Shed Check-In System Operating Manual
Software Version 1.0

Author: Ian Dennison
Tawa MenzShed
Date: 07/07/2024
Version: 1.0

Document Information

Table of Contents

Contents

1 Introduction

1.1 Document Purpose

This document describes the management and use of the Shed Check-In System (SCIS) version 1.0, released on 7/7/2024.

1.2 Intended audience

This document is intended for Administrators who wish to use the features of System Checkin / Checkout and Device Access Control on their environment.

A working knowledge of IT systems (Command Line, Web Browser Usage, Networking) is required for managing this System

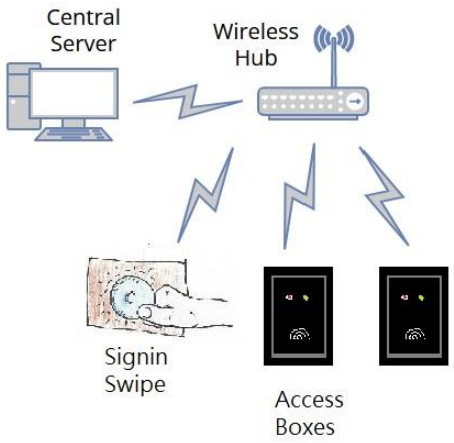
1.3 System Purpose

The Shed Check-In System is an attendance register and machine access management system that automates attendance recording, machine access authorisations and actual machine access.

By maintaining the access register, an Administrator can record machine usage, confirm user attendance and control machine access. This can be used to ensure adequate training on equipment before it is used, and providing accountability in the event of damage or abuse of equioment.

1.4 System Architecture

The Shed Check-In System uses a Client / Server architecture. It maintains a record of Member Details, Access Box Details, Access Permissions and Sign-in / Sign-out actions. It uses wireless technology to communicate between the Access Boxes and Central Server.



1.4.1 Central Server

This is a Unix Host running an Apache Web Server and MySQL Database. It manages the function of tracking sign-ins and authorisations for usage of Machines.

1.4.2 Signin / Signout Swipe

This is a wireless Arduino device with an RFC Reader that interfaces with the Central Server to record sign-ins and sign-outs. There should only be one Signin Swipe per system and it should be co-located with the Central Server where-ever possible.

1.4.3 Access Boxes

These are wireless Arduino devices with an RFC Reader and a Power Relay, that enables or disables power to the connected Tool. These can be identified by a Device ID, or the unique Device WWN derived from the Network component of the Arduino device.

There are 4 basic images that the Access Boxes may use are:

Field	Rationale
machine_box_WWN_High.ino	Works on the WWN based addressing and activates Relay when current is High
machine_box_WWN_Low.ino	Works on the WWN based addressing and activates Relay when current is Low

The “WWN based addressing system” is where the Device ID / Machine ID is assigned at the Central Server, but a link is made between the Device ID on the Server and the unique WWN of the Device Access Box. This allows the same Arduino image to be used on all Device Access Boxes and for swapping of Boxes to be performed by an Administrator rather than requiring a Technician.

1.4.4 Network Router

This is a Home Hub device designed to provide IP Addresses and wireless connection between Arduino devices and the Central Server.

1.5 Definitions

Commented [JB1]: Sorted table alphabetically by term

Term/Acronym	Definition/Full Description
DHCP	Dynamic Host Control Protocol.
DNS	Domain Name System.
Fob	An RFID device (usually round) that is used to identify a User. An alternative to a swipe card..
FQDN	Fully Qualified Domain Name.
HTML	HyperText Markup Language.
MD5	Message Digest. Used to verify data integrity of the CDSF, and during the initial DSMS System deployment.
NTP	Network Time Protocol.
Perl	A computer programming language
RHEL	Red Hat Enterprise Linux.
root (userid)	The super-user / administrator userid on the Linux system

SFTP	Secure File Transfer Protocol. A secure method of file transfer between two systems. SFTP is a subsystem of SSH.
SSH	Secure Shell. A secure method of communication between two systems.
Swipe Card	An RFID Device (usually white and flat) used to identify a User. An alternative to a fob.

2 Installation

2.1 System Requirements

2.1.1 Host Server Requirements

The SCIS System is made from a collection of common components and requires a common system to run it, often referred to as a LAMP stack - that is, Linux, Apache, MySQL, Perl. The System Requirements below should therefore be considered as confirmed working defaults rather than minimum requirements. Depending on the computing equipment available to you and your level of knowledge, you may wish to use alternative configurations.

2.1.1.1 LinuxLite

The system is known to work on Linux Lite 6.4 (Website https://www.linuxliteos.com/index.html). This release is free for non-commercial use. The Linux operating system will require an active internet connection to download any additional software while the Application is installed. After that, it is recommended to host the system on a dedicated network with no connection to the wider internet.

You will require root access on the DSMS Server for the initial setup.

2.1.1.2 Apache 2

Apache, due to its widespread use and stability, is the only web server that the SCIS Application has been tested and confirmed working on. Apache 2 should be installed from your distribution's base repository. No support is offered for alternative configurations..

2.1.1.3 Mysql (aka Mariadb)

Mysql is a relational database product that can store data as used by SCIS. Mysql should be installed from your distribution's base repository.

2.1.2 Tarball Contents

A custom script is used to deploy the tool, and this is combined into a "tarball" along with the necessary Web Files and Database schemas.

Directory	Contents
./	Basic install scripts
./var_www_html	Web pages and scripts
./mysql	Database Creation Scripts

2.1.3 Skills Requirements

Some technical skills will be required to install the SCIS System and build and deploy the Swipe System Boxes.

Skill	Requirement
Computer – Hardware	Procuring and Assembling Hardware Managing Boot Process Basic Network / Router Configuration
Computer – Software	Navigation of Menu and File Paths Modification of Files

	File Transfer and Session Management
Electronics	Component Identification Soldering and Cabling
Electrical	Wire Stripping and Connection Cabling standards

WARNING! Electrical work is covered by different codes in different administrative environments. Make sure you adhere to the rules for your jurisdiction. Electricity can kill!

2.2 SCIS Central Server Installation

See separate documentation for SCIS Server Installation.

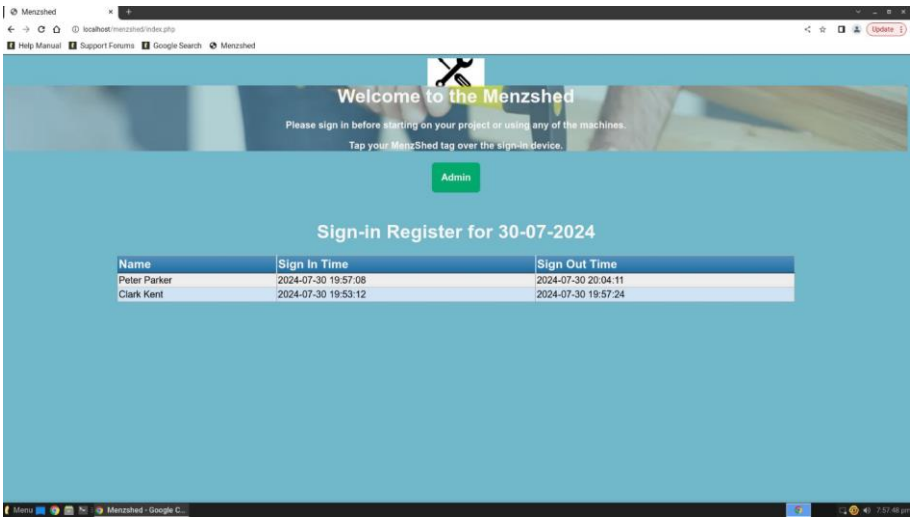
2.3 SCIS Signn and Device Access Box Setup

See separate documentation for SCIS Sign In and Device Access Box Installation.

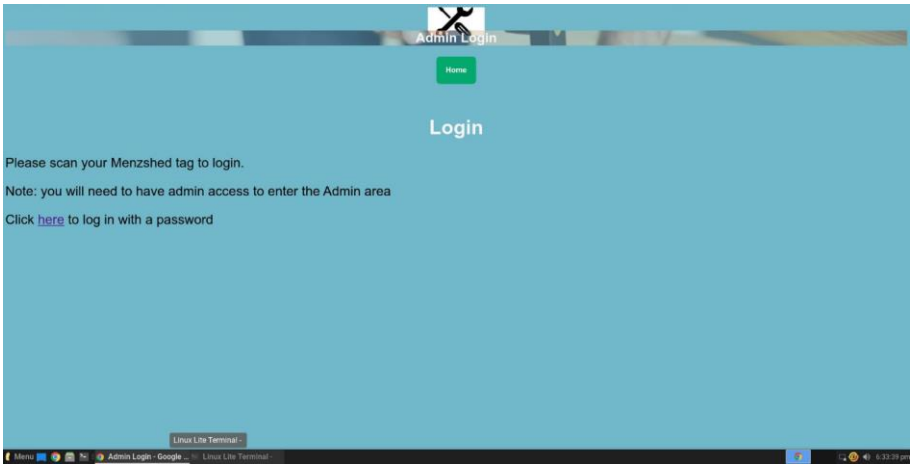
2.4 SCIS Administration

2.4.1 Initial Setup

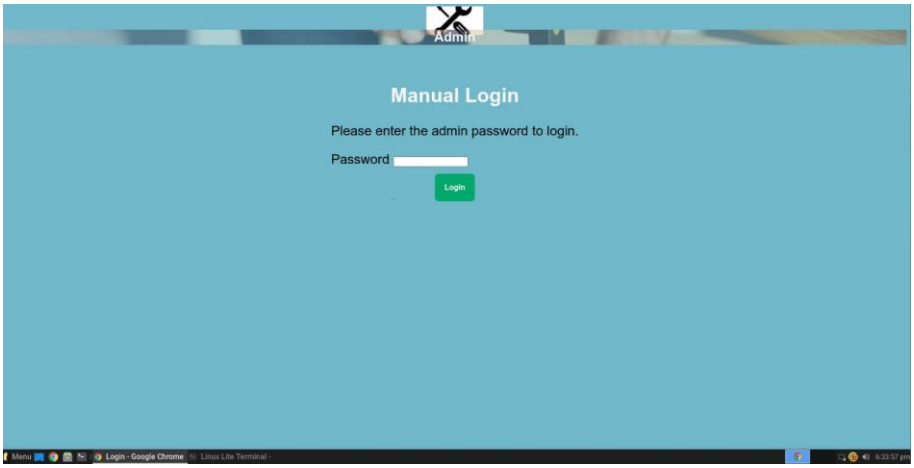
Once the Application has installed, login to the Server itself, start your web browser and navigate to the site http://localhost/menzshed/. You should be presented with the following screen which shows logins and logouts for the current day.



Clicking on “Admin” will take you to the validation screen



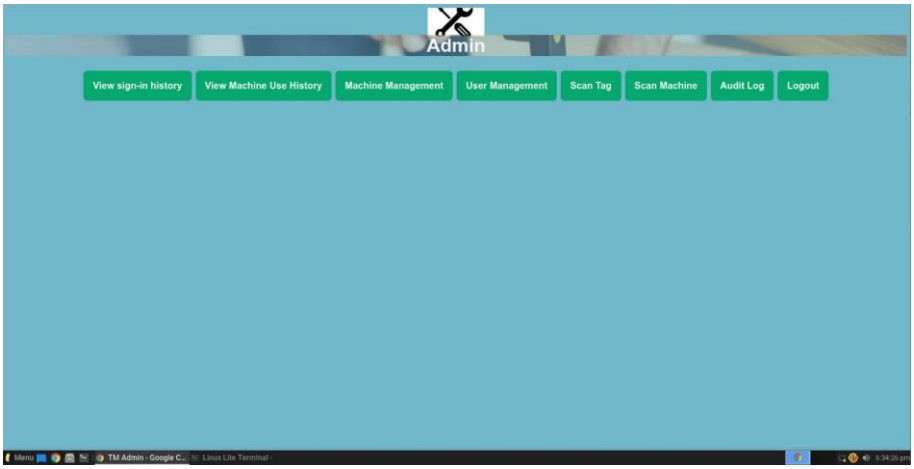
Enter your 4 digit passcode from the installation. If you have set up Users already with Administration rights, they can swipe on the signin box instead to gain access.



This is the default Admin Screen presented.

2.4.2 Default Administration Screen

This is the main administration screen where the System can be maintained. It is made up of the Header area (where the icons are shown), the Body area where content is displayed, and the Footer area where messages are displayed.

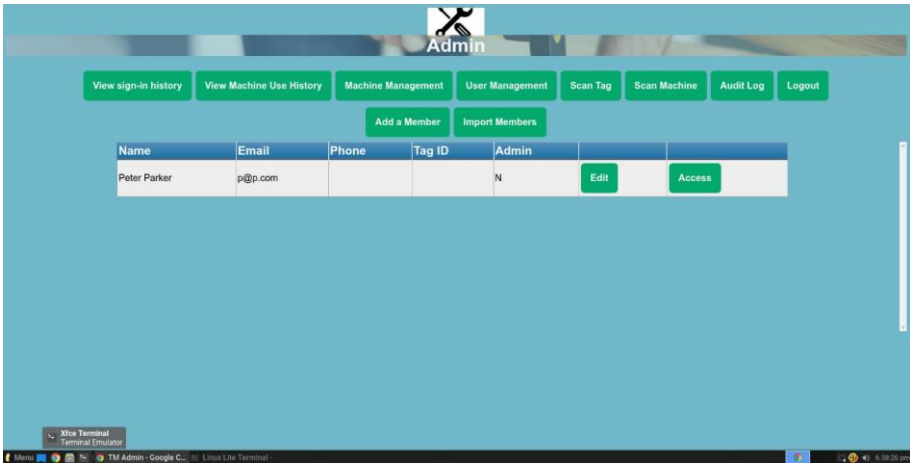


The areas are as follows…

Option	Description
View sign-in History	Provides list of sign-ins and sign-outs for users
View Machine Use History	Shows the machine usage log for users, including failed attempts at access
Machine Management	Management of Machine Configuration
User Management	Maintenance of Users and their rights
Scan Tag	Used to identify Tag IDs
Scan Machine	Allows identification of Access Box WWNs
Audit Log	Display logs of machine current load levels (not enabled in this version)
Logout	Logs out the Administration User from the session

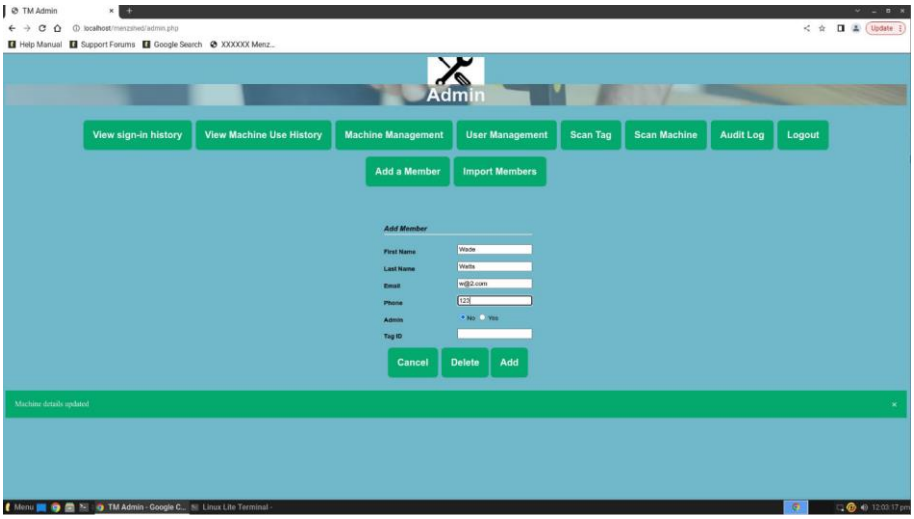
2.4.3 User Administration

Select the “User Management” icon to display the User Administration screen. This will show a list of current users with a summary of their information.



2.4.3.1 Adding a User

Select the “Add a Member” icon and the following screen will be displayed.



The following fields will be displayed:

- First Name: The First Name of the User
- Last Name: The Last Name of the User
- Email: The Email Address of the User (optional)
- Phone: The Phone Number of the User (optional)
- Admin: Whether the User is an Administrator or not
- Tag Id: The Tag ID of the User (to be filled in later)

Select the “Add” Icon to add the user to the system.

2.4.3.2 Modifying a User

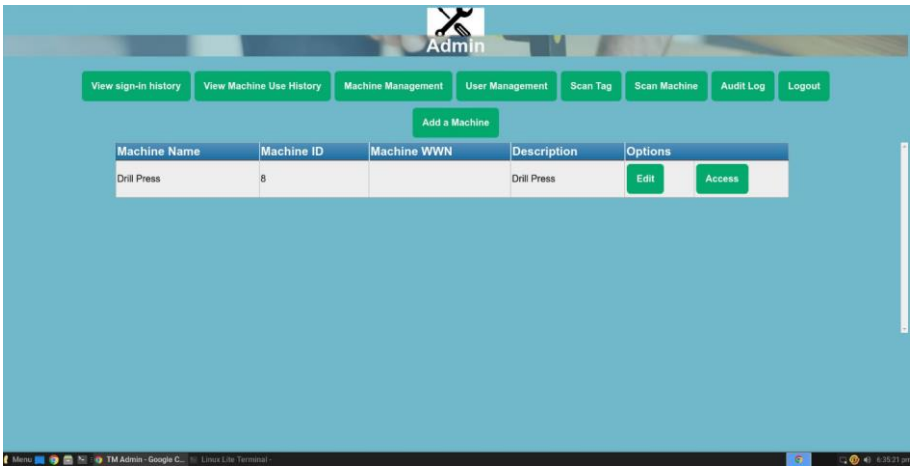
To modify the User, select the “Edit” icon on the list of Users under “User Management”. The same screen for adding should be displayed with the existing values. Select “Update” icon to confirm the changes.

2.4.3.3 Deleting a User

To delete a User, select the “Edit” icon on the list of Users next to the required User, and select the “Delete” icon.

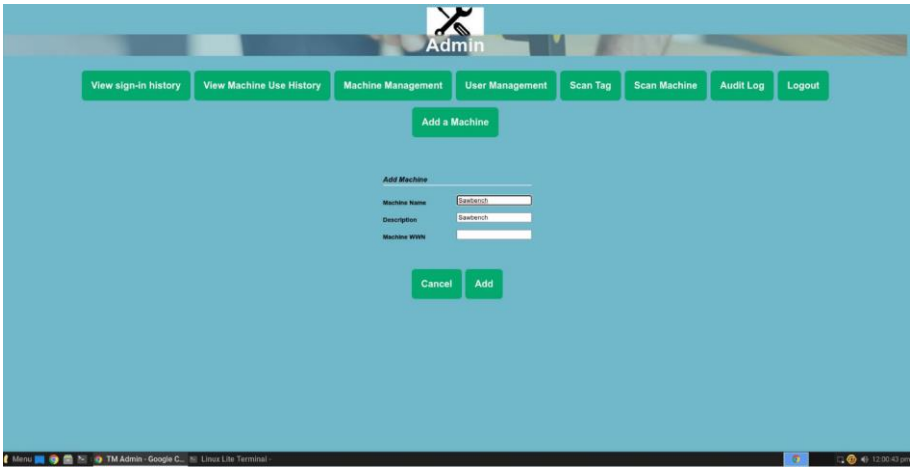
2.4.4 Machine Administration

To display the Machine Administration screen, select the “Machine Management” icon from the header.



2.4.4.1 Adding a Machine

To add a Machine, select the “Add a Machine” icon. You will be presented with the following screen.



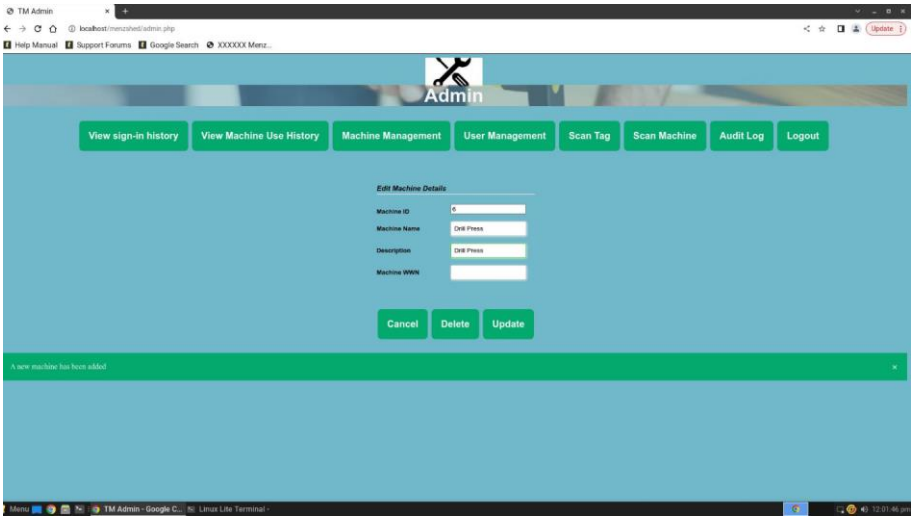
The following fields will be displayed:

- Machine Name: The name of the Machine
- Machine Description: Long form name of the Machine
- Machine WWN – The unique ID of the Access Box connected to the Machine (optional)

To add the Machine, select the “Add” button.

2.4.4.2 Modifying a Machine

To modify a Machine, select the “Edit” button on the Machine List, you will be presented with the following screen. Now the machine is present, the Machine ID will also be displayed.



2.4.4.3 Deleting a Machine

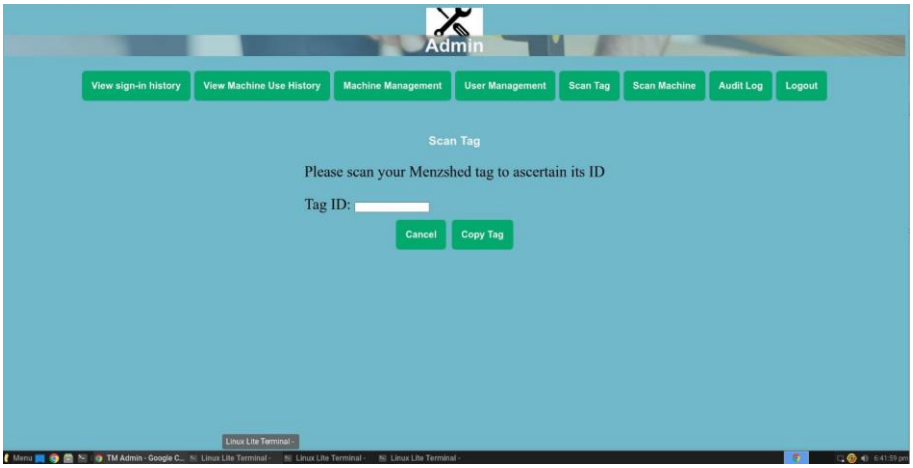
To delete a Machine, select the “Edit” button next to the machine and the “Delete” button on the Edit screen.

2.4.5 User and Machine Registration

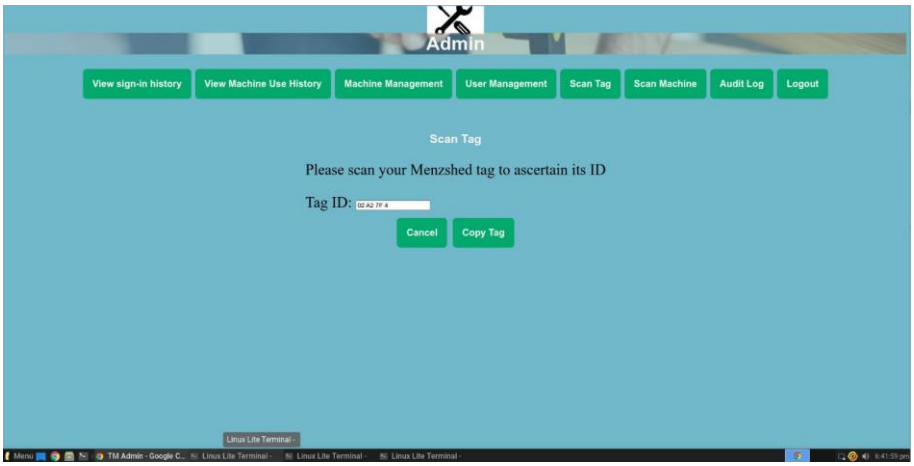
2.4.5.1 User Registration

To assign a Swipe Card or Fob to a User, logon as an Administrator to the Central Server and select the “Scan Tag” button.

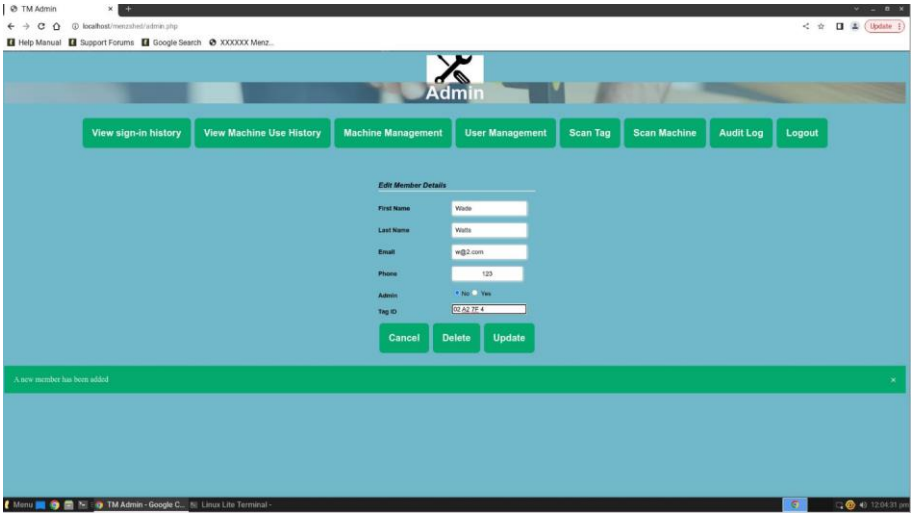
You will be presented with the following screen.



On the Sign-in Box, swipe the Fob to be assigned. After a 1-2 second interval, the unique ID of the Fob will be displayed on the screen. Select the “Copy Tag” button to copy the Tag ID into memory.



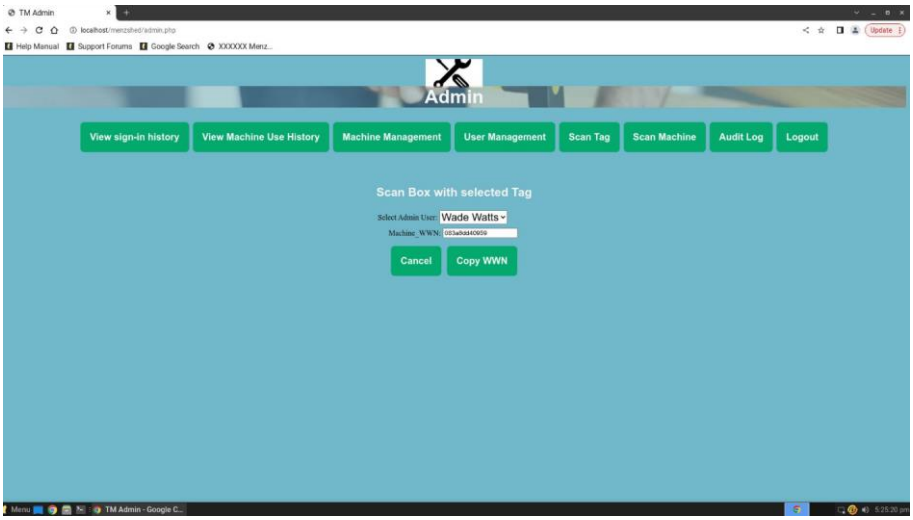
Navigate to the User using the “Edit” function of the “User Management” screen. You can then paste the copied ID to the “Tag ID” field using keys [Control]-V, and update the User with the “Edit” button.



2.4.5.2 Machine Registration

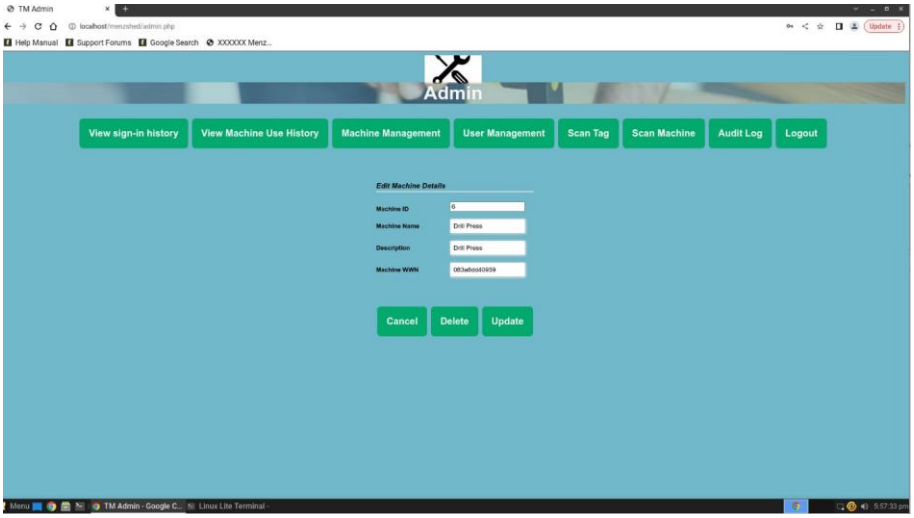
NOTE: This only applies if using a WWN based image on the Device Access Box.

Log into the Admin Area using an Administrator Fob, and navigate to the “Scan Machine” Screen. From the drop-down box, select the Administrator whose tag will be used to identify the Device Access Box. Once this is selected, the screen will refresh every 2 seconds with the latest Device that the Administrator has swiped against.

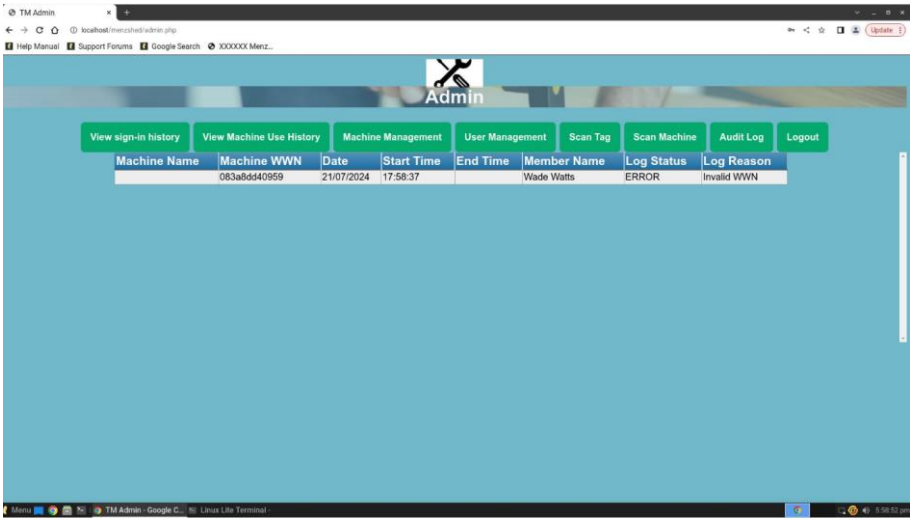


To place the Machine WWN discovered into the Copy buffer, select the “Copy WWN” button.

Now navigate to the Machine Management screen and “Edit” the required machine. Paste the WWN into the “Machine WWN” field using [Control]-V and select “Update”. The system will validate the WWN and if it is used elsewhere, it will prevent you from committing the update.



NOTE: If the Device Access Box is previously unknown to the System, you will see an error message in the Machine Use History for “Invalid WWN”, similar to the one below. This is expected behaviour and more will be explained on error codes later in this document.



2.4.6 Sign in / Sign Out

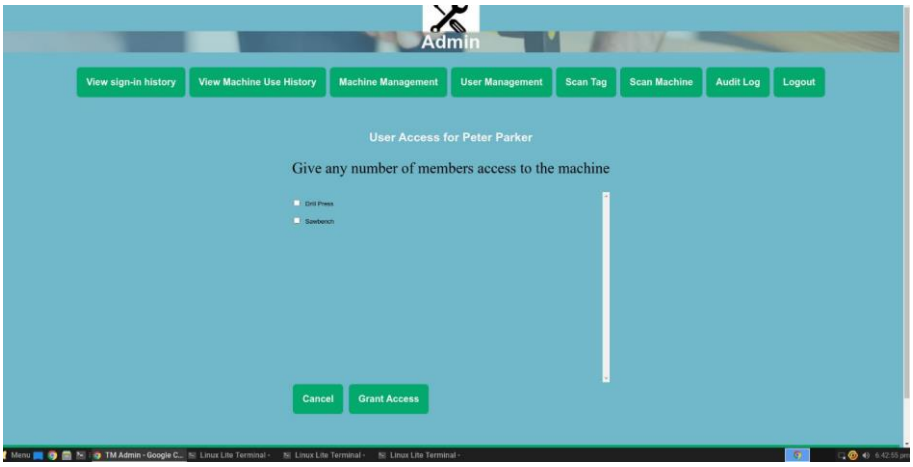
To sign in, ensure the Server Console is out of Administration Mode and showing the Sign in Screen. By swiping your Fob against the Sign In Sensor, you will be logged in, or (if already logged in), logged out. The screen will be refreshed every 2 seconds with the latest information.

2.4.7 Access Granting

Access can be granted for Users to operate Machines in 2 separate ways. Both update the same backend Database, so any changes in one will be reflected in the other.

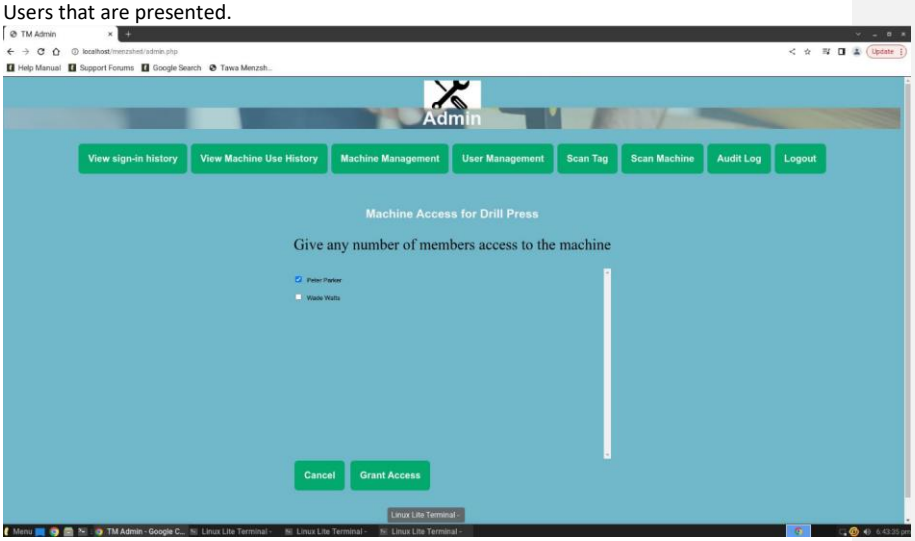
2.4.7.1 Machine based Access Granting

If you navigate to the User Management Menu, and select the “Access” against the Icon of the relevant User, you can grant or deny access to the Machines defined in the system. Select the “Grant Access” icon to submit the changes.



2.4.7.2 User based Access Granting

To grant access to specific Users, navigate to the Machine Management screen and select the “Access” icon next to the relevant Machine. You can then add or remove rights for the Users that are presented.



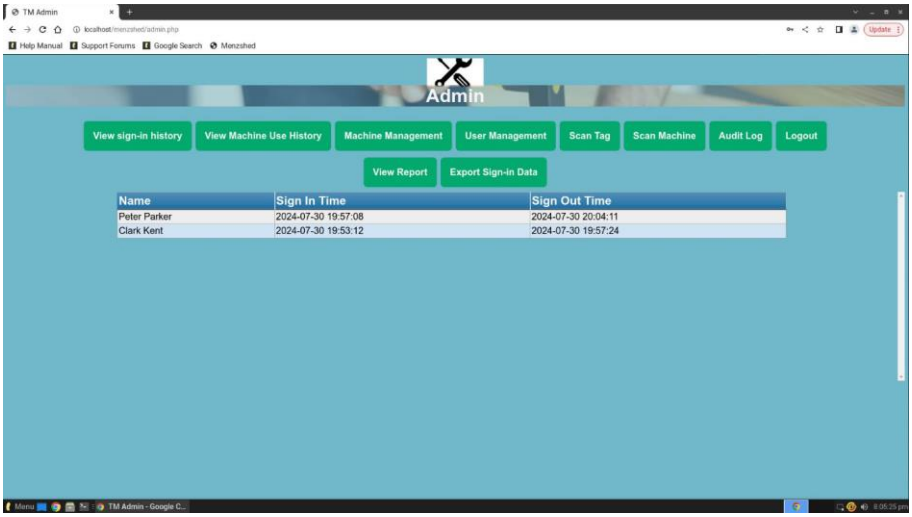
2.4.8 Device Swapping

If you are using the WWN variant of the Access Box Image, you can use the “hot swap” capability.
To replace a broken Device Access Box, swipe the new Device Access Box using the “Scan Machine”, then paste that into the

2.5 SCIS Error Codes and Troubleshooting

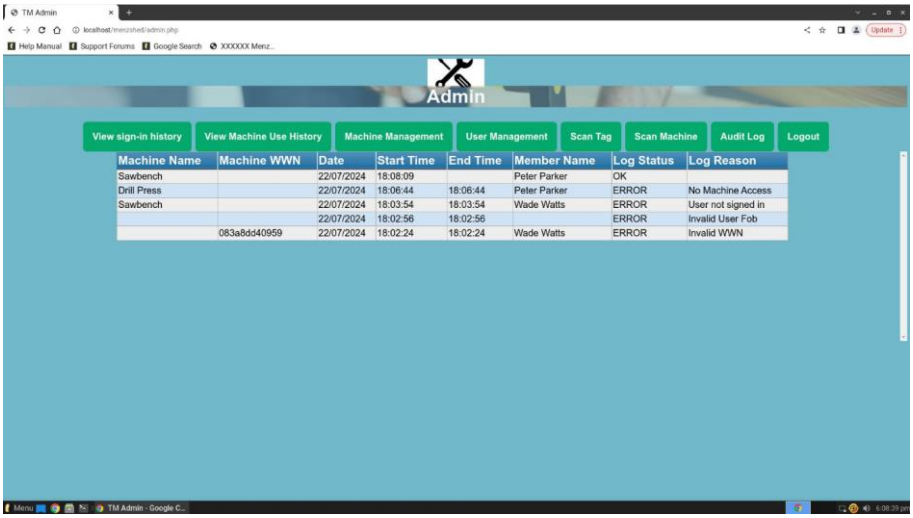
2.5.1 Sign-in Logs

To review the sign-in logs, select the “View sign-in history” button from the main screen.



2.5.2 Machine Logs

There is a set of Audit Logs for Machine use, which can be viewed using the “View Machine Use History”



For a successful Machine Access, the “Log Status” field will show “OK” and the Start and End Date will indicate when the power was enabled and disabled for the Device Access box.

The other error related messages are as follows…

Error	Description
Invalid WWN	Someone has attempted to use a WWN-based Device Access Box, either as an Administrator scanning a box, or a user attempting to use an unknown box.
Invalid User Fob	A swipe action has been performed with a Fob or Card not known to the system.
User not signed in	A valid User has attempted to use a Machine but has not yet swiped in.
No Machine Access	The User is presenting a valid Fob and has signed in but is not authorised to use the Machine.

2.5.3 Access Box Troubleshooting

When initially starting up, a Device Access Box will alternate the Green and Red Leds until it successfully registers with the Server, at which point the Red Led will be constantly on.

When a swipe attempt has been successfully made and approved, the Green LED will be lit.

When a swipe attempt has been successfully made and rejected, the Red LED will flash once and then return to being constantly on.

Sometimes a Device Access Box will not read a swipe action, in which case you should retry 2-3 times about 2-3 seconds apart. The best results come from swiping across the face of the sensor area and against the body of the Access Box.

If no response is still forthcoming, you may need to power cycle the Device Access Box.

It is recommended after usage is finished to power down the Device Access Box.

A Device Access Box will normally provide 30 mins of access at which time it will disable the Power connection. This will happen at the 30 minute point even if the machine is in use. Future releases are planned to detect this situation and provide a more orderly shutdown process.

2.5.4 Administration Gui Troubleshooting

Sometimes when the Scan Tag or Scan Machine tasks are used, they can remain active and background and take over the screen. The way to block this when it happens is to press F5 (on the keyboard) to refresh the screen. This should have been detected and corrected in the code, please alert via the email address if you continue to see this.

2.5.5 Community Forums

While there is no community forum for the SCIS system, you can query the technical staff at scistechnician49@gmail.com on issues related to the SCIS code or highlight any bugs you find. This will be on an as-available basis, and may not necessarily be able to resolve your issue.

Alternatively, there are several excellent public forums for assisting in resolving issues…
https://www.arduino.cc/ - Useful for Arduino related issues (including hardware setup)
https://stackoverflow.com/ - Provides coding and technical advice on web services and linux.

2.5.6 Copyright and Licensing

This suite of Programs is released under the GNU General Public License. The basic rules are as follows:

- You may use this software for any purpose (commercial or private)
- This software must be distributed with all its code available to view / modify
- This software must be made available for no cost
- If you modify this software, you must credit previous contributors to it.
- If you wish to distribute modified versions of this software, you must follow all the rules in this list.

For detailed information, visit the website https://www.gnu.org/licenses/licenses.html

This software is distributed without any warranty or guarantee and is used at the owner's risk.