sureview

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

All materials in this documentation are proprietary and considered confidential to SureView Systems Inc and all affiliates and may not be disclosed without the express written permission of SureView Systems Inc.

The methodology formats and all business applications used herein are copyrighted products of SureView Systems Inc and are only to be used under the written authorization of SureView Systems Inc. Any other use is unlawful. No duplication distribution or alteration is permitted. © 2021 SureView Systems Inc. All rights reserved.

Contents

Contents	3
General	6
Components	7
Minimum Specifications	8
Servers	8
Virtualization	8
Minimum Specifications	10
All physical servers	10
SureView servers (physical or virtual)	10
Witness server (physical or virtual)	10
Workstations	10
Minimum Specifications	11
Receivers	11
Network	12
Software Version	13
System Configuration	14
Pre-Requisites	14
Operating System Installation	14
Network Configuration	15
SQL Server Installation	17
Software Installation	20
Post-Install	22
Mirroring Configuration	22
Manual Failover	22
Forced Service	22
System Settings	24
Features	25
Performance Monitoring	26
Hardware Monitoring	28
Remote Access	30
Tertiary System	31
Logging in and out	32
Password Expiry & Requirements	32
Failed Login Lockout	32

Last User Logout	33
Software Configuration	34
User Permissions	34
Users	36
Event Outcomes	37
Alarm Tags	38
Receivers and Line Profiles	39
Action Plans	39
Sites	40
Site Setup	41
Device Setup	42
Alarm Setup	43
Expected Alarms	45
Contacts (Site Staff and Call List)	47
Dispatch	48
Setup Report	49
Setup Activity	51
Alarm Processing	53
Alarm Queue	53
On Test	54
System Alarms	55
Disarming	56
Alarm Processing	56
Alarms and Restores	57
Audit Trail	58
Site Details	59
Site Notes and Problems	60
Dispatching Guards	61
Action Plans	61
Parking	62
Close and Outcome	63
Standard Alarm Processing Procedure	63
System Failures	65
Failover	65
Server Supervision	65
Network Load Balancing Failure	66
Receiver Supervision	67
Client Connection Loss	68
Hardware Failure	68

Performance Alert	69
Reports	70
Situation Report (Event Report)	71
User Activity History	73
Alarms By Device (Change of status)	74
Alarms By Tag (Opens/Closes)	74
Unscheduled Alarms (Irregular opens/closes)	74
Problems	74
Statistical Performance	74

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 <u>www.ul.com</u>

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

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:

😰 vm1 - Virtual Machines			
9th Cronte / Resister Mill III Console	Edit actions Invested (ECV) C.O. sist		
	p Edit settings - Immix1 (ESXI 6.0 Virtu	ai machine)	
Virtual machine	Virtual Hardware VM Options		he V Ho
SvrA	🔜 Add hard disk 🛛 🛤 Add network ad	dapter 🗧 Add other device	10
🗹 👘 Immix 1	- 🖬 CPU 🛕	10 🔻 💼	10
ImmixWitness	0.000		ness 45
	Cores per Socket	1 * Sockets: 10	
	CPU Hot Plug	Enable CPU Hot Add	
	Reservation	18000 ¥ MHz ¥	
	Limit	Unlimited V MHz V	
	Shares	Normal T 1000	
	Hardware virtualization	C Expose hardware assisted virtualization to the guest OS 👔	
d	Performance counters	Enable virtualized CPU performance counters	
	Scheduling Affinity	Hyperthreading Status: Active Available CPUs: 20 (Logical CPUs) 0, 2, 4-7	
	CPU/MMU Virtualization	Automatic T	
	🕶 🌉 Memory 🛕		
	RAM		
🕄 Recent Tasks			
Task	Reservation	16384 V MB V	Result
Search Datastore		Reserve all guest memory (All locked)	Completed successfully
Acquire Gim Services Ticket			Completed successfully
Acquire Cim Services Ticket		Save	Completed successfully

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

Hyper-V Manager	Settings for Sureview1 on VM1	- 🗆 X	X
File Action View Help	Sureview1 ~	 ↓ 0 	
	Sureview1	Processor You can modify the number of virtual processors based on the number of processors on the physical computer. You can also modify other resource control settings. Winther of virtual processors:	tions II New Import Virtual Machine Hyper-V Settings Virtual Switch Manager Virtual SAN Manager Virtual SAN Manager Virtual SAN Manager Inspect Disk Sopervice Remove Server Refresh View Help Terview1 Connect Settings Turn Off Shut Down Save Pause Reset
JI		QK Cancel Apply	Checknoint

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:

Dev	ce Setup						22
و	Create new device						×
Se	Device Information	Device nu	II Details		Edge Deta	ails	
ті		Title: *			Edge URL:		
Bi		Area: *		~	Edge User:		
		Type: *	Search	^	Edge		
		Host:	Bosch D6600 DMP		Password :		
		Port:	Dynamic Host Generic Email Alarm		A		1
		Username	Generic Stream		Additiona	ai Detaiis	
			Manual Raise Surgard System 3 (TCP)		Receive undefined alarms:	•	
		Password :	Password		Log disarm	red	
					alarms:		
						SAVE CAN	ICEL

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.

	sureview	
	Username 	
	Password	
	LOGIN	
Server: ENT-UL1	FORGOT PASSWORD?	
Server: ENT-UL1 v1.4.25016.0	FORGOT PASSWORD?	

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

1			System		_ 1	n x
	🕘 💿 🔹 🏌 🕎 🕨 Control P	Panel + System and Security + Sy	rstem	~ ¢	Search Control Panel	Q
	Control Panel Home	View basic information	about your computer			•
0	Device Manager	Windows edition				
6	Remote settings	Windows Server 2012 R2 D	atacenter			
۲	Advanced system settings	© 2013 Microsoft Corpora	tion. All rights reserved.	,Windo	ows Server [®] 2012	R2
		System				
		Processor:	Intel(R) Xeon(R) Platinum 8272CL	CPU @ 2.60GHz 2.59 G	Hz	
		Installed memory (RAM):	8.00 GB			
		System type:	64-bit Operating System, x64-bas	ed processor		=
		Pen and Touch:	Limited Touch Support with 11 To	ouch Points		
		Computer name, domain, and	workgroup settings			
		Computer name:	Sureview1		🛞 Change setti	ngs
		Full computer name:	Sureview1			
		Computer description:				
	See also	Workgroup:	WORKGROUP			
	Action Center	Windows activation				
	Windows Update	Windows is activated Rea	d the Microsoft Software License Te	erms		~

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 gualified 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.local192.168.2.62 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:

 \times hosts - Notepad <u>File</u> <u>Edit</u> Format <u>View</u> <u>H</u>elp # 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 localhost # ::1 192.168.2.60 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:

File Cluster Host Options Help • • •	
Ketwork Load Balancing Clusters Host configuration information for hosts in cluster ent-ul sureviewsystems.com (192.168.2.205) Host onfiguration information for hosts in cluster ent-ul sureviewsystems.com (192.168.2.205) Host onfiguration information for hosts in cluster ent-ul sureviewsystems.com (192.168.2.205) Host onfiguration information for hosts in cluster ent-ul sureviewsystems.com (192.168.2.205) Host onfiguration information for hosts in cluster ent-ul sureviewsystems.com (192.168.2.205)	
😑 🗐 [ent-ul.sureviewsystems.com (192.168.2.205) Host (Interface) Status Dedicated IP addresse Dedicated IP addresse	
E ENT HI 1/NI D)	
ENT-UL2(NLB) Converged 192.168.2.206 255.255.0 1 started, persist s	
ENT-UL2(NLB) Converged 192.168.2.207 255.255.0 2 started, persist s	
Log En Date Time Cluster Host Description	—
001 6/17/2021 6:48:14 AM NLB Manager session started	
0002 6/17/2021 6:48:15 AM Loading configuration information from host "Ent-UL1.sureviewsystems.com" for cluster 1	
0003 6/17/2021 6:48:15 AM Loading configuration information from host "Ent-UL2.sureviewsystems.com" for cluster 1	

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.

1	SQL Server 2012 Setup	_ _ ×
Feature Selection Select the Standard features to i Setup Support Rules Setup Role Feature Selection	Eeatures: Instance Features ✓ Database Engine Services SQL Server Benlication	Feature description:
Installation Rules Instance Configuration Disk Space Requirements Server Configuration Database Engine Configuration Error Reporting Installation Configuration Rules Ready to Install Installation Progress Complete	Got Server Replication Got Server Replication Got Server Replication Got Services Got	controlled access and rapid transaction processing and also provides rich support for sustaining high availability. The Database Engine also provides support for the utility control point in the SQL Server Utility. Only Prerequisites for selected features: Already installed: Windows PowerShell 2.0 Microsoft Visual Studio 2010 Redistributables Microsoft .NET Framework 4.0 Windows feature(s) to be turned on: Microsoft .NET Framework 3.5
	Select All Unselect All Shared feature directory: C:\Program Files\Micros Shared feature directory (x86): C:\Program Files (x86)\M	ioft SQL Server\
	< <u>B</u> ack	Next > Cancel Help

SQL Server feature installation:

SQL Server service account same on all servers:

🔍 Services						_		×
File Action View	<u>H</u> elp							
	à 🗟 🛛 📷 🕨 🔳 🕪							
🔍 Services (Local)	Services (Local)							
	SQL Server (MSSQLSERVER)	Name	Description	Status	Startup Type	Log On As	5	^
	Stop the service Pause the service Restart the service Description: Provides storage, processing and controlled access of data, and rapid transaction processing.	Sensor Service Server Shell Hardware Detection Simple Mail Transfer Protoc Smart Card Smart Card Device Enumera Smart Card Removal Policy SNMP Trap Software Protection Special Administration Con Server Verifier	A service fo Supports fil Provides no Transports e Manages ac Creates soft Allows the s Receives tra Enables the Allows adm	Running Running Running Running	Manual (Trig Automatic Automatic Disabled Manual (Trig Manual Automatic (D Manual Manual	Local Syst Local Syst Local Syst Local Serv Local Syst Local Syst Local Syst Local Syst Local Syst	e e e ice e e ice S e	
		SQL Server (MSSQLSERVER)	Provides sto	Running	Automatic	.\svservice	2	
		 SQL Server Agent (MSSQLS SQL Server Browser SQL Server CEIP service (MS SQL Server VSS Writer SSDP Discovery State Repository Service Still Image Acquisition Events Storage Service Storage Tiers Management Superfetch 	Executes jo Provides SQ CEIP service Provides th Discovers n Provides re Launches a Provides en Optimizes t Maintains a	Running Running Running	Disabled Disabled Automatic Manual Manual Manual Manual Manual Manual	Network S Local Serv NT Service Local Syst Local Syst Local Syst Local Syst Local Syst Local Syst Local Syst) rice e rice e e e e	v
	Extended Standard							

SQL Configuration to enable TCP on port 1433:

🚂 Computer Management		- 🗆 ×
File Action View Help		
← ⇒ 2 📰 🖾 🗟 🖬		
🜆 Computer Management (Local)	Protocol Name Status	Actions
✓ [™] System Tools	Shared Memory Enabled	Protocols for MSSOI SERVER
> 🕑 Task Scheduler	Named Pipes Disabled	
> 🛃 Event Viewer	TCP/IP Enabled	More Actions
> 👩 Shared Folders		TCP/IP
> 😣 Local Users and Groups		Mara Actions
> (N) Performance	Protocol IP Addresses	More Actions
Device Manager		
V 🔄 Storage	TCP Dynamic Ports	
> Windows Server Backup	ICP Port 1433	
Disk Management	Active Vec	
 Services and Applications Internet Information Services (IIS) Managements 	Enabled	
S an internet information services (iis) Mana	IP Address 2001:0:34f1:8072:3417:3044:3f57:	
Soprisos	TCP Dynamic Ports	
WMI Control	TCP Port 1433	
SOL Server Configuration Manager	□ IP6	
SOL Server Services	Active Yes	
SOL Server Network Configuration (Enabled No	
SQL Native Client 11.0 Configuration	IP Address fe80::3417:3044:3f57:fd34%6	
SOL Server Network Configuration	TCP Dynamic Ports	
	ILP PORT 1455	
> 🚇 SQL Native Client 11.0 Configuration	TCP Dynamic Ports	
· •••	TCP Port 1433	
	×	
	TCP Port	
	TCP port	
	OK Cancel Apply Help	
L		
<	·	

SQL Ports allowed in Firewall:

@	Windows Firewall with Advanced	l Security	_ 🗆 X
File Action View Help			
🗢 🔿 🙍 🖬 🗟 🖬			
Windows Firewall with Advance	nbound Rules	Actions	
Cuthound Rules	lame Group ^	Profile Enabled Acti A Inbound Rules	5 🔺
Connection Security Rules	Admin	All Yes Allo 🙀 New Rule	
Monitoring	SOL	All Yes Allo V Filter by Prof	ile 🕨 🕨
	BranchCache Content Retrieval (HTTP-In) BranchCache - Content Ret	rAll No Allo ≡ 🍸 Filter by Stat	e 🕨
	SQL Properties	No Allo 🏹 Filter by Grou	up 🕨
	General Programs and Services Remote Comput	ters No Allo View	•
	Protocols and Ports Scope Advanced Local Principals Remot	e Users No Allo Refresh	
	Protocols and ports	Yes Allo 📑 Export List	
	Protocol type: TCP	Yes Allo 🛛 Help	
	Protocol number: 6	Yes Allo SOL	
		Yes Allo Disable Rule	
	Local port: Specific Ports V	Yes Allo	
	1433, 5022	Yes Allo	
	Example: 80, 443, 5000-5010	Yes Allo X Delete	
	Remote port: All Ports V	Yes Allo Properties	
	5 Firmula: 00, 442, 5000,5010	Yes Allo	
	Example: 80, 445, 500-5010	Yes Allo	
	Internet Control Message Protocol Customize	Yes Allo	
		No Allo	
		No Allo	
	ā	. No Allo	
		Yes Allo	
	OK Cancel	Apply	
		2°77	

SQL Version information:

	Quick Launch (Ctrl+Q)
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>P</u> roject <u>T</u> ools <u>W</u> indow <u>H</u> elp	
💿 - 💿 🎦 - 'n - 😩 🔛 📲 🗿 <u>N</u> ew Query 🗿 🖓	🔉 📾 🎰 🕆 라 お 🛛 ツ - ペ - 🛛 🛛 🔎 🚆
🗧 🎬 🚽 🕹 Execute 🔳 🗸	' 15 ē e 17 15 @ e a a o 4 % [*]
Object Explorer 🔹 म 🗙	
Connect 🕶 🍟 🎽 🝸 🖒 🤸	
Sureview2.sureviewsystems.com (SQL Server 11.0.7001.0 - SureviewW.sureviewsystems.com (SQL Server 11.0.7001 -)	
< >	
✓ Ready	

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):

5 SureView Package Installer v1.4	4.1.2			—		×
sureview						
	Database Connection					
	Server :					
	Failover Partner :	Sureview2.mydomain.local				
	Authentication :	Windows Authentication				
		Test				
BACK					Next	

Installer component packages:

🌆 Su	ureView Package Installe	er v1.4.1.2			—		×
	sureview						
Search	i:			Select All	Upd	lated	None
	Rodeer Service	nocinotated	connections				*
 ✓ 	Scheduler	Installed (Same)	Runs automated data tasks.	1.28.0.18			
✓	SureView-DB	Installed (Newer)	Installs database for SureView Enterprise	1.4.24742.0			
v	SureView-DS	Installed (Newer)	Installs data service for SureView Enterprise	1.4.24729.0			
	SureView-Sync	Not Installed	Installs the SureView Sync service, allowing for continuous synchronization of data between SureView and 3rd party systems	1.2.5.0			
✓	SureView-UI	Installed (Newer)	Installs user interface for SureView Enterprise	1.4.24684.0			
	View	Not Installed	UI for view interface	1.28.0.45			
	View Data Service	Not Installed	Stand alone data service for View interface function	1.28.0.20			
	Watchdog	Installed (Newer)	Installs SureView Watchdog service for system monitoring	1.0.0.7			
Int	egration			Select All Up	lated	None	^ ,
	BACK					Next	

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 Properties - Immi	xCloud		– 🗆 X
Select a page General	🖵 Script 🔻 😯 Help		
 Files Filegroups Options Change Tracking 	Ensure that security is database.	configured for mirroring this	Configure Security
 Permissions Extended Properties 	Server network addresse	S	
 Mirroring Transaction Log Shipping 	Principal:	TCP://Ent-UL1.sureviewsystems.com	Start Mirroring
Query Store	Witness:	TCP://Ent-ULW sureviewsystems.com	Pause
	Note: Use fully-qualifie	ad TCP addresses. For example:	Failover
	Operating mode		
	O High performance to the mirror.	(asynchronous) Commit changes at the	principal and then transfer them
Connection	 High safety withou principal and mirror 	t automatic failover (synchronous) – Alwa r	ays commit changes at both the
Server: ENT-UL1 Connection:	 High safety with au Commit changes a automatic failover 	utomatic failover (synchronous) Require it both the principal and mirror if both are to the mirror if the principal becomes una	es a witness server instance. available. The witness controls vailable
ENT-UL1\AdministratorSV			
v₩ <u>View connection properties</u>	Status: Synch synchr	ronized: the databases are fully ronized	Refresh
Progress			
Ready			
			OK Cancel

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:

Settings		23
器 Endpoints	Search	
Events	Areas Security : System Area	
🖿 Interface	Search Default Lockout Period (System only)	
🗳 Maps	System Area Number of hours for incorrect answer user Monitoring Station	lockout
내 Reports	Failed Login Max Attempts (System or	ly]
Security	Bank (Burg) 5 Hotel (Non-UL Fire) Max number of login attempts before User	lockout
오 License	Museum (Non-UL Burg) Failed Login Lockout Minutes (System Office 1 (Fire)	t only]
Security	Office 2 (NI Burg) Customer Group	
* 0-+ <		SAVE

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:

N Performance Monitor	-	\square ×
🔕 File Action View Window Help		_ 8 ×
🗢 🔿 🔁 📷 💥 🖼 🗟 🛛 🖬	DataCollector01 Properties ×	
Name Name	Performance Counters File	
Monitoring Tools DataCollector0	Performance counters: 1	_20210625-000
V 🔓 Data Collector Sets	\LogicalDisk(_Total)\% Free Space Add	
🗸 💐 User Defined	Wemory Available MBytes	
Server Manager Performance	Wetwork Interface(*)\Bytes Total/sec	
	Processor(_local) (% Processor lime	
System		
System Performance		
Event Trace Sessions		
🔚 Startup Event Trace Sessions		
V 🙀 Reports	Log format:	
V 🖳 User Defined	Binary 🗸	
Server Manager Performance	Sample intervalu	
ENT-UL1 20210625-000		
ENT-UL1_20210625-000	Minutes V V V	
> 💽 System	Data <u>s</u> ource name:	
	· · · · · · · · · · · · · · · · · · ·	
	OK Cancel Apply	
< > <		>

Windows Performance Monitor - data collector report:



SureView performance alert settings:

Sett	tings			2
		^		
N	Maps	>	Areas	Health Check : System Area
600	Reports	>		Alert CPU Percent [System only]
>	Security	>	Sustam Arag	80
\$	Setup	>		
	Storage	>		Alert RAM Percent (System only)
			Bank (Burg)	80
Syste	em	~	Hotel (Non-UL Fire)	RAM usage at which to send alerts
			Museum (Non-UL Burg)	Alert Drive Percent [System only]
Hea	lth Check		Office 1 (Fire)	
			Office 2 (NI Burg)	20
Syst	tem		Customer Group	
		- 1	Alarm Processing Permissions testing	
			Site Details Testing	
CONF	GURATION		UL Reporting Test Site	
	Filestores			
	<	Ÿ		SAVE

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):

Alarms - Monitoring Station 🖵	ALARM POINTS	QUICK CONTROL	PROCESS TOP PRIORITY	MANUAL RAISE MANUAL TOUR	? ≡ 🚼
Started \$ Location \$ Event	\$ Prio	ority 🗢 Count 🗢	Actions	Satellite	
a few Monitoring Power Supply Redunda seconds ago Station - Lost from idrac-608XR	ncy has been D2		6 22		AN
			John		y M
				P 129	
			7.52	And A Co	+
			GooReyboard	d shortcuts Map data ©2021 Imagery ©2021 NASA, '	TerraMetrics Terms of Use
Processing Parked Tours On Test					~
Time Location			Event	User	
There are no events being processed.					

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:

SureView	× +				O		[×
\leftrightarrow \Rightarrow G	ent-ul.sureviewsystems.com/immixcc/#/login			٤,	2		٠	9	
		🕞 🖬 Elements Console So		Security \times		03		: :	
		â Overview	Sec	curity overvie	w				
		Main origin (secure)							
	Sureview Username Password LOGIN FORGOT PASSWORD?	 https://ent-ul.sureviewsystems.com Secure origins https://fonts.googleapis.com https://fonts.gstatic.com 	τι •	his page is see Certificate - va The connectio trusted server Secure Certific View certifi Connection - : The connectio authenticated X25519, and A Resources - al All resources of	cure (v lid and ti n to this certificat ate Auth cate ecure co n to this using TL ES_256_C served s n this pa	alid H rusted site is u e issuec ority - C onnectio site is e S 1.2, EC GCM. securely age are :	TTPS) sing a by Gc 22. n settii DHE_f SDHE_f	valid, Dadd ngs ed and ISA wit	
Server: ENT-UL1 v1.4.24909.0									

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

🛃 IIS Crypto	- 🗆 X
IIS (Crypto 2.0
Schannel	Templates Load and save built in or user defined templates. Select a built in template from the drop down box or load your own by clicking the open button. After a template is loaded, click the Apply button to save changes to the computer.
Cipher Suites	FIPS 140-2 Image: Complete Name: FIPS 140-2 Description: Image: Complete makes your server FIPS 140-2 compliant. It is similar to the Best Practices template, however, it is not as secure as Best Practices because some of the weaker DHE cipher suites are enabled. Last Undated: 2016-05-28
(i) About	Best Practices Apply

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).

	surevie	ew
	level1	
	Your password has expired	
	LOGIN	
Server: ENT-UL1 v1 4 25016 0	FORGOT PA:	ssword?

Failed Login Lockout

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

sureview	
level1	
You have been locked out due to too many password attempts.	
LOGIN	
FORGOT PASSWORD?	
Server: ENT-UL1	

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.

Alarms - Monitoring Station	י 🕞 👘	ALARM POINTS	QUICK CONTROL	PROCESS TOP PRIORITY	MANUAL RAISE		? ≣	23
All +								
No Alarms				Мар	Satellite			>
							SIL	
		You a	re the last Operator	logged in	×			
		You are the last op	perator viewing the alarr	n queue, do you wish to contin	ue?			
				CANCEL	ок			+
				Gonela	d shortcuts Map data ©20	21 Imagery ©2021 NASA, Terra	Metrics Terms	s of Use
Processing Parked Tours								
Time	Location			Event		User		
There are no events being processed.								

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:

immix	Monito	ring St			🙎 User 🗕 🗎 Logout			
Dashboard	Alarms	Setup	Reports	Events Came	eras Systen	1		HELP & SUPPORT
SETUP								
What wou	ld you like to do?		1					
#	SITES		1	USERS	z	SCRIPTS	-	SETTINGS
	🔮 Add a Site			😏 Add a User		🚱 Add a Script		🧪 Edit Settings
	🧪 Edit Sites			🧪 Edit Users		🧪 Edit Scripts		
	📀 Data Import	t						

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:

Permissions		11
User Roles	User Groups	
User Roles a	re lists of permissions. A user is not directly given a role - roles are assigned to groups, and users then are added to those groups.	
	ADD RG	DLE
Role Name	Permissions	T
Administrator	CanDownloadEventSearchMedia CanUsekbobie CanViewMobileRaise CanEditMobileRaise CanEditMobileRaise CanViewActivityReportReport CanViewAcamCountbyNoreaReport CanViewAcamCountbyNoreAcamCountbyNoreaReport CanViewAcamCoun	ß
Level 1	CanProcessAlarms CanAccessManualTour CanViewSystemEvents	ľ
Level 2	CanProcessAlarms CanDisarmSites CanAccessManualTour CanViewSystemEvents CanViewSiteArmedState	ľ
Level 3	CanProcessAlarms CanDisarmSites CanDisarmSitesExtended CanViewSiteSetup CanEditDeviceSetup CanEditSiteSetup CanOvleteDisableSite CanAccessManualTour CanViewSystemEvents CanViewSiteArmedState CanTriggerTestMarm	ľ
Level 4	CanProcessAlarms CanDisarmSites CanDisarmSitesExtended CanViewSiteSetup CanEditDeviceSetup CanEditSiteSetup CanEditUserBernissions CanEditUserGroups CanAccessManua Tour CanViewSystemEvents CanViewSiteArmedSitate CanTriggerTestAlarm CanEnableDisableUsers	ß

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



Users

Ilsers'

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.

000/0.								
Users								23
Search								DD USER
Username	🔶 Full Name	🔶 Area	🔶 User Group	Email 🔶 Telephone	💠 Cell 💠 Available as Contact	🗢 Mobile Enabled	🔶 User Enabled	♦ ▼
User	User	Monitoring Station	Administrator					ľ
Levei1	Level 1 Operator	Monitoring Station	Level 1					ľ
Level2	Level 2 operator	Monitoring Station	Level 2				~	ľ
Level3	Level 3 Operator	Monitoring Station	Level 3					ľ
Level4	Level 4 Operator	Monitoring Station	Level 4				×	ľ
Level5	Level 5 Operator	Monitoring Station	Level 5				×	ľ
Admin1	Admin1	Monitoring Station	Administrator		×	×	~	٥

Creating a user including the password complexity:
Users				23
Search		Add User ×		
		Username:*		
Username	🔶 Full Name 🕴	joe.bloggs	led 🔶 User Enabled	÷ T
User				ľ
Level1		Password:		ľ
Level2		Must be at least 6 absorber(a) long		ľ
Level3		X Must have at least 1 number(s)		Ľ
Level4		X Must have at least 1 capital letter(s)		Ľ
Level5		 Cannot have more than 3 consecutive characters in a row Cannot have more than 3 consecutive characters matching the username 		Ľ
Admin1		Cannot have more than 3 consecutive characters in ascending or descending numeric/alphabet i.e. myPasswordABC or		
		Full Name:" Joe Bloggs Email:		
		User Group:		
		Level 1 M		
		Area: *		
		Monitoring Station		
		ADD CLOSE		

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:

Event Category Setur	D										
									ADD EVI	ENT CATEG	ORY
Title	Area Name	Event	Tour	Incident	Preserve	Raise Dispatch	Raise Incident Report	Activity Category	Mobile Quick Close	Parked Note	T
Building wide Emergency	Monitoring Station	~	~								ľ
Active Shooter	Monitoring Station	~	~	~							ľ
Bomb Threat	Monitoring Station	~	~	~							ľ
Fire / Smoke	Monitoring Station	~	~	~							ľ
Powder / Chemical Incident	Monitoring Station	~	~	~							ľ
Criminal Activity	Monitoring Station	~	~								ľ
Other	Monitoring	~	~								ľ

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:

IANAGE SETTINGS FOR: MC	DNITORING STATION			
i Ham da cattinga mark2				
L HOW DO Settings Work?				
Alarm Tags Event Outcomes	Public Holidays Disarm Reasons	s Preferences Routing Groups	Notification Message Templates	
ALARM TAGS				
ALARM TAGS	INCIDENT	ALWAYS RAISE	DEFAULT ROUTING GROUP	
ALARM TAGS	INCIDENT False	ALWAYS RAISE False	DEFAULT ROUTING GROUP	/ ×
ALARM TAGS TITLE Open / Close	INCIDENT False n Tags applied to this site and its sub	ALWAYS RAISE False	DEFAULT ROUTING GROUP	/ *

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.

ashboard Alarms Setup	Reports Events C	Cameras System			HELP & SUPP
Server Status	SYSTEM DEVICES AND LINI	E PROFILES			
File Stores	CURRENT DEVICES				
Endpoints	DEVICE NAME	DEVICE TYPE	IP/HOST	PORT	
System Settings	Surgard S3	Surgard System 3 (TCP)	192.168.2.90	0	× ×
Licensing					😯 Add a Device
Device Types					
System Events	ADD LINE PROFILE				
System Devices	Surgard line 1				
Services	DEVICE	LINE NUMBER	2		
XML Event Types	Surgard S3	1		×	
External Accounts	Surgard S3	Line number mu contain numerio	ust only c values.	•	
Event Type Configuration				UPDATE	CANCEL
System Log					
System History					

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:

Action Library Action Plans + ADD NEW ACTION PLAN Action Plan: CS Burg C
+ ADD NEW ACTION PLAN CS Burg Fire National Industrial • Dispatch 1 required? • Dispatch 1 Name/ID • Dispatch 1 Communication Means • Dispatch 1 Keys Used • Dispatch 1 Keys Used
CS Burg Fire Yes/No I Required + • • National Industrial • Dispatch 1 required? Condition: Yes Dispatch I Required + • • • Dispatch 1 Name/ID Condition: N/A Input I Required + • • • Dispatch 1 Communication Means Condition: N/A Input I Required + • • • Dispatch 1 Keys Used Condition: N/A Yes/No I Required + • •
National Industrial I Dispatch Condition: Yes Dispatch I Required + II I Dispatch 1 Name/ID Condition: N/A Input Imput
Imput Dispatch 1 Name/ID Condition: N/A Input Imput Imput <t< td=""></t<>
 Dispatch 1 Communication Means Condition: N/A Input Condition: N/A Input Dispatch 1 Keys Used Condition: N/A Yes/No Required + 1
🕴 Dispatch 1 Keys Used Condition: N/A Yes/No 📝 Required 🕂 🍵
i Dispatch 1 Notes Condition: N/A Input Required +
🚦 🕶 Is dispatch 2 required? Yes/No 📝 Required 🕂 🍵
🕴 🕶 Dispatch Condition: Yes Dispatch <table-cell> 📝 Required 🕂 🍵</table-cell>
🔋 Dispatch 2 Name/ID Condition: N/A Input 🏹 Required 🕂 🍵
🔋 Dispatch 2 Communication Means Condition: N/A Input 🇹 Required 🕂 🍵
🕴 Dispatch 2 Keys Used Condition: N/A Yes/No 🏹 Required 🕂 🍵
i Dispatch 2 Note Condition: N/A Input Required +
🕄 Call Call List Call Contact <table-cell> Call Contact</table-cell>
i Call: Police Call Contact <table-cell> Required +</table-cell>

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:

Areas					23
					ADD AREA
Title	Address	Telephone	Alt. Telephone	Summary	T
Monitoring Station					ď
ACME					ď
Bank (Burg)	101 E Kennedy Blvd, Tampa, FL 33602	813-333- 1111			ď
Hotel (Non-UL Fire)	100 W Kennedy Blvd, Tampa, FL 33602	813-444- 1111			ď
Museum (Non-UL Burg)	110 W Gasparilla Plaza, Tampa, FL 33602	813-555- 1111			ď
Office 1 (Fire)	400 N Tampa St, Tampa, FL 33602	813-111- 1111			ď
Office 2 (NI Burg)	400 N Ashley Dr, Tampa, FL 33602	813-222-			ď

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:

Areas		6-1 6-1
	Area 10007 Details ×	
	Title:*	
Title Add	Office 1 (Fire)	т
Monitoring Station	Address:*	ľ
ACME	400 N Tampa St, Tampa, FL 33602	ľ
Bank (Burg) 101	813-111-1111	ď
Hotel (Non-UL Fire) 100	Alt. Telephone:	ľ
Museum (Non-UL 110 Burg) 336		ľ
Office 1 (Fire) 400		ľ
Office 2 (NI Burg) 400	1111	ľ

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:

Dev	vice Setup						23
Ċ	Editing Office 1 Surgard						×
		Device 100	06 Details		Edge Details		
Se	Device Information						
Tit	Cameras 0	Title: *	Office 1 Surgard		Edge URL: Edg	e URL	
Ala							
Ba		Area: *	Office 1 (Fire)	*	Edge User: Edg		
DN							
Но		Туре: *	Surgard System 3 (TCP)	× •	Edge Password:		
Inf		Host:					
Ma							
Mu		Port:			Additional Deta	ails	
Of							
U		Username:			Receive undefined alarms:		
		Password:			Log disarmed		
		Foto Velue			alamo		
		Extra value.			Display edge link:		
		Alarm	Ry Area				
		Grouping:		^ `	Line profile:	Line 1 × •	
					Account number:	1111	
						SAVE CAN	CEL

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:

Alarm Setup											23
Office 1										A	DD ALARM
Alarm Title	Туре	Input1	Input2	Area	Device	Priority	Armed	Auto Handle	Match Geofence		Actions
Open	Opening report			Office 1 (Fire)	Office 1 Surgard	100	~	~	×		B 7
Close	Closing report			Office 1 (Fire)	Office 1 Surgard	100	~	~	×		C A
Fire	Fire alarm			Office 1 (Fire)	Office 1 Surgard	2001	~	×	×		B 7
Panic	Panic alarm			Office 1 (Fire)	Office 1 Surgard	1501	~	×	×		B 7
Medical	Medical alarm	-1	-1	Office 1 (Fire)	Office 1 Surgard	1001	~	×	×		B 7
Burg	Burglary alarm			Office 1 (Fire)	Office 1 Surgard	101	~	×	×		B T
Fire supervisory	Fire supervisory	-1	-1	Office 1 (Fire)	Office 1 Surgard	50	~	×	×		B T
Fire trouble restore	Fire trouble restore	-1	-1	Office 1 (Fire)	Office 1 Surgard	50	~	×	×		B T
Fire trouble	Fire trouble	-1	-1	Office 1 (Fire)	Office 1 Surgard	50	~	×	×		C* 🗸

Example of an alarm being configured:

Alarm Setup						11
		Alarm Details		×		
Office 1						
		Area: *	Office 1 (Fire)			
Alarm Title	Туре			1	atch Geofence	Actions
Open		Device: *	Office 1 Surgard			2
Close						☞ #
Fire		Τυρο: *	Fire alarm			e 7
Panic		rype.				┏ 7
Medical						C 🕹
Burg	Burglary	Title: *	Fire			┏ 7
Fire supervisory						2
Fire trouble restore		Input 1: *	-1			2
Fire trouble						2
		Input 2:	-1			
		Priority: *	2001			
		DELETE	SAVE CLOS	SE		

Example of a Runaway alarm in Alarm Queue:

Alarms -	Monitoring	Station (,	ALARM POINTS	QUICK CO	NTROL	PRC	DCESS TOP PRI	ORITY MANUA	AL RAISE	ACTIVITY LOG	MANUAL TOUR	?		23
All 1	•														
Started 🗢	Location	¢	Event		Prior	ity 🗢	Count	Actions	Мар	Satellit	e				>
a few seconds ago	ACME - Hawtho	orne House	RUNAWA' Burg	f Burglary alarm - Zon	e 1 200					5		Carlo I	1		
									House	1	-			-	22
											15			-	
										afte	74 . I	1	-50		T
									C.e.	Sure	View Systems	2. /			
											1 - 7				
											the fee	-	The	Par	+ 3n
															_
	.	- · -							Google	data ©2021 Imag	ery ©2021 , The GeoIn	formation Group Terms	of Use R	eport a m	hap error
Processing	Parked	Tours C	n lest												<u> </u>
Time			Locatio	n				Ev	ent		Us	ser			
There are no	events being proc	cessed.													

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:

Dashbo	oard Alarms	Satup Raport									
EXP		зецир кероп	s Events	Cameras	System					HELP & SUPPOR	
	ECTED ALARM SC	HEDULE DETAILS -									
Alarm	ns : Armed - Closing	report 🗘				Tin	nes set here are loca	al to the sites timezone	:: (UTC-05:00) Easte	ern Time (US & Canada)	
Si	CHEDULE DATE /	TIME <i>i</i> Click and to set the Monday Tuesday Wednesday Thursday Friday Saturday Sunday Holidays	release at a par end time.	ticular time and	d day on the b	ar to set the st	16	en click and releas	e		
									SAV	CANCEL	

Example of a Not Received alarm in the Alarm Queue:

Alarms -	Monitoring Statio	n 🕞	ALARM POINTS	QUICK CON	TROL	PRO	CESS TOP PRIOR	ITY MANUAL RAISE	ACTIVITY LOG	MANUAL TOUR	?		
All 1	•												
Started 🗢	Location	Event		Priority	, \$	Count	Actions	Map Sate	ellite	-	and the second		>
5 minutes ago	ACME - Hawthorne Hous	e NOT REC Forced	CEIVED - Entrance - Door	200	1		\$		100		-		6
								Che	stnut House	E A	-	7	
									sureviewsystems	Parmley Graha	m		N.
													+
								Google		Map Data Terms	of Use R	eport a m	hap error
Processing	Parked Tours	On Test											~
Time		Locati	ion				Event	1	Us	ser			
There are no	events being processed.												

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

Alarms	- Monitoring S	tation	ALARM POINTS	QU	ICK CONT	ROL	PRC	DCES	S TOP PRIORIT	Y MANUAL RAISE	ACTIVITY LOG	MANUAL TOUR	?		
All 1	•														
Started	Location	¢	Event	¢	Priority	¢	Count	¢	Actions	Map Sate	llite	- Alle	a statem		>
6 minutes ago	ACME - Hawthorn	ne House	UNSCHEDULED - Entrance - Do Forced	or	200				Q	5 HB	E				6
										T	1 B	- ARE			E
										Ches	thut House	E		7	29
										S	ureView Systems	1-1			
												Parmley Graha	am 📀		K
												The second			200
										The sale	-				*1
										Google					-
Processir	ng Parked T	ours C	on Test									Map Data Terms	of Use R	port a m	
Time			Location						Event		U	ser			
There are n	o events being proce	ssed.													

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:

Contacts					5.4
Search		Update Contact			ADD CONTACTS ROLES
Full Name) Area	Personal Information		Contact Information	() Actions
Admin1					
Contact 1		Full Name: *		Email:	
Level 1 Operator		Simon Lane (ID: 40)		simon.lane@acme.com	
Level 2 operator					
Level 3 Operator		Area: *		Telephone:	
Level 4 Operator		ACME		813-444-1111	
Level 5 Operator					
Paul Roberts		Contact Roles: *		Cell:	
Simon Lane (ID: 40)		Site owner ×		813-444-2222	
Test Contact					
User		Role Area: *		Site Password:	C .
		Office 1 (Fire) × Bank (Burg) × Search			
		Address:			
		122 Baker Street			
				Notes	
		Is Area Staff	_		
				Receive Notifications	
				Receive setup change emails	
				Receive incident emails	
		DELETE		CLOSE SAVE	

Adding a contact to a call list:

ng Station				💄 User 🗕 🗎 Lo
Setup Reports E	vents Cameras	System		HELP & SUPPO
LANE (ID: 40)				
Jser Details Upload a P	hoto Vser Roles	Call Lists		
MON LANE (ID: 40)			P	REVIOUS FINISH
START TIME	END TIME	DAY(S)	POSITION	
00 : 00	23:59	 Monday Tuesday Wednesday Thursday Friday 	1	× ×
		 Saturday Sunday Public Holidays 		
00 : 00	23 : 59	 Saturčay Sunday Public Holidays Monday Tuesday Wednesday Thursday Friday Saturčay Sunday Public Holidays 	1	/ X
	ng Station Setup Reports E LANE (ID: 40) Jser Details Upload a P MON LANE (ID: 40) START TIME 00 : 00	Ing Station Setup Reports Events Cameras LANE (ID: 40) Junch State Upload a Photo User Roles Jser Details Upload a Photo User Roles Volume MON LANE (ID: 40) START TIME END TIME 00 : 00 23 : 59	ng Station Setup Reports Events Cameras System LANE (ID: 40) June (ID: 40) June (ID: 40) June (ID: 40) Call Lists MON LANE (ID: 40) June (ID: 40) June (ID: 40) DAY(5) Monday Monday 00: 00 23: 59 • Monday • Monday • Wednesday	ng Station Setup Reports Events Cameras System LANE (ID: 40) Jser Details Upload a Photo User Roles Call Lists MON LANE (ID: 40) Vernove Call Lists Position START TIME END TIME DAY(5) Position 00: 00 23: 59 • Monday • Tuesday • Tuesday 1

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:

ffice	1 (Fire))									
ddress:	400 N Tan	npa St, Tan	npa, FL	. 33602		Telep Alten Polic Fire: ULTy Statik Area Line Line Inves Resp	bhone: 8 native T e: 813-11 ype: Fire on has k is active is secur is encry stigator oonse tin	313-111 elepho 111-333 -2222 True ceys: Fa e: False re:	-1111 ne: 3 alse e alse d: False inutes		
ffice 1	Surgard	l (Surgar	d Sys	stem 3	(TCP))						
entifier: evice Ty ost: sername ccount N ne Profil Alarms	10006 pe: Surgar : Number: 1 le: Line 1	rd System 3	(TCP)							
entifier: evice Ty ost: sername ccount N ne Profil Alarms	10006 pe: Surgar s: Jumber: 1 le: Line 1	rd System 3 111 Title	3 (TCP)		Priority	Auto	-handle	1	ExtraValue	Tag
entifier: evice Ty ost: sername ccount N ne Profi Alarms Input1 -1	10006 pe: Surgar s: Number: 1 le: Line 1 lnput 2 -1	rd System 3 111 Title Burg	(TCP)		Priority 101	Auto	handle	1	ExtraValue	Tag
entifier: evice Ty ost: sername ccount N ne Profil Alarms Input1 -1	10006 pe: Surgar s: Number: 1 le: Line 1 lnput 2 -1 -1	rd System 3 111 Title Burg Close	3 (TCP)		Priority 101 100	Auto False True	-handle	1	ExtraValue	Tag
entifier: evice Ty ost: semame ccount N ne Profil Alarms Input1 -1 -1 -1	10006 pe: Surgar Number: 1 le: Line 1 lnput 2 -1 -1 -1 -1	rd System 3 111 Title Burg Close Fire	3 (TCP)		Priority 101 100 2001	Auto False True False	handle	1	ExtraValue	Tag
entifier: evice Ty ost: semame ccount N ne Profil Alarms Input1 -1 -1 -1 -1	10006 pe: Surgar Number: 1 le: Line 1 Input 2 -1 -1 -1 -1 -1	rd System 3 111 Title Burg Close Fire Fire Fire troub	3 (TCP) Dore		Priority 101 100 2001 50	Auto False True False False	-handle	1	ExtraValue	Tag
entifier: evice Ty ost: sername ccount N ne Profil Alarms Input1 -1 -1 -1 -1 -1 -1	10006 pe: Surgar Number: 1 le: Line 1 -1 -1 -1 -1 -1 -1 -1 -1 -1	rd System 3 111 Title Burg Close Fire Fire troub Fire supe	le resto) pore		Priority 101 100 2001 50 50	Auto False True False False False	handle		ExtraValue	Tag
entifier: evice Ty ost: sername ccount N ne Profil Alarms Input1 -1 -1 -1 -1 -1 -1 -1 -1	10006 pe: Surgar Number: 1 le: Line 1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -	rd System 3 1111 Burg Close Fire Fire troub Fire supe Medical	8 (TCP) pre		Priority 101 100 2001 50 50 1001	Auto False True False False False False	handle		ExtraValue	Tag
entifier: evice Ty ost: sername ccount N ne Profi Alarms Input1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1	10006 pe: Surgar Number: 1 le: Line 1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -	rd System 3 1111 Burg Close Fire Fire troub Fire supe Medical Open	8 (TCP) pre		Priority 101 100 2001 50 50 1001 100	Auto False True False False False False True	handle		ExtraValue	Tag
entifier: evice Ty ost: sername ccount N ne Profil Alarms Input1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1	10006 pe: Surgar Number: 1 le: Line 1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -	rd System 3 1111 Title Burg Close Fire Fire troub Fire supe Medical Open Schedules	le resta rvisory Mon) pre Tue X	Wed	Priority 101 100 2001 50 50 1001 100 Thur X	Auto False True False False False False False True	-handle Sat	Sun X	ExtraValue	Tag
entifier: avice Ty ost: sername ccount N ne Profil Alarms Input1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1	10006 pe: Surgar Number: 1 le: Line 1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -	rd System 3 1111 Title Burg Close Fire Fire troub Fire supe Medical Open Schedules	le resta rvisory Mon) pre Tue X	Wed	Priority 101 100 2001 50 50 1001 100 Thur X 1501	Auto False True False False False True Fri X False	-handle Sat	Sun X	ExtraValue	Tag

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:

Insi	ght					5-5 6-0
				Filter Options	×	
		UL	User Activi			16 June 2021 21:42 - 23 June 2021 21:42 📰 🛓 🔗
			Created	Filters	Include/ Exclude	Details
	Avg. Response Time by Operator			Area		
		2	2021-06-22 12:39:3	Office 1 (Fire) X	ຸ 🗖	
UL] TimeZoneID changed from [True] to [False]
	UL Alarms By Device Report		2021-06-22 22:04:1	Event Type		
					•	
	UL Alarms By Tag Report		2021-06-22 22:04:4	Start Date (America/Los Angeles)		ba Office (UL Fire)]
				16/06/2021 21:42	: (UL Fire)] to [Tampa Office]	
			2021-06-22 22:18:1	End Date (America/Los_Angeles)	pa Office 1 (Fire)]	
	UL Statistical Performance			23/06/2021 21:42		St, FL 33602] to [400 N Tampa St, Tampa, FL 33602]
			2021-06-22 22:19:1			I (Fire)] to [Office 1 (Fire)]
						11] to [813-111-2222] TelephonePolice changed from [813-
			2021-06-22 22:37:3	BUN REPORT		Jurgard
Vie			2021-06-22 22:43:03	Admin1 UserID: 20018 has updated response ID: 10017		
	Video Reports by Area		2021-06-22 22:47:10	Admin1 UserID: 20018 has updated response Title: Panic		
		18	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:

Alarms - Monitoring St	tation 🕞	ALARM POINTS	QUICK CONTROL	PROCESS TOP PRIORITY	MANUAL RAISE	ACTIVITY LOG	MANUAL TOUR	? 🔳	79
All									
No Alarms					Map Sa	tellite			>
					Cr	estnut House SureView System	Parmley Gra	aham 📀	
					Google		Map Data Terr	ms of Use Rep	ort a map error
Processing Parked 1	Tours On Tes	t .ocation		Event	Par	ked Until		Parke	•d Bv
01/19/2021 10:41:05 AM	4	CME - Hawthorne Ho	use 📮	UNSCHEDULED	01/	/19/2021 10:53:25 A	м	User	
ocalhost/immixcc/#									

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:

New site 📑	Put Event on Test (Audit Mode)		SITREP RAISE LEAVE END ?
ALL ALARMS 1 OPERATOR DISPATCH DE	For a Fixed Period Until Dat	e/Time	
My Time Area Time Priority Details	Hours: *	Minutes: *	Add action to new category
5:31:06 PM 01/15/2021 10:31:06 AM 10 System Test - Ma , Notes:			Add action from library
	Note: *		
Map Satellite		OK CANCEL	
Google		+ 	

Alarm queue with site on test:

Alarms - Monitoring Station 🖵	ALARM POINTS QUICK CON	TROL PROCESS TOP	PRIORITY MANUAL RAISE	ACTIVITY LOG	MANUAL TOUR	? 🔳	23
No Alarms			Map Sate	ellite			>
Processing Parked Tours On Teel	1		Google	Map data 822	D21 Imagery E2021 NASA	TerralMerice Terral	+ - -
Started L	ocation	Alarm Point	On Test Until	Test	Type Te:	st Note	
01/15/2021 5:31:06 PM T	est - New site 📃	All (01/18/2021 2:01:34 PM	Audit	t Sys	stem Test	
localhost/immixcc/#							

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:

Alarms - Monitoring Station 🖵	ALARM POINTS QUICK CONTROL	PROCESS TOP PRIORITY	MANUAL F	RAISE A	CTIVITY LOG	MANUAL TOUR	?	79	22
All				First	Last				*
No Alarme				Alarm	Alarm ^{\$}	Alarm Details			
NU AIdinis			Ma	01/15/2021 4:33:51 PM	01/15/2021 4:33:51 PM	REMINDER: High Me	mory usa	ge (80%) (
				01/15/2021 4:43:36 PM	01/18/2021 11:50:12 PM	REMINDER: Connect http://localhost:80/R	ion test fo eportServ	or failed to vice/Conn	
				01/15/2021 6:24:46 PM	01/15/2021 6:24:46 PM	High CPU usage (82	%) detecte	ed on MYT	
				01/15/2021 10:33:54 PM	01/18/2021 11:40:28 PM	REMINDER: High Me	mory usa	ge (55%) (
				01/18/2021	01/18/2021				-
								ACK ALL	
			Google			Map Data Te	rms of Use	Report a ma	ap error
Processing Parked 1 Tours On T	Test								~
Time	Location	Event		Parked	Until		P	arked By	
01/19/2021 10:41:05 AM	ACME - Hawthorne House 🗾	UNSCHEDULED		01/19/2	021 10:53:25	AM	U	ser	

Disarming

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

Alar	ns - Monitoring Station 🗖 ALARM POINTS OUICK CONTROL	PROCESS TOP PRIORITY MANUAL RAISE ACTIVITY LOG MANUAL TOUR ? E
Nc	View Masked Alarm Points	Door Held Open
	Search for alarm point	Mask alarm point
	Type to search 👻	Reason * Employee request V
	Find in Area	Mask for a Fixed Period Mask until Date/Time Hours:* Minutes:* 0
		MASK CANCEL
	CME	Put alarm point on test
Prc	400 North Ashley Hawthorne House	History - Most recent 50 alarms for this alarm point
Time		CLOSE
There		

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:

5:00:04 AM	01/20/2021 12:00:04 AM 100	tom - TOM TEST	Link Camera		• ×	~
11:06:22 AM	01/20/2021 6:06:22 AM	Started Processing by User		U		
11:06:23 AM	01/20/2021 6:06:23 AM	Alarm acknowledged : tom - TOM TEST		U		
11:06:28 AM	01/20/2021 6:06:28 AM	Dispatched Mobile 1		U		
11:06:28 AM	01/20/2021 6:06:28 AM	User rejoined event		U		
11:06:33 AM	01/20/2021 6:06:33 AM	Mobile 1 arrived		U		
11:06:35 AM	01/20/2021 6:06:35 AM	Mobile 1 left		U		
11:06:38 AM	01/20/2021 6:06:38 AM	Dispatched Mobile 1		U		
11:06:42 AM	01/20/2021 6:06:42 AM	Mobile 1 left		U		
11:07:41 AM	01/20/2021 6:07:41 AM	User rejoined event		U		
11:08:05 AM	01/20/2021 6:08:05 AM	Dispatched Mobile 1		U		
11:08:05 AM	01/20/2021 6:08:05 AM	User rejoined event		U		
11:09:32 AM	01/20/2021 6:09:32 AM	Mobile 1 arrived		U		
11:10:50 AM	01/20/2021 6:10:50 AM	Mobile 1 left				

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:

Office 1 (Fire)					DISPATCH - 💼 🏴 SITREP	
ALL ALARMS T OPERATOR DISPATCH DEVICES ACTIONS N						
And Area Time Priority Details		Linked Camera	Clips Operator	Standa		± •
ISIS OR AM 96/24/202133.15.08 AM 2001 Fire alorm - Ere - Survivex test alarm	Office 1 /Firs\ Area Dataila			Did the o	Fire Dept pickup? Telephone: 813-111-2222 S NO	
And a nota	Address 400 N Tampa St, Tampa, FL 33602	Primary Contacts Main Phone: 813-111-1111 Local Police: 813-111-3333 Local Fire: 813-111-2222	UL Settings UL Type: Fire Is Area Active?: No Is Investigator Required?: No Is Line Secure?: No Is Line Encrypted?: No		n Lane (ID-40) pickup7 1 Laine 193–444-222 elephone: 873–444-1111 NO	
An annual state of the second state of the sec	All Roles V Name Sito owner Simon La Notes	Phones ne (ID: 40) 813-444-1111	Email Site Pa simon lanegacme.com	ssword P CLOSE		
Anno and an an and an an and an an and an an an and an	h Tennen Hutch hann en 1921 Sam 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1	resman's getter an suntaint owntown carego	Armenti Low (FA) Telan Telana Telana da arment Armenta Anadiment Parkan da arment Parkan da arment			
Google	Keyboard shortcuts Map data \$20210	Boogle Imagery 02021 DIES / Airbus Ma	Itelet			

Verification of a site staff's passcode:

Office 1 (Fire)			(A + DISPATCH - SIT	REP RAISE LEAVE END ?
ALL ALARMS T OPERATOR DISPATCH DEVICES ACTIONS N					
Event ID: 351100					
My Time Area Time Priority Details					
	Office 1 (Fire) Area Details				
Add a note	Address Validate Site Password:	word			
A Search					
Map Satellite CV at addition Satellite	Site owner Notes	VALIDATE	CLOSE		
And a state of the	An a constraint an an cata ta an cata ta	Entretile Venantic generation Sentime Regime and Philosophics Regime and Philo	evine Enbarc odletive United Assemble Autor Assemble Autor Assemble 	Current Queve Bisturs: 1 unarraw	

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}

Bank (Burg)					• •	
ALL ALARMS 1 OPERATOR DISPATCH DEVICES ACTIONS N						
My Time Area Time Priority Details		Linked Camera Clin	s Operator			
3:06:37 PM 06/24/2021 6:06:37 PM 100 Burglary alarm - Burg - SureView test alarm		(Unk Camera)	A %	Standard Actions (0/4)		
	Bank (Burg)					
	Problem: Carnera 1 video loss, Status:	in progress				
	(49 / 500)					
	Start Date / Time (Optional):	End Date / Tim	e (Optional):			
	MM/DD/YYYY / 12:00 AM	• × MM/DD/1	YYY / 12:00 AM O	× lobile: 813-444 elephone: 813-	-2222 144-1111	
Add a note Participation and a second and a	CANCEL SAVE					
Waterfront Park	Created Created By	Starts	Ends			
Come of Contract Mexay Hall						
	No notes tound					
Rivergate Tower				_		
kes College and and the second s				ок		
Aloft Tampa Down	Cown 😪 Traceut - Delivery 💙 Morgan &	Morgan				
Administration of Plant Park	🤉 🔍 🕡 🖓 Hilton Tampa Down	texts Bland VIII Gental	Porking Gatago			
Chick fil A Sherator R	Verwalk Port Brooke Gar		18 contration			
	The states	BUILLIOU Phile Lot	Aurora			
Church of Lampa	PWITC -Sheraton, Hilton Extrained	Cowntown				
Google Oxterd Exclange Jamps Baptist Manor	Keynold Remote Ville data Scott Scott	Peri	ing P	Curren		

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)

Hawthorne House				SITREP	RAISE	LEAVE	END	?
	Close	×						
ALL ALARMS D OPERATOR DISPATCH DE								
Event ID: 961	Criminal Activity							
My Time Area Time Priority Details			Add actio	on to new categ				
11:48:40 AM 01/20/2021 11:48:40 AM 200 Door Held Open	Theft		Add actic	on from library				
	Items taken from counter							
Add a note								
Map Satellite Chestro								
HIDDAY STREET								
Sur P								
C	24 5000							
	OK CAN	CEL						
Google	Map Date Terms of Use Report a map er	ror						

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:

P PRIORITY	I	MANUAL RAISE	MANUAL TOUR	?	9	
Date		Alarm Details	· ·······	,		•
06/25/2021 8:40:50 PM		Immix server con UL1 lost	nmunication from EN	IT-UL2 t	o Ent-	
06/25/2021 8:44:43 PM		NLB server conne ENT-UL2)	ected: 192.168.2.206	(Detec	ted by	
06/25/2021 8:44:49 PM		Ent-UL2.sureview restored (NLB clu converged with h member of the N balancing traffic.	vsystems.com: NLB (uster [192.168.2.205] ost(s): 1,2. It is now a LB cluster and will st)	Connect : Host 2 an activ :art loac	cion 2 re 1	
06/25/2021 8:45:03 PM		Immix server con UL1 restored	nmunication from EN	IT-UL2 t	o Ent-	
					ACK ALI	-

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

OCE	S TOP PRIORIT	Y MANUAL RAI	SE MANUA	AL TOUR	?		1				
_	Date 🔶	Alarm Details					_				
	06/22/2021 6:12:34 PM	Immix server comr	nunication from	1 ENT-UL2 to	o Ent-U	LW lost					
	06/22/2021 6:12:34 PM	Immix server comr	mmix server communication from ENT-UL1 to Ent-ULW lost								
	06/22/2021 6:13:49 PM	Immix server comr	nunication from	ENT-UL2 to	o Ent-U	LW resto	red				
a.	06/22/2021 6:13:51 PM	Immix server comr	nunication from	ENT-UL1 to	o Ent-U	LW resto	red				
						ACK AL					

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.

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.)

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

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.

Date		Alarm Details
06/17/20 12:58:29	21 PM	Surgard Receiver disconnected (192.168.2.91:1025) - Unable to connect
06/17/20 12:59:09	21 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.

Alarms - M	Monitoring	ation 🛃	ALARM PC	DINT	s q	UIC	K CONTR	OL	PROCESS	TOP PRIORITY	MANUAL RAISE	MANUAL TOUR	?	000		
All 1	•															
Started 🗢	Location	¢	Event		\$	Priority	¢	Count	¢	Actions	Мар	Satellite				>
a few seconds ago	Monitoring Station		Power Supply Redunda Lost from idrac-608XRI	ncy has been)2	' ()		2			- map			R.		X
													A A			
											1 John		The second	H		
											240					
											1Kg		N.			+
																-
	_										Google	shortcuts Map data ©20	21 Imagery ©2021 NASA, To	erraMetrio	:s Term	s of Use
Processing	Parked	Τοι	urs On Test													~
Time			Location							Event	1		User			
There are no e	vents being pro	cess	ed.													

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:

Date	Alarm Details					
06/17/2021 1:01:39 PM	High Memory usage (88%) detected on ENT-UL1					
06/17/2021 1:02:16 PM	High CPU usage (98%) detected on ENT-UL1					
	ACK ALL					

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.

Insi	ght				2	3
			Filter Options	×		
Se		Alarms by Device R			7 Days 🗙 🗸 17 June 2021 13:48 - 24 June 2021 13:48 🖽 🛓 🔗	
		Created T	- Filters	Include/ Exclude	Details	
			с — Агаз			
Pe		2 2021-06-22 12:48:25 Eastern	Office 1 (Fire)	↓ ■	alarm	
	Alarm Count by Operator				alarm	
		4 2021-06-22 14:04:26 Eastern	c – Device			
	Avg. Processing Time by Area			~		
	Avg. Processing Time by Operator	6 2021-06-22 14:57:29 Eastern	Start Date (America/Log_Angeles)			
			17/06/2021 13:48	 		
	Avg. Response Time by Area	8 2021-06-22 15:02:04 Eastern	End Date (America/Los_Angeles)			
			24/06/2021 13:48		alarm	
u		10 2021-06-22 15:25:55 Eastern			alarm	
	OL Alarms by Device Report	12 2021-06-22 15:40:29 Eastern	RUN REPORT			
		14 2021-06-22 15:40:36 Eastern	Standard Time Office 1 Surgard - Burglary alarm - Burg - SureViev			
	UL Statistical Performance	16 2021-06-22 15:40:51 Eastern	Standard Time Office 1 Surgard - Burglary alarm - Burg - SureViev	v test alarm		
		18 2021-06-22 15:40:57 Eastern	Standard Time Office 1 Surgard - RUNAWAY Burglary alarm - Burg	g - SureView te:	st alarm v	

A tabular report with filter options open:

A non-tabular report:

Insight			11
Search Reports	5	UL Statistical Performance Report	
Alarms By S		Start Dolle (America/Los_Angeles) 17/06/2021 20:48	
Performance Alarm Count	▼ t by Operator	End Date (xmericat.cat.segles) 24/06/2021 20:48	
Avg. Proces	sing Time by Area		
Avg. Process Operator	sing Time by		DOWNLOAD PDF
Avg. Respon	ise Time by Area		
Avg. Respon	ise Time by Operator		
UL			
UL Alarms B	y Device Report		
UL Alarms B	y Tag Report		
UL Problems	s Report		
UL Site Setu	p Report		
UL Statistica Report	al Performance		
UL Unsched	uled Alarm 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:

Event Search		GO TO EVENTIAL OF
Results: 32 events found SEARCH AGAIN	Event 100448 - System Test	STREP COMREGIO MESAL 🛓
System Test UL Reporting Test Size 4:05:45 PM- (MIT Standerd Time	Event Type: Alarm Event Start Time: 06/10/2021 4:57:05 PM	Extent on sizes dip
System Test UL Raparing Test Ske 406:39 PM - GAT Skeederd Time	Event End Time: 06/15/2021 4-30:04 PM Time Zone: OMT Standard Time	and the second sec
Missing Adult Airm Processing Permissions testing 81206 AM-UTC	Area: UI. Reporting Test Site Operator(s): User	
System Test Heri Heri 42731 AM-UTC-11		
System Test test elle 1 439927AM-UTC-11		
System Test Alam Processing Permissions Lesting 8:38:39 AM-UTC		
System Test twi etc 1 44012 AM - UTG-11		
No Outcome Assigned Alem Processing Permissions testing 8:43:14 AM- UTC	ALL ALABAS) OPERATOR DISPATCH DEVICES ACTIONS NOTES	. Google and account of the stand account of the st
System Trest Alam Processing Permissions testing 8:32:46 AM-UTC	Event ID: 100448 My Time Area Time Priority Details ES705 AM 06/10/2021 4:57:05 PM 100 Default Alarm -SureView test alarm	Linked Camera Clipa Operator
No Outcome Assigned Alarm Processing Permissions Leating 8:57:00 AM - UTC		
System Test UL Reporting Test Size 4:37:05 PM - GAIT Sizedend Time		
System Test Merizzing Brasion 731:13 AM- GMT Standard Time		
System Test		

Pop up to select what to include in the SitRep:

Generate Situation Report							
Summary							
Test Note Optional selection to add to repo Map Current Audit Trail Event Thumbnail Video Snapshots	rt	6					
	GENERATE REPORT	CLOSE					

Example SitRep:
Affected Location: Tompo Office			
UL Tune: Purelani	7		
Site has keys: Eaks			
Area is active: Taise			
Area is active: True			
Line is secure: Faise			
Line is encrypted: Faise			
Response time: 20			
Response time:: 30			
Event started: Thursday, June 17	, 2021 11:41:50 AM (Eastern Standard Time)		
oummary:			
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
15	6/17/2021 11:42:06 AM	Action completed: Call: Police - Call Police "813-222- 2222" User entry: "Call Made"	User

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.