TZ Networked Day Lockers Admin Guide

Document Number	**101691-030**
Document Classification	**Public**
Distribution	**General**
Revision	**E**
Date	**23 February 2023**

TZ. Intelligent Control

Contents

1. Preliminaries

1.1 Disclaimer

This Guide is intended to assist customers with the use of their TZ Networked Day Locker System.

Customers acknowledge that these guidelines are not intended to be an exhaustive statement of all relevant user information.

While TZ Limited (TZ) has used all due care and skill to ensure that the information contained in this document is accurate, correct, and current at the time of publication, it does not warrant or represent that the information is free from errors or omissions and does not accept responsibility for any error, omission, or defect in the information.

1.2 Purpose of Document

This document provides a User Guide for the TZ Networked Day Locker System. Accordingly, this document presents the basic information required to reasonably understand how to use the System as an Administrator.

Notwithstanding the above, this document is not intended to be an exhaustive statement of all relevant data. If any additional information should be required, please contact your local Sales Representative.

1.3 Important Notes

This document should be used by competent professional personnel with the knowledge, experience, and authorisation to administer the TZ Networked Day Locker System.

The contents of this document may be updated from time to time and therefore please ensure that you are using the current edition of the guide.

2. Introduction

This Admin Guide provides information on the usage of the TZ Networked Day Locker System, from the perspective of an Admin.

This document is a Guide for Admins only. There are separate Guides for Users and Concierges.

There are two major components to the TZ Networked Day Locker System:

- The Locker Banks themselves, which comprise columns of Lockers, with a touch screen and primary scanner at a central area, and secondary scanners at various other locations. Locker Banks are typically located in multiple places of an Organisation, grouped into Neighbourhoods. Users can reserve Lockers, then access them by scanning their card or entering their PIN

- A web-based Portal, where Permanent Staff can login and manage their Locker Reservations or change their PIN

There are four types of people who interact with the System:

- Permanent Staff – employees based in a Neighbourhood who can have exclusive use of a Locker within the same Neighbourhood

1. Visitors – these may be employees from other Neighbourhoods, or external visitors. Visitors can temporarily reserve a Locker

- Concierges – these are Permanent staff members who also have management privileges. They can:
  - Manage Reservations on behalf of other Users
  - Manage Shared Lockers
  - Add or Edit Users
  - View Reports
  - Open any Locker at a Locker Bank

- Remove the contents of a Locker and end its Reservation

2. Admins – these are special Users who can change the configuration of the System

Where this document refers to Users*, it is specifically referring to* Permanent Staff *and* Visitors.

There are five types of Locker Reservation supported by the System:

- Permanent - these are created/managed/cancelled only by a Concierge

3. Flexible - these are created and managed by an employee, and they don't expire.

- Visitor - these reservations have an Expiry Date and are intended for temporary use by transient employees or external visitors.

4. Shared - these are shared Lockers with an Expiry Date.

- Single Use – these are short term Reservations that can be used only once, i.e. for storage while using a gym

Permanent Staff are restricted to at most one Permanent/Flexible, one Visitor and one Single Use Reservation in the System at any time. Permanent Staff can have multiple shared reservations.

3. The Role of the Admin

Admins are staff who are responsible for configuration of the TZ Networked Day Lockers system. They can:

- Edit Locker Bank details and settings
- Manage Users
- Bulk upload Users, and optionally pre-allocate Lockers to Users
- Setup Neighbourhoods, Concierges, or other Admins
- Manage settings such as email settings, templates, and distribution lists
- An alert is sent to Admin by email if a Locker forced open (unauthorised/ unexpected). This is also added to system event report.

All the above configuration is accomplished through the Admin Portal, as described in Section 4.

Admins are NOT involved with day-to-day activities within the TZ Networked Day Locker System. This is the responsibility of the Concierges.

Note that responsibility for the setup and maintenance of the Locker Banks or the System itself is with the TZ installation and maintenance team, who also have Admin privileges.

Note that there are some configuration tasks that are outside the scope of the Admin Portal. These include:

- Adding Locker Banks to the System
- Configuring the Lockers available at a Locker Bank

Any changes in these areas can only be performed by a member of the TZ installation and maintenance team.

4. Using the Admin Portal

The Admin Portal is designed to be accessed from anywhere within a defined network via a web browser. Prior to first use, TZ staff will setup the Admin Portal and any Admin accounts.

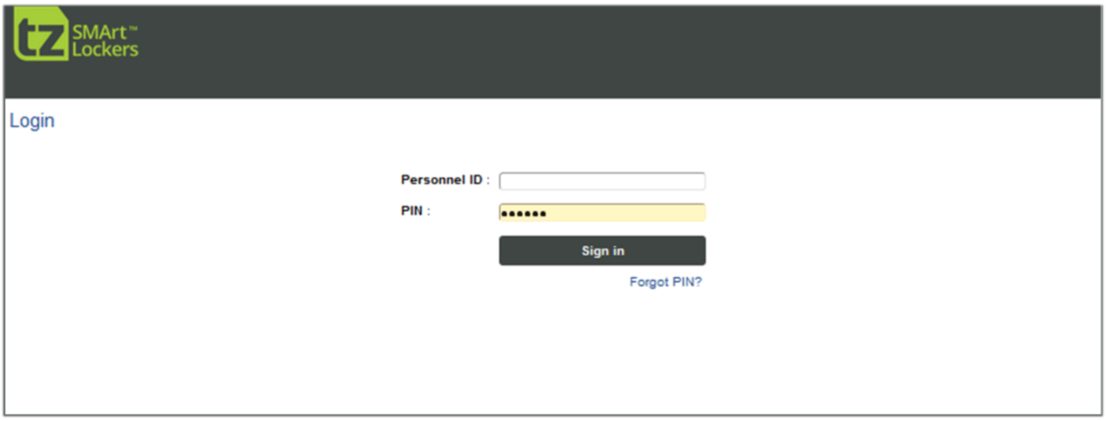


Figure 1: Login Screen

Note that the Employee Self-Service Portal is a web-based application. Please be aware that the browser experience may vary across different browsers. For best results, please always use the latest version of Chrome or Firefox only.

To login, enter the Personnel ID and PIN of an Admin (or if AD authentication is enabled, enter the AD username and AD password of an Admin) then press the *Sign in* button.

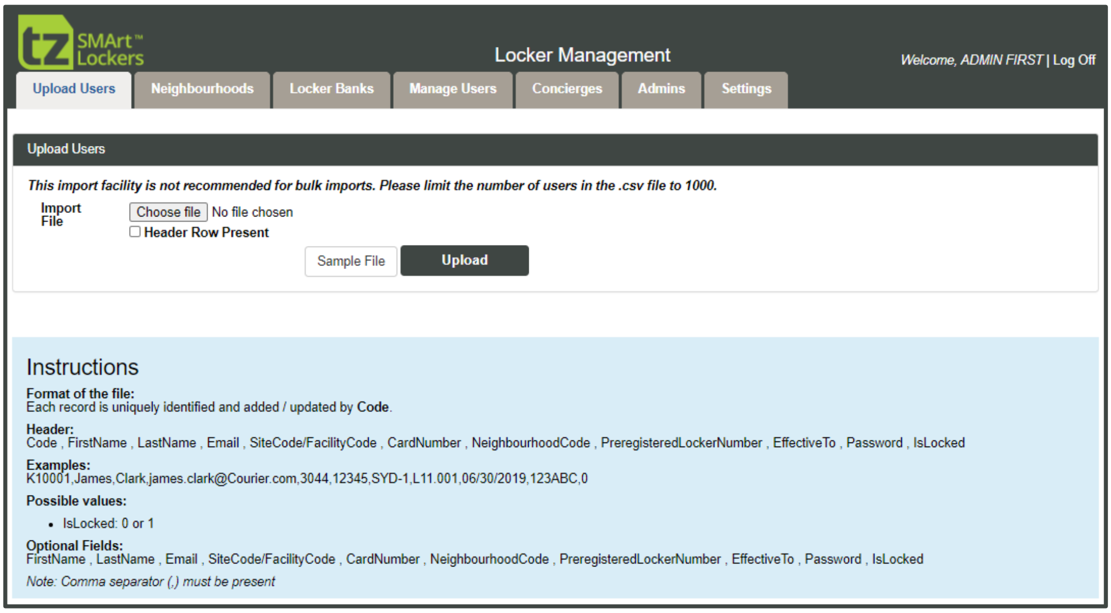
Unlike other Users, it is not possible to have an Admin account PIN reset via the Forgot PIN? link below the Sign In button. If you have forgotten the Admin PIN, please contact a member of the TZ installation and maintenance team..

Upon successful login with Admin credentials, the first tab of the Admin Portal will be presented.

The following subsections describe the capabilities of each tab.

4.1 The Upload Users tab

The Upload Users tab allows Users to be bulk imported from a .csv (comma separated values) file. These Users can optionally have Lockers pre-allocated to them if their Neighbourhood is specified. Only Users who have a Neighbourhood specified can have Lockers pre-allocated.



This import facility is not recommended for bulk imports. Please limit the number of users in the .csv file to 1000.

Import File: Choose file No file chosen

□ Header Row Present

Instructions

Format of the file:
Each record is uniquely identified and added / updated by **Code**.

Header:
Code , FirstName , LastName , Email , SiteCode/FacilityCode , CardNumber , NeighbourhoodCode , PreregisteredLockerNumber , EffectiveTo , Password , IsLocked

Examples:
K10001,James,Clark,james.clark@Courier.com,3044,12345,SYD-1,L11.001,06/30/2019,123ABC,0

Possible values:

- IsLocked: 0 or 1

Optional Fields:
FirstName , LastName , Email , SiteCode/FacilityCode , CardNumber , NeighbourhoodCode , PreregisteredLockerNumber , EffectiveTo , Password , IsLocked

Note: Comma separator (,) must be present

Figure 2: Upload Users screen

A sample upload .csv file can be obtained by pressing the *Sample File* button.

The fields that can be included in the .csv file are:

FIELD	DESCRIPTION
Personnel ID	The User's unique employee number
First Name	The User's first name (optional)
Last Name	The User's last name (optional)
Email	The User's email address (and where the User's PIN will be sent following upload) (optional)
Site Code	The Site Code for the User's card (use 0 where USB card readers are used) (optional)
Card Number	The User's card number (optional)
Neighbourhood	The Neighbourhood of the User (if left blank, then the User will be a visitor) (optional)
Locker Number	Use this field to pre-allocate a Locker (must match Locker numbering format used during initial Locker Bank commissioning) (optional)
Termination Date	The last employment date of the User (in format YYYY-MM-DD) (optional)

PIN	If specified, this must conform to the specified password regex (refer Section 4.7.8) and any other password security features that have been enabled, such as can't use common passwords or reuse recent passwords. Where this field is left blank, it defaults to equal the card number, or if no card number is provided, a random 6-digit number will be generated (optional)
IsLocked	0 indicates not locked,1 is locked (terminated) (optional)

For the optional fields, commas must still be included to delimit the fields. An example of a .csv file is:

- 1001363,John,Smith,js@tz.net
- 1001364,Mary,Lee,mary@tz.net,,,ADL,,2015-06-30
- 1001365,Bob,Dobson,bd@tz.net,64560,33333,PAR,D08.001,
- 1001366,Jane,Mah,jane@tz.net,64560,44444,PAR,D08.002,2015-09-30,123456

Don't use Microsoft Excel to work with .csv files. Use a text editor such as Notepad, as Excel will often change the format of the file automatically in ways that stop the Upload function working correctly.

Prior to upload, please ensure that the email system has already been setup and an email template for User creation has been configured which includes all desired details, such as the Locker number, PIN and URL for the Employee Portal.

Prior to upload, please ensure that all the Locker Banks are online, to avoid Users trying to access their pre-allocated Lockers before the Locker Bank has been updated (Locker reservations made offline only take effect once the Locker Bank comes online)

When ready to Upload:

- Press the *Choose file* button and browse to the desired .csv file
- Optionally tick *Header Row Present* if such initial row exists in your csv file
- Press the *Upload* button

If there is a formatting problem with the .csv file, a message will be displayed stating that the Uploaded File is not in the correct format and the whole file will be rejected. Check the file and correct as necessary before trying again.

If successful, the file contents will be processed immediately. Account creation emails will be sent to new Users to inform them of their PIN. An email will also be sent to the address configured for Import Data notifications on the User Import Settings screen, that reports the results of the import such as how many succeeded and failed.

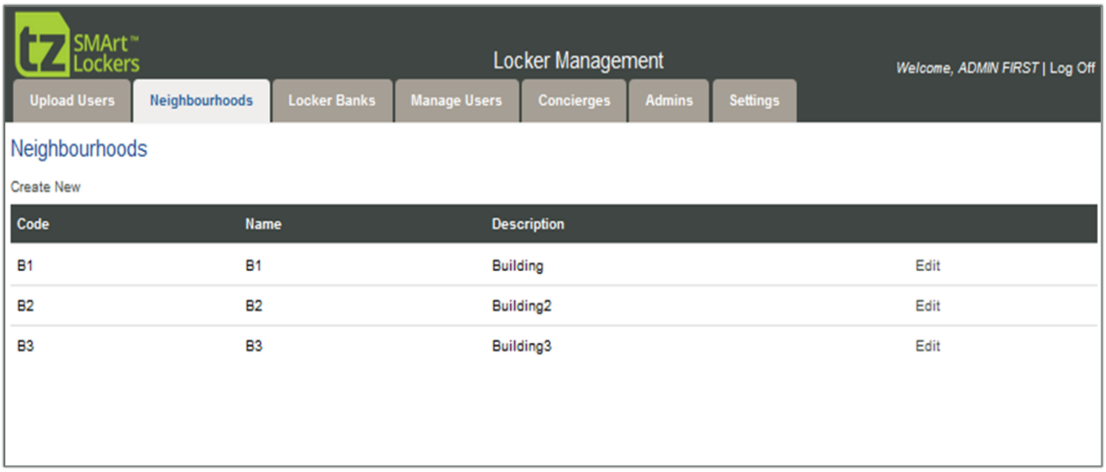
If a Personnel ID already exists in the System, then the User details will be overwritten with those from the .csv file. If a Locker is pre-allocated, then the Reservation for any previous Locker will be converted to a Visitor Reservation.

4.2 The Neighbourhoods tab

This tab lists the Neighbourhoods available to the System. Locker Banks and Concierges are associated to Neighbourhoods.

To create a new Neighbourhood, click the *Create New* link at the top left of the screen. To edit the details for a Neighbourhood, select the *Edit* link in the rightmost column for that Neighbourhood.

When Azure AD integration is enabled, there will also be an *Advanced* link visible for each Neighbourhood.



Neighbourhoods

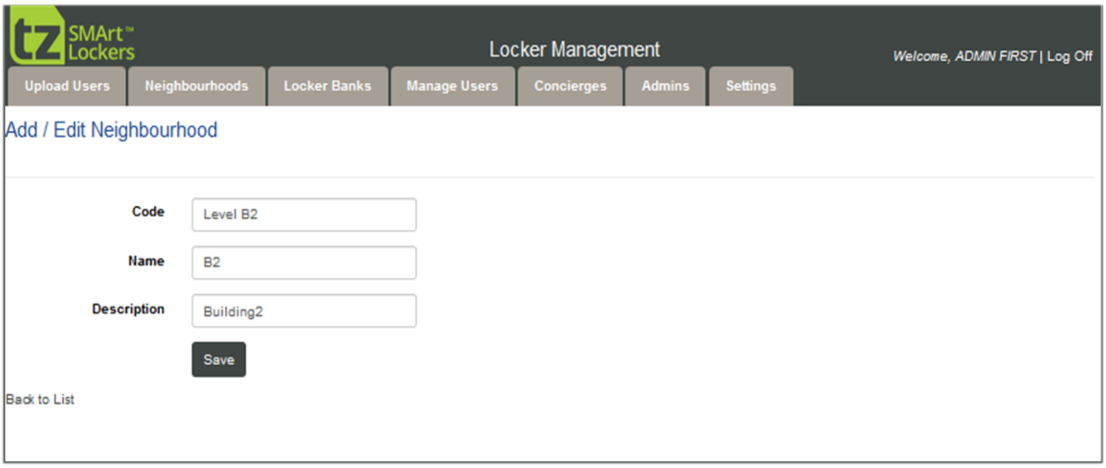
Create New

Code	Name	Description	
B1	B1	Building	Edit
B2	B2	Building2	Edit
B3	B3	Building3	Edit

Figure 3: The Neighbourhoods screen

4.2.1 Add / Edit Neighbourhood

This screen allows adding/editing of code, name and description fields with a Save button. The code is used internally and displayed where space is a premium, otherwise the name is used instead to refer to the Neighbourhood. The description is not used outside this screen.



Add / Edit Neighbourhood

Code: Level B2

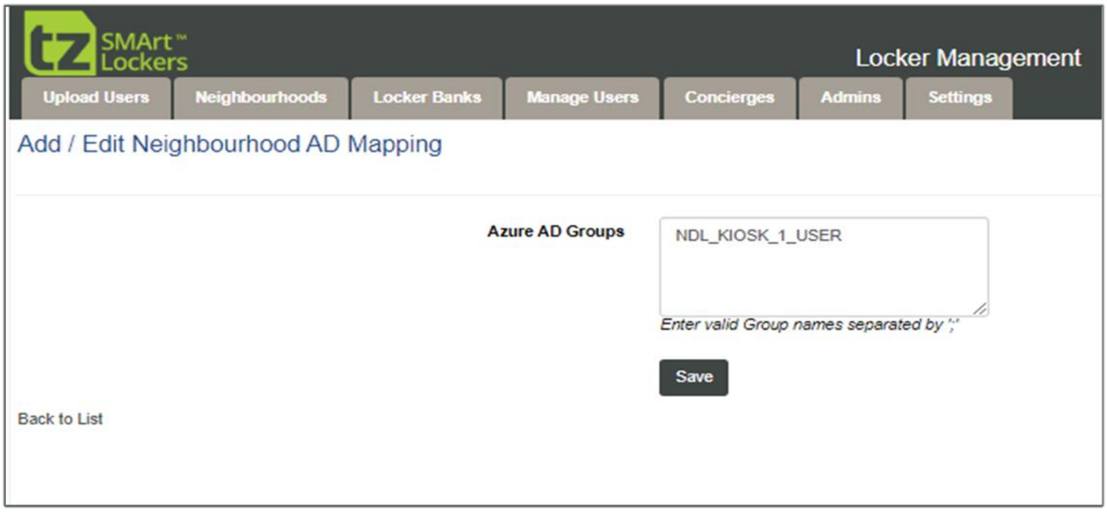
Name: B2

Description: Building2

Figure 4: Add/ Edit Neighbourhood screen

4.2.2 Add/ Edit Neighbourhood AD mapping

If you have enabled Azure AD integration, then selecting the *Advanced* link for a Neighbourhood will display the following screen:



Add / Edit Neighbourhood AD Mapping

Azure AD Groups: NDL_KIOSK_1_USER

Enter valid Group names separated by ';'

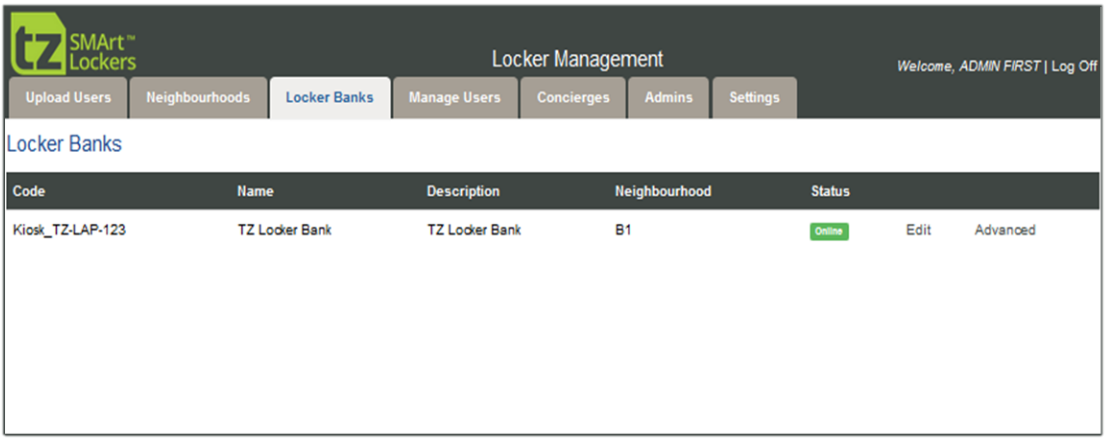
Figure 5: Add/ Edit Neighbourhood AD mapping screen

This screen allows you to define the Azure AD group to Neighbourhood mapping. As Users are pushed or pulled from Azure, they will be assigned to the Neighbourhood corresponding to their Azure group mapping.

As Users are assigned to one Neighbourhood only within the System, this means they must similarly also belong to one Azure AD group only too.

4.3 The Locker Banks tab

This tab lists the Locker Banks available to the System. Locker Banks are added to this list when they are first setup by a member of the TZ installation and maintenance Team.



Locker Banks

Code	Name	Description	Neighbourhood	Status		
Kiosk_TZ-LAP-123	TZ Locker Bank	TZ Locker Bank	B1	Online	Edit	Advanced

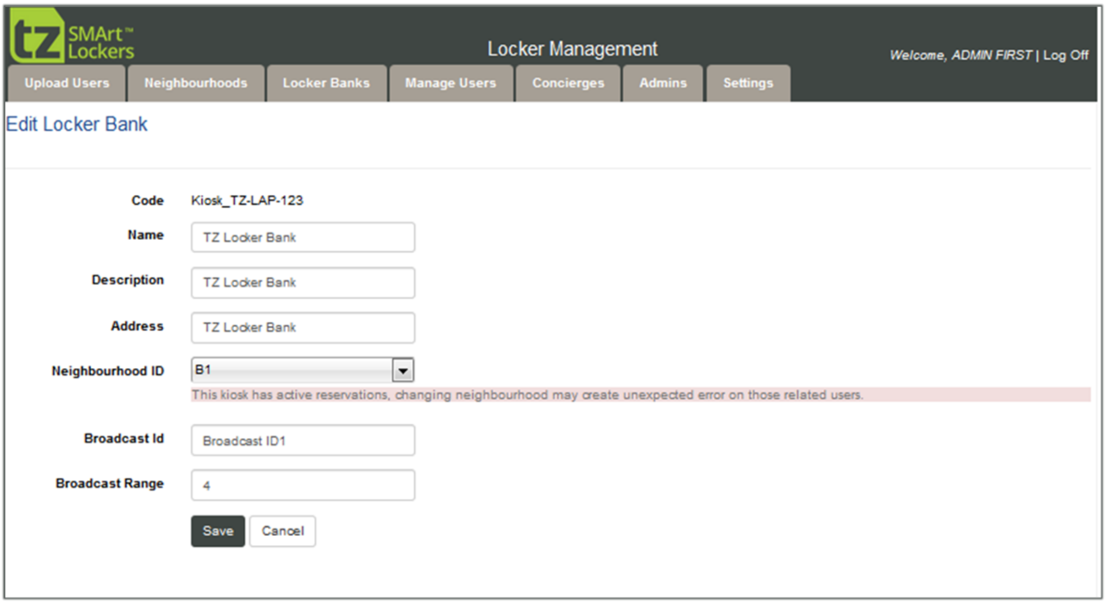
Figure 6: The Locker Banks screen

To edit the details for a Locker Bank, select the *Edit* link in the second last column for that Locker Bank. To edit advanced Kiosk settings, select the *Advanced* link in the rightmost column for that Locker Bank.

4.3.1 Edit Locker Bank

This screen allows editing of Locker Bank details such as the Name and Neighbourhood with a Save button.

Kiosk code is used internally and displayed where space is a premium, otherwise the name is used instead to refer to the Locker Bank. The description is displayed on the Kiosk when a User is welcomed following card scan or manual login, while the address is only shown on the Concierge home screen of the Kiosk



Edit Locker Bank

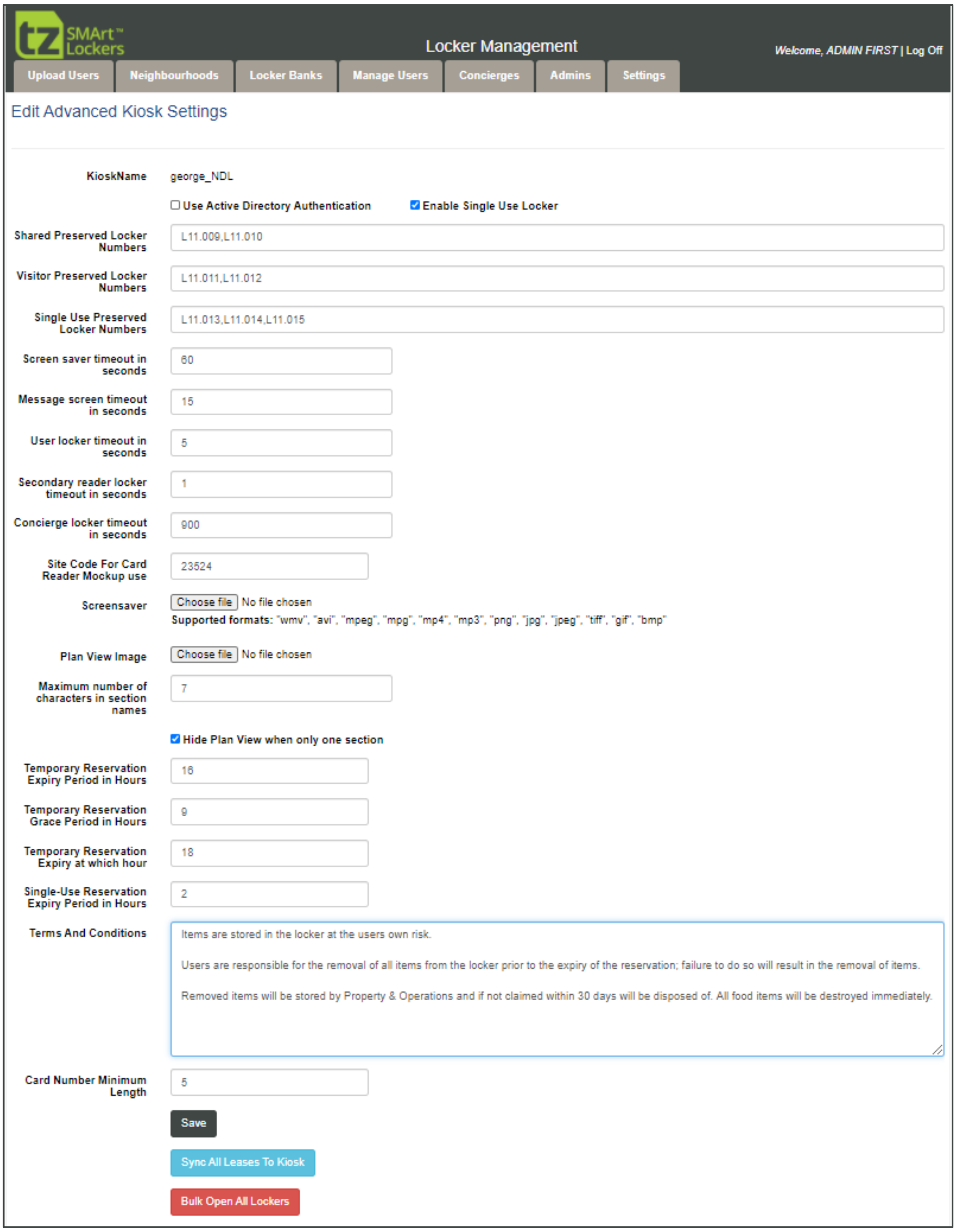
Code	Kiosk_TZ-LAP-123
Name	TZ Locker Bank
Description	TZ Locker Bank
Address	TZ Locker Bank
Neighbourhood ID	B1
Broadcast Id	Broadcast ID1
Broadcast Range	4

This kiosk has active reservations, changing neighbourhood may create unexpected error on those related users.

Figure 7: The Edit Locker Bank screen

4.3.2 Edit Advanced Kiosk Settings

This screen allows editing of advanced Kiosk settings, per Locker Bank.



Edit Advanced Kiosk Settings

KioskName	george_NDL
	□ Use Active Directory Authentication ☑ Enable Single Use Locker
Shared Preserved Locker Numbers	L11.009,L11.010
Visitor Preserved Locker Numbers	L11.011,L11.012
Single Use Preserved Locker Numbers	L11.013,L11.014,L11.015
Screen saver timeout in seconds	60
Message screen timeout in seconds	15
User locker timeout in seconds	5
Secondary reader locker timeout in seconds	1
Concierge locker timeout in seconds	900
Site Code For Card Reader Mockup use	23524
Screensaver	No file chosen Supported formats: "wmv", "avi", "mpeg", "mpg", "mp4", "mp3", "png", "jpg", "jpeg", "tiff", "gif", "bmp"
Plan View Image	No file chosen
Maximum number of characters in section names	7
	☑ Hide Plan View when only one section
Temporary Reservation Expiry Period in Hours	16
Temporary Reservation Grace Period in Hours	9
Temporary Reservation Expiry at which hour	18
Single-Use Reservation Expiry Period in Hours	2
Terms And Conditions	Items are stored in the locker at the users own risk. Users are responsible for the removal of all items from the locker prior to the expiry of the reservation; failure to do so will result in the removal of items. Removed items will be stored by Property & Operations and if not claimed within 30 days will be disposed of. All food items will be destroyed immediately.
Card Number Minimum Length	5

Figure 8: Edit Advanced Kiosk Settings screen

The following table summarises the settings that can be changed on this screen:

FIELD	DESCRIPTION
Use Active Directory Authentication	When disabled (which is the default), Users enter their Personnel ID and PIN if attempting manual login at the Locker Bank. When enabled, Users will instead enter their AD username and AD password, and these credentials will be authenticated by the AD Server.
Enable Single Use Locker	When enabled, Single Use Lockers will be offered at the Kiosk (requires you to define a list of Single Use Preserved Locker Numbers in the associated field)
Shared Preserved Locker numbers	This is the list of Lockers set aside for exclusive use by Shared Reservations
Visitor Preserved Locker numbers	This is the list of Lockers set aside for exclusive use by Visitor Reservations
Single Use Preserved Locker Numbers	This is the list of Lockers set aside exclusively for single use (requires you to have enabled Single Use Lockers)
Screen saver timeout in seconds	The length of time the Locker Bank waits for input before returning automatically to its home screen (default 60)
Message screen timeout in seconds	The length of time the Locker Bank displays warnings or error messages (default 15)
User Locker timeout in seconds	The length of time the Locker Bank waits at the Locker open screen before continuing with the workflow (default 5)
Secondary reader Locker timeout in seconds	The length of time the Locker Bank waits for the Locker open event before continuing with the workflow, when secondary scanner is used (default 1)
Concierge Locker timeout in seconds	The length of time the Locker Bank waits at the Locker open screen when opened by a Concierge via the Admin screen before timing out (default 900)
Site code for Card Reader Mock-up use	For internal use only
Screen saver	The screensaver to be used by the Locker Bank (.png file recommended). Recommended size is 1024 x 768 pixels for best results
Plan View image	The plan view image to be used by the Locker Bank (.png file recommended). Recommended size is 720 x 540 pixels for best results (optional)
Maximum number of characters in section names	The maximum length of any section name referenced on the plan view. Recommended to have single letter section names like A, B, S, etc.

Hide Plan View when only one section	For simple Locker layouts that have only one section, then a plan view is unnecessary. In such cases, tick this option to hide any references to plan view in the Locker Bank workflows.
Temporary Reservation Expiry Period in Hours	The number of hours of expiry to apply prior to a Temporary Reservation expiring (not including grace period - default 24)
Temporary Reservation Grace Period in Hours	The number of hours of grace to apply prior to a Temporary Reservation expiring (default 24)
Temporary Reservation Expiry at which hour	The hour at which Temporary Reservations expire, in 24hr time format (default 18, i.e. 6pm). Only applies when expiry period + grace period < 24 hours
Single-Use Reservation Expiry Period in Hours	The number of hours a Single Use Locker reservation lasts for
Terms and Conditions	The text to be used when displaying Terms and Conditions on the Locker Bank
Card number Minimum Length	The minimum number of digits for a valid card number. Card numbers with less digits will have leading zeroes added to the front when scanned at the Locker Bank. Note that changing this value also requires manual configuration change to the Portal and Server; please refer to the Release Notes for information on what configuration changes are required.

To change any of these settings:

- Edit the associated text field.

- Press the *Save* button to immediately update the value

If enabling User Active Directory Authentication, then you must also have set the appropriate Active Directory settings and tested to ensure that the connection to the AD Server is operational; please refer to Section 4.7.6.

Also, AD authentication can only succeed when the Locker Banks can communicate with the AD Server. If there is some network or other issue preventing this, the User will not be able to login to the Locker Bank using the manual method.

There are also two other functions available on this screen:

- Sync all Leases to Kiosk - This feature is meant only to be used in emergency circumstances, such as if a Locker Bank has been replaced and all leases pertaining to the Locker Bank need to be restored to it. During normal operation, leases are always automatically synced to the Locker Bank whenever it is online

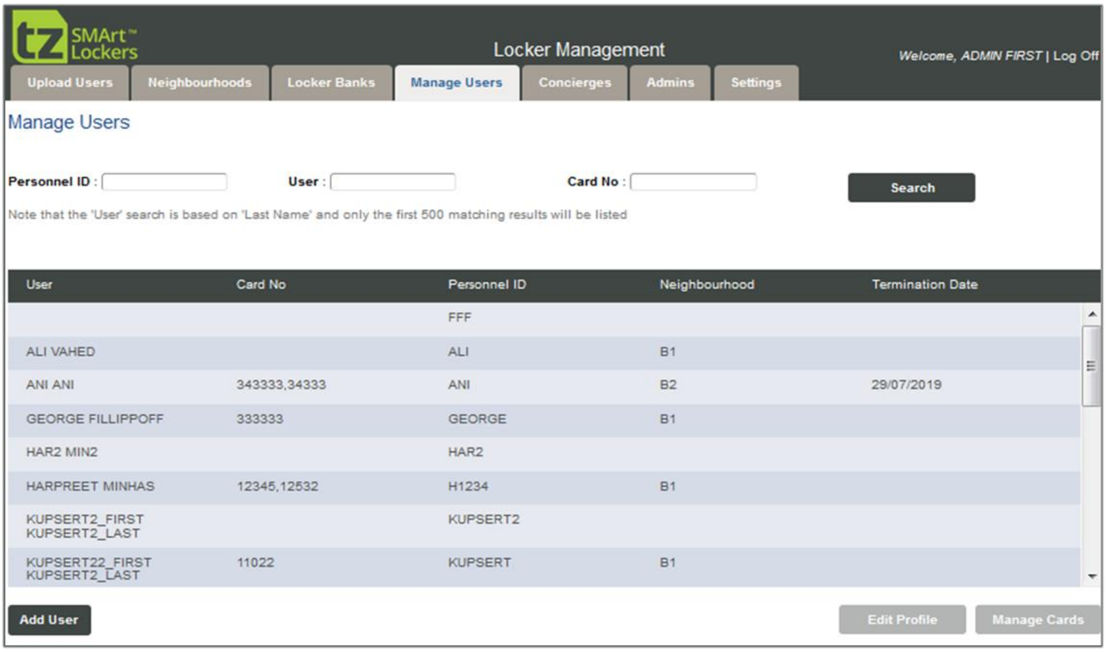
- Bulk Open All Lockers – Another feature meant only to be used in emergency circumstances.

4.4 Manage Users tab

The Manage Users tab provides User Management features, including the update of User details, Cards, and Neighbourhoods (except those Users that have been converted to Concierges, which are managed via the Concierges tab).

To locate a User (who is not a Concierge), set the filter criteria, then press the *Search* button to see the Users that fit the criteria. Filter criteria available are:

- the Personnel ID of a User
- the name of a User (case insensitive, first few letters of last name)
- the Card Number of a User



Manage Users

Personnel ID : User : Card No :

Note that the 'User' search is based on 'Last Name' and only the first 500 matching results will be listed

User	Card No	Personnel ID	Neighbourhood	Termination Date
		FFF		
ALI VAHED		ALI	B1	
ANI ANI	343333,34333	ANI	B2	29/07/2019
GEORGE FILLIPPOFF	333333	GEORGE	B1	
HAR2 MIN2		HAR2		
HARPREET MINHAS	12345,12532	H1234	B1	
KUPSERT2_FIRST KUPSERT2_LAST		KUPSERT2		
KUPSERT22_FIRST KUPSERT2_LAST	11022	KUPSERT	B1	

Figure 9: The Manage Users screen

To create a new User, click the *Add User* button at the bottom left of the screen.

If the System has been configured to import Users automatically from external systems, then DO NOT add such Users manually via the Add User button, but instead have then added via the external system, then wait until they are imported. The only exception is if you are adding Visitors from outside the organisation.

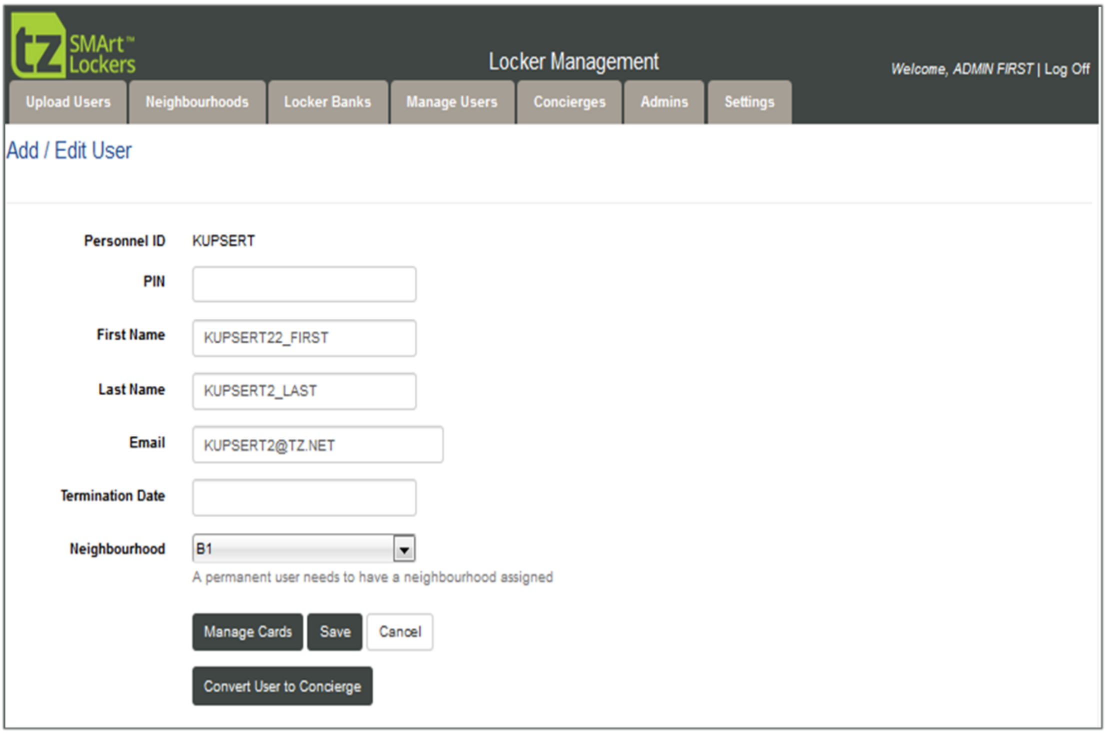
To edit an existing User, click somewhere in their row, then press the *Edit Profile* button at the bottom right of the screen.

To manage the cards of an existing User, click somewhere in their row, then press the *Manage Cards* button at the bottom right of the screen.

Inactive Users (those who have a termination date in the past) are also listed. Concierges are listed in the Concierge tab.

4.4.1 Adding/Editing Users

This screen allows adding of User details with a Save button.



Add / Edit User

Personnel ID KUPSERT

PIN

First Name KUPSERT22_FIRST

Last Name KUPSERT2_LAST

Email KUPSERT2@TZ.NET

Termination Date

Neighbourhood B1

A permanent user needs to have a neighbourhood assigned

Figure 10: The Add/Edit User screen

The following table summarises the fields available for Users:

FIELD	DESCRIPTION
Personnel ID	A unique employee number. This cannot be edited once added
PIN	A password that the User can use to access both the Employee Portal (where they can change their Reservations), or to access the Locker Bank if they cannot use their card for any reason. The password must conform to the specified password regex (refer Section 4.7.8), and any other password security features that have been enabled such as can’t use common passwords or reuse recent passwords
First Name	The User’s first name
Last Name	The User’s last name
Email	The email address for this User (this is the address where the User’s PIN will be sent when created or reset)
Termination Date	The last employment date of the User. Their Reservations will automatically convert to Visitor Reservations after this day (optional).

Neighbourhood	The User's Neighbourhood. If this matches the Neighbourhood assigned to a Locker bank, then reservations will be of type Permanent/Flexible, otherwise of type Visitor. A User with no Neighbourhood can only ever make Visitor Reservations

After pressing *Save*, if a new User was successfully added, then the Manage Cards screen will now be displayed, to allow their cards to be linked (refer to Section 4.4.2 for further details).

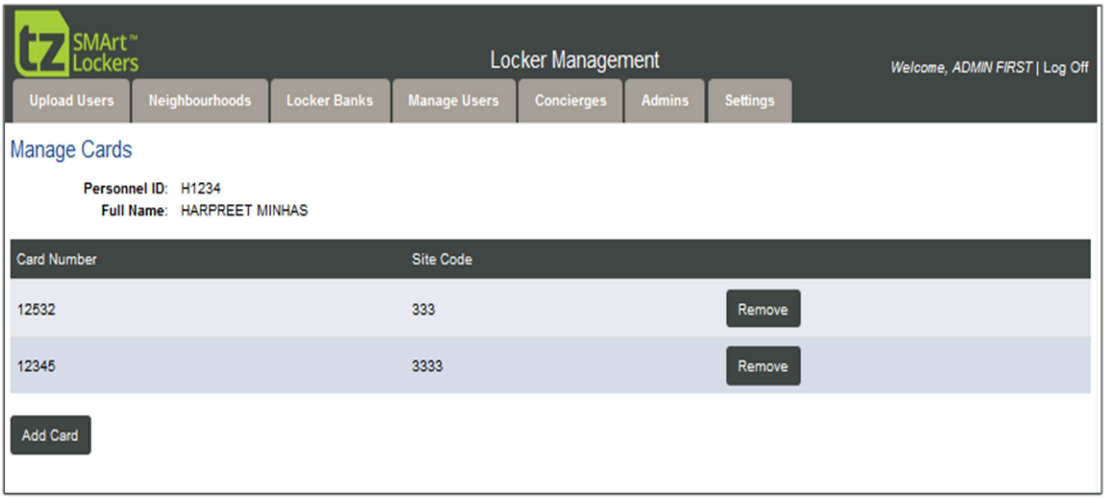
If you change a User's Neighbourhood, any reservation they have in their current Neighbourhood will be converted to a Visitor Reservation, and any Visitor Reservation in the new Neighbourhood will be converted to a Flexible Reservation (unless there is more than one, in which case they will remain unchanged).

If you have many Users to add and the System has not been configured to import Users automatically from external systems, then it is much quicker to use the Upload Users feature.

Inactive Users (those who have a termination date in the past), will have their fields shown as read only, will show a note above the fields that 'This User is inactive', and will have an additional button labelled Reactivate that can be used to reactivate the User.

4.4.2 Manage Cards screen

This screen allows the cards of a User to be managed. Users can have zero or more cards. Where they have no card, they will have to enter credentials to gain access to their reservations. Where they have one or more cards, they can swipe any of those cards at a Locker Bank to gain access to their reservations. If a User loses their card, it should be removed from the User so that the card cannot be used to access the User's reservations anymore.



Personnel ID: H1234
Full Name: HARPREET MINHAS

Card Number	Site Code	
12532	333	Remove
12345	3333	Remove

Figure 11: The Manage Cards screen

To add a new card:

- Press Add Card button.
- Enter the Card Number and Site code (there is a specific Site Code for each Site, e.g. San Jose, Oakland, etc., and cards from one Site typically cannot be used at a different Site)
- Press Save button.

To remove an existing card:

- Press *Remove* button shown next to the existing card.

Be careful editing or removing the Card numbers of existing Users, as their existing reservations will no longer be accessible using the old card number.

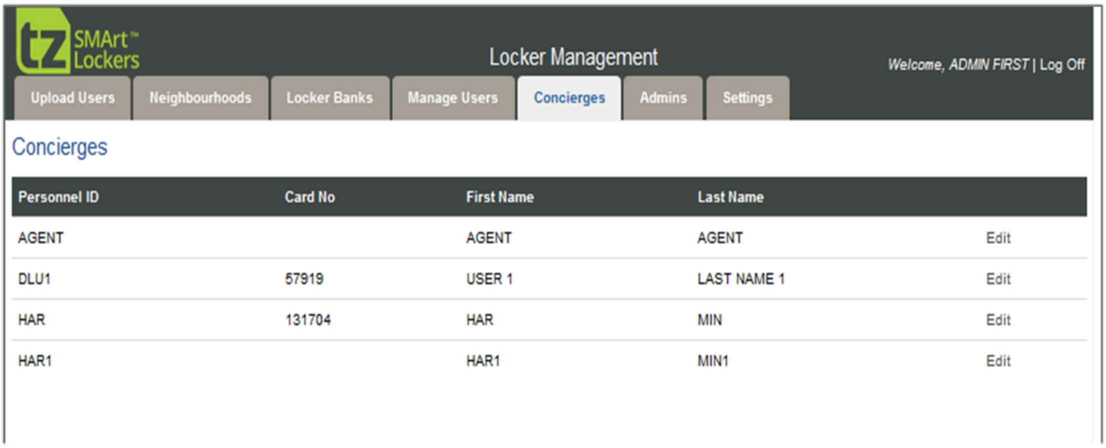
4.4.3 Converting Users to Concierges

If you select an existing User and edit them, there is an extra button available on the Add/Edit User screen labelled *Convert User to Concierge*. Use this button to create Concierges in the System.

If the System has been configured to import Concierges automatically from AD or AAD, then don't use this conversion feature, instead update the Users AD/AAD record to set the appropriate field that has been configured in the Authentication Settings screens as the Concierge discriminator (refer to Section 4.7.6).

4.5 The Concierges tab

The Concierges tab lists the Concierges in the System. Only Concierges can log into Concierge Portal or perform admin tasks at the Kiosk.



Concierges

Personnel ID	Card No	First Name	Last Name	
AGENT		AGENT	AGENT	Edit
DLU1	57919	USER 1	LAST NAME 1	Edit
HAR	131704	HAR	MIN	Edit
HAR1		HAR1	MIN1	Edit

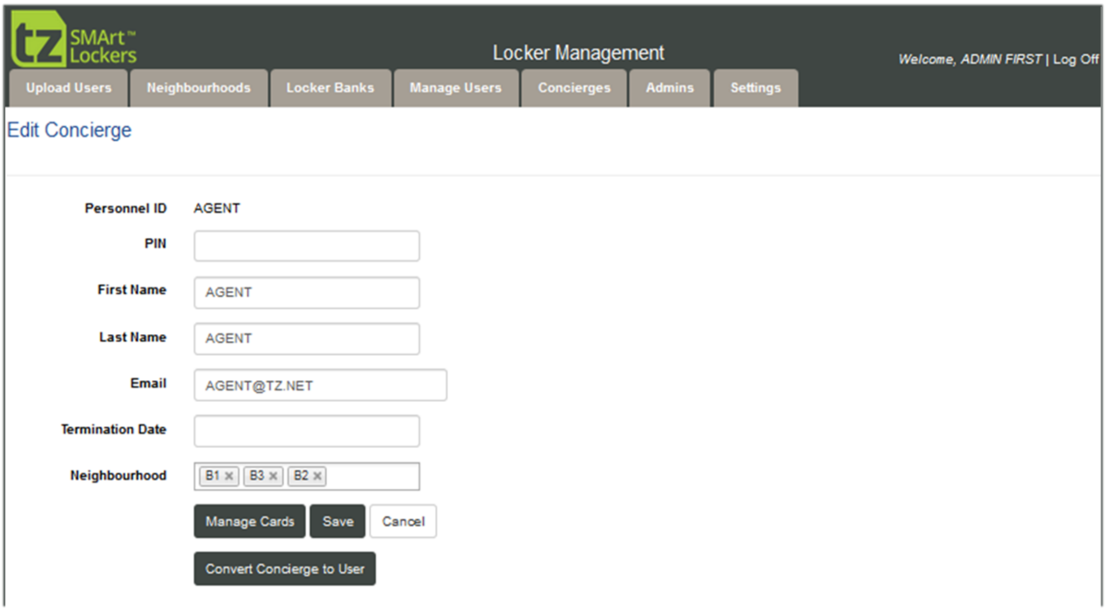
Figure 12: The Concierges screen

To create a Concierge, refer to Section 4.4.3.

To edit a Concierge, select the *Edit* link in the rightmost column for that Concierge.

4.5.1 Edit Concierge

Concierge details can be edited by changing the values in this screen.



Edit Concierge

Personnel ID	AGENT
PIN	
First Name	AGENT
Last Name	AGENT
Email	AGENT@TZ.NET
Termination Date	
Neighbourhood	B1 × B3 × B2 ×

Figure 13: Edit Concierge screen

The fields on this screen are the same as the fields on the normal Add/Edit User screen. The only difference is that the Neighbourhood field can contain a list of multiple Neighbourhoods. These will be the Neighbourhoods over which the Concierge will have jurisdiction.

- Click in the field to make visible a drop-down list from which an additional Neighbourhood can be added
- Click on the cross icon of an existing Neighbourhood to remove it from the field

Remember to press the *Save* button after editing a Concierge.

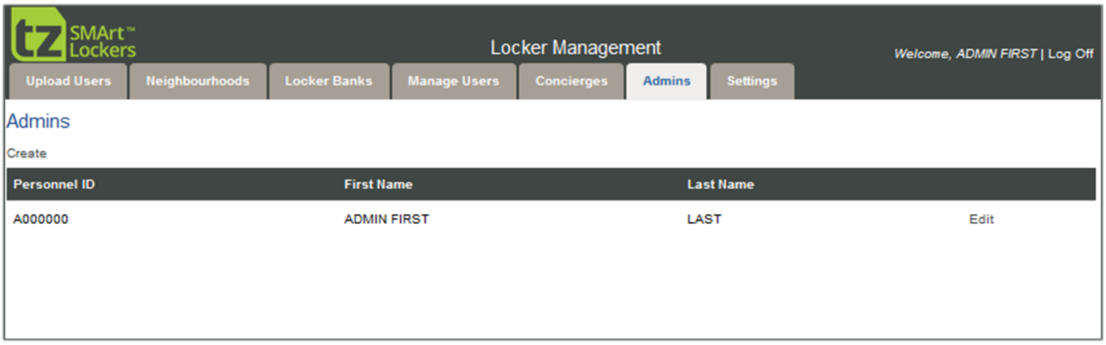
The *Manage Cards* button can be used to manage the Concierge's cards in the same way as a normal User's cards.

Use the *Convert Concierge to User* button to convert Concierges back to normal Permanent Users.

If the System has been configured to import Concierges automatically from AD or AAD, then don't use this conversion feature, instead update the User's AD/AAD record to un-set the appropriate field that has been configured in the Authentication Settings screens as the Concierge discriminator (refer to Section 4.7.6).

4.6 The Admins tab

The Admins tab lists the Admins in the System. Only Admins can log into Admin Portal



Admins

Personnel ID	First Name	Last Name	
A000000	ADMIN FIRST	LAST	Edit

Figure 14: Admins Screen

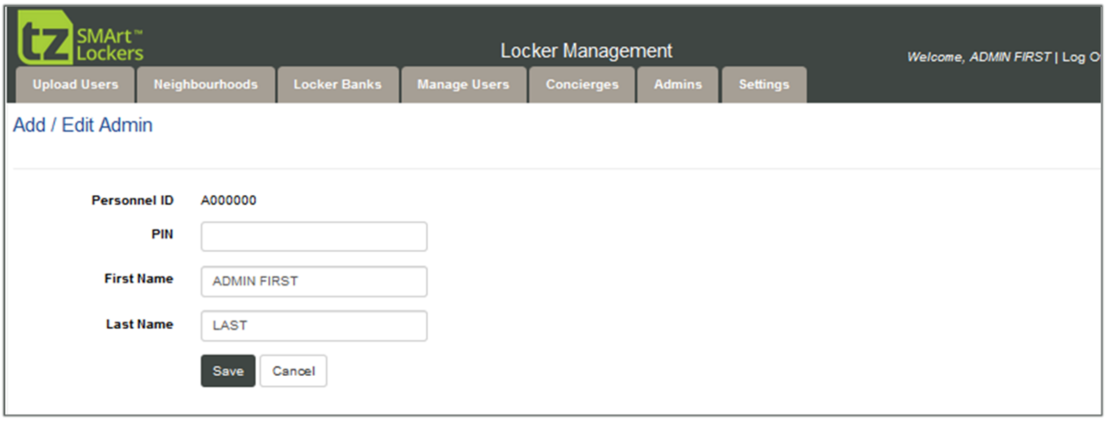
To create a new Admin, click the *Create* link at the top left of the screen.

To edit an Admin, select the *Edit* link in the rightmost column for that Admin.

If the System has been configured to import Admins automatically from AD or AAD, then don't use this conversion feature, instead update the Users AD/AAD record to set the appropriate field that has been configured in the Authentication Settings screens as the Super Admin discriminator (refer to Section 4.7.6).

4.6.1 Add/ Edit Admin

Admin details can be edited by changing the values in this screen.



Add / Edit Admin

Personnel ID	A000000
PIN	
First Name	ADMIN FIRST
Last Name	LAST

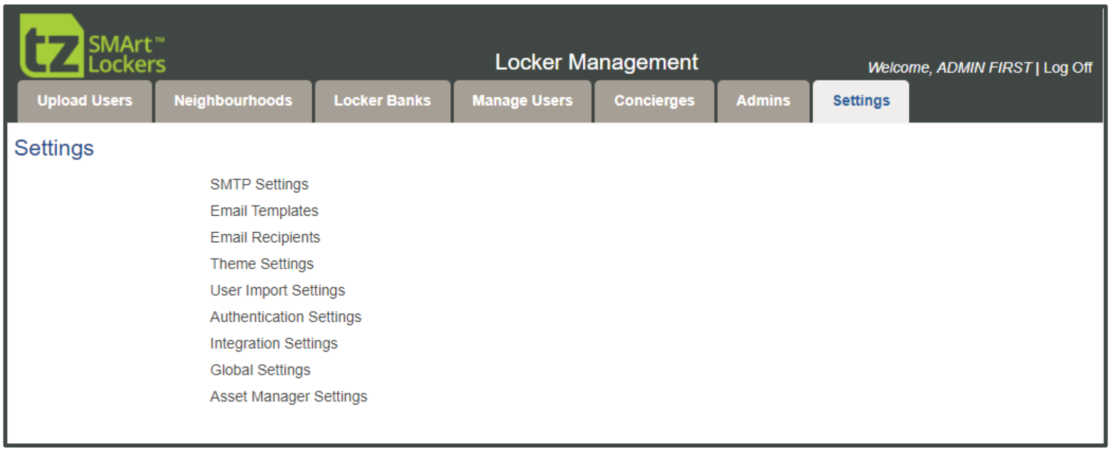
Figure 15: The Add/Edit Admin screen

The following table summarises the fields available for Admins:

FIELD	DESCRIPTION
Personnel ID	A unique ID. This cannot be edited once added
PIN	A password that the Admin can use to access the Admin Portal. The password must conform to the specified password regex (refer Section 4.7.8), and any other password security features that have been enabled such as can't use common passwords or reuse recent passwords
First Name	The Admin's first name
Last Name	The Admin's last name

4.7 Settings tab

The Settings tab allows various System related settings to be changed.



Settings

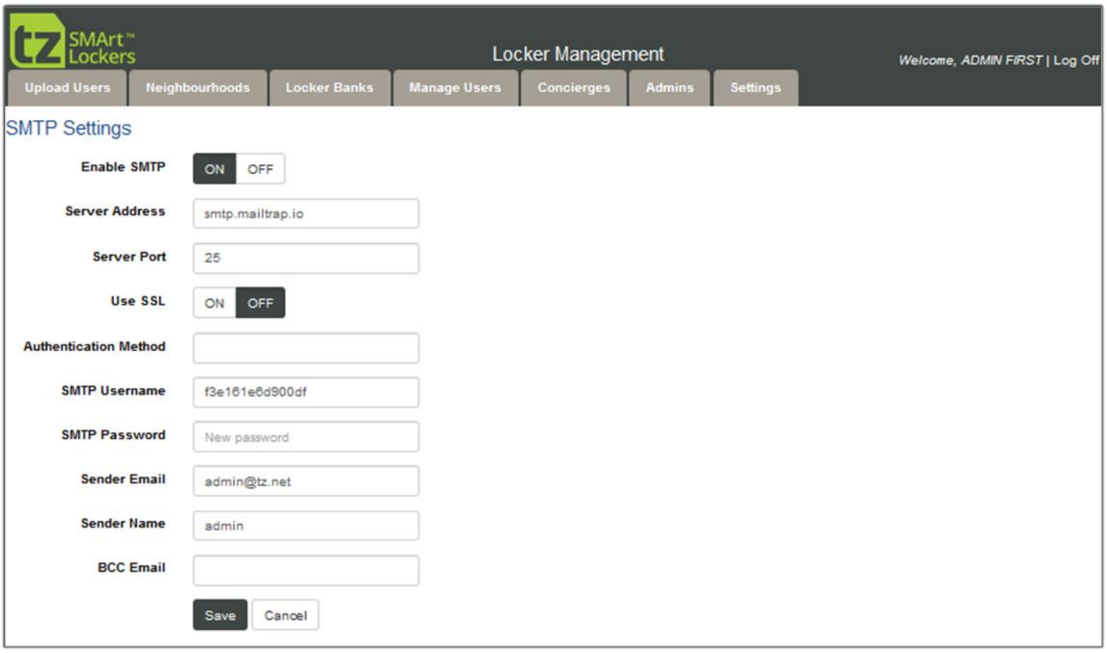
SMTP Settings
Email Templates
Email Recipients
Theme Settings
User Import Settings
Authentication Settings
Integration Settings
Global Settings
Asset Manager Settings

Figure 16: Settings screen

4.7.1 SMTP settings

SMTP settings screen displays a form to capture configuration information about the email gateway for the Portal to successfully send email notifications to recipients.

This feature can be reached by selecting the *SMTP Settings* link from the Settings screen.



SMTP Settings

Enable SMTP	[✓ ON] OFF
Server Address	smtp.mailtrap.io
Server Port	25
Use SSL	ON [✓ OFF]
Authentication Method	
SMTP Username	f3e161e6d900df
SMTP Password	New password
Sender Email	admin@tz.net
Sender Name	admin
BCC Email	

Figure 17: SMTP Settings screen

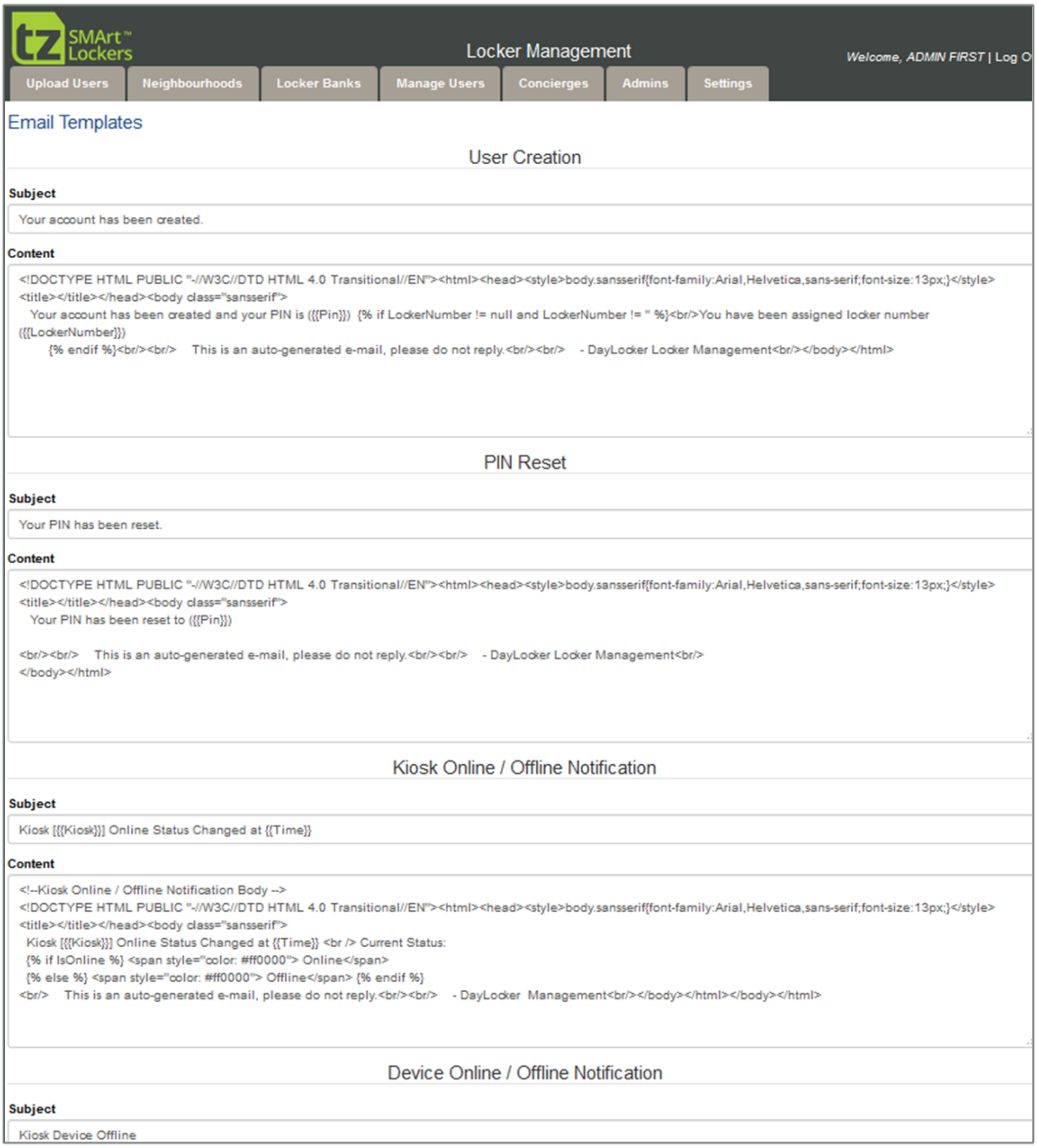
To change any of these settings:

- Edit the associated text field.
- Press the *Save* button to immediately update the value

4.7.2 Email Templates

The Email Templates screen contains the message templates used when the System generates an email notification for events.

This feature can be reached by selecting the *Email Templates* link from the Settings screen.



Email Templates

User Creation

Subject

Your account has been created.

Content

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN"><html><head><style>body.sansserif{font-family:Arial,Helvetica,sans-serif;font-size:13px;}</style>
<title></title></head><body class="sansserif">
  Your account has been created and your PIN is ({{Pin}})  {% if LockerNumber != null and LockerNumber != '' %}<br/>You have been assigned locker number
({{LockerNumber}})
      {% endif %}<br/><br/>    This is an auto-generated e-mail, please do not reply.<br/><br/>    - DayLocker Locker Management<br/></body></html>
```

PIN Reset

Subject

Your PIN has been reset.

Content

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN"><html><head><style>body.sansserif{font-family:Arial,Helvetica,sans-serif;font-size:13px;}</style>
<title></title></head><body class="sansserif">
  Your PIN has been reset to ({{Pin}})

<br/><br/>    This is an auto-generated e-mail, please do not reply.<br/><br/>    - DayLocker Locker Management<br/>
</body></html>
```

Kiosk Online / Offline Notification

Subject

Kiosk [{{Kiosk}}] Online Status Changed at {{Time}}

Content

```
<!--Kiosk Online / Offline Notification Body -->
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN"><html><head><style>body.sansserif{font-family:Arial,Helvetica,sans-serif;font-size:13px;}</style>
<title></title></head><body class="sansserif">
 Kiosk [{{Kiosk}}] Online Status Changed at {{Time}} <br /> Current Status:
 {% if IsOnline %} <span style="color: #ff0000"> Online</span>
 {% else %} <span style="color: #ff0000"> Offline</span> {% endif %}
<br/>    This is an auto-generated e-mail, please do not reply.<br/><br/>    - DayLocker  Management<br/></body></html></body></html>
```

Device Online / Offline Notification

Subject

Kiosk Device Offline

Figure 18: Email Templates screen

There are Email Templates for the following events (with both the subject line and body being editable):

- User Creation
- PIN reset
- Kiosk online/ offline Notification

- Device online/ offline Notification
- Delegate/ Un-delegate access to Locker Notification
- Shared Reservation Created Notification

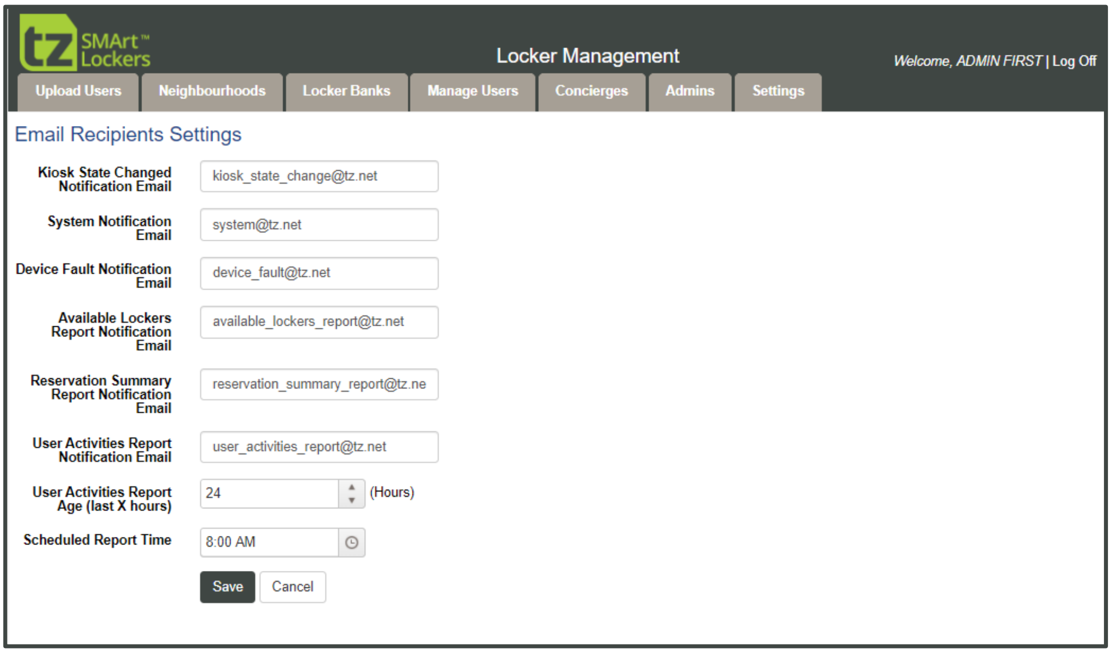
To change any of these settings:

- Edit the associated text field.
- Press the Save button to immediately update the value

4.7.3 Email Recipients

The Email Recipients Settings screen contains the nominated email addresses that the System directs reports and notifications to, as well as some report settings.

This feature can be reached by selecting the *Email Recipients* link from the Settings screen.



Locker Management

Welcome, ADMIN FIRST | Log Off

Email Recipients Settings

Kiosk State Changed Notification Email	kiosk_state_change@tz.net
System Notification Email	system@tz.net
Device Fault Notification Email	device_fault@tz.net
Available Lockers Report Notification Email	available_lockers_report@tz.net
Reservation Summary Report Notification Email	reservation_summary_report@tz.ne
User Activities Report Notification Email	user_activities_report@tz.net
User Activities Report Age (last X hours)	24 (Hours)
Scheduled Report Time	8:00 AM

Figure 19: Email Recipients screen

There are three reports emailed out by the System daily, the *Available Lockers Report*, *Reservation Summary Report* and *User Activities Report*. Use the *Scheduled Report Time* field to set the time of day when these are generated and set the associated *Notification Email* field to the desired email recipients for that report. For the *User Activities Report*, you can also set the age to apply to the report using the *User Activities Report Age (last X hours)* field.

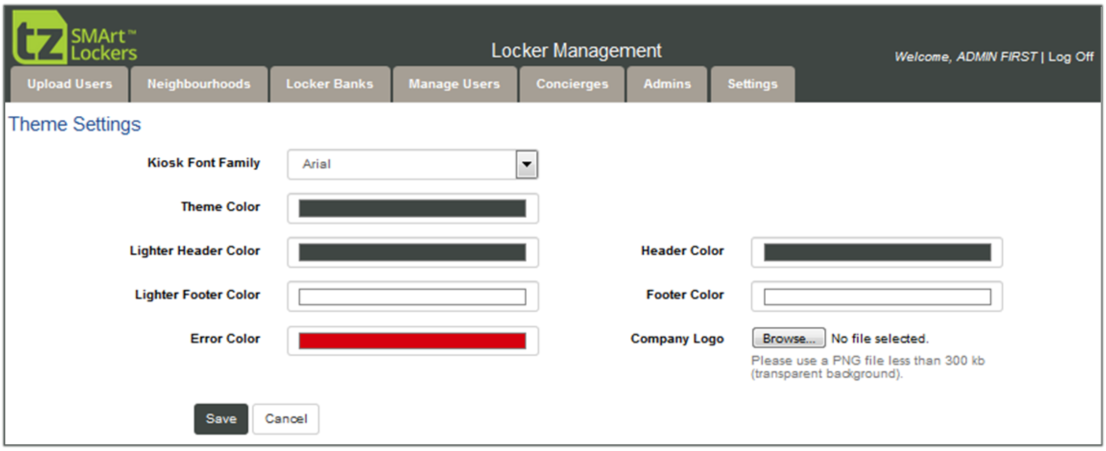
To change any of these settings:

- Edit the associated field.
- Press the *Save* button to immediately update the value

4.7.4 Theme Settings

The Theme Settings screen contains settings for colours, fonts, and company logo to be used in the System

This feature can be reached by selecting the *Theme Settings* link from the Settings screen.



Theme Settings

Kiosk Font Family	Arial		
Theme Color	⬛		
Lighter Header Color	⬛	Header Color	⬛
Lighter Footer Color	⬜	Footer Color	⬜
Error Color	🟥	Company Logo	No file selected. Please use a PNG file less than 300 kb (transparent background).

Figure 20: Theme Settings screen

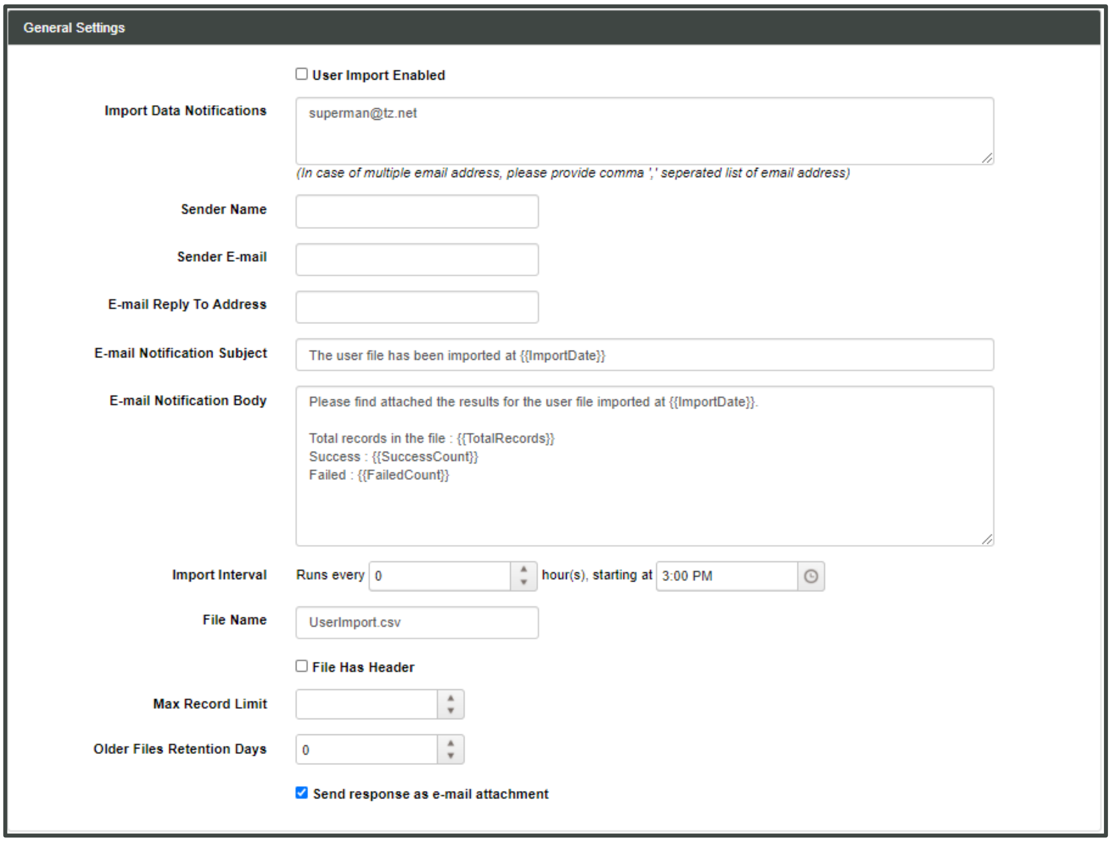
4.7.5 User Import Settings

Bulk User import via csv file can be initiated in the following ways:

- Manually, by using the Admin Portal's Upload Users feature (refer to Section 4.1)
- Automatically, by configuring a pickup point where the csv file will be placed which can either be an FTP or SFTP endpoint or a network share (but only one location at a time), and the System will periodically automatically import the file

For the automatic method, use the *User Import Settings* screen to configure all the required settings, including general settings as well as specific endpoint settings and credentials. This feature can be reached by selecting the *User Import Settings* link from the Settings screen.

The screenshot below shows the General settings related to User import.



General Settings

☐ User Import Enabled

Import Data Notifications: superman@tz.net
(In case of multiple email address, please provide comma ',' seperated list of email address)

Sender Name:

Sender E-mail:

E-mail Reply To Address:

E-mail Notification Subject: The user file has been imported at {{ImportDate}}

E-mail Notification Body:
Please find attached the results for the user file imported at {{ImportDate}}.

Total records in the file : {{TotalRecords}}
Success : {{SuccessCount}}
Failed : {{FailedCount}}

Import Interval: Runs every 0 hour(s), starting at 3:00 PM

File Name: UserImport.csv

☐ File Has Header

Max Record Limit:

Older Files Retention Days: 0

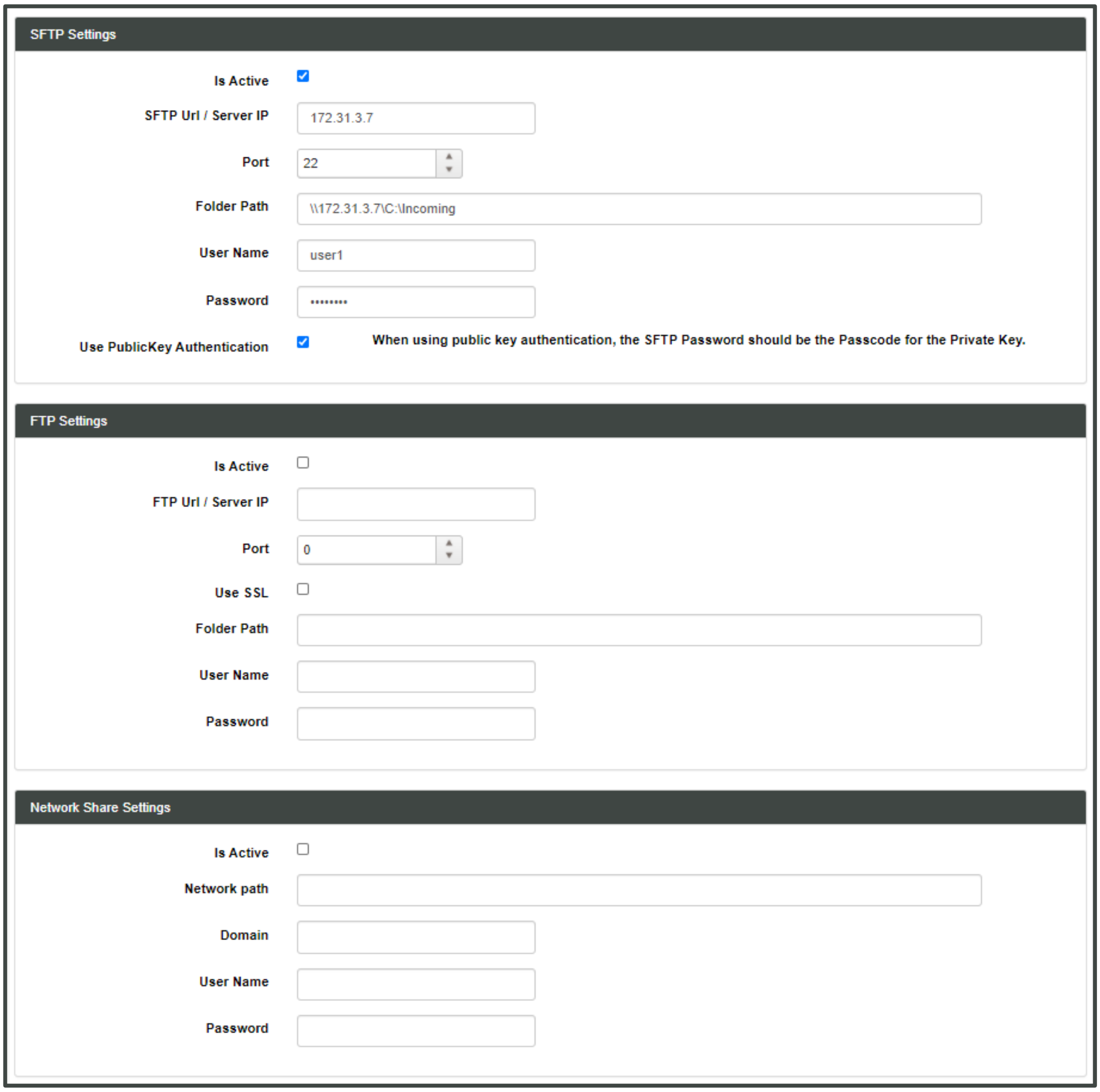
☑ Send response as e-mail attachment

Settings that must be specified are:

- *User Import Enabled* – tick this to enable the automatic import feature
- *Import Data Notifications* – use this to specify one or more email recipients to receive the results of each automatic import
- *Import Interval* – set as desired
- *File Name* – this should reflect the file name of the csv file that will be picked up automatically
- *File has Header* – tick this to indicate that the first row of the file is a header row that should be skipped
- *Max Record Limit* – make sure to set a value for this, i.e. 250

A sample csv file can be obtained by pressing the *Sample File* button.

Below the general settings are individual panes for setting the supported endpoint types, refer to the screenshot below:



SFTP Settings

Is Active	☑
SFTP Url / Server IP	172.31.3.7
Port	22
Folder Path	\\172.31.3.7\C:\Incoming
User Name	user1
Password	••••••••
Use PublicKey Authentication	☑ When using public key authentication, the SFTP Password should be the Passcode for the Private Key.

FTP Settings

Is Active	□
FTP Url / Server IP	
Port	0
Use SSL	□
Folder Path	
User Name	
Password	

Network Share Settings

Is Active	□
Network path	
Domain	
User Name	
Password	

Remember, only one endpoint type is supported at a time. You must choose only one of the three methods, tick *Is Active* checkbox, then provide the other required details for the automatic import to successfully find and pick up the csv file.

4.7.6 Authentication Settings

The Authentication Settings screen contains settings for using existing external authentication for Users in the System, such as an organisations AD (Active Directory) Server or Azure AD Server. This includes the importing of Users from such external systems, as well as live authentication of these Users when they login to the Portal or Kiosks.

This feature can be reached by selecting the *Authentication Settings* link from the Settings screen.

If using Authentication, use the *Provider Type* dropdown control to choose between *Active Directory* or *Azure Active Directory*. To turn off external authentication, select the blank item from the *Provider Type* dropdown and press the *Save* button.

When AD or AAD authentication is enabled, then Users will be automatically imported to the System. The ramifications on system operation in this case are:

- The source of truth for imported Users has now shifted to their AD/AAD record. As such, do not edit such Users within the Portal anymore, since any edits made internally will be overwritten on next import. Such Users will need to have all their details updated in their AD/AAD record instead (this includes their passwords, their card details (if stored in the AD record), their Neighbourhood, and their roles, i.e. if they are Concierge or Admin or neither). Similarly, Users will need to have their AD/AAD record disabled or updated with an Expiry Date set to have their usership terminated within the System (further details below).

- Users will be imported from either defined AD Container paths (in the case of AD) or Azure AD groups (in the case of AAD), If a User doesn't fit the criteria defined for the Super Admin or Concierge roles (as specified in the Provider Type screens detailed below), they will be imported as regular Permanent Users with a Neighbourhood.

- If desired, you can still have 'local' Users within the System that are still managed within the Portal as normal rather than imported from AD/AAD. For example, you may want to create Guest Users locally (since it is not possible to import Guest Users, i.e. Users without a Neighbourhood). But for this to work, you must have enabled the 'Mixed Mode Authentication' options in the Authentication Settings screens. Where Mixed Mode is enabled, then the order of authentication is first the AD/AAD external system, then the local System.

- Card data can also be imported according to the attribute mappings configured if it exists in the AD/AAD record of the Users. However, at organisations where no card data is stored in the AD/AAD external system, then cards will have to be associated to Users via the Card On-boarding process (where cards are associated to Users on first time card swipe at a Kiosk – refer to the User Guide for more details).

- Because authentication is now done at the AD/AAD Server, then the Asset Manager and Kiosks must always be online to those systems via the network.

Please note that the specification of a User's Neighbourhood differs between AD and AAD as follows:

- When AD is used, a User's Neighbourhood is defined by an attribute in the AD User's record

- But when AAD is used, a User's Neighbourhood is instead defined by the AAD group to which they belong (in conjunction with the configured AAD group to Neighbourhood mapping – refer to Section 4.2.2)

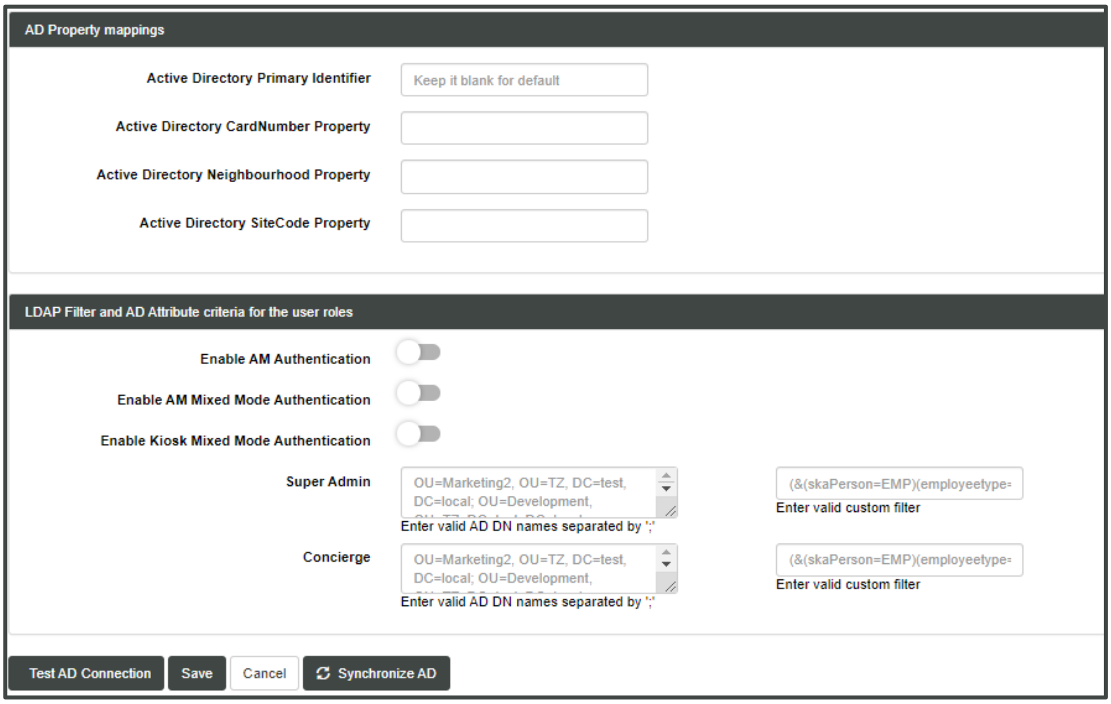
During User import, there are two scenarios that will lead to User deactivation in the System:

- If a User account is disabled in AD/AAD, then on next user sync, that User will have their termination date set to yesterday within the System.

- If a User account has their Expiry Date set to a date in the past, then on next user sync, that User will have their termination date set to the same date within the System.

In both cases, the next time the termination service runs in the System (it runs daily in the background), the User will be deactivated. If the User happens to have any Permanent or Flexible Reservations, those reservations will be converted to Visitor Reservations, with Expiry Date two (2) days into the future (shifted to the following Monday in the case of a weekend expiry) at 6pm.

Deactivated Users can be reactivated in AD by either re-enabling their account or clearing their Expiry Date (or setting it to a future date).



AD Property mappings

Active Directory Primary Identifier: Keep it blank for default

Active Directory CardNumber Property

Active Directory Neighbourhood Property

Active Directory SiteCode Property

LDAP Filter and AD Attribute criteria for the user roles

Enable AM Authentication

Enable AM Mixed Mode Authentication

Enable Kiosk Mixed Mode Authentication

Super Admin: OU=Marketing2, OU=TZ, DC=test, DC=local; OU=Development,

Enter valid AD DN names separated by ';'

(&(skaPerson=EMP)(employeetype=

Enter valid custom filter

Concierge: OU=Marketing2, OU=TZ, DC=test, DC=local; OU=Development,

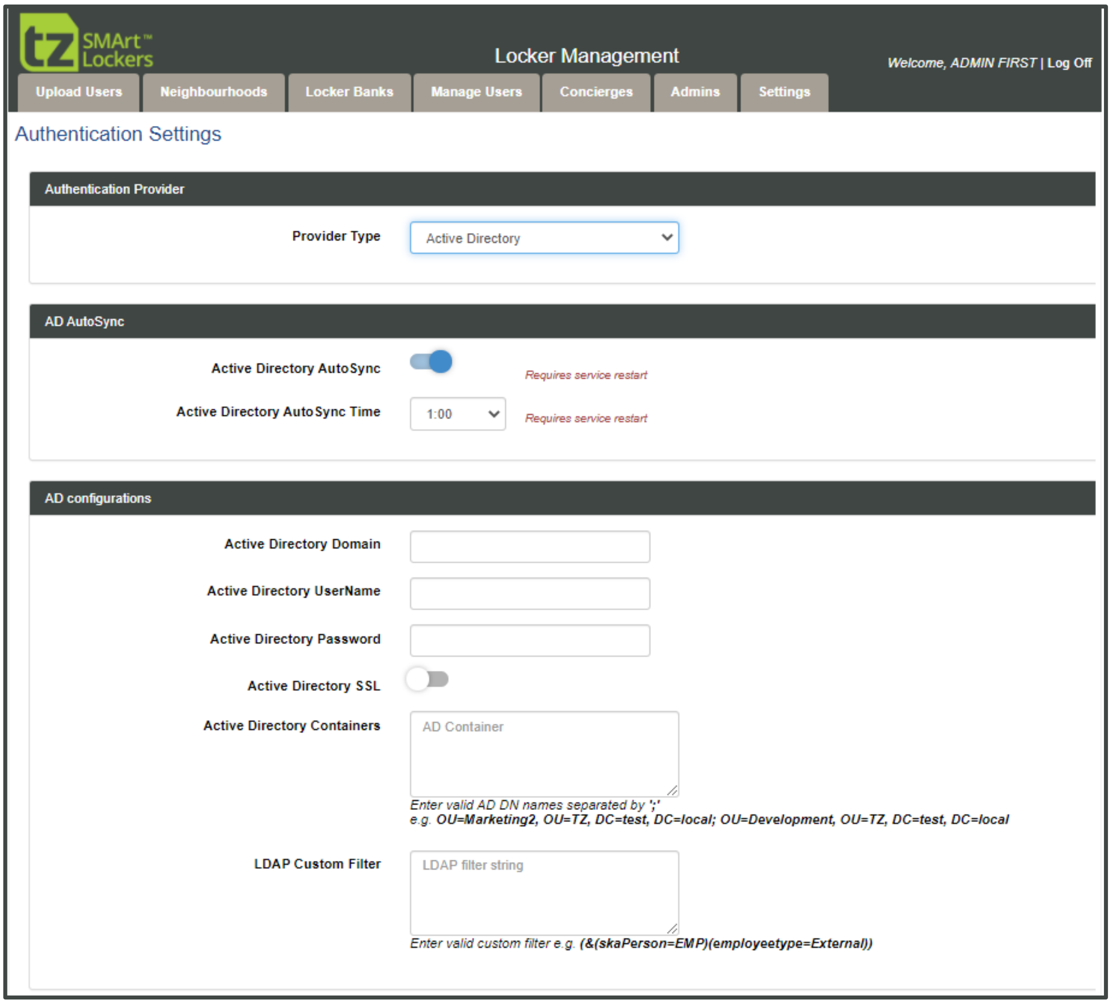
Enter valid AD DN names separated by ';'

(&(skaPerson=EMP)(employeetype=

Enter valid custom filter

4.7.6.1 Active Directory Settings

When *Provider Type* is set to *Active Directory*, the following settings will be shown:



Authentication Settings

Authentication Provider

Provider Type: Active Directory

AD AutoSync

Active Directory AutoSync: ON — Requires service restart

Active Directory AutoSync Time: 1:00 — Requires service restart

AD configurations

Active Directory Domain

Active Directory UserName

Active Directory Password

Active Directory SSL: OFF

Active Directory Containers: AD Container

Enter valid AD DN names separated by ';'
e.g. **OU=Marketing2, OU=TZ, DC=test, DC=local; OU=Development, OU=TZ, DC=test, DC=local**

LDAP Custom Filter: LDAP filter string

Enter valid custom filter e.g. **(&(skaPerson=EMP)(employeetype=External))**

Figure 21: Active Directory Settings screen

The following table summarises the settings that can be changed on this screen:

FIELD	DESCRIPTION
Active Directory AutoSync	When this is OFF, Users will not be auto imported from Active Directory daily (changing this setting requires the service to be restarted to take effect)
Active Directory AutoSync Time	If AutoSync is ON, this is the daily time at which the AD sync service will execute in the background (changing this setting requires the service to be restarted to take effect)
Active Directory Domain	The host name or IP address of the AD Server
Active Directory UserName	The username to be used when connecting to the AD Server
Active Directory Password	The password to be used when connecting to the AD Server

Active Directory SSL	Whether to use SSL or not when connecting to the AD Server (default off)
Active Directory Containers	AD Container path which contains all the Users to be imported (multiple paths can be defined separated by a semi-colon).
LDAP Custom Filter	A filter that can be set to further limit the Users being imported based on attributes of the AD record (optional)
Active Directory Primary Identifier	The attribute in an AD record to map to the Personnel ID when syncing. When left blank, the default is the sAMAccountName (optional) If *you are not using AD authentication at the Locker Banks, but simply importing your User base to the System, then this field can be mapped to any appropriate identifier type field in your AD record, i.e. student ID, driver's license or similar. But if you plan to enable AD authentication at your Kiosk, then either leave this field blank or set it to map to UserPrincipalName*
Active Directory CardNumber Property	The attribute in an AD record to map to the card number when syncing (optional).
Active Directory Neighbourhood Property	The attribute in an AD record to map to the Neighbourhood when syncing (optional).
Active Directory SiteCode Property	The attribute in an AD record to map to the sitecode when syncing (optional).
Enable AM authentication	If enabled, Users can login to Portal using AD credentials
Enable AM Mixed Mode Authentication	If enabled, Users can login to Portal using both local as well as AD credentials
Enable Kiosk Mixed mode Authentication	If enabled, Users can login to Kiosk using both local as well as AD credentials
Super Admin	AD Container path(s) which contain the Admins to be imported (multiple paths can be defined separated by a semi-colon). Next to this is an attribute filter that can be optionally used to discriminate between Admins, Concierges, or neither
Concierge	AD Container path(s) which contain the Concierges to be imported (multiple paths can be defined separated by a semi-colon). Next to this is an attribute filter that can be optionally used to discriminate between Admins, Concierges, or neither

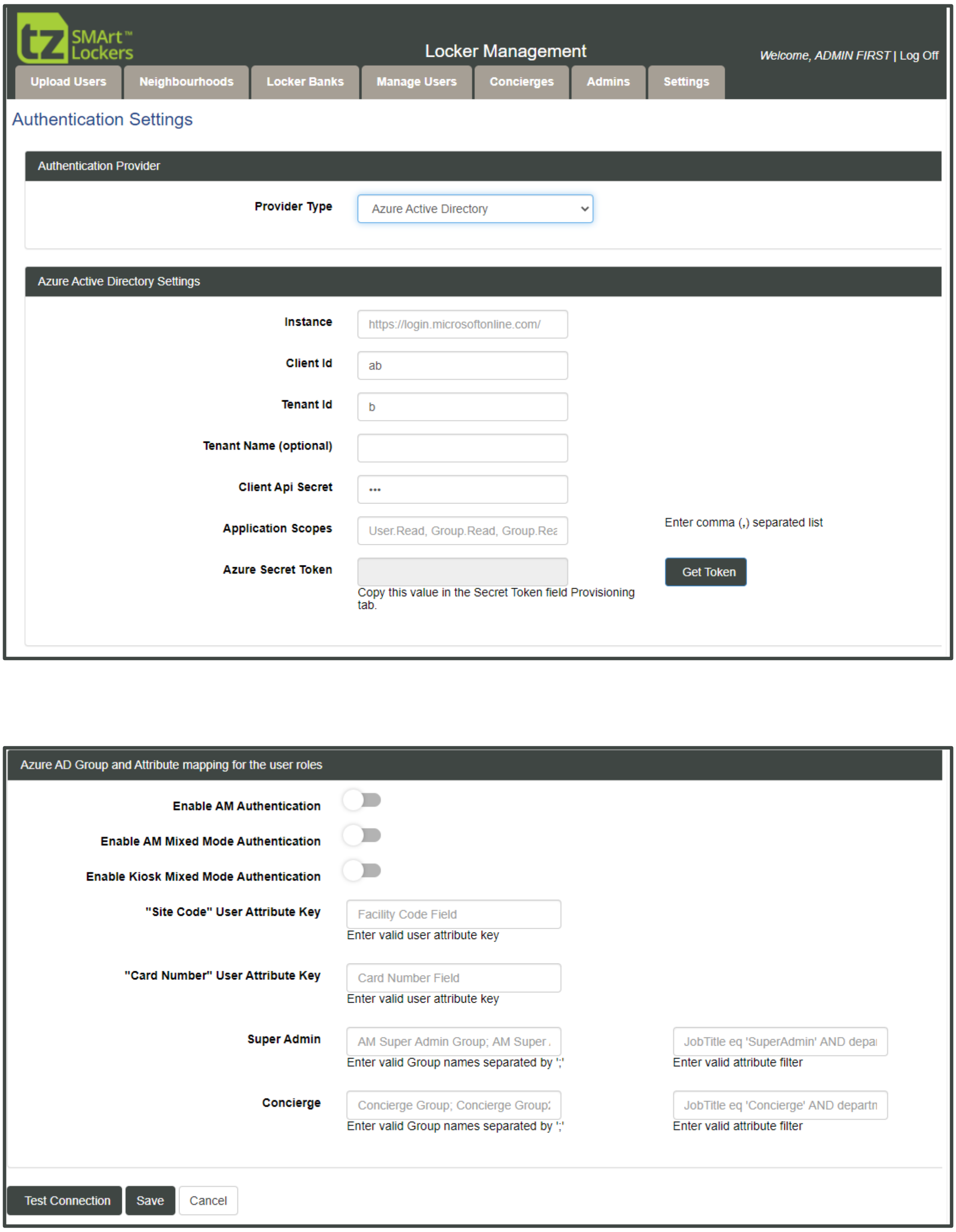
To change any of these settings, edit the associated text field, then press the *Save* button to immediately update the value.

> To test the AD connection, save your changed settings first, then press the *Test AD Connection* button.

> To trigger an immediate AD sync, press the *Synchronize AD* button.

4.7.6.2 Azure Active Directory Settings

When *Provider Type* is set to Azure Active Directory, the following settings will be shown:



Authentication Settings

Authentication Provider

Provider Type: Azure Active Directory

Azure Active Directory Settings

Instance: https://login.microsoftonline.com/

Client Id: ab

Tenant Id: b

Tenant Name (optional):

Client Api Secret: •••

Application Scopes: User.Read, Group.Read, Group.Rea — Enter comma (,) separated list

Azure Secret Token: — Copy this value in the Secret Token field Provisioning tab.

Azure AD Group and Attribute mapping for the user roles

Enable AM Authentication

Enable AM Mixed Mode Authentication

Enable Kiosk Mixed Mode Authentication

"Site Code" User Attribute Key: Facility Code Field — Enter valid user attribute key

"Card Number" User Attribute Key: Card Number Field — Enter valid user attribute key

Super Admin: AM Super Admin Group; AM Super . — Enter valid Group names separated by ';' — JobTitle eq 'SuperAdmin' AND depai — Enter valid attribute filter

Concierge: Concierge Group; Concierge Group; — Enter valid Group names separated by ';' — JobTitle eq 'Concierge' AND departn — Enter valid attribute filter

Figure 22: Azure Active Directory Settings screen

The following table summarises the settings that can be changed on this screen:

FIELD	DESCRIPTION
Instance	Default is *https://login.microsoftonline.com/* .
Client Id	Client ID (copy this from Azure and paste here)
Tenant Id	Tenant ID (copy this from Azure and paste here)
Tenant Name	(optional) TheTenant name
Client Api secret	Client Secret (copy this from Azure and paste here)
Application Scopes	Default is *User.Read, User.Read.All, Group.Read.All* (corresponds to the permissions granted in Azure)
Azure Secret Token	Azure secret token to be copied to Azure AD as part of the provisioning (the *Get Token* button will become visible once above settings are entered and saved; pressing it copies the secret token to clipboard for pasting to Azure)
Enable AM Authentication	If enabled, Users can login to Portal using AAD credentials.
Enable AM Mixed Mode Authentication	If enabled, Users can login to Portal using both local as well as AAD credentials.
Enable Kiosk Mixed Mode Authentication	If enabled, Users can login to Kiosk using both local as well as AAD credentials
"Site Code" User Attribute Key	The attribute in an AAD record to map to the card sitecode when syncing (optional).
"Card Number" User Attribute Key	The attribute in an AAD record to map to the card number when syncing (optional).
Super Admin	AAD group(s) which contain the Admins to be imported (multiple groups can be defined separated by a semi-colon). Next to this is an attribute filter that can be optionally used to discriminate between Admins, Concierges, or neither
Concierge	AAD group(s) which contain the Concierges to be imported (multiple groups can be defined separated by a semi-colon). Next to this is an attribute filter that can be optionally used to discriminate between Admins, Concierges, or neither

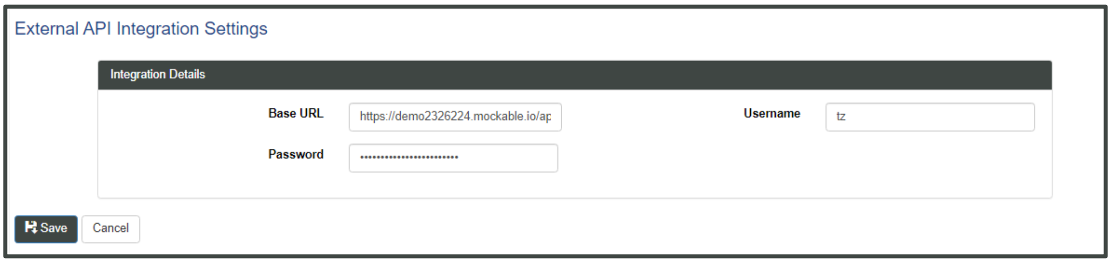
To change any of these settings, edit the associated text field, then press the *Save* button to immediately update the value

> To test the AAD connection, save your changed settings first, then press the *Test Connection* button.

4.7.7 Integration Settings

The External API Integration Settings screen contains settings for posting events in the System to an external REST based API.

This feature can be reached by selecting the *Integration Settings* link from the Settings screen.



External API Integration Settings

Integration Details

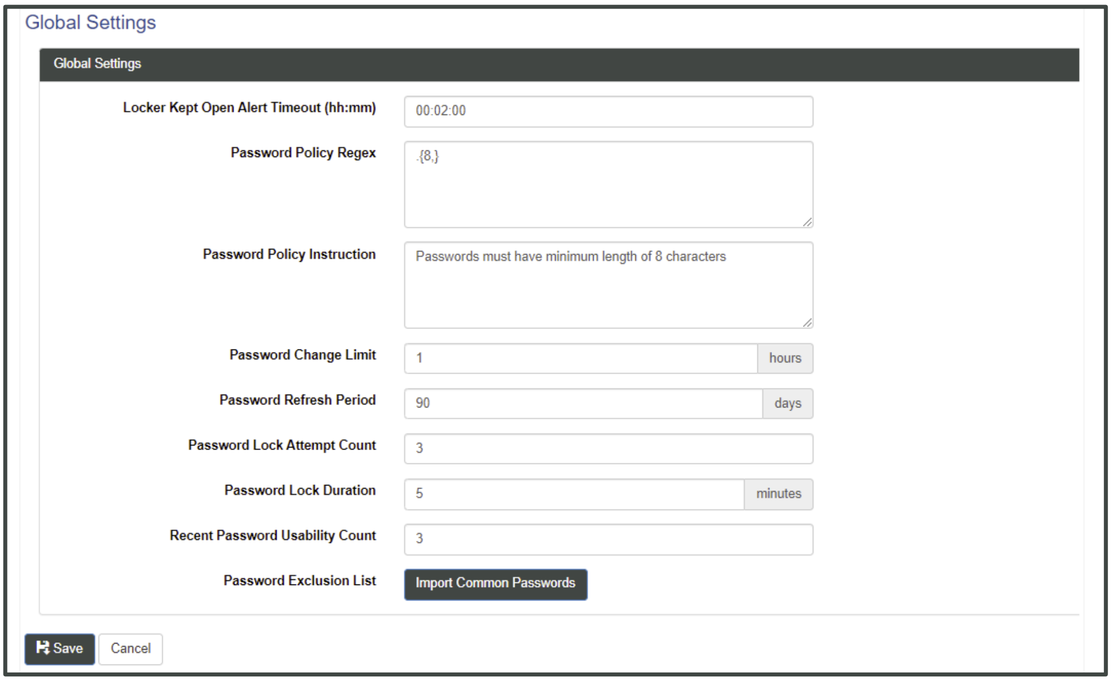
Base URL	https://demo2326224.mockable.io/ap	Username	tz
Password	••••••••••••••••••••••••••		

Set the fields on this screen as relevant for the external API endpoint and press the *Save* button. The System will then send Events as they occur to the external system. For more information, refer to the TZ Networked Day Locker Integration Spec.

4.7.8 Global Settings

The Global Settings screen contains settings for the System that are global in nature, rather than specific to each Kiosk.

This feature can be reached by selecting the *Global Settings* link from the Settings screen.



Global Settings

Global Settings

Locker Kept Open Alert Timeout (hh:mm)	00:02:00
Password Policy Regex	.{8,}
Password Policy Instruction	Passwords must have minimum length of 8 characters
Password Change Limit	1 hours
Password Refresh Period	90 days
Password Lock Attempt Count	3
Password Lock Duration	5 minutes
Recent Password Usability Count	3
Password Exclusion List	Import Common Passwords

Figure 23: Global Settings screen

The following table summarises the settings that can be changed on this screen:

FIELD	DESCRIPTION
Locker Kept Open Alert Timeout	If a Locker is left open by a User or Concierge for longer than this value, then a Locker Kept Open alert will be raised internally and output to any external integration API.
Password Policy Regex	This value defines the required regex for any entered password to validate against.
Password Policy Instruction	This value defines the message to be shown to the User if the Password Policy Regex is not satisfied when a new password is entered.
Password Change Limit	This value determines how many times in the specified period that the User is allowed to change their own password. Does not affect password update performed by Concierge/Admin when editing a User's profile. Set this to 0 to have no change limit.
Password Refresh Period	This value determines how long until a password expires, and the User is required to change it. Set this to 0 to disable password expiry.
Password Lock Attempt Count	This value determines how many times an incorrect password can be entered before the User account is temporarily locked. Set this to 0 to disable account locking.
Password Lock Duration	This value determines how long a User account is temporarily locked.
Recent Password Usability Count	This value determines how far back in password history before a previously used password can be re-used. Set this to 0 to disable password history checking.
Password Exclusion List	Press the *Import Common Passwords* button to view instructions on importing a list of common passwords that you want to enforce cannot be used

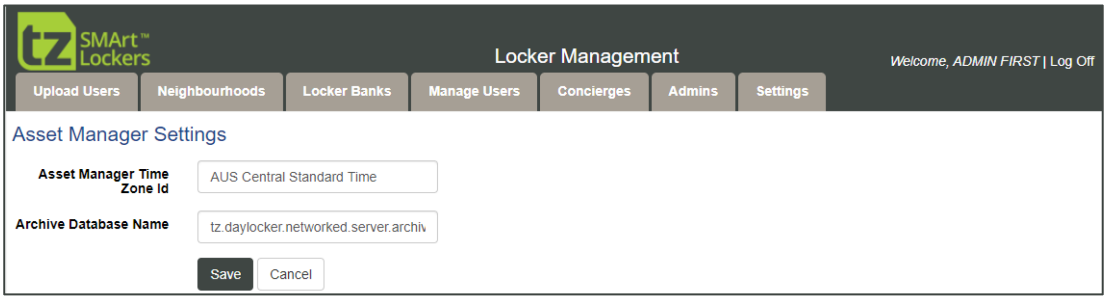
To change any of these settings:

- Edit the associated text field.
- Press the *Save* button to immediately update the value

4.7.9 Asset Manager Settings

The Asset Manager Settings screen contains settings specific for Asset Manager operation which are configurable.

This feature can be reached by selecting the *Asset Manager Settings* link from the Settings screen.



Asset Manager Settings

Asset Manager Time Zone Id: AUS Central Standard Time

Archive Database Name: tz.daylocker.networked.server.archiv

To change any of these settings:

- Edit the associated text field.
- Press the *Save* button to immediately update the value

END OF DOCUMENT