Sensurity UNIVERSE User Manual

Contents

Contents

info@sensurity.com
www.sensurity.com

Contents

info@sensurity.com
www.sensurity.com

Sensurity UNIVERSE User Manual

Introduction

Introduction

Sensurity UNIVERSE allows management and configuration of the Sensurity devices and alarms.

The following functionality is available through the Sensurity UNIVERSE application:

- Manage users, roles and individual access levels
- Install, view, pair and delete devices.
- Build, edit and delete networks containing devices
- Change device settings
- View the location of devices on Google Maps
- Identify the location of triggered devices on Google Maps
- Receive alarm notifications as desktop notifications, SMS text message or by phone call
- View alarm information including the type of alarm
- Choose from five languages
- Receive alerts when firmware updates are available for your devices

System Overview

Sensurity devices utilise the **SIA Open Supervised Device Protocol** to provide two-way communications with devices. Sensurity's OSDP compliant devices support OSDP Secure Channel Session (OSDP-SCS) which utilises 128-bit AESCMAC.

Sensurity UNIVERSE is a Windows Service/Linux daemon that operates in the background of a PC and operates a number of OSDP Control Panels (CP's). UNIVERSE can control up to 127 OSDP Peripheral Devices with an interface that allows commands to be issued to each device to control and monitor their operation, along automated polling and reporting of alarms.

Interaction with the service is achieved through an asynchronous TCP/IP socket that is secured using **Secure Socket Layer** (SSL) and a username/password. Data in the form of XML strings are exchanged with the service using this socket.

The UNIVERSE interface has been chosen to provide the greatest compatibility with a range of programming languages and target operating systems, in addition to secure data storage and routing.

XML data is readily understood, highly portable and provides a rapid deployment path for integration of Sensurity products with other security management platforms and external devices. To read more about integrating Sensurity with your wider security system, please visit www.sensurity.com/resources/integrations.

info@sensurity.com
www.sensurity.com

Sensurity UNIVERSE User Manual

Installation and Set-Up

Installing the Desktop Application (Windows)

System Requirements

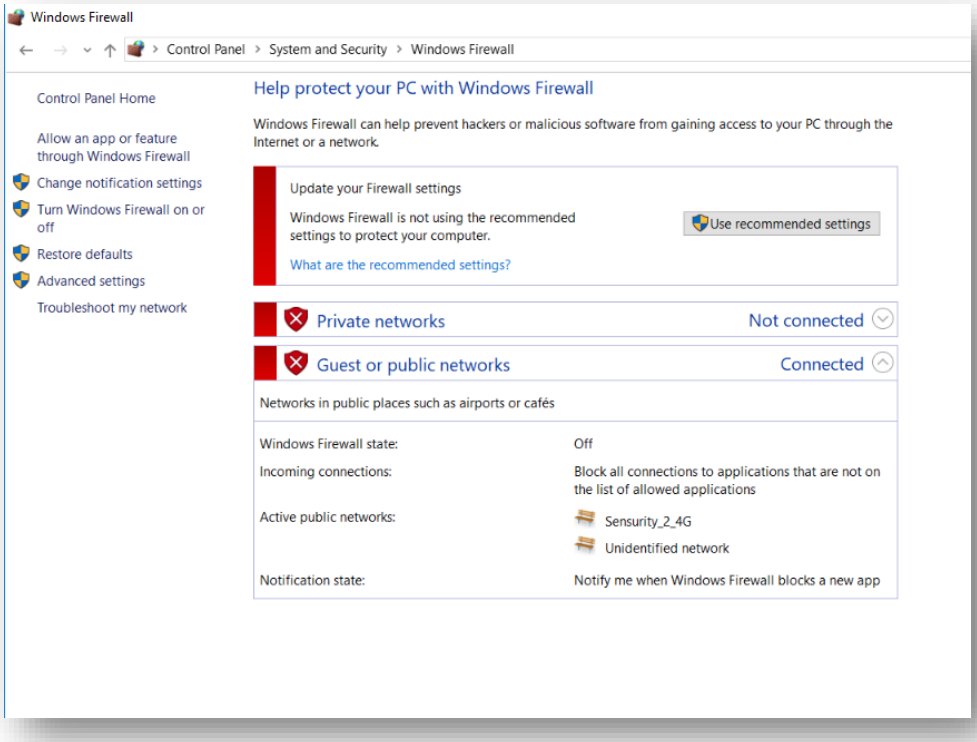
- Windows 10 or higher
- Minimum 8GB RAM recommended
- Core i7 Quad Core Processor or higher
- SSD recommended

Please Note: UNIVERSE does not run on Windows Internet Explorer. Alternative web browsers that we can recommend are Google Chrome, Firefox and Microsoft Edge.

Disabling the Firewall

For the UNIVERSE application to communicate in order to monitor and configure the Halo or Vigil devices, the Firewall on the PC must be disabled. To do this, follow the sequence below.

1. Open the ''Control Panel' menu on your desktop
2. Select 'System and Security', then 'Turn Windows Firewall on or off'
3. Next turn off your public and your private firewalls

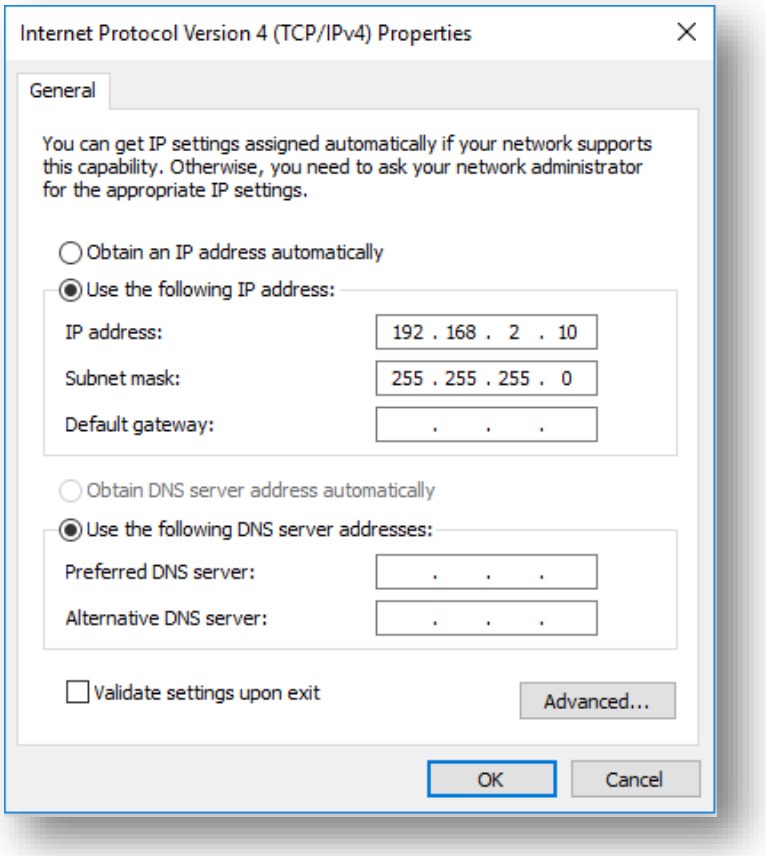


info@sensurity.com
www.sensurity.com

Installation and Set-Up

Network Set-up

1. Open the 'Start' menu on your desktop
2. Select 'Control Panel'
3. Select 'Network and Sharing, then 'Change Adaptor Settings'
4. Select the ethernet connection to the Halo/Vigil network
5. Click 'Properties'
6. Select Internet Protocol 4 **TCP/IPv4** and click 'Properties'
7. Select 'Use the following IP Address'
8. Set the IP address to **192.168.2.10** and click 'Ok'



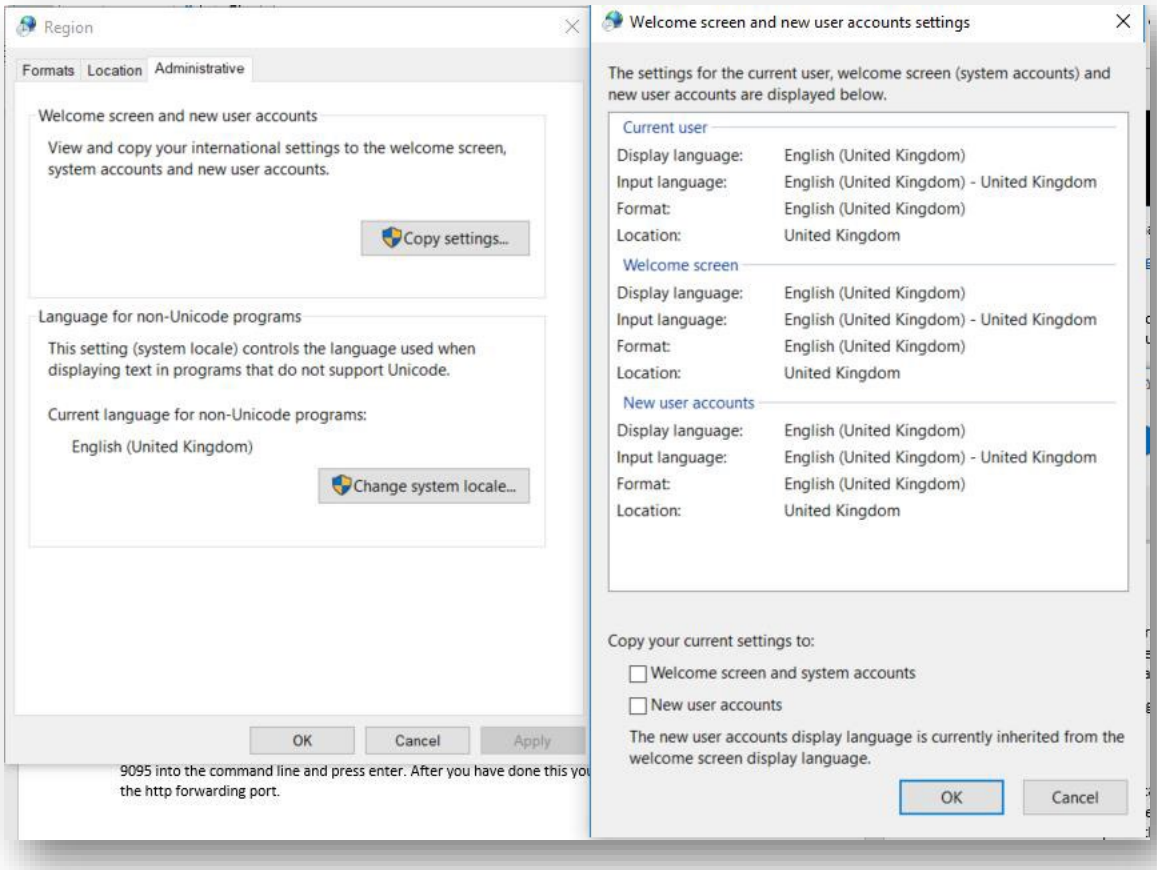
info@sensurity.com
www.sensurity.com

Installation and Set-Up

Language and Region Settings

Different regions and languages interpret numbers differently, UK uses a '.' as a decimal separator whereas Continental Europe use a ','. To ensure numbers, decimals, GPS coordinates etc. are interpreted correctly by the application, the Regional Setting should be changed as follows:

1. Open the 'Start' menu on the PC
2. Choose 'Control Panel'
3. In control panel click 'Clock and Region'
4. Click 'Region'
5. Go to the 'Administrative tab' and change your current system locale to 'English'
6. Restart PC
7. Under 'Copy your current settings to:', check the box for 'Welcome screen and system accounts'.
8. Click 'Ok', then 'Apply' and finally click 'OK' again.
9. Under the formats tab change your settings to 'English'



info@sensurity.com
www.sensurity.com

Sensurity UNIVERSE User Manual

Installation and Set-Up

Installing the UNIVERSE Application

1. Download the application from: www.sensurity.com/products/universe/
2. Unzip the downloaded file and run the installation script – 'Sensurity Universe Web.exe'
3. Follow any on screen instructions.
4. During installation your computer may restart. After installation you will be asked to restart again. Both restarts must be completed in full to successfully install the application.

info@sensurity.com
www.sensurity.com

Logging In

On application start, login to the Sensurity UNIVERSE application using the following details:

Username: admin@sensurity.com
Password: 123qwe

This will allow creation of custom users with defined roles. The passwords for the default users may be changed or the user deleted if not required.

Dashboard

This is the main menu form which the required sections can be chosen:

Users	- Add, edit or deleted
Services	- Add, edit
Networks	- Add
Alarms	- View
FAQ	- typical questions answered
Update	- remotely update firmware – applicable to Halo only
SMS	- setup SMS to mobile phones on Alarm conditions
Historical Alarms	- View older alarms Purged from the Alarms Screen
Analysis	- View alarm patterns
Firewall	- enable/disable PC firewall from within the UNIVERSE application
Logs	- view logging information from the Halo or Vigil devices

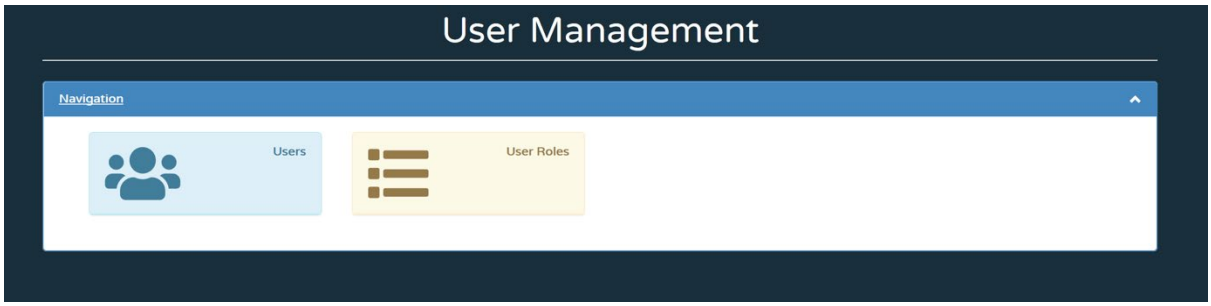
Further details on these sections can be found within this document.

User Management

The section enables Users to be added, edited or deleted. Different user roles need to be assigned based on how the user needs to interact with the system.

Important: If the default 'Admin' user is not to be used, in order to set up a new user with these privileges then they must be set as a Service User.

Simply check the checkbox 'Add user to Service' when adding a new user to give admin privileges.



Associating different roles with each user allows for different behaviours - monitoring, reconfiguring etc. Below is a list of roles available:

1. Admin
2. Engineer
3. IT
4. Security
5. SuperAdmin *
6. Tester
7. User *

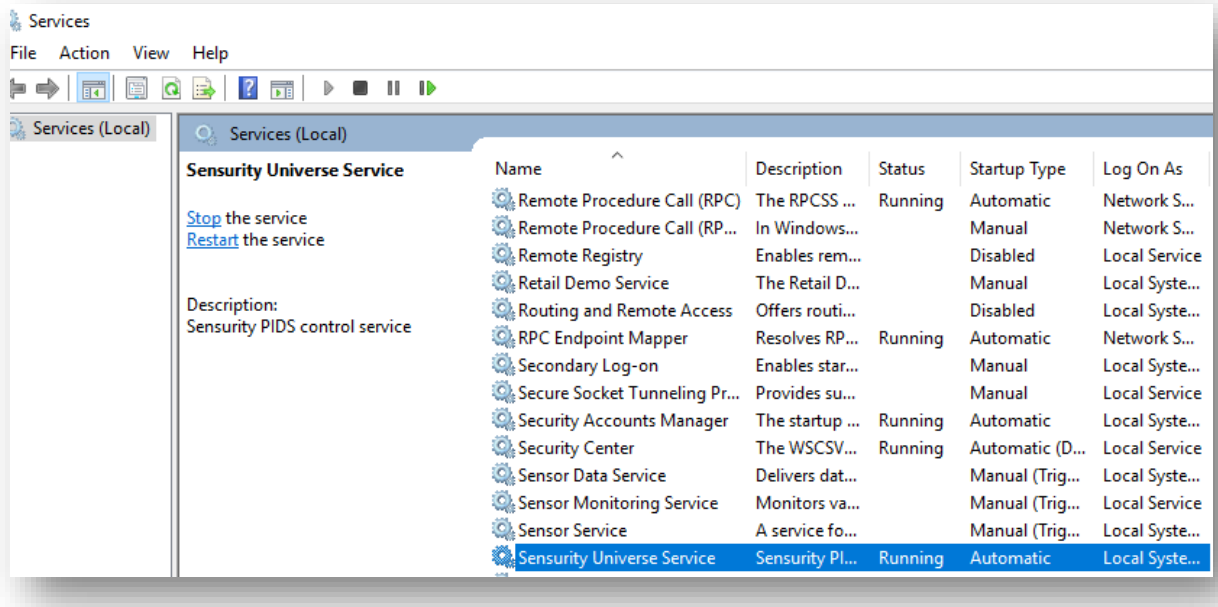
* It is recommended that only SuperAdmin and User roles are assigned. SuperAdmin gives full system wide monitoring and configuration capabilities while the User role gives only monitoring capabilities, alarms may be acknowledged, configuration parameters may be viewed but not changed.

info@sensurity.com
www.sensurity.com

Setting Up Services, Networks and Devices

Services

- The 'Services' settings control the communication between UNIVERSE and the Sensurity devices exchanging monitoring and configuration information.
- In 'Services' a new service can be created with the following parameters to be set:
    - Alias
    - URL
    - Port
    - Self-signed
    - Certificate
- Multiple services may be added if multiple communications channels are required; each service may communicate with a number of networks.
- The service is built on Microsoft Windows, therefore, the service status can be checked, started or stopped from within the the Windows Services Manager.



info@sensurity.com
www.sensurity.com

Networks

Within the 'Networks' tab you can:

- Add a new network
- View status of an existing network
- Edit the network
- Delete the network
- View devices connected to that network

Add a Network

- Click on the green button ( ) situated bottom-right corner and filling in the required information:
    - Service to be associated with the network
    - Network unique name
    - Master port (default 27043)
    - Slave port (default 27042)
    - TCP only
    - Baud retry Delay in seconds

Port numbers may be different values, however if not set to default the port numbers on the associated Halos/Vigils must be changed to these values

Once the network has been added, it will appear under the network tab as shown below. It can take a few seconds for the new network to connect.

The network icon is colour coded:

- Green – Running with no alarms
- Red – The network is in an alarmed state.

Clicking on the Network icon will display the menu items to delete, edit, view network parameters or view associated devices.

If the network icon is Red then viewing the devices will identify which device is alarmed, the device alarming will be red.

info@sensurity.com
www.sensurity.com

Configuration of multiple networks

Multiple Networks can be provisioned, however configuration parameters such as the Port numbers etc. must be different. The name of each network associated with a service must be unique as the name is used for identification purposes.

The sequence of events in which devices are moved between networks must be followed in order as to not loss communications with the devices. If not followed correctly it may lead to device needing to be reset back to factory defaults and starting the process again from scratch.

To Add devices to a new Network:

1. Change the Server Port, the IP Address and Server IP Address on each device. Server Port must coincide with that of the new Network.

2. Change the Server/Adapter IP Address on the desktop/laptop running the Sensurity UNIVERSE application to match this.

3. Add a new Network matching the configuration of the devices, making sure the Network Slave Port matches the device Server Port.

Devices

This is either a Halo or Vigil Perimeter Intrusion Device. These devices have similarities with differences highlighted within this document.

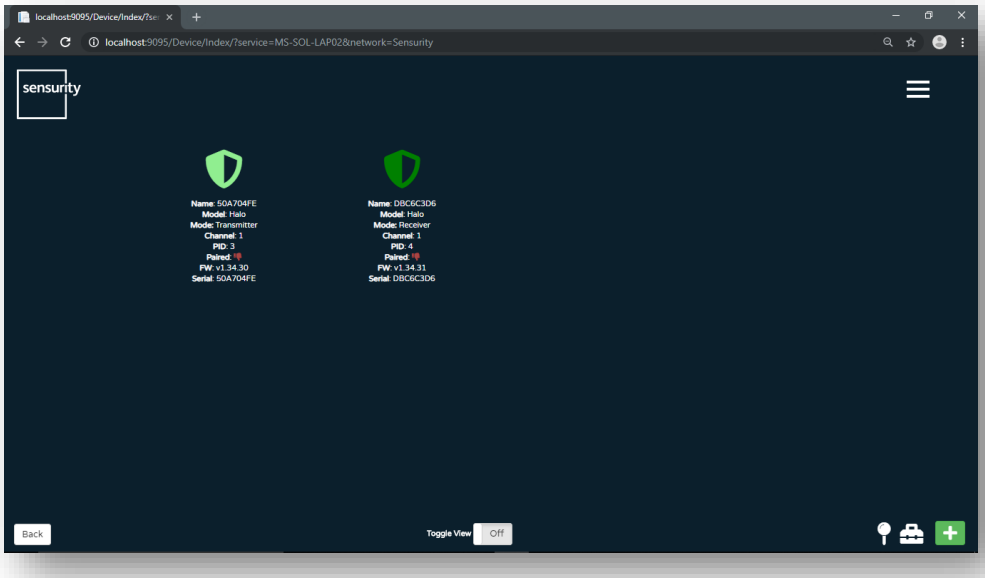
- Devices can only be viewed within their network.
- To view devices from the main dashboard, go to Networks then click on the associated with the devices and select 'View Devices'.
- From here, the following menu option are available:
    - Reset
    - Remove
    - View device information
    - View alarms

Add a Device

To add a new Device:

- Select the green button () in the bottom-right corner of the view.
    - Before adding a device, ensure that the associated network is successfully 'Connected'.
    - During device installation a number of connection alarms will appear on the screen. Wait for these to clear before installing another device.
    - Ensure that a unique Device Address is set for each individual device. If two devices have the same Device Address, errors will occur and communication to these devices will be lost.
- Select the white pin () to navigate to Google Map showing overlaid devices. The line drawn between paired devices highlights the link and is selectable to view alarms which have occurred on that link.
- Within each network 126 devices may be installed.
- Select the toolbox () to revert device layout back to the initial design.
- Toggle View displays devices in a list.

info@sensurity.com
www.sensurity.com

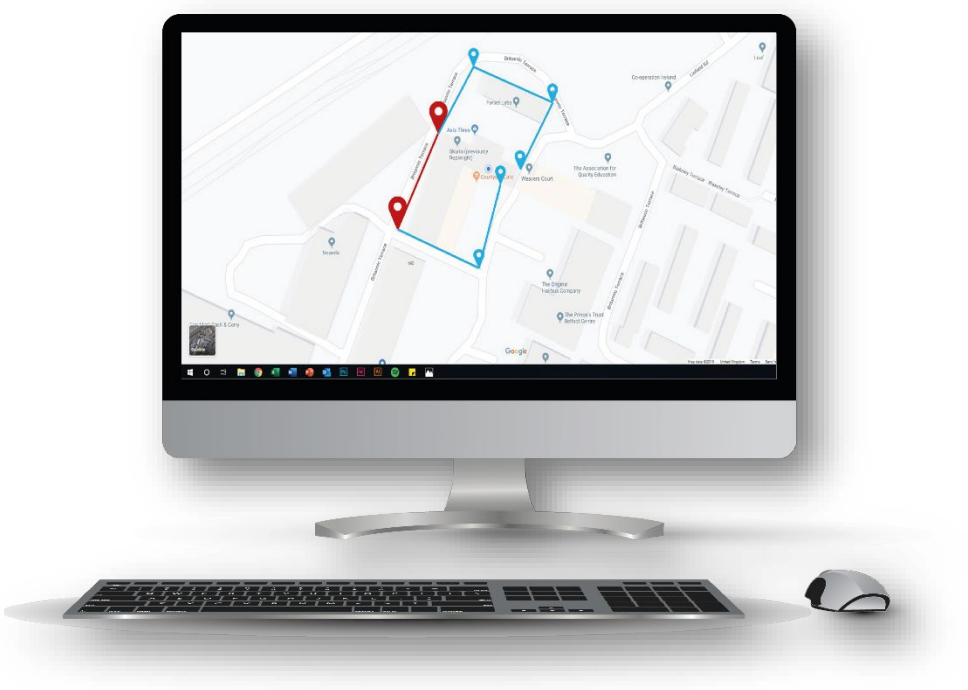


The device icon is colour coded:

- Green – Running with no alarms
- Red – The device is in an alarmed state

info@sensurity.com
www.sensurity.com

Device Map Overlay

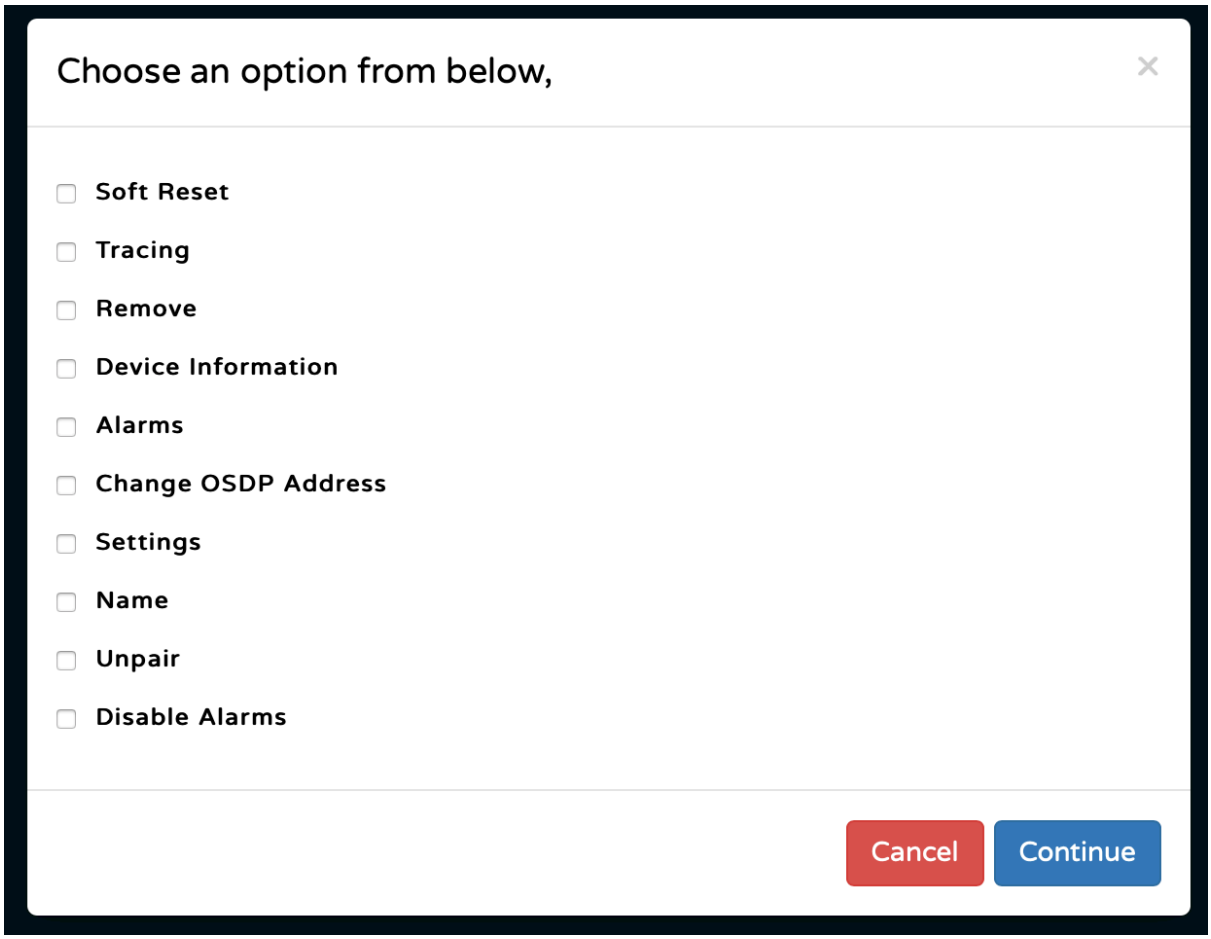


Each Sensurity device is built with an in-device GPS locator which will automatically place the device's location onto the UNIVERSE map overlay.

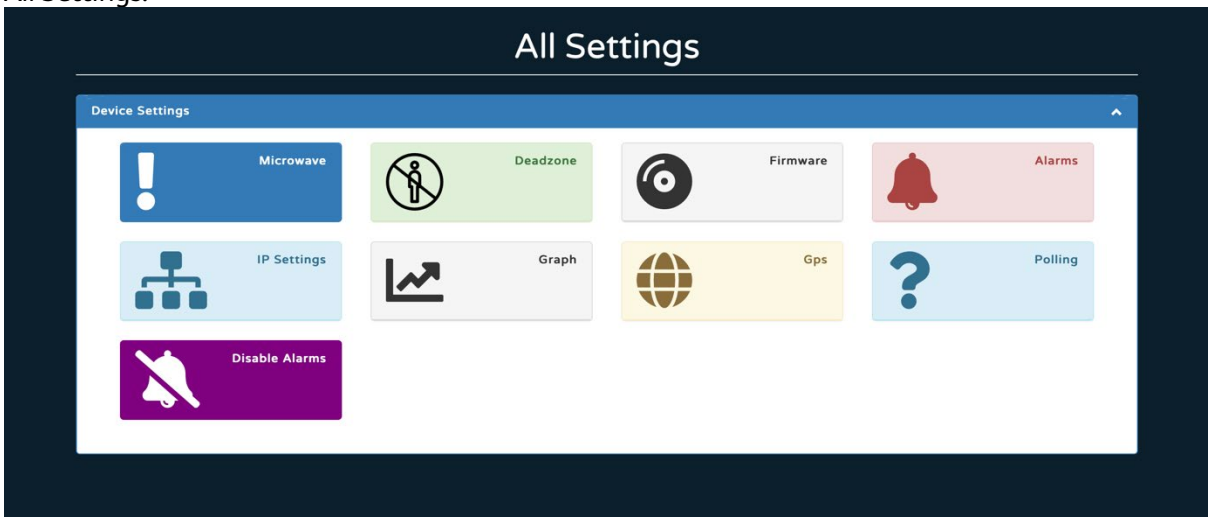
If GPS reception is poor, then the devices can be manually dragged and dropped into their appropriate position.

Settings

To view settings, left click on the device icon using a mouse, if using a touch screen then tapping the icon will display the menu options shown below. Select 'Settings' and then 'Continue'.



All Settings:



info@sensurity.com
www.sensurity.com

From within 'All Settings' configuration information for the following can be viewed, changed or saved.

- Microwave
- Dead zone
- Alarms
- IP Address
- GPS
- Graph
- Firmware
- Disable Alarms
- Polling

Microwave Settings

Select between the three different Algorithms A, B or C. Set the Sensitivity of the selected algorithm and the range, distance between Rx and Tx.

Operating Mode

Configure device as Transmitter or Receiver.

Operating Channel

Select Operating Channel between 1 and 37. Both Transmitter and Receiver must be configured to operate on the same channel.

Algorithm A

"Detect All Events" – Suitable for perimeters that have a "sterile zone"

Algorithm B

Optimum rejection of fast moving objects such as small animals, thrown objects and birds and a combination of DSP techniques rejecting parallel movement. Suitable for areas with small animals. Will detect walking and running events. Will not detect stealth attacks such as crawling.

Algorithm C

Combination of DSP techniques rejecting parallel movement, fast moving objects, small animals and foliage. Will detect walking, running and stealth attacks such as crawling. Suitable for installs close to paths and roadways or narrow corridors.

Sensitivity

Set the sensitivity of the configured algorithm between 0 and 7 where 0 is the least sensitive and 7 is the most sensitive.

Range

Set the actual distance between the Transmitter and Receiver in meters, up to a maximum of 200m.

Deadzone Settings

Set the sensitivity of the Upper and Lower IR Deadzones between 0 and 7. A value of 0 disables the Deadzones whereas a value of 7 sets them to the most sensitive value. Reduce the sensitivity is nuisance Deadzone alarms are occurring.

Deadzones are only available on Halo and not Vigil.

Firmware

Allows for a new firmware load to be distributed from a remote location to each Halo device.

This functionality is not supported on Vigil.

Alarm Mappings

Relay settings can be configured to be Normally Open or Normally Closed, along with the duration that they are to be activated. Alarms can easily be selected to activate either Relay.

Relay 1 – Normally Open/Normally Closed/Disabled

Relay 2 – Normally Open/Normally Closed/Disabled

Relay On Duration – 0 to 30 seconds, individually selectable for each Relay.

Alarms – Select check box for alarms to activate Relay 1 and select check box for those to activate Relay 2.

Only Relay 1 is available on Vigil.

IP Settings/Network Settings

This allows the Halo or Vigil device to be integrated into any network configuration and communicate with the PC hosting the UNIVERSE application. Parameters that can be configured include:

- IPv4 Address
- IPv4 Gateway
- IPv4 Netmask
- Server Address – Adapter IP Address on PC running UNIVERSE
- Server Port - Slave port of Network

Graph

Only available for the Receiver, when enabled displays a real-time graph of the received signal strength (RSSI in counts). Average RSSI is 2000 counts.

GPS Settings

The GPS location can be determined from the Halo on-board GPS, however in locations where the signal may be low or for Vigil devices, these may be dragged and dropped to the exact location on Google maps and saved.

Whether the UNIVERSE uses the GPS location obtained from the device or from a location previously saved by the application can be set here.

GPS is only available on Halo and not on Vigil.

Disable Alarms

Select to disabled for this device for up to 4 minutes.

Device Pairing

All Sensurity devices work in pairs as a Transmitter and Receiver. When an intrusion occurs between a Transmitter and Receiver, although it is the Receiver which detects the intrusion both the devices show as “Alarmed”.

1. Establish which icons, Transmitter and Receiver, are to be paired
2. Drag and drop one icon over the other.
3. Pairing is complete - This will colour code the icons and set the Transmitter and Receiver to the same operating channel.

info@sensurity.com
www.sensurity.com

Alarms

Alarms

When an alarm occurs, an alarm notice pop-up will appear. If you click on the notice you will be taken to the Alarm View associated with the triggered device.

Types of alarm notices:

1. **MICROWAVE** – A microwave intrusion alarm has been triggered
2. U**PPER DEADZONE** – An upper dead zone intrusion alarm has been triggered
3. **LOWER DEADZONE** – A lower dead zone intrusion alarm has been triggered
4. **HUB DEVICE CONNECT** – An IP device has connected to a network
5. **HUB DEVICE DISCONNECT** – An IP device has disconnected from a network
6. **CONNECT** – An OSDP Peripheral Device has successfully connected to an OSDP network and alarm polling has commenced
7. **DISCONNECT** – An OSDP Peripheral Device has disconnected from a OSDP network ◦
8. E**NVIRONMENTAL** – An environmental alarm has been triggered (e.g. excessive temperature gradient, low/high temperature threshold exceeded)
9. E**RROR** – A device error alarm has been triggered
10. **POWER** – A device power alarm has occurred
11. **TAMPER** – A device tamper alarm has occurred
12. **ADC 0** – An input device alarm has been triggered on input 0
13. **ADC 1** – An input device alarm has been triggered on input 1
14. **ADC 2** – An input device alarm has been triggered on input 2
15. **ADC 3** – An input device alarm has been triggered on input 3
16. **HUB CONNECT** – The communications interface of an OSDP network has been initialised
17. H**UB DISCONNECT** – The communications interface of an OSDP network has been stopped
18. **UNKNOWN** – An unspecified alarm event has occurred

To View all Alarms

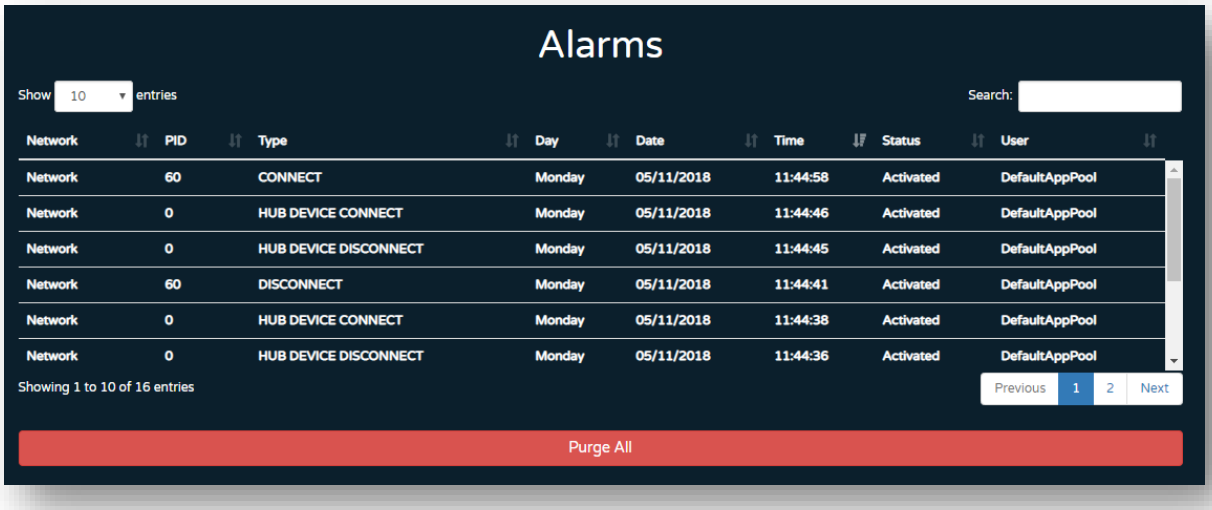
On the Dashboard click the “Alarms” tile.

To View Alarms by Device

From the Dashboard click “Networks”, double-click the required network and then click on the required Device. Select “Alarms” from the menu.

info@sensurity.com
www.sensurity.com

Alarms



Acknowledging and Accepting Alarms

When an Alarm condition occurs, the user may Acknowledge the alarm to indicate that the alarm condition is known and that further action will be taken.

Once an investigation into the alarm has taken place the alarm may be Accepted to indicate that the alarm condition has been dealt with.

To Acknowledge

Select the alarm and right click, check ‘Acknowledge’ and select ‘Continue’. This will set the alarm status to Acknowledged. The alarm will appear in the list as ‘Acknowledged’.

To Accept

Select the alarm and right click, check ‘Accept’ and select ‘Continue’. This will set the alarm to Accepted and it will no longer be visible in the alarms list, it will still exist in the database.

To Save Alarms To File

Select the toolbox ( ) to export the alarm list to a CSV file. The file will be saves to the PC desktop.

info@sensurity.com
www.sensurity.com

Alarms

SMS Text Messages and Voice Call

If the SMS message option is selected during user creation, then Alarm alerts will be sent to the associated mobile telephone number, containing the following information transmitter and receiver:

- Alarm Type
- Network on which the Alarm has occurred
- The ODSP address of the triggered Device
- A link to the Device's location on Google Maps

Users may also opt-in to receive a voice call with this same information, in this instance the link to the device location on Google Maps is not available.

To edit these settings, from the main Dashboard go to, Users → Users, click 'Edit' on the required user and check or uncheck the box for "Can Receive SMS".

Once selected, to receive SMS, a validation of contact details is required. To do this:

- Click on the 'SMS' tile which has now appeared on the Dashboard.
- Select 'Verify Caller ID'
- Enter the supplied code into the phone using the keypad as requested.
- A confirmation message will be received if the phone number has been successfully validated.

Alarms

Historical Alarms

Purged Alarm activity can be viewed on this screen. Alarms may be searched for a specific Alarm Type, Network ID or Day/Date on which the alarm occurred. Just start typing the required information into the search field.

Purging Alarms

Purging Alarms clears the current Alarms List and stores them in the database, freeing up memory to accommodate further alarms. It is recommended as a housekeeping exercise that the Alarms are purged on a regular basis.

To do this, click the “Alarms” tile on the dashboard and then click “Purge All”. Purged alarms will not be deleted and can be viewed in the Historical Alarms screen.

Updating Alarms Remotely

Alarms may be updaterd remotely via SMS, to do this follow the steps below:

1. Start Ngrok as explained in the Ngrok section.
2. Open the Ngrok Configuration Tile displayed on the main Dashboard
3. Enter the Ngrok URL to configure the SMS Remote Acknowledgement/Accept feature as shown in example below.
4. When an event occurs two additional SMS kinks will be sent to the configured mobile number, one for acknowledge and one for accept. Simple click on the required link.

info@sensurity.com
www.sensurity.com

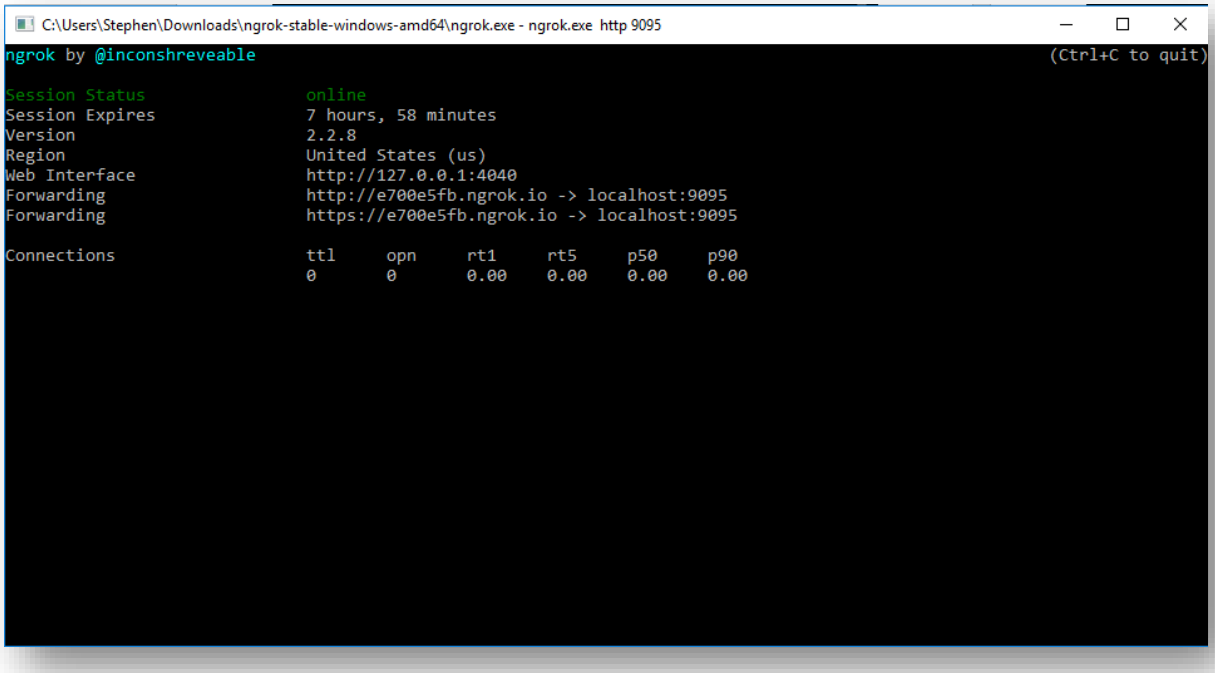
Remote Web Application - Ngrok

To access the web application remotely use the latest version of ngrok. This can be downloaded from the following link:

https://ngrok.com/download

Download and run on the PC that has is running the UNIVERSE application. Extract all and place 'ngrok.exe' in the Documents Folder for later use.

1. Double click ngrok.exe.
2. Enter ngrok.exe http 9095 in the pop-up console window.
3. The remote application can now be accessed via the http forwarding port using the supplied link. In the case below the link is http://e700e5fb.ngrok.io.



Note, this is a temporary link and will be lost is the remote PC is restarted. If the Ngrok session is restart a new link will be supplied. To maintain the link over PC restart then a Ngrok subscription is required, the link can then be configured as required with a user specified domain i.e. http://sensurity.ngrok.io.

Updates

Updates

To ensure you receive notifications when updates are available, please subscribe to our newsletter at www.sensurity.com/news

Before installing a new update, you must uninstall your current version. To uninstall, go to your computer's Control Panel and choose Programs and Features.

Find the UNIVERSE program in the list, click it, then click Uninstall.

To install the most recent version of UNIVERSE, go to https://sensurity.com/our-software and follow the instructions.

info@sensurity.com
www.sensurity.com