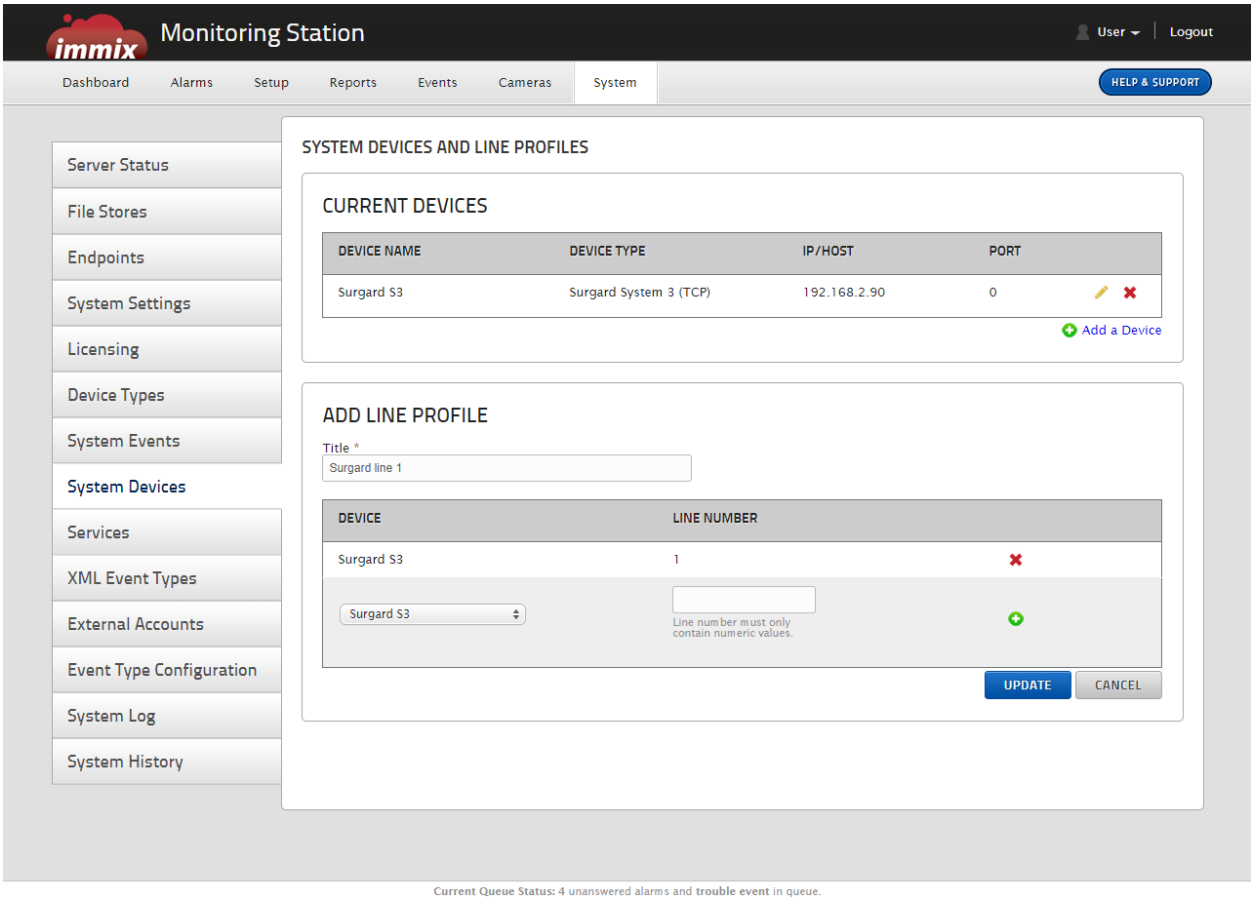
Alarm tags:



Receivers and Line Profiles

The Receivers you have are currently added in the V1 setup interface in the System->System Devices tab and are set with their type, connection details, and a line profile listing the lines that exist on the receiver.
Refer to the SureView support portal documentation for the particular integration for further instructions.

A Surgard System 3 receiver configured with a line profile:



Action Plans

Action Plans can be configured to define the set of steps an operator must take when processing different types of alarms instead of leaving them to manually perform actions and add the results to the audit trail.

The available steps include:

- Requesting information to be entered
- Contacting emergency services
- Contacting site call lists

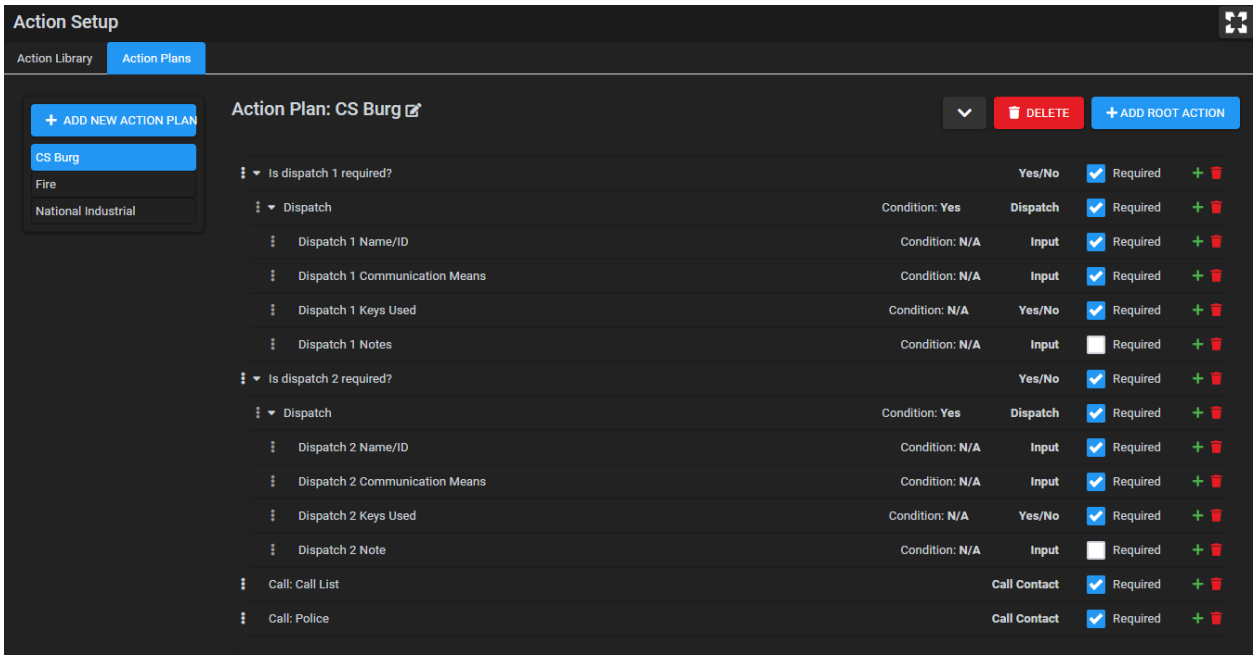
- Dispatching

These are configured in the Action Setup menu item and are created as follows:

1. Create a number of Actions in the Action Library
2. Create an Action Plan which uses

Note: setting an action as Required means it must be performed by operators before they can close the event (see the “Alarm Processing” section below).

An action plan involving dispatching 2 guards (collecting information during the process), contacting the site call list, and the police:



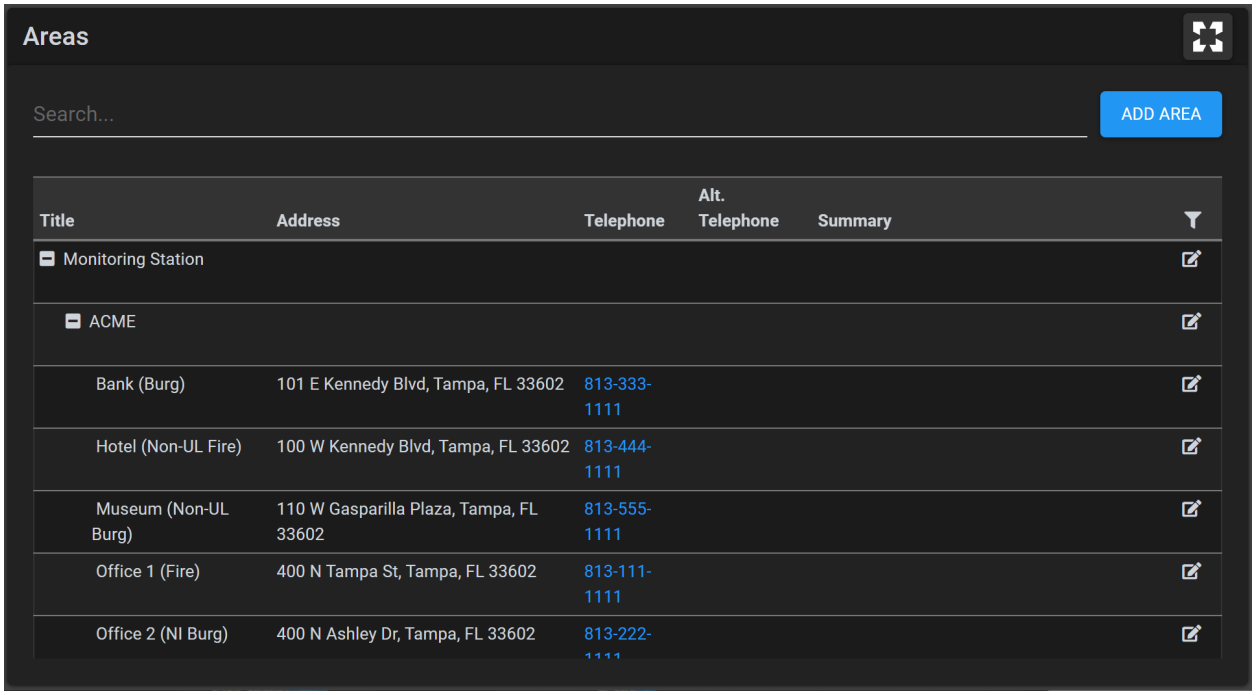
Sites

The SureView system operates using a tree with:

- The monitoring center at the top level (containing all the operators, supervisors, and system administrators)
- Areas which can be...
    - Sites (an “Account” in UL terms)
    - Customers containing a number of Sites

Areas are configured in the “Areas” menu item

The tree with some customers and sites:

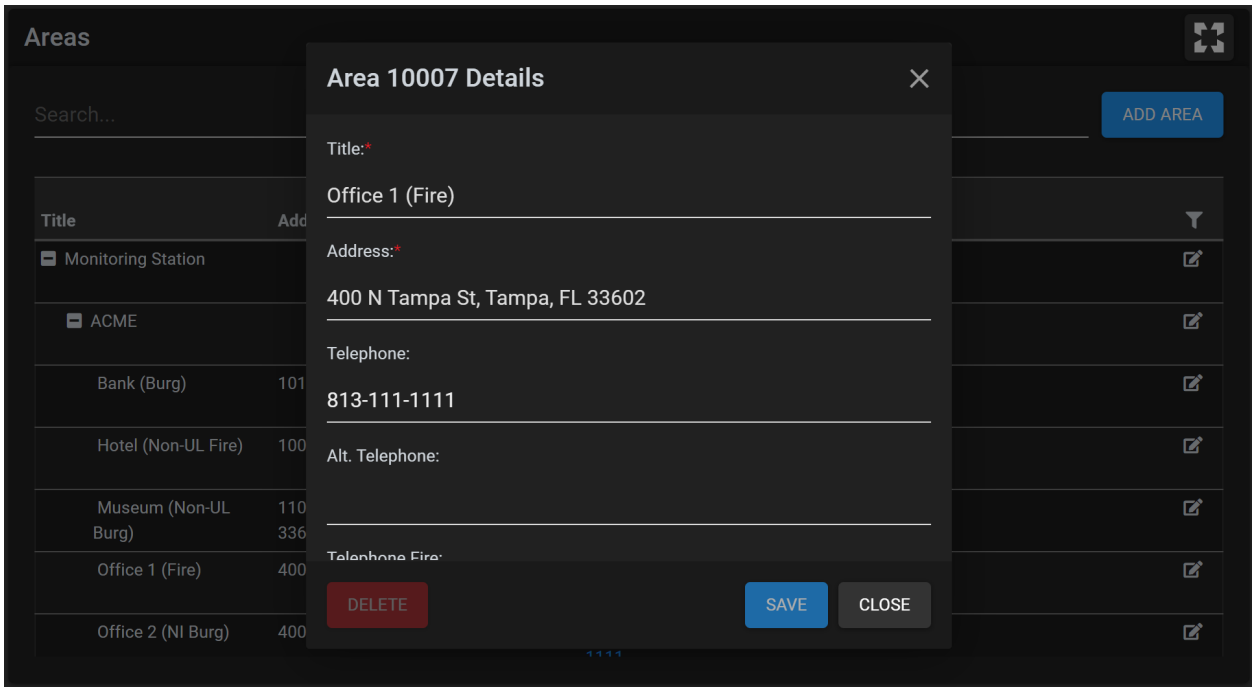


Site Setup

To add a customer or site go to the Areas screen, click “Add Area”, then complete the popup form including the address, phone numbers, and UL settings such as the classification and response time.

NOTE: the Address is important as this is used for Dispatch to know which sites are covered by patrol zones (see the Dispatch section below)

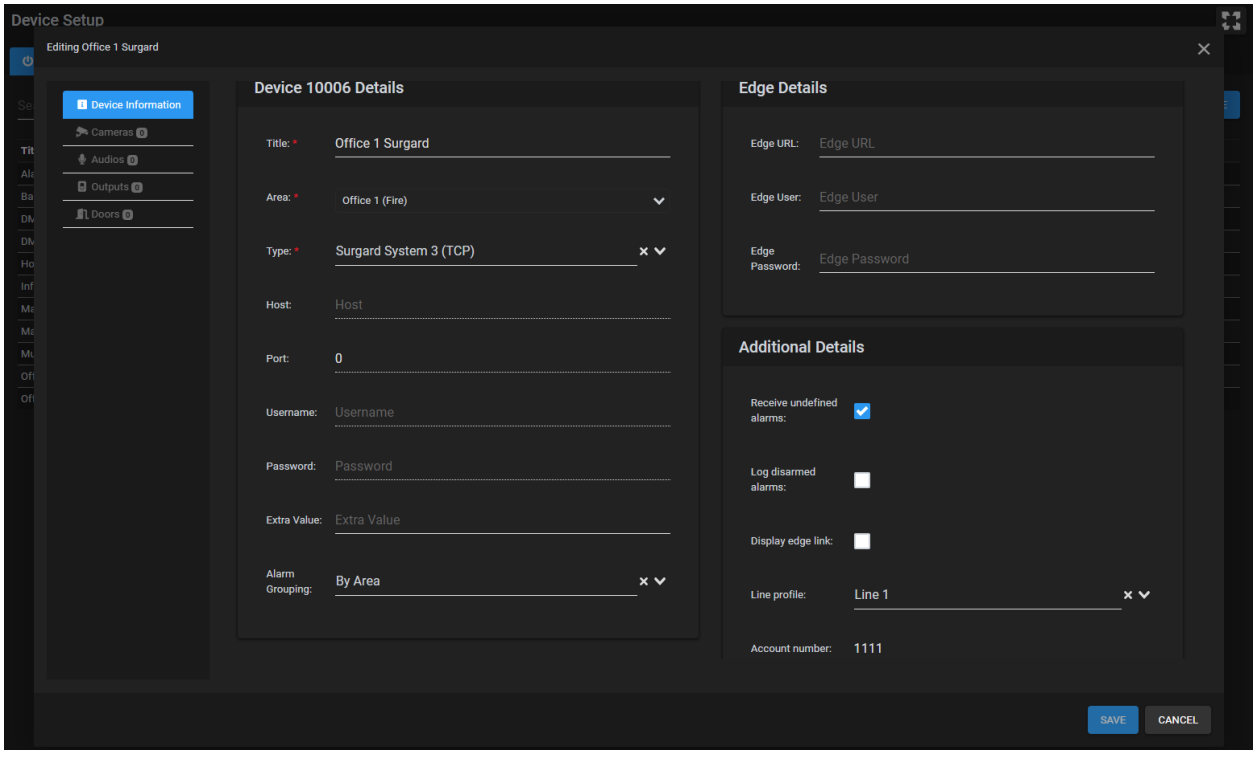
Site setup:



Device Setup

Monitored panels are called “Devices” which are added in the “Device Setup” menu item. Click “Add Device” and enter the Area (site), Type (for example “Surgard System 3”), Account Number (for example “1111”), and Line Profile on the receiver that was set up at the system level above.

Device setup with a Surgard panel account added:



Alarm Setup

Alarms are configured in the Alarm Setup menu item and provide names, priorities, and actions for each zone and signal type from a monitored panel.

In accordance with UL 1981 the alarms must be prioritized in the following order to ensure they appear in the queue in the given order (highest first), noting that UL certificated alarms must be higher than their non-certificated equivalent (i.e. if “2001” is used for UL fire alarms, then 2000 should be used for non-UL fire alarms)
For example:

1. Fire (eg “2001” for UL certificated and “2000” for non-UL)
2. Panic (eg “1501” and “1500”)
3. Medical (eg “1001” and “1000”)
4. All others to lower

Note that anything set to priority 1000 or higher will cause the alarm to always be presented to operators for processing, regardless of whether the site or alarm is armed.

Also in accordance with UL, open/close alarms must be specifically reported on, so you must create a tag called “Open/Close” (see “Alarm Tags” section above) and apply this to the Open and Close alarms. These can then be reported on via the “Alarms by Tag” report (see “Reports” section below).

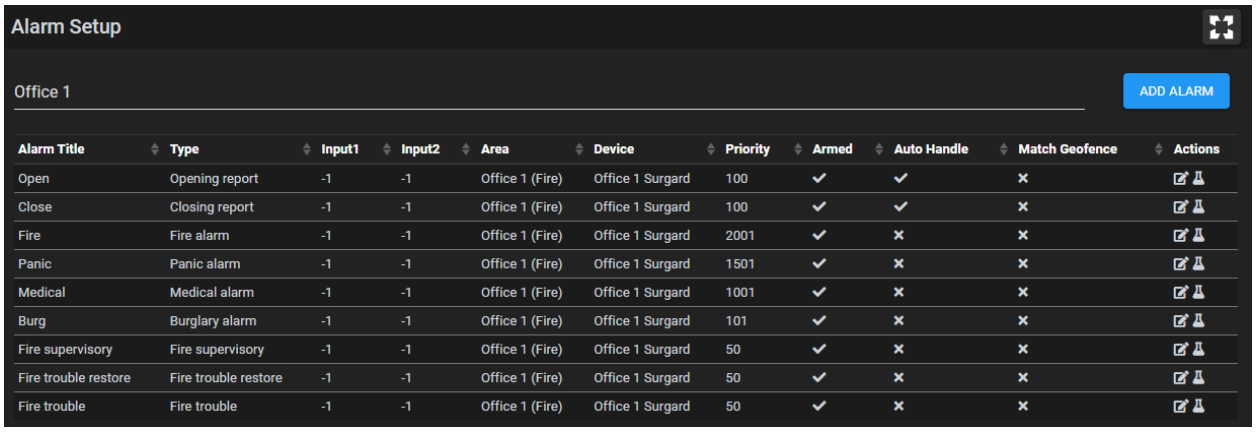
The Runaway setting allows alarms occurring more than X times in Y minutes to be marked as “RUNAWAY” in the queue to inform the operator that they have exceeded the threshold.
Note: The recommendation is to use a minimum of 6 times in 1 minute.

The Action Plan setting allows you to configure the action plan that will be presented to the operator to follow when processing this type of alarm.

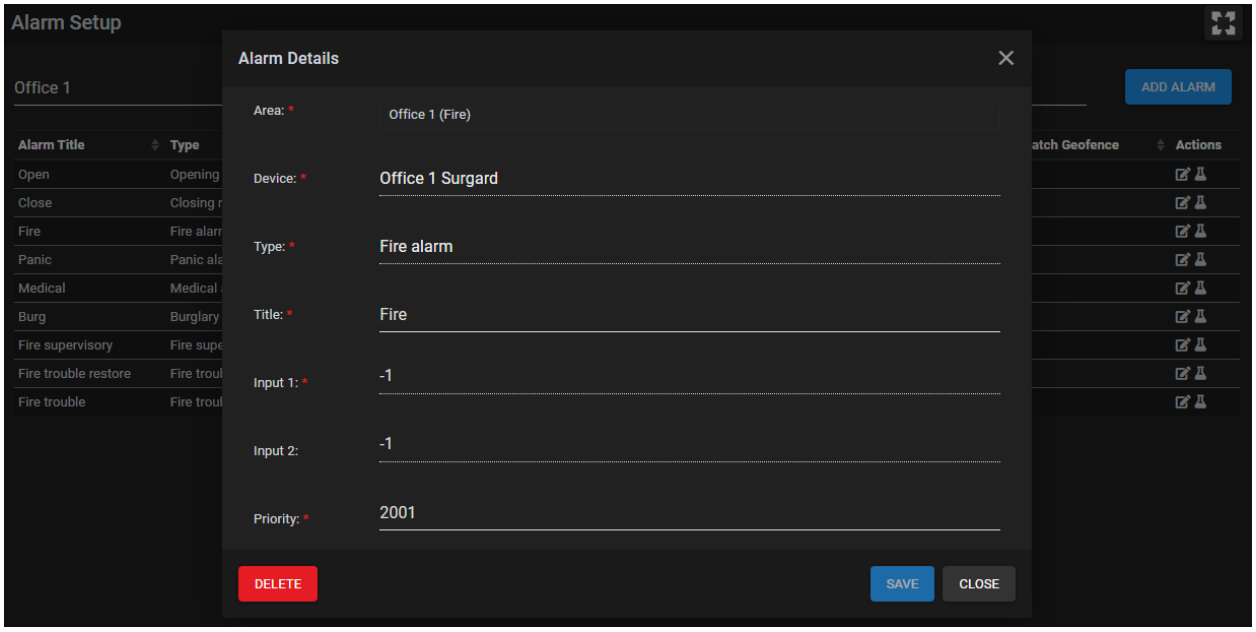
The Auto Handle setting allows you to set alarms that you want to be audited but not presented to operators for handling. This can be used for maintenance related alarms such as battery failures etc. Note: this must not be applied to UL certificated alarms such as Life Safety etc.

The “Trigger a test alarm” action button simulates the particular alarm being received allowing you to see what would happen when it is received from a Receiver.

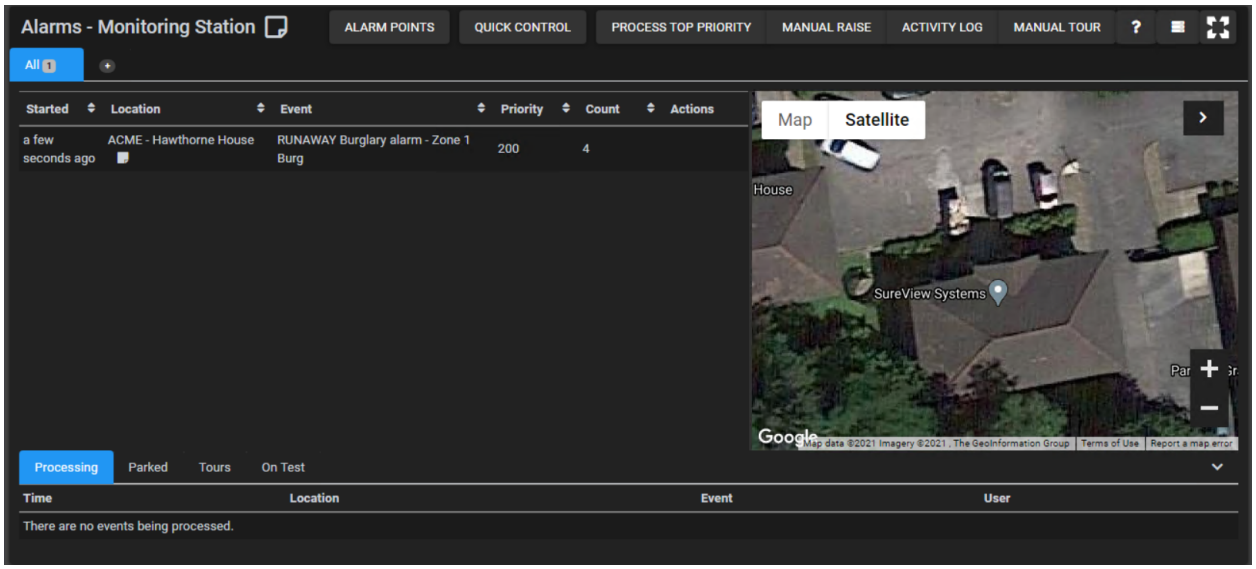
Alarm setup showing opening, closing, burglary, panic, and fire alarms configured:



Example of an alarm being configured:



Example of a Runaway alarm in Alarm Queue:



Expected Alarms

Expected Alarms provide schedules of when certain alarms should occur and provide warning if they occur early or do not occur at all. This is typically used for Open/Close alarms to set a period of time when a site's alarm panels are expected to be disarmed and armed.

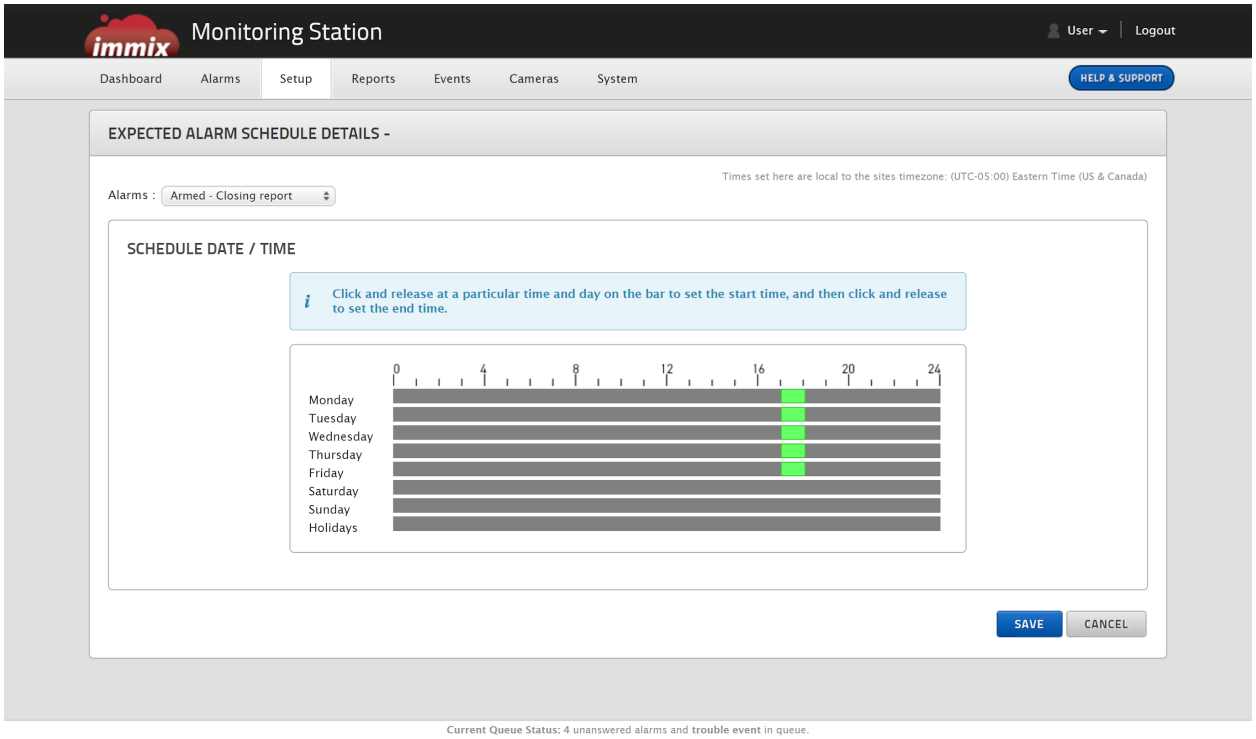
Alarms are marked in the following manner to denote their status:

- If the alarm is *not received* at the end of the schedule, an alarm will be raised saying "NOT RECEIVED"
- If the alarm is received *before* the schedule it will be prefixed with "UNSCHEDULED"
- If the alarm is received *during* the schedule it will appear normally without any additional text. It can also be set to be Auto Handled if you do not want the alarm to appear in the queue.

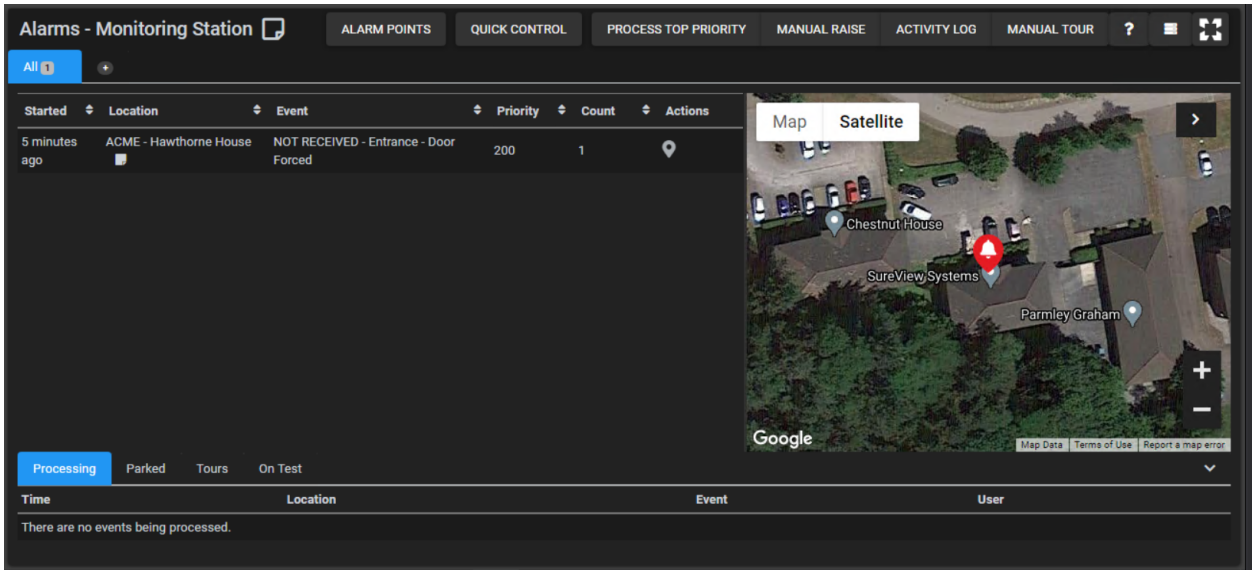
Alarms that do not meet the schedule will also be shown in the "Out Of Schedule" report (see Reports section below)

The schedules are currently added in the V1 setup interface choosing the alarm, times, and days that you expect it to occur.
NOTE: in order to add a grace period just set the schedule to start sooner and/or end later, i.e. a Close alarm expected between 17:00 and 18:00 can be set to be expected between 16:55 and 18:05 to give a 5 minute grace period either side.

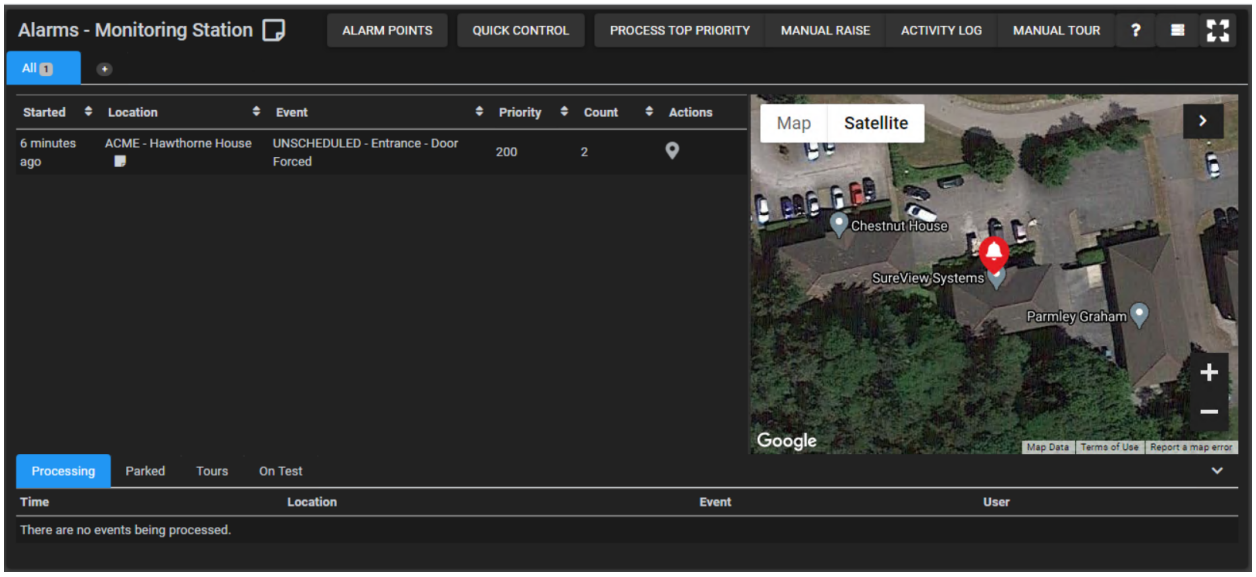
Example of a Close alarm being set as expected between 17:00 and 18:00 Mon-Fri:



Example of a Not Received alarm in the Alarm Queue:



Example of an early (unscheduled) alarm in the Alarm Queue:



Contacts (Site Staff and Call List)

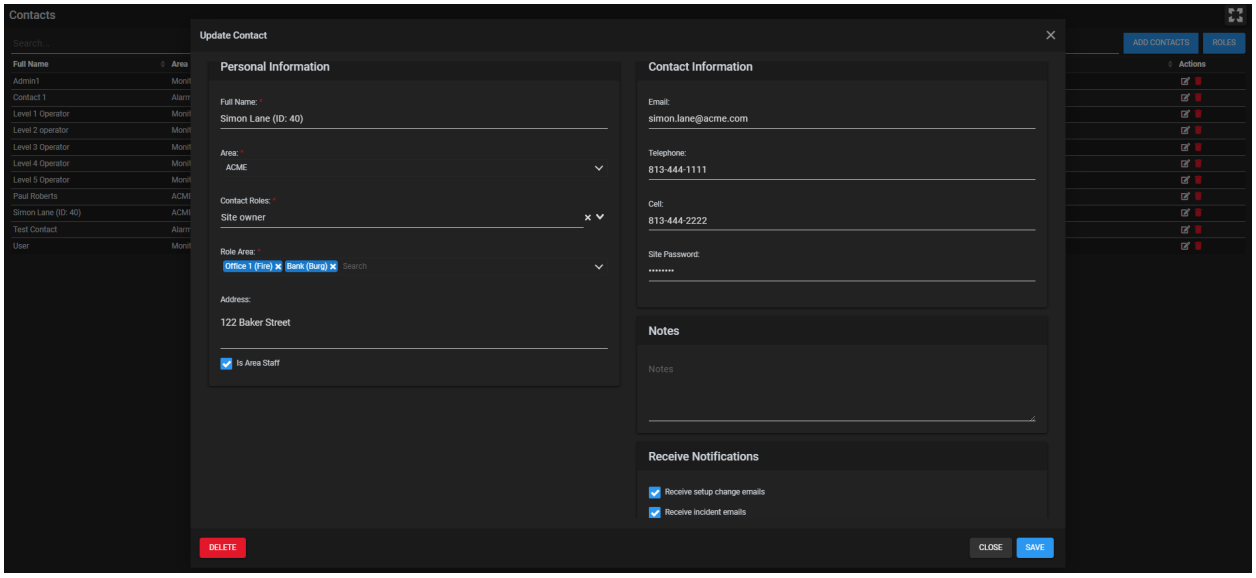
Contacts for sites are added in the “Contacts” menu item, with the “Role Area” list being the sites that the person is a contact for.

Ticking “Is Area Staff” causes the person to appear as Site Staff on the Details screen when operators process alarms and providing a “Site Password” allows verification of their identity (see the “Alarm Processing” section below).
You may add additional information after their name such as their UserId on the panel that will be sent with Open/Close signals to allow operators to match contacts to their panel user.

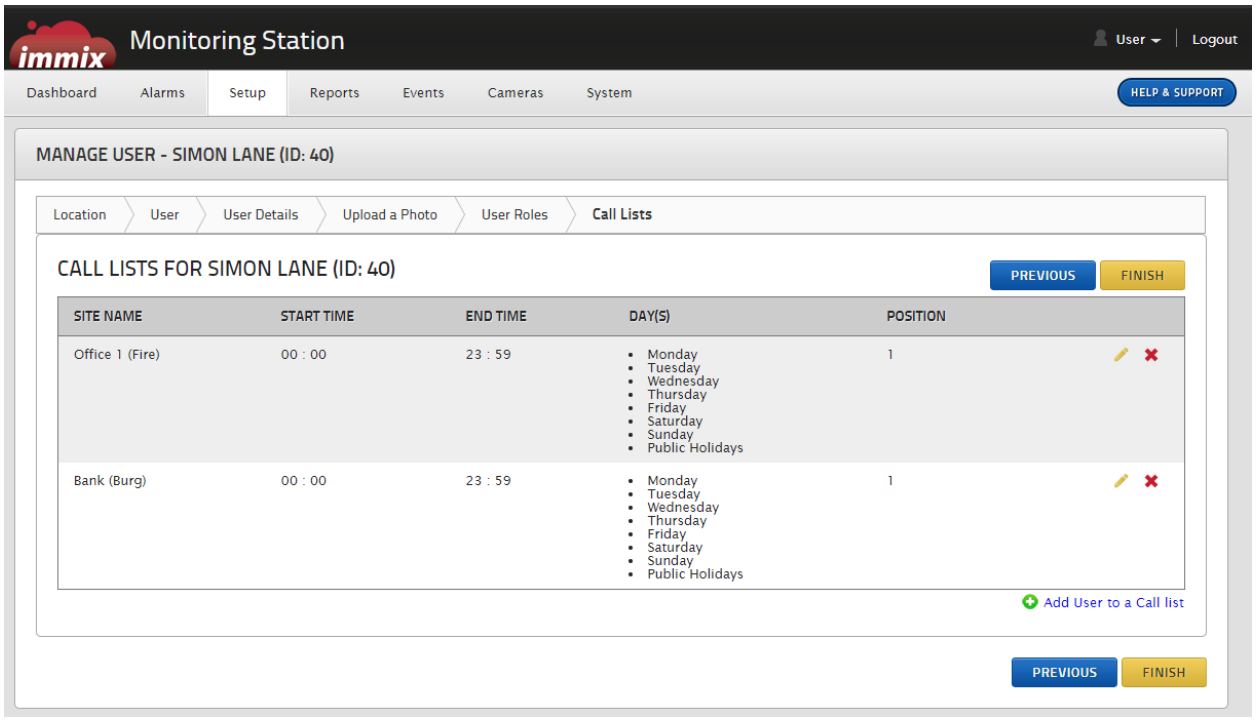
Providing an Email address and ticking the “Receive incident emails” box allows them to receive an automatic email any time an event is closed out with an “Incident”-type outcome, and optionally ticking the “Receive setup change emails” box allows them to receive an automatic email any time changes are made to the site.

Providing a Telephone number allows them to be added to the Call List to show when operators process alarms.
NOTE: call lists are currently set up in the V1 interface by going to Setup -> Edit Users -> choosing the area they belong to -> choosing the person -> Call Lists tab

Adding a contact, set as Area Staff and to receive emails:



Adding a contact to a call list:



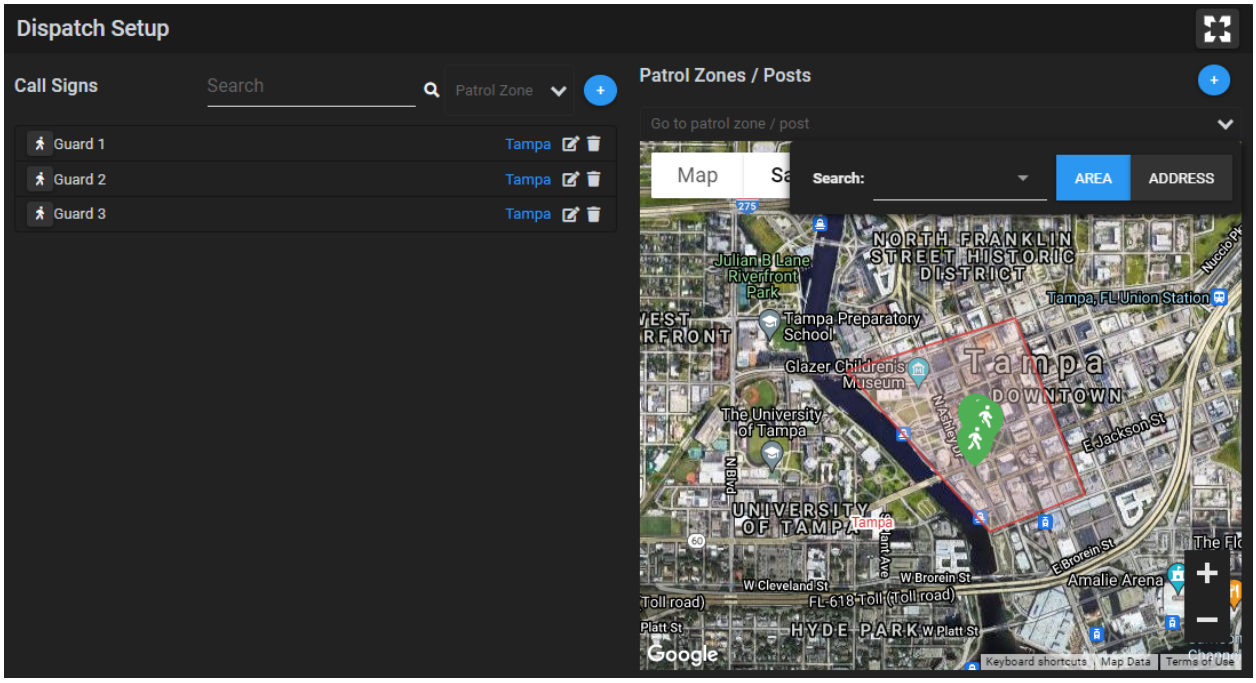
Dispatch

Dispatch is set up in the “Dispatch Setup” menu item and allows you to add guards (called “Call Signs”) and specify which sites they cover (called “Patrol Zones”)

To add a patrol zone use the rightmost “+” button, provide a name, then click the map to draw a polygon for the area it covers (this could be multiple sites in a campus, one site, or part of a site).

To add a guard use the leftmost “+” button and provide a name, then drag them into the patrol zone they belong to.

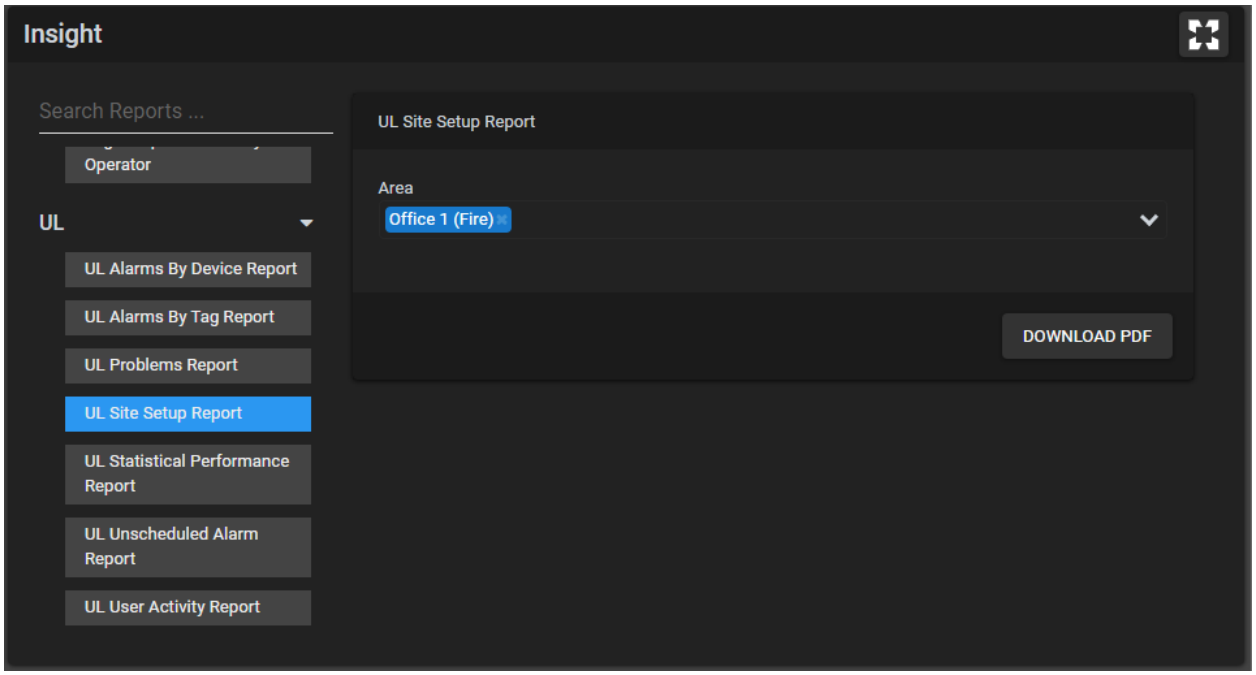
Dispatch setup with a patrol zone containing a number of guards:



Setup Report

The Site Setup report provides a textual list of the current configuration of the site. This can be downloaded by opening the Insight menu item, choosing the “UL Site Setup Report” then choosing a site (area) and clicking “Download PDF”.

Site Setup Report download:



Site Setup Report:

UL Site Setup Report

Office 1 (Fire)

Address: 400 N Tampa St, Tampa, FL 33602

Telephone: 813-111-1111
Alternative Telephone:
Police: 813-111-3333
Fire: 813-111-2222
ULType: FireTrue
Station has keys: False
Area is active: False
Line is secure: False
Line is encrypted: False
Investigator required: False
Response time: 0 minutes

Office 1 Surgard (Surgard System 3 (TCP))

Identifier: 10006
Device Type: Surgard System 3 (TCP)
Host:
Username:
Account Number: 1111
Line Profile: Line 1

Alarms

Input1	Input 2	Title	Priority	Auto-handle	ExtraValue	Tag
-1	-1	Burg	101	False		
-1	-1	Close	100	True		
-1	-1	Fire	2001	False		
-1	-1	Fire trouble restore	50	False		
-1	-1	Fire supervisory	50	False		
-1	-1	Medical	1001	False		
-1	-1	Open	100	True		

Expected Alarm Schedules

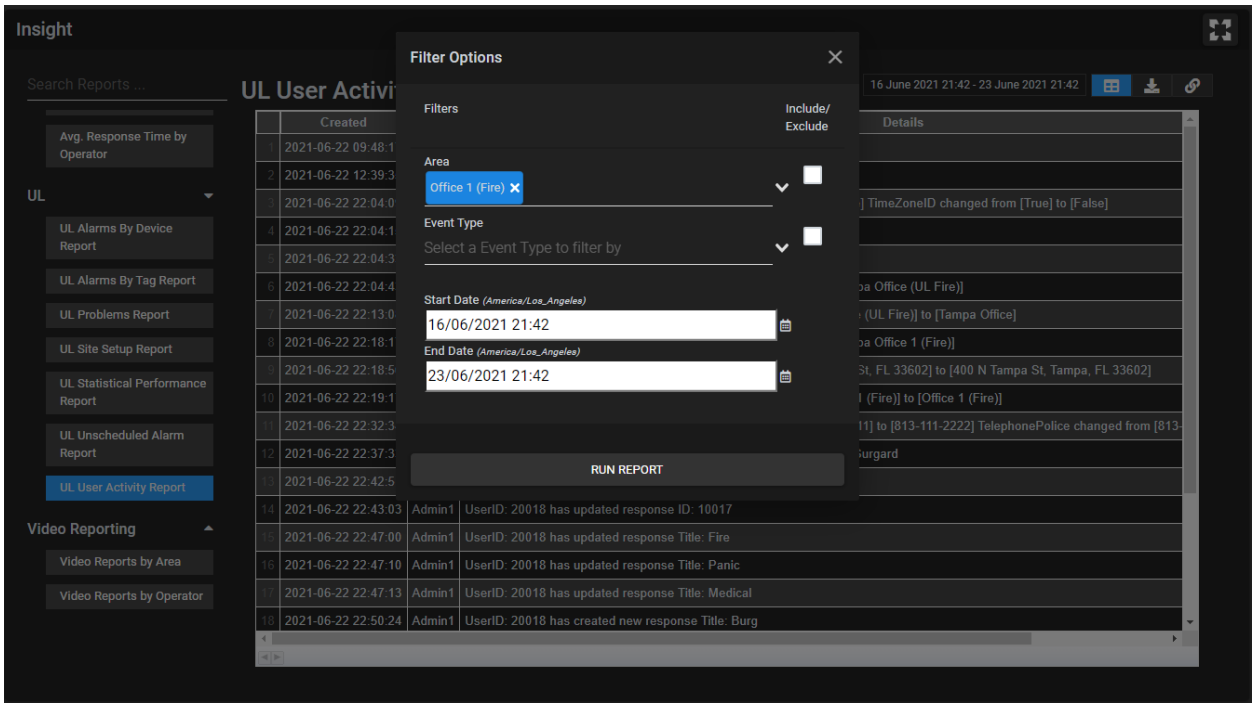
Times	Mon	Tue	Wed	Thur	Fri	Sat	Sun	Public Holiday
13:00 - 14:00	X	X	X	X	X	X	X	-

-1	-1	Panic	1501	False		
-1	-1	Fire trouble	50	False		

Setup Activity

The history of all changes made to a site can be viewed by going to Insights, selecting the “UL User Activity Report”, and filtering it by a specific site (area)

Site Setup Activity:


Insight
Search Reports ...
Avg. Response Time by Operator
UL
UL Alarms By Device Report
UL Alarms By Tag Report
UL Problems Report
UL Site Setup Report
UL Statistical Performance Report
UL Unscheduled Alarm Report
UL User Activity Report
Video Reporting
Video Reports by Area
Video Reports by Operator
UL User Activi
16 June 2021 21:42 - 23 June 2021 21:42
Filter Options
Filters
Include/ Exclude
Area
Office 1 (Fire)
Event Type
Select a Event Type to filter by
Start Date (America/Los_Angeles)
16/06/2021 21:42
End Date (America/Los_Angeles)
23/06/2021 21:42
RUN REPORT
Created
Details
2021-06-22 09:48:1
2021-06-22 12:39:3
2021-06-22 22:04:0
2021-06-22 22:04:1
2021-06-22 22:04:3
2021-06-22 22:04:4
2021-06-22 22:13:0
2021-06-22 22:18:1
2021-06-22 22:18:5
2021-06-22 22:19:1
2021-06-22 22:32:3
2021-06-22 22:37:3
2021-06-22 22:42:5
2021-06-22 22:43:03 Admin1 UserID: 20018 has updated response ID: 10017
2021-06-22 22:47:00 Admin1 UserID: 20018 has updated response Title: Fire
2021-06-22 22:47:10 Admin1 UserID: 20018 has updated response Title: Panic
2021-06-22 22:47:13 Admin1 UserID: 20018 has updated response Title: Medical
2021-06-22 22:50:24 Admin1 UserID: 20018 has created new response Title: Burg

Alarm Processing

Alarm Queue

The alarm queue shows sites that are in alarm with the highest priority alarm that has occurred in each. The list is ordered by the highest priority first and then oldest date.

The priorities of alarms are configured by a setup user via the Setup section as explained in “SureView Configuration” above.

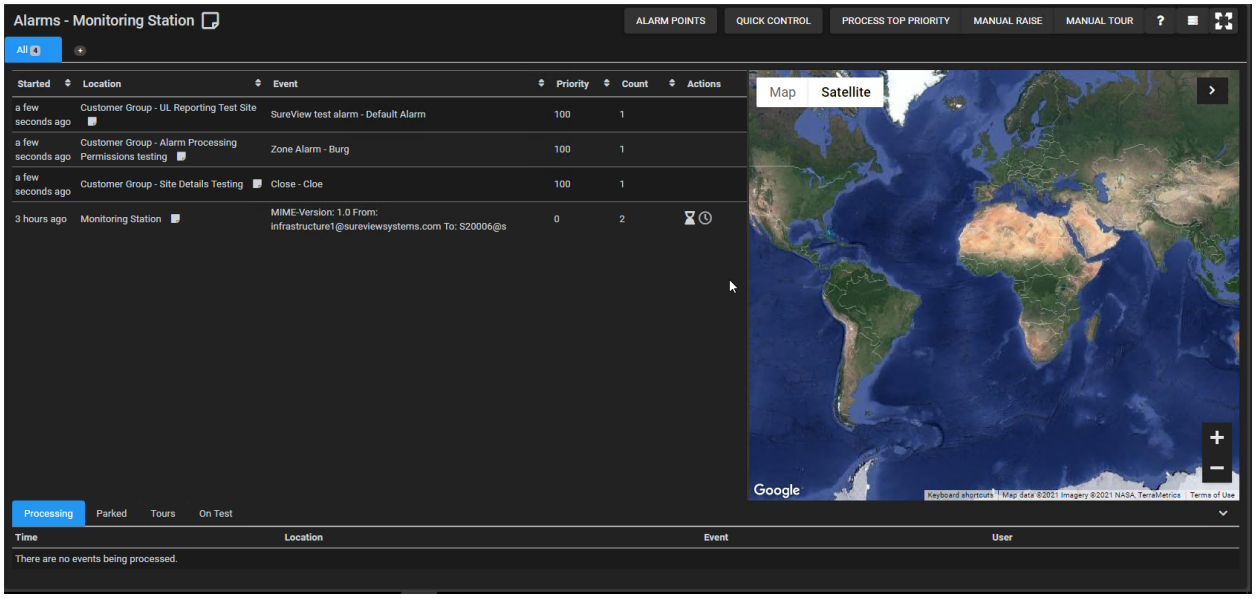
While there are alarms in the queue there is an audible alert played and the screen flashes red (important: the PC sound must not be disabled in order to be alerted about alarms while running other programs)

“Old” alarms which have not been processed within the configured system setting will have a “Clock” icon shown next to them.

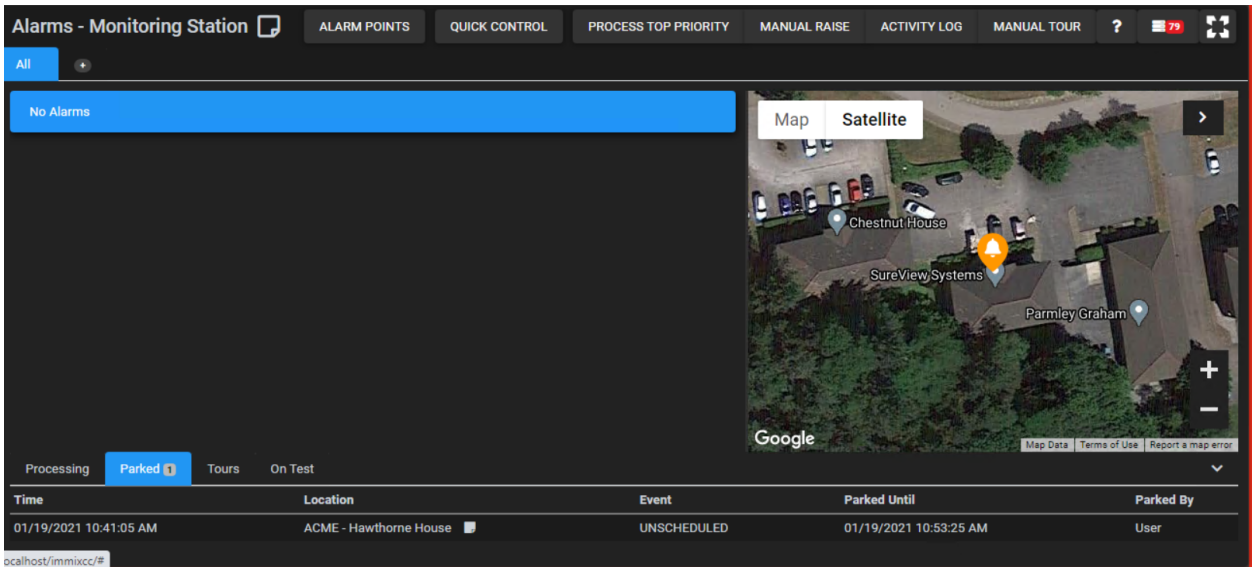
Alarms that are being processed by other users show in the “Processing” list at the bottom.

Alarms that are parked show in the “Parked” list at the bottom and will automatically return to the queue when either the parked time expires or a new alarm comes into the event. When a parked alarm returns to the queue it will have the Hourglass icon denoting that it was previously parked.

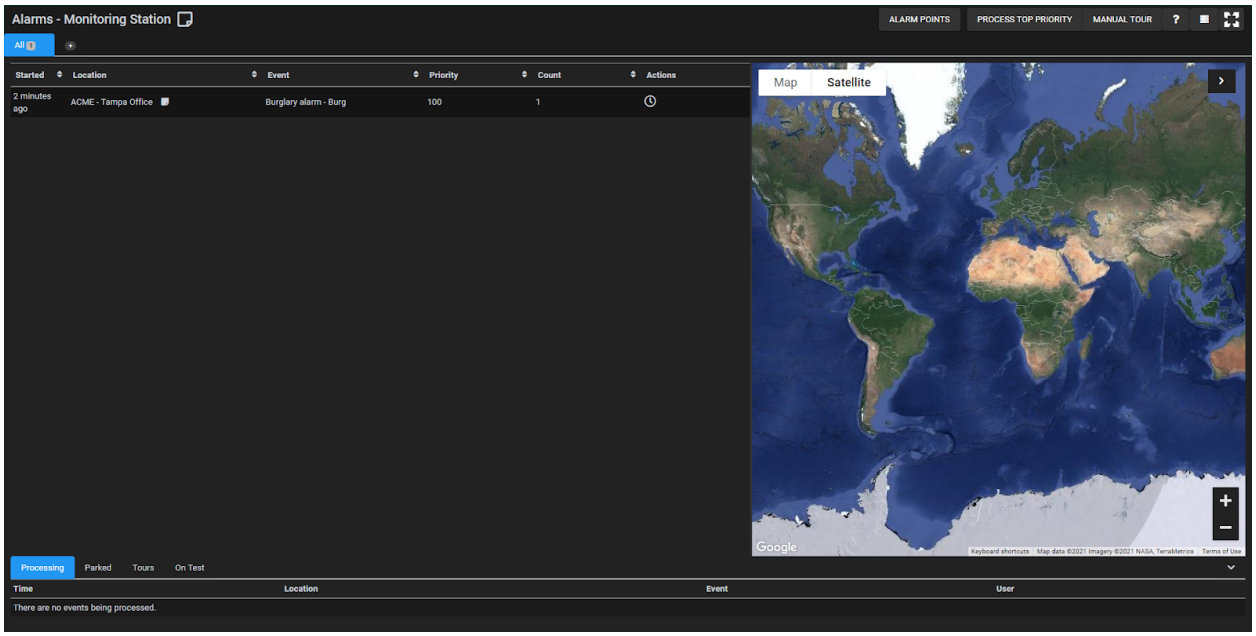
Alarm queue showing some unprocessed alarms:



Alarm queue showing a parked event:



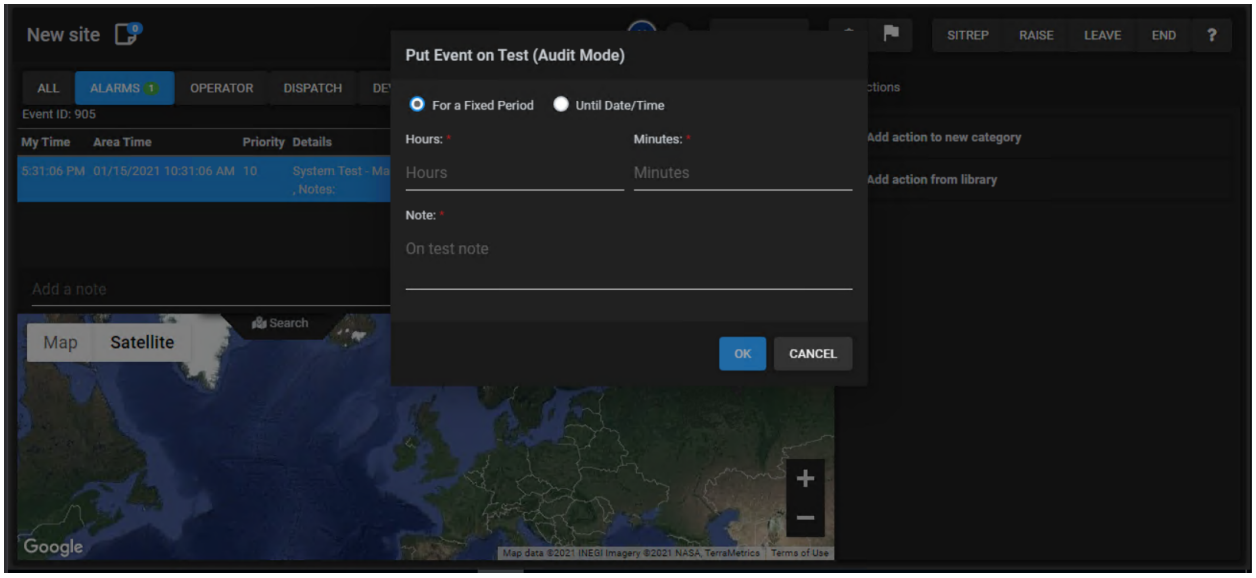
An old alarm highlighted in the queue:



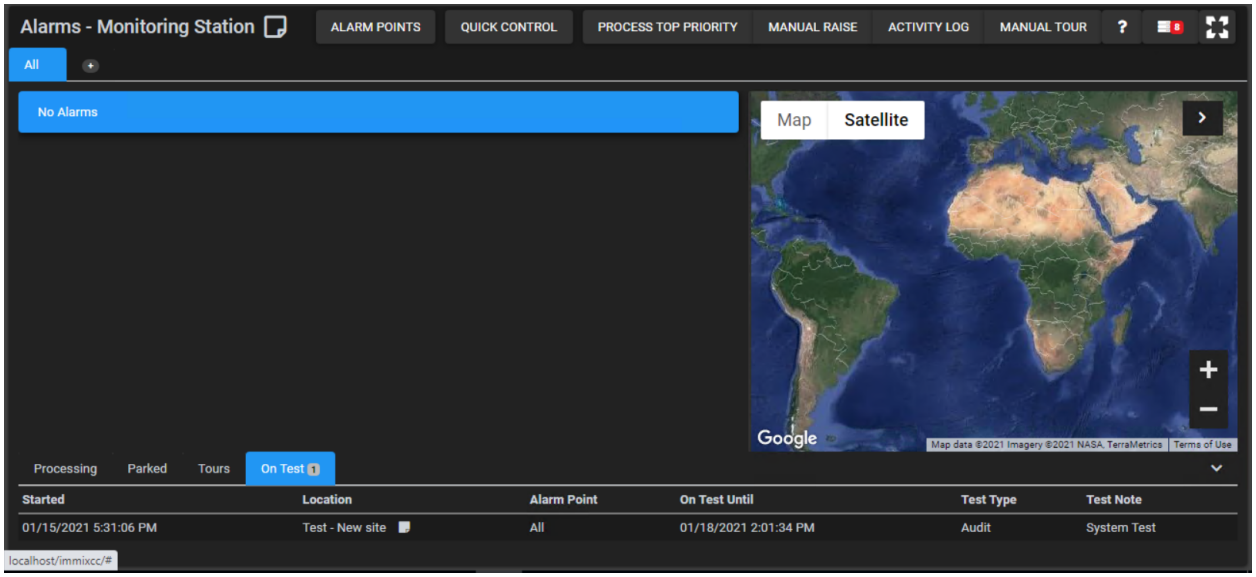
On Test

Sites can be placed “on test” to allow testing of alarms without having them presented to operators for processing. This is performed from within an event itself. Access the event and click the “Put this site on test (Audit Mode)” button with the clipboard icon. This will display a pop up box requiring you to enter the length for the test.

Putting a site on test:



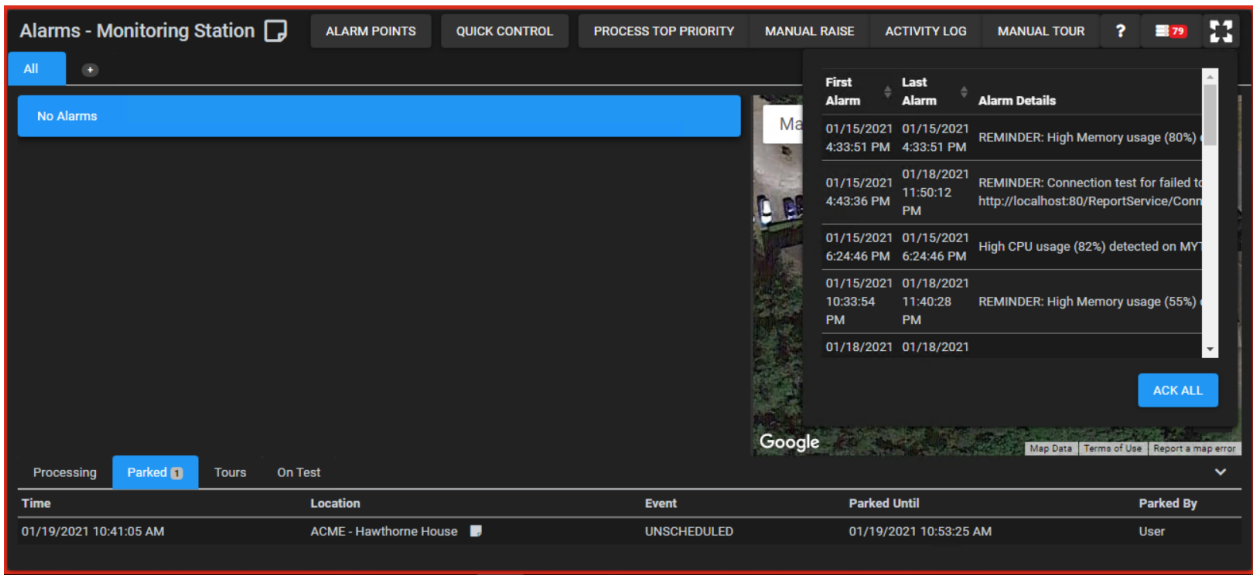
Alarm queue with site on test:



System Alarms

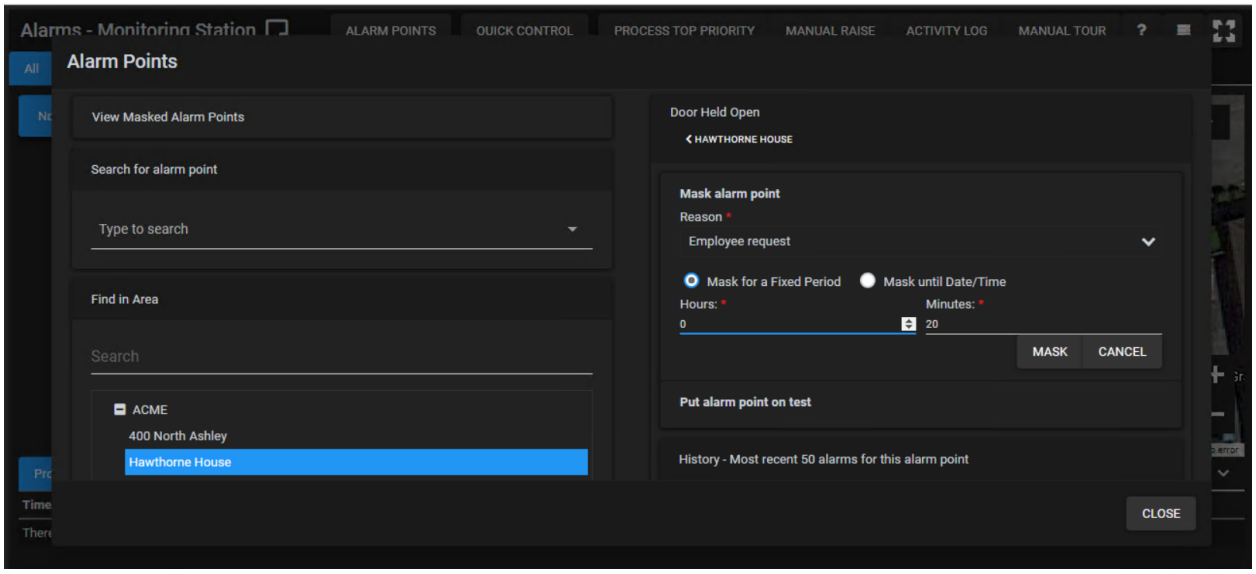
System trouble alerts such as network failure shown in System Events List at the top-right next to the menu button.
Refer to the “System Failures” section below for more information on the different types of messages and required actions.

A system alarm showing loss of connection to a DMP Receiver:



Disarming

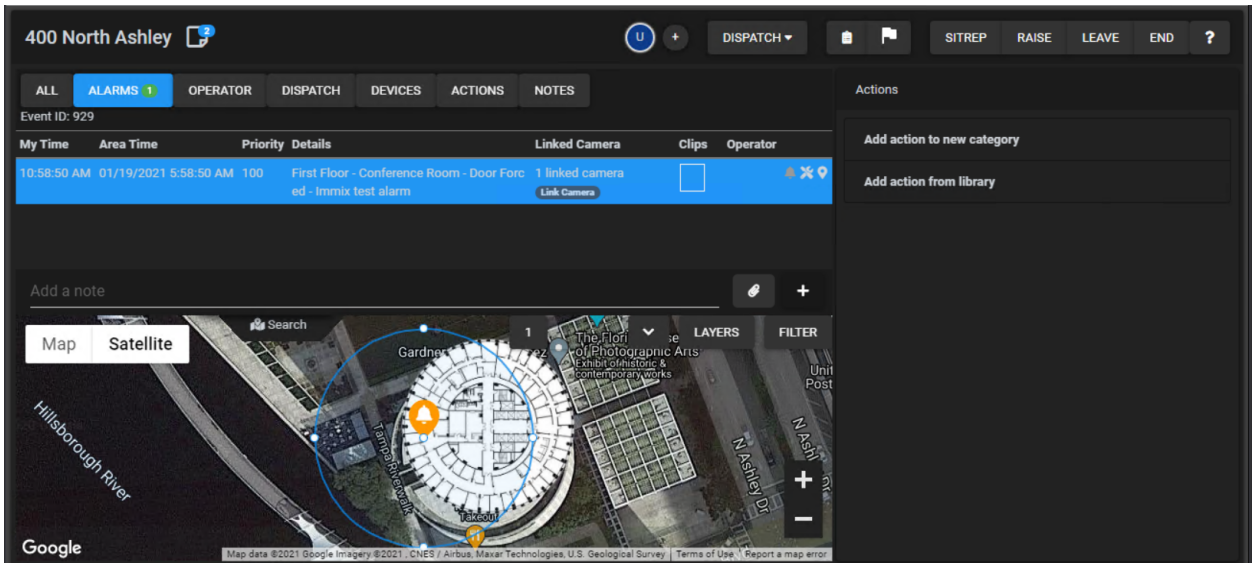
Faulty alarms can be disarmed for up to 24 hours by level 2 users using the “alarm points” menu from the alarm queue.



Alarm Processing

When an alarm has been selected from the queue for processing the user is taken to the Site Monitor screen to process it.

Alarm processing screen showing alarms inside event:



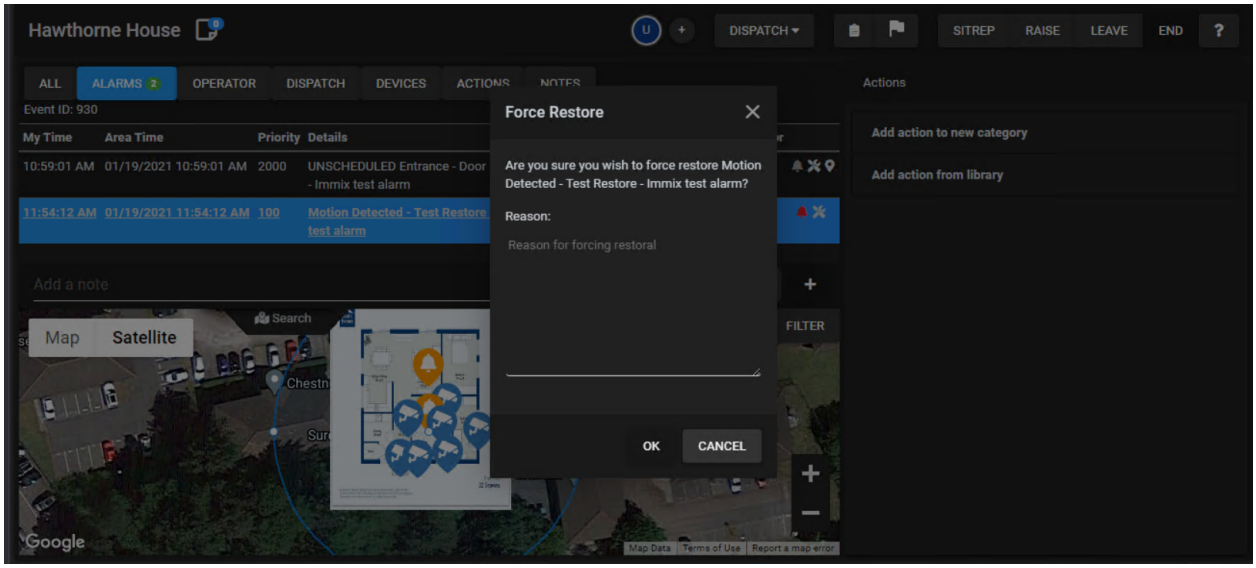
Alarms and Restores

The Alarms tab displays all alarms that have occurred in the event ordered by the highest priority first and then the newest date.

Alarms that are bold and underlined indicate that they have not been restored and operators cannot close the event until they have been restored (the event can be parked though).
The alarm can be forcefully restored in the software by clicking the Red bell icon to the right of the alarm's entry in the list. The user will be prompted if they wish to forcefully restore the alarm and this action will be audited.

Alarms that are red indicate that they have not been acknowledged (clicked) by the operator. All alarms must be acknowledged before the event can be closed.

An alarm awaiting a restore (shown in bold and underlined) being forcefully restored:

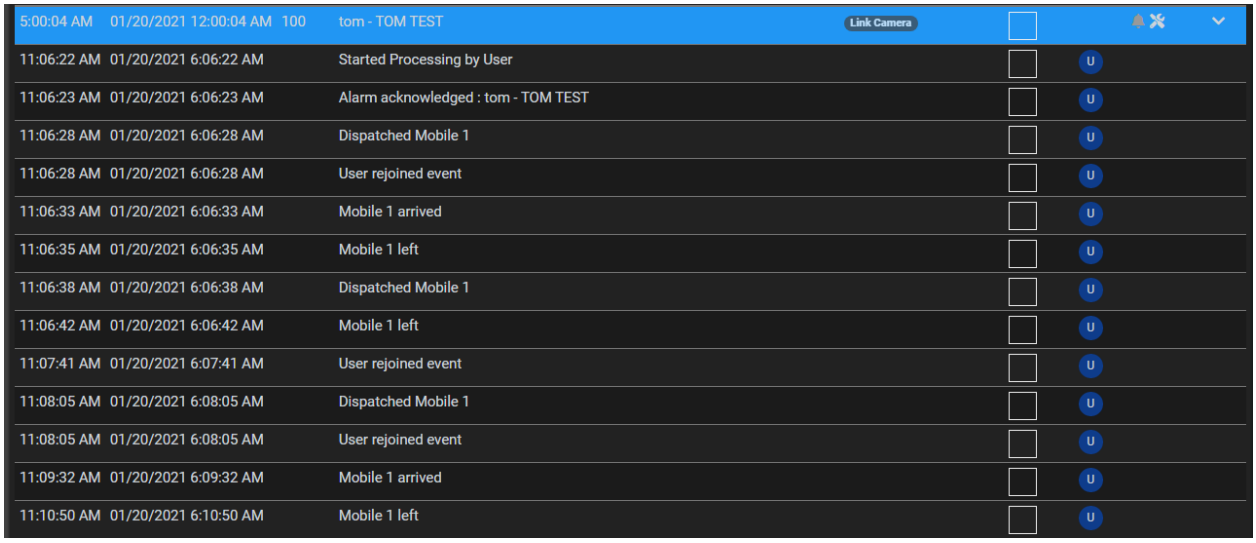


Audit Trail

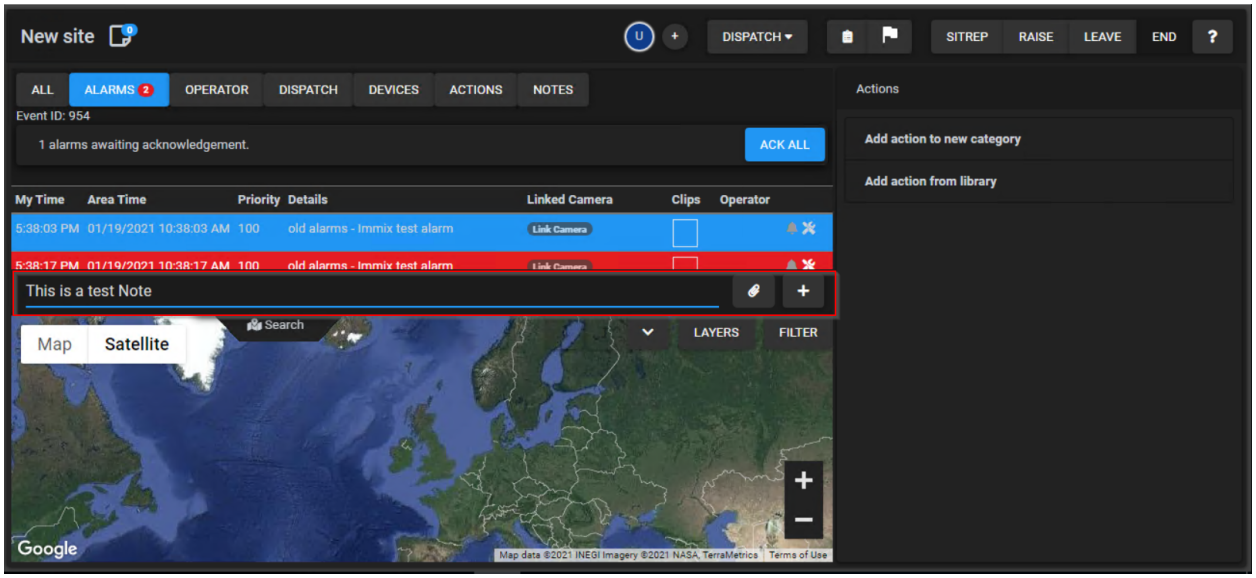
Everything occurring in the event is logged into the audit trail, from the received alarms to the operator actions that are taken.

At any point the operator can add a note to the audit trail via the “Add a note” box and plus button.
This can be used for external actions happening outside of the software such as noting information that was received during a phone call with emergency services, any site staff, or dispatched guards.

Audit trail of an event:



Adding a note into the audit trail:

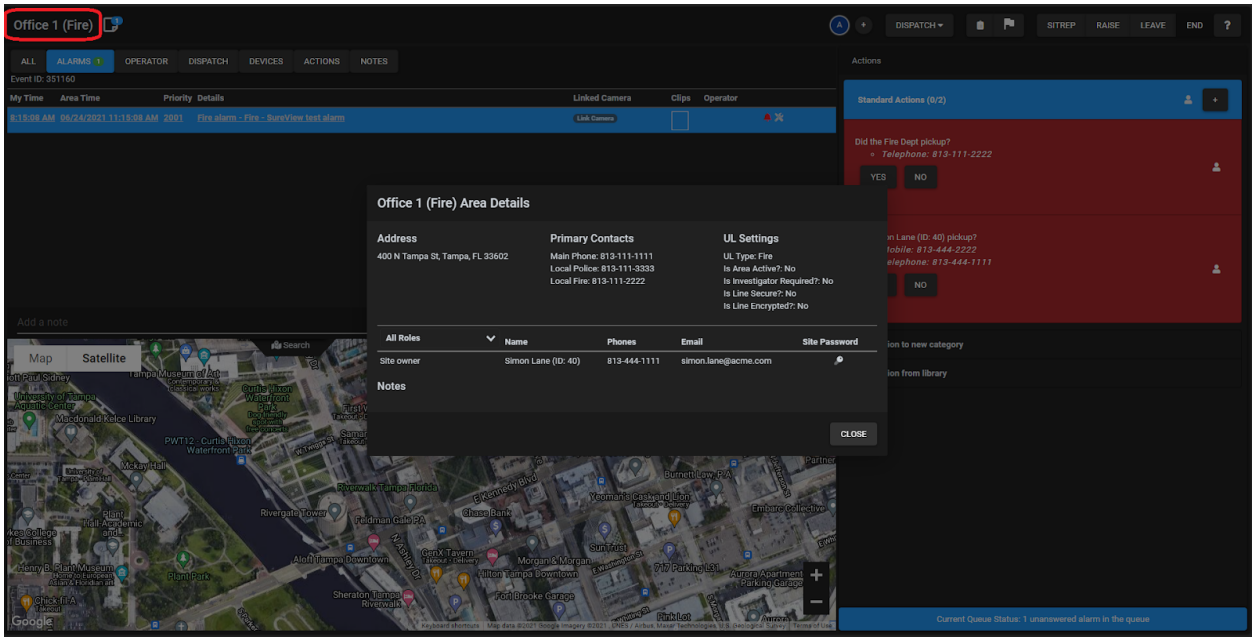


Site Details

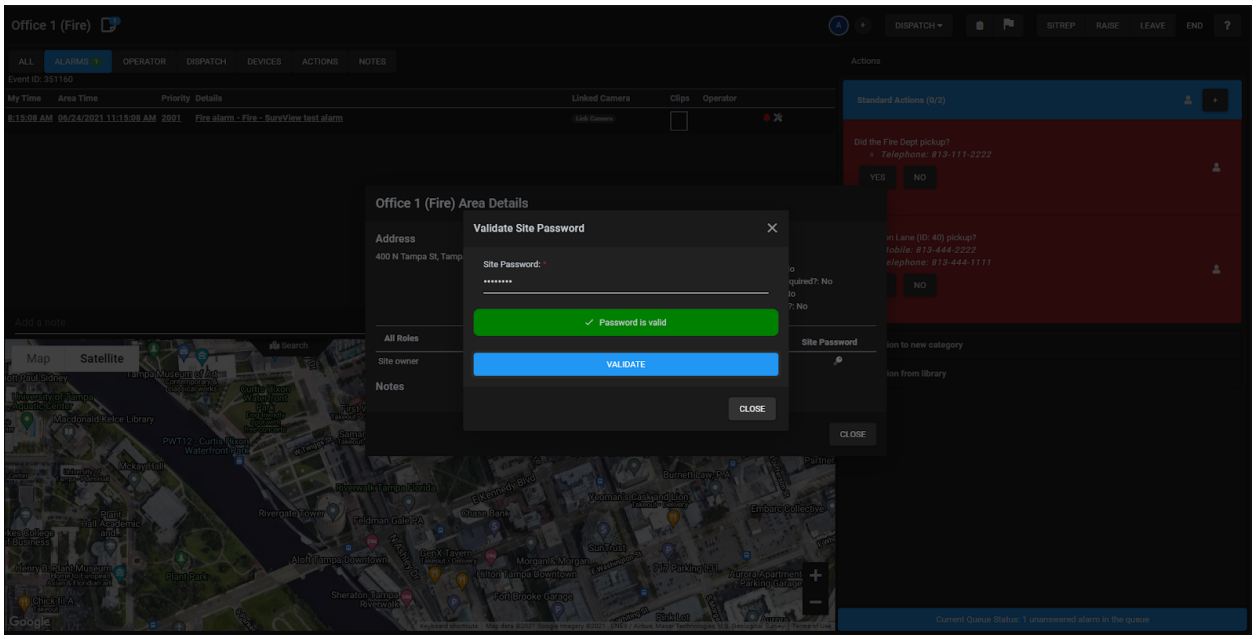
The Details window is accessed by clicking the site name in the top left and shows information about the the site including:

1. **Site Details**: Details about the site including the address, phone numbers, and UL details.
2. **Site Staff**: Details of the staff members for the site. Verification of identity is also possible by clicking the key icon and entering the password they have provided to be informed if it is valid or invalid.

Site details:



Verification of a site staff's passcode:

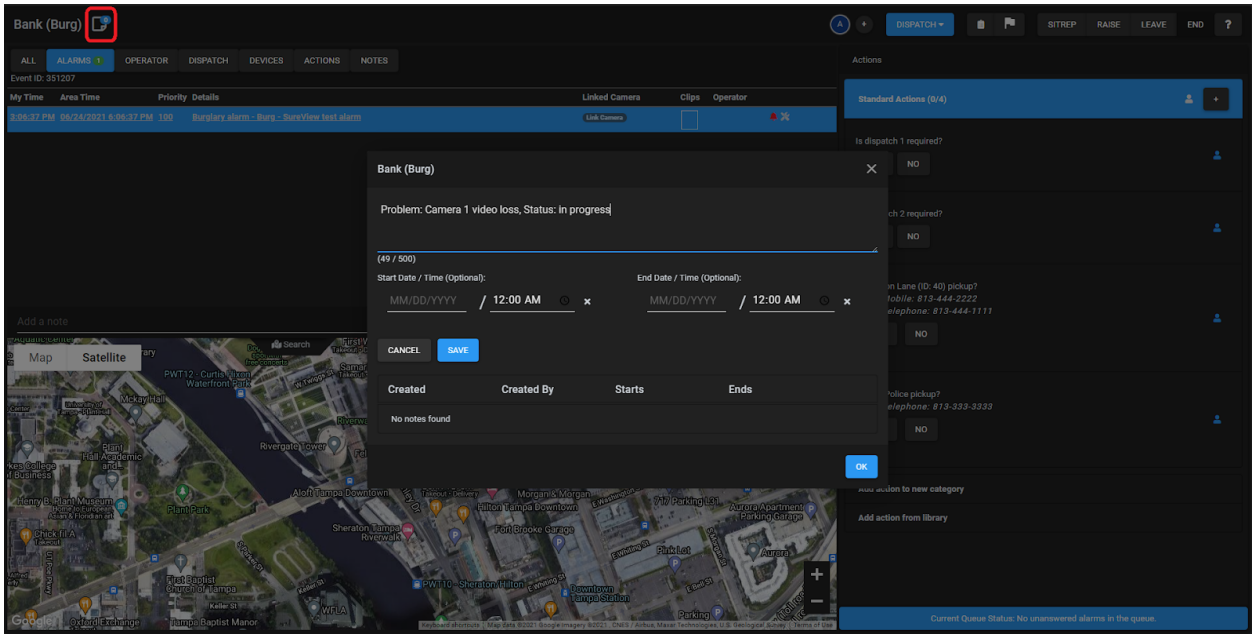


Site Notes and Problems

Site Notes can be added using the Note icon next to the site name and are used to record any information pertaining to the site to be visible to operators any time an alarm is processed on the site. This could be special instructions or to log problems such as maintenance issues.

If the note is added in the following format it will be treated as a “Problem” which will show in the Problems Report in Insights:
`Problem: {text}, Status: {text}`

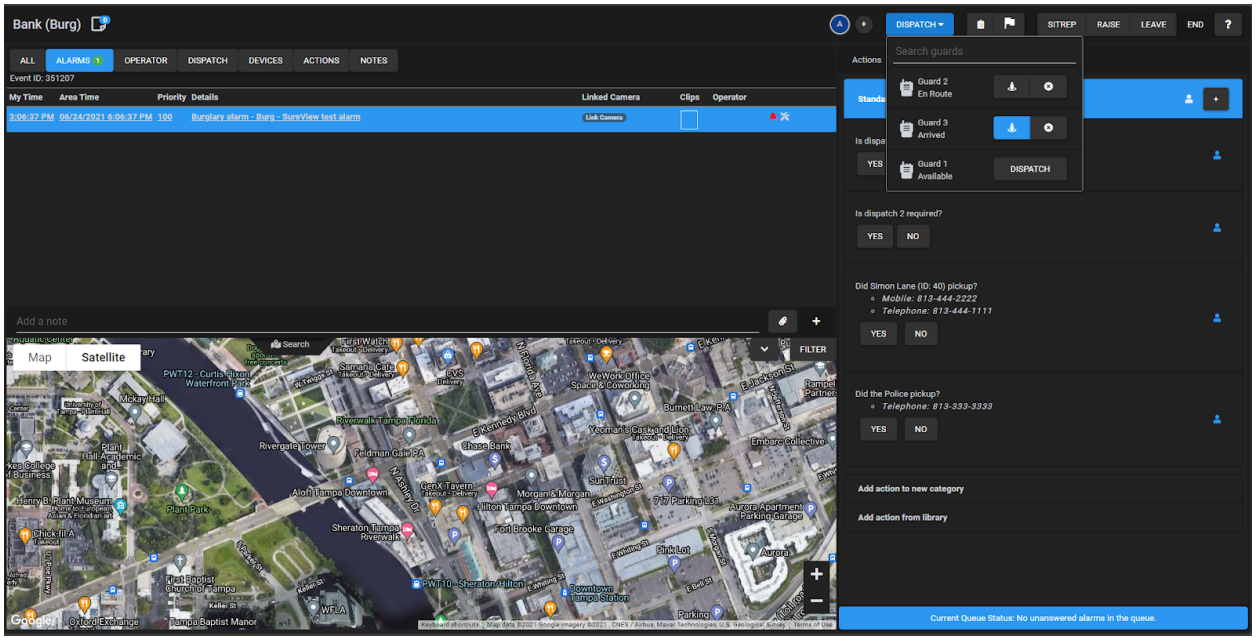
Example of a Site Note being added, using the special Problem format:



Dispatching Guards

Dispatching guards is done via the Dispatch button at the top-right. Clicking it will show the list of guards available for the site, their availability, and buttons to mark them as dispatched/arrived/left.

Dispatch window with 3 guards, one available for dispatch, one en-route, and one arrived:



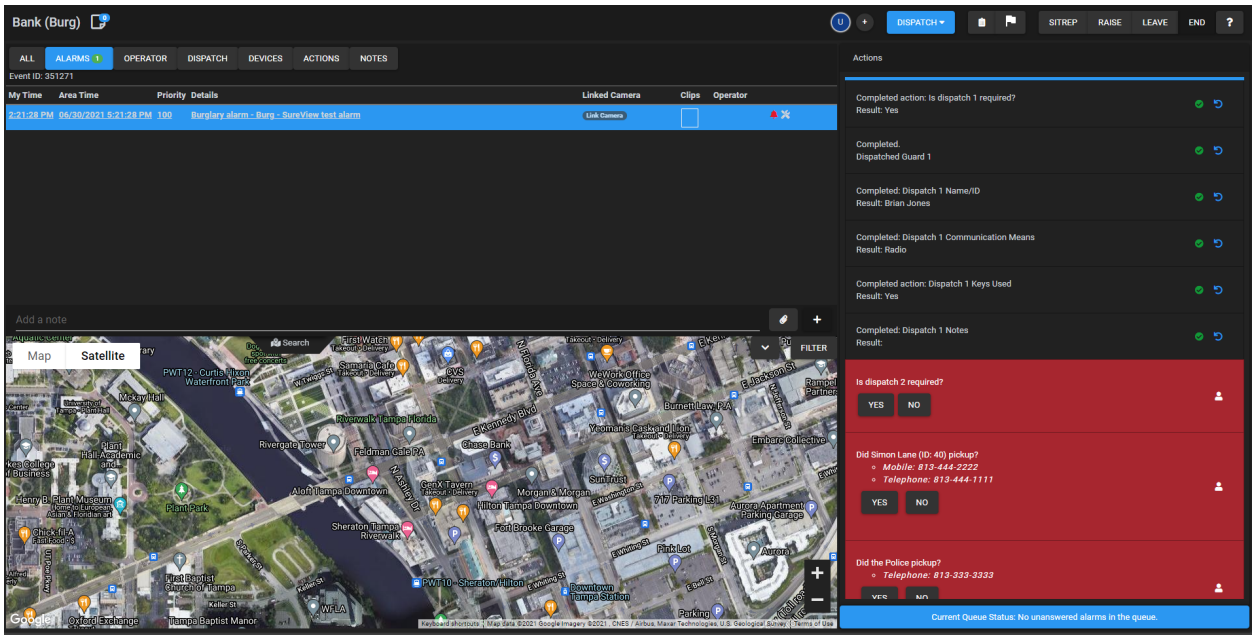
Action Plans

If any alarms have been configured with an Action Plan to guide the operator's actions then this will be shown in the "Actions" pane on the right-hand side of the screen.

As the actions are completed by the operator the results and entered information is stored in the audit trail in the same way as if it was entered manually (see "Audit Trail" section above).

Actions shown in red are required and will stop the event from being closed until they are completed.

An action plan showing some actions completed and some required ones outstanding:

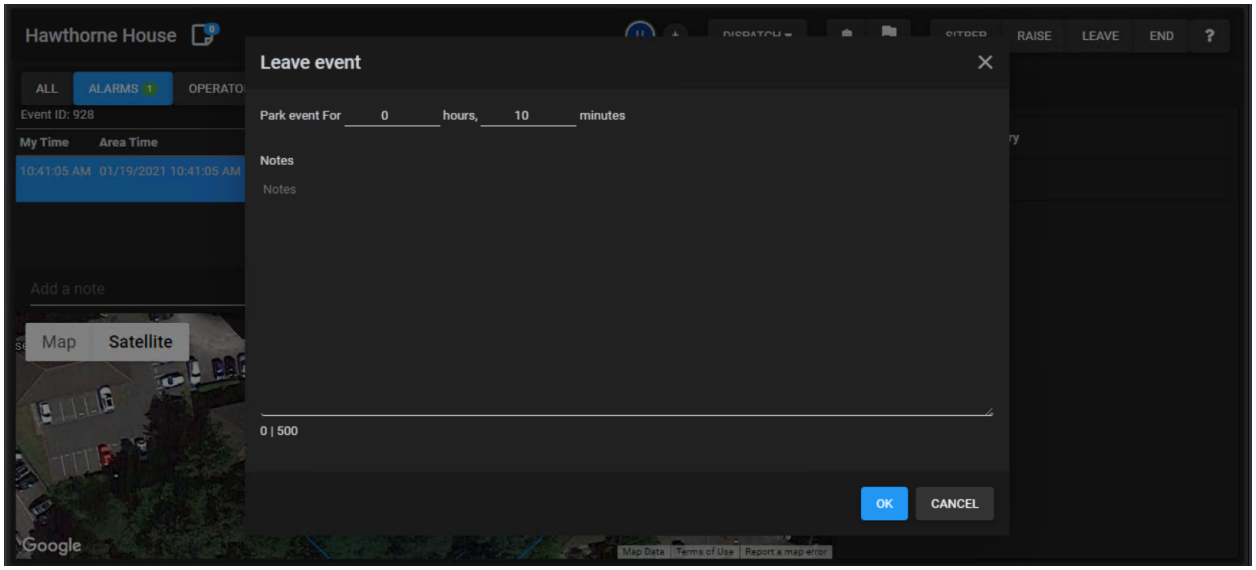


Parking

An event can be parked to be reviewed by another operator or to be resumed at a later time.

To park an event use the “Leave” button to the top right of the event. This will allow you to enter the length of the park then will place the event in the parked queue. If not resumed within the time limit it will return to the alarm queue. Entering 0 in both the hours and minutes field will immediately return it to the alarm queue.

Parking an event:

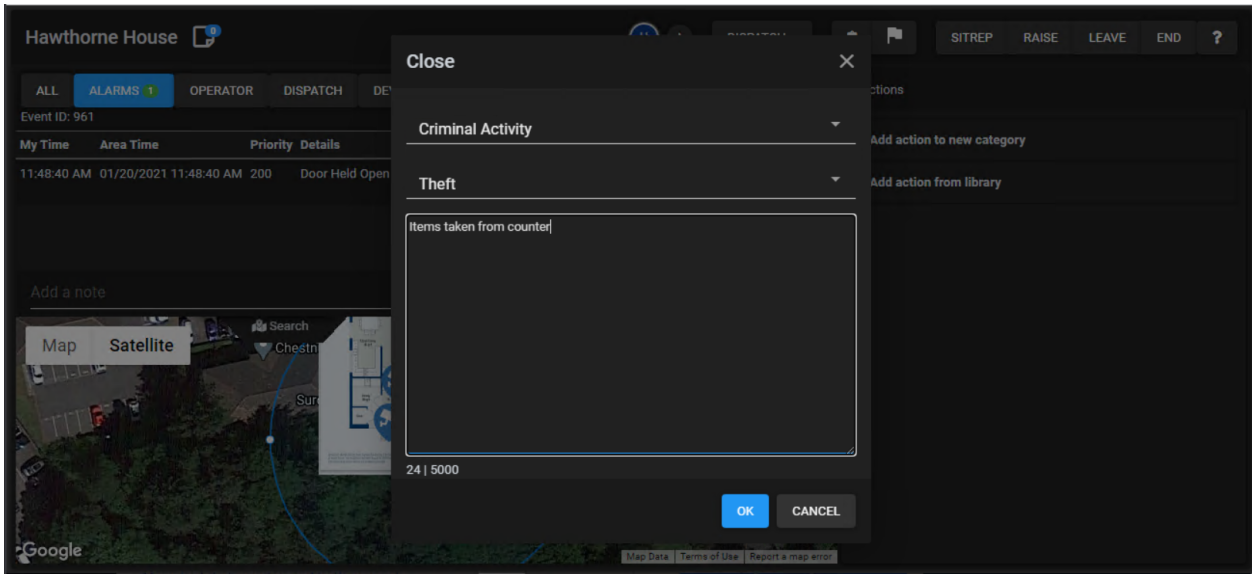


Close and Outcome

When processing of an event is complete the operator closes the event via the “End” button. Note this button only becomes accessible after all outstanding actions are complete including acknowledgement of alarms, receipt of restores for any restorable alarms, and processing of any required Action Plan steps.

Clicking the button asks the user to provide an outcome and optionally provide a description note, they are then returned to the alarm screen to process the next alarm.

The report for the event can then be found in the “Event Search” screen (see the “Reports” section below)



Standard Alarm Processing Procedure

Alarms must be processed and verified in accordance with UL 2050 and UL 827. The recommended general procedure for processing an alarm is as follows (see the other sections of this document for guidance on how to use each feature):

1. Process the alarm from the alarm queue.

2. Review and acknowledge the alarms that have occurred in the Alarms tab.

3. If required, view the Details window to see the list of site staff and optionally verify their passcodes.

4. If required, dispatch an investigator and audit the following items:
    a. When they were dispatched
    b. When they arrived

   c. When they left
   d. Their name / employee ID
   e. Any notes such as whether keys were used, the communication means etc

5. If required, notify the Subscriber / Police / Fire auditing the following items:
   a. Who was contacted
   b. Whether they answered
   c. Any notes such as a reference code from the emergency services dispatcher

6. Perform any remaining actions preventing the closure of the event such as completing any required Action Plan steps or acknowledging any alarms.

7. Close the event and provide the outcome.

NOTE: the operator actions can either be guided via an Action Plan (see “Action Plans” section above) or done manually with notes being entered into the audit trail (see “Audit Trail” section above). Action Plans are recommended as it standardizes the handling of the event instead of leaving it up to the operator.

System Failures

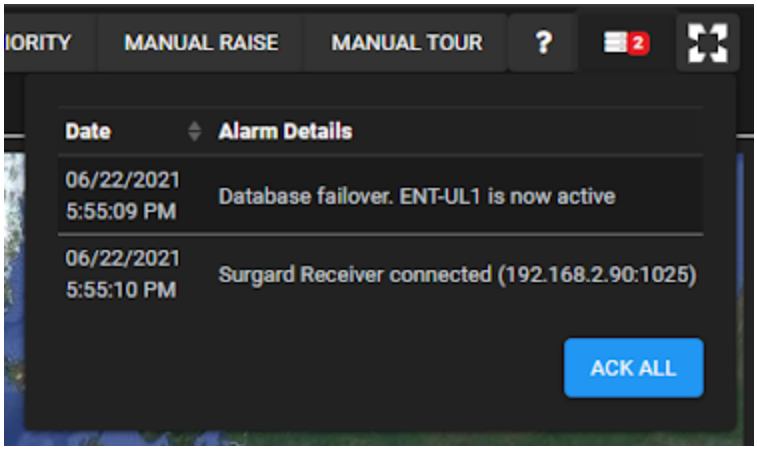
Any system failures will be raised as alarms into the queue screen.

Failover

A database failover will be raised as a System Event stating “Database failover” and noting which server has become the Principal.

If this occurs then the clients will continue as normal as they connect using the NLB IP address as well as any receivers that connect to the shared IP address (Surgard) or are connected to by SureView (DMP).
Any receivers that connect to the current Principal server (Bosch) will need their settings changed to point to the new principal server that is noted in the alarm.

Example of a Database Failover from server #2 to server #1:

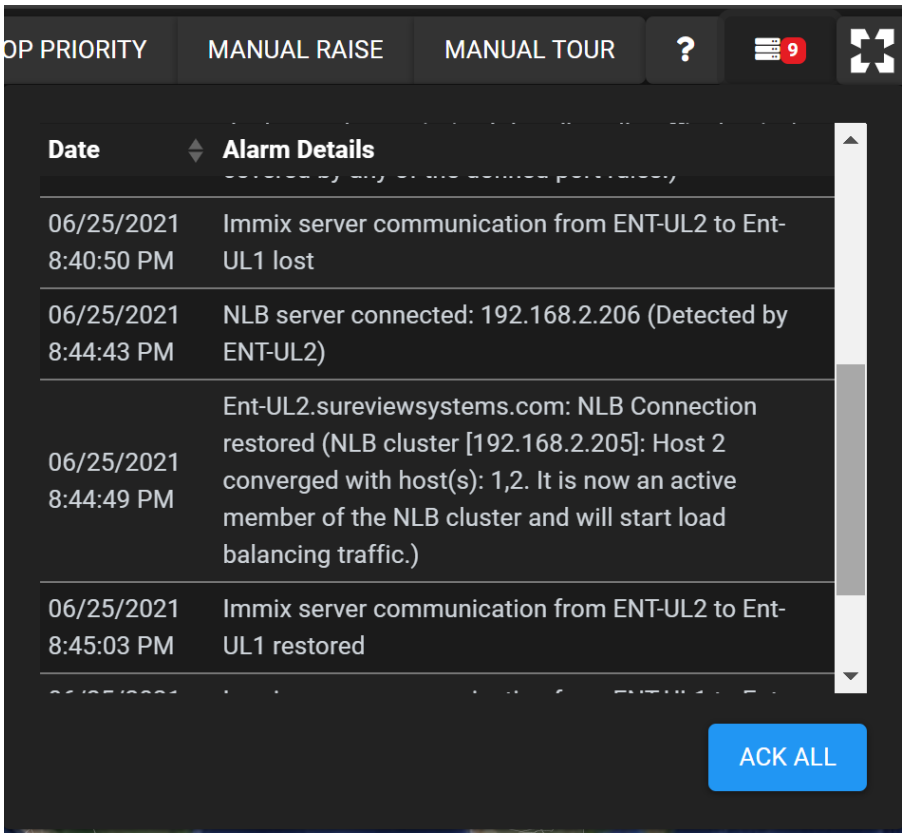


Server Supervision

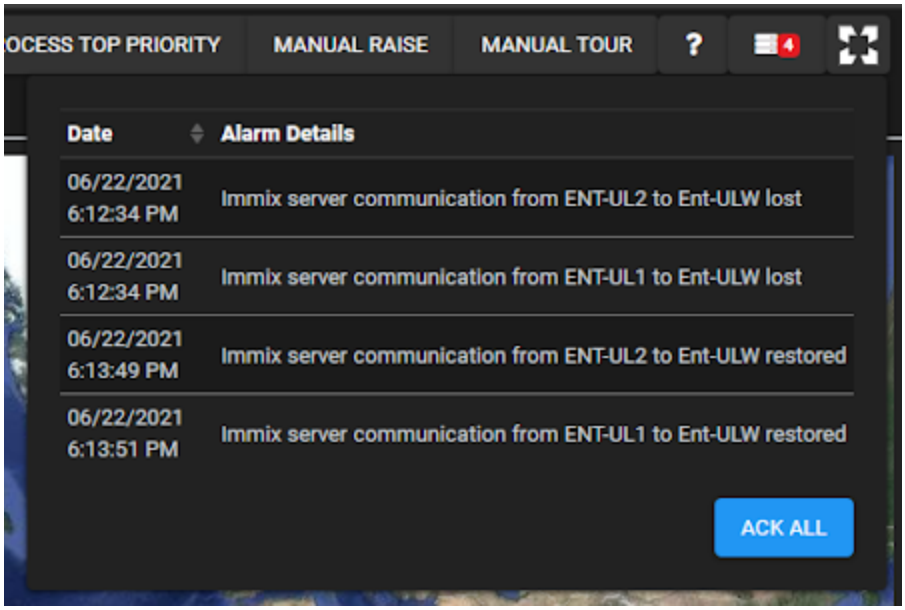
The loss of a server is raised as a System Event stating “SureView server communication from [detecting server] to [lost server]”.

Unless it has caused a failover then no action is required other than notifying your IT team to rectify the problem.

Example of server 2 (the principal at the time) detecting the loss and eventual restore of server:



Example of both servers detecting loss and restore of the Witness:

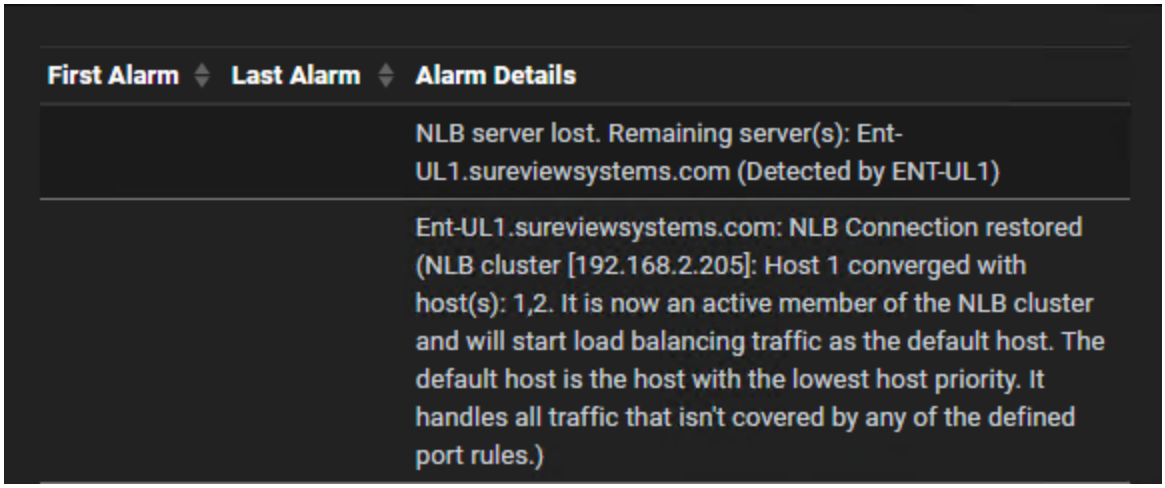


Network Load Balancing Failure

Loss of one of the Network Load Balancing (NLB) connections will be raised as a System Event stating “NLB server lost” and noting which servers are left in the NLB cluster and which server detected the failure.

Unless it has caused a failover then no action is required other than notifying your IT team to rectify the problem.

Example showing server 2 being disconnected leaving server 1 (detected by server 1):



First Alarm	Last Alarm	Alarm Details
		NLB server lost. Remaining server(s): Ent-UL1.sureviewsystems.com (Detected by ENT-UL1)
		Ent-UL1.sureviewsystems.com: NLB Connection restored (NLB cluster [192.168.2.205]: Host 1 converged with host(s): 1,2. It is now an active member of the NLB cluster and will start load balancing traffic as the default host. The default host is the host with the lowest host priority. It handles all traffic that isn't covered by any of the defined port rules.)

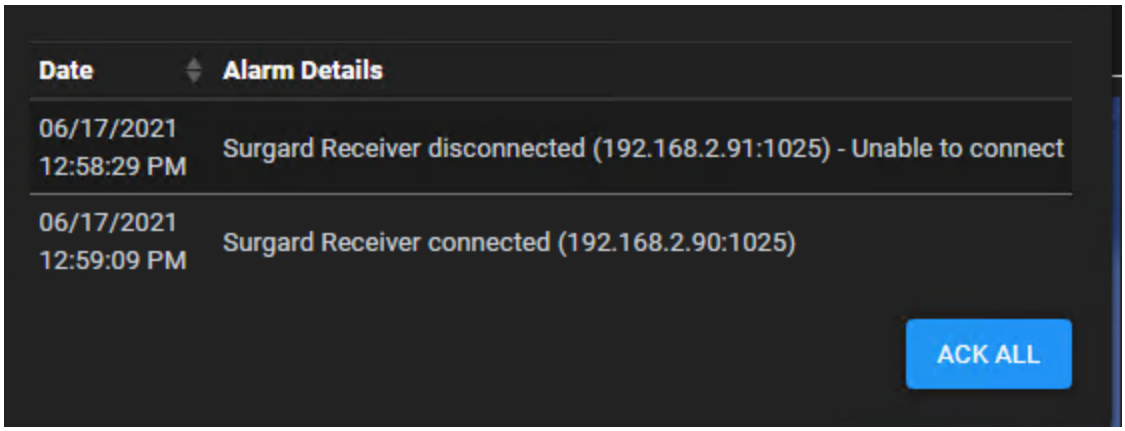
Receiver Supervision

Loss of communication with receivers will be raised stating the receiver having the issue.

This must be raised to your IT team immediately to fix as it means SureView will no longer be able to receive alarms from that receiver which will now be in manual mode printing out signals.

As soon as communication is restored again you will receive a restoration alarm and signals will come back into SureView.

Example of a receiver disconnecting then reconnecting:

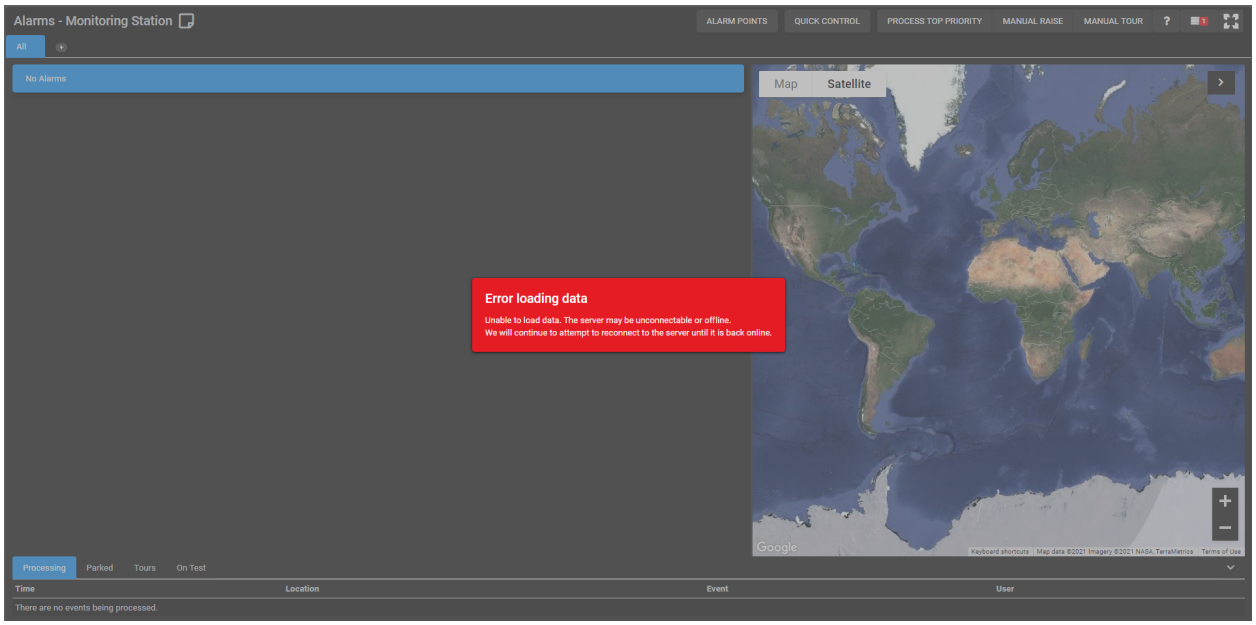


Date	Alarm Details
06/17/2021 12:58:29 PM	Surgard Receiver disconnected (192.168.2.91:1025) - Unable to connect
06/17/2021 12:59:09 PM	Surgard Receiver connected (192.168.2.90:1025)

ACK ALL

Client Connection Loss

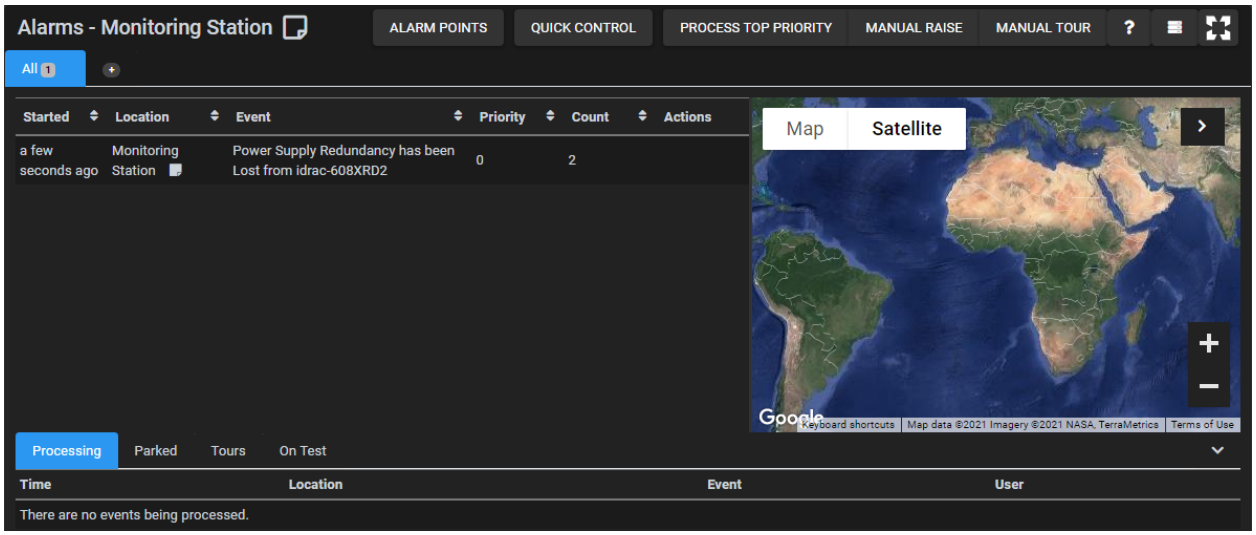
Any loss of connection to the servers (either due to a database failover or NLB disconnection) will result in the interface showing a message stating that it cannot communicate with the servers.
When connection is reestablished the message will disappear and the operator can continue normal use.



Hardware Failure

Any server hardware failure (SNMP alert) will be sent to SureView as an alarm. Unless it has caused a failover then no action is required other than notifying your IT team to rectify the problem.

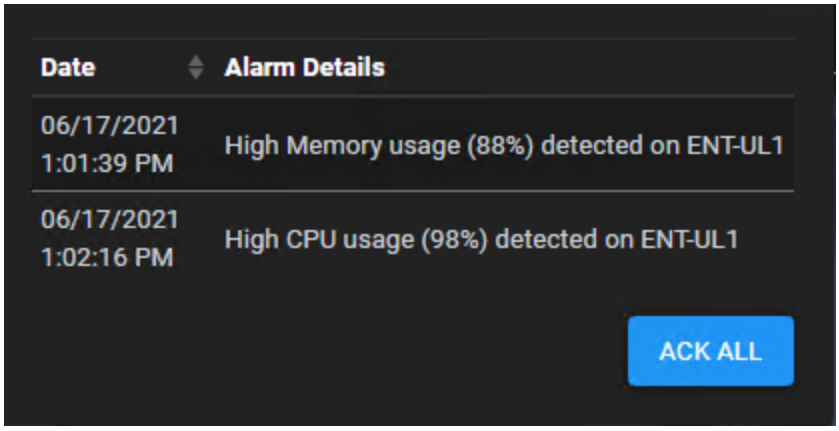
Examples of hardware failure alarms (power supply redundancy lost):



Performance Alert

Any performance alert will be sent to SureView as an alarm. Unless it has caused a failover then no action is required other than notifying your IT team to rectify the problem.

Example performance alerts:



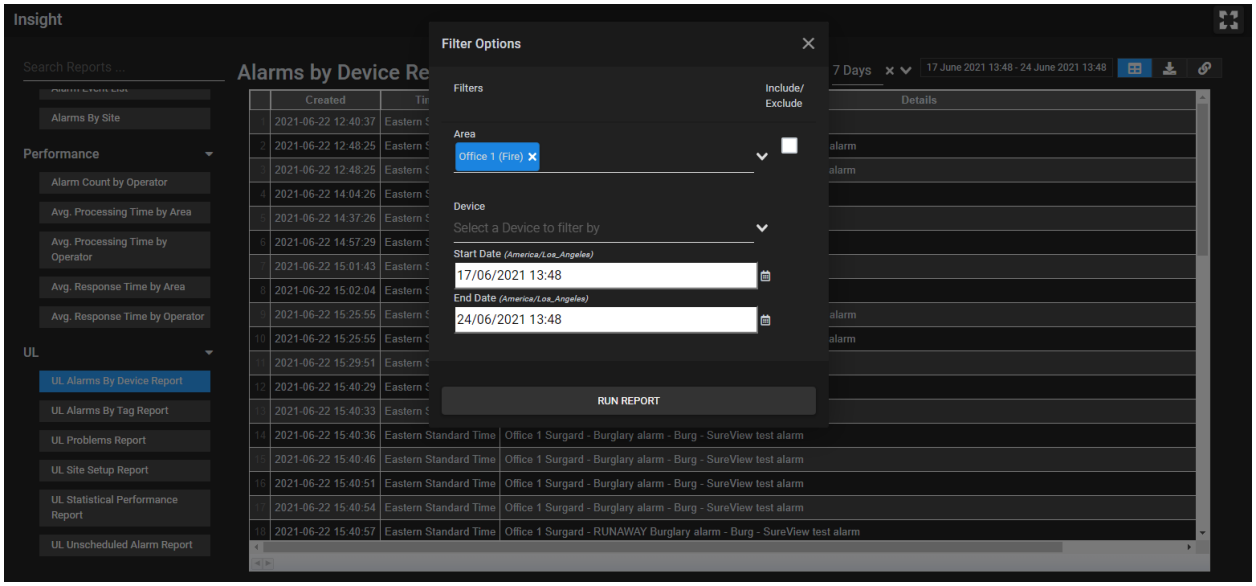
Reports

The majority of reports are accessed via the “Insight” menu item, with the only exception being the event report which comes from the “Event Search” item.

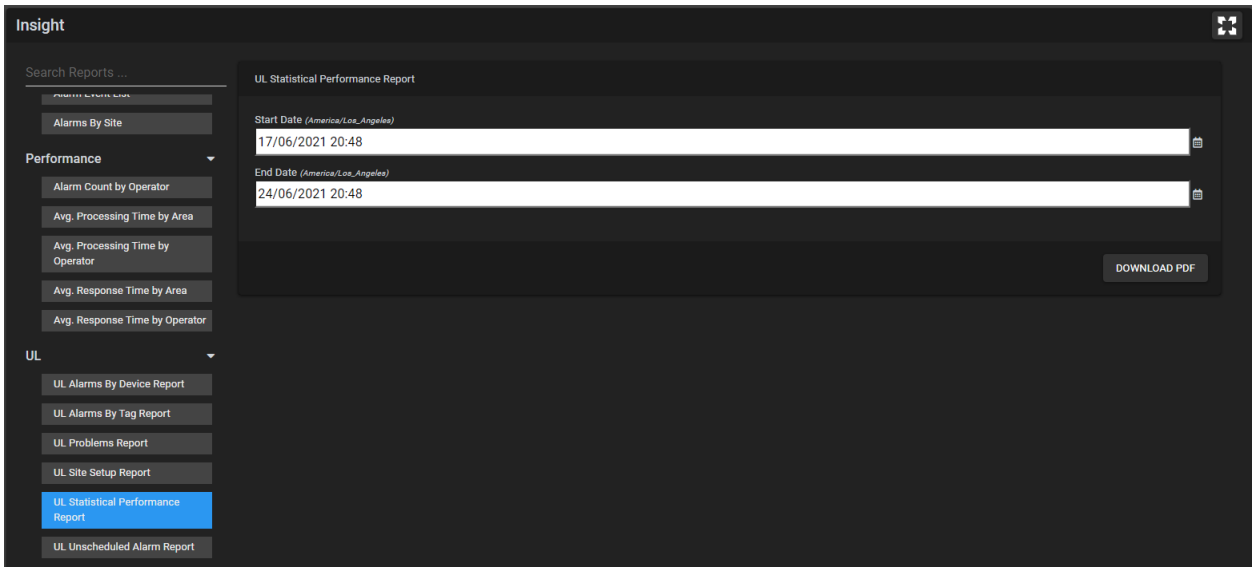
In Insights the list of reports is provided on the left, and there are two types of report:

- Tabular reports display directly in the interface with a “Filter” button to filter the results by report-specific values (times, site etc) and a button to download the details as CSV (you can also use the browser’s “Print to PDF” feature to obtain a PDF)
- Non-tabular reports just provide the filter parameters directly and provide a button to download a PDF.

A tabular report with filter options open:



A non-tabular report:

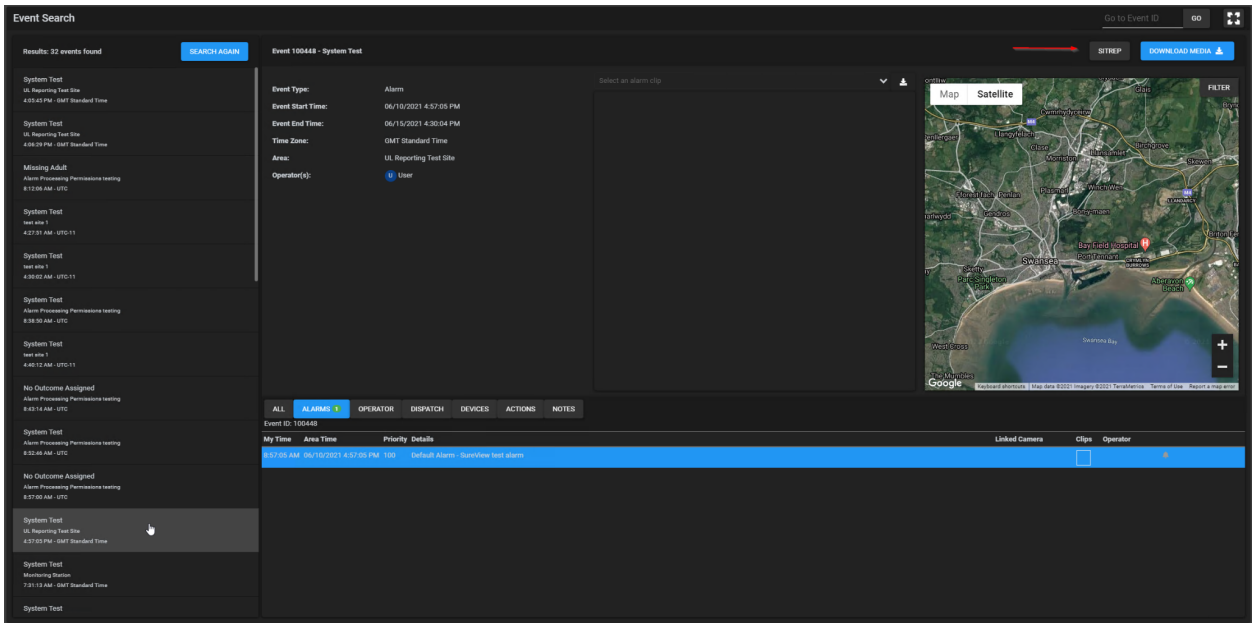


Situation Report (Event Report)

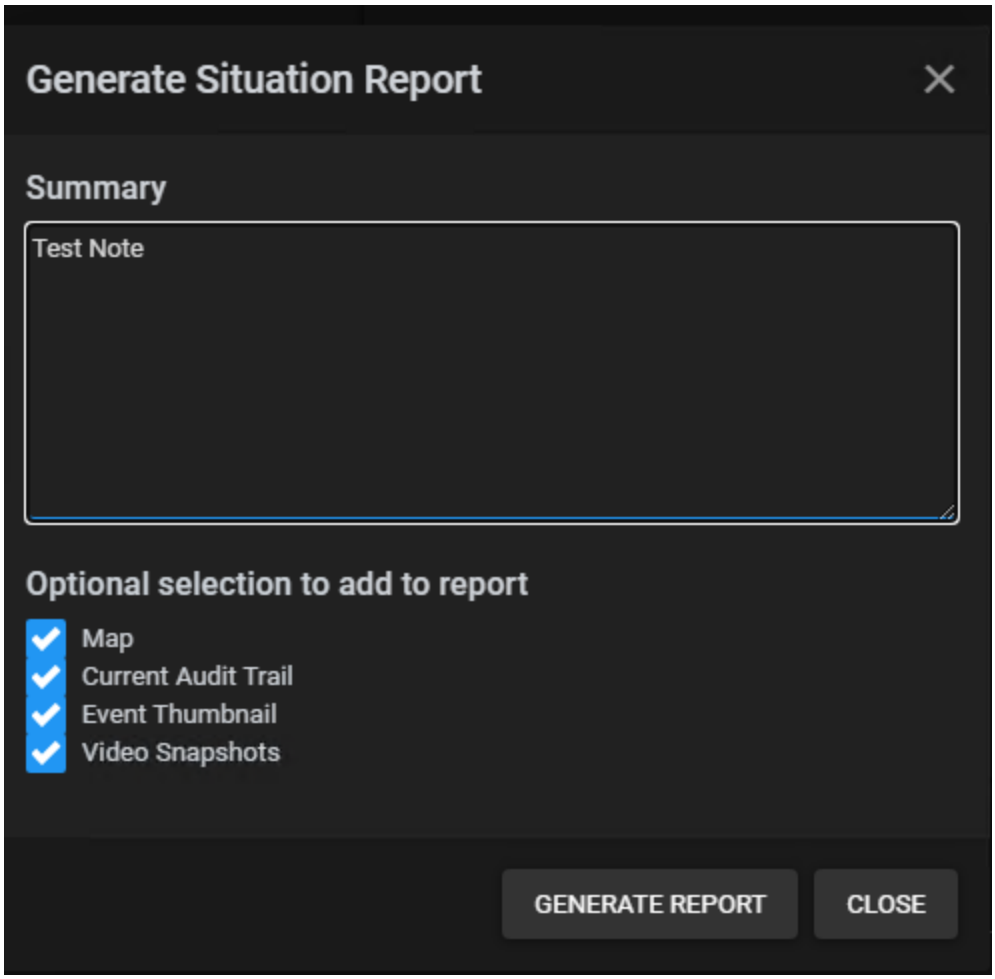
The Situation Report (SitRep) can be viewed/downloaded from the Event Search screen by finding the given event and clicking the “SitRep” button.
This report provides:

1. The details of the site, including address and UL details.
2. The full audit trail output of the event including any alarms and operator actions (such as investigators being dispatched, arriving, and leaving the site, and notifications of subscribers and emergency services) with timestamps and elapsed times for each.

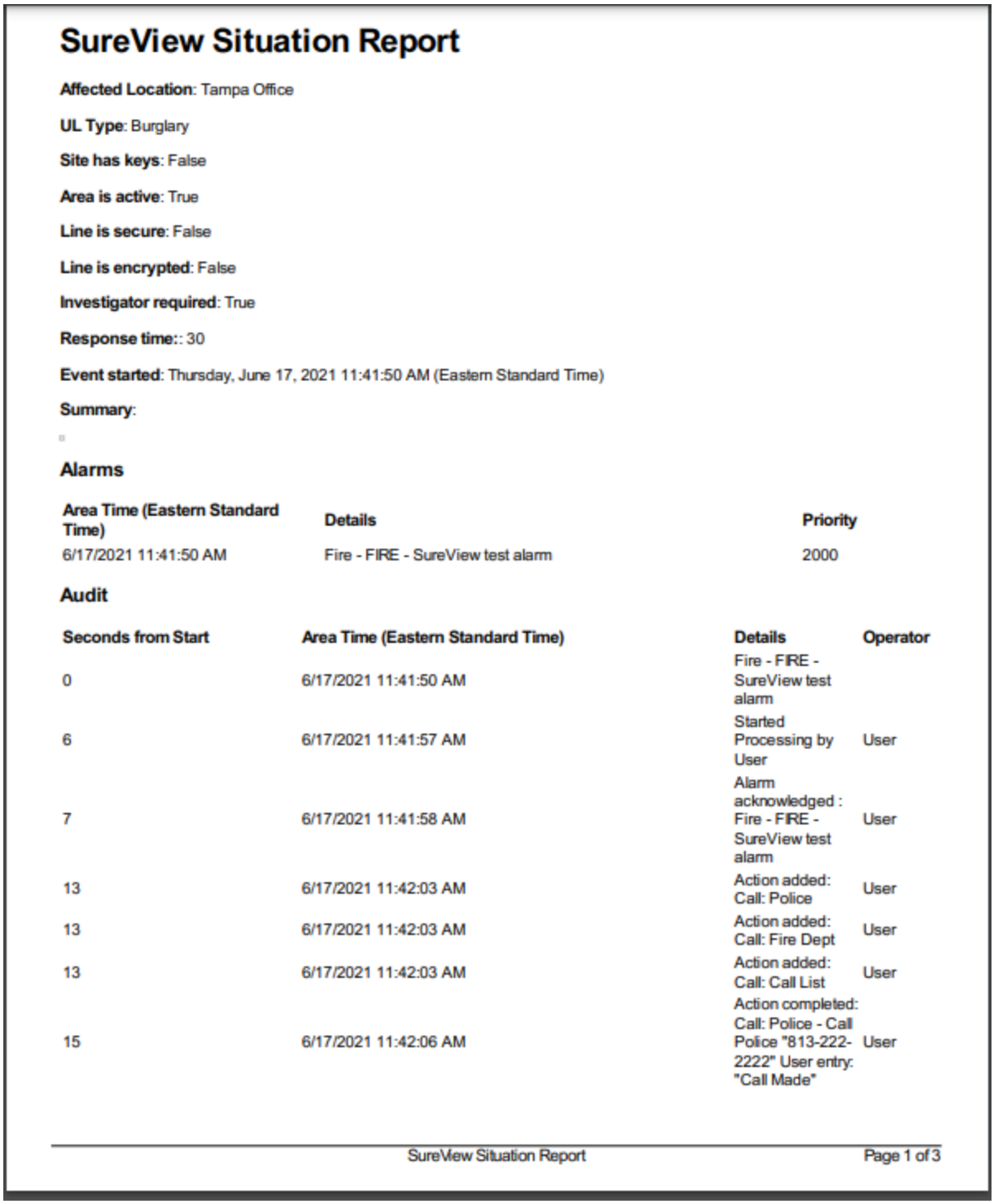
Using Event Search to find an event:



Pop up to select what to include in the SitRep:



Example SitRep:



SureView Situation Report

Affected Location: Tampa Office

UL Type: Burglary

Site has keys: False

Area is active: True

Line is secure: False

Line is encrypted: False

Investigator required: True

Response time:: 30

Event started: Thursday, June 17, 2021 11:41:50 AM (Eastern Standard Time)

Summary:

Alarms

Area Time (Eastern Standard Time)	Details	Priority
6/17/2021 11:41:50 AM	Fire - FIRE - SureView test alarm	2000

Audit

Seconds from Start	Area Time (Eastern Standard Time)	Details	Operator
0	6/17/2021 11:41:50 AM	Fire - FIRE - SureView test alarm	
6	6/17/2021 11:41:57 AM	Started Processing by User	User
7	6/17/2021 11:41:58 AM	Alarm acknowledged : Fire - FIRE - SureView test alarm	User
13	6/17/2021 11:42:03 AM	Action added: Call: Police	User
13	6/17/2021 11:42:03 AM	Action added: Call: Fire Dept	User
13	6/17/2021 11:42:03 AM	Action added: Call: Call List	User
15	6/17/2021 11:42:06 AM	Action completed: Call: Police - Call Police "813-222-2222" User entry: "Call Made"	User

SureView Situation Report Page 1 of 3

User Activity History

The “UL User Activity Report” provides a timestamped list of all actions taken by users including logging in and out and changing settings. Filtering by a specific site allows you to see just the actions taken by users on that site.

Alarms By Device (Change of status)

The “UL Alarms By Device Report” provides a list of all change of status signals. Filtering by a specific site allows you to see just the signals for that site.

Alarms By Tag (Opens/Closes)

The “UL Alarms By Tag Report” provides a list of all open/close signals received and the time they occurred by choosing to filter on the “Open/Close” alarm tag that has been applied to all open/close alarms in setup as described above.

Unscheduled Alarms (Irregular opens/closes)

The “UL Unscheduled Alarm Report” provides a list of all signals that were received outside of their Expected alarm schedule including Open/Close signals.

Problems

The “UL Problems Report” provides a list of all problems on sites.

Statistical Performance

The “UL Statistical Performance Report” provides a statistical analysis of operator acknowledgement time and runner response time.