Site Monitor

Version 5.3

1 Table of contents

1 Table of contents 2
2 Installation 3
2.1 Components 3
2.1.1 Monitoring Service 3
2.1.2 Desktop User Interface 3
2.1.3 Web User Interface 3
2.2 Requirements 3
3 Configuration 4
3.1 Monitoring Service 4
3.2 Desktop User Interface 4
3.3 Web User Interface 4
3.4 Server Configuration Tool 5
4 Administration 6
4.1 Initial Setup and Login 6
4.2 Users 6
4.3 Networks 7
4.3.1 Connection types 7
4.3.2 Panels 8
4.3.3 Snoozing 8
4.3.4 Adding an Eco232 Panel 8
4.4 Events 9
4.4.1 Conditions 9
4.4.2 Actions 9
4.5 Reports 9
4.5.1 Interface History 9
4.5.2 Network History 9
5 Normal Operation 10
5.1 Main window 10
5.1.1 Navigation 10
5.2 Devices 10
5.3 Scanning Analogue Values 10
5.4 Enable / Disable 11
6 Cassini Web Server Configuration 12

2 Installation

2.1 Components

Site Monitor version 5 is split into three distinct components. With suitable configuration, there is no requirement to install all components on the same PC, but you may do so if you wish.

2.1.1 Monitoring Service

This component runs as a pair of Windows services in the background while ever the PC is turned on, assuming the services are set to automatic start up. To change this behaviour please refer to the documentation for your version of Windows for more details on service administration. This component is responsible for providing the link from the PC to the panel network, event monitoring and the XML interface to clients.

2.1.2 Desktop User Interface

This is a dialog based Windows client suitable for connecting to the monitoring service via TCP for viewing and configuring the network status and events. This client provides full access to all logged and real-time monitoring events as well as the ability to perform simple commands such as enable, disable and analogue value retrieval. Depending on your edition, this software may require a license key.

2.1.3 Web User Interface

Providing the same functionality as the desktop user interface, this ASP.Net web application allows access via a web browser (such as Internet Explorer, Mozilla, Opera...etc.). This gives the advantage of quick access from any location or computer without the need to install the desktop user interface client. To use this component, a suitable ASP.Net enabled web server must be installed. It is also important to note that no web server is provided by the Site Monitor package. However, you can use any ASP.Net 2 enabled web server, such as Microsoft IIS or UltiDev Cassini.

2.2 Requirements

All components require that Microsoft .Net v2.0 (or compatible) be installed. The monitoring service also requires Microsoft SQL Server Compact v3.5 SP1 or above and a Windows based PC capable of running services (Microsoft Windows 2000 and above). For the connection to the network, your PC will also require at least one available Serial or USB port.

To use the web user interface component, you must ensure a suitable ASP.Net enabled web server is installed. This web interface is designed for all standard compliant browsers, such Internet Explorer 6 and above, Mozilla, Opera, Safari...etc.

3 Configuration

3.1 Monitoring Service

By default, the service listens on port 60000 for incoming connections from clients. If however you do wish to change this, it can be configured by loading the Server Configuration application located within the Start Menu. If you would like to access this service from a remote location, such as from other locally networked computers or from across the Internet, then you will need to ensure you open port 60000 (or the port you have changed this value to) on any appropriate router or firewall.

Note 1: You must restart the service for any changes to take affect.

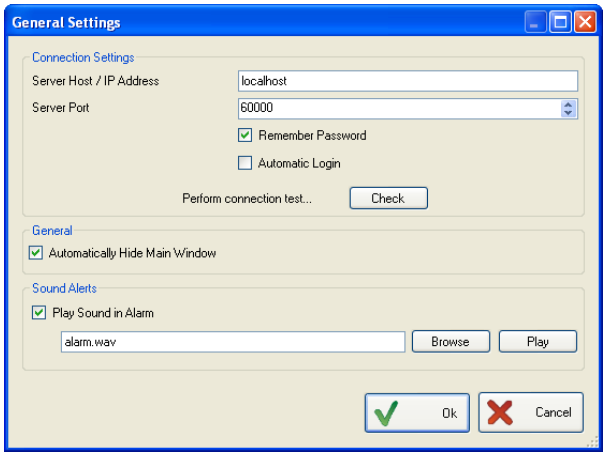
Note 2: You need to know this number when connecting a client, see below for details.

Note 3: Remote access will require the configuration of any appropriate router or firewall.

If you do need to manually Start, Stop or Restart the service, then this can be done by clicking on the appropriate short cut located within the Start Menu.

3.2 Desktop User Interface

By default, the interface connects on port 60000 to a service on the local PC. In most cases, this will work just fine. However, if you have changed the port (as above) or are running the service on a different computer and are trying to access it over a network (LAN, VPN, the Internet etc.), you will be asked to enter the host name of the computer running the service and port number it is configured to listen on. If you are having difficulty with any of the above, please contact your network administrator for assistance.



These options can be accessed by clicking on the spanner icon on the login window or the 'Settings' drop down menu on the main window. From this icon you also have access to general application behaviour settings and also the sound alert settings. These enable you to play specific warning sounds when the Desktop User Interface detects state changes.

3.3 Web User Interface

Initially you will need to ensure you have a ASP.Net enabled web server installed, which will most likely be either Microsoft IIS or UltiDev Cassini. Then you will need to register the web user interface with your web server. If you had Cassini installed already during installation of Site Monitor, then you will have been given the option to automatically register the web user interface. However, to manually perform the register, you will need the appropriate directory path. This should be the 'web' sub directory, within the main installation folder of Site Monitor.

Once the web user interface is registered then you may need to configure the connection settings to the service. By default, this also connects on port 60000 to a service on the local PC. In most cases, this will work just fine. However, if you have changed the port (as above) or are running the service on a different computer and are trying to access it over a network (LAN, VPN, the Internet etc.), you will need to update the web user interface settings. To modify the standard behaviour, this can be configured by loading the Server Configuration application located within the Start Menu.

For further information on the actual setup of UltiDev Cassini, then please refer to section 6 in this document.

3.4 Server Configuration Tool

If you have installed either the Monitoring Service or the Web User Interface, you will find a short cut item within the Start Menu which loads the Server Configuration tool. This tool will enable you to quickly change the vital settings that affect those two services. The primary purpose of this tool is to change the standard port value. Any changes to the service settings will automatically result in a prompt to restart the service for the changes to take effect.

- **Listen on Port** – This is the port value which the Monitoring Service will accept connections.
- **Database Path** – The physical location of the Monitoring Service database.
- **Enable Anti-Hammering** – This option enables the built in password protection system. This means any user who fails to provide a valid username and password five times in row will be locked out for up to 10 minutes.
- **Server Host / IP Address –** This should be the host or IP address of the computer running the Monitoring Service. If both the web and service are running on the same computer, then 'localhost' will generally work fine.
- **Port** – This should be the port value of the computer running the Monitoring Service. If both the web and service are running on the same computer, then this value should match the 'Listen on Port' setting.

4 Administration

4.1 Initial Setup and Login

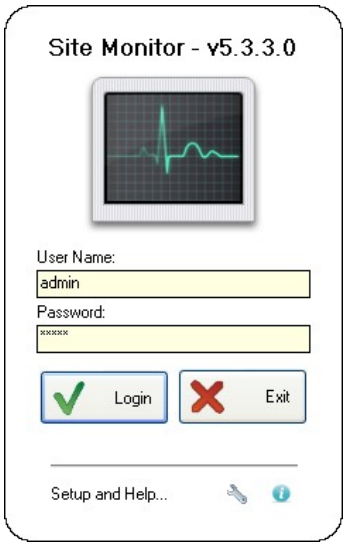
Once the desired components are installed, running and connected, you're ready to setup your new monitoring system. When using the software for the first time and you are prompted with a user name and password window, use the following credentials:

Username: **admin**

Password: **admin**

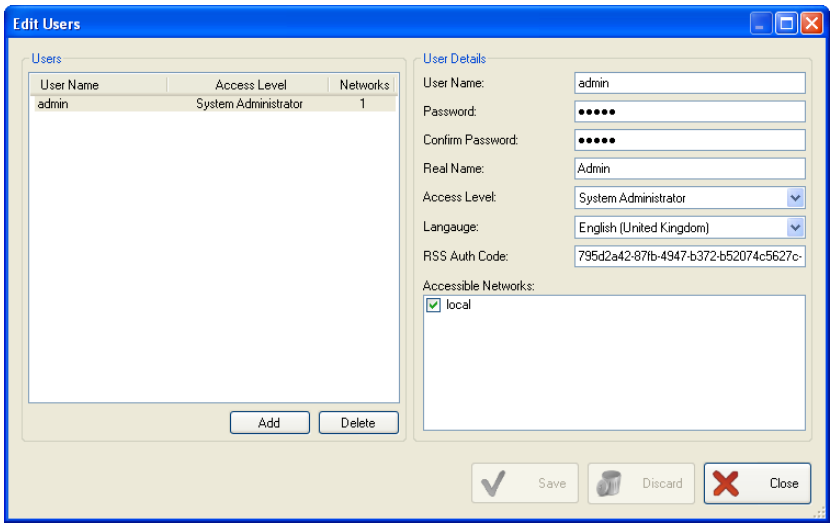
Please note that passwords are case sensitive. Every time you load the desktop user interface or access the web user interface, you will be required to re-login.

IMPORTANT: We strongly recommend you change the password for the default 'admin' user.



4.2 Users

Site Monitor is designed to enable local and remote access, and so to ensure security is maintained, access is restricted to specific username and passwords. There are also four available access levels which users can be assigned to. These ensure only the right individuals can access the appropriate features of Site Monitor. The default 'admin' account is configured to enable full access, and so via that account you can create as many users as your system requires.



Access levels and available features:-

Feature	System Administrator	Network Administrator	Technician	Viewer
Manage Networks	Yes	-	-	-
Manage Panels	Yes	Yes	-	-
Edit Users	Yes	-	-	-
Edit Events	Yes	-	-	-
Global Commands	Yes	Yes	Yes	-
Enable Commands	Yes	Yes	Yes	-
Disable Commands	Yes	Yes	Yes	-
View Logs	Yes	Yes	Yes	Yes
View Status	Yes	Yes	Yes	Yes
Generate Reports	Yes	Yes	Yes	Yes
Clear History Log	Yes	Yes	Yes	Yes

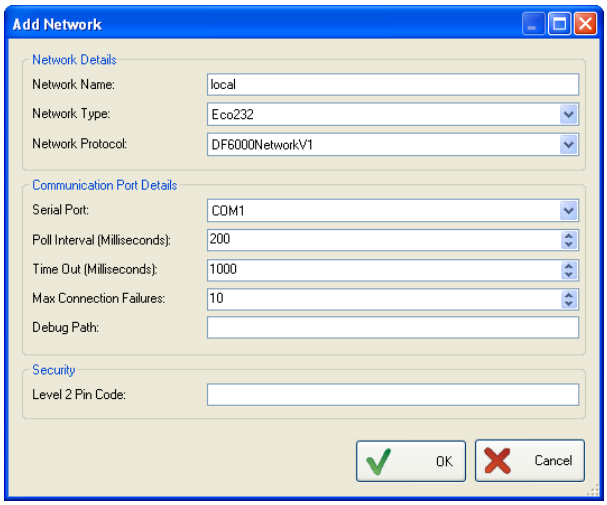
- **System Administrator**: Full access for setup and system management. The default account 'admin' is set to this.
- **Network Administrator**: Reduced access for setup and network management.
- **Technician**: For the typical user who wishes to view network status and logs, and to allow 'Level 2' equivalent control (e.g. enable/disable devices, global reset, global silence... etc.).
- **Viewer**: Highly restricted user who can only view network status.

The setting 'RSS Auth Code' is used only by the web user interface and should be pre-filled with a cryptic value. This enables RSS and Atom feeds to be supported by compatible readers. We recommend that only unique and in-guessable values be entered here. Additionally, if you want to disable support for RSS and Atom feeds for this particular user, you can simply delete the value and leave it blank.

All users can change their own language and password. We recommend that most systems have at least two System Administrators to protect against password loss.

4.3 Networks

A network represents a single connection to a panel network. If the service PC has more than one serial/USB port, then it is possible to connect and manage multiple networks from a single PC. However, in almost all cases, only a single network is required.



4.3.1 Connection types

Site Monitor 5 supports pluggable connection types, that is, it can be extended to connect using a variety of methods. Currently only one type is provided, the Eco232. Users of previous versions of Site Monitor will be familiar with this device.

4.3.1.1 Eco232

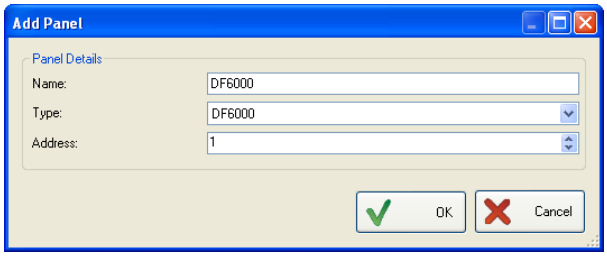
Most settings for this device do not need changing from the defaults. “Serial Port” does however need to be set correctly to match whichever serial port on the PC the device is connected to. Note that once a network has been added, the serial port assigned to it will be in use while ever the monitoring service is running. See Snoozing if you need to use the serial port for something else temporarily.

4.3.1.2 Level 2 Pin Code

For additional security you can assign a pin code to a network. This will ensure that any users with access to features that can alter the state of the network, such as Enable, Disable and Global Reset, they can only do so if they know the right pin code. Leaving this option blank will mean no pin code is required. We recommend that this code be set to the same as the level 2 code on the panels.

4.3.2 Panels

To gain access to all features of Site Monitor, you need to provide it with details of your network. You can either manually add the panels or more simply retrieve this information from a Site Installer database file.



4.3.2.1 Add Panel

When adding a panel, you will be prompted for the panel name, type and network address. It is important that these details accurately match the setup of the real physical network and panel. Once a panel has been added, you can then select 'Find Devices/Zones'. This will perform a scan of the panel and retrieve a list of all accessible devices and zones.

4.3.2.2 Sync with Site Installer

This can be done by selecting this option and providing the original Site Installer database with which the network panels were commissioned. If the site is changed at any time in the future, it is recommended that you upload the modified Site Installer database into Site Monitor.

4.3.3 Snoozing

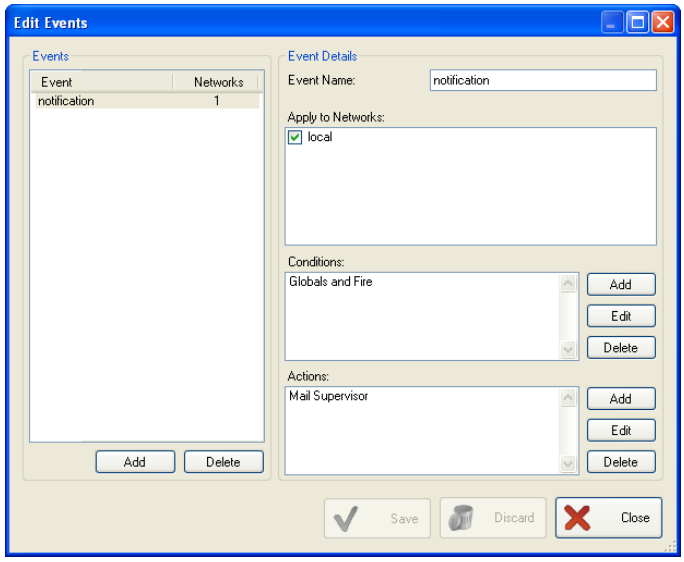
It may be desirable to stop monitoring and disconnect from a network for a short period of time, such as to use the serial port on the PC for some other purpose. Snoozing a network will allow you to do this. After the given time period has elapsed, the monitoring service will automatically reconnect to the network and continue normal operations. Alternatively, you can unload the service by clicking on the 'Stop Services' short cut from within the Start Menu. To restart the service, simply click on 'Restart Services' short cut also located within the Start Menu.

Some devices, such as the Eco232, will buffer network messages for a period of time until the monitoring service collects them. In this case, the timestamps of these messages will reflect the time they were collected by the service, not the time they were originally transmitted by the panel.

4.3.4 Adding an Eco232 Panel

If your PC is connecting to the network via a Eco232 device, then it is recommended that you add a Eco232 device to the Panel list and assign it an appropriate address (this can be done via the normal Add Panel option). If you are using a Site Installer database, then we recommend you add an Eco232 device to that database prior to performing a Sync. Having a Eco232 panel added to the panel list gives the advantage of the device being able to monitor panels itself and for other panels to monitor it. Please note that from within Site Installer, it is not necessary to upload any commission data to the Eco232 device directly, it is simply added as an indicator to the real physical network design.

4.4 Events



Site Monitor is designed to run automatically and continuously, ensuring network activity is logged and users have a portal in which to quickly and remotely view the status of the network. As it is almost certain that incidents will occur while the a user is not observing, you can setup automated actions to run when specific conditions are met. A typical example is an email sent to a technician whenever a panel detects a fault.

Please Note: Only System Administrators can setup events.

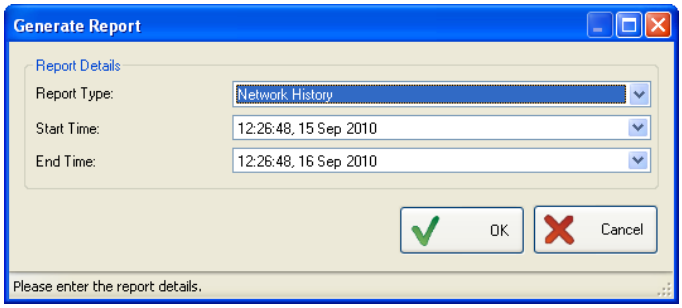
4.4.1 Conditions

Any packet received from the network can be used has a condition. This means that actions can be triggered if any panel is manually reset, goes into alarm, detects a fault and much more.

4.4.2 Actions

When a condition is met, its associated actions will be processed. Presently you can only define a 'Send Email' action, which allows you to send a brief description of the incident to a specific email address. To send the email to multiple addresses, separate the addresses in the 'To' field with ';' characters (e.g. *address1@domain.com;address2@domain.com*).

4.5 Reports



To simplify monitoring of past events, you can quickly generate HTML reports. When generating a report, you will prompted for the report type and the start and end times of the information included in the report. By default the start and end times will be set to the last 24 hours. You will then be asked to provide a location in which to save the report. Please be patient once the report generation as begun, as some systems which have been running for a long time will contain a lot of data and it may take a short period of time to generate and transfer the report to your system. Once a report has been made, it will automatically be opened and displayed.

4.5.1 Interface History

This represents all the messages stored by the service. This will reflect information such as completed device/zone scans, any detected problems (such as connection issues, bugs or setup errors) and more.

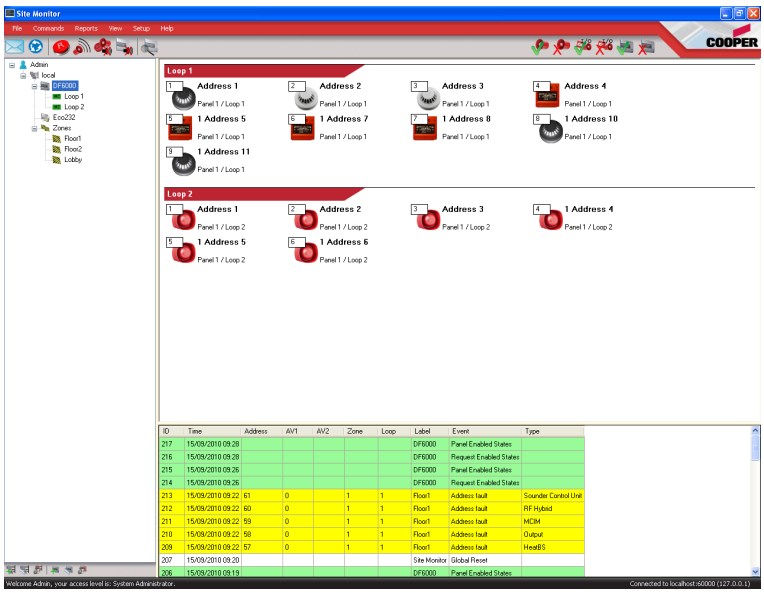
4.5.2 Network History

This is a record of all packets received off the network. This is essentially a log of everything that has occurred and includes information such as resets, faults, alarms, enabled/disabled commands and much more. This report is very similar to the history log that appears in Desktop and Web User Interfaces.

5 Normal Operation

5.1 Main window

Site Monitor's desktop and web user interfaces are designed to offer quick navigation amongst the various networks, panels, zones and devices that have been added. The interface also provides you with up to date information on the live status of everything on the network, highlighting any potential problems and logging all network activity.



5.1.1 Navigation

After you successfully log in, the main window will be shown. This is split into 3 distinct parts; the navigation tree on the left, the device view on the top right and the history log on the bottom right. Generally you will move around the elements of the network by selecting an item in the navigation tree. The device view and the history log will then update and display the appropriate information for your selection. The navigation tree is organised by networks, of which each contains a list of panels and a sub list of the available zones.

5.2 Devices

When you select a panel, loop or zone, the device view on the right will show a list of all available devices within the section you have chosen. Each device will be shown along with an image that represents what that particular device generally looks like. Additionally, each device contains some text detailing its name, location on the network and recent status information if available. The small white box overlaying the image represents the device's address on the loop. If the device is not in a normal state, it will be highlighted with a non-white colour. The following describes the meaning of these colours...

- None/White: Device is normal.
- Flashing Red: Device is in Alarm mode.
- Pink: Device is in Pre-Alarm mode.
- Yellow: There is a fault with the device.
- Grey: The device is disabled.

5.3 Scanning Analogue Values

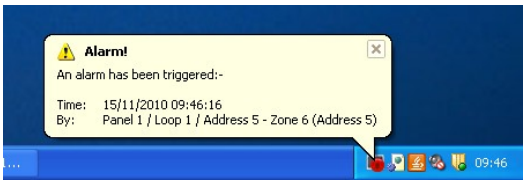
If you want to update the status of the devices, you can perform an Analogue Value Scan. This can be performed on a per panel, per loop, per zone or per device basis. To activate a scan, simple select the required network element and click on on the appropriate icon along the top of the window (Analogue Value Scan icons include a small magnifying glass). A single device scan will only take a few seconds but all others may take a few minutes, depending on the number of devices involved.

5.4 Enable / Disable

Cooper panels allow you to disable and enable various systems and devices, and so these options can also be accessed within Site Monitor. If you wish to enable or disable a device, simply select the device and click on the appropriate icon along the top of the window (enable icons have a green tick and disable icons have a red cross).

5.5 Desktop Interface Only Features

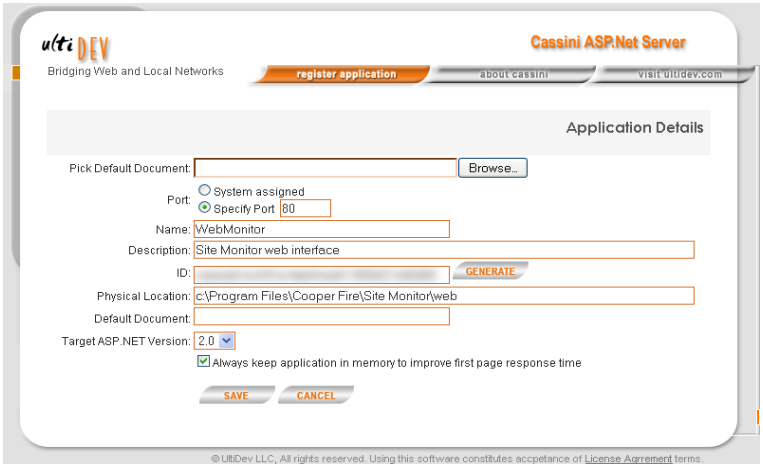
Because the desktop interface software is an installed product, it provides additional monitoring features which can provide easier access and more obvious alerts to problems. By default closing the main window will not exit the application but will instead minimise it to the tray icon area (the icons immediately adjacent to the system clock). You can quickly re-open Site Monitor by double clicking on the appropriate icon. Additionally, if an alarm condition is triggered in a selected network, a notification bubble will automatically appear in the tray icon area. There is also the option to play a warning sound. Combined these features provide you with an option to run a client permanently and so ensure any nearby or operating users should be quickly informed of a problem.



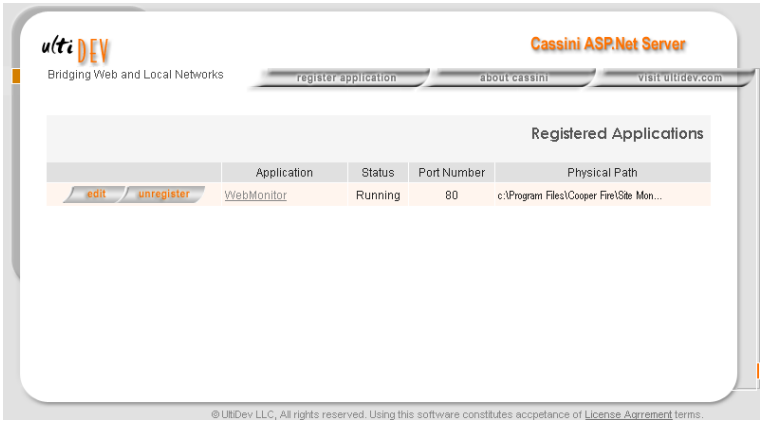
6 Cassini Web Server Configuration

This document only covers configuration of UltiDev Cassini as it is expected that anyone running Microsoft IIS knows the registration process.

1. Install UltiDev Cassini (freely available from http://www.ultidev.com/products/Cassini/) and start the Cassini Web Server Explorer.
2. Once your browser has opened and the configuration page is loaded, click “register application”.
3. Fill out the form as shown, noting the following:-
    1. Port: The default for all websites is 80, but this may conflict with another service. If you can't or don't want to use 80, your clients must be aware of this.
    2. Name and description: These can be filled out as you wish, they're just for your reference.
    3. ID: Use the generate button.
    4. Physical location: Must be the 'web' sub directory, within the main installation folder of Site Monitor.
    5. Target ASP .Net version: Must be 2.0.



4. Click save and if all is well, you will have a remotely available website for Site Monitor.



5. You can click the link in the “Application” column to go to your site.
6. It is important that you you stop the web server service during upgrades of Site Monitor.