AlcoMeasure®

Server

Server Software Manual

Rev 1.02, 3/05/2021

1 Contents

2 Introduction

AlcoMeasure Server (AMS) is a set of software components designed to streamline the remote management of AlcoMeasure devices. It is designed to be used in parallel with the AlcoMeasure Utility (AMU) desktop program. Where AMU connects to individual devices for configuration and data retrieval, AMS remotely monitors any number of connected devices at once without the need for an operator.

AMS automatically downloads the test log and device status from all connected devices, storing them in a database for access by the client. It can also be configured to send email or custom alerts when a test result on any connected device is recorded above a configurable threshold. Emails can also be generated by the system to notify if a device goes offline, and to periodically report the status of the server software.

AMS is designed to be deployed on a client's private network. The client can specify their own Microsoft SQL Server database or use the built in SQLite database. The database is completely open and accessible to the client. It has also been tested in the cloud running in a Microsoft Azure virtual machine. This could be managed by the client or managed by All-Systems Electronics at extra cost.

AMS provides a fully featured web interface with optional HTTPS security. This interface is useful for seeing the state of the server, database, and connected devices. It also allows the user to browse the log history of all connected units, with advanced filtering options to find all relevant data. The web interfaces home screen also shows all recent over-limit tests, as well as any recent server events.

To connect, the Server functionality must be unlocked in each AlcoMeasure device. They must also be configured with the Hostname/IP and Port of the AMS installation. Once configured, they will automatically connect to the server.

Every effort has been made to ensure the accuracy of this manual. All-Systems Electronics (ASE) reserves the right to make modifications to this manual, as well as the hardware and software referred to in this manual.

3 Product Information

3.1 Manufacturer

Postal Address	Contact	
All-Systems Electronics Pty. Ltd. 16 Hope Street Seven Hills, NSW 2147 Australia	Telephone: E-mail: Website:	+61 2 9624 4644 sales@all-systems.com.au www.all-systems.com.au

3.2 Distributor

Postal Address	Contact	
Breathalyser Sales & Service 128 O'Riordan Street Mascot, NSW 2020 Australia	Telephone: E-mail: Website:	+61 2 8338 1555 admin@breathalyser.com.au www.breathalyser.com.au

3.3 Specifications

Operating Systems	Microsoft Server 2012, 2016, 2019 Microsoft Windows 7, 8, 10 Ubuntu Linux 18.04.4 LTS, 20.04 LTS
Databases	SQLite3 Microsoft SQL Server 2012 or newer, including Express versions
Web Browser	Google Chrome, Firefox, Microsoft Edge (Required for the web interface)
Connectivity	TCP/IP, HTTP, HTTPS
Email functionality	Requires a separate SMTP server (Gmail, Outlook.com, or custom SMTP)
Default Webpage Port	80, 443
Default Device Port	26001
Licensing	Licensed per device connection Test mode (unlicensed) allows 1 device connection
Compatible Device Firmware	1.0800 and newer. Device serial numbers after 400 are required for HTTPS/SSL/TLS encryption. Contact the distributor for more information.

4 System Overview

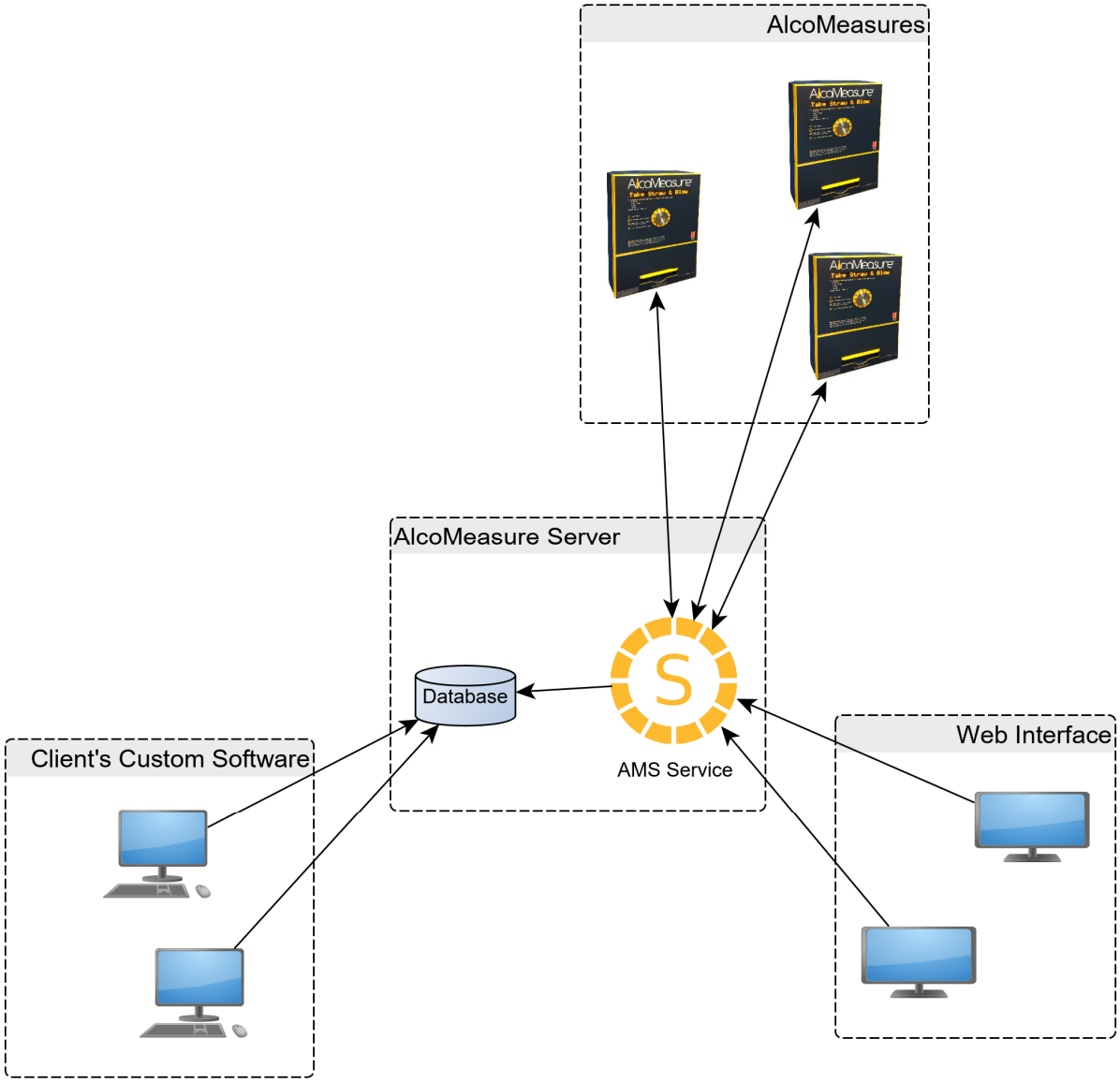


Figure 1 - Basic System Overview

As shown in Figure 1, the Server system is made up of several components.

The core components of the system are the server software, here labelled as “AMS Service”, the Database, and the Web Interface.

The AMS Service is responsible for collecting data from the AlcoMeasures and updating the database. It also provides the “Web Interface”. The AMS Service is proprietary, and it is not expected that the client would need to interface with this software. The AMS Service is discussed in more detail in section 6.2.

However, once the Database has been updated with information from the connected AlcoMeasures, this data is available for the client to use freely. Normally the client would not need to access the database directly. However,

if they wish to write custom software to interact with the system then the database is available for them to do so. Further information on the database can be found in section 14.

The Web Interface is the built-in user interface for accessing the server. It provides easy access to the Server's current status, as well as providing a mechanism for searching through log events from all connected AlcoMeasures. It can be accessed with any modern web browser and provides https security and a login if required. Further information on the web interface can be found in section 7.

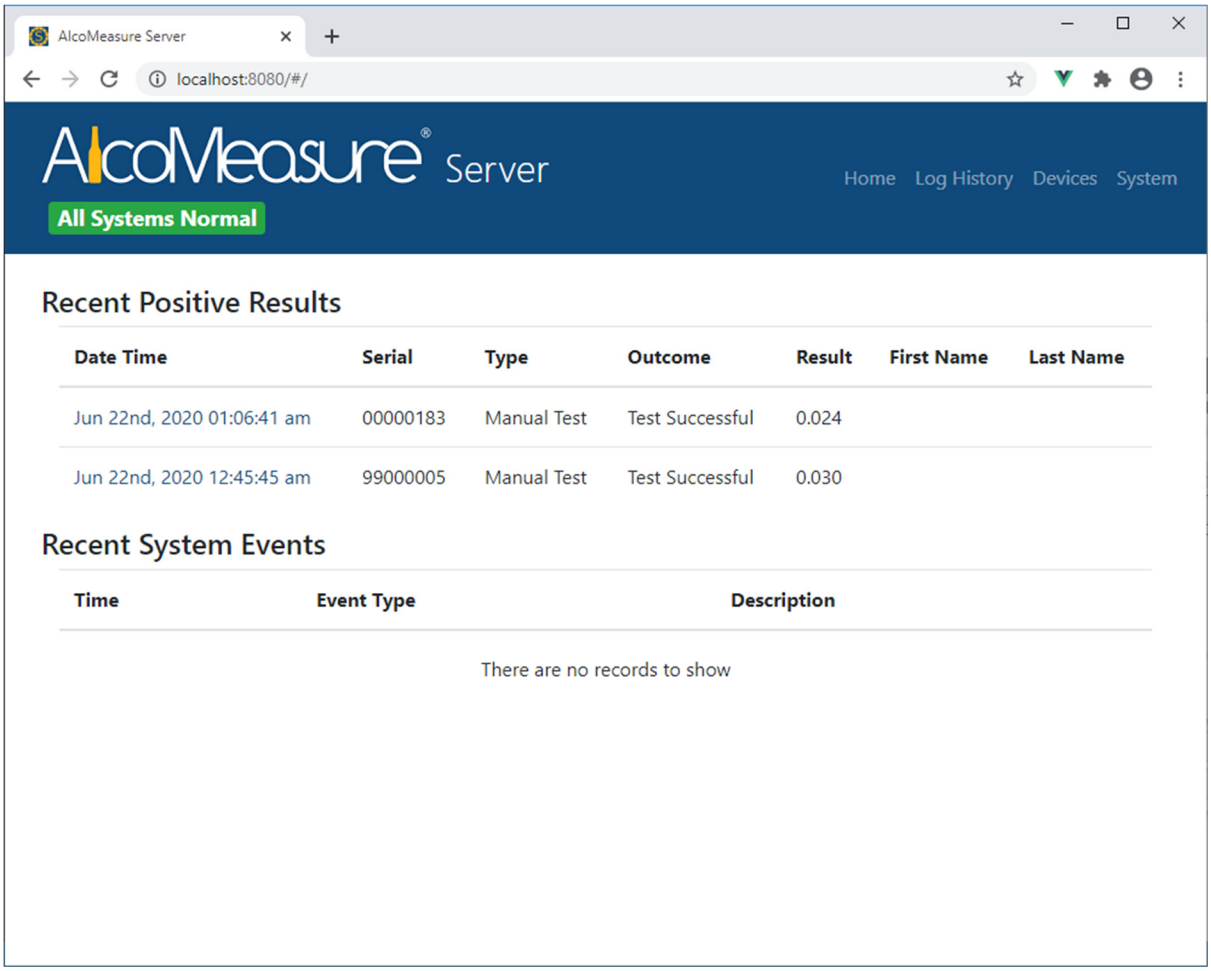


Figure 2 - Web Interface Home Page

5 AlcoMeasure Server Installation

The AMS software is provided as a Windows Setup executable. It must be run at administration level since it will register and start a windows service, as well as adding a system tray icon to the auto-start list.

If the server is already installed, the setup program will warn that it must close the existing programs. Select the "Automatically close the applications" option and press Next[1]. Once completed, the service should be running and there should be an AMS icon in the System Tray.

5.1 Configuring Ethernet Ports

The Windows firewall needs to be configured to allow traffic on 2 separate ports.

AlcoMeasure devices will connect to the server by default on port 26001. This needs to be opened to allow incoming connections from over the network.

If the web interface is to be used, it is available on port 80 by default. AMS will function properly without external access to this port, however it may be useful to open this port for troubleshooting and diagnostics purposes.

Alternatively, the web interface can be configured for HTTPS, which uses port 443 by default. In this case, port 443 would need to be opened in the firewall to provide external access.

[1] It sometimes takes a few seconds to close all current connections and leave the database in a stable condition. If Setup complains that it couldn't close the program, simply press "Retry".

6 Software Architecture

The Server software consists of a Windows Service called AlcoMeasureServer.exe, and a System Tray application that can control the service called AlcoMeasureServerController.exe. Upon installation, the service is registered in Windows to auto start.

The System Tray application auto-starts with Windows or can alternatively be started from the Start Menu where it is simply named “AlcoMeasure Server”.

The service is configured using a file named AlcoMeasureServer.ini. This is normally configured using the “Server Configuration” option in the System Tray Application. However, it can be edited manually. Any time this file is changed the service must be restarted for the change to take effect. See section 9 for more information.

A licence file named AMSLicence.ini is required for the product to allow devices to connect. Without a valid licence file AMS will run in “Test Mode” which allows for a single device to connect. See section 11 for more information.

AMS requires access to a database. By default, it will create an SQLite database called “ams.db”, although alternative databases can be configured. See section 13 for more information.

6.1.1 File Locations

The following paths assume a Windows installation on C drive.

6.1.1.1 Default Executable Location

- C:\Program Files (x86)\All-Systems Electronics\AlcoMeasure Server
    - AlcoMeasureServer.exe
    - AlcoMeasureServerController.exe

6.1.1.2 Default Data Location

- C:\ProgramData\AlcoMeasureServer:
    - AlcoMeasureServer.ini
    - ams.db
    - AMSLicence.ini

6.2 Windows Service

The AlcoMeasureServer.exe service is a normal windows service, and can be controlled in any of three ways:

- System Tray Application, as described in section 6.3.
- Windows Task Manager Services tab.
- Windows Services tool.

When the service is run for the first time it will configure itself with the following recovery options:

- First crash, restart service in 60 seconds.
- Second crash, restart service in 120 seconds.

- Third crash, and every after, restart service in 10 minutes.
- The crash counter will be reset after 1 day.

The recovery settings can be manually configured using the Windows Services tool.

6.3 System Tray Application

The system tray icon gives a clue as to the current state of the service:

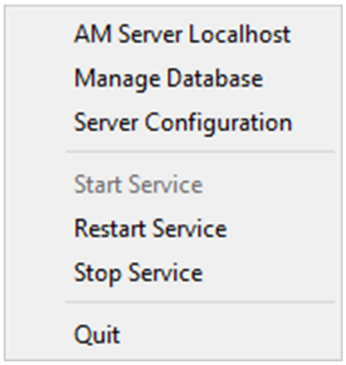
 - Service is uninstalled.

 - Service is stopped.

 - Service is starting.

 - Service is running.

Right clicking the system tray icon provides the following menu:



AM Server Localhost: Opens the web interface.

Manage Database: Opens a form where the database can be managed. The database connection can also be set/changed from this form.

Server Configuration: Opens a form where the server can be configured. The server must always be restarted after changing these settings for them to take effect. The “Restart Service” option can be used for this.

Start Service: Starts the Windows service.

Restart Service: Restarts the Windows service.

Stop Service: Stops the Windows service.

Quit: Closes the system tray application. The service will continue running in the background if installed.

6.4 Event Log

By default, the windows service will post events into the Windows Event Log that can be retrieved by the system administrator for troubleshooting purposes. These events are posted under “Windows Logs\Application” in the Event Viewer and have “AlcoMeasureServer” as the Source.

These events are also posted to the “EventLog” table in the database once the database is configured. See section 7 for more information on how to access the Event Log in the Web Interface.

Finally, if email notifications are enabled then events can be automatically emailed to the administrator when they occur. The configuration of email notifications is described in section 10.4.

7 Web Interface

AMS's Web Interface is the default User Interface for monitoring the system and accessing data retrieved from the managed AlcoMeasures. It is served up by the Windows service and can be accessed from any modern desktop browser. Being entirely built in Bootstrap Vue, it can also be easily viewed via mobile phone or tablet.

The Web Interface has several configurable items, especially concerning security. These are described in detail in section 9.

7.1 Site Layout

7.1.1 Menu Bar

The Interface's Menu Bar sits at the very top of the web site. It consists of the AlcoMeasure Logo on the top left, the Status Summary on the bottom left, and the menu on the right.

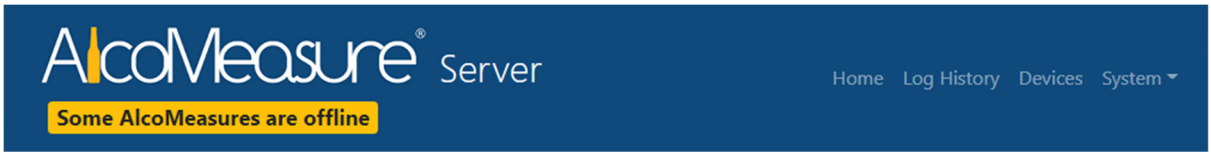


Figure 3 - Menu Bar with 1 AlcoMeasure disconnected

The Status Summary gives the status of the server at a glance. It will usually display one of the following messages:

All Systems Normal: All expected devices are connected and operating normally.

All AlcoMeasures are offline: No devices are currently connected. The "System" page may be used to work out why no devices are connected.

Some AlcoMeasures are offline: Some devices are not currently connected. The "Devices" page will show what devices are currently disconnected.

Server Unavailable: The web page has loaded, but the server software has since stopped responding. Perhaps the service is no longer running.

It may also display short error messages. Clicking on the Status Summary will navigate to the "System Status" tab, where the problem can be more easily diagnosed.

The menu on the far right provides buttons to navigate to all the main tabs of the Web Interface. If the screen width is small enough, the menu will collapse into a drop-down menu. This makes it easier to navigate on devices with small screens.

7.2 Home

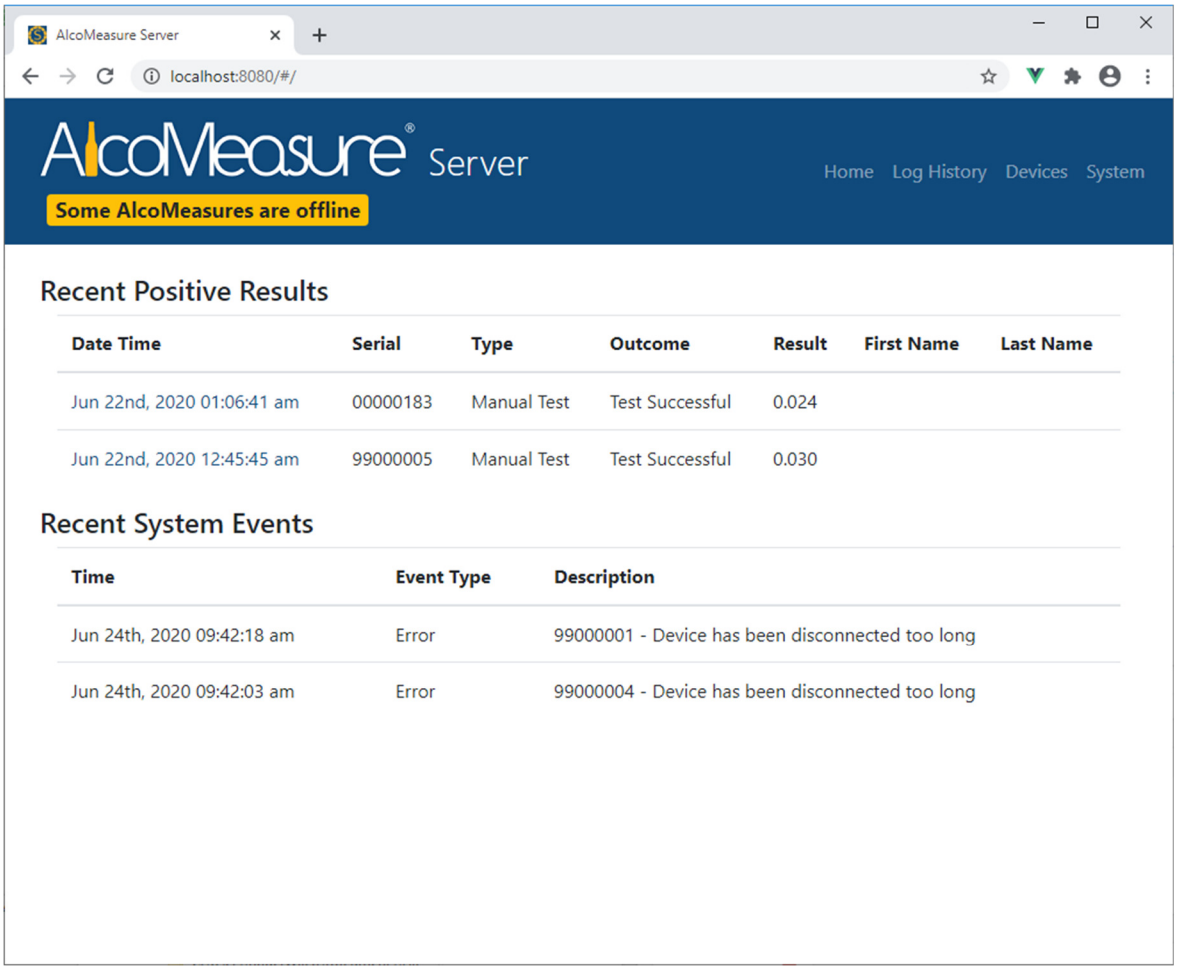


Figure 4 - Home Screen showing recent tests and system events.

The Home page provides a summary of recent events that have occurred.

7.2.1 Recent Positive Results

Any positive tests that have been recorded over the past 14 days will be displayed here.

The default limit is 0.001 g/210L, however this is configurable. See section 9 for more information.

This table mostly functions the same as the Log History table, described in section 7.3.

The Serial, Location and Device Name fields will be displayed here if they are selected on the Log History page.

7.2.2 Recent System Events

Any “Warning” or “Error” level system events that have occurred in the last 7 days will be displayed here.

This table mostly functions the same as the System Events table, described in section 7.5.2.

7.3 Log History

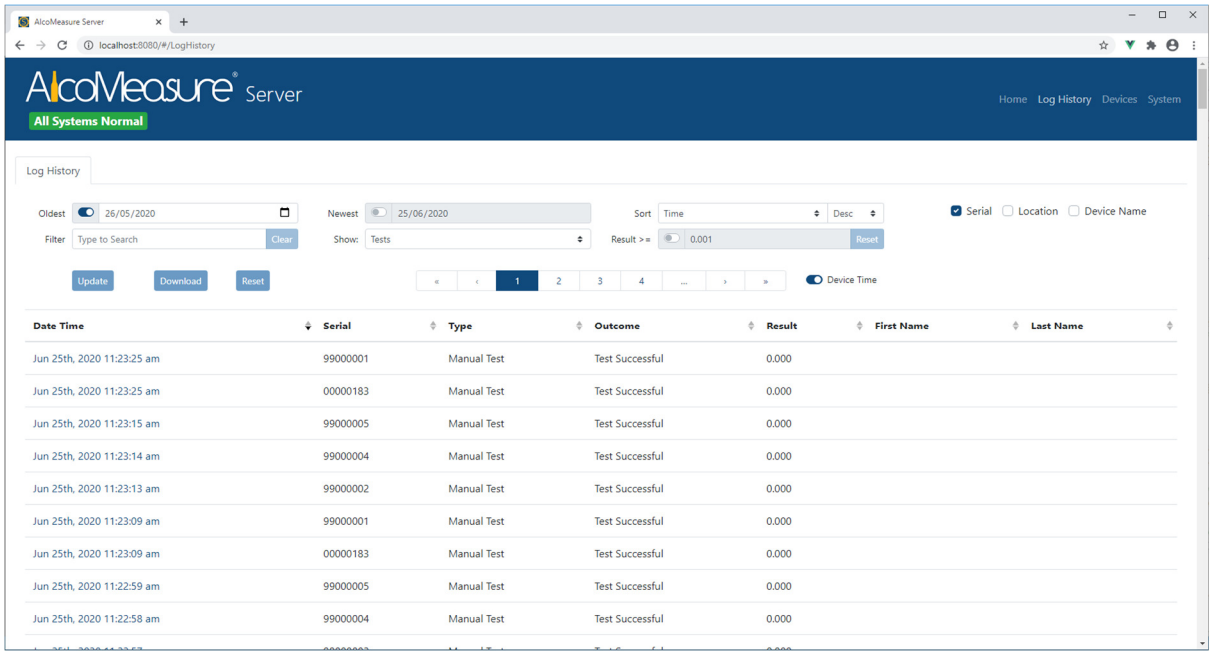


Figure 5 - Log History page showing recent tests from all devices.

The Log History page is the main section for searching and viewing data from the AlcoMeasure devices.

When first opened, it will load the last month worth of logs from all devices, using whatever filter options were used last time the form was opened.

7.3.1 Filtering Logs

Filter options can be changed, and the columns to display can also be changed. These will take effect after the "Update" button is pressed, or next time the page is loaded.

Some filter options will be saved as browser cookies and will remain next time the page is accessed. These are:

- The columns to show (Serial, Location, Device Name)[2]
- The log type to Show (Tests, Calibrations, Everything)
- The result to filter
- Whether to display device time or browser time

These cookies also effect how the logs are displayed on the Home page.

The log results can further be filtered using the "Filter" string. This will be applied to all columns except Date Time. If multiple words are put in the Filter, separated by a space, then a log record will need to contain a column containing both words for it to be shown.

[2] Enabling any of these columns can slow down the log search, as they are found in a separate database table.

For example, if we want to find any errors for the device with serial number 00000956, we should first ensure that the “Serial” column is enabled. Then in the Filter box, we should put: “00000956 error”, without quotation marks, and press “Update”.

The log table will display a maximum of 250 logs at a time. If more than this exist with the current filter options, they can be accessed by selecting subsequent pages at the top or bottom of the table.

7.3.2 Downloading Logs

Pressing the “Download” button will download the filtered results as a CSV file. If the displayed results are split over multiple pages, all results will still be downloaded. This will download all data except for any associated photos. These can be accessed by viewing each log records Log Report.

7.3.3 Log Reports

Every log record in the Log History table can be viewed as a Log Report. Simply click on the Date Time for the log record, and a report will be generated and shown in a new tab. This report can then be saved to PDF or printed using your browser built in functionality.

If the log type is a test, then the report will be labelled “Test Report”. It will contain the result, the result limit, the users ID or First and Last name, if applicable. It will also display any photos that were taken at the time of the test.

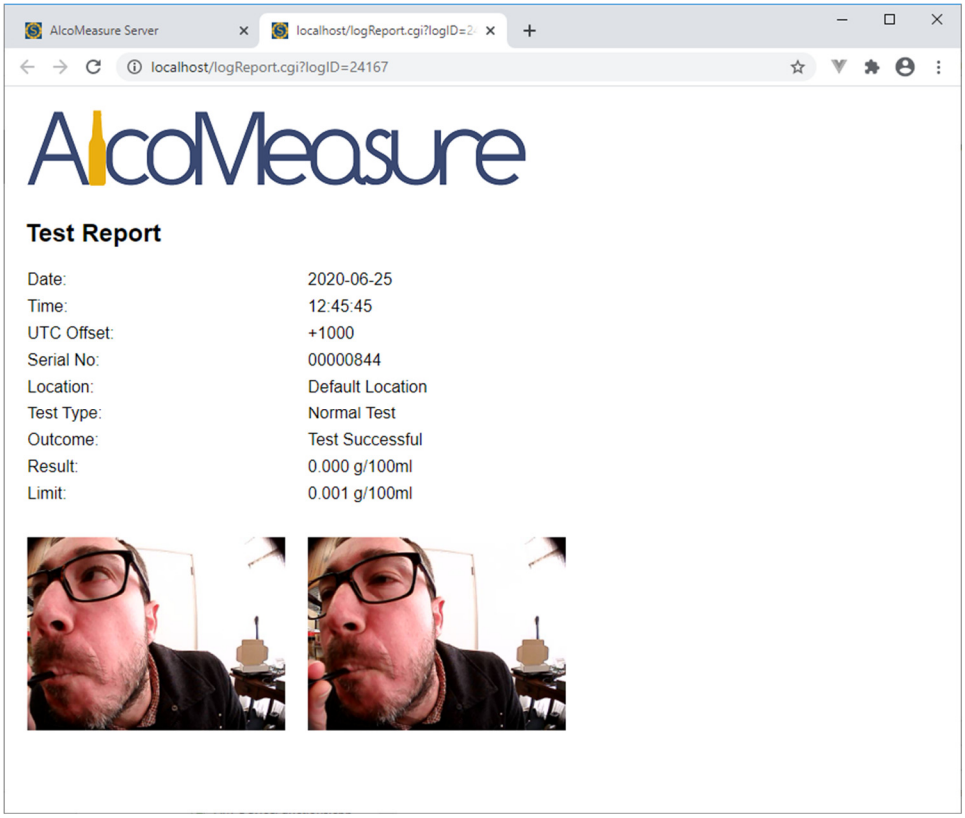


Figure 6 - Test Report showing photo.

This test report can also be automatically emailed whenever a test occurs. Further information can be found in section 9.1.

If the log record was not a test, then information applicable to the log type will be displayed.

7.4 Devices

The Devices page provides a summarised snapshot of the state of each known device.

If more detailed information for a device is required, the hostname for each device is provided. This can be used to connect to the device with "AlcoMeasure Utility" and perform more advanced diagnostics.

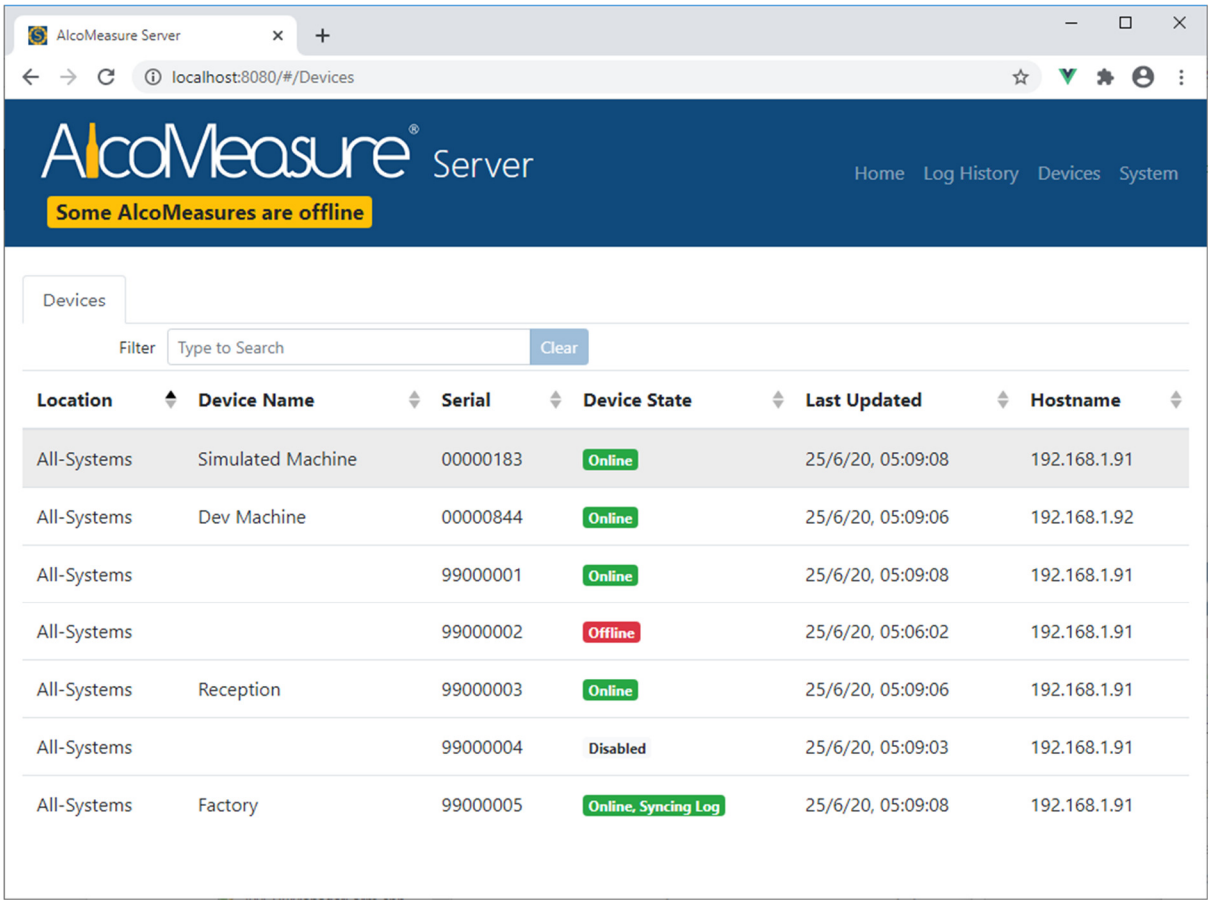


Figure 7 - Devices page showing status of all known devices

The "Filter" can be used to search for particular devices and is applied to every column.

The possible devices states are:

Online: The device is currently online and functioning normally.

Offline: The device is currently offline.

Online, Syncing Log: The device is uploading all logs since it was last connected.

Online, Unlicenced: The device is connected, but no licence was available for it. All devices connect in the "Unlicenced" state. If a licence is available, the device will move to the "Online" state within a few seconds. If the device stays in the "Unlicenced" state for more than 10 seconds, then all the licences are already taken. The licence file will need to be updated according to section 11.

Comms Error: The device has stopped returning valid replies. The server will force it to disconnect in an attempt to get it to recover.

Comms Error, Unrecoverable: The server has forced it to disconnect too many times and has declared it unrecoverable. The device needs to be checked to make sure it is operating normally.

Disabled: The device has been configured as disabled in the database. It will be disconnected immediately upon trying to establish a connection.

7.5 System

The System page is the main section for checking the health of the server software, and for diagnosing system problems. It is made up of 3 tabs, “System Status”, “System Events”, and “Documentation” which are described below.

7.5.1 System Status

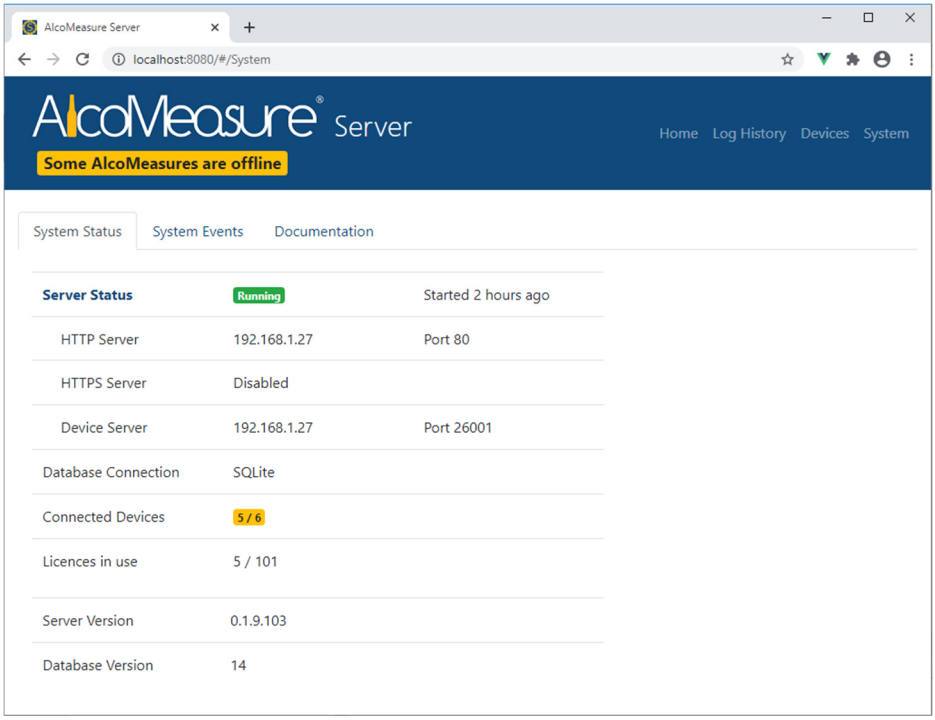


Figure 8 - System Status tab, showing 1 disconnected device.

The “System Status” tab provides an overview of the current state of the Server software.

The status as indicated at the top of the page can be any of the following:

Starting: The server is currently starting up.

Running: The server is currently running as per normal.

Stopping: The server is stopping.

Stopped: The server is stopped. This indicates that the service has either been stopped by the system admin, or it has crashed and has not been able to start back up.

Error: The server software is in an error state. An error message will be displayed next to the status.

If either the HTTP or HTTPS servers are enabled, their IP addresses and ports will be listed.

The database type will be shown next to “Database Connection”.

The “Connected Devices” shows the number of devices that are currently connected, out of the total count of known devices. If any devices are disabled, these are not counted as “known” devices.

The “Licences in use” shows the number of devices that are currently licenced, out of the total number of licences allowed for this server instance.

The “Server Version” shows the current version number of the installed server software, encompassing the service, system tray application, and web interface.

The “Database Version” shows the current database version. This is kept independent of the “Server Version” to keep track of when the database structure itself is changed.

7.5.1.1 Server Status Report

At the top left of the “System Status” tab is a link called “Server Status”. Pressing this causes a new tab to open with a report showing the current status of the server.

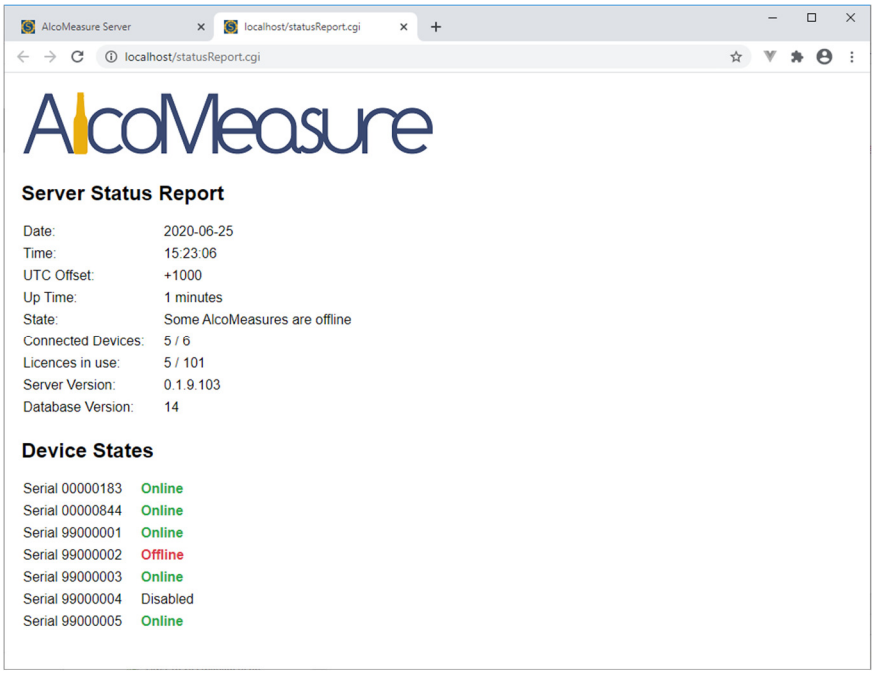


Figure 9 - Server Status Report showing most AlcoMeasures connected.

This status report can be printed or saved to PDF using the browsers built in features.

The status report can also be automatically emailed once a day. See section 10.6 for details.

7.5.2 System Events

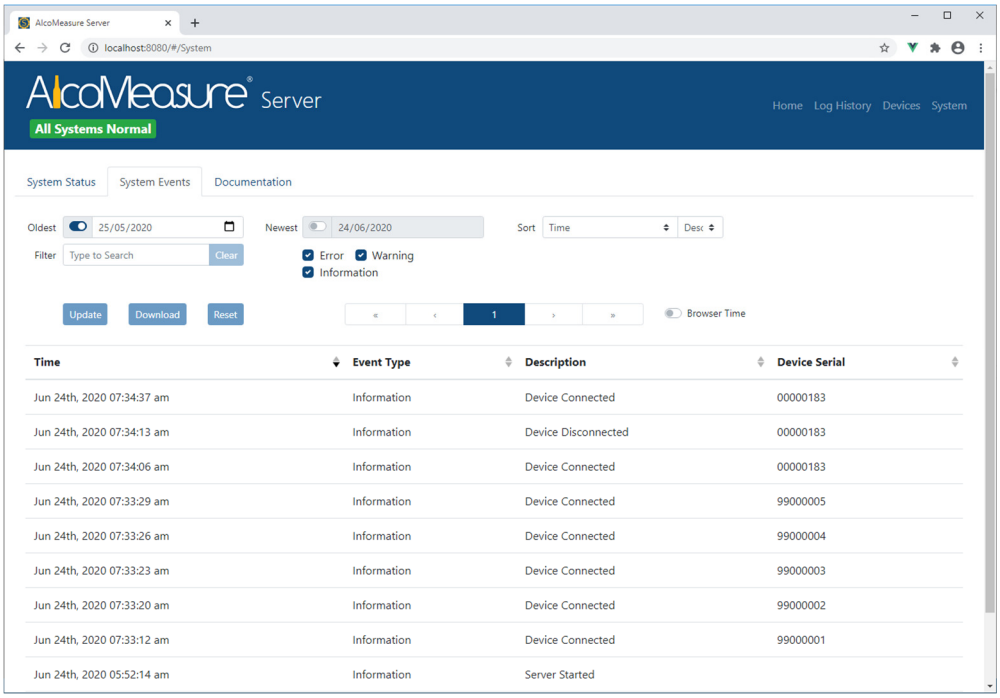


Figure 10 - System Events Page

The “System Events” page is the main section for searching and viewing events that have occurred in the server software.

When first opened, it will load the last month worth of events, using whatever filter options were used last time the form was opened.

7.5.3 Filtering Events

Filter options can be changed, and the columns to display can also be changed. These will take effect after the “Update” button is pressed, or next time the page is loaded.

Some filter options will be saved as browser cookies and will remain next time the page is accessed. These are:

- The event type to Show (Errors, Warnings, Information)
- Whether to display device time or browser time

The log results can further be filtered using the “Filter” string. This will be applied to the description and serial columns only. If multiple words are put in the Filter, separated by a space, then a log record will need to contain a column containing both words for it to be shown.

The log table will display a maximum of 250 logs at a time. If more than this exist with the current filter options, they can be accessed by selecting subsequent pages at the top or bottom of the table.

7.5.4 Downloading Logs

Pressing the “Download” button will download the filtered results as a CSV file. If the displayed results are split over multiple pages, all results will still be downloaded.

7.5.5 Documentation

The documentation tab provides several useful links.

It contains a link to this manual, as well as to the Server Brochure, as stored in the host machine.

It also contains a link to the AlcoMeasure GitHub repository, which contains up to date software, firmware, and documentation for the AlcoMeasure.

It also contains a link to the All-Systems Electronics Web page.

7.6 Device Users

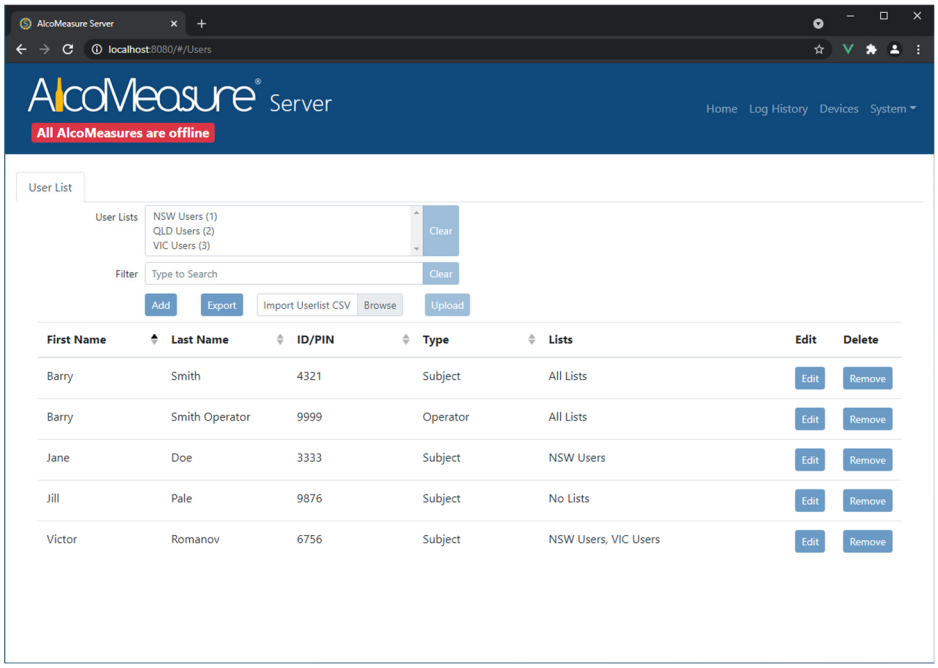


Figure 11 - Device User List

The “Device Users” page is used for configuring users. If a device is configured to require a valid ID to start a test, either via the built-in keypad or by another means, then a user list needs to be configured for the device.

Users can be added, edited and removed from the system regardless of whether any user lists exist. However, in order for users to be made available to the devices, at least one user list must be configured and assigned to a Location as described in sections 8.2 and 8.3.

Each device is associated with a single location, and each location is associated with a single user list. However, users can be associated with any number of user lists: None, one, many, or all.

This allows devices to be split between multiple locations, each with their own user list, but to still have some common users. For example, there may be devices in NSW and QLD, and each of these can have a separate user

list. However, there may be a truck driver or manager that regularly moves between both states and therefore needs to be in both user lists.

7.6.1 User List Management

When a user list is associated with a device through a location, that user list will be uploaded to the device. This will happen automatically approximately 5 minutes after the last change to that user list has occurred.

If a change needs to be reflected immediately, or if there is a problem with the user list in a device, they can be synced manually by pressing the “Sync all User Lists” button on the “System Status” page. In general, this should be avoided, since it will cause all devices to be immediately resynced with their respective user lists, which is usually not necessary and can be somewhat resource intensive for the device.

While all users can be added to a single user list, if there are a lot of users then the best way of managing them is to split them into multiple user lists. This is because each time a change is made, the entire user list for that device must be rewritten to the device. The larger the list, the longer it will take to write.

It should also be noted that when a test is taken, the username is reconciled to the log entry in the device, and then synchronised up to the server software. This means if a user is removed from the system, or an ID is reassigned, the name that was assigned to the ID when the test was taken will remain in the log, it will not be updated to a new name.

7.6.2 User List Table

The device user list table is shown in Figure 11. If no user lists are selected, and if no text is entered into the Filter field, then the table will show all users in the system.

To show only the users associated with a particular list, one or more lists can be selected from the “User Lists” combo box.

Text can also be entered into the “Filter” field. This will search all columns in the table, including the list columns.

To see the users not associated with any list, enter “No Lists” into the filter.

To see the users associated with every list, enter “All Lists” into the filter.

Users can be exported by pressing the “Export” button. Whatever filters have been applied to the display will also be applied to the export.

7.6.3 Adding and Editing Users

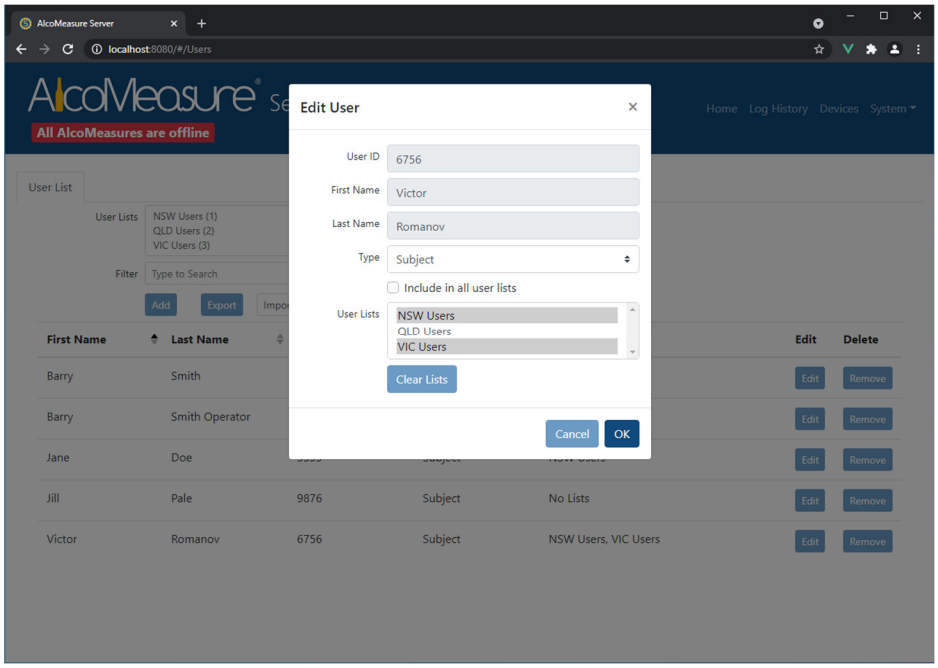


Figure 12 - Add Device User

To add a new user, press the “Add User” button above the user’s table. The following fields are available:

User ID: A unique identifier for the user. Can be numbers and characters, and no longer than 20 characters long.

First Name: The user’s first name. Either the first or last name must be filled in.

Last Name: The user’s last name. Either the first or last name must be filled in.

Type: Either “Subject” or “Operator”. This should normally be set to subject. The operator is only required to trigger a formal test.

Include in all user lists: If ticked, the user will be automatically included in all user lists, including future user lists. This should usually NOT be used for all users, to avoid making user lists too big. It is provided for convenience in the case of a manager that needs access to every device, or a floating user that may need to take a test on any device.

User Lists: The lists the user is associated with. This can be none, one, or many.

7.6.4 Importing Users

Users can be imported in bulk from a csv file. If an ID doesn’t exist, it will be added. If an ID already exists, the details associated with that ID will be updated with the details from the file.

If at least 1 user already exists in the system, pressing the “Export” button will provide an example csv file to work with.

The columns are as follows:

1. User ID. Must be no longer than 20 characters.
2. First Name. Must be no longer than 50 characters.
3. Last Name. Must be no longer than 50 characters.
4. Type. This should normally be set to “subject”.
5. All lists. This should either be 0 or 1.
6. Associated lists. This column contains the ID’s of all lists the user should appear in, separated by semi-colons. List ID’s are displayed in the list table.

   For example, if the user should appear in lists 1, 5 and 7, this column should contain the following: 1;5;7

Once the csv has been prepared, it can be uploaded through the web interface.

7.6.5 Removing Users

To remove a user from the system, press the “Remove” button next to the user.

If a user is no longer to be used, they do not necessarily need to be removed from the system. If they are no longer associated with any user lists, and if the “Include in all user lists” box is unchecked, they will not be made available to any devices.

However, if an ID needs to be reused, the old user will need to be removed from the system.

8 Device Management

Once the AlcoMeasure Server configuration is done, and the database connection is configured, the rest of the management of the system is handled through the Database Manager form, accessed from the System Tray application.

Alternatively, this could be done by manually editing the database, as described in section 14.2, but this is not the preferred method.

8.1 Adding Devices

Every device connected to the system needs to exist in the "Devices" database table.

If the "Auto-Add Devices to Database" option is selected (section 10.1.2) then the device will be added to the devices table automatically when it first connects.

However, if this option is disabled then the device will need to be manually added to the database before it can connect. This is done with the "Manage Devices" form.

When a device connects to the Server for the first time, if no Device Config exists for the device already then, a new one will be created. These can be found on the "Manage Device Configs" form.

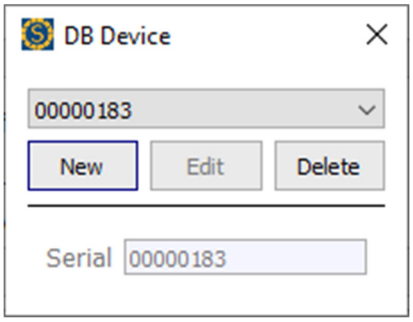


Figure 14 - Device Manager Form

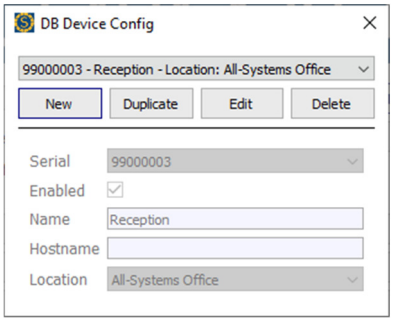


Figure 13 - Device Config Manager Form

Once a device has successfully connected to AMS it will appear in the Devices table in the Web Interface as shown in section 7.4.

8.1.1 Device Config Form

The "Device Config" form is used to configure the specific device using the following options:

Enabled: Tick the if the device is enabled, untick if the device is unavailable or otherwise not allowed to connect.

Name: The name of the device.

Hostname: A URL or Fully Qualified Domain Name that can be used to identify the device. This is displayed on the "Devices" page in the Web Interface. If this is left empty, then the devices reported IP address is displayed instead.

Location: The Location Config to be used for this device. All advanced configuration for the device is managed through the Location Config rather than the device itself.

8.1.2 Removing Devices

To remove a device, along with its associated configuration and all its log records, the "Manage Devices" form can be used. Simply select the appropriate device and press Delete. A prompt will remind the user that all logs will be deleted as well.

If there are many logs in the database this procedure can take quite a while, during which time it can appear that the form is not responding. Leave the form to finish on its own.

8.2 Location Management

To configure more advanced items like notifications or time zones, Devices are grouped together into "Locations". Each location is then given the desired configuration.

This is accomplished by adding a "Location" config with the "Manage Location Configs" form and then linking the location to each device.

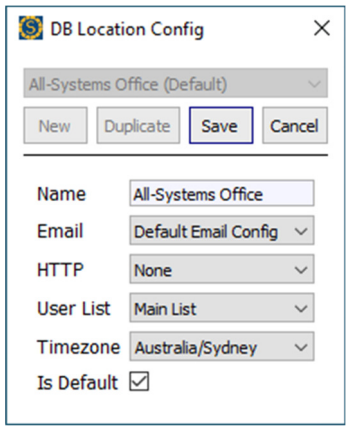


Figure 15 - Location Config Form

If a Location Config is marked as the "Default" config then whenever a new device is added to the system, it will be assigned this Location by default.

8.2.1 Location Config Form

Name: The name for the configuration.

Email: The email configuration to use for all devices in this location.

HTTP: The HTTP notification configuration to use for all devices in this location.

User List: The user list to use for all devices in this location.

Timezone: The time zone to use for all devices in this location.

8.3 User List Configuration

In order to allow users to be managed through the server software, at least one User List Configuration must be specified. The user list simply needs to be provided with a name, and then to be associated with a location as described in section 8.2.

Once a user list has been created, users can be added to the list as described in section 7.6.

9 Test Notifications

AlcoMeasure Server can be configured to send a notification whenever a subject's test result is over a pre-defined threshold on a connected device. There are two types of notifications, Email and HTTP, both of which are described here.

9.1 Email Notifications

Email notifications can be sent whenever a test result occurs over a pre-defined threshold. These are configured using the System Tray application and navigating to "Manage Database", and then selecting "Manage Email Configs".

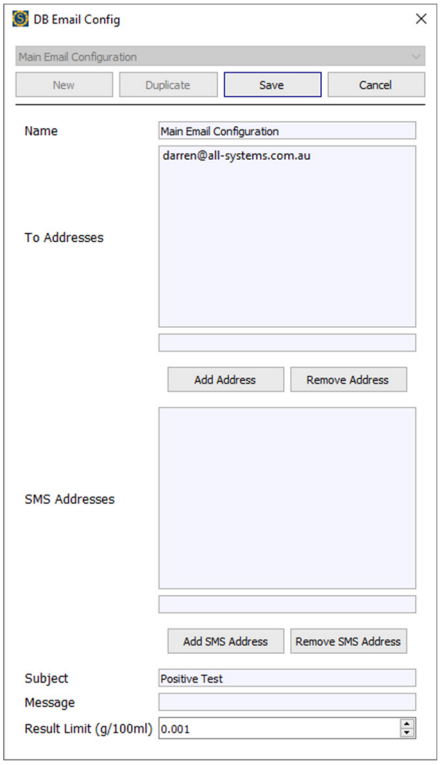


Figure 16 - Email "Test Over Limit" Configuration

For an email notification to be configured for a device, the Email Configuration needs to be created on this form, and then the Location associated with the Device in question needs to be linked to the Email Configuration.

If "To Addresses" are set for the Email Config, then the contents of the email will be the same as the "Test Report" shown in Figure 6.

If "SMS Addresses" are set for the Email Config, then the contents of the email will be a summarised version using plain text and less than 160 characters. This is meant for use with an Email-to-SMS service.

If both "To" and "SMS" addresses are supplied, then both types of email will be sent.

Email notifications are only sent for tests that were taken in the previous 24 hours. This means that when a device synchronises its log for the first time, older tests will not get emailed.

9.1.1 Email Notification Config

Name: The name of the configuration.

To Addresses: The list of addresses that the HTML Test Report will be sent to.

SMS Addresses: The list of addresses that the plain text message will be sent to.

Subject: The subject field of the email.

Message: A message that will appear at the top of the email body. Leave empty if not needed.

Result Limit: The limit used for determining whether the email needs to get sent or not. Note that the email is sent if the test result is >= than the result limit. This means that the result limit can be set to 0.000 to send an email for every test. This value is set in whatever the server units of measure are.

9.2 HTTP Notifications

HTTP notifications are custom notifications that can be sent whenever a test result occurs over a pre-defined threshold, or possibly just for every test. They allow a HTTP request to be configured that can connect to a user-defined service and post a message. This can contain data from the test in a format specified at configuration time.

HTTP notifications are only sent for tests that were taken in the previous 24 hours. This means that when a device synchronises its log for the first time, older tests will not get sent.

9.2.1 HTTP Notification Config

HTTP Notifications are configured using the System Tray application and navigating to “Manage Database”, and then selecting “Manage HTTP Notification Configs”.

For a HTTP notification to be configured for a device, the HTTP Configuration needs to be created on this form, and then the Location associated with the Device in question needs to be linked to the HTTP Configuration.

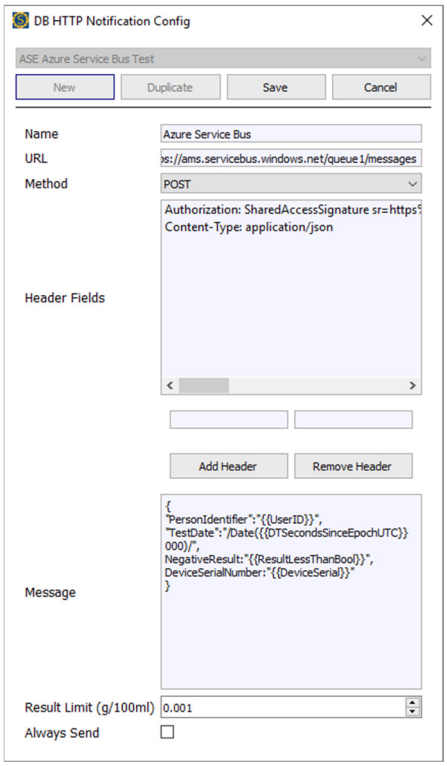


Figure 17 - HTTP Notification Configuration

Name: The name for the configuration.

URL: The URL that the HTTP request is to be sent to. If SSL/TLS encryption is required then the request should start with HTTPS, otherwise HTTP should be used.

Method: The HTTP method to use. Options are:

- POST
- PUT
- GET

Headers: Any custom headers that should be sent as part of the request. Each header Name and Value pair needs to be provided and added to the list. If authentication is required for the service, this should be supplied as part of the header.

Message: The body of the request. This can contain variables that will be automatically filled in by the server before being sent. A variable appears in a set of {{ }} braces. Possible variables are:

- {{DTSecondsSinceEpochUTC}}
  - The time in seconds since 1st January 1970. This is given in UTC time.
- {{UserID}}
  - The ID of the test subject.
- {{ResultGreaterEqualBool}}
  - Inserts “true” if the result was greater or equal than the result limit, otherwise inserts “false”.

- {{ResultLessThanBool}}
    - Inserts “false” if the result was greater or equal than the result limit, otherwise inserts “true”.
- {{DeviceSerial}}
    - The serial number of the device the test occurred on.

Result Limit: The limit used for determining whether the email needs to get sent or not. Note that the email is sent if the test result is >= than the result limit. This value is set in whatever the server units of measure are.

Always Send: A flag set to true if the notification should be sent for every test, regardless of the result.

10 Server Configuration

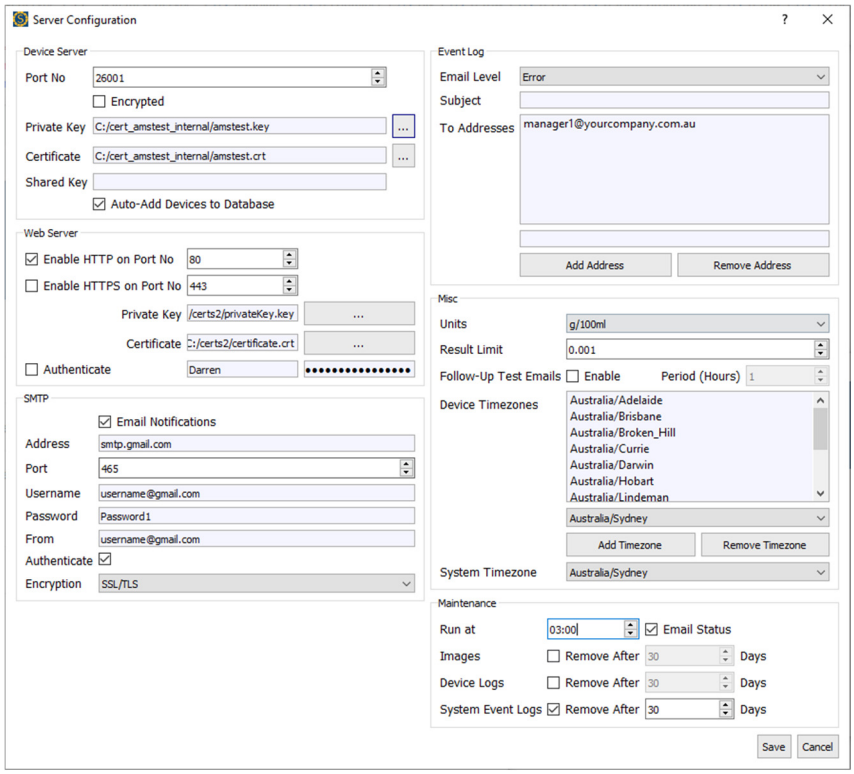


Figure 18 - Server Configuration Form

The service component of AMS is configured using the System Tray "Server Configuration" form. This configuration is stored in the AlcoMeasureServer.ini configuration file. The file can be edited manually, but it is recommended to use the "Server Configuration" form to avoid possible problems.

Anytime a setting is changed on this form, the service must be restarted for it to take effect.

10.1 Device Server

The device server by default will be setup to run on port 26001 with no security credentials. This simplifies the setup of the server software on an intranet. The configured port will just need to be opened on the host machine to allow devices to connect.

10.1.1 Device Server Security

The configuration of extra security for the server software can increase the complexity of configuring and managing devices. Since the software is primarily for use on an intranet, these are off by default.

However, if the server software is being hosted on a cloud service, or if devices are connecting over the Internet, then it is strongly advised to setup additional security.

There are two forms of security that can be configured: encryption, and a shared key.

10.1.1.1 Device Server Encryption

When enabling encryption for the device server, SSL/TLS technologies will be employed to encrypt the connection between the individual devices and the server. The server's signed certificate is also stored on the device to authenticate the server to the device and encrypt the communication.

To enable this, the "Encrypt" checkbox must be ticked.

Then, a digitally signed certificate must be created that identifies the domain name of the server[3]. This must be uploaded to the host machine and linked using the Device Server "Certificate" file path setting. This certificate must then be uploaded into each device that is to connect to the service, as described in section 12.

Finally, a private key must be generated[3]. This must be uploaded to the host machine and linked using the Device Server "Private Key" file path setting.

The private key must be kept safe, and never handed out.

10.1.1.2 Device Server Shared Key

To authenticate each device to the server, a shared key can be configured in the server.

The same key must then be supplied for each device, as described in section 12.

10.1.2 Auto-Add Devices

When this is enabled, any AlcoMeasure device that connects to the server software for the first time will be automatically added to the database. This simplifies the configuration of devices.

If this is disabled, devices that are not already present in the database will be rejected. Devices can be added as described in section 8.1.

10.2 Web Server

The main interface to the AlcoMeasure Server software is provided through a web server. This can be made available as an insecure HTTP server, or a secure HTTPS server, or both.

By default, the HTTP server is enabled on port 80. This simplifies the initial setup of the software and is fine if the server is for internal use on an Intranet.

However, if the server software is being hosted on a cloud service or is otherwise accessible over a public network then it is strongly advised to use the HTTPS server instead.

[3] The generation of digitally signed certificates and private keys for web technologies is beyond the scope of this document.

10.2.1 HTTPS Server

The use of the HTTPS server enables the server to the user when accessing it through a web browser. It also encrypts the communication between the server and the browser.

A digitally signed certificate must be created that identifies the domain name of the server[3]. This must be uploaded to the host machine and linked using the Web Server "Certificate" file path setting.

Also, a private key must be generated[3]. This must be uploaded to the host machine and linked using the Web Server "Private Key" file path setting.

The private key must be kept safe, and never handed out.

10.2.2 Web Server Authentication

Authentication can also be enabled for the web server, regardless of whether HTTP or HTTPS is being used.

This authenticates the user to the server, disallowing unauthorised access.

At this point, only a single user/password can be configured.

10.3 Email SMTP Configuration

AMS provides the ability to send out email notifications. For these emails to work it must be configured to connect to an existing SMTP service.

To send any email notifications, the "Email Notifications" options must be enabled.

The SMTP configuration options provided should be filled out according to your SMTP provider. Note that in general the "From" setting should be the same as the "Username" setting.

Once configured, the email functionality can be tested by temporarily setting the "Email Level" to "Information" and then restarting the service. AMS posts a "Server Started" Information event to the event log. If the email is not received, check the event log for a failure message to help diagnose the problem.

10.3.1 Gmail SMTP Configuration

The following settings show how to use an existing Gmail account and Gmail's SMTP to send email alerts.

Note that the Gmail account must be configured with an "App Password" for this to succeed.

Address	smtp.gmail.com
Port	465
Username	username@gmail.com
Password	alsdknoruvnascke
From	username@gmail.com

Authenticate	Yes
Encryption	SSL/TLS

10.4 Event Log Notifications

The event log is described in section 6.4. However, the system can be configured to automatically email some or all system events as they are added to the event log.

The "Email Level" setting allows these notifications to be disabled or set to a particular level. If a level is chosen that is not "None", then events at the chosen level and higher will be emailed.

For example, if "Information" is selected then ALL events will be emailed. However, if "Error" is selected then only Error level events will be emailed.

The Subject field for the event notification emails can be set, as well as the addresses these notifications should be sent to.

10.4.1 Device disconnected event

An Error event will be added to the event log if a device has been disconnected for more than 10 minutes. If the "Email Level" is not set to "None" then this event will also be emailed.

10.5 Misc. Configuration

10.5.1 Units

Sets the units of measure that is used throughout the application. Note that the default in Australia is g/210L of Breath Alcohol.

10.5.2 Result Limit

Sets the limit that is used for displaying results on the Home page, as well as in Test Reports generated in the Web Interface. This is NOT the result limit that is used for email/http notifications. These are configured in the database.

10.5.3 Follow-Up Test Emails

When "Over Limit" emails are configured, if a user records a result over the configured threshold an email will be sent. However, if a subsequent test by the same user records a result under the configured threshold, no email will be sent.

The Follow-Up email functionality causes all subsequent user tests within a configured period to be emailed, even though they fall beneath the configured threshold.

Enabled: Enable/disable the functionality.

Period: The number of hours that follow-up emails should be sent for. If the user blows a negative test with this many hours of their positive test, it will get emailed.

10.5.4 Device Time zones

There are many possible time zones that can be configured for each device. This list of time zones narrows down the possibilities so that each device can be more easily configured.

To add a time zone to the list, select it in the drop-down and press “Add Timezone”. To remove a time zone from the list, select it in the list and press “Remove Timezone”.

10.5.5 System Timezone

The selected time zone will be used by all internal date and time calculations. This will default to the host machines time zone but can be changed.

10.6 Server Maintenance

Server Maintenance is a special event that runs once a day at the configured time.

Run at: The time of day at which the maintenance event is scheduled.

Email Status: If ticked, the Server Status Report will be emailed using the addresses configured for the “Event Log” in section 10.4. See section 7.5.1.1 for more information on the status report.

Images: If enabled, images will be removed after the set number of days.

Device Logs: If enabled, device logs will be removed after the set number of days.

System Event Logs: If enabled, system events will be removed after the set number of days.

11 Server Licencing

The server software is licenced by All-Systems Electronics.

Licences are managed by the AMSLicence.ini file. This file is auto-generated the first time the server application is run.

If more devices are connected to the server than available licences, these devices will remain connected, but no logs will be downloaded from the device. This means that notifications will also not work for the unlicenced connections.

The server software allows a single device to connect without being licenced. However, to connect more devices, the licence must be validated as follows:

1. Run AlcoMeasure Server.
2. Use the System Tray application to stop AlcoMeasure Server.
3. Navigate to C:\ProgramData\AlcoMeasureServer.
4. Copy the file AMSLicence.ini.
5. Email the licence file to sales@all-systems.com.au
6. When the validated file is emailed back, copy it over the original licence file.
7. Use the System Tray application to start AlcoMeasure Server.

The “System” page should now show has the correct number of licences, and more than 1 devices should be able to fully connect to the system.

12 Device Configuration

For an AlcoMeasure WM1 to connect to AlcoMeasure Server it must be configured using AlcoMeasure Utility.

Before following these steps, ensure that the “AM Server” feature is Enabled by connecting with AlcoMeasure Utility and checking the Extra Features on the Diagnostics tab. If it is Disabled, contact the Distributor described in section 3.2 to organise an unlock.

To configure a device, perform the following:

1. Ensure that the device is available on the network. The easiest way to do this is to connect to the device over Ethernet.
    a. If the device is unavailable, check its network configuration on the “Diagnostics” tab. Refer to the AlcoMeasure WM1 User Manual for more information.
2. Connect to the device with AlcoMeasure Utility.
3. Open the “Configuration” tab, followed by the “System” tab.
4. Press “Read Config from Unit”.
5. Find the “Server” group on the page.
6. Tick “Enabled”
7. Fill in the “Hostname” of the server instance. This can either be an IP address or a fully qualified domain name.
8. Set the “Port No” to the correct port. This can usually be left to default.
9. If the server has been configured with a Shared Key, that key needs to be entered into the “Shared Key” field.
10. If the encrypted option has been enabled on the server, then the “Encrypted” option needs to be ticked in the device.
11. If the encrypted option has been enabled on the server, then the server has been configured with a digitally signed certificate. This certificate can be stored on the device to authenticate the server and improve security.
    a. If this is required, tick the “Validate with Certificate” option.
    b. Before attempting to connect the device to the server, follow the instructions in section 12.1 to install the certificate on the device.
12. Press “Write Config to Unit” to update the device with the new settings.
13. Restart the device for the settings to take effect.

After these steps have been followed the AlcoMeasure WM1 should automatically establish a connection to AMS. AMS’s web interface can be used to determine what devices have successfully connected to the server. If the device is not listed at all then it has never connected to the server. If the device appears in the list but says disconnected, then it has connected at some point but is not currently connected.

12.1 Digitally Signed Certificate

If the “Validate with Certificate” option was selected in the device system configuration, then the servers certificate needs to be uploaded to the device.

1. Connect to the device with AlcoMeasure Utility.
2. Open the “Diagnostics” tab.
3. The Network “Server Cert” section shows the details of any certificate currently stored on the device.
4. Press “Set” next to Server Cert.
5. Navigate to the server’s digitally signed certificate file.
6. Press “Open”. If the certificate was valid, it will be written to the device.
7. Check that the details shown next to “Server Cert” match the Server instance the device needs to connect to.
8. Restart the device for its settings to take effect, and for it to connect to the Server.

13 Database Configuration

AlcoMeasure Server's most important feature is its database.

By default, an SQLite database will be created in the default data directory (section 6.1.1). This database is fine for light usage with a few units connected. However, if many tests are going to be performed, especially with photos, it may be worth considering setting up a SQL Server instance instead.

The database connection is configured by right clicking the System Tray application and selecting "Manage Database".

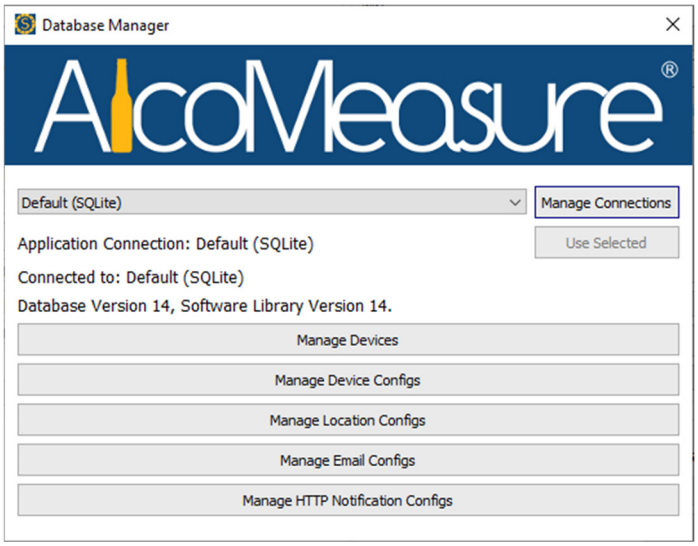


Figure 19 - Database Manager

The drop-down list shows all available connections. To switch to a different connection, select it from the list and press "Use Selected".

The Database Manager form will show the selected connections database version, and the software library version. The database version is the current version of the actual database structure. The software library version is the version of database that is expected by the AlcoMeasure software. There may be some instances where the server software can run fine with a slightly older version of database, but in general the database will need to be upgraded.

Normally, the current database connection will be automatically upgraded by the software. However, if the connection is manually switched using the "Database Manager", the user will be prompted to Upgrade the new database connection before it can be set as the current connection.

To add a new connection, press "Manage Connections". In this screen, existing connections can be edited, and new connections can be created. To create a new connection, press "New".

The following sections describe how to configure the different database types.

13.1 SQLite Configuration

SQLite is the default database type, since it is easy to configure and backup, and highly portable. A default SQLite connection/file will be created when AlcoMeasure Server runs for the first time.

When creating a new SQLite connection, the only thing that needs to be specified is a path to the database file. If the file already exists, then that database will be used. If the file does not already exist, a new file will be created at the specified path.

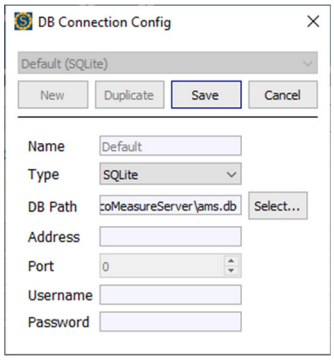


Figure 20 - SQLite Database Connection

The SQLite database can be easily browsed and edited using several freely available tools. We recommend using SQLite Studio which can be found at https://sqlitestudio.pl. Because the default location of the SQLite database is in C:\ProgramData, SQLite Studio must be run with administrator privileges to edit the database.

Visit https://www.sqlite.org for information on SQLite.

13.2 Microsoft SQL Server Configuration

If the default SQLite database is not suitable then AlcoMeasure Server can be configured to connect to an instance of Microsoft SQL Server instead. AlcoMeasure Server will work with both Express and professional versions of SQL Server.

Before configuring the connection in AlcoMeasure Server, the SQL Server database must already be created along with a user that has full permissions on the database.

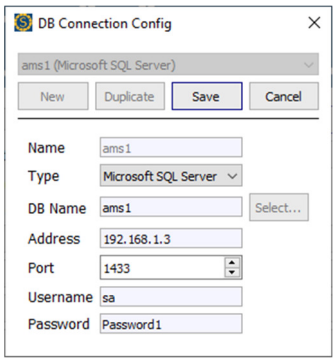


Figure 21 - MS SQL Server Connection

To connect to the MS SQL Server instance, the following settings need to be provided:

DB Name: The name of the database in the SQL Server instance.

Address: The IP address/hostname of the SQL Server instance.

Port: The port number of the SQL Server instance.

Username: The username of the user account created in SQL Server with permissions to modify the database.

Password: The password of the above user account.

Administration of a Microsoft SQL Server database is beyond the scope of this document.

14 Database Design

The AMS database is automatically populated when the service first runs and successfully connects to a database.

If the database needs to be modified to accommodate a new feature or change, the database will be automatically upgraded when the AlcoMeasure Server instance runs. If the upgrade is successful, the version number stored in the database will be updated to reflect the change. If the upgrade fails, an error message will be posted to the event log and the server will fail to start.

Many tables in the database help AMS run in a stable and consistent manner, and therefore editing by an outside program or administrator is not recommended. These are listed in section 14.1.

Tables that can be edited by the system administrator or by client software are listed in section 14.2.

A database browser can be used to show the exact structure of each table as well as the relationship between tables.

In most cases the primary key is the first column of the table, ends with the suffix “ID”, and is auto-incrementing.

14.1 Read Only Tables

These tables can be viewed by the client but should not be edited. AlcoMeasure Server relies on these tables maintaining a consistent state.

14.1.1 Info

Contains a single row holding the current state of the database.

dbVersion: The current version of the database.

Heartbeat: A timestamp automatically updated by the server software approximately every 10 seconds. This can be monitored by client software to determine if the AMS service is still running.

errorMessage: If the AMS software is in an error state, this field will hold the current error message.

restrictUtility: A flag that stops the database from being edited by the utility. This is set by the server software so that if an instance of the AlcoMeasure Utility software connects to the same database they do not compete with writing logs and status.

dbSoftwareMinimum: NA

ServerState: The current state of the server. Options are:

- Stopped
- Starting
- Running
- Stopping
- Error

14.1.2 EventLog

All system event logs generated by the server software. These can be purged periodically using the "Maintenance" functionality described in section 10.6.

timeStamp: The time of the log, in server software time (see section 10.5.5).

serial: If the event refers to a specific device, this will hold the devices serial number. Otherwise, it will be NULL.

event: The message associated with the event.

type: The type, or level, of the event. Options are:

- Information
- Warning
- Error

14.1.3 Devices

All known devices are listed in this table. This table includes each device's current status, as well as other state information used the server to manage the device. The preferred method of editing this configuration is described in section 8.1.

Serial: The serial number of the device.

Connected: True if the device is currently connected, otherwise false.

lastUpdated: The time the device was last updated, using the time zone information configured for the device.

Syncing: This field is no longer used.

State: The last known state of the device. Options are:

0. Disconnected
1. Connected
2. Syncing Log
3. Unlicenced
4. Comms Error
5. Comms Error Giving Up
6. Invalid

Status: The status data as downloaded from the device.

Diagnostics: The diagnostics data as downloaded from the device.

Network: The network data as downloaded from the device.

lastLogRecord: Details of the last downloaded log record. This is used for the log syncing mechanism.

UpdateState: Used for syncing data to the device, i.e.: the user list.

14.1.4 DeviceLogs

All logs downloaded from all devices are stored in this table.

The column names given are appropriate for a “test” type log but may not make sense for other log types.

Tests can be found by searching for all logs for a device where the “type” column contains the word “test”, case insensitive.

The date and time columns are separate, because of how they are stored in a device. They are stored as the local time of the device, regardless of the server time zone.

The “offsetFromUTC” column is the offset in seconds between UTC time and the timestamp provided in the date and time columns. This is calculated using the devices configured time zone, and handles daylight saving time.

If any of the image columns contain a filename, then the associated image will be stored in the “DeviceImages” table.

14.1.5 DeviceImages

The images associated with the logs in “DeviceLogs”. If a log row in “DeviceLogs” has multiple images, each image is represented by a single row in the “DeviceImages” table.

Although filenames use an incrementing number to differentiate them, there is the possibility that multiple images could have the same filename. For this reason, the filename cannot be relied upon to match an image to a log record. The “DeviceLogsID” field should be used to reconcile images to a log record, and then the “imageNo” can be used to determine whether it is the first, second or third image (0,1,2).

The image data is stored in the “data” column as jpg data.

14.2 Editable Tables

14.2.1 DeviceConfigs

The preferred method of editing this configuration is described in section 8.1.1.

Every known device must have a configuration. Usually these will be automatically generated when a device first connects to the system.

The device config sets a few settings for the device, and then links the device to a location.

All other configuration is handled through the linked location.

LocationID: The key of the location this device is linked to.

DeviceName: The name of the device.

HostName: The hostname of the device. If this is NULL, then the IP address from the device’s network data is used in the server software instead.

Disabled: A flag disabling the device. If this is true, the device will not be allowed to connect to the server. This means any previous config and records for the device can be kept in the system, but the device will not be counted as a “known” device.

14.2.2 Location

A location config provides a means of grouping multiple devices together to ease configuration. The preferred method of editing this configuration is described in section 8.2.1.

Name: The name of the location.

EmailConfigID: The key of the email config used by this location. NULL if no config is specified.

Timezone: The time zone to use for this location.

NotificationConfigID: The key of the notification config used by this location. NULL if no config is specified.

DefaultConfig: True for whichever location is the default. This can only be set for a single location. If a new device connects, and a default location is specified, that location will be set for the new device.

UserListsID: They key of the user list associated with this location.

14.2.3 EmailConfig

A table for configuring “Over Limit” email notifications. The preferred method of editing this configuration is described in section 9.1.

fromAddress: The address that the email is being sent from. This should usually be the same as the from address in the SMTP config described in section 10.3.

toAddresses: A comma separated list of addresses that will be the recipients of the email.

smsAddresses: A comma separated list of addresses that will be the recipients of a minimised version of the email.

Subject: The subject field of the email.

Message: A message that will appear at the top of the email body. Leave empty if not needed.

resultLimit: The limit used for determining whether the email needs to get sent or not. Note that the email is sent if the test result is >= than the result limit. This means that the result limit can be set to 0 to send an email for every test. This value is set in whatever the server units of measure are.

Name: The name for the configuration.

14.2.4 NotificationConfig

A table for configuring HTTP notifications. The preferred method of editing this configuration is described in section 9.2.

Name: The name for the configuration.

url: The URL that the HTTP request is to be sent to.

Method: The HTTP method to use. Options are:

- POST
- PUT
- GET

Headers: Any custom headers that should be sent as part of the request, comma separated.

Message: The body of the request. This can contain 1 or more "variables" that will be filled in automatically by the server software.

resultLimit: The limit used for determining whether the email needs to get sent or not. Note that the email is sent if the test result is >= than the result limit. This value is set in whatever the server units of measure are.

alwaysSend: A flag set to true if the notification should be sent for every test, regardless of the result.

14.2.5 Users

A table for specifying users. The preferred method of configuring users is described in section 7.6.

FirstName: The user's first name.

LastName: The user's last name.

ID: The user's ID.

Operator: 0 if user is a subject (default), 1 if a user is an operator.
Operators cannot take tests; they are only useful for starting formal tests.

AllLists: 1 if the user should automatically appear in all lists, otherwise 0 (default).

14.2.6 UserLists

A table for specifying user lists. The preferred method of configuring user lists is described in section 8.3. Users are assigned to user lists with the UserListMap table described in section 14.2.7.

Name: The name of the user list.

LastUpdated: A timestamp recording when the user list was last modified (Entry was added, edited or deleted).

Version: A version number that is used to synchronise user lists to devices. This is incremented by 1 whenever the user list should be synced to all associated devices.

Modified: A flag indicating whether the user list has been modified. This is used by the internal syncing mechanism and should not be changed.

14.2.7 UserListMap

A table for linking users to user lists. This allows a user to appear in none, one, or many user lists. The preferred method of linking users to user lists is described in section 7.6.

UserListsID: A user list key to associate with the user.

UsersID: A user key to associate with the user list.