Floorsight / Floorsense / Smartalock System Architecture and Security V4.0

Abstract

An overview of the Floorsense/Floorsight system architecture and security

Sensitivity = Internal Office and General Customer Correspondence

Introduction

This document describes the data security elements present in the standard Floorsense (including Smartalock) system so as to be evaluated against a clients IT security requirements.

There are 2 types of system deployments with each having different sets of sensor devices and thus security considerations – *Floorsense* and *Floorsight*.

- *Floorsense* provides a occupancy reading for the area it is attached to providing customers with occupancy data relating to workspaces without knowing anything about the end users at each workspace.
- *Floorsight* has the same occupancy sensor, but also provides a top of desk combo RFID reader with Wireless/Wired charger. Floorsight allows end users to tag on and off workspaces with building swipe cards or smartphones. Floorsight provides customers with detailed occupancy data coupled with specific user utilization, wayfinding, location searching and more detailed reporting.
- *Floorsight with Smartalock* adds the Smartalock locker system into the Floorsight deployment which adds locker reservation and sharing to the data model associated with each user.

System Architecture Options

There are different possible locations for the control logic and client data source repository – either on premise hosted at the client site, or hosted by Floorsense in our cloud service, or a mixture option called Hybrid where an on-premise controller houses all client data and control logic, but the source of such client data (ie user names, email addresses) is located in a client cloud repo such as Azure AD / Microsoft Graph and is accessed via a SSO method.

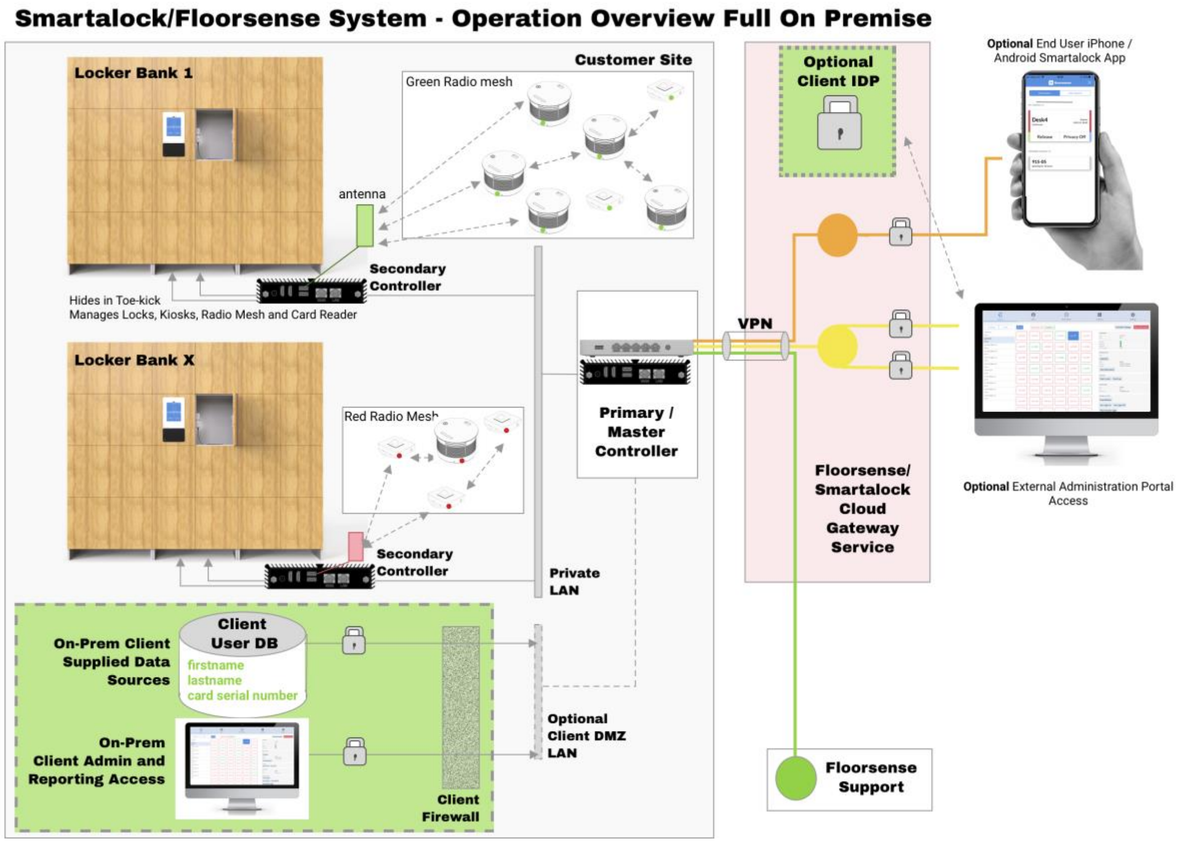
The following table summarises the differences in System Architecture options

Architecture Option	Fully On Premise	Hybrid	Cloud
Master Controller Location	On Premise	On Premise with VPN to FS Cloud	Master Controller hosted as a VM at FS Cloud (Amazon AU or NZ)
End User Database Source Options	Typically On Premise via client Firewall – SSO source is option	SSO / Microsoft Graph generated	SSO / Microsoft Graph generated

System Architecture – On Premise

The below drawing shows the typical deployment architecture and traffic flows between system components in a full Floorsense / Floorsight / Smartalock deployment where the main controller (“Master” or “Primary” controller) is physically located at the client site. Under this option if client does not wish to have end user smartphone access, the Internet VPN connection would only be used for Floorsense to provide remote support. (Green line)

No other Application traffic flows would leave the clients site. Client data such as user names and their swipe card CSNs can be introduced to the Master controller via an internal firewalled DMZ network.

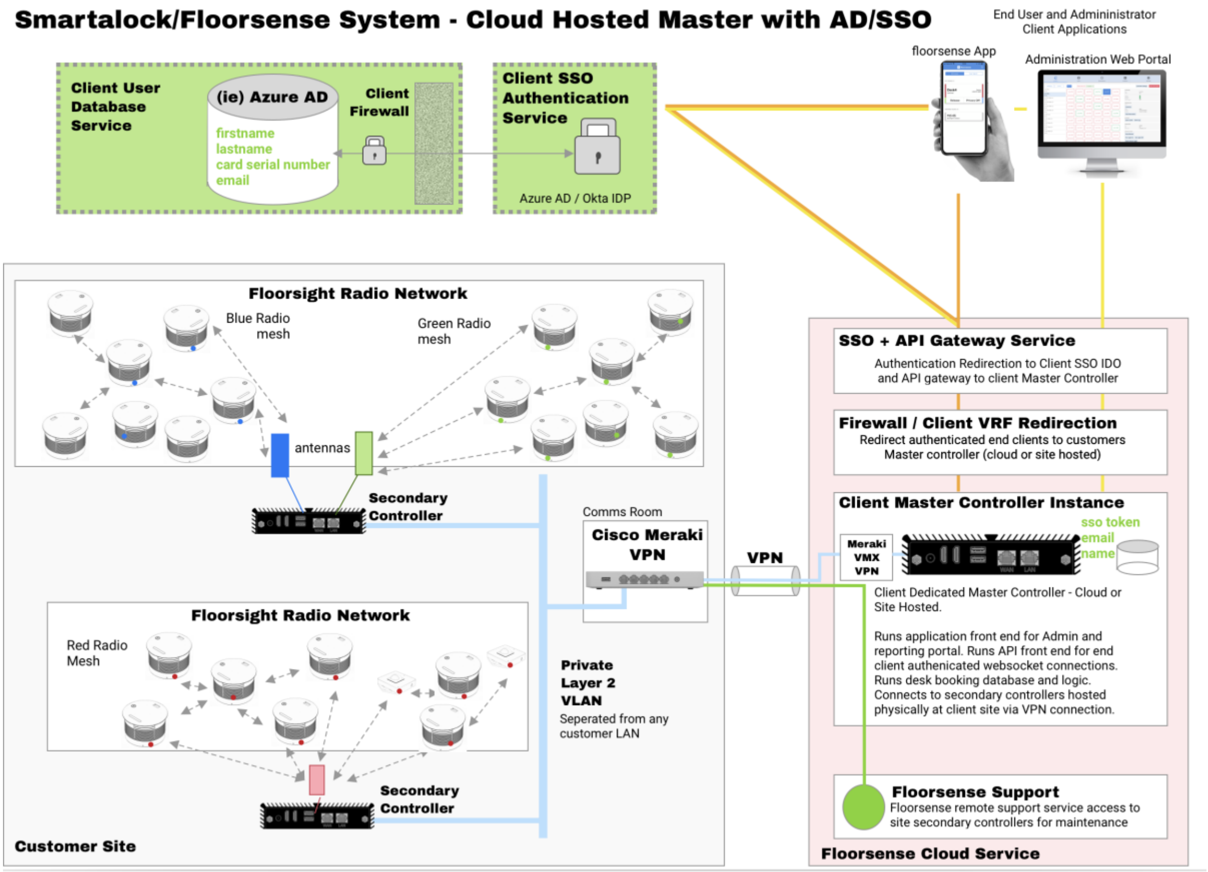

Smartalock/Floorsense System - Operation Overview Full On Premise
Locker Bank 1
Customer Site
Green Radio mesh
antenna
Secondary Controller
Hides in Toe-kick
Manages Locks, Kiosks, Radio Mesh and Card Reader
Locker Bank X
Red Radio Mesh
Secondary Controller
Primary / Master Controller
Private LAN
VPN
Optional Client IDP
Optional End User iPhone / Android Smartalock App
Optional External Administration Portal Access
Floorsense/ Smartalock Cloud Gateway Service
On-Prem Client Supplied Data Sources
Client User DB
firstname
lastname
card serial number
On-Prem Client Admin and Reporting Access
Client Firewall
Optional Client DMZ LAN
Floorsense Support

System Architecture – Cloud Hosted

Typically Cloud hosted solution moves the physical location of the Master/Primary controller to a dedicated virtual machine container hosted by Floorsense. The location of the container is dependent on the majority of the clients physical sites. For example for Australian customers the Master/Primary controller VM is hosted within Amazon AWS service in Sydney, Australia.

The typical reason for cloud hosting is where a customer has multiple sites with a shared user database between all sites, and also to improve availability and reduce dependence on the WAN link of any single site for the other sites to work.

The below drawing shows the architecture for a Cloud hosted Primary controller, with SSO as the authentication and data source from client side:



Smartalock/Floorsense System - Cloud Hosted Master with AD/SSO

Authentication Redirection to Client SSO IDO and API gateway to client Master Controller

Redirect authenticated end clients to customers Master controller (cloud or site hosted)

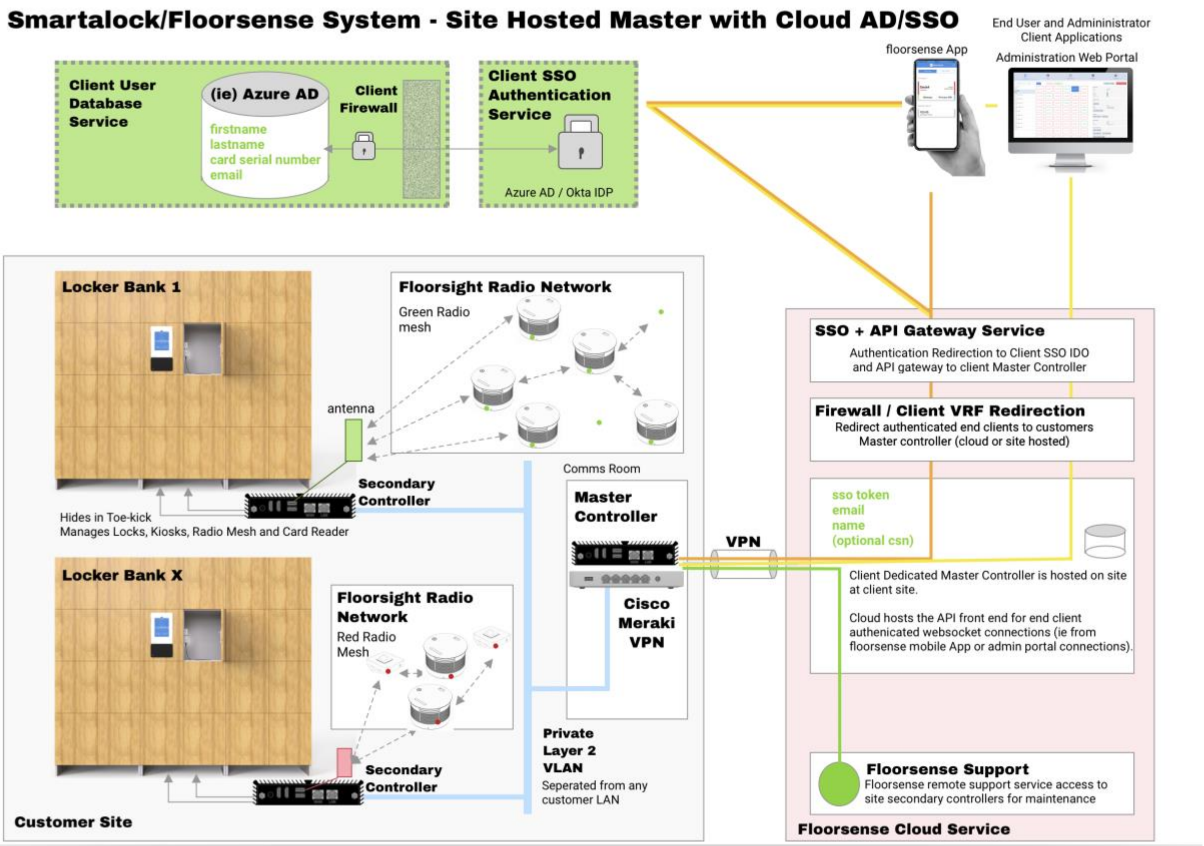
Client Dedicated Master Controller - Cloud or Site Hosted.

Runs application front end for Admin and reporting portal. Runs API front end for end client authenicated websocket connections. Runs desk booking database and logic. Connects to secondary controllers hosted physically at client site via VPN connection.

Floorsense remote support service access to site secondary controllers for maintenance

System Architecture – Hybrid

The Hybrid Architecture is practically identical to the Cloud model, however moves the Master controller function on premise such that the Client has more control and is not dependent on the Internet operating for reservation functions to operate. This model suits larger single-site customers. No on-site integration is made to any client data sources as these are still integrated with via cloud services and single sign-on.


Smartalock/Floorsense System - Site Hosted Master with Cloud AD/SSO
End User and Admininistrator Client Applications
floorsense App
Administration Web Portal
Client User Database Service
(ie) Azure AD
firstname
lastname
card serial number
email
Client Firewall
Client SSO Authentication Service
Azure AD / Okta IDP
Locker Bank 1
Floorsight Radio Network
Green Radio mesh
antenna
Secondary Controller
Hides in Toe-kick
Manages Locks, Kiosks, Radio Mesh and Card Reader
Comms Room
Master Controller
Cisco Meraki VPN
VPN
Locker Bank X
Floorsight Radio Network
Red Radio Mesh
Secondary Controller
Private Layer 2 VLAN
Seperated from any customer LAN
Customer Site
SSO + API Gateway Service
Authentication Redirection to Client SSO IDO and API gateway to client Master Controller
Firewall / Client VRF Redirection
Redirect authenticated end clients to customers Master controller (cloud or site hosted)
sso token
email
name
(optional csn)
Client Dedicated Master Controller is hosted on site at client site.
Cloud hosts the API front end for end client authenicated websocket connections (ie from floorsense mobile App or admin portal connections).
Floorsense Support
Floorsense remote support service access to site secondary controllers for maintenance
Floorsense Cloud Service

Master Controller Function

The Master controller for a Floorsense system has 3 primary functions:

1) coordination and control of all desk sensors present on a single client site (for example a desks occupancy state, LED state, USB and Qi charger states.
2) Collection and processing of desk event data for analytics and reporting.
3) Presentation front end web interfaces for administration and reporting, along with a cut-down web interface for presenting on end user touchscreen kiosks

For *Floorsight* based systems the Master controller also performs:

4) Storage of all user records and their card numbers or mobile UUIDs along with their current desk reservations (Floorsight only)
5) API front end for accepting brokered connection from Floorsense cloud from end user Smartphones running the Floorsense App. (Floorsight only)
6) For Systems that also include Smartalock, the Master controller also holds Locker reservation data and locker numbering.

Slave Controllers

A Slave controller is a cut down smaller version of the Master controller, using the same embedded appliance hardware. The Slave controller is responsible for the operation of just the portion of the sensor network that it has radio antennas for. The Slave controller on Floorsight/Smartalock system synchronizes the portions of the user database and desk / locker reservations for just the desk sensors within its part of the radio mesh or lockers it is directly connected to, and allows the system to continue to operate for these nodes in the event that the master controller fails.

As indicated the Slave/Secondary controller can also function as a Smartalock controller used in our locker system. Typically in this case the therefore the Floorsense slave and Smartalock slave controller are the same hardware and physically resides in the toekick of a locker bank, and the antenna shares the cable channel installed into the locker carcass to be placed on top of a locker bank.

Sensor Devices

There are 2 flavours of sensor devices – *Floorsense* and *Floorsight*. Floorsense provides a occupancy reading for the area it is attached to, whereas Floorsight also provides a top of desk RFID reader, Wireless/Wired charger, Bluetooth beacon for smartphone detection, LED indicator and speaker.

Both Floorsense and Floorsight however have identical communications hardware.

Each Floorsense or Floorsight sensor devices communicates via a proprietary, encrypted, low frequency radio network back to its assigned slave controller. This network is self forming and self healing based on mesh networking principles contained in the OpenThread 802.15.4 specification. In New Zealand and Australia the radio operates in the 915-928 mHZ ISM frequency band within the transmit power, interference and duty cycle limitations as set out in the each countries regulations[1][2]

Floorsense sensors regularly transmit the current occupancy state back to slave controller which in turn passes this information for the Master controller. Slave controllers can also transmit control messages to the Floorsense sensors to alter the PIR sensor configuration thresholds.

Floorsight sensors also transmit occupancy state to slave controllers, but in addition will transmit the CSN of any building swipe card presented to the integrated RFID reader as well. The slave controller can transmit a variety of control messages to Floorsight – changing the state of the LED to indicate occupied or reserved status, enable/disable the Qi wireless charger, play audio samples or alter configuration defaults.

Note that neither Floorsense or Floorsight devices store any end user data.

Floorsense Cloud Service

The Floorsense cloud performs 4 functions

- Act as reverse SSL proxy for connecting end user administrator to the Master controllers Web interface for system administration and analytics reporting.

[1] NZ: Regulation 9 of the Radiocommunications Regulations 2001 via section 116(1)(b) of the Radiocommunications Act 1989

[2] AU: Radiocommunications (Short Range Devices) Standard 2004 via subsection 162(1) of the Radiocommunications Act 1992

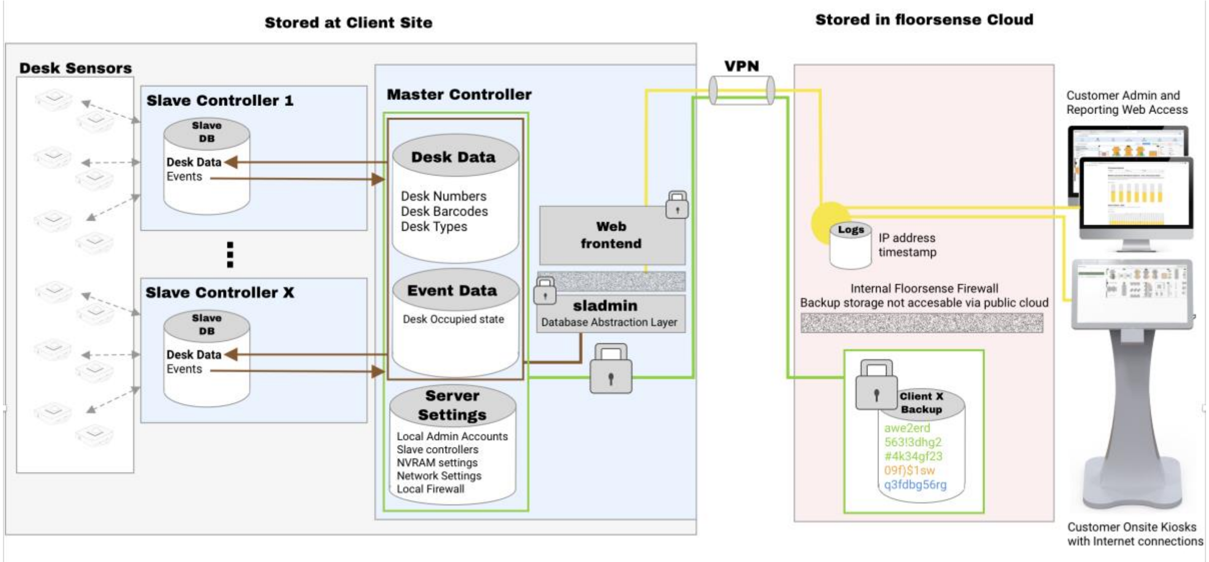
- Act as reverse SSL proxy for connecting any end user kiosk touchscreen to a cut down web based kiosk – used for end users to see a real time floorplan heatmap and find where other users are currently located
- Act as a gateway for Floorsense technical support to gain access to site Master controller for firmware updates, security patches and remote support.
- (for Floorsight only) Acts as an application gateway / firewall for connecting end user smartphones running the Floorsense App to the correct Master controller's API interface

The data communication security and customer personal information protection are documented in the sections below.

What Client Data is stored by the Floor**sense** System?

Practically no personally identifiable client data is stored either onsite or in the Floorsense cloud with a Floorsense occupancy sensor system. As per the below diagram the client data needed to support Floorsense is:

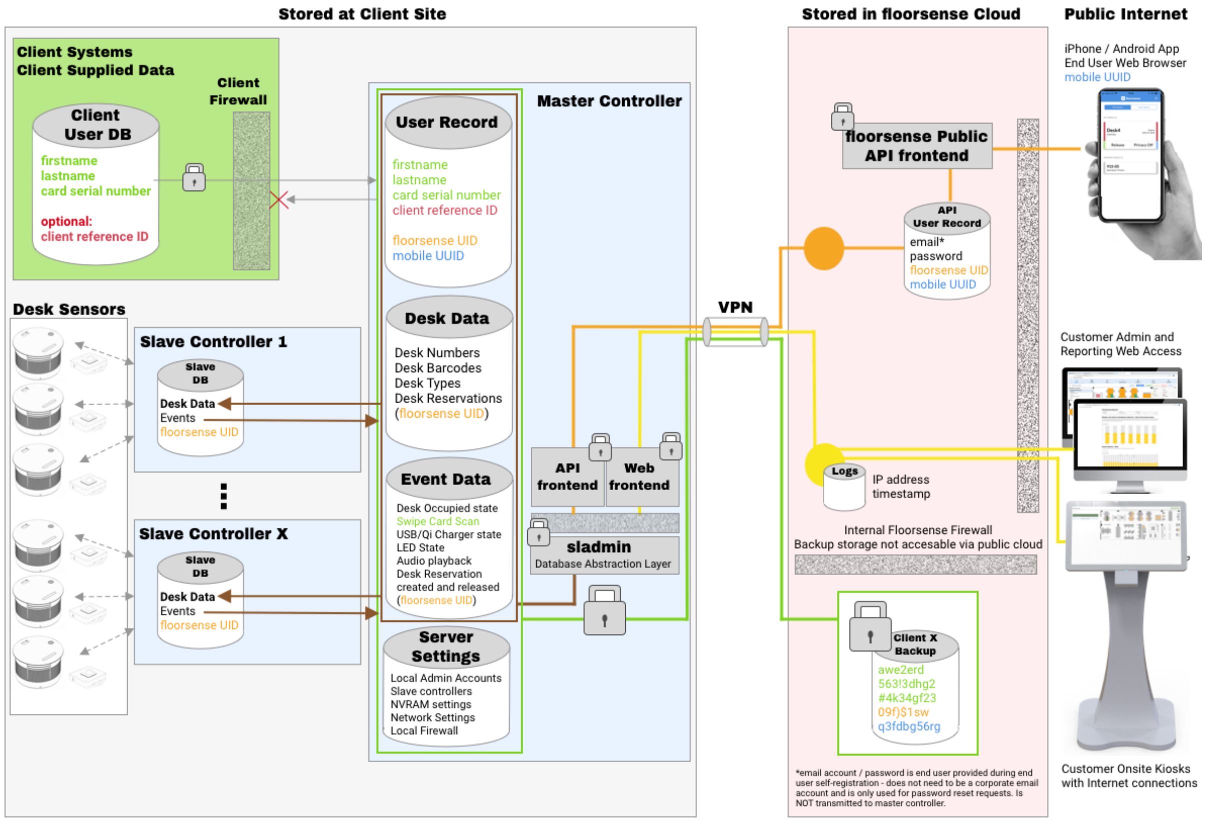
- Floorplans with identified desk numbers



What Client Data is stored by the Floor**sight** System?

The Floorsight system has the following client introduced data:

- Floorplans with identified desk numbers
- User identifiers such as firstname, lastname or alternatively a employee number
- User swipe card CSN numbers if swipe cards are used for desk reservation checkin



Method used to introduce client data

Floorsight data provided by each client is limited to end users names, email address and their swipe card serial number. Optionally the client can choose to also provide additional data for example a unique ID from their source system in order to maintain the end user record reliably (ie when more than 1 person has identical name, the Unique ID is used to update the correct record in the system)

Client data is stored in the Master controller's user database (green and red text in above drawing). These can be introduced and maintained in the system via 4 possible methods:

1) Creation manually via the Master controllers web interface, and then maintained by the same web interface
2) Imported one time at from an external client database (ie as a CSV file) during system commissioning but then adds moves and changes are performed via the Master web interface
3) Bulk Imported at the beginning via API process from external client database (ie Security card system or Printer system), and then incrementally updated via same API process.
4) Auto-generated via Single Sign On integration. As users are authenticated by Clients IDP, the authorization token contains firstname, lastname and email address. The master controller can auto-create a user with these credentials as they are authenticated.

The most secure and recommended option is 4) Single Sign On. Using this method requires no direct integration between a source system and the master controller.

In all cases the method to upload is via TLS 1.2 encrypted HTTPS method, or alternatively via secure copy (SCP). The Floorsense Master controller only accepts connection using the latest ciphers, so a modern browser and operating system should be used on the client computer.

Cloud Service Tenant Segregation

The Floorsense cloud service mitigates risk to client data via the following methods

- Restricting the client data that is stored in the cloud in the first place
- Using network and compute resource segregation for each client
- Employing robust entitlement checks on end users access to cloud services
- Segregation of customer log files into separate encrypted containers
- Pre-encrypting database backups at source prior to transmitting to the cloud, and not storing the decryption key in the cloud

Minimum of cloud hosted client data

We believe the best method to protect client data from attack is to not store it in the first place. Therefore, Floorsense stores NO client data in the cloud. Floorsight only stores the following minimal information in the cloud:

1) end user email account provided when they registered for App access (any email account, ie gmail rather than a corporate email account unless SSO is enabled)
2) end user self generated password provided during App access registration (only used if SSO is not configured – for SSO customers, no password is stored on Floorsight/Floorsense/Smartalock system)
3) the end users randomly generated Floorsense UID on the clients Master controller (end user provides this via the encrypted setup code during system registration)

This data is the minimum needed to identify and authenticate the end user, their smartphone and then associate them with the correct end client Master controller to which an encrypted web-socket is then established.

Note that the following end user data is **NOT** stored in the cloud service even if its introduced by the client into the master controller:

- The users first name or last name
- The users current or previous locker or desk reservations
- The users swipe card number
- Any statistics relating to the end users location, desk occupancy or access of system services
- Any administration details for the clients Master controller (ie logins, passwords etc)

Compute and Network Segregation

For On-Premise and Hybrid deployments all client data is naturally segregated from any other client data because it is hosted onsite on physically dedicated hardware (Master controller), and accessed via segregated VPN tunnels from our cloud service. Access to the service passes through the Floorsense cloud web application firewall which performs layer 7 inspection on all traffic prior to reaching the Master controller. For Cloud hosted master controllers each customer has their own VM segregated at network and logical layer from other cloud hosted master controllers.

Robust Entitlement Checks

Access from the Floorsense cloud service to a clients onsite Master controller is protected at multiple levels

- Access is authenticated via a combination of the end users email address, password, encrypted Master controller ID / UID, and mobile device UUID, or via Single Sign On (SSO) Once authenticated the Floorsense cloud service generates a short term access token which is used in an TLS bearer header to generate an encrypted web-socket connection to the clients Master controller via our reverse proxy
- Access is only granted for 5 minutes before the dynamically generated token expires and a new token must be generated. This prevents replay style attacks
- Access is encrypted via TLS using only latest cipher suite (ie no SSLv2 and earlier, AES256 based)
- Password policy enforces user created password meet minimum standards (Contain a mixture of Uppercase, lowercase, numbers and special characters and be over 8 characters long)

Client Segregated Data

Any data that is stored in the cloud (for example any log files sent from master controller) is segregated from other clients data by means of different encrypted containers

Client Backups Encrypted at Source

Where clients elect to allow a backup of their master controller to be stored in our cloud service, it is first encrypted prior to transmission. The encryption key is held by the client and not known to us or stored anywhere in the cloud.

Can Floorsense / Floorsight run without *any* client data?

For a Floorsense sensor only system no client data is required other than a floorplan with desk numbers such that occupancy reports are useful.

For a Floorsight sensor system that operates in purely “adhoc” allocation mode (first in first served) there is no requirement for ANY client data to be introduced to the Floorsense Master. Users can simply reserve desks using their building swipe card, the Floorsense system will use its own dynamically generated internal UID (Floorsense UID) for the end user, and bind this to the also dynamically learnt card serial number when the swipe card is first presented to a desk RFID reader.

In this mode however it will be very difficult for a client to easily recognise which end user is the owner of which desk at any point in time by their actual name – Floorsight reports on desk reservation will be via the Floorsense UID and swipecard CSN only. There will be **no** ability to use the Floorsense App to reserve a desk. This mode may still be suitable for shared desk facilities that issue swipe cards and merely want to track on which card number is currently reserving which desk.

Client Data Storage on the Master Controller for Floorsight system

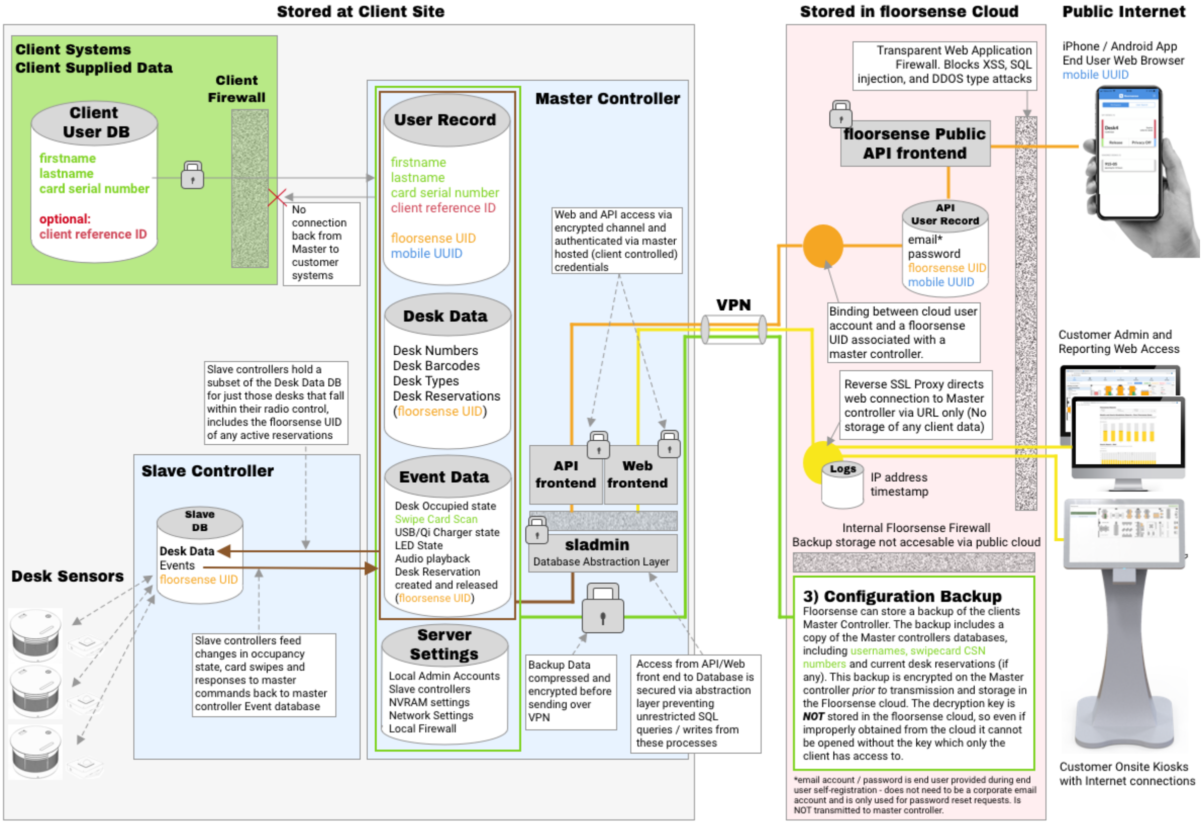
Once introduced, the client data (first name, last name, email, card number) is merged into a larger user record in the Master controller database. Additional entries in the user record include the system generated UID, along with any associated Mobile UUID learnt from cloud for this user (discussed below). The record will also hold any current desk reservations for this user.

This data is stored in the live database which is disconnected from any direct API/Web access. All interactions with the live database go through a security abstraction layer executable which restricts the types of queries and writes to the database that can be made and provides for excellent protection against typical SQL injection attacks.

Other databases on the Master controller include the Desk database and the Events database. These databases do not store any client specific data, but are linked back to a user record via the Floorsense UID.

When a user runs a report on the local web interface of the Master controller, client data records from the database maybe accessed depending on the report requested.

For example a desk utilization by user report will access the event database, desk database and user database to find all desk reservations and then reverse lookup the Floorsense UID associated with those reservations with the client firstname/lastname to make the report. The report itself is generated dynamically and streamed to the users browser in a HTTPS POST message. The report itself is never saved on the Master controller at all, and client data is not stored outside the database except for as long as it takes to run the report (1-2 seconds).


Stored at Client Site
Stored in floorsense Cloud
Public Internet
Client Systems
Client Supplied Data
Client User DB
firstname
lastname
card serial number
optional:
client reference ID
Client Firewall
No connection back from Master to customer systems
Master Controller
User Record
firstname
lastname
card serial number
client reference ID
floorsense UID
mobile UUID
Desk Data
Desk Numbers
Desk Barcodes
Desk Types
Desk Reservations
(floorsense UID)
Event Data
Desk Occupied state
Swipe Card Scan
USB/Qi Charger state
LED State
Audio playback
Desk Reservation created and released
(floorsense UID)
Server Settings
Local Admin Accounts
Slave controllers
NVRAM settings
Network Settings
Local Firewall
Web and API access via encrypted channel and authenticated via master hosted (client controlled) credentials
API frontend
Web frontend
sladmin
Database Abstraction Layer
Backup Data compressed and encrypted before sending over VPN
Access from API/Web front end to Database is secured via abstraction layer preventing unrestricted SQL queries / writes from these processes
Slave controllers hold a subset of the Desk Data DB for just those desks that fall within their radio control, includes the floorsense UID of any active reservations
Slave Controller
Slave DB
Desk Data
Events
floorsense UID
Slave controllers feed changes in occupancy state, card swipes and responses to master commands back to master controller Event database
Desk Sensors
VPN
Transparent Web Application Firewall. Blocks XSS, SQL injection, and DDOS type attacks
floorsense Public API frontend
API User Record
email*
password
floorsense UID
mobile UUID
Binding between cloud user account and a floorsense UID associated with a master controller.
Reverse SSL Proxy directs web connection to Master controller via URL only (No storage of any client data)
Logs
IP address
timestamp
Internal Floorsense Firewall
Backup storage not accesable via public cloud
3) Configuration Backup
Floorsense can store a backup of the clients Master Controller. The backup includes a copy of the Master controllers databases, including usernames, swipecard CSN numbers and current desk reservations (if any). This backup is encrypted on the Master controller prior to transmission and storage in the Floorsense cloud. The decryption key is NOT stored in the floorsense cloud, so even if improperly obtained from the cloud it cannot be opened without the key which only the client has access to.
*email account / password is end user provided during end user self-registration - does not need to be a corporate email account and is only used for password reset requests. Is NOT transmitted to master controller.
iPhone / Android App
End User Web Browser
mobile UUID
Customer Admin and Reporting Web Access
Customer Onsite Kiosks with Internet connections

Master Controller Backups

The Master controller can optionally be configured to make a backup of its databases and configuration such that should the Master controller fail, a replacement Master controller can be reinstated directly from the backup file. For a full Floorsight system, this backup file will include client data (ie firstname, lastname, email, cardnumber). The backup is stored in the our encrypted cloud facility (Amazon Australia for AU clients, Inspire.Net for NZ clients). The storage location for backups is physically segregated from any front end system, as will only be accessed by Floorsense staff in the event of disaster recovery.

The Backup file is generated by taking copies of the live databases once a day along with some other system configuration files which record for example network settings. The collection of files is then compressed and encrypted *on the Master Controller* itself using a pre-shared key NOT stored anywhere other than a Floorsense offline location. The encrypted and compressed backup file is transmitted via encrypted VPN to the Floorsense cloud service where it is stored in a client segregated storage location.

The backup storage location is not accessible via any front end web service

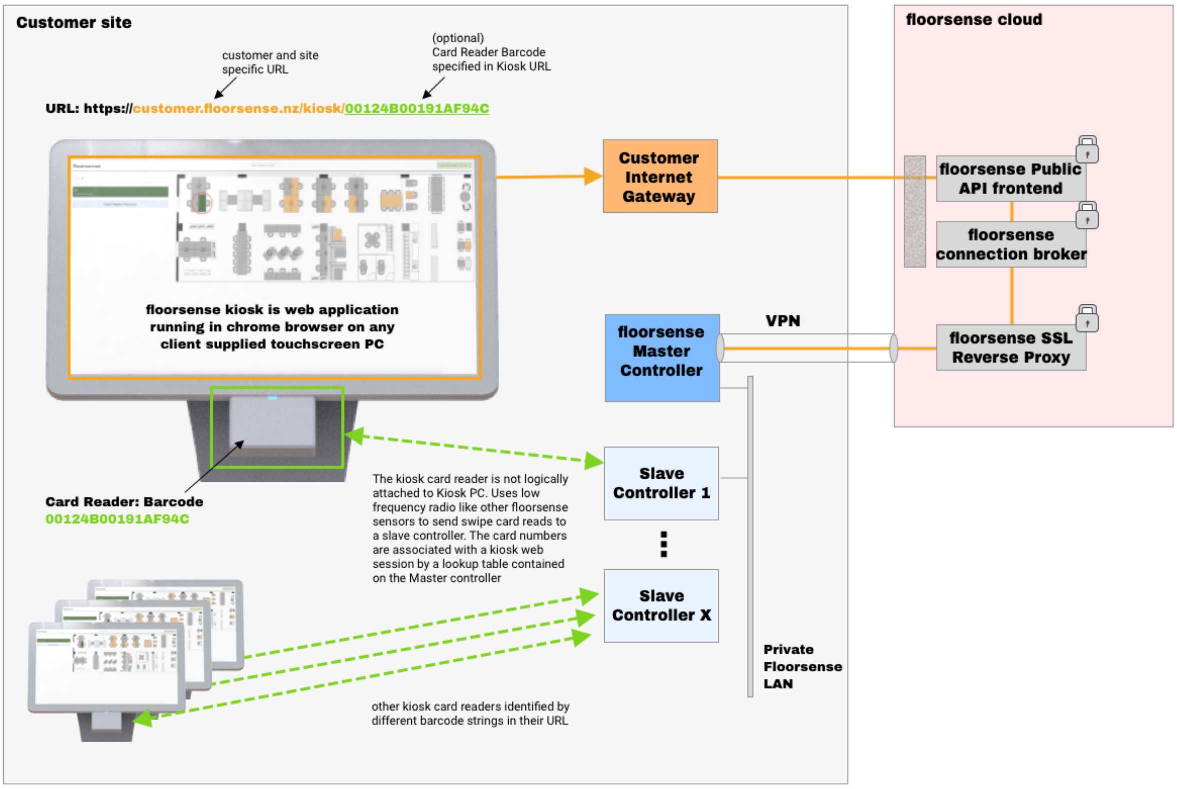
Analytics Data

The Master controller can optionally export event data (Desk occupancy state changes, card reads, reservation creations and releases) along with other system events to the Floorsense cloud service for data analysis. The event data does not contain any client data, as the only user reference included in event records is the internal Floorsense UID for the user, not the client firstname or lastname.

Upload of event data is periodic, and both encrypted via the IPSEC tunnel running between the client site and the Floorsense cloud, as well as then transmitted via TLS 1.2 encryption.

Self Service Kiosk

Both Floorsense and Floorsight systems includes the ability for end users to view the live floorplan, and with Floorsight directly pre-book desk(s) and perform other functions such as searching for other users via the kiosk web application running on a client provided touchscreen PC running the chrome browser.


Customer site
customer and site specific URL
(optional) Card Reader Barcode specified in Kiosk URL
URL: https://customer.floorsense.nz/kiosk/00124B00191AF94C
floorsense kiosk is web application running in chrome browser on any client supplied touchscreen PC
Card Reader: Barcode 00124B00191AF94C
Customer Internet Gateway
floorsense Master Controller
VPN
Slave Controller 1
Slave Controller X
Private Floorsense LAN
other kiosk card readers identified by different barcode strings in their URL
floorsense cloud
floorsense Public API frontend
floorsense connection broker
floorsense SSL Reverse Proxy

The kiosk card reader is not logically attached to Kiosk PC. Uses low frequency radio like other floorsense sensors to send swipe card reads to a slave controller. The card numbers are associated with a kiosk web session by a lookup table contained on the Master controller

The registration, authentication, and linking of a self service kiosk to a system requires the knowledge of the unique URL for the sites Master controller, which is basic authentication protected. In addition the barcode number of the card reader is needed to bind to any reader. The source IP address of kiosk connections can also be further white listed to prevent external kiosk connections from outside the client site from connecting to the Floorsense cloud.

Access from a kiosk PC to the Floorsense cloud also traverses our layer 7 web application firewall - preventing DDOS, XSS and malformed URLs from ever making it to the connection broker, reverse SSL proxy or the site Master controller.

The barcode of the attached card reader included in the kiosk URL allows the master controller to match up which kiosk web session is interested in card read events from which card reader(s). When card read events from an attached reader arrive at the master controller, AND there is a current long poll https POST from the kiosk web session waiting for a card number, then the master controller responds to the correct kiosk web session with the number allowing a desk pre-reservation to take place within the app logic.

Administration and Reporting Access

Access to the Master controllers administration and reporting web portals is typically achieved through 1 of 2 methods:

1) Via customer administrator web browser making connection to the public URL of the master controller. This connection goes via the Floorsense cloud and secured via the flow shown in the below drawing “Admin via Floorsense Cloud”. This access can also be SSO authenticated for Admin Level access.
2) Via an internally routed LAN connection between a customer browser PC and the Master controller DMZ interface. This method requires no internet access for the customer browser PC, however does require the Master controller to have a LAN connection to a customer provided firewall, and routing changes applied to the Master controller. This method is summarized in the below drawing “Admin via Direct DMZ Access”

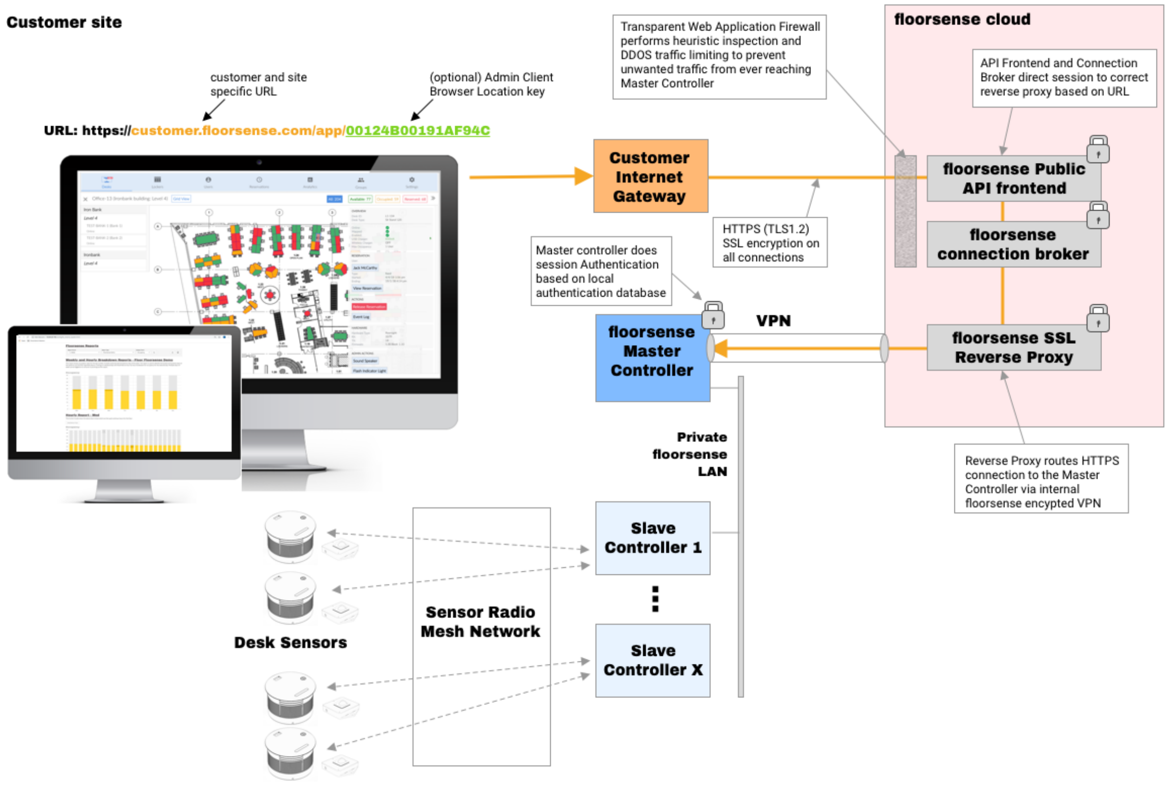

Customer site
customer and site specific URL
(optional) Admin Client Browser Location key
URL: https://customer.floorsense.com/app/00124B00191AF94C
Transparent Web Application Firewall performs heuristic inspection and DDOS traffic limiting to prevent unwanted traffic from ever reaching Master Controller
floorsense cloud
API Frontend and Connection Broker direct session to correct reverse proxy based on URL
Customer Internet Gateway
floorsense Public API frontend
floorsense connection broker
HTTPS (TLS1.2) SSL encryption on all connections
Master controller does session Authentication based on local authentication database
VPN
floorsense Master Controller
floorsense SSL Reverse Proxy
Private floorsense LAN
Reverse Proxy routes HTTPS connection to the Master Controller via internal floorsense encypted VPN
Slave Controller 1
Sensor Radio Mesh Network
Desk Sensors
Slave Controller X

Figure 1 Admin via Floorsense Cloud

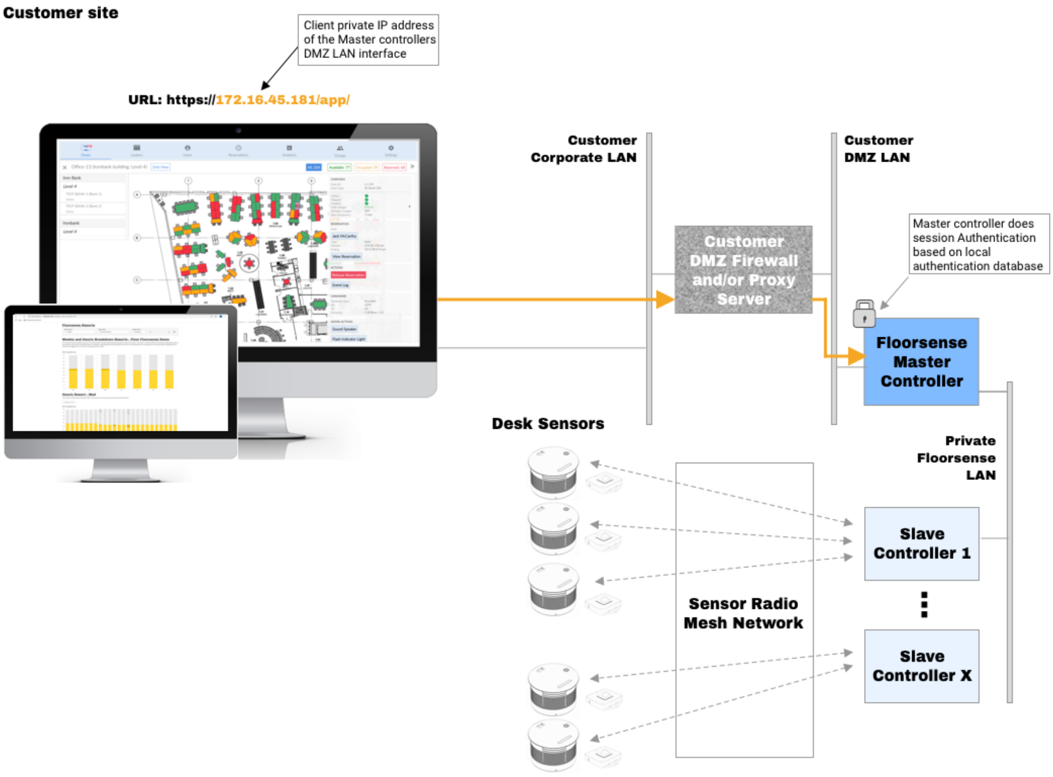

Customer site
Client private IP address of the Master controllers DMZ LAN interface
URL: https://172.16.45.181/app/
Customer Corporate LAN
Customer DMZ LAN
Customer DMZ Firewall and/or Proxy Server
Master controller does session Authentication based on local authentication database
Floorsense Master Controller
Desk Sensors
Private Floorsense LAN
Slave Controller 1
Sensor Radio Mesh Network
Slave Controller X

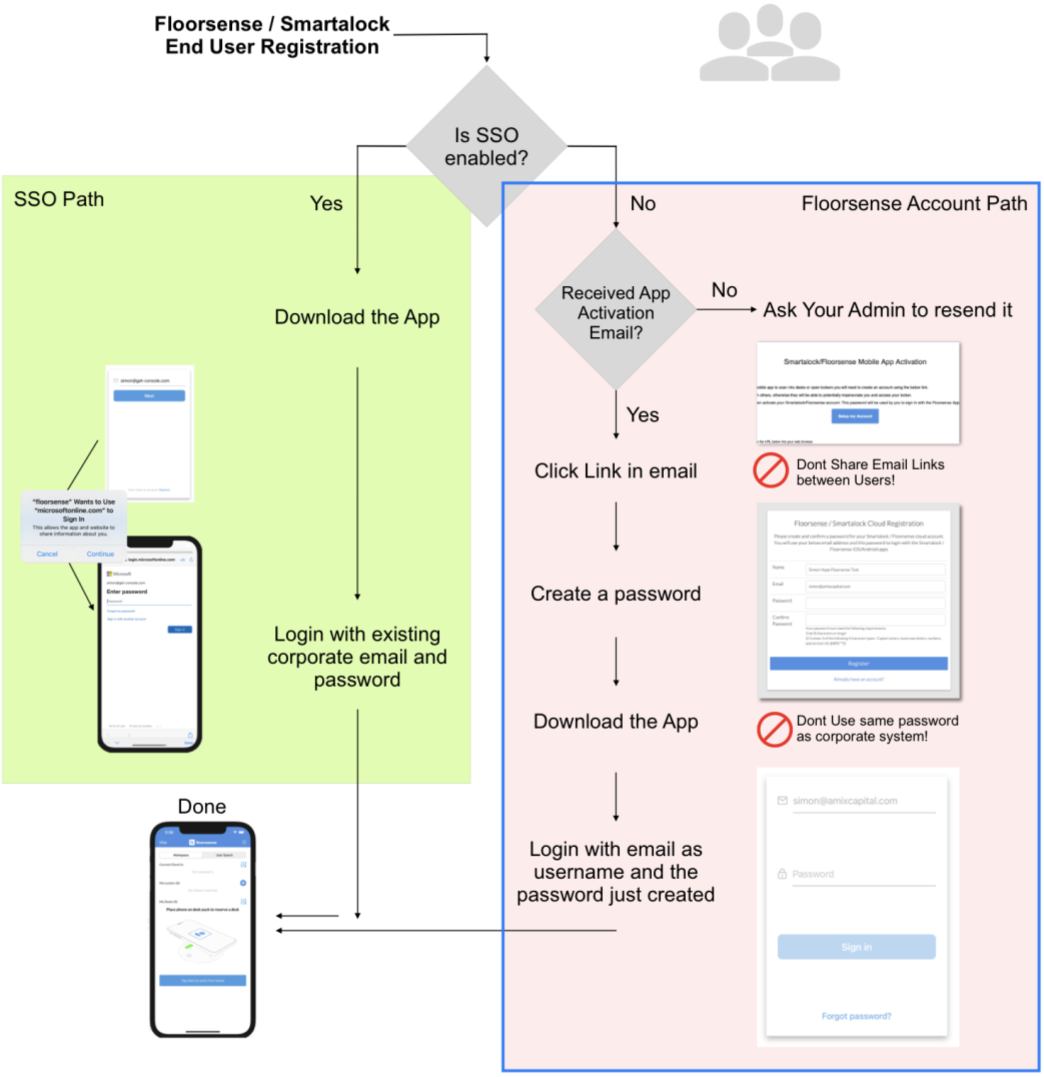
Figure 2 Admin via Direct DMZ Access

In either Administration access method however, the customer browser session is authenticated via a local authentication database stored on the Master controller. There are 2 different sets of credentials required for authentication – providing either access to the Desk administration or for providing access to the Analytics and reporting portal.

Floorsight End User Self Service Portal and Smartphone App

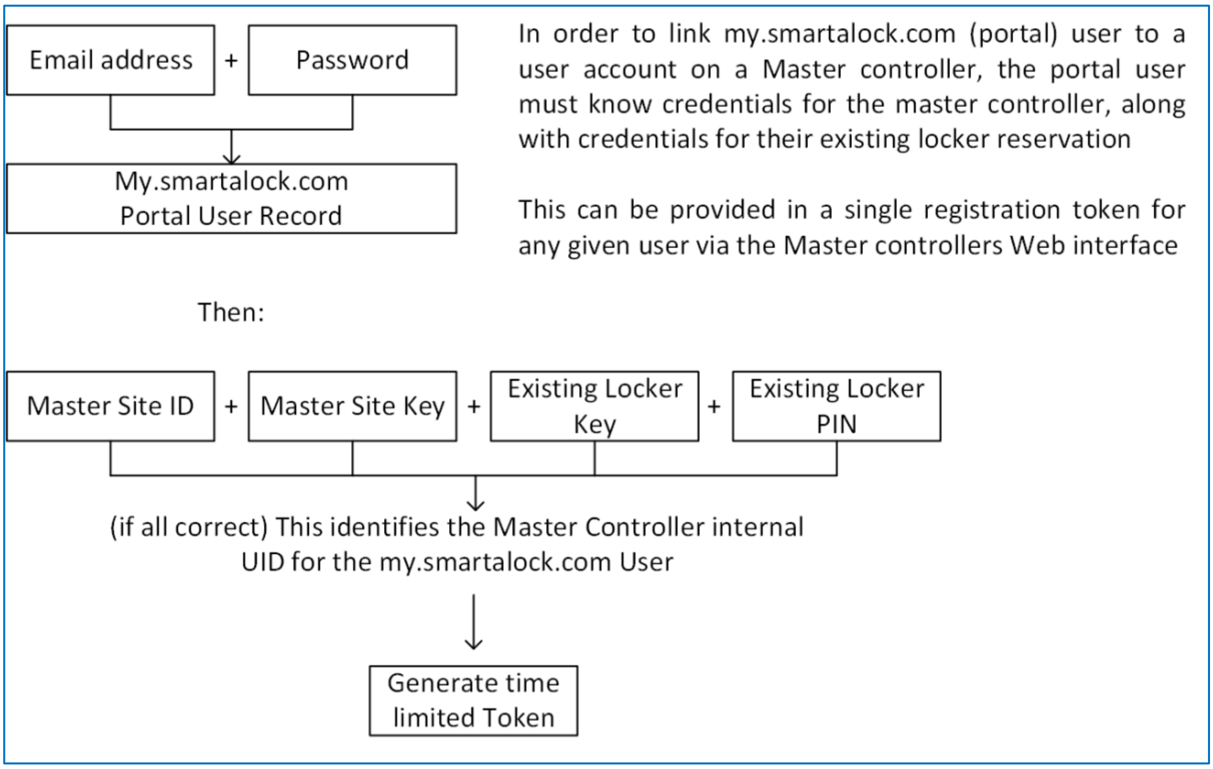
The full Floorsight system includes the ability for end users to manage the desk (and locker) lifecycle such as remotely releasing a desk and/or locker, and optionally finding other users if they have current desk reservations via either a web app or native iOS/Android App. The web app is provided via the **my.smartalock.com** / **my.floorsense.com.au** (both URLs end up at same portal) which services **both** lockers and/or desks from a single URL (regardless of whether the client has the Smartalock locker system), whereas at the time of writing the Smartphone app is specific to either desks (Floorsense) or lockers (Smartalock).

Authenticating users for App or Self Service Portal is either via SSO or via account creation at the portal itself. The following flow chart comprises the steps. SSO is preferred and more secure as no end user password is ever created, stored or transmitted to our system.


Floorsense / Smartalock
End User Registration
Is SSO enabled?
SSO Path
Yes
Download the App
Login with existing corporate email and password
"floorsense" Wants to Use "microsoftonline.com" to Sign In
Cancel
Continue
Enter password
Done
No
Floorsense Account Path
Received App Activation Email?
No
Ask Your Admin to resend it
Smartalock/Floorsense Mobile App Activation
Yes
Click Link in email
Dont Share Email Links between Users!
Create a password
Floorsense / Smartalock Cloud Registration
Register
Download the App
Dont Use same password as corporate system!
Login with email as username and the password just created
simon@amixcapital.com
Password
Sign in
Forgot password?

Non SSO Process

Prior to using either the web or native smartphone app, the non-SSO end user must self register at the my.smartalock.com website. The registration and access method is summarized in the below flow chart for Lockers. If the site is a *Floorsight only* installation without any Smartalock lockers, then the registration method requires a setup code to be provided by the system administrator before the end user can complete registration at my.smartalock.com (see Floorsight Only End User Registration below)


Email address
+
Password
My.smartalock.com Portal User Record
Then:
Master Site ID
+
Master Site Key
+
Existing Locker Key
+
Existing Locker PIN
(if all correct) This identifies the Master Controller internal UID for the my.smartalock.com User
Generate time limited Token

In order to link my.smartalock.com (portal) user to a user account on a Master controller, the portal user must know credentials for the master controller, along with credentials for their existing locker reservation

This can be provided in a single registration token for any given user via the Master controllers Web interface

Access to the my.smartalock.com portal is always via https (TLS 1.2) regardless of whether the method is the native iOS / Android App or via a web browser.

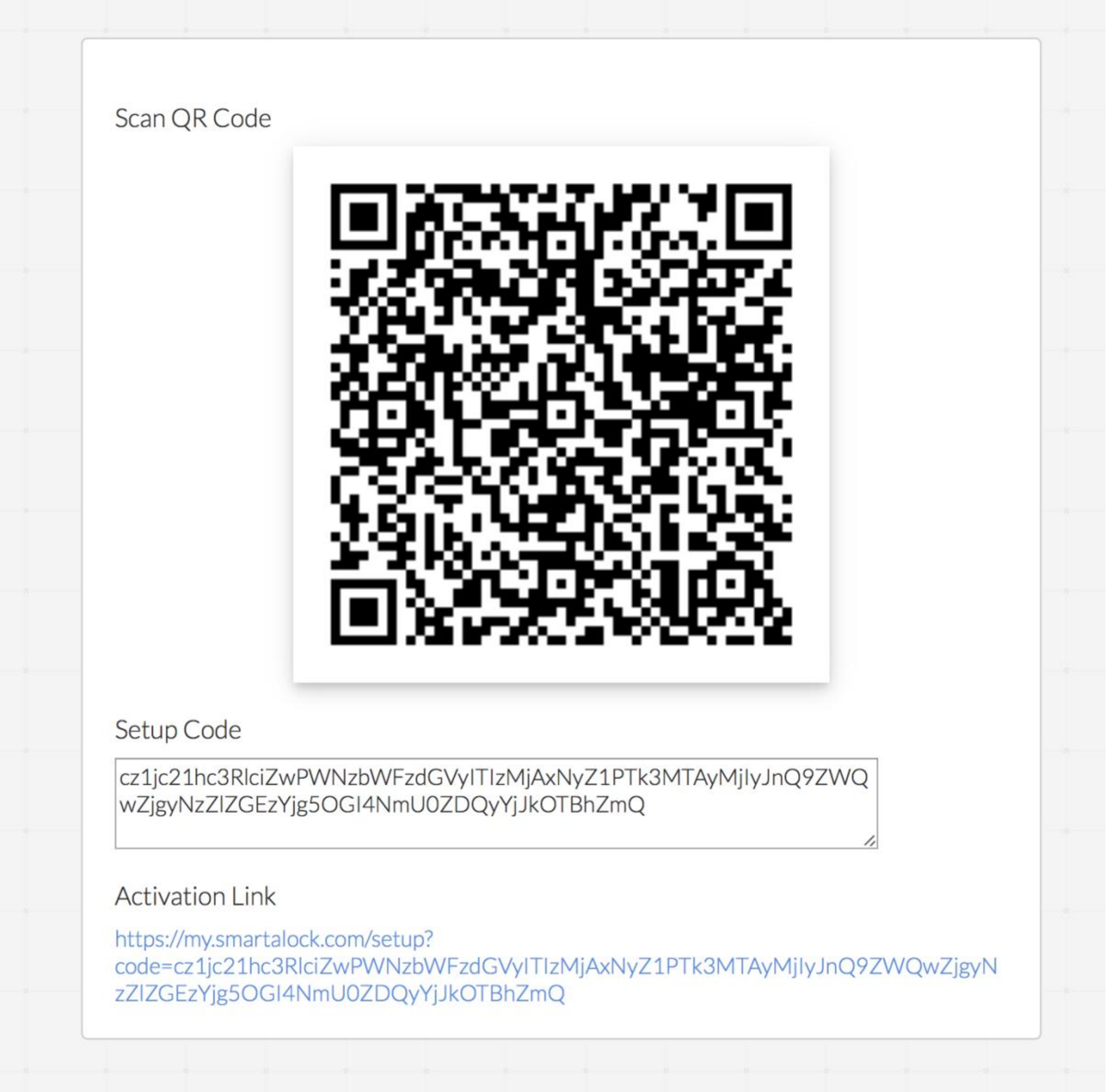
The my.smartalock.com credentials are created by the user at first visit to this self-service portal site. They are never transmitted to any Master controller and are stored in an encrypted database within the Floorsense/Smartalock cloud. The credentials consist of an email address and user selected password. The email account does not have to relate to any email account that the end user uses as employee, nor does the password need to match any other password the user may use on a client system. The email account is however verified prior to login to prevent spam accounts being created.

An end users my.smartalock.com account is linked to a particular clients Master controller and user record on that Master controller via a validation process which can be either automatic or manually approved by the client.

For automatic validation, the user must have an existing locker on a Smartalock locker bank (or an existing desk reservation) and also know the Master controllers site key and secret key which are visible from the Master controllers web interface only (also embedded as a QR code that end user can scan). The Master controllers site key and secret are the first part of linking a my.smartalock.com user to a particular master controller, and then to link to an actual user record on the master controller, the end user must know their locker number and PIN number for that locker.

Floorsight Only End User App Registration

To ease the enrolment for a large number of non-SSO portal users *or* for sites that have Floorsight only (so cannot provide a locker number / PIN), The complete combination of the master controller credentials + a single end users UID credentials can be encoded into a single (user unique) setup token which can be generated by the master controllers web administration interface. The token is embedded in a QR code for scanning into the Floorsight/Floorsense App, or alternatively presented as a URL or code that can be cut and pasted into the my.smartalock.com portal after registration.



Scan QR Code

Setup Code

cz1jc21hc3RlciZwPWNzbWFzdGVyITIzMjAxNyZ1PTk3MTAyMjIyJnQ9ZWQ
wZjgyNzZlZGEzYjg5OGI4NmU0ZDQyYjJkOTBhZmQ

Activation Link

https://my.smartalock.com/setup?
code=cz1jc21hc3RlciZwPWNzbWFzdGVyITIzMjAxNyZ1PTk3MTAyMjIyJnQ9ZWQwZjgyN
zZlZGEzYjg5OGI4NmU0ZDQyYjJkOTBhZmQ

For manual validation, a super user from the client may login and approve requests from users to be linked to the master controller. No access through to a master controller is allowed by default.

As can be seen, no actual client provided data (firstname, lastname, card serial number) is ever passed through or ever known the my.smartalock.com portal, nor can this data be manipulated or changed via the portal.

If a portal user is successfully linked to a master controller UID, a time limited access bearer token is created. Using this token, the portal website effectively acts as a transparent proxy for API requests made by the my.smartalock.com or App user through to the correct master controller. The access token is periodically renewed via secure method (not discussed) which provides anti-replay protection.

The client administrator is able to remotely revoke any existing bindings between a master controller and the my.Floorsense.com portal at anytime.

Floorsense/Floorsight Internet Requirements

As per the previous sections above, the Master controller connects to the Floorsense cloud service via encrypted VPN. Depending on the deployment model, the VPN service runs either between the Master Controller itself using the OpenVPN protocol or via a dedicated Cisco Meraki VPN appliance installed at the site and terminates on the closest Floorsense Cloud VPN gateway hosted in country. This requires an Internet connection provided by the client that is **VPN Friendly**.

Should the client provided Internet connection be logically routed through intermediary firewalls and/or other client controlled appliances that inspect or manipulate the data packets from the Floorsense Master controller, this can cause the VPN to not connect or become unstable.

Internet Presentation

The VPN appliance (Cisco Meraki) or Master controller have a 10/100/1000 copper ethernet port for connecting to the Internet. Neither of these appliances can reliably connect to a Guest WIFI network that has Internet access directly via WIFI. If the only practical way to provide Internet at a site is via Guest WIFI, then customer should also provide a WIFI/Ethernet bridge so that the presentation to Floorsense equipement is via Copper.

What is VPN Friendly?

The following details technical requirement for routers, firewalls, transparent proxies and other client devices that may impact the reliable operation of the Floorsense Cloud connection

Internet Proxies

The Floorsense cloud connection (VPN service) cannot be proxied either at layer 3 or layer 2. When the Internet connection is being routed through a proxy server (such as Bluecoat, F5 etc), then https proxy/inspection should be disabled to allow the VPN establishment and tunnelled packets to reach the Floorsense cloud service without any modification.

Firewall / Router Packet Modification

The following have been known in the past to interfere with the Cloud connection:

- IP MTU modification. The client network equipment should not do any IP MTU modification of packets to or from the Floorsense cloud. Examples include changing the DF bit on packets or modifying the TCP Maximum Segment Size (MSS) on the establishment TCP SYN packet.

- TCP Sequence Number Randomization. Some client firewalls when performing inspection or NAT will randomize and rewrite the TCP sequence number of the outgoing VPN packet from the Master controller to Floorsense Cloud VPN gateway. This can interfere with the VPN tunnel establishment and ongoing operation. Firewalls such as the Cisco ASA will do TCP randomization on sequence numbers even when NOT performing any IP NAT translation. This should be disabled for traffic from the Master controller.

- Performing multiple many-to-1 IP NAT translations on the VPN traffic. The VPN connection can handle NAT as the VPN connection is always initiated from the internal Master controller towards the Floorsense cloud, however more than 1 chained NAT connection where the VPN tunnel has to traverse multiple NATs (where each NAT is doing an overload where many internal IPs are sharing a single outside IP) then this can break VPN tunnel establishment. Multiple 1:1 NAT translations are acceptable.

- Silent TCP Resets of tunnel traffic with an aggressive TCP idle time. When the VPN tunnel is established, if the intermediary client firewall believes the TCP connection is idle and tears it down silently it will cause 1-way connectivity issues and intermittent performance issues with Floorsense App users. TCP idle time should be set to 3600 seconds.

IP Addressing

By default Floorsense devices run a DHCP client to obtain an IP address from the customers Internet router. Static IP addressing is also possible by request. Note that if the customer provides an WIFI/Ethernet bridge, some Wireless controllers will ignore the DHCP address request from Floorsense devices as it originates from a different or second MAC address from the WIFI bridge.

Required Ports on Internet Firewall

Where the connection between the Floorsense Master controller and the Floorsense cloud service will traverse a customer firewall the following table identifies the IP addresses and TCP/UDP ports that are required to be open from *inside to outside*. Note that NO ports are required to be open directly from the outside (internet) into the inside (Floorsense VLAN).

Source_IP	**Destination_IP**	**Ports**	**Protocol**	**Direction**	**Description**
Your network that provides internet to Floorsense Master Controller	108.161.147.0/24, 199.231.78.0/24, 209.206.48.0/20	7734	TCP	outbound	Backup firmware downloads
Your network that provides internet to Floorsense Master Controller	209.206.48.0/20	7752	TCP	outbound	Throughput tests live tool

Your network that provides internet to Floorsense Master Controller	108.161.147.0/24, 199.231.78.0/24, 64.62.142.2/32, 209.206.48.0/20	7734	TCP	outbound	Backup configuration downloads
Your network that provides internet to Floorsense Master Controller	209.206.48.0/20	80	TCP	outbound	Backup Meraki cloud communication
Your network that provides internet to Floorsense Master Controller	209.206.48.0/20	80, 443	TCP	outbound	Meraki Splash pages
Your network that provides internet to Floorsense Master Controller	199.231.78.0/24, 108.161.147.0/24, 64.62.142.12/32, 209.206.48.0/20	7351	UDP	outbound	Meraki cloud communication
Your network that provides internet to Floorsense Master Controller	199.231.78.0/24, 64.156.192.245/32, 108.161.147.0/24, 209.206.48.0/20	9350	UDP	outbound	Meraki VPN registry
Your network that provides internet to Floorsense Master Controller	Any	123	UDP	outbound	NTP time synchronization
Your network that provides internet to Floorsense Master Controller	8.8.8.8/32	53	UDP	outbound	Meraki Uplink connection monitor
Your network that provides internet to Floorsense	8.8.8.8/32, 209.206.48.0/20		ICMP	outbound	Meraki Uplink connection monitor

Master Controller					
Your network that provides internet to Floorsense Master Controller	203.114.130.32/30		IP	outbound	VPN tunnel to Floorsense Cloud
Your network that provides internet to Floorsense Master Controller	121.79.226.232/28		IP	outbound	VPN tunnel to Floorsense Cloud
Your network that provides internet to Floorsense Master Controller	121.79.251.204/32		IP	outbound	VPN tunnel to Floorsense Cloud