Touch Cloud Application Quick Setup Guide for Sagem COSY Phone

Richard Dickety

March 15, 2011

Table of Contents

1 Introduction

Touch is designed to be user friendly... we hope that you will be able to log on to the application, work your way around, and get yourself up and running without too much help. Have a play with it... don't worry you can't break it!

But if you are stuck this guide is designed to walk you through the main elements of functionality within the system, namely...

- **Setting up users**. To include mobile users, managers and customers;
- **Logging on to the mobile application;**
- **Activating tags**. This must be done in order to swipe tags and therefore prove attendance;
- **Setting up check-points.** Attendance can be proven without doing this, but managers will not be able to use action lists, location based messaging, shift management etc without live checkpoints;
- **Assigning tags to check points.** Once checkpoints are created within the system, you must assign tags to them to enable action lists, location based messaging, shift management etc;
- **Setting up shifts.** This will enable you to monitor shift activity. Master this and you should be selling premium SLA's to your customers, and **charging** a premium;
- **Sending messages to mobile users** directly, or via check-points. This means that you can prove to your customers that messages have been sent, received, and read... with timed reports;
- **Giving your customers' access** to reports. If you are selling premium SLA's, chances are customers will expect to be able to see in real-time that you are delivering;
- **Setting up alerts.** You or your colleagues will automatically be sent an e-mail or SMS when check-points are not swiped within defined time parameters ;
- **Sending incident reports** from the phone to the cloud application;
- **Setting up instructions** of actions to be completed at specific checkpoints;
- **Viewing and filtering reports**.

2 Using the Cloud Application for the First Time

2.1 Introduction

Being a security solution, we have implemented certain measures to ensure that only authorised persons will have access to your account. We want you to know that we treat your confidentiality seriously.

2.2 Setting Up Your Account

Before doing anything, you must first set up an account password. After setting up the password, any changes or queries that you wish to make regarding your account will be answered only once you or one of your colleagues has quoted your unique password. Customer services will not allow either your name or your company name to be used as your account password.

In order to set up your account password please call MoCo Customer Services on...

0800 62 11 11.

Once your password has been set up, MoCo will create an account for you on the Touch system, and will give you a manager username and password. When you have your log-in details, please go to...

www.mocotouch.com

... and log onto the application using this username and password.

2.3 Setting Up Mobile Users

In order to start using the system to monitor patrols and prove attendance, you will need to set up some users. At this stage, it is most important that you set up at least one mobile user, so that some tags can be set up and assigned.

There are 4 kinds of users[1] within the system...

- **Mobile Users** – who can only log on to the mobile phone application;
- **Managers** – who can log on to the cloud (web)-based application, and the mobile phone based application. These users can set up and delete users and all elements of functionality within the system;
- **Supervisors** – who can log on to the cloud based application only, and will only be able to view the system without changing or updating anything;

[1] As many users, of any kind, can be set up on the cloud application as you wish

- **Customers** – who can log on the cloud based application only, and will only be able to view reports, and moreover only the reports of check-points that have been allocated to them by Managers.

To set up some users...

1. Click on “Logins” in the toolbar at the top, and then select “Users” from the menu on the left.

2. Go to the bottom of the page, and select “Add a new user”.

This will bring up a new screen where you need to enter your users’ information, to include at least a unique username and password. The email address is not mandatory and does not need to be unique.

The username and password will be the details the user will need to use to gain access to both the phone application and/or the cloud (web)-based application, dependent on what type of user you are setting up (see Introduction).

Make sure the start date of the user account is the day before the current day; otherwise they will not be able to log on until the following day. There is no need to enter an end-date, but you may wish to do this especially for customer access if you are making them pay for access to their reports. This gives you the opportunity to switch off their access at the end of any agreed contract period. Also do not forget to mark the user as “Active”.

DON’T FORGET TO CLICK “SAVE”, AND...

You must now assign the user to a group, which will be one of the four groups shown above. The user will not be able to log on to anything unless they have been assigned to a group.

3 Using the Phone for the First Time

3.1 Introduction

Please note that this guide in intended for users of the Sagem COSY Phone. If you are using any other phone please download an alternative guide from our web-site or call MoCo Customer Services on 0800 62 11 11.

Now that you have set up some users on the system, including at least some mobile users, you are in a position to get people to log onto the phone application. This means that they can set up tags (if required), or if you have manually set up tags through the cloud application (see section 4.2), then they can just start doing their rounds whilst proving their attendance.

3.2 Logging on to the Phone

Switch the phone on by holding down the on/off button located on the very top of the phone above the screen.

Select the "Menu" soft key, which will present four icons on the screen. Select the bottom icon ("Advanced"). A whole screen of icons will appear, by selecting the icon in the middle of the bottom row ("Entertainment") then Java will start. When Java has opened select "Applications", after which "Touch" will appear on the screen. By selecting Touch, the application will open.

The end user will then be presented with a log-in screen, where they will need to enter their log-in details as allocated to them by a manager when setting up mobile users (see section 2.3**Error! Reference source not found.**).

When the phone says "Touch is listening" and the Touch logo is displayed, the end user has successfully logged onto the application. If you have the cloud application open and are at the "Home" screen, click refresh (normally F5), and you will be able to see at the bottom of the page that this user has just logged in.

If the end user enters the wrong details then they will be informed and given the opportunity to re-enter their details.

3.3 Swiping Tags

It should be remembered that the RFID reader is located towards the centre of the battery compartment on the back of the phone. RFID tags are most successfully swiped if the end-user holds the phone with their palm facing towards the phone screen, and gently lowers the phone battery cover at the back of the phone against the RFID tag, in the middle. When successfully swiped, the phone will beep and vibrate.

4 Activating Tags

4.1 Introduction

Once some mobile users have been set up within the system, you are now in a position to get those mobile users to go around and set up some tags.

If you already have tags set up on sites, and you have a note of the RFID numbers, then it is possible to manually enter those numbers into the system to activate the tags. However, the system has been set up to enable end-users to assign tags by simply swiping them and assigning a short-name. The main benefits of this are that managers and mobile users never need to be exposed to lengthy RFID identifying numbers, also end-users can carry on with their rounds immediately after activating a tag, in order to prove their attendance. The tags can then subsequently be allocated to checkpoints at a later stage.

Both methods of activation will be dealt in this guide.

4.2 Manual Activation of Tags through Cloud Application

Select the "Assets" tab, and then select "Tags" from the menu on the left or the main screen.

At the bottom of the page, you will have the option to "Add a new tag". Select this option.

A short-name can then be given to the tag, along with the unique RFID identifier of the tag you are setting up, if known. If not, skip this section and go straight to section 4.3.

Once the tag has been given a name and the RFID number entered, click save, and the tag will be active on the system. The tag can now be allocated to a check-point (see section 6), or if swiped the activity will be recorded under the "Activity" report within the cloud application.

4.3 Automatic Activation of Tags by Mobile Users through Mobile Phone

Once logged onto the mobile phone application, the end user should select "Menu" by pushing the right-hand blue short-cut key at the top of the numeric key-pad.

From this menu the mobile user should select "Activate Tag". This will bring up a new screen where the end-user can allocate a short-name to the tag. At this stage it is only necessary to give a short-name, such that a manager on the cloud application can easily identify the site and specific location of the tag to be assigned. Once a short name has been entered, the tag should be scanned (as described in section 3.3). The phone will say...

"Tag scanned – press Activate to proceed".

By clicking "Activate", the tag is registered on the cloud application, and the following message appears...

"Tag activated thank you".

The mobile user can now swipe this tag and this activity will be reported within the "Activity" report on the cloud application. Therefore the mobile user can immediately start to prove their attendance, before a manager is able to assign tags to check-points.

Please note however that the tag must be scanned in addition to the initial activation for swipes to appear in the "Activity" or "Proof-of-attendance" reports.

5 Checkpoints

5.1 Introduction

A checkpoint is exactly what it says... it is a place within a site that will have a tag fixed to a wall or another convenient point, and by swiping the tag you can prove that a person has been there.

You can set up tags, and swipe them, without associating them with check-points in the system... and this would still show up in the activity report. But if you do this you would not be able to associate the tags with sites, customers or addresses. Nor would you be able to do more complicated things like make them part of shifts, or set up action lists or alerts associated with the check point.

5.2 How to set up a Checkpoint

1. Click on “Assets” in the toolbar at the top, and then select “Checkpoints” from the menu on the left.
2. Go to the bottom of the page, and select “Add a new checkpoint”.

This will bring up a new screen where you need to enter...

- A new unique name of the check-point;
- A site name. This is a drop down menu where you can associate the check-point with sites already set up, or alternatively you can enter a new site name by clicking on the “Add New” icon;
- At least the first line of the address of the check-point. At this point...

DON’T FORGET TO CLICK “SAVE”

6 Assigning Tags to Check-points

6.1 Introduction

There are 2 ways that tags can be associated with checkpoints. This can either be done via the check-points themselves or via reports.

The system has been designed so that mobile users can go out, position and assign tags, and still be able to swipe the unassigned tags and prove their attendance on the system. Managers can then go into the system afterwards, and associate tags with the required checkpoints.

6.2 Assigning Tags via the Checkpoint Screen

Once a checkpoint has been saved (see section 5.2), you will see the word “Tag” appears below the checkpoint details. If you are not in this screen already select “Assets” then “Checkpoints”, and click the “Edit Checkpoint” icon of the required check-point.

By clicking on the yellow tag icon underneath the check-point information, this will bring up all of the unassigned tags within the system in a new window. Simply select the green tag icon to the right of the required tag, and that tag will now be associated with the checkpoint.

You will see the tag name appear within the checkpoint details.

6.3 Assigning Tags via the Reports Screen

As long as a tag has been swiped at least once in addition to the actual set-up of the tag via the phone, then activity will appear in the “Activity”, or “Unassigned Activity” report.

Select “Reports” and then click on either the “Activity”, or “Unassigned Activity” report. The report will show “Unassigned Tag: [NAME OF TAG]” within the report, and there will be 1, 2 or 3 icons to the right of all of the report activities (dependent on how many modules of the system you have allocated to you). Click the location icon situated next to any of the report activities of the required tag, and this will bring up all checkpoints that do not currently have a tag associated with them. Select the green tag icon next to the required checkpoint and the tag will now be associated with that checkpoint.

You will notice that all of the report activities of the previously unassigned tag will now show the name of the selected checkpoint.

7 Rostering

7.1 Introduction

In order to aid your compliance to BS7499, this module will allow you to define when guards need to arrive and leave your sites, and will alert you if no-one has turned up within 10 minutes of the beginning of their shift. It will also alert you if no-one has clocked out within 10 minutes of the end of the defined shift.

It should be stated that this functionality at this stage does not contain full rostering capability; its sole intention is to enable guarding companies to set up shifts and assign those shifts to a sites, thereby enabling you to monitor log-in and log-out activity at your sites.

7.2 Setting Up Rosters

Select "Rosters" from underneath the "Actions" tab.

Select "Add a New Roster" at the bottom of the page. You will be asked to give the Roster a name, which logically will probably be the name of the site to which you wish to allocate shifts. Once you have given the Roster a name, then a graphic will appear on the screen showing any shifts allocated to that site.

Above that graphic is a box where the sites being allocated to a roster should be selected. Sites will only be shown if a tag has been allocated to the site. Tags are allocated in exactly the same way as allocating a tag to a checkpoint. Please see section 6.

Once the site(s) have been selected to be part of the roster, then the start and end times of the shifts within the roster need to entered.

To do this, click on the "Add a new shift to this roster" button at the bottom of the page. Then add the start and end times of the shifts for each day that is applicable.

7.3 Starting and Ending Shifts

The tag that has been allocated to the sites associated with the roster will now need to be swiped within 10 minutes of the start of each shift allocated to the roster, in order to show that a guard is present on-site.

Similarly, the tag will need to be swiped again a maximum of 10 minutes after the end of each shift to show that the guard has left site.

If neither of the above happens then an on-screen alarm will be raised, and an entry will be added to the "Alarms" report. The person that is logged onto the system that acknowledges the alarm will be acknowledged within the alarms report as the person that dismissed it. MoCo recommends that a procedure should be put in place that needs to be followed once any alarm is acknowledged.

8 Check-Call Management

8.1 Introduction

According to BS7499, all guards must call into your control room and let you know that they are OK, at least every hour. Each and every call must be recorded for audit purposes.

Touch now enables you to send a message to your guards, asking if they are OK, at regular intervals of at least 30 minutes, but not more than 60 minutes. This is in order to comply with BS7499.

8.2 Setting Up Check-Call Management

Check call management of a guard is activated by the guard when they swipe the site tag of a site that has been selected as being "check-call managed".

So by going to "Sites" under Assets, and by editing a site, if the "Check-Call Managed" button is checked, then the guard will automatically be sent a message to enter a pin every X minutes, where X is the number defined by a supervisor under "My Company Details" under the home tab. Please ensure that a number between 30 and 60 minutes is entered.

A supervisor will also need to define a duress PIN to be entered if the guard is in danger and a normal PIN if the guard is OK. The duress PIN for the whole customer environment is defined under "My Company Details" under the home tab. The normal PIN to be entered if the guard is OK is allocated to each individual guard under the individual user details under "Assets".

8.3 Responding to Check-Calls

The guard will simply be asked by the phone to enter a PIN after the time interval set by you or your supervisor. If they are OK they should enter their normal PIN, if not, the duress PIN.

If a duress PIN is entered, the pop-up alarm will be entered requiring someone to acknowledge the alarm and then implement a process to ensure that the guard's welfare is checked.

The same thing will happen if the check-call is not responded to within 15 minutes.

9 Patrol Management and Premium SLA's

9.1 Introduction

The patrol management module is designed to enable you and your supervisors to monitor patrols while they are happening, and to produce compliance reports to demonstrate adherence to agreed customer service level agreements (SLA's).

It enables multiple sites and check-points to be selected quickly and easily, and associated with patrol and tagging patterns. Patrol activity can then be monitored from a single screen, or your adherence to the set patterns and SLA's can be proven and reported quickly and easily after the patrol has been completed.

So for example, if you had a customer that wanted particular check points to be swiped every 30 minutes, with a 10 minute leeway, this shift pattern can quickly be set up and monitored for multiple sites and checkpoints. More importantly, a non-compliance report can be produced after the patrol, so that your adherence to the promised SLA can be **proven**.

MoCo strongly suggests that you should charge a premium for such SLA's dependent on their stringency.

9.2 Setting up Patrols

A manager of the cloud application needs to select the "Actions" tab, followed by "Patrols" from the menu on the left.

You will be presented with a list of any shifts that have already been set up within the system. In order to set up a new shift, the "Add a new patrol" icon at the bottom of the page should be selected.

This will bring up a new screen, where the following information must be entered...

- Name of the patrol;
- Extra information (for example site ID number, customer ID number etc);
- The start and end dates of the patrol pattern (if the patrol is starting on the current day make sure that the previous day is selected as a start date);
- Alarm if missed check-box. This will activate on-screen alarms in addition to the real-time-monitoring report if a check-point is missed, and any missed check-points will be added to the "Alarms" report;
- The sites and check-points to be checked. All sites and check-points will be shown here, you just need to select the appropriate ones by ticking the check-boxes;
- The days (select tick boxes) and start times of the shift, along with the tagging interval of the check points. Then the variance allowed, in other words the leeway you will grant the end-

user either side of the selected time to swipe the tag before a box turns red. There must be a variance of at least 5 minutes, plus or minus[2].

DON'T FORGET TO CLICK "SAVE"

9.3 Real-time Monitoring

Once you have set up one or more shifts, click on the "Reports" tab at the top, and then select "Real-time Monitoring" from the menu on the left.

You will be presented with a screen which is designed for you, or a supervisor, to monitor shift activity in real-time. Across the top of the report you will see the time of day, and down the left hand side you will see the names of the shifts that are currently "within-scope".

"Within scope" simply means that shifts will only show within this report when they are currently active. In a nutshell, this means that if you set up a shift that includes activity only on a Wednesday from 9 'til 5pm, if you viewed the report on a Tuesday then no reference would be made on the report to that shift. So it would just not show up.

When a shift is in scope, the activity relating to the shift is divided up into 5 minute blocks. This is because the variance setting within the system is managed in 5 minute blocks, as a minimum. So if the shift was set up such that a check-point was set to be swiped every hour with a 5 minute variance, this would mean that the check-point would need to be tagged somewhere between 5 to, and 5 past the hour.

The report would deal with this by showing two coloured blocks on the row for that checkpoint, under every hour. The blocks are colour coded as follows...

- Blue – the checkpoint is currently due to be tagged;
- Red – the checkpoint was not tagged at the specified required time;
- Green – if the block is showing green before the checkpoint is due to be tagged, then this just means that this swipe activity is out of scope. In time it will turn blue, obviously at the point at which it becomes due;
- Green – if the block is showing green after the checkpoint was due to be tagged, this means that the checkpoint was successfully tagged at the required time.

The report automatically refreshes every 5 minutes, but a refresh can be forced by pushing the F5 button within your web-browser. This means that the report can be viewed, or monitored, for example on a large screen or a projector, by an individual or a number of people.

If a check-point that is due to be swiped is missed it will immediately turn from blue to red, and the person that is currently assigned to that shift can be contacted to find out what has gone wrong.

[2] The minimum swipe interval that can be entered is 15 minutes, with a 5 minute plus or minus variance.

9.4 Non-Compliance Report

This report is designed to give you a clear view, and also a downloadable Excel report, of any tagging activity that not happened within the time parameters set within “Shifts”.

There are 2 separate reports under this tab.

Scan Windows Without Scans

This will show any shifts, and the check-points associated with those shifts, that were not tagged within the set shift patterns. The report also makes clear which “window” of required activity was missed.

Scans Outside Scan Windows

This report shows any shifts, and the check-points associated with those shifts, where the check-points have been tagged but tagged outside of the required activity “window”

10 Messaging

10.1 Introduction

The messaging function within Touch serves several purposes, but perhaps the most important point to note is that if the Touch application is used to send a message rather than an SMS...

- It is completely **free**;
- You can prove when the message was **sent** via a standard report;
- You can prove when the message was **received** by the mobile user via a standard report;
- You can prove when the message was **read** by the mobile user via a standard report**.**

Moreover, if you needed to send a message to a mobile user within an area with variable mobile phone signal, the message will be delivered as soon as signal is obtained, as long as...

1. the message was sent via a check-point (see following section), and;
2. the checkpoint was swiped by the end user.

If the message is sent directly to the end-user, the phone checks for messages automatically every 15 minutes. If the phone is out of signal at that point, then it will check again in another 15 minutes.

10.2 Via a Checkpoint

To send a message via a “check-point”...

1. Click on “Assets” in the toolbar at the top, and then select “Checkpoints” from the menu on the left;

2. Select the checkpoint that you wish the message to be associated with, and click the edit icon. The checkpoint information screen will open;

3. In the message box on the right, type the message that you wish to be sent. Do not forget to click “Save”.

The message will be received by all and any users that swipe this check-point, as soon as they swipe. If the mobile is out of a signal area, the message will be delivered and the end-user will be made aware as soon as they have signal after the tag was swiped.

As soon as you delete the message from the check-point message box, the message will no longer be sent. Do not forget to click “Save” when you do this.

10.3 Directly to Mobile Users

To send a message directly to an end-user...

1. Click on “Actions” in the toolbar at the top, and then select “Messages” from the menu on the left.

2. Go to the bottom of the page, and select “Add a new message”.

This will bring up a new screen where you simply need to enter the message text, and the user to whom you wish you send it. The end-user will receive the message within the next 15 minutes. When it is delivered, the system will record the time of delivery, also the time that it was read.

11 Customer Access

11.1 Introduction

Touch is geared towards enabling you to deliver a higher level of service to your customers than they may have previously experienced. MoCo believes that the final piece in terms of delivering this experience is to allow your customers the ability to monitor you and your staff's activity themselves at any time of day, via a web-browser.

You may also choose to mention to your customers that all reporting activity is stored on a cloud based server hosted by Microsoft Azure. See appendix 16.1 for more information about this service, but in short it is highly secure, data is backed up on a daily basis and all information held is completely tamper-proof. Touch is therefore a completely secure source of information about the activity of you and your staff, which you can supply to your customers in real-time.

Note that your customers will only have to access to reports, and will only be able to view sites and check-points to which you grant them access.

11.2 Setting Up a Username and Password for Your Customers

The initial stage of granting your customers' access to Touch is to set them up on the system as a user. Please refer to section 2.3**Error! Reference source not found.** for how to do this, making sure that at the final stage the user group that they are assigned to is "Customer".

Once you have completed section 11.3 simply supply the username and password that you have set up, tell them to log on to www.mocotouch.com, and they will have instant access to all checkpoints assigned to them.

11.3 Granting Your Customers Rights to View Their Sites and Check-points

Each check-point must individually be assigned to a customer, in order that they can view only the activity reports for their sites and check-points.

To do this, click on the "Assets" tab and then click through to "Checkpoints". This will bring up a list of all of the check-points within the system.

In order to assign a check point to your customer, you will need to edit the checkpoint. On the right of each record, you will see an "Edit Checkpoint" icon, click through and it will bring up the whole checkpoint record. Once opened, at the bottom of the page you will see "No Customer Assigned", with a person icon next to it. Click on this icon, and it will open a new window containing a list of names of any user in the system that is set up as a customer.

By clicking on the icon to the right of a customer record, that customer will be assigned to that checkpoint. When your customer then logs in to the system, they will be able to see only the proof of attendance reports relating to checkpoints you have assigned to them.

12 Alerts

12.1 Introduction

The alerts module is designed to proactively inform you if a required checkpoint has been missed. It will instantly send an email or SMS as soon as a tag is not swiped within parameters set by a manager.

You can set up the system to alert any email address or any mobile phone by SMS.

12.2 Setting up Alerts

Select the "Actions" tab, and then select "Alerts" from the menu on the left. A list of any alerts set up within the system will be in front of you.

At the bottom of the screen select "Add a new alert" and a new screen will open where the following information must be entered...

- Name of the alert;
- Description. We advise just a quick explanation of what the alert is going to do for your own reference;
- The start and end dates of the alert (if the alert is starting on the current day make sure that the previous day is selected as a start date);
- The time that the check point needs to be swiped, with an allowance (if required);
- Assignment. This is where you define which checkpoint the alert relates to, and whether it only applies to a single, or all users;
- Alert method. This is where you define whether the alert is sent via SMS or email (or both), and which email address and/or mobile the SMS is to be sent to. The text that is to be contained within the alert should also be entered at this point;
- Repetition. Finally you need to specify which days of the week the alert is to be active on.

DON'T FORGET TO CLICK "SAVE"

If the check point is not swiped at the specified time, taking any allowance into consideration, then the system will alert you via your chosen method.

13 Incident Reports

13.1 Introduction

At any stage whilst going around swiping tags, it may be important for a mobile user to record an incident, or unusual activity, on the cloud application. This module enables the end-user to do exactly that, by taking a photograph, adding text to it, and if required (although this is completely optional) associating the incident with a checkpoint.

This functionality comes installed on the phone, and no set-up is required on the cloud application. Any incidents can be viewed under the "Reports" tab.

13.2 Sending an Incident Report

The mobile phone user needs to select menu from the application main screen, and to select "Incident Report".

This will open up a new screen, with the option to "Take a picture". By pushing the "Camera" option, this will open up the camera and the mobile user can take a photo of whatever it is that they need to report. They will be asked if they wish the application to use the camera, they need to respond "Yes". The photo taken will populate the form on the screen.

If the mobile user wishes to associate the incident with a checkpoint, they should now swipe the appropriate tag. The form now says "Tag scanned, thank you".

By selecting "OK" on the left "soft-key", this will bring up a blank form where the end user can enter as much text as they wish which will be associated with the incident.

By pressing "OK" the incident is sent back to the cloud application, where it can be viewed under the "Reports" tab, and "Incident Reports".

An on-screen alarm will also be raised on-screen as soon as the incident report is received.

14 Action Lists

14.1 Introduction

Action lists enable managers of the system to set up a very specific list of instructions, which will need to be completed every time a mobile user swipes a tag at a checkpoint. The action list can also be made specific to individual mobile users.

All questions and instructions are of course written and defined by managers of the system within the cloud application. There are 4 categories of instruction, namely...

1. To get a mobile user to respond to a question with a simple yes or no response;
2. To get a mobile user to respond to a question in free-form text;
3. To require the mobile user to send back a photograph;
4. To require the mobile user to make a phone call to a number defined by a manager within the cloud application (potentially their office number or even an ARC).

14.2 Setting up Action Lists

Select “Actions” from the tabs at the top, then “Action Lists” from the menu on the left.

A list of any action lists previously set up will appear on the page in front of you. To set up a new action list, go to the bottom of the page and select “Add a new Action List”.

First of all, you need to give the action list a name, and select the checkpoints (or all checkpoints) and mobile users (or all users) that you wish the action list to be applicable to. At this stage...

DON’T FORGET TO CLICK “SAVE”

You will now be offered a new list of “Action Items”. There will at this stage be no action items, so you will need to select “Add a new action item”. This will bring up a new window, where you need to enter in the prompt that the mobile user will be asked, what kind of response you require from the drop-down menu (see section 14.1 above for “categories of instruction”), any extra information if required, and the tick-box as to whether the response is mandatory or not.

Note that if you require the mobile user to make a phone call, then the extra information field needs to be populated with the phone number to be called. As many action items can be added to an action list as you wish.

Note that if the questions need to be presented to the end-user in a particular order, then the green up and down arrows to the right of the action items will move them up and down.

14.3 Responding to Action Lists

As soon as a check-point with an action list associated with it is tagged, the mobile user will be informed by the phone that there are action list items to be completed, and that they should select the menu, then “Action Lists” to view the commands or questions being asked.

On going into action lists, the user will be presented with a list of any incomplete action lists. They are labelled by the checkpoint to which they have been assigned. It should be pointed out that no action lists should be left incomplete within the phone, as this will impact the phone memory and can lead to the application mal-functioning. Exiting and re-opening the application should alleviate any problems.

Once the relevant action list has been selected, the mobile user will be presented with a clear form to be completed. They can scroll up and down using the cursor key on the phone, and their position within the form will be shown by a scroll bar on the right. Any photos taken will be shown within the form, and a red phone will turn to a green tick once a required phone call has been made.

If the mobile user does not complete a mandatory question they will be reminded to do so, and will not be allowed to send the form until they have.

When they have completed the form the “OK” blue soft-key button should be selected, and the mobile user will be informed that the form has been sent.

If for any reason the action list still shows within the list, you should advise the mobile user to go into the action list again and complete the form again. If it still does not disappear ask the mobile user to exit the Touch application and log-in again.

15 Viewing and Filtering Reports

15.1 Introduction

This is where managers and customers can view all activity associated with your or their checkpoints and sites.

The reporting suite is fairly self-explanatory and requires little explanation, by simply clicking and selecting the various types of reports it can be seen what can be viewed and what the various filtering options are.

Please note also that any report can be filtered and the results exported to an Excel spreadsheet. Simply go the bottom of the report page where you will see the export to Excel option.

15.2 Reports and Filtering Options

When you or your customer logs into the reports section of the module from your web-browser, you will see the following reports...

Activity

A report showing any and all "swipe" activity recorded on the system, including tags that have not been associated with checkpoints. Can be filtered by date and mobile user.

Alarms

A report showing any and all alarms that have been raised within the system, along with the names of people that have dismissed the alarms. For example duress calls, or missed check-calls, clock on/off to site activity and patrol scans.

Check-Call Management

A report listing anybody that is currently clocked onto a site and is currently being managed by the check-call functionality of the system.

Clock-in/out

A report filtered to only show activity from tags that are associated with people. In other words, clock-in, clock-out activity. Can be filtered by date and any user of the system.

Log-ins

A quick way of viewing when any mobile user has logged into the mobile phone application. Can be filtered by date and user.

Proof-of-attendance

A report filtered to show any “swipe” activity from tags that are associated with “checkpoints”. In other words, any clock-in or out activity, or swipes against unassigned tags or assets would not be shown in here. Can be further filtered down by user, site or check-point.

If there are action list responses associated with “swipes” in this report, they can be viewed by clicking a link which brings up a new screen containing only the responses from that check-point. Photographs and calls made can be viewed from here.

Action-list Responses

A report filtered to show only responses to any action lists that have been set up by managers. Photographs taken and records of phone calls made from action lists will be immediately accessible in here.

Asset Control

This module is currently disabled within the system.

A report filtered to show any “swipe” activity against assets that have been associated with tags will be shown in here. So any keys that have been tagged in or out by mobile users, or for example any address information gleaned from those keys, will be shown in this report. Can be further filtered down by user; checkpoint; site or location.

Real-time Monitoring

Offers the ability to view and monitor any activity that has been associated with particular shifts. As soon as checkpoints are missed they go red on the moving, timed schedule graphic, and the guard can be immediately contacted. Pending actions are shown as blue and completed actions are shown in green.

Only shifts that are “in-scope” are automatically shown.

Unassigned Activity

Filters any activity associated with tags that have not yet been assigned to “checkpoints”, people or assets. Can be further filtered by date and mobile user.

16 Appendices

16.1 Microsoft SQL Azure Secure Hosting

SQL Azure Database is a cloud database service from Microsoft. SQL Azure provides web-facing database functionality as a utility service. Cloud-based database solutions such as SQL Azure can provide many benefits, including rapid provisioning, cost-effective scalability, high availability, and reduced management overhead.

SQL Azure is a key component of the Microsoft data platform offering flexibility and scalability; reliability and security; and developer agility. Let's begin by looking at some of these features.

Key Features

SQL Azure Database offers the high availability and functionality of an enterprise data centre without the administrative overhead that is associated with an on-premise solution. This self-managing capability enables organizations to provision data services for applications throughout the enterprise without adding to the support burden of the central IT department or distracting technology-savvy employees from their core tasks to maintain a departmental database application.

Low-Friction Provisioning

When you use the traditional on-premise data infrastructure, the time that it takes to deploy and secure servers, network components, and software can slow your ability to prototype or roll out new data-driven solutions. However, by using a cloud based solution such as SQL Azure, you can provision your data-storage needs in minutes and respond rapidly to changes in demand. This reduces the initial costs of data services by enabling you to provision only what you need, secure in the knowledge that you can easily extend your cloud-based data storage if required at a future time.

High Availability

SQL Azure is built on robust and proven Windows Server® and SQL Server technologies, and is flexible enough to cope with any variations in usage and load. The service replicates multiple redundant copies of your data to multiple physical servers to ensure data availability and business continuity. In the case of a disaster, SQL Azure provides automatic failover to ensure maximum availability for your application.

Published service level agreements (SLAs) guarantee a business-ready service. When you move to SQL Azure, you no longer need to back up, store, and protect data yourself.

Scalability

A key advantage of the cloud computing model is the ease with which you can scale your solution. Using SQL Azure, you can create solutions that meet your scalability requirements, whether your application is a small departmental application or the next global Web success story.

Global Scalability

A pay-as-you-grow pricing model allows you to quickly provision new databases as needed or scale down the services without the financial costs associated with unused capacity. With a database scale out strategy your application can utilize the processing power of hundreds of servers and store terabytes of data.

SQL Azure runs in worldwide data centres, so you can reach new markets immediately. If you want to target a specific region, you can deploy your database at the closest data centre. You can harness this global scalability to build the next generation of Internet-scale applications that have worldwide reach, but without the infrastructure costs and management overhead.

Multi-Tenant Support

Independent software vendors (ISVs) who develop Software+Services (S+S) offerings must provide adequate isolation for individual customers' data. ISV's must be able to charge each customer the right price for the data storage services that they have consumed. SQL Azure provides the flexibility that ISVs need to segregate customer data and implement multi-tenant billing, which enables you to build a global S+S solution quickly and easily.

Developer Empowerment

One of the potential obstacles to building great cloud-based applications is the requirement for developers to learn new tools, programming platforms, and data models. However, SQL Azure is built on top of the TSQL language and is designed to be compatible with SQL Server with a few changes, so developers can use their existing knowledge and skills. This reduces the cost and time that is usually associated with creating a cloud-based application.

Familiar Client Development Model

When developers create on-premise applications that use SQL Server as a data store, they employ client libraries that use the Tabular Data Stream (TDS) protocol to communicate between client and server. There is a large global community of developers who are familiar with SQL Server and have experience of using one of the many client access libraries that are available for SQL Server, such as Microsoft ADO.NET, Open Database Connectivity (ODBC), JDBC and the SQL Server driver for PHP. SQL Azure provides the same TDS interface as SQL Server, so developers can use the same tools and libraries to build client applications for data that is in the cloud.

Proven Relational Data Model

SQL Azure data is stored in a way that is very familiar to developers and administrators who use SQL Server. You can create a SQL Azure Server which is a group of databases that are spread across multiple physical machines. This SQL Azure Server is in some ways conceptually analogous to a SQL Server instance and acts as an authorization boundary just as in SQL Server. You can also set geo-location at this level. Windows® Azure™ and SQL Azure data centres are located worldwide; if your application is relevant to a specific region, you can increase performance by geo-locating it there.

Within each server, you can create multiple databases that have tables, views, stored procedures, indices, and other familiar database objects. This data model ensures that your database developers can use their existing relational database design and Transact-SQL programming skills, and easily migrate existing on-premise database applications to the cloud.

SQL Azure servers and databases are logical concepts that do not correspond to physical servers and databases. This abstraction enables the flexible provisioning that was described earlier in this paper. Administrators and developers can concentrate on data model design because SDS insulates them from the physical implementation and management.

Synchronization and Support for Offline Scenarios

SQL Azure is part of the rich Microsoft data platform which integrates with the Microsoft Sync Framework to support occasionally connected synchronization scenarios. For example, by using SQL Azure and the Sync Framework, on-premise applications and client devices can synchronize with each other via a common data hub in the cloud.