



Welcome to the future of streamlined and efficient operational data

*Introducing Connected Safety Net's
dynamic, digital ecosystem*

 **+44 20 80592758**
 **info@connectedsafetynet.co.uk**
 **connectedsafetynet.co.uk**



At Connected Safety Net, we're dedicated to revolutionising operational business processes. Our cutting-edge digital platform is engineered to seamlessly manage safety compliance and streamline operational processes, ensuring optimal efficiency and safety at every turn.

Imagine a dynamic digital ecosystem where every aspect of your operations is meticulously monitored and managed in real-time. From crucial safety compliance protocols to the intricate details of daily work activities, CSN empowers employees to work confidently and efficiently, while maintaining a sharp focus on productivity and resource utilisation.

Gone are the days of disjointed processes and fragmented data. Incident reporting, accident tracking, near-miss analysis, inspections, audits and work activities are seamlessly integrated into a single, intuitive app portal. Every aspect of your operation is synchronised, optimised and primed for success.

Experience the power of Connected Safety Net and join us in shaping the future of operational business processes in the digital age.



The current challenges

- Current solutions tend to focus on individual parts of the end-to-end process & are not joined up.
- The result is inefficiencies in operational processes resulting in increased costs.
- Traditional paper-based solutions have high admin costs, they're messy and relevant supporting data is not always available.
- Data is dispersed across multiple locations making analysis challenging.
- Organisations are unable to easily access the data required to meet business objectives.

The solution



CSN Capture

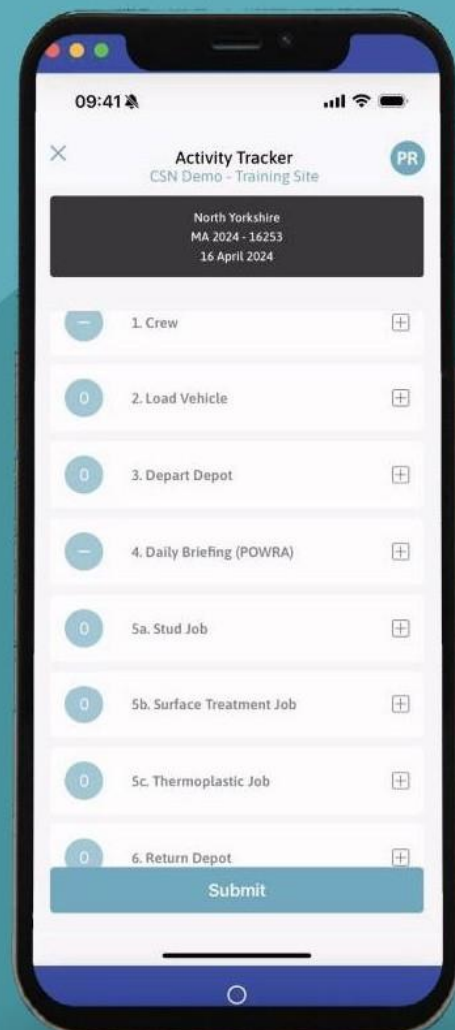
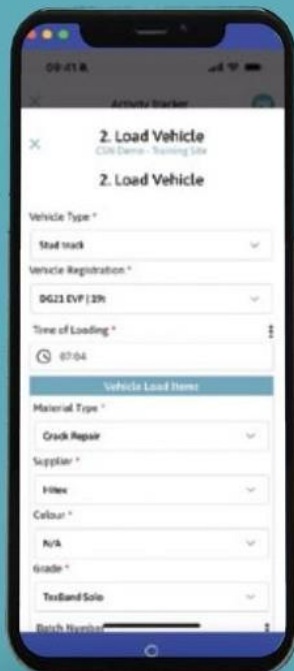
A digitisation factory to automate any business process



CSN Capture: A digitisation factory to automate any business process

Our easy-to-use app & portal is the gateway to streamlined, efficient business operations:

- Replace traditional, cumbersome paper-based processes with innovative technology solutions
- Automate processes to effortlessly transform physical & digital documents into seamless digital workflows
- Turn tedious tasks into strategic initiatives and embrace operational excellence
- Unlock exceptional efficiency & productivity and be more sustainable with our paperless ecosystem





CSN Capture: A cloud-native platform for enterprise process digitisation, automation, and operational intelligence

1. Platform Overview

CSN Capture is a cloud-native, enterprise-grade platform designed to digitise and automate any operational, compliance, or safety process. Built on Microsoft Azure and architected for global deployment, it provides a configurable no-code environment where organisations can create, deploy, and evolve digital workflows without developer involvement.

The platform centralises the entire lifecycle of operational data: form design, mobile capture, workflow automation, document control, analytics, scheduling, and AI-assisted decision support. All components operate within a unified digital ecosystem, enabling organisations to replace paper systems and fragmented tools with a single, resilient, continuously improving platform.



2. Core Functional Capabilities

2.1 No-Code Digital Form & Workflow Builder

- Drag-and-drop creation of dynamic, multi-layered forms
- Conditional logic, branching and validation rules
- Smart components: dates, signatures, scoring, media capture, barcode/QR scanning
- Public-facing form support via QR code or URL
- Instant publication to mobile and web clients

The screenshot displays the NET No-Code Digital Form & Workflow Builder interface. On the left, a sidebar contains a top section with 'Name' (Emaar ID), 'Status' (Draft), and a 'Publish' button. Below this are 'Form Details' and 'Question Types' sections. The 'Question Types' section lists various input types: Single Select Dropdown, Multi Select Dropdown, Text Input (Single Line), Text Input (Multi Line), Date Selector, Time Selector, 1D Barcode, 2D/QR Barcode, GPS Location, and Signature Box. The main workspace is divided into two panels. The top panel is for a 'Single Select Dropdown' question, showing fields for 'Question Prompt' (Understanding operational working processes), 'Question Description' (Analyse the effects of operational processes and make sure we are effective in the way we work), 'Placeholder' (Operational working processes), and 'Action Form' (Action Tracker (Incidents)). It also includes checkboxes for 'Rqd', 'Notify' (checked), and 'NonCom'. A 'Connect to drop-down list' checkbox is present, along with an 'Add Parameter' button and a list of parameters: Workflow one, Workflow two, Workflow three, and Value. The bottom panel is for a 'Time Selector' question, showing fields for 'Question Prompt', 'Question Description', and 'Action Form' (No Action Form Selected). It also includes checkboxes for 'Rqd', 'Notify', and 'NonCom'.



2. Core Functional Capabilities

2.2 Native Mobile Applications

- Offline data capture with auto-sync
- Photo, video, and file attachments captured in-app
- Speech-to-text input for rapid field reporting
- Device-level geolocation for metadata tagging
- Real-time status tracking of submitted forms

2.3 Guided Operational Workflow

- Step-by-step guided actions ensure consistent data capture
- Automated task routing and assignment
- Action tracking with escalations and reminders
- Multi-stage approval workflows
- Integrated signature capture and verification

2. Core Functional Capabilities

2.4 Multi-Language & Globalisation Framework

- Native UI support for multiple languages (English, French, German, Arabic, etc.)
- Real-time machine translation covering 200+ languages
- Dual-language user input/output for globally distributed teams
- Configurable localisation for date formats, address structures, currencies, measures

OH&S Audit

English

Urdu

Hindi

Malayalam

Tamil

Back

Save

CSN Attend Intersec Safety Show...

EXPERIENCE

THE FUTURE OF SAFETY

WITH CSN AT

INTERSEC DUBAI

Watch on YouTube

Please ensure that all required fields are completed. If you require clarification or guidance on any item, click the hamburger icon located at the top right corner of each question and select 'View Info' for detailed instructions.

Area Coach Name *

Enter Name

Mobile Number *

Enter Mobile Number

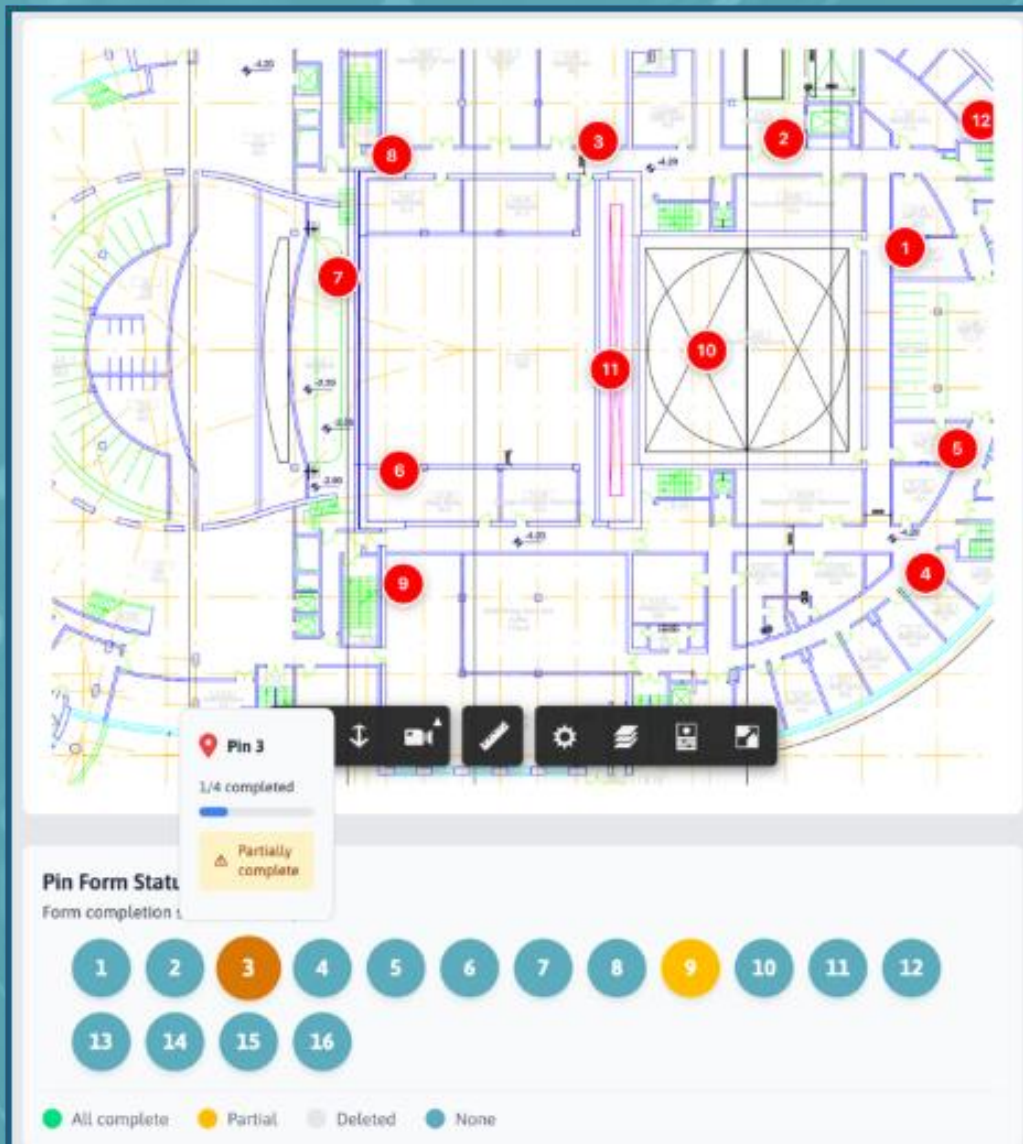
Address *

Are you at the address?

3. Advanced Platform Capabilities

3.1 CAD/PDF Annotation Engine

- Secure upload of CAD, PDF, and technical drawings
- Pin-placement directly onto diagrams
- Each pin can instantiate a workflow, inspection, defect, or action
- Photo and narrative attachments linked to each annotation
- Available on both web and mobile



3. Advanced Platform Capabilities

3.2 Integrated Booking & Scheduling Engine

- Resource scheduling for staff, contractors, vehicles, rooms, or equipment
- Availability logic with auto-conflict resolution
- Customer booking confirmation and reminders
- Can be deployed for engineering, workforce scheduling, hotel/spa bookings, etc.

001

Booking Form

Home / App Menu / Booking Form / F6084-039-00001

Open

Action

Print PDF

Notifications

Action	Date & Time	Name	Comments
Saved	22/JUL/2025 11:43	Falzan Zahoor	

Back

Edit

Booking Name

Audit Booking

Booking Purpose

To conduct audit

Appointment

<

>

today

September 2024

month

week

day

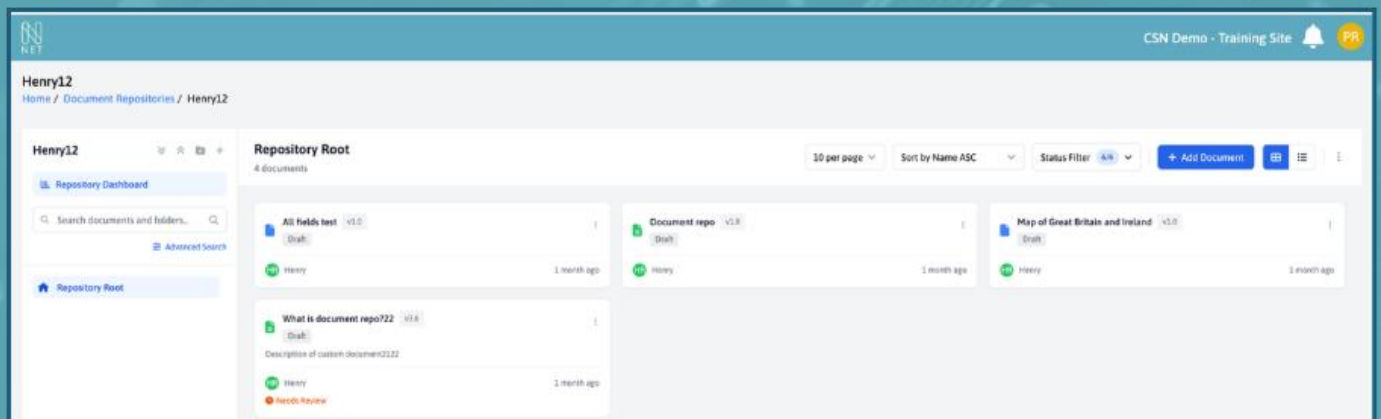
list

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21

3. Advanced Platform Capabilities

3.3 Enterprise Document Repository

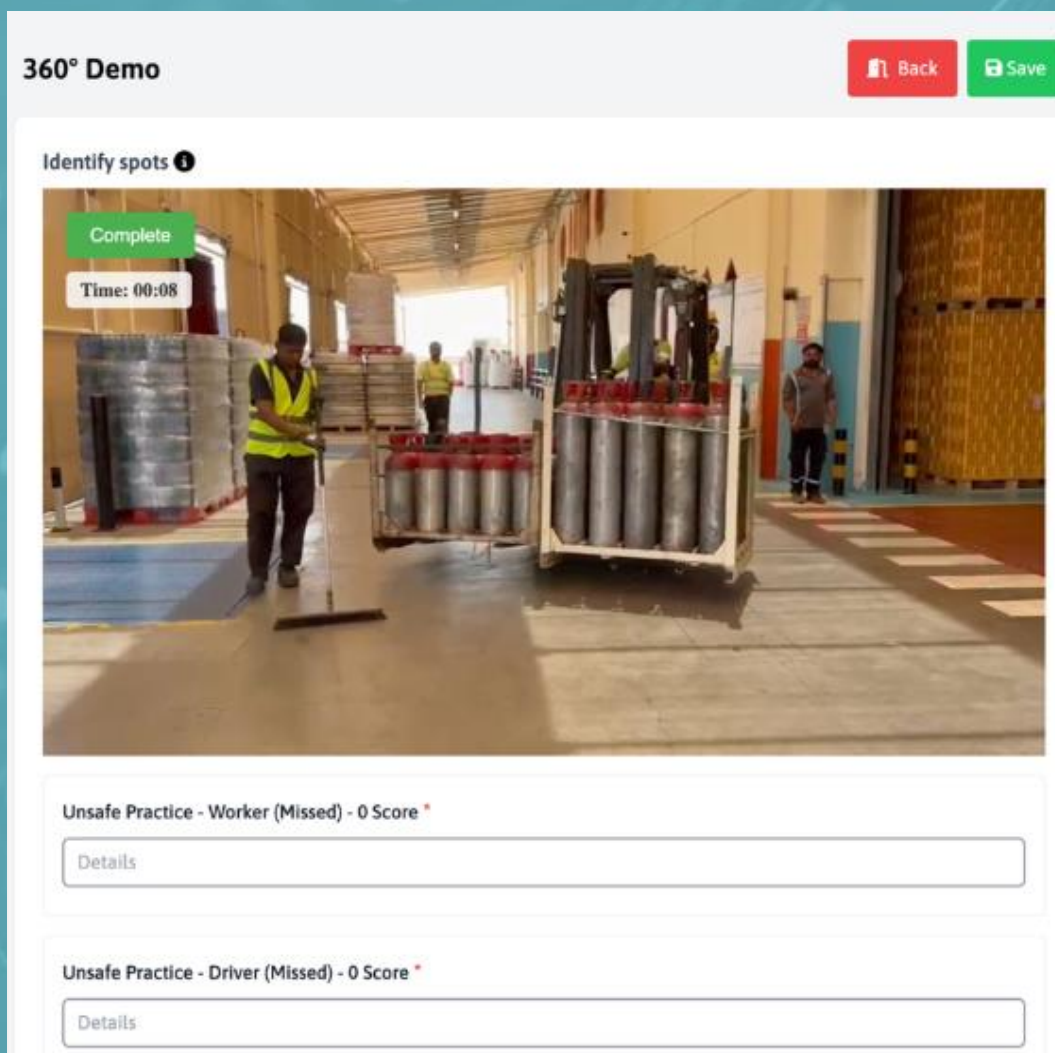
- Unified repository for all documents
- Metadata-driven indexing for rapid retrieval
- Role-based access with encrypted storage
- Version control with full audit log history
- Read-receipt and acknowledgement workflow
- Secure policy distribution with expiry tracking
- Document hierarchies and role-based access
- Mandatory review with traceable signature confirmation



3. Advanced Platform Capabilities

3.4 Workforce Engagement & Gamification

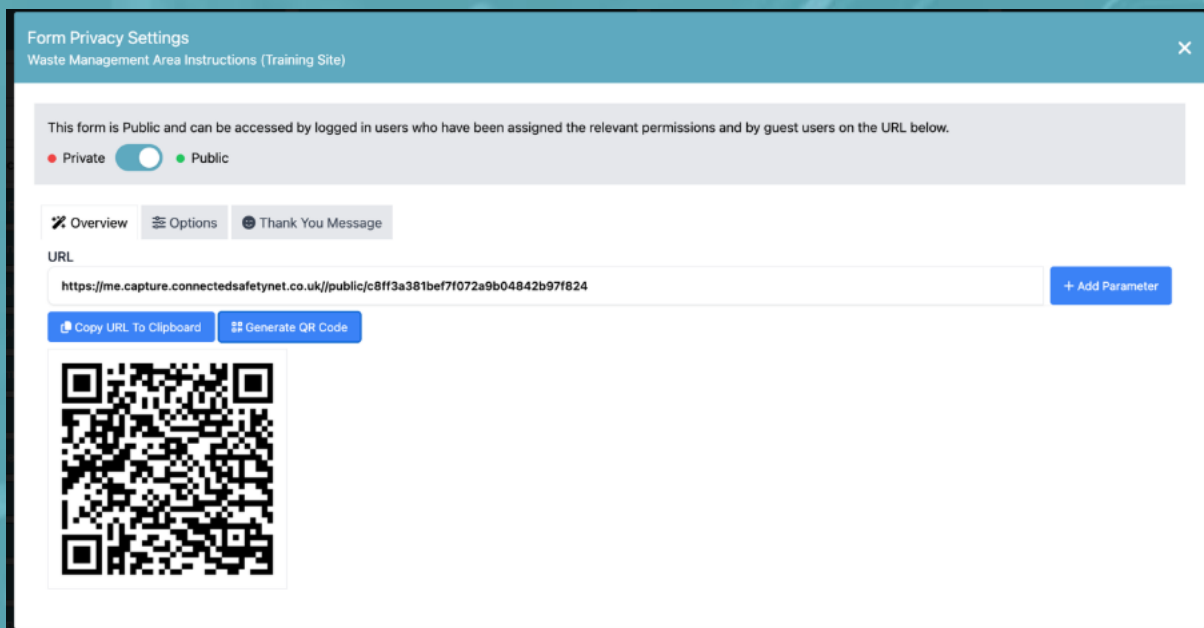
- Achievement-based recognition system
- Badge levels: Bronze, Silver, Gold, Platinum
- Tied to training, compliance, safety performance, or custom metrics
- Boosts engagement for field and frontline teams



3. Advanced Platform Capabilities

3.5 Asset & Inventory Management

- QR/barcode-based asset identification
- Asset lifecycle logging (maintenance, inspections, expiry)
- Consumable monitoring with automated reordering trigger points

A screenshot of a 'Form Privacy Settings' dialog box for 'Waste Management Area Instructions (Training Site)'. The dialog has a blue header bar with a close button (X) in the top right. Below the header, a grey box contains the text: 'This form is Public and can be accessed by logged in users who have been assigned the relevant permissions and by guest users on the URL below.' Below this, there are two radio buttons: 'Private' (with a red dot) and 'Public' (with a green dot and a selected toggle). Underneath, there are three tabs: 'Overview' (selected), 'Options', and 'Thank You Message'. The 'Overview' tab shows a 'URL' field with the text 'https://me.capture.connectedsafetynet.co.uk//public/c8ff3a381bef7f072a9b04842b97f624' and a '+ Add Parameter' button to its right. Below the URL field are two buttons: 'Copy URL To Clipboard' and 'Generate QR Code'. At the bottom, there is a large QR code.

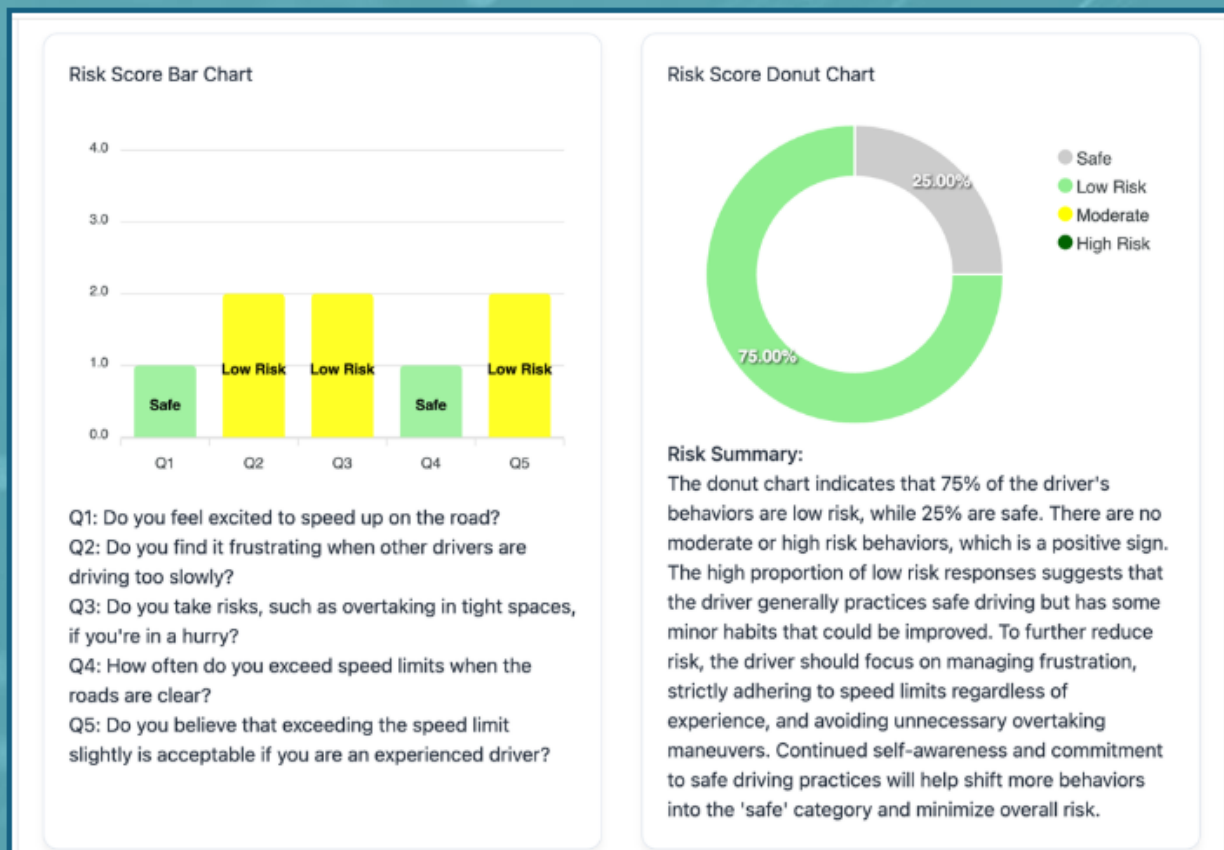
3.6 Digital Permit & Contractor Management

- Configurable Permit-to-Work workflows
- Contractor onboarding, qualification, and licence tracking
- Real-time alerts for expired or missing documents
- Embedded risk assessment and approval routing

4. AI, Automation & Insights

4.1 AI Agents & Automated Operations

- Automated scheduling, confirmations, and routine communication
- Natural language interaction for querying system data
- Auto-generated summaries, insights, and workflow updates
- AI-driven pattern detection and anomaly alerts



4. AI, Automation & Insights

4.2 Predictive Analytics

- Forecasting risks, trends, behaviours and compliance gaps
- Supports telematics-driven predictive driver scoring
- AI-generated psychometric insights using microlearning and behavioural data
- Machine learning models continuously improve from organisational data

Connected AI

Paul Richardson
Aviation

Please analyse all the data you have and tell me what's the most significant risk that we need to be mindful of and be planning for to mitigate

What is the most significant risk that we need to be mindful of and plan to mitigate, based on your analysis?Based on the analysis of the provided data, the most significant risk that needs attention and mitigation planning is the presence of corrosion and structural defects in aircraft components. Multiple instances of corrosion and minor structural cracks have been identified across various inspection reports. Specifically, corrosion was noted on components such as wing flaps, wheel hubs, and elevator hinges, while minor structural cracks were observed on the fuselage frame.

These issues pose a risk to the structural integrity and safety of the aircraft if not addressed promptly. The potential impact includes compromised aircraft performance, increased maintenance costs, and potential safety hazards if left untreated.

To mitigate these risks, it is crucial to implement a robust maintenance and inspection program that includes:

1. Regular and thorough inspections using Non-Destructive Testing (NDT) methods like Eddy Current to detect early signs of corrosion and cracks.
2. Immediate repair and treatment of identified corrosion and structural defects to prevent further degradation.
3. Enhanced monitoring and documentation of affected components to track their condition over time and ensure timely interventions.
4. Training and equipping maintenance personnel with the necessary tools and knowledge to address these issues effectively.
5. Establishing a proactive corrosion prevention program that includes protective coatings and environmental controls.

By focusing on these strategies, organizations can ensure the continued safety and airworthiness of their aircraft while minimizing the risk of operational disruptions.

4.3 AI Compliance & Safety Intelligence

- Real-time monitoring of trends and legislation changes
- Automated updates to workflows when compliance requirements evolve
- Intelligent risk scoring and recommended preventive actions



5. Integration & Interoperability

5.1 API Connectivity

- RESTful APIs secured by Auth0 JWT tokens
- Endpoints for data extraction, ingestion, and system orchestration
- Support for bi-directional integrations with ERPs, HRIS, EHS, CAFM platforms

5.2 Analytics & Reporting

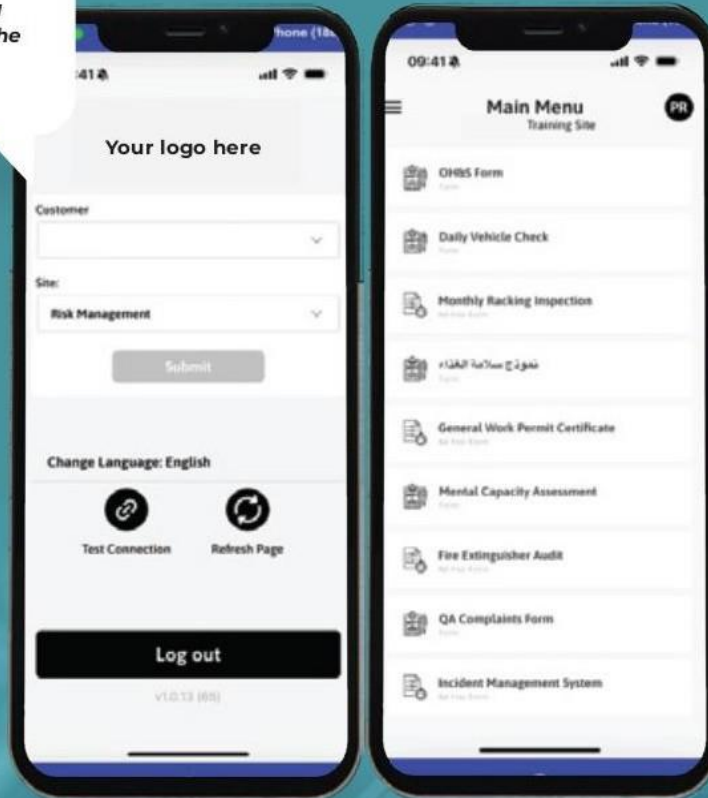
- Native integration with Microsoft Power BI
- Data connectors for enterprise warehouses and lakes
- Custom dashboards for operations, safety, compliance, training, and ESG
- Real-time drill-down analytics with live data feeds

5.3 External Services

- Azure Monitor for performance and health telemetry
- Azure Logic Apps for automated workflows and alerting
- Support for Single Sign-On (SSO) standards
- Webhooks for real-time push notifications



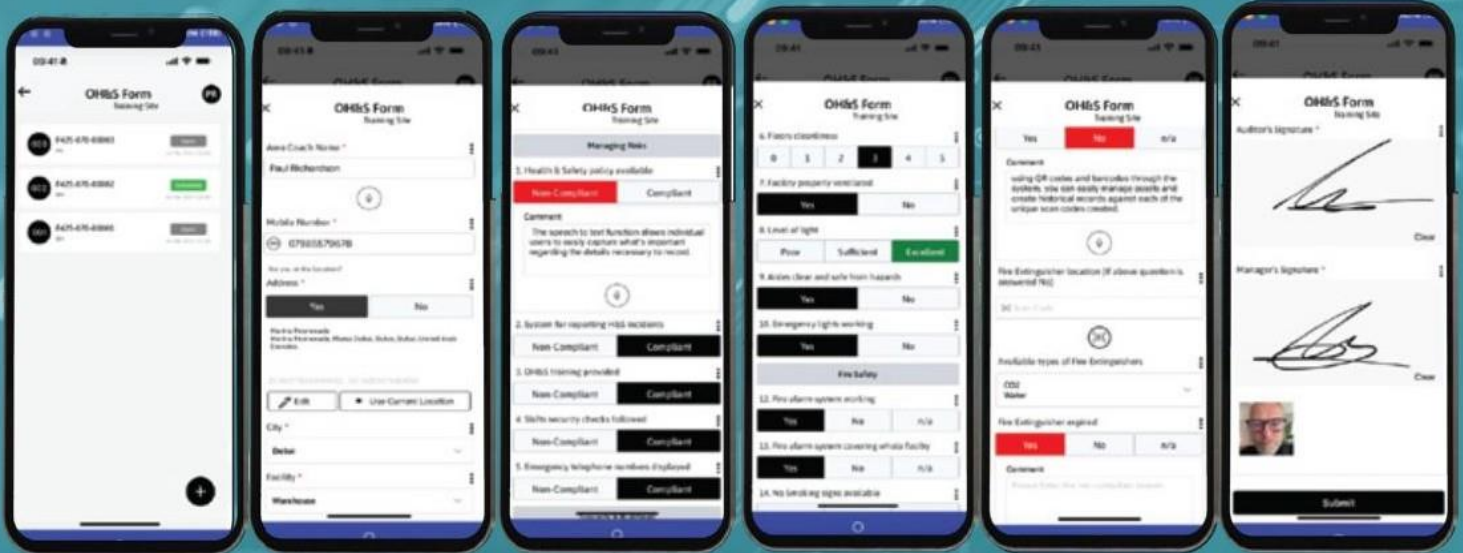
Customisation ranges from the simplicity of the log-in menu to visually engaging main menu forms to suit the businesses unique needs



Bespoke, dynamic forms

Instant reporting via the app

Multiple language capability



Simple, intuitive features

Automatic GPS location

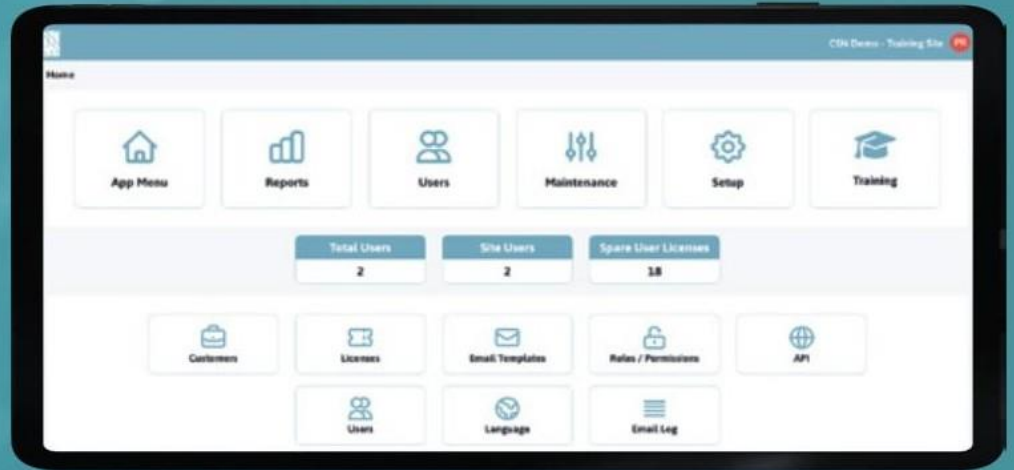
Speech to text capability

Signature verification process

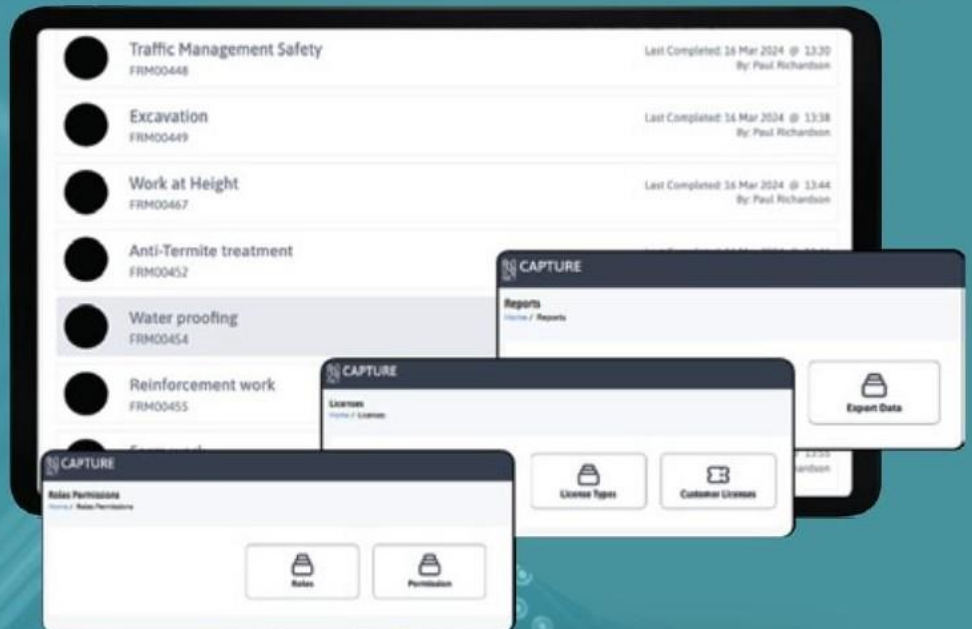
Single digital storage location gives seamless access to comprehensive, historical data such as audits, incidents, inspections, risk assessments



Straightforward and simple overview of business initiatives from the desktop



Critical documents can be seamlessly uploaded from both mobile applications and desktop offering unparalleled flexibility and prompt submission regardless of location or device

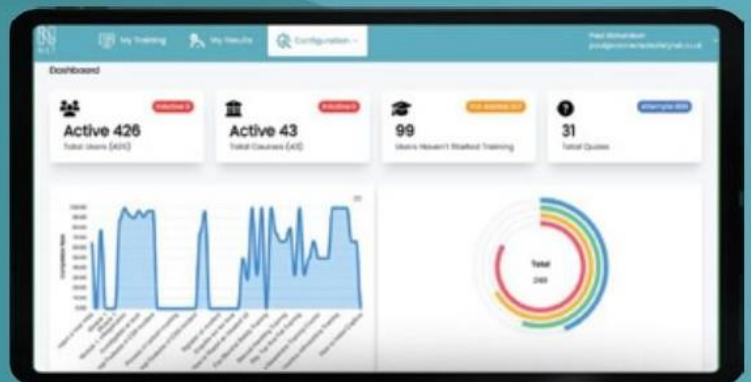
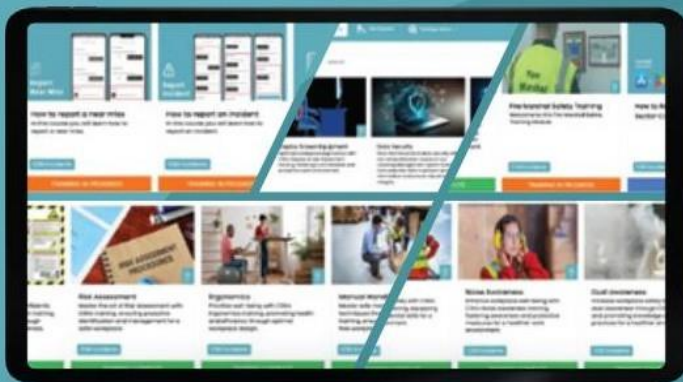


The maintenance menu allows you to modify processes without needing to recreate new forms



Power BI integrated dashboards with interactive drill down capability

E-learning portal available to enable self learning, with dashboard to monitor progress



WELCOME TO YOUR CSN LEARNING EXPERIENCE

Install or Access CSN Capture

To install/access the 'CSN Capture' App you will need:

- A smart Phone (Android or iOS)
- An internet connection (WiFi or 3G/4G/5G)
- A computer to access CSN Capture desktop using browser



Android user – Open the 'Google Play Store' to access & install the app.



iPhone user – Open the 'App Store' to access & install the app.



This is the CSN Capture App. Make sure the app you're about to install resembles the image above.

Note: Depending on service level agreement, mobile devices may be supplied with CSN Capture App pre-installed.

Note: The Capture Desktop works the best with Google Chrome browser in a computer.

CSN Capture Learning Module

This module covers:

- ✓ Launch the 'CSN Capture' App
- ✓ Navigate the app
- ✓ View forms & packs
- ✓ Explore & understand the features
- ✓ CSN Capture web portal

Note: To get the most out of this module, begin to use 'CSN Capture' App on mobile device and then proceed to CSN Web Portal.

Instructions:

- Read the course-content carefully.
- Towards the end, use the knowledge to complete a Capture form.
- Finally, complete the quiz!



Launch the CSN Capture App

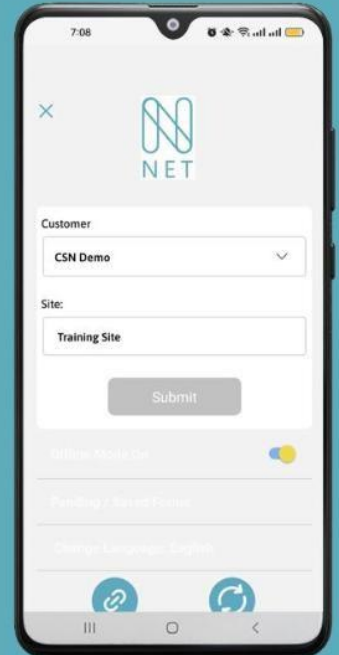


Tap the CSN Capture icon  to launch the app.

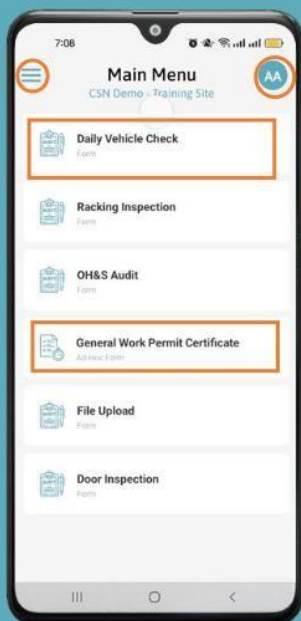
The '**user credentials**' are sent to a registered email address. Please refer to a personalised "**Welcome Pack**" to find login details.

Always contact **CSN Support**, if assistance is needed at any moment.

Support email: support@connectedsafetynet.co.uk



Understand the Main Menu



Once successfully logged in, the "**Main Menu**" loads.

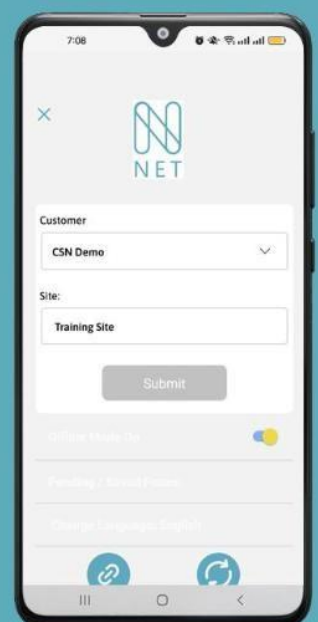
The main menu features the following:

1. Ad-Hoc Form (Pack in Capture Web-Portal)
2. Form (Form in Capture Web-Portal)
3. Hamburger menu
4. Profile icon

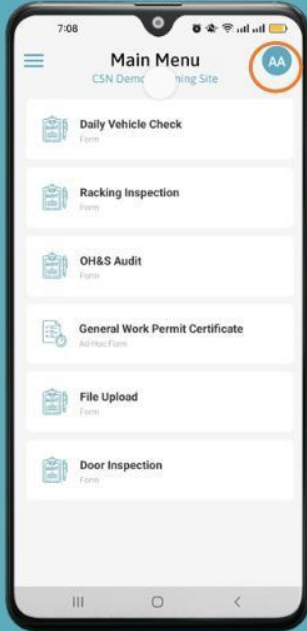
Hamburger menu:

Tapping the hamburger menu, loads the homepage of the app (*please refer to the image on the right*)

The homepage allows switching between site(s), test connectivity, refresh the page and log out from Capture.



Access the User Profile

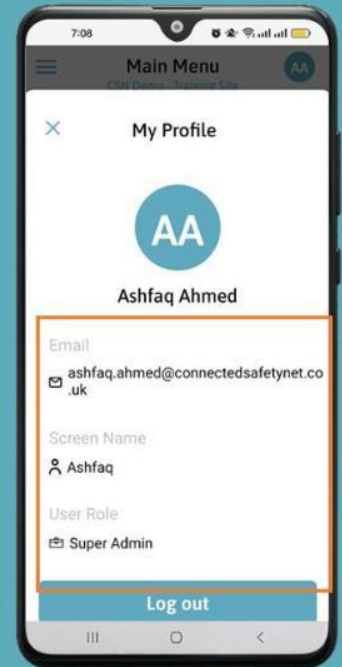


From the Main menu, tap the name icon to the top-right corner to access user profile.

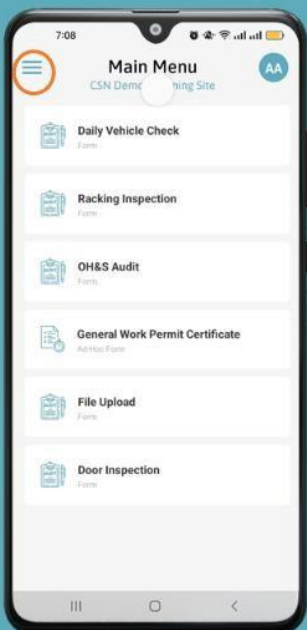
The user profile reveals:

1. Email address
2. Screen name
3. User role

Congratulations, you're all set to use the CSN Capture App!

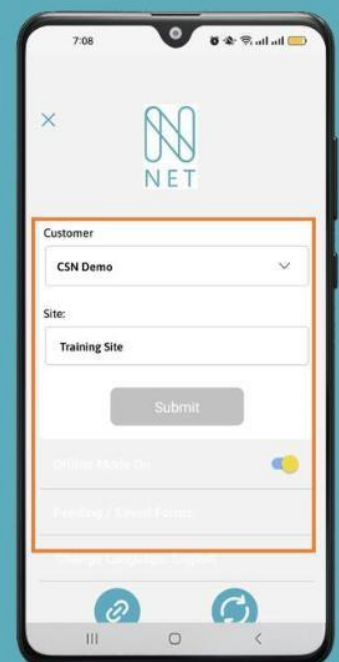


Access the Hamburger Menu



Tap the hamburger icon  to the top-left corner to access following options.

1. Switch between site(s) if multiple sites are assigned.
2. Offline Mode toggle on/off  to use the app without internet connectivity.
3. Tap Pending/Saved forms to access incomplete or forms to be submitted.
4. Change Language allows to switch between language(s), if multiple language in use.
5. Tap  to test internet connectivity and/or tap  to refresh the app page.



Understand & Differentiate Between Form & Ad-Hoc Form

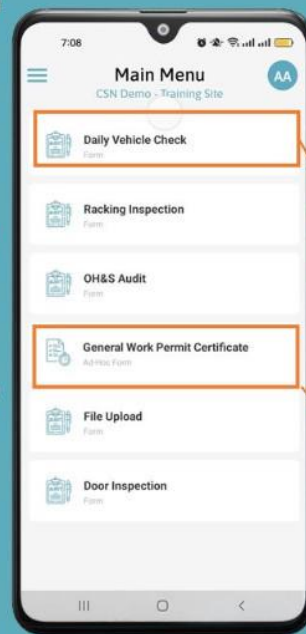
CSN Capture features two kinds of information capture capabilities.

1: The **'Form'** is a single layer combination of questions to be answered (ideally followed with a signature field) moving on to submit.

(Note: The term **Form** and **Standalone form** is used interchangeably.)

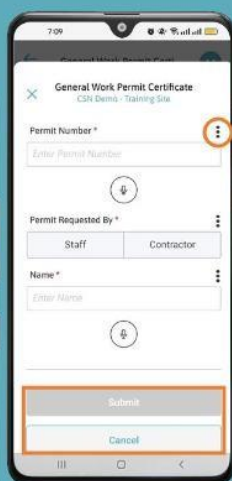
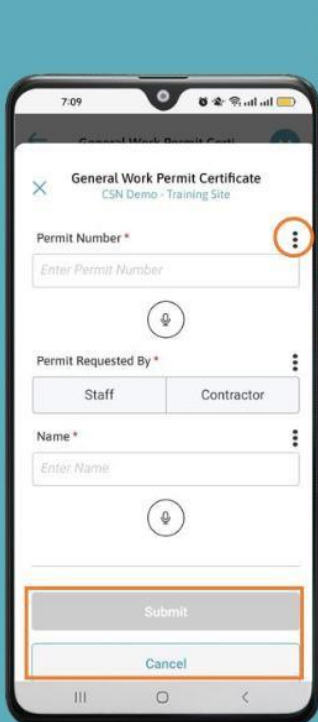
2: The **'Ad-Hoc Form'** is multi layer combination of questions to be answered. The top layer creates an entry into the system to access component forms. Once all the component forms are saved, the top layer enables the submission of an Ad-Hoc Form.

(Note: The term **Pack** and **Ad-Hoc Form** is used interchangeably)



(Note: The icon of **Pack** is different to the **Form** in CSN Capture.

Create A New Ad-Hoc Form

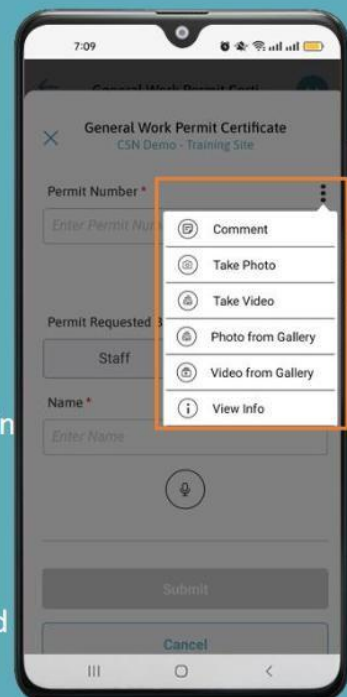


Tap the desired Ad-Hoc Form and proceed tap the **+** icon. It loads the Ad-Hoc form to add initial answers to.

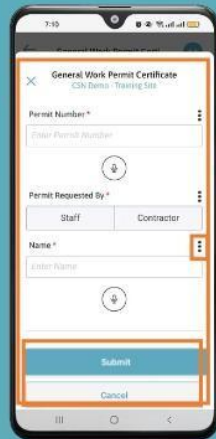
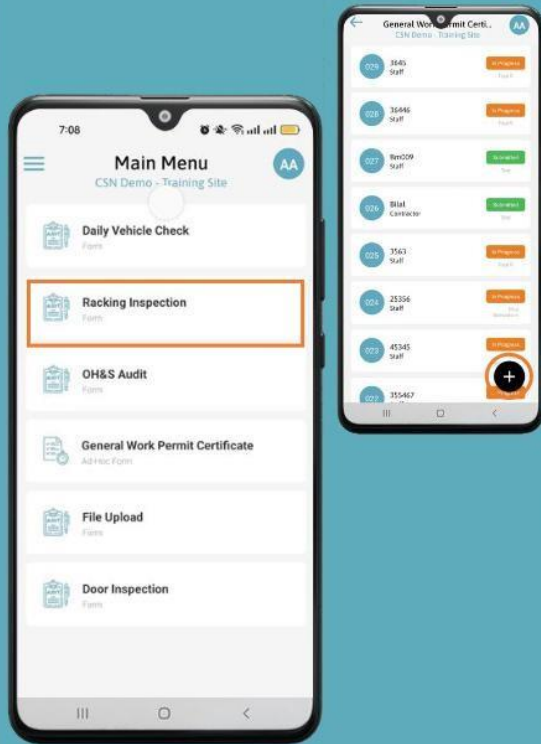
For instance in this Ad-Hoc form, select the desired date, enter your name, select location, add the relevant information and tap **'Submit'**.

Tap **'Cancel'** to go back to main menu.

To choose from additional answer options against each question, tap the three dotted icon.



Create A New Standalone Form

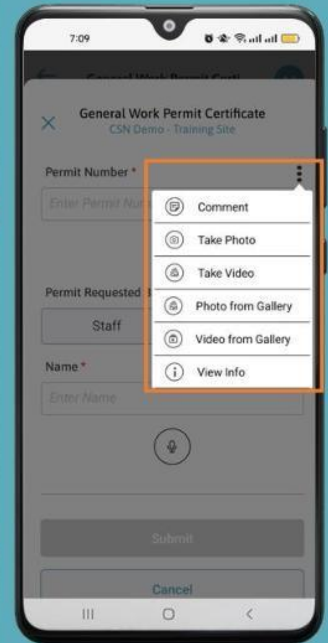


Tap the desired form and proceed tap the **+** icon. It loads the standalone form to add answers to.

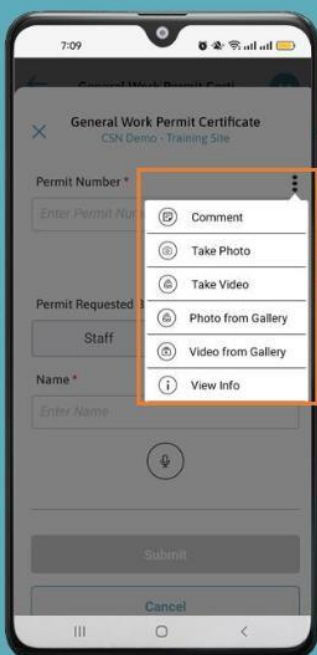
For instance in this Standalone Form answer all the questions, and tap 'Submit'.

Tap 'Cancel' to go back to Capture App main menu.

To choose from additional answer options against each question, tap the three dotted icon.

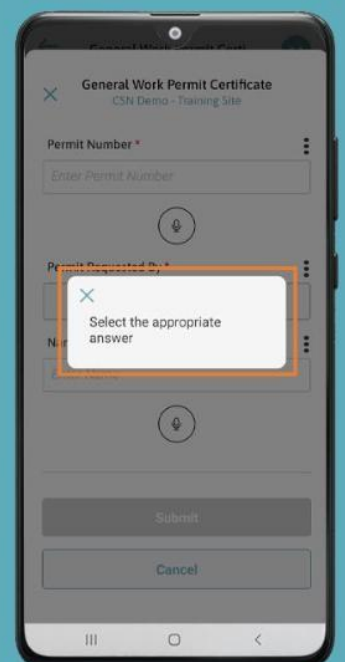


Understand 3-Dot Menu Options



The answer 3-dots menu, reveals the following answer options:

- 1. Comment:** Tap to launch the comment box for the respective question.
- 2. Take Photo:** Tap to take photo as evidence for each question.
- 3. Take video:** Tap to record video as evidence for each question.
- 4. Photo from Gallery:** Tap to attach existing video from phone's gallery.
- 5. Video from Gallery:** Tap to attach existing video from phone's gallery
- 6. View info:** Tap to view more information about the question, this may contain expanded query or specific requirements of the question.



Speech to Text Feature

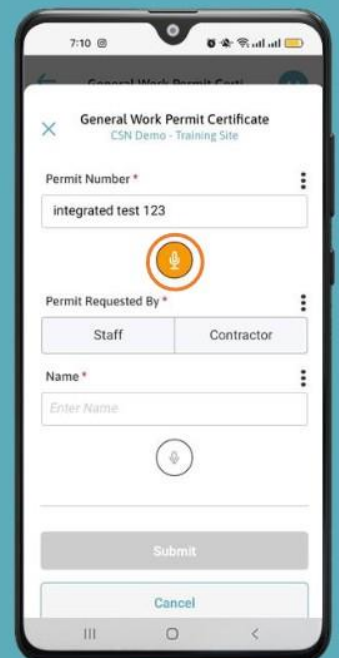
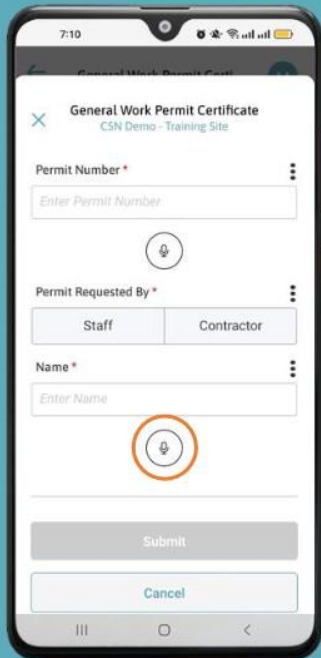
The CSN Capture app has "**Speech to Text**" capabilities.

When a comment box is available or is launched from the question menu, tap the "**microphone**" icon  and speaking into the mic to add text in the comment box. (see image on the left).

Added text can be edited. Tap the microphone to speak into the mic again to add more text, when needed.

Note: If you are using speech to text feature for the first time the mobile device asks for permissions to access microphone.

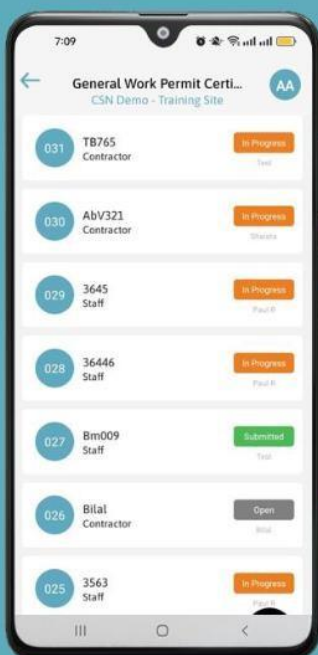
Note: The microphone icon  turns Orange during the voice capture.



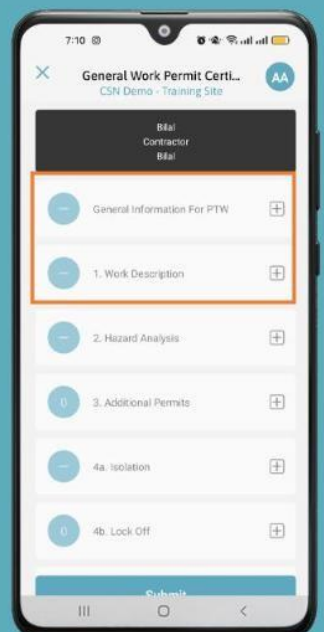
Explore the New Ad-Hoc Form

Tapping the submit button creates a new **Ad-Hoc Form**. The status of the Ad-Hoc Form is presently '**Open**'.

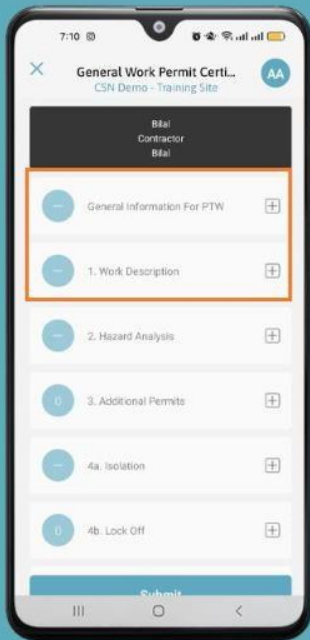
Tap the open Ad-Hoc Form to proceed, and it load the component audit forms.



Open

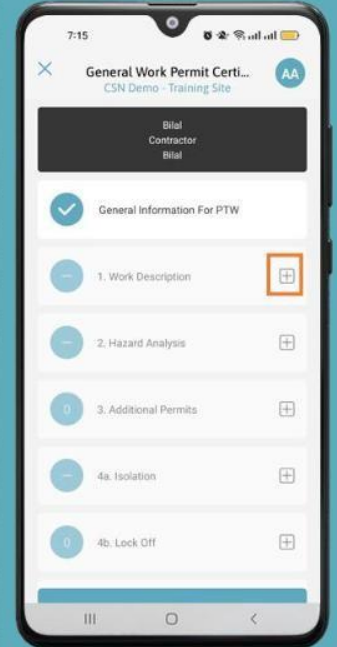


Launch the Component Forms

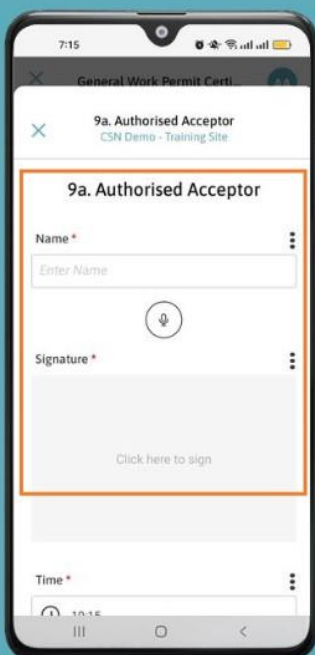


The new audit pack loads the component audit forms.

Tap  against each component audit form to load and add answers.



Answer Options – Text Field(s)

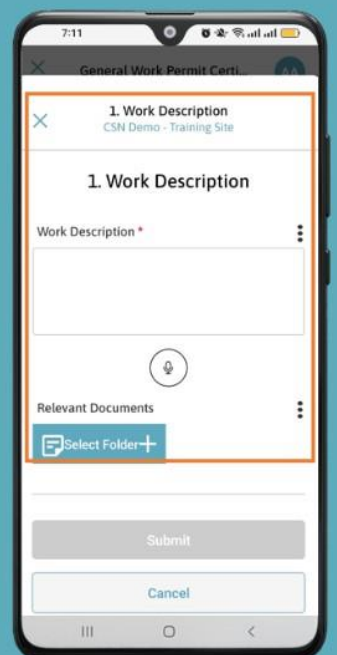


CSN Capture feature a variety of answer options, and each option is covered one by one.

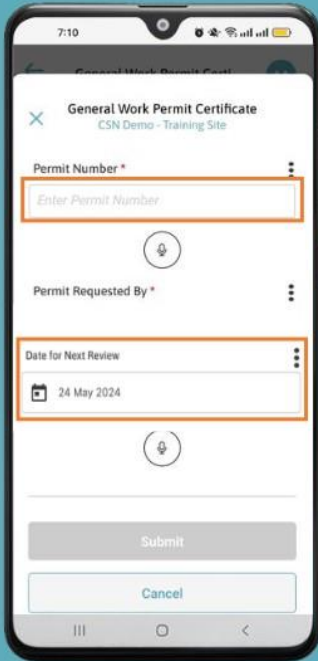
1: Text Field – allows to add text by typing the answer or adding text by using 'speech to text' feature. The text field can be plain text, alpha-numeric, or only numeric.

To add text, tap the text field and use the mobile device's keyboard to type answers. Alternatively tap the microphone icon to use 'speech to text', where available.

Note: The added text can be edited and answer added can be corrected as many times.



Answer Options – Date/Time Selector



General Work Permit Certificate
CSN Demo - Training Site

Permit Number *

Enter Permit Number

Permit Requested By *

Date for Next Review

24 May 2024

Submit

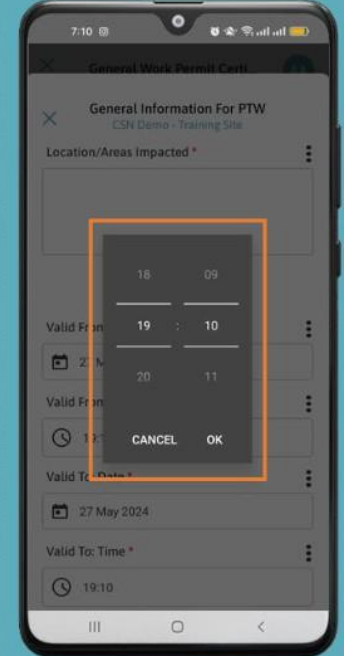
Cancel

CSN Capture feature a variety of answer options, and each option is covered one by one.

2: Time Selector – allows to select time. Tap the time field and time selector sub-window pops up. Select the desired time tap **CANCEL** **OK**

3: Date Selector - allows to select date. Tap the date field and date selector sub-window pops up. Select the desired date tap **CANCEL** **OK**

Note: The selected time/date can be edited and selected again.



General Information For PTW
CSN Demo - Training Site

Location/Areas Impacted *

Valid From

Valid To

Valid To: Date *

Valid To: Time *

18 : 09

19 : 10

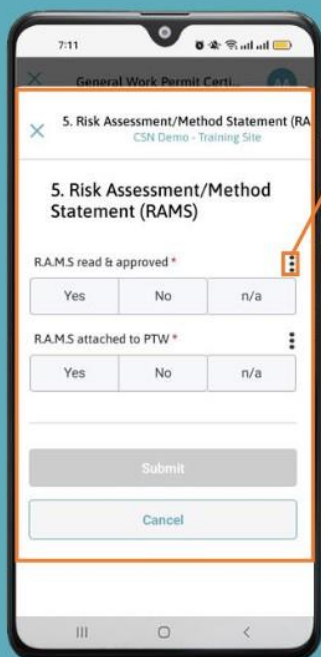
20 : 11

CANCEL OK

27 May 2024

19:10

Answer Options – Radio Button/Score



General Work Permit Certificate
CSN Demo - Training Site

5. Risk Assessment/Method Statement (RAMS)

RAMS read & approved *

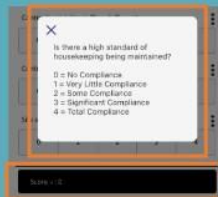
Yes No n/a

RAMS attached to PTW *

Yes No n/a

Submit

Cancel



Is there a high standard of housekeeping being maintained?

0 = No Compliance
1 = Very Little Compliance
2 = Some Compliance
3 = Significant Compliance
4 = Total Compliance

Score = 0

Score = 0

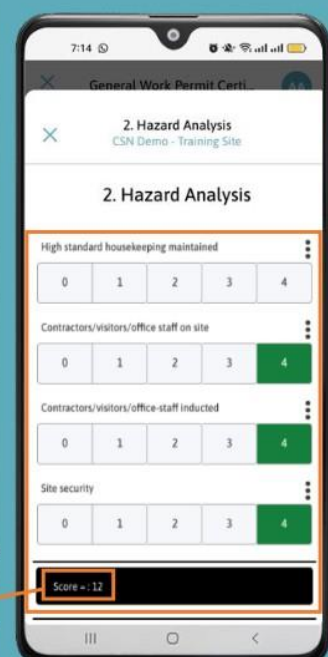
Before the answer selection the score is zero

CSN Capture feature a variety of answer options, and each option is covered one by one.

4: Radio Button – allows to select from the options the best answer against the given question. Tap the **three-button icon**, and tap **view info** to access the question details.

5: Score - Based off the selection the scoring feature populates the total compliance score achieved.

Note: The radio button response can be edited and based off the new selection, the scoring automatically updates.



General Work Permit Certificate
CSN Demo - Training Site

2. Hazard Analysis

High standard housekeeping maintained

0 1 2 3 4

Contractors/visitors/office staff on site

0 1 2 3 4

Contractors/visitors/office staff induced

0 1 2 3 4

Site security

0 1 2 3 4

Score = 12

Score = 12

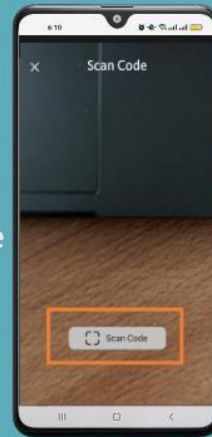
The score is now updated

Answer Options – Bar/QR Code Scan

6: Bar Code – allows to scan the bar/QR code using mobile device's camera. Tap the code scan icon  to activate the camera. Direct the camera lens to the code. The device picks up the embedded code information, and places it in the scanned code field

Note: The mobile device asks for permission to use camera when using this feature for the first time.

Note: The code scan is editable, and the new scan replaces the previously captured information.



qr.inc.hp.com/go/c42135



Scan Successful

Answer Options – Dropdowns

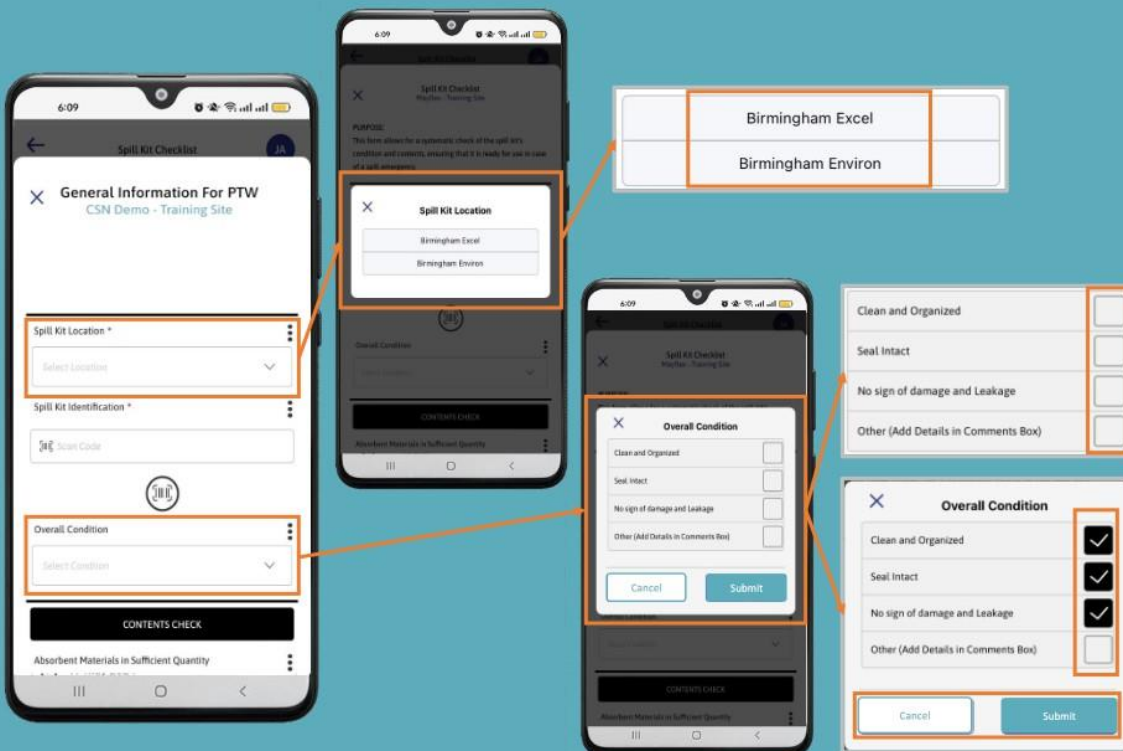
7: Dropdowns – allow to select from a pulldown/pop-up menu of available options.

Single Select Dropdown – offers to select a single item from a pre-loaded menu.

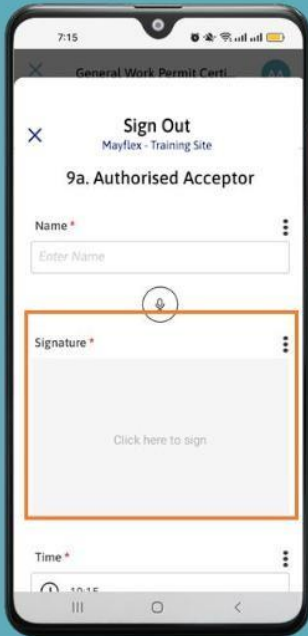
Multi-Select Dropdown – offers to select multiple options using check box(s) and tap **Submit**. Tap **Cancel** to go back.

Note: The selected options can be changed anytime to update the answers.

Note: Scroll up/down to navigate the dropdown.



Answer Options – Signature Pad

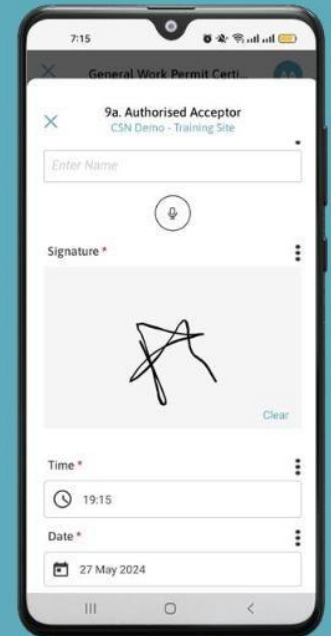


8: Signature Field – CSN Capture allows to add signature. Where available, navigate towards signature field and tap to activate the freehand **Signature Pad**.

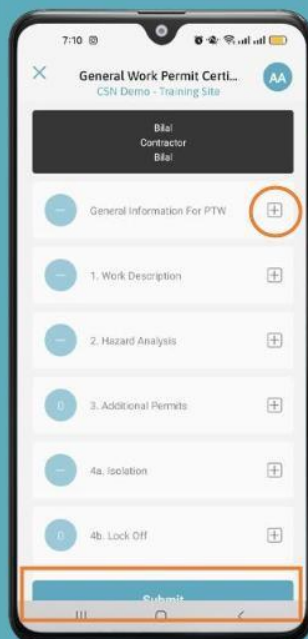
Tap the freehand field and use the digitiser to input signature.

Note: Tap 'Clear' to remove the added signature and to start over.

Note: Single or multiple signature fields are available depending on the audit form.



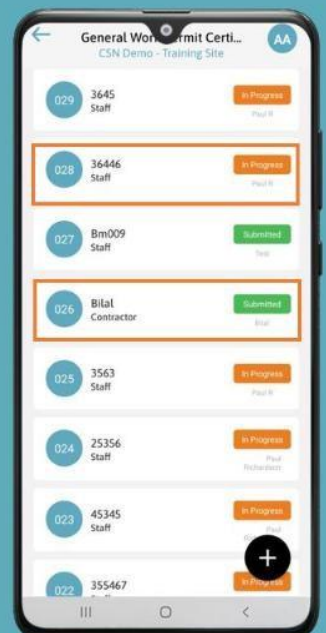
Complete An Ad-Hoc Form



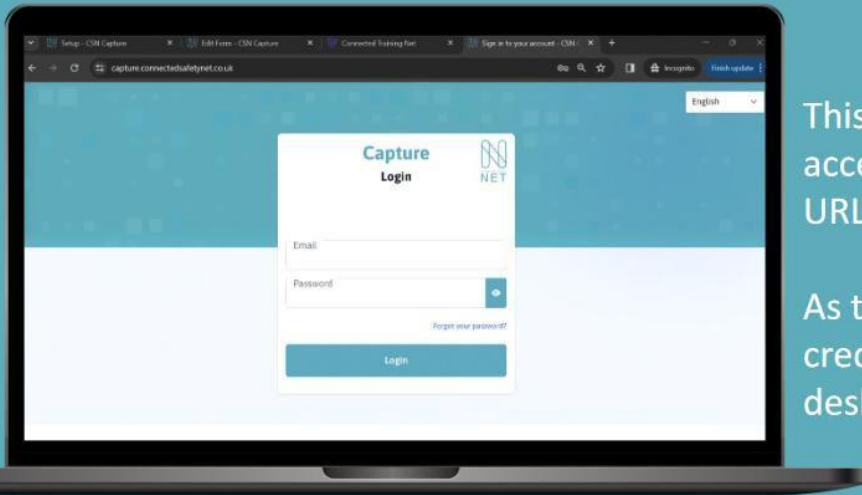
When all the component forms are completed using answer options, a tick mark validates the completion.

Tap the **Submit** button to save the **Ad-Hoc Form**. The status now turns to 'Submitted'

The **Ad-Hoc Form** maintains the status as 'In Progress' while the user keeps adding the information.



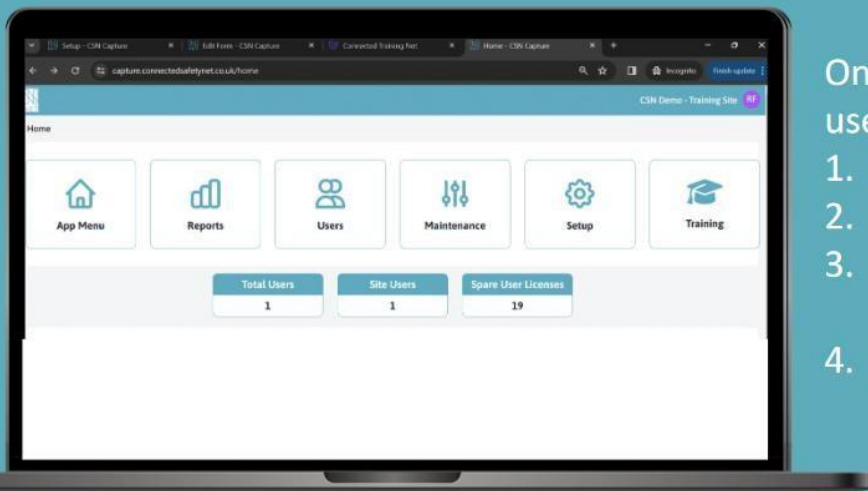
Access the CSN Capture Web Portal



This the Capture web portal, you can access it on the following URL: capture.connectedsafetynet.co.uk

As the page loads, enter the CSN credentials to use the CSN Capture on desktop.

CSN Capture Desktop – Main Page



On the Capture web portal, you can use the following features:

1. View forms on "App Menu"
2. View reports on "Reports" tab
3. Manage team and users on "Users" tab
4. Redirect to the training portal using "Training" tab

Understand & Differentiate Between Audit Pack & Forms

Standalone Form/Form
Icon in Capture Desktop




Daily Vehicle Check
Forms
FRM00133

Last Completed: 04 Apr 2024 @ 19:43
By: Sahish Munir

1: Click 'App Menu' to navigate to listed audit packs.

In Capture Desktop, standalone form is termed as a Form.

In Capture Desktop, Ad-Hoc Form is termed as Packs.

2: Click the desired icon/form to proceed.

Ad-Hoc Form/Packs in
Capture Desktop




General Work Permit Certificate
Packs

Create A New Pack/Form

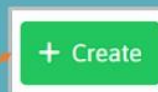
Select Statuses

Select many statuses

☐ Open
☐ Submitted
☐ Closed
☐ In Progress

Status filter in Ad-Hoc
Form/Packs

Status filter in Standalone
Form/Form

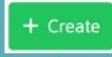


4 of 4 Statuses Selected

☒ Open
☒ Submitted
☒ In Progress
☒ Closed

Closed
10 May 2024 (09:05)
Open
13 Apr 2024 (10:01)

Use the filter dropdown to refine on previously performed audit pack results.

Click  to launch a new audit pack or form.

App Menu

Home / App Menu / General Work Permit Certificate


General Work Permit Certificate



Select Statuses

Select many statuses

☐ Open
☐ Submitted
☐ Closed
☐ In Progress

027 3643 Staff

In Progress

Pass R

028 3644 Staff

In Progress

Pass R

027 36209 Staff

Submitted

Test

028 3746 Contractor

Submitted

Test

028 3563 Staff

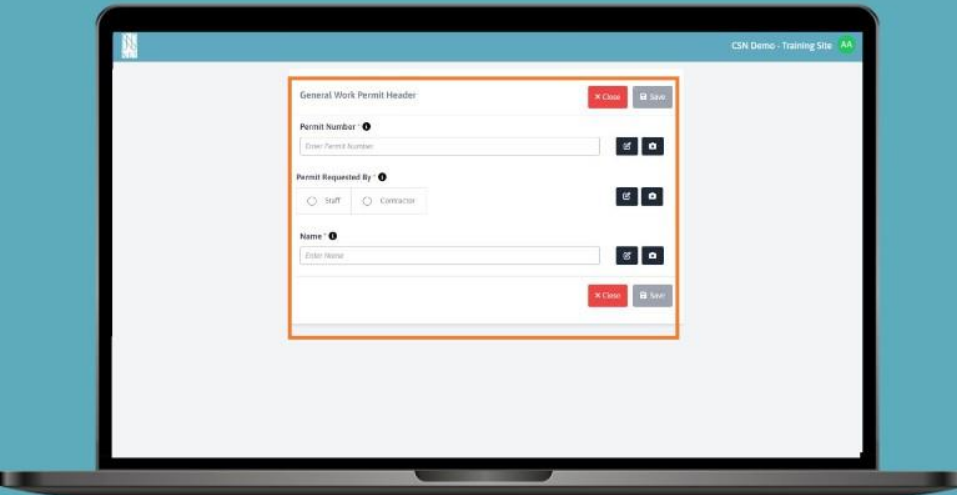
In Progress

Pass R

Create A New Form Using Capture Desktop

From the form's opening page, start selecting the appropriate answers against each question using a combination of dropdown, radio buttons, or enter information in the text box.

- Click  against each question to launch zoomed view.
- To add a comment with an answer click  icon.
- To upload an image/video click  icon.

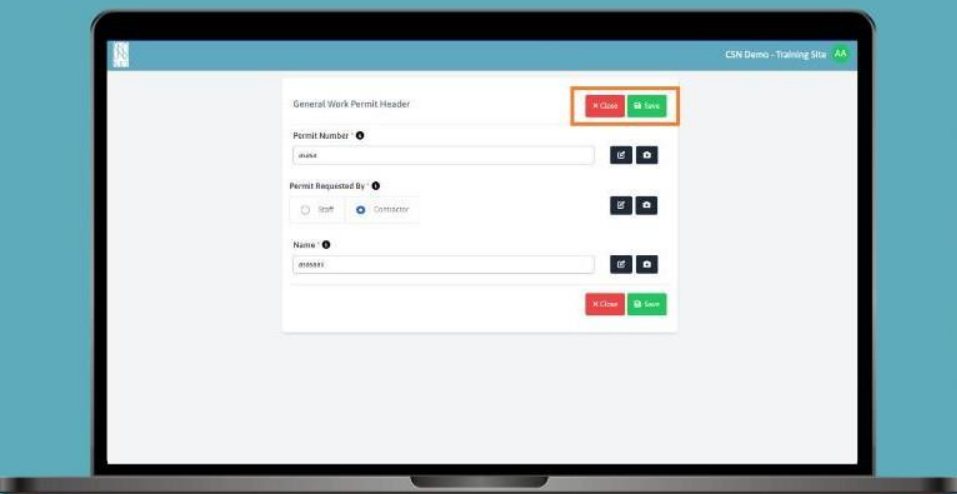


Save the Form Using Capture Desktop

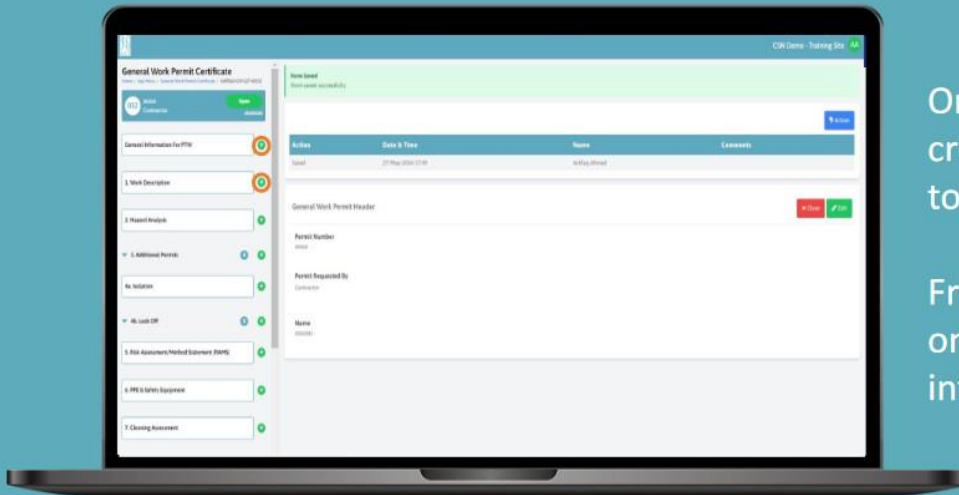
After submitting all the answers on the form:

Click  to save the form.

Click  to go back to form's creation page.



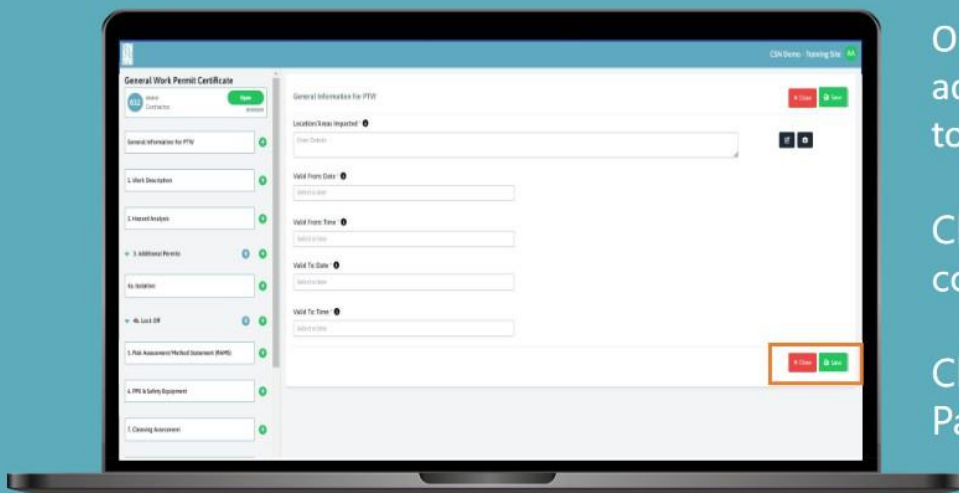
Access Audit Pack Component Forms



Once a new Audit Pack has been created, proceed to add information to component forms.

From the relevant Audit Pack page, on the left side panel click  to add information to component forms.

Save A Form Using Capture Desktop

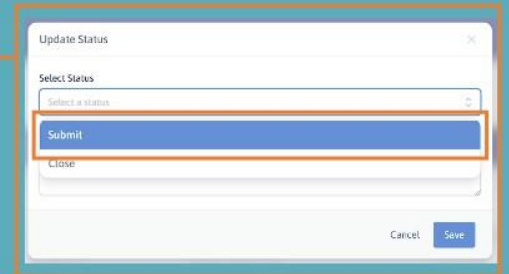
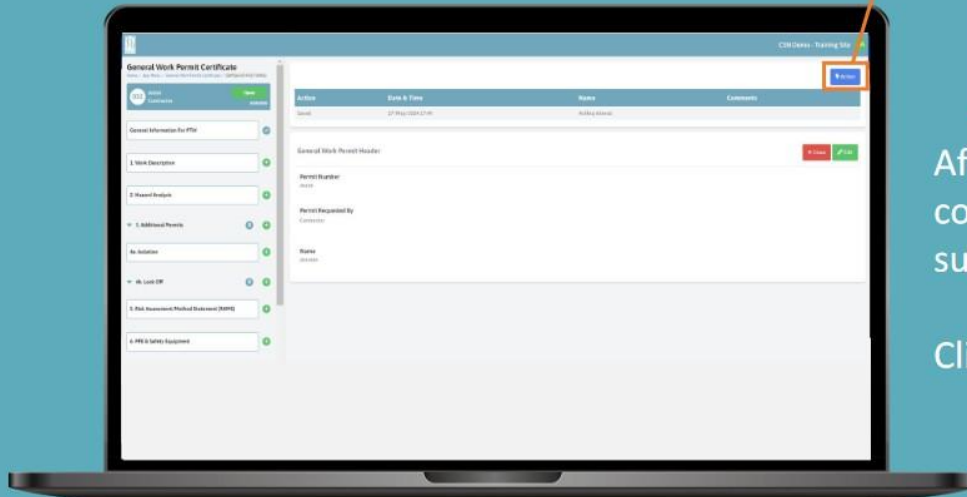


Once all the information has been added to component forms proceed to save the form.

Click  to save the component form.

Click  to go back to Audit Pack opening page.

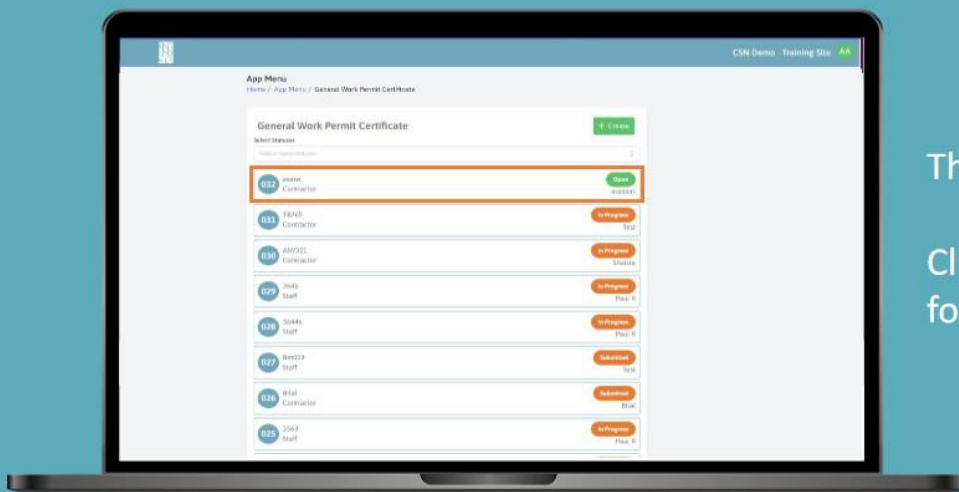
Save A Pack Using Capture Desktop



After submitting the information in component forms, click **Action** to submit or close the audit pack.

Clicking **Submit** saves the audit pack.

View/Edit Submitted Form Using Capture Desktop



The form is now submitted.

Click to view or edit the submitted form.

CSN Infrastructure Context

To make the CSN Infrastructure more resilient, the following actions have been implemented.

- Utilising Azure Front Door and WAF for security and resilience
- Create multiple instances of the web front end (node.js) and bring each under a load balancer
- In the backend, to mitigate any data loss due to corruption or crashes, Azure's database backup and restore procedures are being used, and an additional replica instance has been created.

MySQL Database Backup and Restore

For Backup and Restore procedures, default Azure facilities have been used which are as following:

- Full backups occur once every week.
- Differential backups occur twice a day.
- Transaction log backups occur every five minutes.
- The first full snapshot backup is scheduled immediately after a server is created.
- That first full snapshot backup is retained as the server's base backup. Subsequent snapshot backups
- are differential backups only.
- Differential snapshot backups occur at least once a day. Differential snapshot backups do not occur on a fixed schedule.
- Transaction log backups occur every five minutes.
- Backup retention period is 7 days.

Azure Monitor (Capacity Utilization)

The five capacity utilization charts shown on the page are:

- CPU Utilization % - shows the top five machines with the highest average processor utilization
- Available Memory - shows the top five machines with the lowest average amount of available memory
- Logical Disk Space Used % - shows the top five machines with the highest average disk space used % across all disk volumes
- Bytes Sent Rate - shows the top five machines with highest average of bytes sent
- Bytes Receive Rate - shows the top five machines with highest average of bytes received

Alerts set up on the Azure Monitor

The following alerts are set up on the Azure Monitor for the VM's- cs-load-vm1 and cs-loadvm2

- START Alert- Whenever the VM is started it will give out the alert. This enables us to get mail when the system gets started.
- Restart Alert- Whenever the VM is restarted it will give out the alert. This enables us to get mail when the system gets started.
- PowerOff Alert- Whenever the VM gets switched off we will receive a mail.
- DISK IOPS Alert- Whenever the Disk IOPS is greater than the max (here 90%) we will receive a mail so that we can identify whenever there would be performance issues due to disk input output operations.

Monitoring using Logic Apps

To address extreme scenarios such as VM Crashes or abrupt shutdowns Azure Logic App is being used to constantly monitor the virtual machines for down time scenarios and send appropriate alert messages to the concerned individuals.

Using the control flow of a Logic App we can determine when the web server on the VM is experiencing downtime and send an email when the conditions are met.

Database Backup and Restore

Azure Database for MySQL automatically creates server backups and stores them in user configured locally redundant storage in the case of CSN. Backups can be used to restore your server to a point-in-time. Backups can be used to restore your server to a point-in-time.

These backups can only be used for restore operations in Azure Database for MySQL. You can use MySQL dump to copy a database.

Backup type and frequency

Full backups occur once every week. Differential backups occur twice a day. Transaction log backups occur every five minutes. The first full snapshot backup is scheduled immediately after a server is created. That first full snapshot backup is retained as the server's base backup. Subsequent snapshot backups are differential backups only.

Differential snapshot backups occur at least once a day. Differential snapshot backups do not occur on a fixed schedule.

Transaction log backups occur every five minutes.

Backup retention

Backups are retained based on the backup retention period setting on the server. You can select a retention period of 7 to 35 days. For CSN, we have selected the default retention period, which is 7 days.

Backup storage cost

Azure Database for MySQL provides up to 100% of your provisioned server storage as backup storage at no additional cost

Restore

In Azure Database for MySQL, performing a restore creates a new server from the original server's backups and restores all databases contained in the server.

Point-in-time restore is available with either backup redundancy option and creates a new server in the same region as your original server utilizing the combination of full and transaction log backups.

Deleted servers can be restored only within five days of deletion after which the backups are deleted. The database backup can be accessed and restored only from the Azure subscription hosting the server. To restore a dropped server, refer documented steps. To protect server resources, post deployment, from accidental deletion or unexpected changes, administrators can leverage management locks.

Independent of your backup redundancy option, you can perform a restore to any point in time within your backup retention period. A new server is created in the same Azure region as the original server. It is created with the original server's configuration for the pricing tier, compute generation, number of vCores, storage size, backup retention period, and backup redundancy option.

Database Replicas

The read replica feature allows you to replicate data from an Azure Database for MySQL server to a read-only server. Replicas are new servers that you manage similar to regular Azure Database for MySQL servers. For each read replica, you're billed for the provisioned compute in vCores and storage in GB/ month.

The read replica feature helps to improve the performance and scale of read-intensive workloads. Read workloads can be isolated to the replicas, while write workloads can be directed to the master.

If a source server has no existing replica servers, the source will first restart to prepare itself for replication.

When you start the create replica workflow, a blank Azure Database for MySQL server is created. The new server is filled with the data that was on the source server. The creation time depends on the amount of data on the source and the time since the last weekly full backup. The time can range from a few minutes to several hours. The replica server is always created in the same resource group and same subscription as the source server. If you want to create a replica server to a different resource group or different subscription, you can move the replica server after creation.

Every replica is enabled for storage auto-grow. The auto-grow feature allows the replica to keep up with the data replicated to it, and prevent an interruption in replication caused by out-of-storage errors.

In a regular scenario a read replica is unavailable for application-based transactions, however, if the database instance to which the replica belongs is removed, the read replica itself becomes available and can then be used as a regular database instance.

Azure Monitoring

Azure Monitor for VMs monitors the performance and health of your virtual machines and virtual machine scale sets, including their running processes and dependencies on other resources. It can help deliver predictable performance and availability of vital applications by identifying performance bottlenecks and network issues and can also help you understand whether an issue is related to other dependencies.

Azure Monitor for VMs stores its data in Azure Monitor Logs, which allows it to deliver powerful aggregation and filtering and to analyze data trends over time. You can view this data in a single VM from the virtual machine directly, or you can use Azure Monitor to deliver an aggregated view of multiple VMs.

Client onboarding is a critical process for CSN to ensure that new clients have a smooth and successful transition into using our software.

1. CSN follows this client onboarding process:
2. Introduction and Welcome
3. Gather Information
4. Training and Education
5. Customization and Configuration
6. Data Migration (if applicable)
7. Testing and Feedback
8. Go-Live
9. Client Support
10. Follow-Up and Review
11. Documentation and Resources
12. Account Management

By following these steps, CSN ensures a successful onboarding experience for our clients, setting them up for long-term satisfaction and success with our software and services

Clients can request the data extraction, and we extract the data for them.

Clients also have the ability to use the reporting feature in the desktop version to extract the data themselves without assistance.

In case of client offboarding the default procedure that we would follow at the end of a contract (if it's not renewed):

- 1) All the data is extracted, sent and removed.
- 2) All of the users are removed from our systems.
- 3) We ensure that all customizations and assets are removed as per client request.
- 4) Any files held in our storage are deleted. However (at the client request), we can hold onto any data that they would want us to hold temporarily e.g. 12 months.

Support scripts are followed for the most common incidents. Users report incidents via the standard support channels (email, phone, web chat).

Service Constraints

While our products offer robust functionalities, it's important to note some constraints. These may include planned maintenance arrangements to ensure system integrity and security. The application must also be deployed on the Azure cloud environment.

Service Levels

On receiving a support request through email or a support-ticket on the support portal, the support coordinator will take following immediate actions:

- Creation of ticket in our support tool if a call received or any other scenario if the ticket has not been created, with relevant information, documents, priority and support level.

We provide 3 support levels:

Level-I No code change is required. Eg, password reset.

Level-II Code changes or server configuration required. Eg. Crashes and sever performance issue.

Level-III Cross functional knowledge and coordination is required along with programming skills.

The ticket type Incidents comes under this level if they are not resolved by the level II support. Service Requests with all urgencies/priorities come under this level. All these tickets are managed by mainstream teams in their regular releases. All levels are included with our default service support package. We provide both an account manager and a named support engineer for all our customers as the main contact.

After sales support

The support team is then responsible for managing post production customer support. The support team uses a support portal (Jira) to manage the life cycle of support tickets. Case Types Ticket Status Ticket Priority/Urgency Support Level-I Support Level-II Support Level-III We provide incidents reports from our support portal on demand.

For Live clients, the response time is strictly a 2-hour window on business days. Phone support is also available from 9 to 5 (UK time), Monday to Friday

Technical requirements

Following are the technical requirements to access CSN Incidents:

- Hosting: Microsoft Azure Cloud
- iOS or Android (Mobile app)
- Modern web browser (Web portal)

Outage and maintenance management

We report service outages via email alerts. Our support desk will also be in direct contact with customers if it is a serious outage.

Hosting options and locations

CSN clients typically join the multi-tenanted CSN Azure infrastructure managed by the CSN team, as the economies of scale realized through this approach, along with the benefit that the whole system and hosting is supported by a single team, generally make this a preferred option for clients.

This multiclient infrastructure is tightly controlled by the CSN team from a security perspective, with access being granted to Azure only when this is strictly necessary for the execution of a team members duties. However, if required the system can be deployed onto a customer specific MS Azure account for each customer, and it is expected that if this approach is chosen, the customer IT team will own their respective account and hold the Azure 'Owner' privileges.

On this basis it will be the responsibility of the customer IT team to manage user access to the infrastructure in alignment with their own security policies. When this approach is followed, the CSN team will require 'Contributor' access to each customer MS Azure account to deploy, maintain and support each instance of the system.

CSN team user accounts that are granted access to customer MS Azure accounts will be kept to a select few who justifiably need access to deliver their activities on behalf of CSN and the customers of CSN.

Where possible the CSN team will comply with the customer security policies around management of user accounts and will also consider industry best practice.

Access to data (upon exit)

Clients can request the data extraction, and we extract the data for them. Clients also have the ability to use the reporting feature in the desktop version to extract the data themselves without assistance.

This is the default procedure that we would follow at the end of a contract (if it's not renewed):

- 1) All the data is extracted, sent and removed.
- 2) All of the users are removed from our systems.
- 3) We ensure that all customizations and assets are removed as per client request.
- 4) Any files held in our storage are deleted. However (at the client request), we can hold onto any data that they would want us to hold temporarily e.g. 12 months.

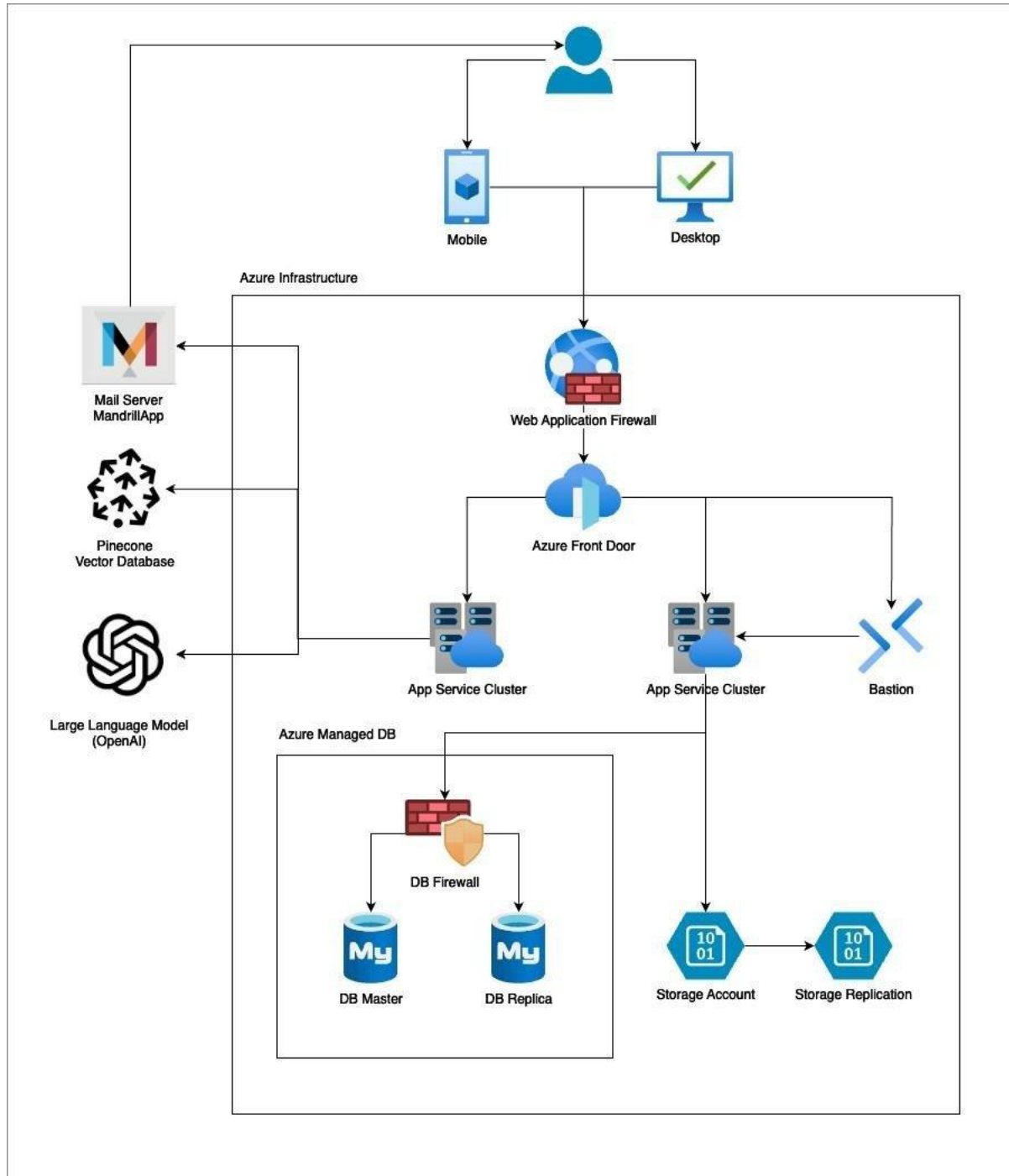
Security

This section is intended to provide an overview of the security measures taken when designing and developing the Connected Safety Net software product (CSN). It will also outline the systems approach to user authentication and management of user access, both to the system itself, and to the infrastructure on which it is hosted.

Finally, it will also cover the approach taken to ensuring protection of sensitive data in accordance with prevalent data protection legislation. For any follow up queries relating to the CSN product and how it is secured, please contact the CSN management who will be happy to assist.

Security Architecture

The security architecture has been designed to deliver defense in depth and is described in the below architecture diagram with accompanying bullet point descriptions.



The system is designed to be hosted on Microsoft Azure infrastructure; a deliberate choice taken to leverage the best practice security principles in place across the Azure cloud hosting stack.

- All components of the application and database layers of the system are secured behind a standard firewall.
- Internal communication between services, virtual machines and databases is conducted via encrypted API.
- External communication through the firewall to the user interface layer components is conducted via encrypted API secured using Auth tokens.
- An external 3rd party industry standard service, Auth0, is used for creation and destruction of client auth tokens.
- The web application is secured with SSL certification and https protocol.
- The mobile application utilizes React Native coding language and all data held within the app wrapper is encrypted at rest.
- Where pictures and videos are taken using the Apps feature set, these files are deleted from the device gallery as soon as they have been successfully transmitted through the API.
- There is an additional VNet security firewall within MS Azure to add a further layer of defense for production databases.
- MS Azure Key Vault is used for holding secrets that enable secure CI/CD via GitHub Actions

Vulnerability Assessment

Regular penetration testing of the application and the infrastructure is a key part of CSN's security approach. This testing is targeted to be conducted at least annually and will also be planned in on an ad-hoc basis following a major development release.

The testing identifies vulnerabilities of the system to the latest threats and gives the development team the guidance on where to focus security improvement activities. Generally, High and Medium level vulnerabilities will be addressed as soon as possible with a fix and release, while Low and Informational level vulnerabilities will be added to the product backlog to be addressed through the product development lifecycle when time and resources allow.

The latest penetration test was conducted on the December 2024 by Crowe Advisory Services. The overall risk rating for both Mobile App and Web Portal components of the platform was Low, with 3x Low risk vulnerabilities being identified on the Mobile App, and 2x Low risk vulnerabilities being identified on the Web Portal. The full penetration testing report will be available from the CSN management team.

The penetration test for 2025 is currently underway and will be completed soon.

Infrastructure Access Management

CSN clients typically join the multi-tenanted CSN Azure infrastructure managed by the CSN team, as the economies of scale realized through this approach, along with the benefit that the whole system and hosting is supported by a single team, generally make this a preferred option for clients. This multiclient infrastructure is tightly controlled by the CSN team from a security perspective, with access being granted to Azure only when this is strictly necessary for the execution of a team members duties.

However, if required the system can be deployed onto a customer specific MS Azure account for each customer, and it is expected that if this approach is chosen, the customer IT team will own their respective account and hold the Azure 'Owner' privileges. On this basis it will be the responsibility of the customer IT team to manage user access to the infrastructure in alignment with their own security policies.

When this approach is followed, the CSN team will require 'Contributor' access to each customer MS Azure account to deploy, maintain and support each instance of the system. CSN team user accounts that are granted access to customer MS Azure accounts will be kept to a select few who justifiably need access to deliver their activities on behalf of CSN and the customers of CSN. Where possible the CSN team will comply with the customer security policies around management of user accounts and will also consider industry best practice.



Contact us now!

☎ +44 20 8059 2758

✉ info@connectedsafetynet.co.uk

🌐 connectedsafetynet.co.uk