lilitab

lilitab KMS
and
SMARTDOCK

User Guide
v3.51

Lilitab LLC
39B Larkspur Street
San Rafael, CA 94901
Phone: (888)705-0190
support@lilitab.com

Contents

Introduction

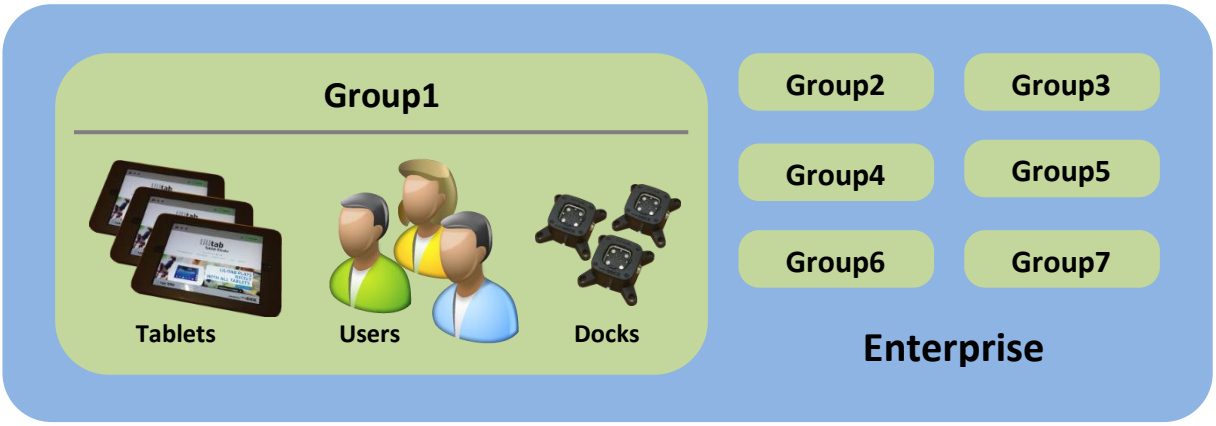
Welcome to Lilitab Kiosk Management System, or **Lilitab KMS**. Lilitab KMS is a cloud-based, enterprise-class kiosk management system, which provides both local and corporate managers with visibility throughout their kiosk deployment.

Lilitab KMS:

- Administers system resources, user accounts, and provides diagnostic data about the health and performance of the kiosk infrastructure.
- Manages and administers SmartDOCK deployments in multiple-user environments, providing a chain of custody for mobile assets.
- Collects statistical metrics generated by the deployer's business application, integrates them with the kiosk deployment structure, and reports performance by group, region, and category.
- Provides enterprise-wide administration and visibility through a cloud-based portal, accessible by internet browser from anywhere.

System Overview

A Lilitab KMS system collects multiple **tablets**, **docks**, and **users** into **groups**. Multiple groups, in turn, are organized in an **enterprise**.



Within each group, all elements interoperate freely – any user can use any tablet with any dock. A group might correspond to a single business location or perhaps a department at a location. Each group is independently configurable, and can be locally administered.

All groups also report to an enterprise. Corporate administrators with enterprise-level permissions have visibility of all group data, can organize groups by category and region, can set enterprise-wide policies, and can drill down into each group to interrogate and maintain all elements of the system.

Setting Up the Mount

The instructions below relate to setting up a Picture Mount SmartDOCK. Other mount systems are similar. Please refer to the installation instructions that came with your mount.

Step 1: With the SmartDOCK held level and at the desired height, mark the location of each mounting hole on the mounting surface.

Step 2: Drill pilot holes of the prescribed size for each of the mounting holes.

Step 3: Select mounting hardware appropriate for the material from which the mounting surface is made. Simple wall anchors (shown) are recommended for wallboard. The holes in the Picture Mount are 0.2" (5.1mm) in diameter. A #8 x 1.25" screw is recommended for most installations.

Step 4: With holes drilled and (as appropriate) anchors placed, position the SmartDOCK and screw it securely to the wall.

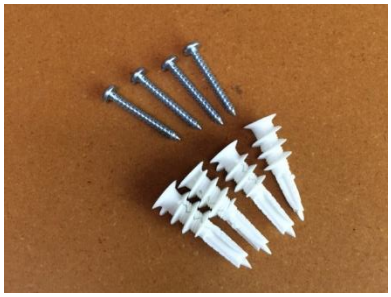
Step 5: Plug the USB charging cable that protrudes from the mount into a 12W (5V @ 2.4A) power supply. Lilitab recommends using the Apple 12W USB Power Adapter.

A few seconds after it is plugged in, the SmartDOCK will cycle itself to self-test and let you know it is ready for use.

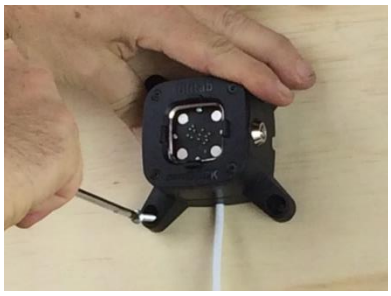
Step 1:

Step 2:

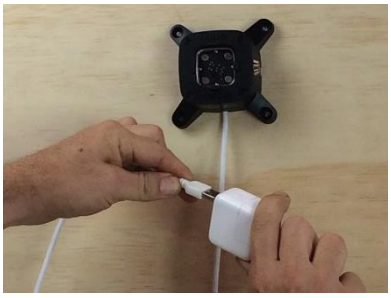
Step 3:



Step 4:



Step 5:



Launching the App

Step 1: Before closing the head unit, plug the lightning connector into the tablet. If you are using a SmartDOCK, the lightning connector should have an orange overmold. If you are using a regular MagDOCK, the lightning connector should have a black overmold.

Step 2: Install the "Lilitab KMS" app (available free in the App Store) and launch the app. You do not need to dock the tablet in the mount to launch the app.

Step 3: If this is the first time the app has been launched, you will be directed to the Registration Wizard to register the tablet. The Registration Wizard will guide you through the process of creating a new enterprise and/or group and adding a tablet to that group. For step-by-step instructions in using the Registration Wizard, see **page 9**.

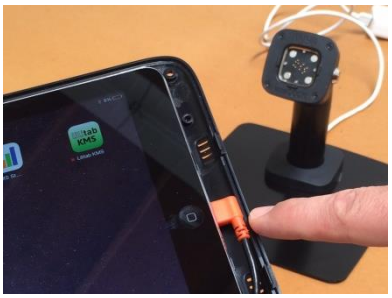
If you haven't already, you may set the head on the SmartDOCK. The dock will automatically lock itself and, if the dock is new to the group, you will then be asked to register the dock. For step-by-step instructions in using the Dock Wizard, see **page 12**.

Step 4: When tablet registration is complete, the app will open onto the home page. To unlock the SmartDOCK, press the "Press to Unlock" button in the upper right corner to bring up the PIN Pad.

Step 5: To unlock the tablet, first enter your 3-digit UserID using the keypad or by showing your badge to the camera. If requested, then provide your 4-digit PIN. If a valid PIN is entered, the SmartDOCK will unlock and the green "Unlocked" icon and message will appear. The head unit may now be removed from the SmartDOCK.

For more details on how to unlock the head unit, either using a Pin Pad or a QR Code, please see **page 13**.

Step 1:

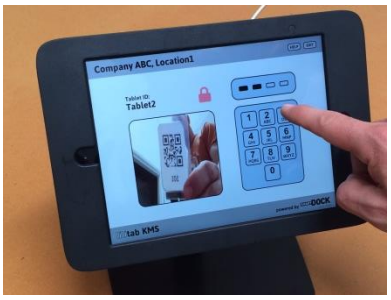


Step 2:

Step 3:

Step 4:

Step 5:



Accessing the Admin Portal

From the app:

Step 1: Pull the tab in the upper right corner down to expose the KMS header and footer.

Step 2: Press the "Lilitab KMS" logo at the right end of the footer. This will take you to the portal login screen.

Step 3: Log in to the portal by providing your admin Username and Password.

Step 4: Upon successful login, you will arrive in the dashboard for the group to which the tablet is registered. If you have enterprise admin credentials, you may exit the group to access the enterprise dashboard.

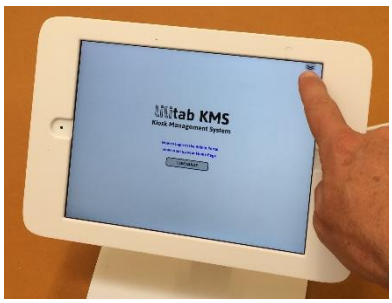
From a browser:

Step 1: Open any browser and go to "https://kms.lilitab.com".

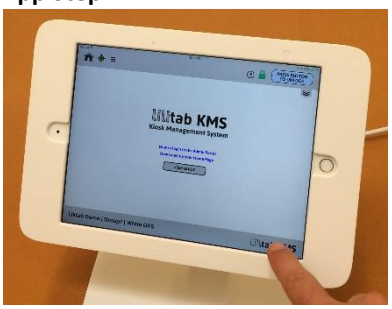
Step 2: At the login screen, enter the Enterprise ID, along with your admin Username and Password.

Step 3: Upon successful login, you will enter the portal. If you have enterprise credentials, you will start at the enterprise dashboard. If you have group credentials, you will start in your group.

App Step 1:



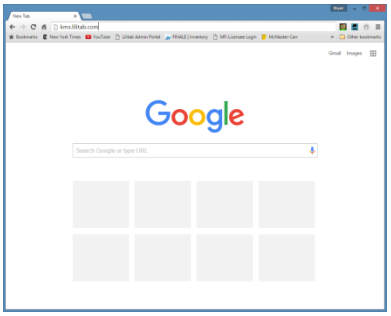
App Step 2:



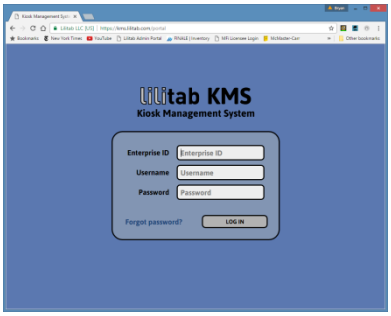
App Step 3:

App Step 4:

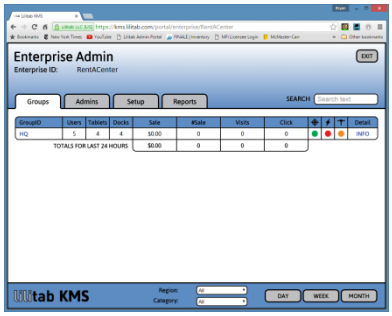
Browser Step 1:



Browser Step 2:



Browser Step 3:



System Setup

The first step in setting up a Lilitab KMS deployment is to specify the EnterpriseID, GroupID, and TabletID for each device. These attributes identify the device in the organization, and group devices for shared access.

Registration Wizard

When the Lilitab KMS app launches for the first time after being installed, it will open into a registration wizard. The registration wizard guides and assists the user in setting up a new deployment. The registration wizard can be used in any of the new-tablet configuration scenarios:

- **Setting up a new enterprise**
- **Creating a new group within an enterprise**
- **Adding a tablet to an existing group**

When the registration wizard opens, it prompts the user to enter an Enterprise ID, Group ID, and Tablet ID.

These parameters identify the unique “coordinates” to which the tablet will be registered. These coordinates locate the tablet in the KMS network and are used to segment access to the device and data.

If you are setting up a tablet for the first time, you may want to contact your system administrator, who will provide you with your Enterprise ID and Group ID.

Creating a New Enterprise

If this is the very first tablet in your company to use Lilitab KMS, you will need to create a new Enterprise ID for your company.

Generally, the person to create a new Enterprise ID will be a corporate system administrator, as they will become the Agent (primary contact) for the corporate enterprise account.

Of course it's fine for anyone to create a new enterprise account, even just to experiment. Administrative responsibilities for the enterprise can be transferred to another person at a later time.

To create a new Enterprise:

Step 1: Enter (or confirm) the Enterprise ID, Group ID and Tablet ID on the first screen of the registration wizard. If the Enterprise ID provided is unique, the wizard will confirm that your intent is to create a new enterprise and group.

Step 2: After confirming that you are creating a new enterprise you will next be asked to provide the full name, email, and phone number of the primary administrative contact for the enterprise account. Then specify whether you would like to use email or text message for confirmation. Email and phone (text message) are used for second-channel authentication.

Step 3: After entering the confirmation code that you receive in email or text message, supply a username and password. The username and password will be used to access the admin portal.

Step 4: After providing username and password, you will also be asked for password recovery questions and answers, should you need to recover your password. Then you will be asked for the enterprise business address.

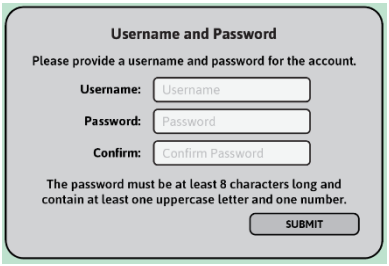
Step 5: If you are using SmartDOCKs, you can next set up a User ID and Unlock PIN to use to unlock tablets in the initial group from docks in that group. An unlock badge, that can be used with the tablet camera, can be texted to the agent phone number. If not using SmartDOCKs, you can skip this step.

Step 6: Finally, you will have the option to set up credit card payment now or answer a three-question survey and set up payment later. In either case, the new enterprise will start a one-month period during which to try out all KMS features free of charge.

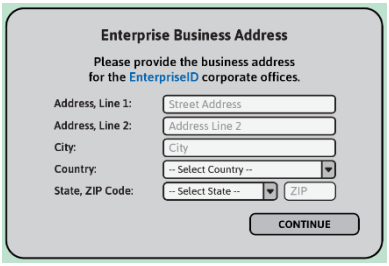
Step 1:

Step 2:

Step 3:

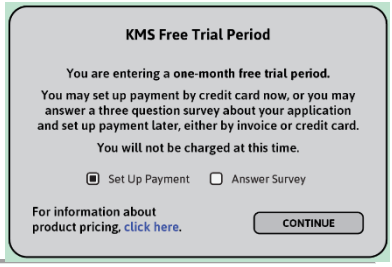


Step 4:



Step 5:

Step 6:



Creating a New Group

In Lilitab KMS, the Group refers to a local network of kiosks, generally all existing in the same business location. Each enterprise will have multiple groups, one at each location, and each group reports to the enterprise.

Members of a Group ("Users") may use their UserID and PIN to unlock any tablet in their Group from any dock. Any transactions which occur within a group will be associated with that group when reported in the enterprise portal.

Generally, a new Group can be created ad-hoc and on-site using the tablets in that group. The primary group administrator is called the group "Owner". This person could be the store manager or local IT specialist.

To create a new Group within an existing Enterprise:

Step 1: Enter an existing Enterprise ID and new Group ID on the first screen of the registration wizard. If the Enterprise ID provided matches an existing enterprise, the wizard will confirm that your intent is to add a new group to that enterprise.

Step 2: After confirming that you are creating a new group in an existing enterprise, you will next be asked to provide the full name, email, and phone number for the group owner. Group owners have portal access (for their group only) to administer the group's assets and view group-level reports. Then specify whether you would like to use email or text message for confirmation. Email and phone (text message) are used for second-channel authentication.

Step 3: After entering the confirmation code that you receive in email or text message, supply a username and password. The username and password will be used to access the admin portal at the group level.

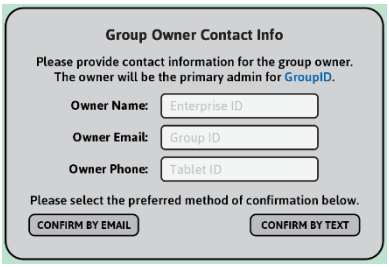
Step 4: After providing username and password, you will also be asked for password recovery questions and answers, should you need to recover your password. Then you will be asked for the group business address.

Step 5: If SmartDOCKs will be used in the group, you can next set up a User ID and Unlock PIN for the group owner to use to unlock tablets in the group. An unlock badge, uasble with the tablet camera, can be texted to the group owner phone number. If not using SmartDOCKs, you can skip this step.

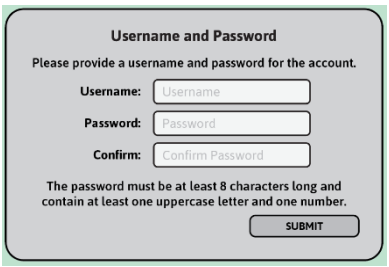
Step 6: Group creation is now complete. You may now exit to the app, where you can add additional accessories, for example, or to the portal, where group settings may be configured or modified.

Step 1:

Step 2:



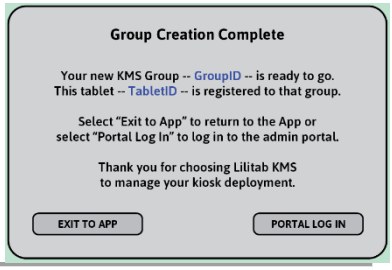
Step 3:



Step 4:

Step 5:

Step 6:



Adding a Tablet to a Group

Once an enterprise and one or more groups have been created, additional tablets can easily be added to a group.

To add a new Tablet to an Existing Group:

Step 1: Enter the Enterprise ID and Group ID of the Group to which the tablet will be added. Provide a Tablet ID.

Step 2: If the Enterprise ID and Group ID entered match an existing enterprise and group, you will next be asked to confirm that it is your intent for the tablet to join the group.

Step 3: To authorize the addition of the new tablet to the group, enter the credentials of the group owner (or any enterprise admin).

Release Tablet: If a tablet is registered in KMS to a different group (and is active in that group) an enterprise admin or owner from the group to which it is registered will need to provide credentials to release the tablet from that group.

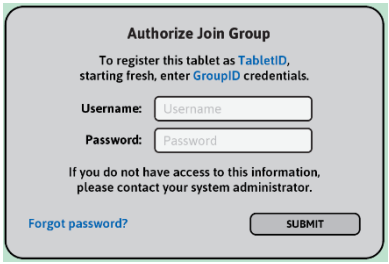
Bring or Leave Data: If a tablet is registered in KMS and is being moved to different coordinates, either within the same group or to a different group, you will be asked what you would like to happen to the data associated with the tablet at its old coordinates. A tablet can have only one data set associated with it. If you want to keep the data from before, select "bring data". If you "leave data", then you may assume any data at the new coordinates.

Assume Data or Start Fresh: If there is data at the destination coordinates and you are not bringing data from other coordinates, then the tablet may assume the data at the new coordinates. This may be desired, for example, if the new tablet is intended to replace a lost or broken tablet. If a registering tablet assumes the identity of an existing tablet in this way, the existing tablet (possibly lost or broken, in the example) will be made inactive.

Step 1:

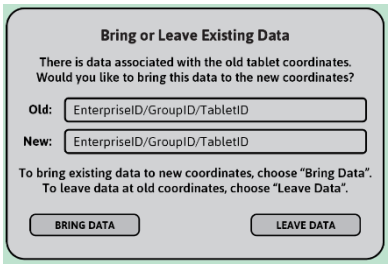
Step 2:

Step 3:

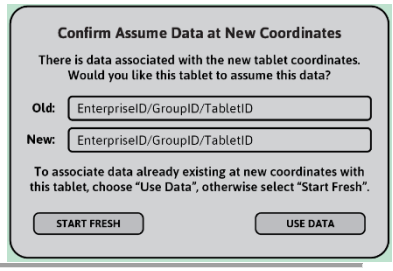


Release Tablet:

Bring or Leave Data:



Assume Data or Start Fresh:



Adding SmartDOCKs to a Group

If you are using SmartDOCKs in your deployment, the next step after registering tablets to a group in an enterprise, is to register docks into that group.

To register a dock in a group, simply dock a tablet from that group onto the dock. If KMS is running (or is launched) you will then be taken to a wizard which will allow you to add the dock to the group.

To add a Dock to a Group:

Step 1: If the dock has never been registered and a tablet is docked to it, a wizard will appear and you will be asked to provide a Dock ID to identify the dock in the tablet's group.

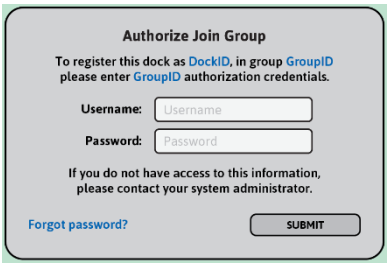
Step 2: Next you will be asked to provide authorization credentials to formally register the dock in the group.

Join Group: If the dock has been previously registered to a different group and you will be asked if you would like the dock to be registered to the tablet's group ("Join Group") or if the tablet is "just visiting" and the dock should remain in its existing group ("Unlock Only").

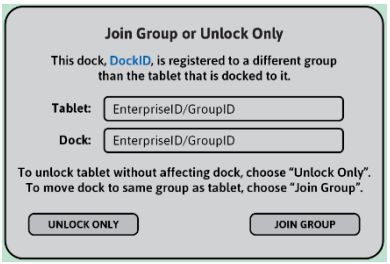
Release Dock: If the intention is to change the registration of the dock from a different group to the tablet's group, an admin or owner of the group to which the dock is registered must provide credentials to release it from that group before it can be registered to the tablet's group. This release is not needed if the dock is deleted from the original group first.

Step 1:

Step 2:



Join Group or Unlock Only

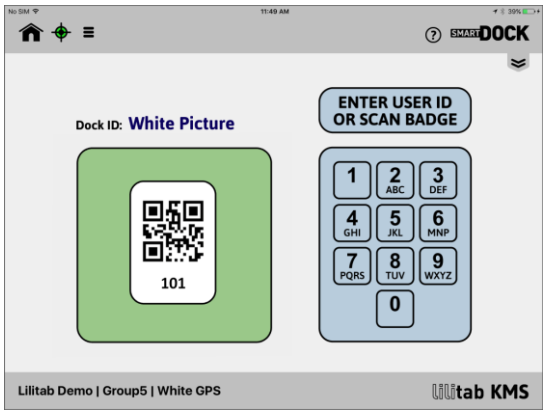


Release Dock

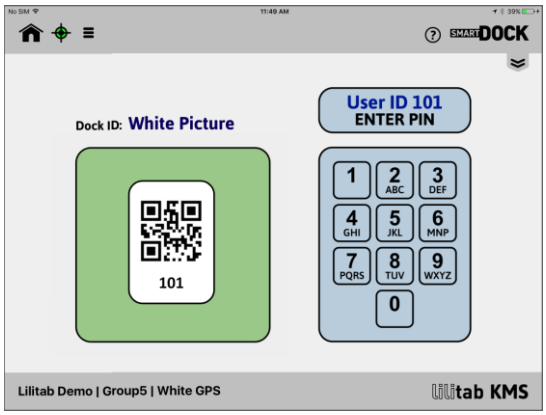
Dock Unlock with the PIN Pad

Lilitab KMS uses a PIN Pad interface to both unlock the Lilitab SmartDOCK. First the user enters their 3-digit UserID on the PIN Pad then the user enters their 4-digit PIN using the keypad.

Step 1: Enter User ID



Step 2: Enter 4-Digit PIN



Using a QR Code Badge to Unlock Dock

A QR Code Badge can also be used to unlock a SmartDOCK. How the badge works depends on the setting for "Include Unlock PIN in QR Code" (See "Group Detail Screen", page 17). If "Include Unlock PIN" is selected, the user only needs to show their QR Code to the camera to unlock the SmartDOCK. If "Include Unlock PIN" is not selected, the user will need to remember and enter their PIN on the keypad. If they do not have a badge, the user can always manually enter their UserID and PIN.

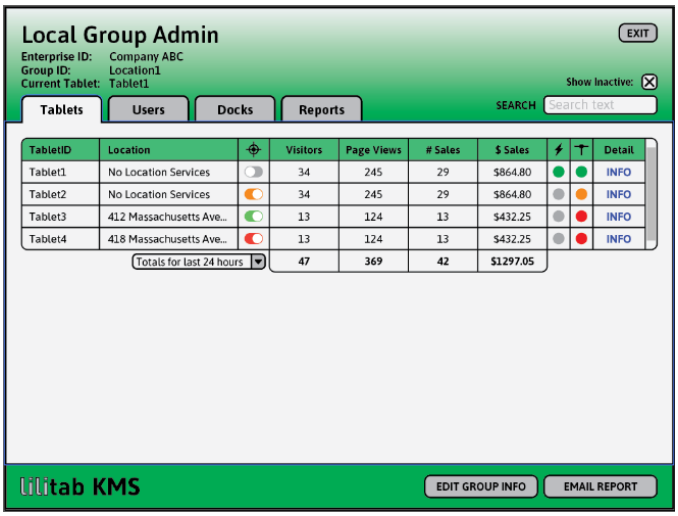
Unlock Icon

The unlock icon, which appears in the pull-down header on the main page, gives feedback about the state of the SmartDOCK as shown at right.

	SmartDOCK locked and operating normally. Ready to unlock.
	SmartDOCK unlocked. Ready to remove head unit. This icon will also show if head unit undocked.
	Power not available, SmartDOCK stalled, or communication error. Check power supply. If stalled, try again or use key to unlock. If communication error, quit and restart app or use key to unlock.
	Power not available or SmartDOCK stalled. Check power supply. If stalled, lift head and try again or use key to lock.

Local Group Admin

The local group admin interface allows group owners and managers to administer the tablets, users, and docks which constitute the elements of the local group.



Tablet Admin Tab

The tablet screen lists the tablets in the group, their location, and the last user to access each tablet.

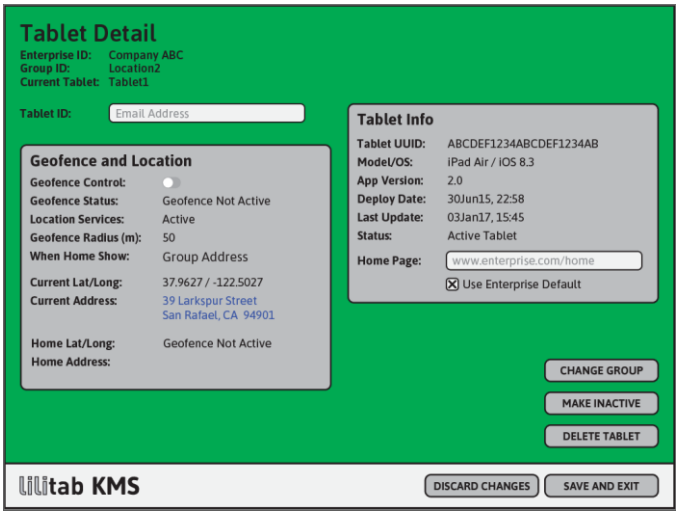
The tablet list as well shows statistics gathered from each tablet. These statistics are gathered by the Lilitab KMS SDK, and can include:

- Visitors
- Page Views
- Transactions
- Sales

Other statistics can also be gathered, depending on configuration at the enterprise level.

The tablet list is searchable and statistics can be filtered to show the most recent 24 hours, week, and month of data from each tablet.

The “Edit Group Info” button in the footer can be used to access the Group Detail screen. See “Group Detail Screen” on page 17 for details about configuring group settings.



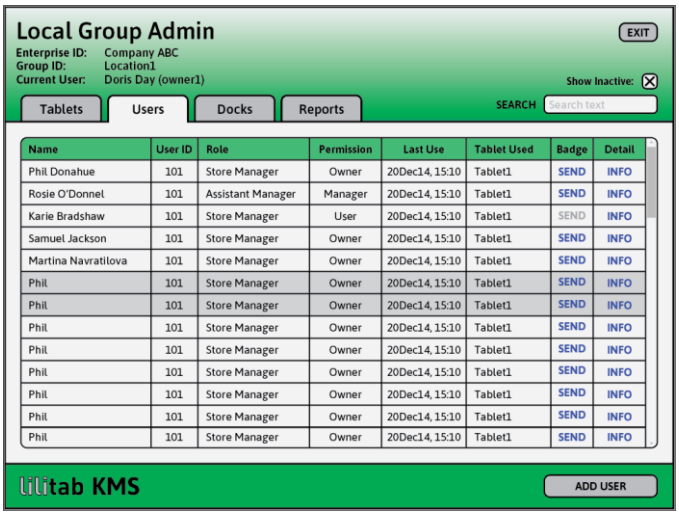
Tablet Detail Screen

Tapping “INFO” in the right column of the tablet list displays detail information for the subject tablet, including:

- Geofence Control and Status
- Current Location
- Home Location (if geofence active)
- Model and iOS Version
- App Version and Deploy Date
- Tablet-Specific Home Page

If the administrator has necessary permissions, there are also controls provided to change the tablet’s group, make the tablet inactive (temporarily suspend tablet communication with server and remove from active tablet lists, but retain data associated with tablet), or delete the tablet (revoke registration and delete all data).

User Admin Tab



The Users tab on the Local Group Admin page provides access to tools for administering group user accounts.

The user list shows top level data about each user in the group, including

- User ID
- User Name
- Permission Level
- PIN Renew

If the "SEND BADGE" link is tapped, that user will be sent a QR Code that they can use on the PIN Pad screen (see page 13). The checkbox at the top can be used to show/hide inactive users and the button in the footer facilitates the addition of new group-level users.

User Detail Screen

Selecting "Add User" or tapping "INFO" in the right column of the user list displays detail information for the subject user, including:

- User ID
- User Name
- User Role
- User Phone
- User Email
- Permission Level

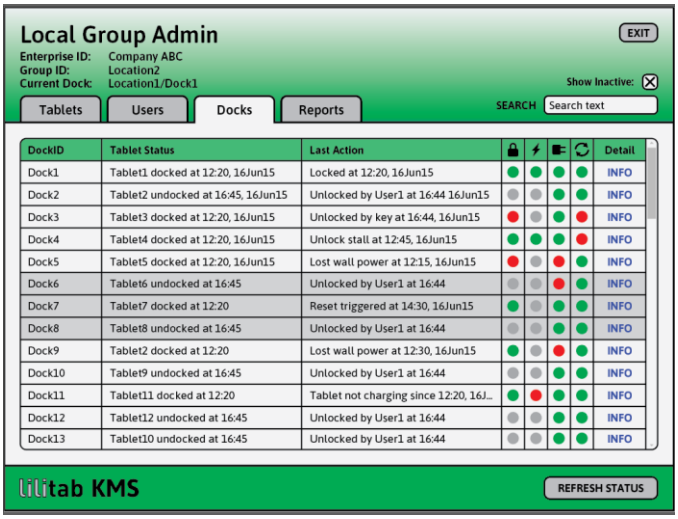
If the user has Owner or Manager permissions, the Portal Access panel will show their portal username and allow password renewal.

Using the controls on the detail page, group admins can modify user attributes, renew passwords, reissue PINs, and suspend or delete users.

Group level permission privileges are shown in the table at right.

	User	Manager	Owner
Unlock SmartDOCK	X	X	X
Access Group Portal		X	X
Create/Modify Users		X	X
Register/Release Tablets/Docks			X
Create/Modify Managers			X

Docks Admin Tab



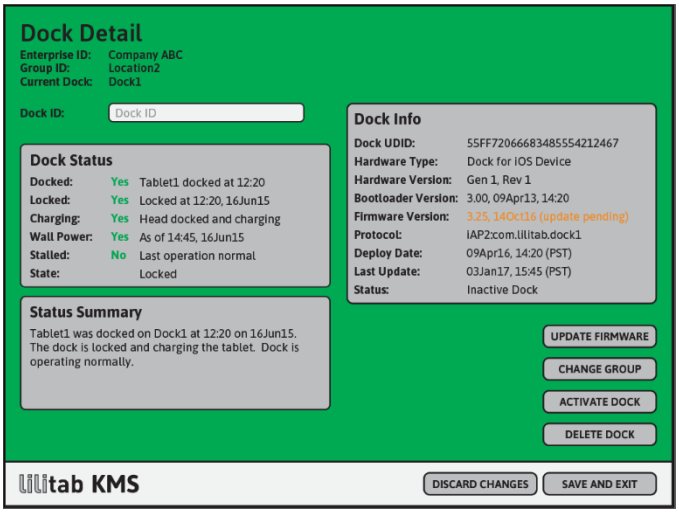
The Docks tab on the Local Group Admin page provides access to tools for monitoring and maintaining the dock infrastructure relied on by a group.

Note that only SmartDOCKS can register and appear in the Dock List.

The dock list shows top level data about each dock in the group, including

- Dock ID
- Tablet Presence (if any)
- Last Action (last event on that dock)
- Docked/Locked Status
- Power/Charging Status
- Stall Status

Dock Detail Screen



Tapping “INFO” in the right column of the dock list displays detail information for the subject dock, including:

- Last User to unlock Dock
- Last Tablet on Dock
- Current State
- Docked/Locked Status
- Power/Charging Status
- Dock Jam/Stall Status
- Plain Language Status Summary

For each dock attribute, both the current value and the duration since last change are shown. The dock can be renamed by modifying the DockID.

If the administrator has necessary permissions, there are also controls provided to change the tablet’s group, make the tablet inactive (temporarily suspend tablet communication with server and remove from active tablet lists, but retain data associated with tablet), or delete the tablet (revoke registration and delete all data).

Group Detail Screen

Selecting “Edit Group Info” from the footer of the User Admin screen will take you to the Group Detail screen.

Using this screen, the Responsible Owner can modify and update group-specific attributes and configuration options.

Responsible Owner

The responsible owner is the top-level system administrator at the group level. Only the responsible owner may modify group configuration settings, and only the responsible owner can modify other owner accounts. Each group has one responsible owner. The responsible owner can designate another owner as responsible owner.

Tablet Access

Select “Include Unlock PIN in QR Code” to send a user’s PIN to them as part of their access badge. If not checked, user will need to enter PIN manually.

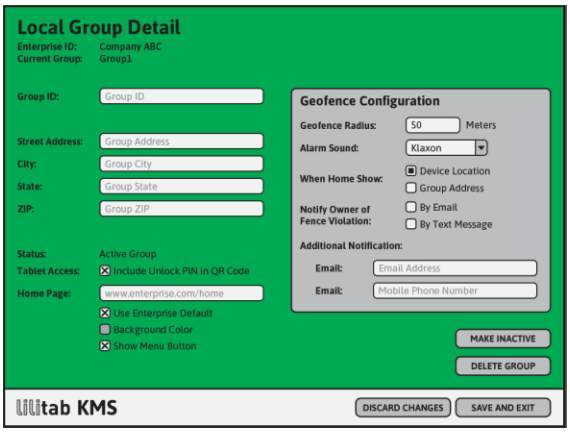
Home Page

The “Home Page” field specifies the default URL for tablets in the group. This field is not editable if “Use Enterprise Default” is checked. “Use Enterprise Default” cannot be unchecked unless “Allow Group Level Override” is permitted under enterprise browser configuration policies.

For more information on setting up tablet home page, “Managed Browser Administration” on page 28.

Other Options

The Responsible Owner can also modify the GroupID, change the address, specify the background color, and select whether the menu button is available on the Lilitab KMS app home screen (hiding recommended for most public use, as menu includes firmware update).



Geofence Configuration

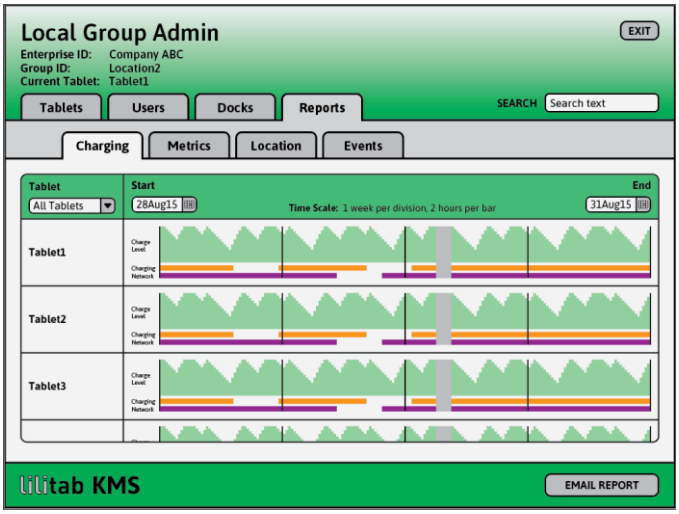
Geofence configuration controls are specific to each group and include the geofence radius, alarm sound, and notification options.

See “Geofence Administration” on page 29 for more information on setting up geofences.

Reports

Lilitab KMS offers a suite of reports that allow you to compare and review trends in various aspects of tablet use and performance over time. The reports are accessed by tapping the "Reports" tab at the Group level.

Charging Report



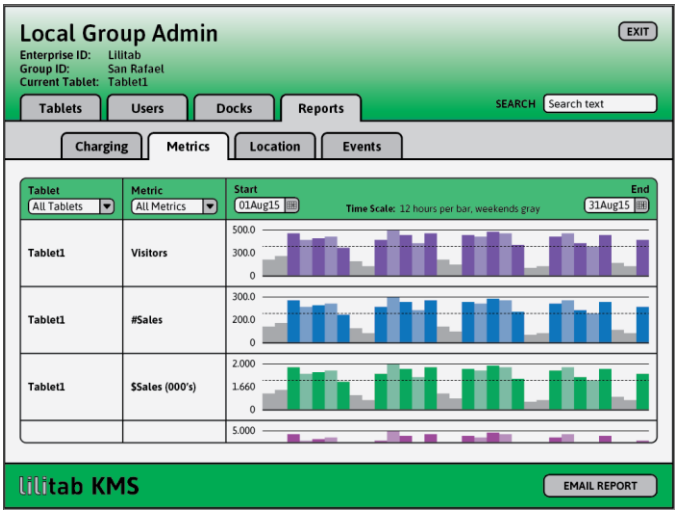
The Charging Report shows the charge level for each tablet in the group. Individual tablets can be selected from the "Tablet" dropdown or isolated using a search string.

The report generates a charge level graph for the specified tablets that starts on the specified start date and ends on the specified end date.

In addition to charge level, the report shows and orange bar to indicate when the tablet is charging and a purple bar to indicate network connectivity. A gap in either bar indicates that the tablet was not charging or not connected to the network at that time. A gray region in the graph indicates that no information is available for that time range, usually because the app was not active.

If the mouse pointer is hovered over the graph, it will report the charge level at that time as a percentage value.

Metrics Report



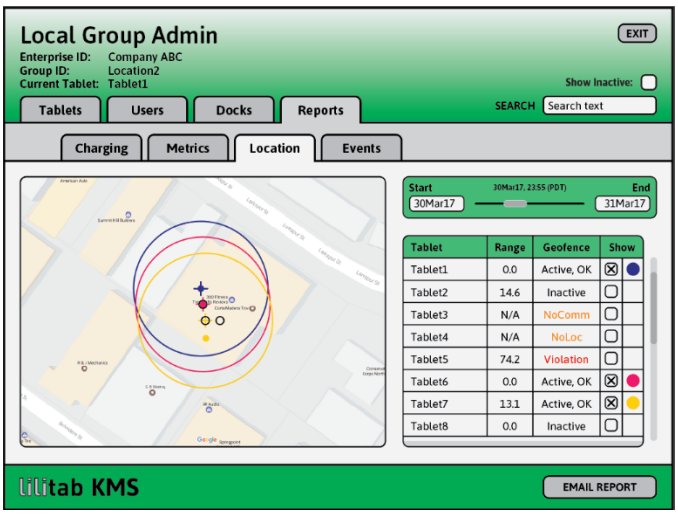
Clicking on the "Metrics" tab opens up the Metrics Report. The Metrics Report shows reported metrics and can be sorted by Tablet or by Metric.

Similar to the Charging Report, the date range for the Metrics Report can be modified by changing the Start and End date fields. Hovering the mouse pointer (or tapping on tablet) will report the value and time range of a specific metric. The value shown is the total amount accumulated for that metric in the specified time interval.

Metrics are customizable statistical measures which need to be configured in the KMS-enabled website or app that is being delivered on the tablet.

For more information and in instructions on how to configure metrics, go to page 31, "Metrics Administration".

Location Report



The Location Report allows for review of historical location information for any tablet in the group.

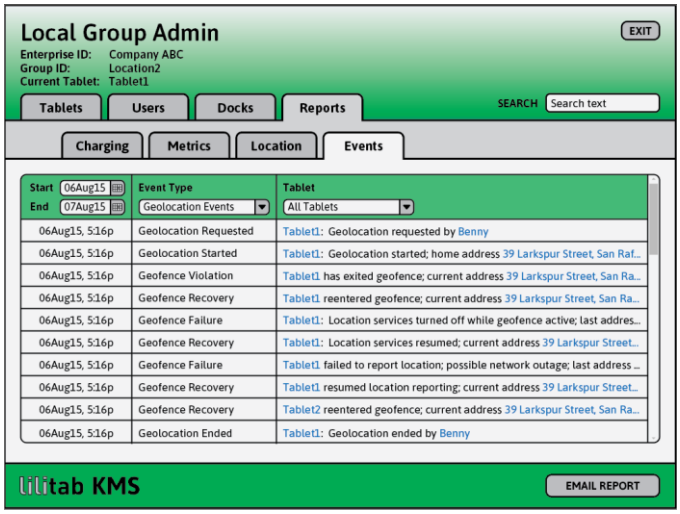
A slider in the upper right corner facilitates selection of start and end date. Moving the slider left and right between the start and end dates sets the specific date and time for the map view.

Below the time slider is a list of the tablets in the group. Selecting a tablet to "Show" will include the tablet in the map. The map will automatically zoom out to show all tablets.

If any geofences are active at the time being shown, they will be shown as a circle in the same color as the tablet to which they apply, with the radius of the circle reflecting the radius of the geofence. The "home location" of the geofence is represented by a cross in the associated color. See "Geofence Administration" on page 29 for more information on setting up geofences.

If SmartDOCKs are in use, those registered to the group will be shown as black circles on the map.

More information about any element in the map can be obtained by hovering over that element.



Event Log

The "Events" tab provides access to an event log. For any specified date range, any or all of the following event types can be shown:

- All Events
- User Admin
- Tablet Admin
- Tablet Status
- Geofence
- Dock Admin
- Dock Status
- Group Admin

The above event groups can further be filtered by tablet in the third column of the report. In conjunction with Event Type and Tablet, the search field may be used to further narrow the filter results.

When the desired report is ready, the "Email Report" button can be used to send the report to the active administrator.

Enterprise Portal

The enterprise portal is a cloud-based resource designed to provide corporate managers and regional directors visibility throughout their kiosk deployment. The portal provides diagnostic data about the health and performance of the kiosk infrastructure as well as reporting statistical metrics generated by the business application.

Portal Login Screen

The portal can be accessed from a standard browser at:

https://kms.lilitab.com

When a new enterprise is created, the agent specified will receive an email containing login instructions and credentials. From the portal, the enterprise agent can create additional enterprise-level accounts as needed.

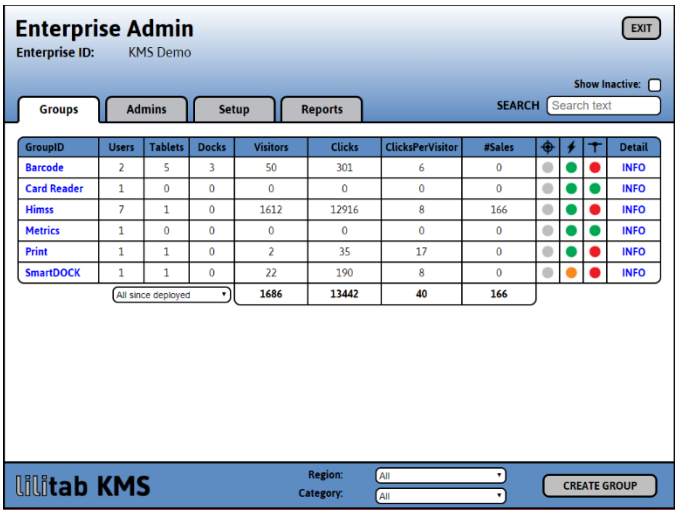
Enterprise Groups Tab

The group admin screen lists the groups in the enterprise, along with rolled-up statistics for each group.

The group list is searchable and can be filtered for duration, region, and category. Region and Category attributes can be set on the Setup tab.

For each group, the number of Users, Tablets, and Docks active in the group are listed. As well, the group list shows statistical totals for each group meeting the active filter criterion.

From the Group Admin screen, the enterprise admin can click on the Group ID in the first column to drill down into each group for direct access to front-line kiosk data.

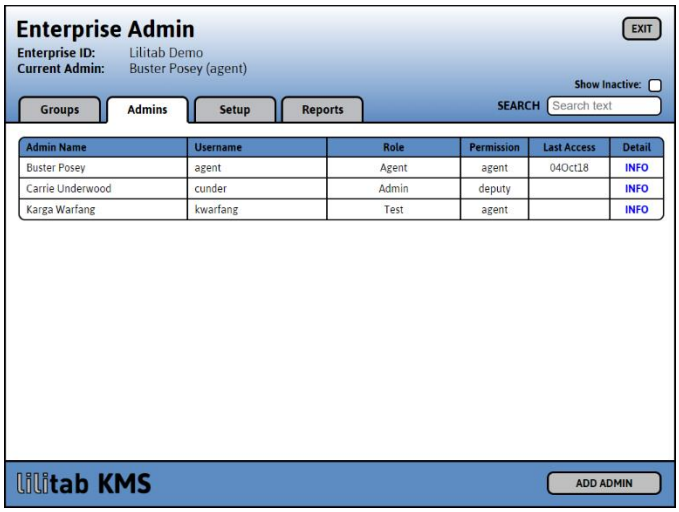


Tapping “INFO” in the right column of the group list displays detail information for the group.

There are multiple ways to create new groups. One way is by a tablet registering into a new group and the person registering that tablet providing responsible owner information. This is called “ad hoc” tablet registration. If Enterprise administrators desire to rearrange and reconfigure tablets among groups, there may be a desire to create a new group from the administration portal. The “**Create Group**” button at the bottom of the Groups page facilitates this. When the admin selects the “Create Group” button, they will be taken to a “Local Group Detail” form to provide information (GroupID, group address, group policies) for that group, from which the new group will then be created. Once created, tablets and docks can be moved into the new group from the detail page of those assets.

Enterprise Admins Tab

The Admins tab on the Enterprise Portal page provides access to tools for administering enterprise admin accounts.



The admin list shows top level data about each enterprise admin, including

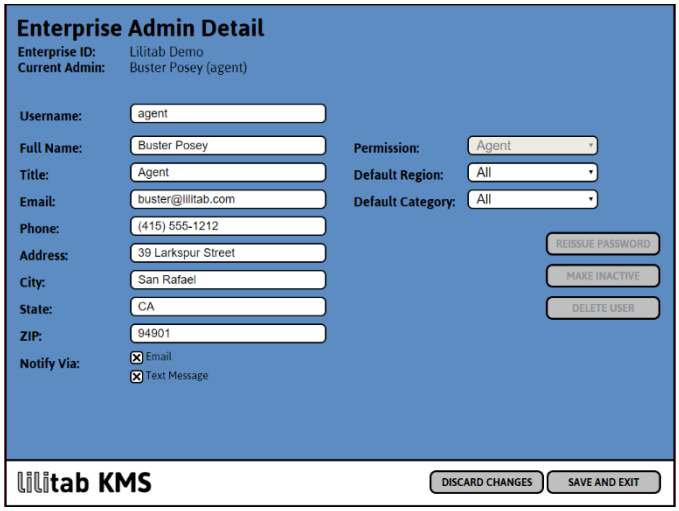
- Admin Name
- Username
- Role
- Permission Level
- Last portal access

Buttons in the lower right corner can be used to add a new enterprise admin or show inactive admins.

Enterprise Admin Detail

Selecting “Add Enterprise Admin” or tapping “INFO” in the right column of the admin list displays detail information for the subject enterprise admin, including:

- Admin Username
- Admin Name
- Admin Title
- Admin Email
- Admin Phone
- Admin Address
- Permission Level
- Default Filter Settings



Each item above can be modified. As well the password can be designated for renew (admin sent email or text message to reset their password), and the user account made inactive or deleted.

Enterprise-level permission privileges are shown in the table at right.

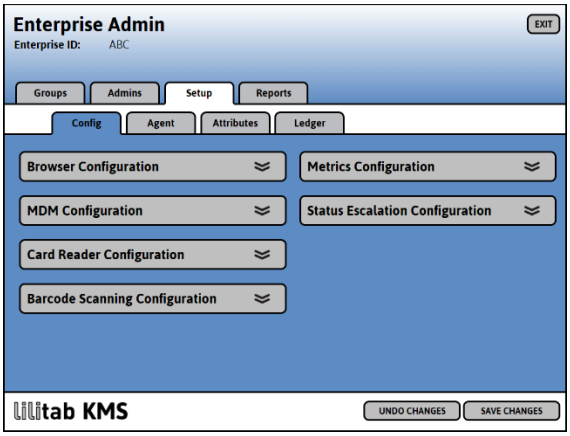
	Admin	Deputy	Agent
Access Portal	X	X	X
View Group Detail	X	X	X
Create/Modify Admins		X	X
Setup Filters/Statistics		X	X
Specify Filters/Statistics			X
Grant Agent/Deputy Permission			X

Enterprise Setup Tab

Selecting the third tab on the Enterprise Admin screen will take the admin to the Enterprise Setup tab, which has four subtabs for enterprise-specific configuration options.

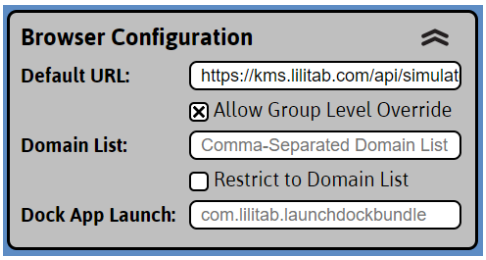
Config Tab

The Config tab within Setup collects a series of configuration panels which allow the enterprise agent to enable and configure enterprise functionality. To open each panel, simply click or tap on it.



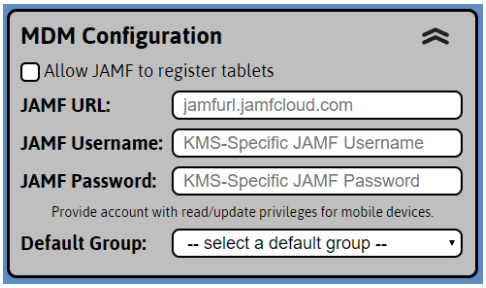
Browser Configuration Panel

The "Default URL" field specifies the default home page for all tablets in the enterprise. This home page will be the required home page for all tablets in the enterprise unless "Allow Group Level Override" is checked. Whether or not "Allow Group Level Override" is checked, browsing on all tablets within the enterprise can be limited to a comma-delimited list of approved domains and subdomains as specified in "Domain List".



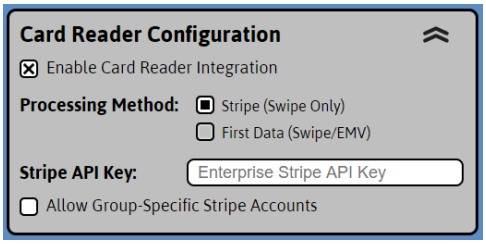
MDM Configuration Panel

The MDM configuration panel supports integration with JAMF MDM software. Using this integration, tablets that are managed by JAMF and to which KMS-enabled apps are deployed will automatically register in KMS. For more information on JAMF integration, see the "JAMF Integration" section of this User Guide.



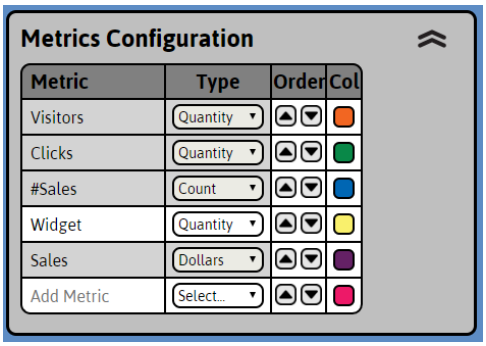
Card Reader Configuration Panel

The Card Reader configuration panel enables the KMS integration with the eDynamo card reader and Stripe processing method. For detailed configuration instructions, see the "Card Reader Integration" section of this User Guide.



Metrics Configuration Panel

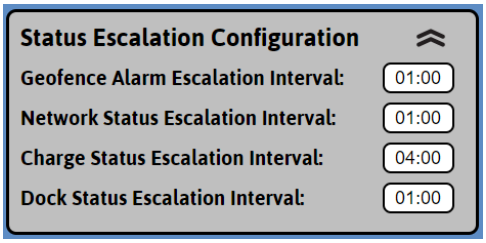
The Metrics configuration panel allows administrators to create new metrics and ratios of metrics for business-driving parameters that they want to measure. Metrics are posted to KMS by the web application and allow performance measures to be associated with individual kiosks and groups of kiosks. The top four metrics listed in the panel are readily visible in the tablet list and group list. For more information about metrics, see "Metrics Administration" in this User Guide.



Status Escalation Configuration Panel

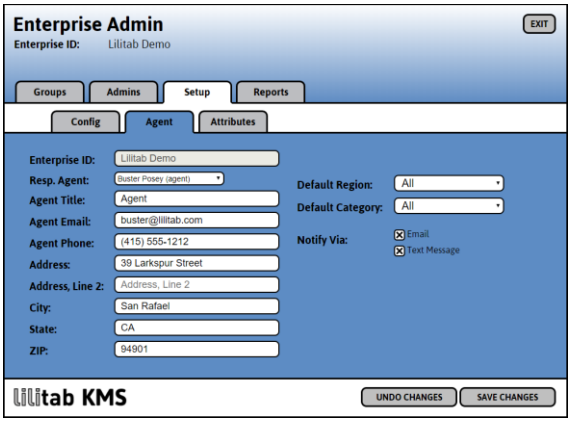
The Status Escalation Configuration panel sets the intervals at which status indicators for geofence, network, charge status and dock status escalate.

When a status alert first registers (at the group level) it turns from green to orange. After one status interval, it will turn from orange to red at the group level and to orange at the enterprise level. And after a second status interval, the indicator will turn red at the enterprise level.



Responsible Agent Tab

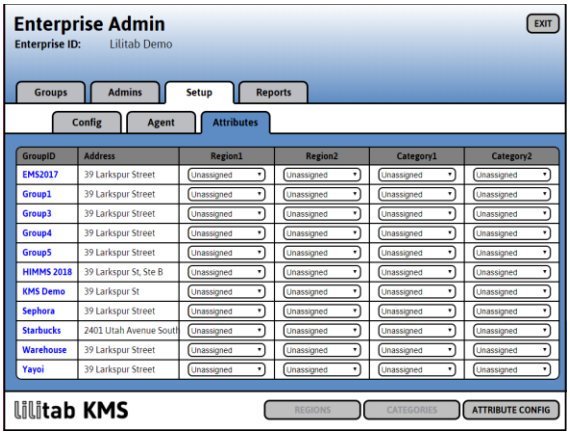
The responsible agent is the top-level system administrator at the enterprise level. Only the responsible agent may modify enterprise configuration settings, and only the responsible agent can modify other agent accounts. Each enterprise has one responsible agent. The responsible agent can designate another agent as responsible agent.



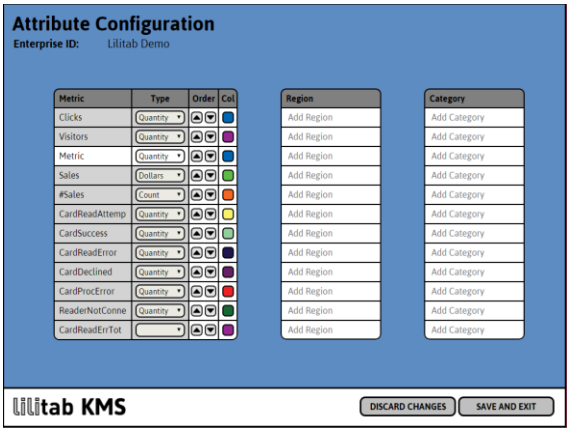
Attributes Tab

The Attributes tab on the Enterprise Setup screen provides access to tools for assigning region and category attributes to each group in an enterprise. Regions and Categories are useful for sorting large enterprises to isolate groups in the same geographical area or of similar business type. The Setup tab is only accessible to enterprise admins with “Agent” or “Deputy” permission.

Using the pull-down menus on this tab, enterprise admins can assign region and category attributes to each group in an enterprise. All enterprise-level users can then use these assigned attributes to filter the group list by using the Region and Category pulldowns in the Groups footer. This allows regional managers, for example, to view the aggregate performance metrics of just the groups in their region.



Pressing the “Attribute Config” button in the footer of the “Setup” screen will take the enterprise admin to the Attribute config screen.



On this screen, the admin can set up:

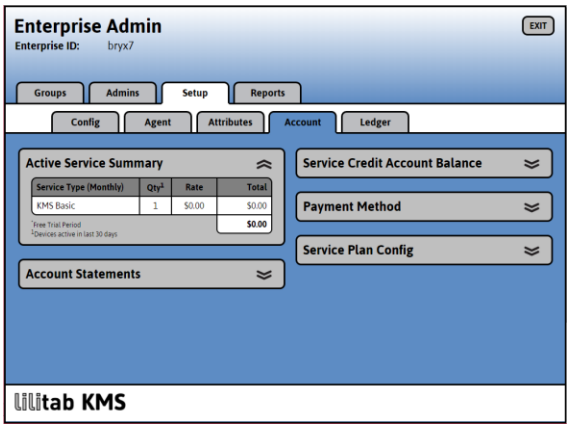
- Metrics
- Regions
- Categories

The “Metrics” list shows metrics that can be reported by tablets in the enterprise. The gray metrics are default and cannot be deleted. Metrics that start with “#” are a count of posts to the metric by the same name (but without the “#”). The order of the metrics can be changed with the “up” and “down” arrow buttons in the third column. The top four metrics will appear on the Tablet List page (at the group level) and, aggregated, on the Group List page (at the enterprise level).

For more information and in instructions on how to configure metrics, go to page 31, “Metrics Administration”.

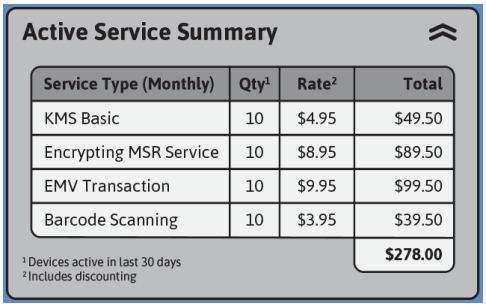
Account Tab

The Account tab provides the enterprise agent with access to the billing details for the enterprise. The Account tab is only visible to the responsible agent.



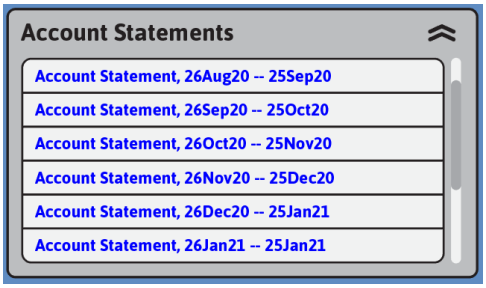
Active Service Summary Panel

The Active Service Summary panel summarizes the services that are active in the account. Note that if bulk service credits are purchased at a discount, the billing rate listed in the active service summary may not include this discount.



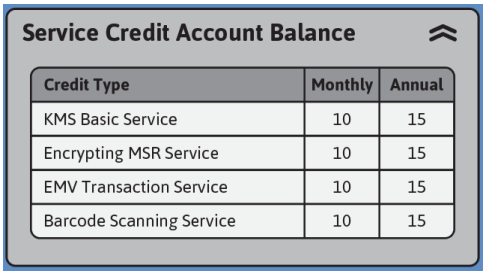
Account Statements Panel

The Account Statements panel provides access to past billing statements.



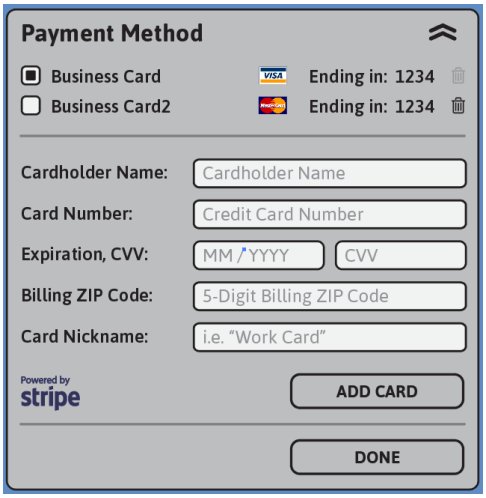
Service Credit Account Panel

The Service Credit Account holds service credits that were purchased in bulk for the account. These service credits will be applied first, before services are charged for in any other way. Use of bulk service credits allows payment by invoice and supports larger deployments for which credit card payment is impractical.



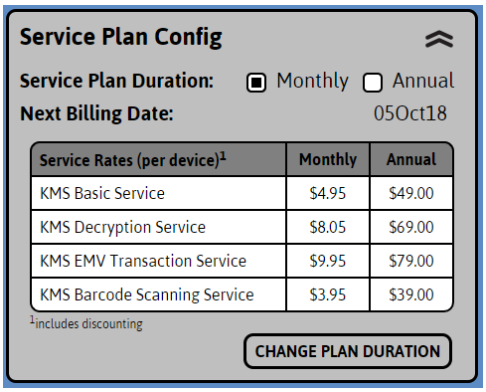
Payment Method Panel

The Payment Method panel allows the enterprise agent to provide (or change) a credit card for payment of service plan renewal charges. If payment by invoice is preferred, please contact Lilitab sales to purchase bulk service credits.



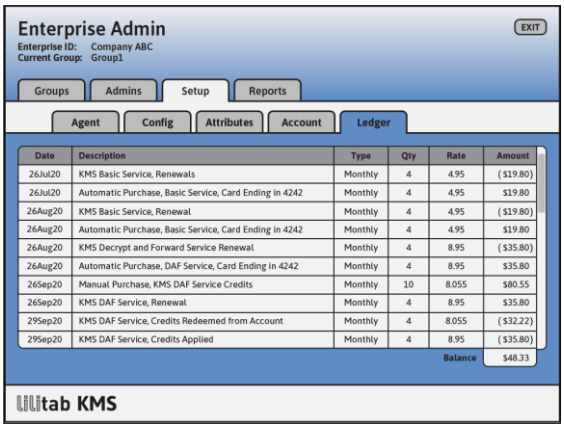
Service Plan Config Panel

The Service Plan Config panel allows the enterprise agent to change the duration of the enterprise service plans from monthly to annual. The change will take place at the next service plan renewal for each device/accessory. The amount paid for any unused service plan credits may be applied toward purchase of service plan credits of the new duration. The Service Plan Config panel includes a table with pricing of each service plan type and duration.



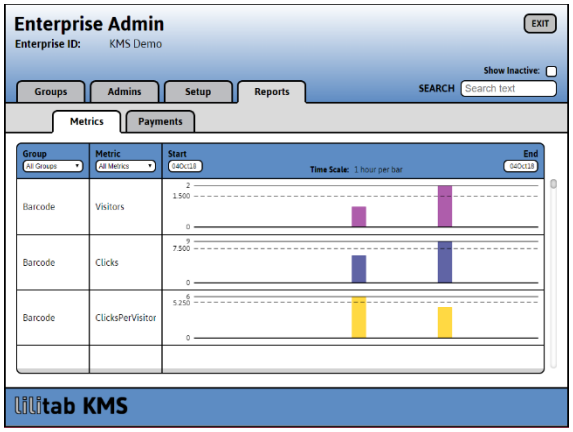
Ledger Tab

The Ledger tab, also visible only to the enterprise agent, provides a chronological history of all charges and payments in the enterprise account.



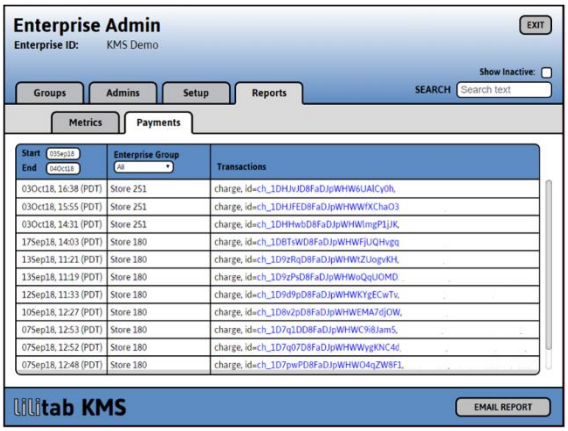
Enterprise Reports Tab

Lilitab KMS provides enterprise-level reports for metrics and, when enabled, payments.



Enterprise Metrics Report

The Enterprise Metrics report allows enterprise admins to compare performance at the group level and between different groups. All metrics that are reported from each tablet are associated with that tablet's group, and can be viewed in similar fashion to the group-level metrics report.



Enterprise Payments Report

If the card reader integration is enabled, enterprise agents and deputies can review the payments report for a complete record of processed transactions. No sensitive cardholder data is present in the entries, but the payment parameters – customer name, amount, result, etc. – can be viewed by clicking on the transaction ID. For Stripe transactions, the transaction ID is the Stripe transaction ID and may be further examined in your Stripe portal. The payments report allows administrators to identify the occurrence of failed transactions and, as needed, determine the root cause.

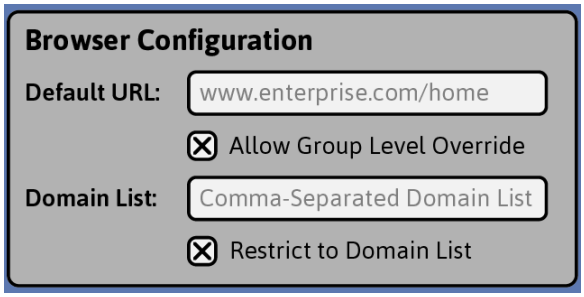
Advanced Administration Features

Managed Browser Administration

Overview

Lilitab KMS offers several ways to manage what content is displayed in the browser window (Main Screen). These controls allow specification of the home page at the enterprise, group, and individual tablet level. As they are accessed from the admin portal, all settings may be configured remotely.

Enterprise Browser Configuration



The Browser Configuration panel, accessed on the Enterprise Detail screen, provides controls for setting enterprise-wide browsing policies. The specified "Default URL" will appear as the default home page for all groups and tablets in the enterprise. If "Allow Group Level Override" is checked, custom home page URLs can be set by enterprise or group admins at the group level. If "Allow Group Level Override" is not checked, all tablets in the group must use the enterprise default URL as their default URL. Whether or not "Allow Group Level Override" is checked, browsing on all tablets within the enterprise can be limited to a comma-delimited list of approved domains and subdomains as specified in "Domain List".

Group Level Home Page Controls

At the group level, home page controls are found on the Group Detail and Tablet Detail page. On the Group Detail page, the "Home Page" field specifies the default URL for tablets in the group. This field is not editable if "Use Enterprise Default" is checked. If "Use Enterprise Default" is checked, the Enterprise Default URL will self-populate in the Home Page field. "Use Enterprise Default" cannot be unchecked unless "Allow Group Level Override" is permitted under enterprise browser configuration policies. If "Use Enterprise Default" is unchecked, the URL specified in the Home Page field on the Group Detail page will be the default URL for all tablets in the group.

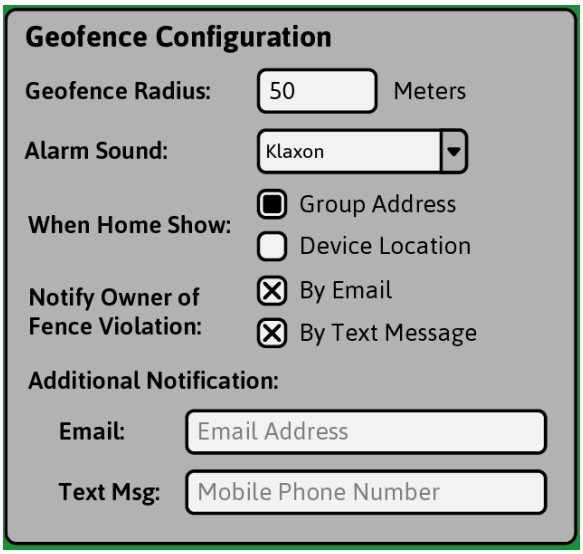
On the Tablet Detail page, the "Home Page" field is found in the Tablet Info panel. If the "Use Group Default" box is checked, the tablet Home Page will default to the group home page (which in turn may default to the enterprise home page). If the "Use Group Default" box is unchecked (which requires that "Allow Group Level Override" be checked at the enterprise level) a tablet-specific home page may be set in the Home Page field.

Geofence Administration

Overview

Lilitab KMS leverages Location Services, in combination with remote administration and reporting, to provide a complete suite of asset protection and location features. These features include:

- Remote geofence initiation and monitoring
- Group-specific geofence configuration
- Audible and silent alarms
- Email and/or text message notifications
- Tablet current location by street address
- Remote disabling of KMS application
- Geofence event logging and reporting



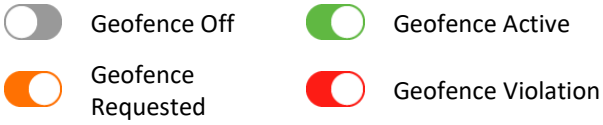
Geofence Configuration Panel

The geofence configuration panel, available on the Group Detail page, provides access to the primary geofence controls. The panel allows the group owner to specify the geofence radius, alarm sound, and specify notification recipients and methods.

When setting Geofence Radius, administrators should consider the type of tablet being used. While "WiFi Only" tablets will work with KMS geofencing, the location accuracy is limited by the ability of the tablet to estimate its location base on the relative signal strength of nearby WiFi access points. Because this makes WiFi location estimation inherently unstable, **to prevent false alarms, Lilitab recommends a geofence radius buffer of at least 25 meters beyond the expected movement area when using WiFi tablets**. Cellular tablets have on-board GPS, and give more accurate location, generally to within 5-10 meters. Cellular tablets are also able to report their location when away from known WiFi access points.

Initiating Geofence Monitoring

Once the geofence is configured as desired, the geofence for each tablet can be activated by toggling the geofence switches on the Tablet Admin Screen.



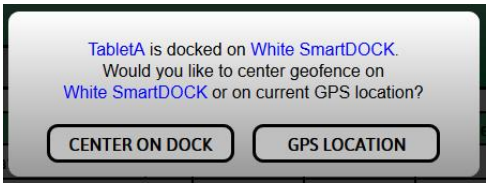
TabletID	Location	
Tablet1	No Location Services	
Tablet2	No Location Services	
Tablet3	412 Massachusetts Ave...	
Tablet4	418 Massachusetts Ave...	

To turn the geofence on, tap the switch. When first turned on, the switch will turn yellow. If location services are not yet turned on for the tablet, the app will request location services, and if enabled, will return the geofence origin ("home location") and the switch will turn green. The switch will turn red if a geofence violation is detected. Tapping the switch again will turn the geofence off.

Setting the Home Location

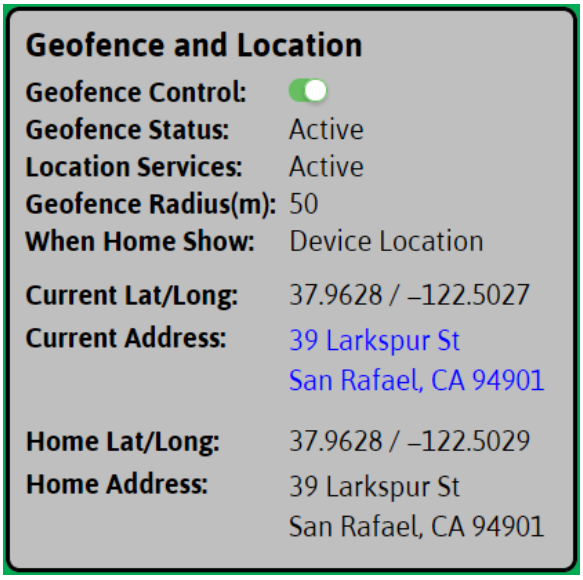
The Home Location is the center of the geofence. It is the reference point, relative to which a geofence violation will occur if the tablet moves outside the specified geofence radius.

When a geofence is requested, the Home Location can be set with either a GPS Location or SmartDOCK as reference.



GPS Location: This is the default reference for the geofence center, determined when the geofence is initiated. GPS location is always used when the geofence is turned on with the tablet undocked.

Center on Dock: If a geofence is turned on *while the tablet is docked to a SmartDOCK*, a popup will appear, allowing that SmartDOCK to be specified as the home location. "Center on Dock" is recommended when using WiFi tablets, as it allows the app to re-center the geofence regularly, both reducing WiFi drift and eliminating false alarms while docked.



Geofence Alarm

If the geofence is violated, the alarm will sound and notifications (if enabled) will be sent. The geofence can be recovered – and the audible alarm silenced – by moving the tablet back within range and ensuring that location services and network are active. The alarm can also be silenced by turning the geofence off.

Location Monitoring

In addition to showing the tablet location and geofence status on the Tablet Dashboard, more detailed information can be found on the Tablet Detail page for each tablet. On the Tablet Detail page, you will find:

- Summary of geofence status and settings
- Home Location (center of geofence)
- Current Location (Lat/Long and street address)

Event Group	Event Name	Event Description
Geofence	Geofence Requested	TabletID: Geofence requested by UserID
Geofence	Geofence Started	TabletID: Geofence started – *Radius* meter radius
Geofence	Geofence Stopped	TabletID: Geofence ended by UserID
Geofence	Geofence Violation	TabletID: Geofence violation – last used by UserID
Geofence	Geofence Recovery	TabletID: Geofence recovered – tablet returned to geofence
Geofence	Geofence Recovery	TabletID: Geofence recovered – location services turned on
Geofence	Geofence Recovery	TabletID: Geofence recovered – GPS services restored
Geofence	Geofence Recovery	TabletID: Geofence recovered – network restored
Geofence	Geofence Failure	TabletID: Geofence lost – location services turned off
Geofence	Geofence Failure	TabletID: Geofence lost – GPS services not working
Geofence	Geofence Failure	TabletID: Geofence lost – network not available

Location Reporting

Tablet location, both current and historic can be reviewed in the Location Report (see page 19). Additionally, all geofence events are logged and available for review in the Event Log, with filters by tablet, date, and event type (see page 19).

Metrics Administration

Overview

Metrics are a powerful way to collect usage data from your KMS-enabled kiosks. KMS metrics can be set up to measure and monitor almost any activity at the kiosk – tagged and categorized based on the tablet and group where it was collected – and report that data both at the group and enterprise level.

For example, metrics can be used to monitor the number of visitors to the kiosk and how many pages they viewed (a measure of interest). Indeed the "Visitors" and "Clicks" default metrics are designed to collect that data by default.

Metrics are designed to operate as "time-dependent accumulators". When a metric is triggered, its value is submitted with a timestamp to KMS through secure, authenticated channels. The accumulated results can be viewed for individual tablets, group totals, and enterprise totals for various time intervals. As such, metrics serve as performance monitors, posting directly to the Tablet List and Group List dashboards at the group and enterprise levels, respectively.

Metrics Configuration

Metrics are configured using the Metrics Configuration Panel on the Attribute Configuration page, accessed from the footer of the "Setup" tab at the enterprise level. Metrics are established as common measurements throughout the enterprise. Up to 10 different metrics (variables) can be defined in the panel. Metrics can have different types that define how they will display, including Quantity (integer value), Dollars (shown as $##.##), Decimal (decimal value), Hours (shown as decimal hours), and Minutes (shown as decimal minutes).

The top four (4) metrics will be shown in the group-level Tablets List and enterprise-level Groups List. The metrics can be reordered in the list using the Up/Down arrows in the third column of the metrics list.

Count Metrics

KMS also facilitates counting the number of transactions on a particular metric, so that such statistics as average transaction size and transaction volume over time can be measured. To create a count metric, precede the metric name with a "#". A count metric will incrementing by one for every post to that metric. Since it is a derived measure, a count metric cannot be posted to directly.

Incorporating Metrics in Web Pages

Once a Metric is set up in the list of enterprise metrics, posting data to it is straightforward. The code sample shown at right is all that is needed. Simply declare "kmsMetrics.js" in your web page and call "kms.postMetric" with the name of the metric and the amount to post to that metric. The example at right will post a transaction of $12.34 to the "Sales" metric when the link is clicked on by the user. This would also increment the "#Sales" counter by one.

```
<html>
<head>
 <script
src="https://kms.lilitab.com/js/kmsMetrics.js"
type="text/javascript"></script>
</head>
<body>
 <div id="kmsMetrics"></div>
 <a href="#"
onclick="kms.postMetric('Sales',12.34); return
false;">kms.postMetric('Sales',12.34)</a>
</body>
</html>
```

Incorporating Metrics in Native iOS Apps

Metrics can also be posted by native iOS apps. If you are building a native app, you will want to incorporate the KMS SDK, which includes methods for posting Metrics.

Please contact Lilitab support for questions about incorporating Lilitab KMS SDK in your custom app.

Viewing Metrics in the Portal

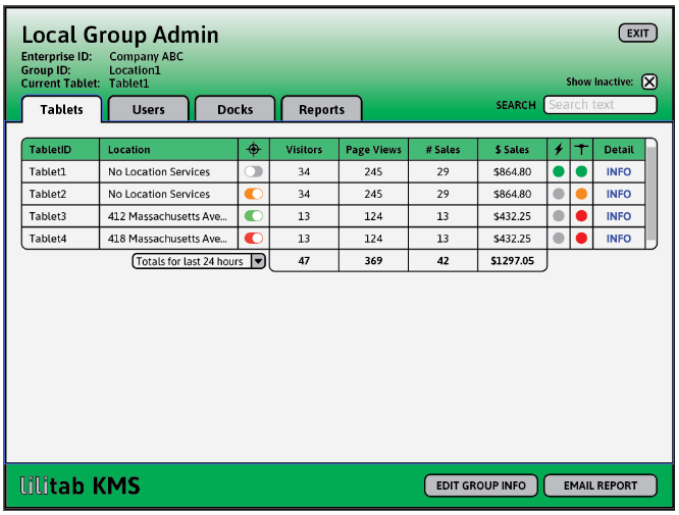
All metrics are viewable in the Lilitab KMS admin portal, at both the Group and Enterprise level.

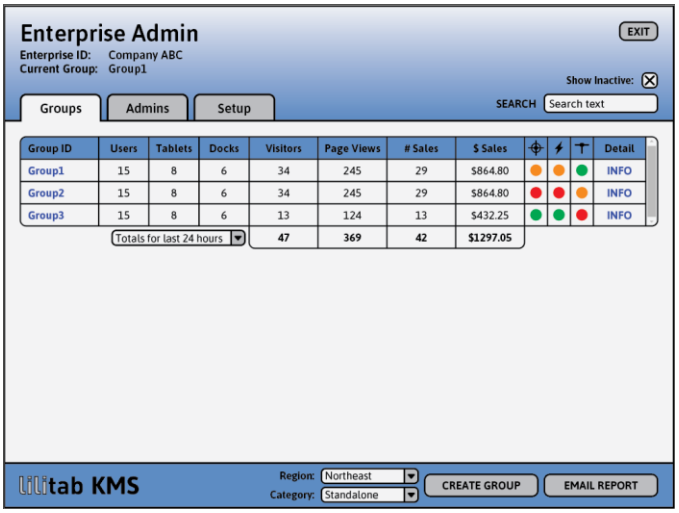
At the group level, the accumulated sum of metrics posted to the group is broken down by tablet. Using the dropdown menu next to the totals, the portal user can specify how far back they want to see metrics results. Duration options are:

- Today
- Last 24 Hours
- This Week
- Last 7 Days
- This Month
- Last 4 Weeks
- This Quarter
- Last 3 Months
- This Year
- Last 12 Months
- Since Deployment

The same options are available to Enterprise-level administrators at the Enterprise Admin level, with the metrics results for each group rolled up and the total for the enterprise shown on the bottom line.

The lists, both at the group and enterprise level can be filtered with the search tool and at the enterprise levels by the Region and Category attributes. Only visible rows in the table will be included in the totals. Tablets that are made inactive will not be included in metrics totals for that group at the enterprise level.





JAMF Integration

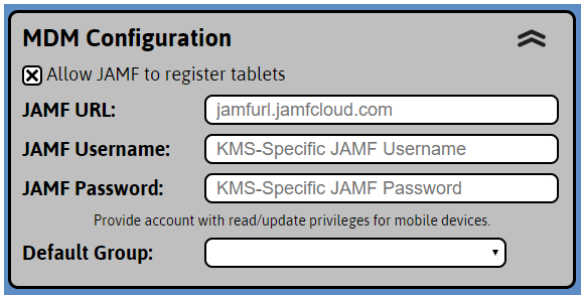
Overview

The KMS JAMF Integration allows tablets to deploy from JAMF and self-register in KMS. This allows the tablet to resume its KMS identity, home page, coordinates, support for peripheral functions, and associated KMS metrics and monitoring functions, even after a JAMF wipe and app redeployment. The integration also replicates the JAMF department and tablet name structure in KMS, so that there is correspondence between the systems.

Step 1: Enable MDM integration in KMS

Once KMS is set up, enable JAMF integration by checking "Allow JAMF…" on the MDM Configuration panel in Enterprise Setup. Then provide JAMF credentials (username/password) and your JAMF URL.

Do not use root credentials. Instead create a new user in JAMF with dedicated read/update credentials for KMS.



Step 2: Set up JAMF webhooks

Back in JAMF, set up "mobileDeviceEnrolled" and "mobileDeviceUnenrolled" webhooks to notify KMS when a device is enrolled or unenrolled. This allows KMS to provide a registration token to that tablet.

To set up the webhooks, go to "Settings > Global Management > Webhooks" in your JAMF instance and configure two webhooks as follows:

Event	Target URL
MobileDeviceEnrolled	https://kms.lilitab.com/api/webhook/mobileDeviceEnrolled/EnterpriseID
MobileDeviceUnEnrolled	https://kms.lilitab.com/api/webhook/mobileDeviceUnenrolled/EnterpriseID

For the integration to work, you must replace the highlighted string with your own KMS EnterpriseID.

Step 3: Setting up a JAMF Smart Group:

In addition to the webhooks, you must also set up a "Smart Group" – and place the device in that smart group – so that JAMF can make sure KMS does not deploy without the necessary registration token.

To set up a Smart Group, follow the instructions here:

http://docs.jamf.com/9.98/casper-suite/administrator-guide/Smart_Mobile_Device_Groups.html

In that Smart Group, specify the presence of the "Position" attribute as a scope requirement for deployment of KMS apps. You will also, of course, want to add all tablets that deploy KMS apps to that Smart Group.

For information on configuring scope requirements, see:

http://docs.jamf.com/9.98/casper-suite/administrator-guide/Scope.html

Step 4: Set up apps for distribution

You will next set up the KMS apps you wish to deploy with JAMF. These might be in-house apps such as KMS Unlock and Sortie or they might be App Store apps such as Lilitab KMS.

For information on how to configure in-house apps in JAMF, see:

http://docs.jamf.com/9.98/casper-suite/administrator-guide/In-House_Apps.html

The Bundle Identifier and download URL for KMS Unlock and Sortie are as follows:

Bundle Identifier	Download URL
com.lilitab.stanfordunlock	https://kms.lilitab.com/ipas/KMSUnlockV1.91.ipa
com.lilitab.sortie	https://kms.lilitab.com/ipas/Sortie.ipa

For information on how to configure App Store apps in JAMF, see:

http://docs.jamf.com/9.98/casper-suite/administrator-guide/App_Store_Apps.html

Step 5: Set up the app Configuration Dictionary

The configuration dictionary is provided to the app when it is deployed to the tablet. This crucial file carries with it the necessary information for the KMS-enabled app to self-register in KMS.

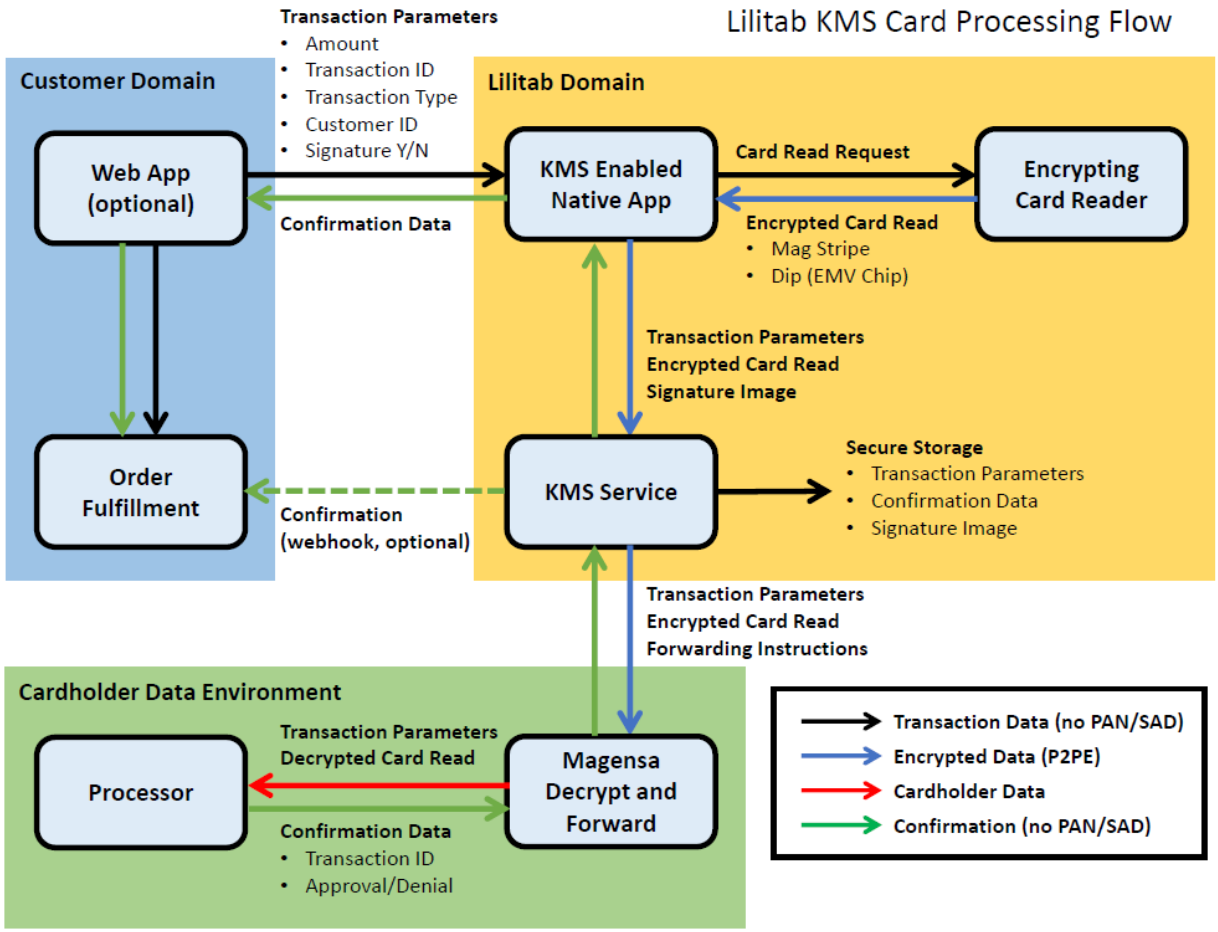
To set up the Configuration Dictionary, open JAMF to "Mobile Devices > Mobile Device Apps", select the Lilitab app that you are deploying, then go to the "App Configuration" tab. Into the "Preferences" box, cut-and-paste the following dictionary:

```
<dict>
        <key>UDID</key>
        <string>$UDID</string>
        <key>regToken</key>
        <string>$POSITION</string>
        <key>EnterpriseID</key>
        <string>EnterpriseID</string>
        <key>GroupID</key>
        <string>$DEPARTMENTNAME</string>
        <key>TabletID</key>
        <string>$DEVICENAME</string>
        <key>TabletName</key>
        <string>$DEVICENAME</string>
        <key>Room</key>
        <string>$ROOM</string>
</dict>
```

For the integration to work, you must replace the highlighted string with your own KMS EnterpriseID.
You should not need to change anything else in the dictionary shown above.

Card Reader Integration (eDynamo + Stripe)

This section will provide instructions and explanation of how to set up the eDynamo card reader and payment capture via Stripe using the Lilitab KMS platform. Before we get started, please review the processing flow shown below:



System Components

There are four primary areas that need to be properly configured to receive payment in Stripe via a Lilitab KMS system:

1. **iOS Application:** This guide assumes that you will be using the Lilitab KMS app as the native iOS application for managing kiosk operations. The Lilitab KMS app facilitates registration of the tablet to the Lilitab KMS server (enabling secure back-end communication), manages the card reader, and displays a web asset in a full-screen webview (for customer-driven UI display). For more information about the Lilitab KMS app, please consult the Lilitab KMS User Guide. For the purposes of Stripe integration, configuration of the Lilitab KMS App involves installation of the app (**v3.1 or higher**) and using the app to register the tablet and card reader to the Lilitab KMS Service.

2. **KMS Service:** Once a tablet has been registered to Lilitab KMS, the account is opened and can be administered using credentials established when the first tablet is registered. For Stripe integration, you will need to log into Lilitab KMS and use the administrator interface to configure Stripe as your selected processing method and provide your Stripe API Key.

3. **Stripe:** To obtain your Stripe API Key, you will need to open a Stripe account. When you do so, you will provide Stripe with a destination bank account where funds will be deposited and you will receive a Stripe API Key. Lilitab KMS then uses the Stripe API Key to direct card swipe transactions to Stripe for processing.

4. **Web Application:** Finally, you will incorporate the appropriate calls in your web asset to initiate a credit card capture and processing sequence, and to receive the result. This is typically associated with a "Pay Now" button, or something similar. From there, the Lilitab KMS App will activate the card reader, overlay a card swipe UI, collect a card swipe (and signature, if desired) and, upon completion of processing, return the transaction result and control back to the web application.

Equipment Needed

To get started, you will need the following hardware:

- **Tablet**: You will need a 9.7", 10.5", or 12.9" iPad. Only iOS devices are supported at this time.
- **Card Reader**: You will need a Liliswipe or eDynamo card reader with Magensa Encryption Key. Contact your Lilitab sales representative to purchase or if you have a card reader and are not sure that it has the correct encryption.
- **Head Unit**: You will need a head unit with card reader accessory appropriate for your model of iPad and selected card reader.
- **Mount**: When it comes time to install the kiosk, you will need a Lilitab mount appropriate for your location. Many mount styles are available, typically ordered together with the head unit.
- **WiFi**: You will need robust WiFi available to the tablet, both for initial setup and for use. Enterprise-grade monitored networking components, such as Cisco Meraki Aps, are strongly recommended.

KMS App and Portal Setup

Once you have your equipment in place, the next step is to install the Lilitab KMS App.

- **Install App**: The app is available in the App Store. Search for "Lilitab KMS", then download and install the app on the tablet. You want **Version 3.1 or higher**. The app icon is shown at right.

- **Registration Wizard**: After installing, launch the app. If the app is being launched on the tablet for the first time, you will enter a registration wizard, which will prompt for needed information to register the tablet. If this is the first tablet to be registered, you will create a new enterprise at this time, and the person registering the tablet will become the owner of the enterprise account. Ownership of the account can be changed as needed. Refer to "System Setup" on page 8 of the Lilitab KMS User Guide for detailed instructions on initial KMS setup.

Upon completing the registration wizard, you can enter the KMS administrative portal from any browser.

- **Card Reader Configuration**: To set up swipe, an enterprise administrator will need to open the "Card Reader Configuration" panel on the Config tab under Enterprise Setup. On that tab, select "Enable Card Reader Integration, then specify Stripe for the Processing Method and enter your Stripe API Key (secret key from the Developers/API keys page in the Stripe dashboard) in the field provided.

- **Browser Configuration**: You will also want to set the default home page for KMS so that your desired web asset is displayed. To test your swipe integration, you may also want to set the swipe test page as the KMS Home Page: https://kms.lilitab.com/api/simulator/cardReadDemo. The KMS Home Page can be set at the enterprise, group, or individual tablet level. For information on how to set the KMS Home Page, consult the KMS User Guide under "Managed Browser Administration".

Card Reader Setup

Before leaving the KMS Dashboard, you will next want to make sure you "Show Menu Button" in the Lilitab KMS app header. This is important for connecting the card reader in the next step. This option is on the Group Detail screen, accessed from the footer of the Tablets tab. Make sure "Show Menu Button" (bottom of left column on Group Detail screen) is checked.

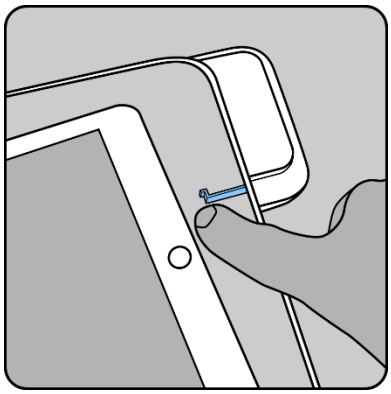
When you complete your work in the KMS portal and press "Exit" you should next see the home page you set in Browser Configuration. If you did not set up a home page, you will instead see a placeholder screen.

Now it is time to connect your card reader. If you are using a Liliswipe direct-connected card reader, and are connected to the reader, you are already connected and you will be directed to the Card Reader Registration Wizard (see below). If you are using an eDynamo Bluetooth card reader, you need to enable Bluetooth on the tablet (if not already enabled) and connect to the reader first.

To enable Bluetooth, go to "Settings" and make sure that the "Bluetooth" function is turned on.

To connect your eDynamo Bluetooth card reader, return to Lilitab KMS, open the menu, and select "Connect Reader" at the bottom of the menu. This will open a submenu that shows available Bluetooth readers that you can connect to. Consult the label on the eDynamo accessory housing for the Bluetooth Identifier of the reader in your head unit.

If this Bluetooth Identifier is not showing in the Connect Reader menu, it may be because the reader needs to be made “discoverable” by putting it in Pairing Mode. The “discover” button can be accessed as shown in the picture at right. You may need to move the tablet aside. For more detailed Bluetooth pairing instructions, you may press the “Bluetooth Help” button at the bottom of the Connect Reader submenu.



Once the Bluetooth Identifier of the reader in your head unit appears in the Connect Reader submenu, select that reader. If necessary provide a “0000” pairing code at the prompt. When the reader is successfully paired to the tablet, the button for reader will turn blue in the Connect Reader submenu. You should then be able to select “Reader Status” on the menu and to confirm that your reader’s Bluetooth Identifier reflected.

Registering the Card Reader

Once the card reader is connected, you will then be sent to the KMS Card Reader Registration Wizard. This wizard will allow you to name the card reader and will collect admin credentials to authorize addition of the subject card reader to the enterprise. Once card reader registration is complete, the card reader is associated with that tablet in KMS and ready to start processing transactions according to enterprise settings.

Testing the Card Reader

To perform a simple functional test of the card reader, select “Test Reader” from the KMS menu. This will bring up the swipe UI as a prompt to swipe a card. Swiping a card through the card reader should result in a block of (encrypted) text appearing in the subsequent “Card Read Result” window.

If no text appears in the window, verify the orientation of the card or try a different card. If still no text appears, disconnect the tablet, reconnect the tablet to the card reader, and try again. If still no text appears in the “Test Reader/Card Read Result” window, contact Lilitab support.

Stripe Setup

To use the Stripe integration, you will need to establish and configure a Stripe account.

- **Account Setup**: Go to stripe.com and click on the "Create Account" button to get started in creating an account.

- **Set up Banking**: Once your Stripe account is created, you will need to specify a bank account in which to deposit proceeds from Stripe transactions. Select Balance/Settings from the Stripe dashboard and enter a bank account number.

- **Get API Key**: To allow KMS to direct payments to your Stripe account, you will need to enter your Stripe API Key into the correct field in the KMS dashboard. To get your key, go to the Developers/API keys page in the Stripe dashboard and copy your Secret API Key. Then log in to KMS and paste the API Key into the "Stripe API Key" field in the "Card Reader Configuration" panel on the Config tab under Enterprise Setup.

- **Allow Swipe Data**: While KMS does not handle any cardholder data, Stripe will be getting raw card swipe data, as it will be getting the necessary charge card information in decrypted form. For Stripe to accept swipe data (which may be fraudulent in other circumstances) Stripe requires explicit permission. On the Stripe dashboard, go to "Business Settings/Integration", then click "Advanced Settings" and enable "Process payments unsafely".

Web Page Setup

Once your tablet has Lilitab KMS loaded, you've configured card reading in the KMS Portal, and connected Lilitab KMS to your configured Stripe account, the last step is to add the necessary code to launch the swipe capture process from your web page.

The easiest way to do this is to view and copy source code from the swipe demo page:

https://kms.lilitab.com/api/simulator/cardReadDemo

Testing Stripe Processing

After setting up your Stripe account you can make sure everything is working properly – without actually making charges – by using a test key from Stripe.

To get your test key, go to https://dashboard.stripe.com/account/apikeys in your Stripe dashboard and click the toggle for "View test data" so that it turns orange. Click "Reveal test key token", then copy the token, log in to KMS, and paste the test key into the "Stripe API Key" field in the "Card Reader Configuration" panel on the Config tab under Enterprise Setup.

Then, in the Lilitab KMS app, use the swipe demo page (set https://kms.lilitab.com/api/simulator/cardReadDemo as the KMS home page), enter a transaction amount, and swipe the test card provided with your hardware. It should be labelled "Stripe Test Card".

If everything is configured correctly, a block of text should appear in the demo page window after the card swipe that looks something like this:


```
{
    "transactionId": "FC202621-3DC5-4598-9B57-F8D8C7C3F338",
    "cardData": {
        "status": "ok",
        "Track2": "4242000000004242=18120000000000000000",
        "Track1": "B4242000000004242^TEST/CARD 01
^18120000000000000000000000000000",
        "rawData": "\u0002%B4242000000004242^TEST/CARD 01
^18120000000000000000000000000000?;4242000000004242=18120000000000000000?|0
600|1415BACB091CC3E965CB7F92DB5C8C587DB7FF164098F6A7C14B25BE1FA5CE23242522
36D122675BAD54456DBDA24C7B39807CDFBA8F6EDC1D702D29AF688137D71D60022A6EF652
6AC9B611B24FB71A|582454FEB3E2E3839D9A51C3AEC68C3D4F91C8FE80E7433818736B336
9777FA8FBEF6212FD6A7357||61402200|E7A1C5679A36133E5C92CD5FF13A4C96A60CF259
8ED2E25C7524970419B2C0BF4B0EA0D882357ADBC8D9957DD277ED4A5A81229901888B07|B
36D8D7092616AA|B01914267E6A1A46|9011880B36D8D700003F|8D49||0000\r",
        "swipeTimestamp": "2018 Apr 18, Wed 15:44:17 PDT",
        "signature": "big block of text",
        "transaction-amount": 4,
        "readerUUID": "37FFDB054848363922880243"
    },
    "kmsServerResponse": {
        "reason": "reason message",
        "code": 201
    },
    "swipeResponse": {
        "stripeSuccessFlag": true,
        "parsedJsonPayload": {
            "amount": 500,
            "object": "charge",
            "id": "ch_1CIP0lJ8Tu4aD1LNPHRq9qct",
            "refunded": false,
            "currency": "usd",
            "refunds": {
                "has_more": false,
                "object": "list",
                "data": [],
                "total_count": 0,
                "url": "/v1/charges/ch_1CIP0lJ8Tu4aD1LNPHRq9qct/refunds"
            },
            "created": 1524091463,
            "metadata": {},
            "captured": true,
            "balance_transaction": "txn_1CIP0mJ8Tu4aD1LN2fQ2Uwxk",
            "amount_refunded": 0,
            "fraud_details": {},
            "paid": true,
            "source": {
                "last4": "4242",
                "metadata": {},
                "country": "US",
                "object": "card",
```

```
                "brand": "Visa",
                "exp_month": 12,
                "name": "TEST/CARD 01",
                "fingerprint": "L8MT5IfviohAOohB",
                "funding": "credit",
                "id": "card_1CIP0lJ8Tu4aD1LNdVDN7OHM",
                "exp_year": 2018
            },
            "status": "succeeded",
            "outcome": {
                "network_status": "approved_by_network",
                "seller_message": "Payment complete.",
                "risk_level": "normal",
                "type": "authorized"
            },
            "livemode": false
        },
```


If you see something else, double check all your settings, verify that the card reader is working (see "Testing the Card Reader" above) and make sure that the test key is properly copied into the "Stripe API Key" field in KMS.

If you swipe a **live (valid) card** while running Stripe in test mode, you will see, among the rest of the response data, the following parsedJsonPayload:


```
        "parsedJsonPayload": {
            "error": {
                "code": "card_declined",
                "message": "Your card was declined. Your request was in
test mode, but used a non test card. For a list of valid test cards,
visit: https://stripe.com/docs/testing.",
                "charge": "ch_1CAoWWJ8Tu4aD1LNVGDAGUNe",
                "type": "card_error",
                "decline_code": "test_mode_live_card"
            }
        },
```


If you swipe an **expired card** while running Stripe in test mode, you should see:


```
        "parsedJsonPayload": {
            "error": {
                "code": "expired_card",
                "charge": "ch_1CJ9psJ8Tu4aD1LNlJk9Rovc",
                "message": "Your card has expired.",
                "param": "exp_month",
                "type": "card_error",
                "doc_url": "https://stripe.com/docs/error-codes/expired-card"
            }
        },
```

If you swipe an **EMV test card** while running Stripe in test mode, you should see:

```
        "parsedJsonPayload": {
            "error": {
                "type": "invalid_request_error",
                "message": "This looks like an EMV test card but the
request is missing a valid source of ICC data. ICC data should be passed
in source[emv_auth_data]."
            }
        },
```

If the **API Key** provided in the KMS Card Reader Configuration panel is invalid, you will see:

```
        "parsedJsonPayload": {
            "error": {
                "type": "invalid_request_error",
                "message": "Invalid API Key provided:
sk_test_**********************6Uj2"
            }
        },
```

If a card is **declined** due to something like insufficient funds, you will see:

```
        "parsedJsonPayload": {
            "error": {
                "code": "card_declined",
                "charge": "ch_1CJ9S5J8Tu4aD1LNvOwTigRF",
                "message": "Your card was declined.",
                "decline_code": "generic_decline",
                "type": "card_error",
                "doc_url": "https://stripe.com/docs/error-codes/card-
declined"
            }
        },
```

If a card is declined due to it being rated as a **high risk for fraudulent activity**, you will see:

```
        "parsedJsonPayload": {
            "error": {
                "code": "card_declined",
                "charge": "ch_1CJ9XUJ8Tu4aD1LNE7Lzqt9z",
                "message": "Your card was declined.",
                "decline_code": "fraudulent",
                "type": "card_error",
                "doc_url": "https://stripe.com/docs/error-codes/card-
declined"
            }
        },
```

If a card is declined due to in **incorrect security code** (a highly unlikely occurrence for a non-fraudulent card-present transaction) you will see:


```
        "parsedJsonPayload": {
            "error": {
                "code": "incorrect_cvc",
                "charge": "ch_1CJ9k4J8Tu4aD1LN8llrdikk",
                "message": "Your card's security code is incorrect.",
                "param": "cvc",
                "type": "card_error",
                "doc_url": "https://stripe.com/docs/error-codes/incorrect-cvc"
            }
        },
```


If a card has an incorrect number because it **fails its checksum (Luhn Test)**, you will see:


```
        "parsedJsonPayload": {
            "error": {
                "code": "incorrect_number",
                "message": "Your card number is incorrect.",
                "param": "number",
                "type": "card_error",
                "doc_url": "https://stripe.com/docs/error-codes/incorrect-number"
            }
        },
```


Stripe ideally wants testing done by using specific “test numbers”. These numbers can be seen at https://stripe.com/docs/testing#cards. To use with a card reader, these numbers need to be programmed onto the magnetic strip of test cards. A set of these cards may be made or purchased from Lilitab. If you need Stripe test cards, contact your Lilitab project coordinator or sales representative.

These test cards are useful for verifying that your web asset properly handles potential error conditions, including:

- Charge succeeds with elevated risk_level
- Charge declined with a card_declined code
- Charge blocked due to risk level of “highest”
- Charge is declined with an incorrect_cvc code
- Charge is declined with an expired_card code
- Charge is declined with a processing_error code
- Charge declined with an incorrect_number code (fails the Luhn check)

Going Live!

Once you have gotten a successful test swipe using a Test Key from Stripe and a Stripe Test Card from Lilitab, and verified that your application handles common error codes, the next step is to go live! This entails simply exchanging the test key with your live key. To get your live key from Stripe, go to https://dashboard.stripe.com/account/apikeys in your Stripe dashboard and click the toggle for "View test data" so that it turns gray. Then click "Reveal live key token", copy the token, log in to KMS, and paste the **live key** into the "Stripe API Key" field in the "Card Reader Configuration" panel on the Config tab under Enterprise Setup. Then click "Save Changes" at the right end of the Enterprise Setup footer.

Once the live key is in place, card swipes will process normally and will result in funds transfer from the credit account to the bank account specified in Stripe.

Other Payment Platforms

In addition to the software integration with the eDynamo and Stripe, as described above, Lilitab offers **hardware integrations** with the Verifone e355, the Square Contactless and Chip Reader, and the Magtek MagneSafe Intellihead OEM MSR. A hardware integration means that the Lilitab Head Unit will hold the device in an attractive and ergonomic fashion and provide power to the device. Software connectivity must be implemented by the customer using a custom iOS app. The Verifone e355 communicates via either Bluetooth or WiFi, and the Square Contactless and Chip Reader communicates with the tablet via Bluetooth. In both cases, customers will need to integrate the appropriate SDK into their own custom iOS app in order to utilize these card readers. As well, customers can integrate the **KMS SDK** into their custom app. KMS SDK allows customers to deploy a full suite of remote management and network monitoring tools, leveraging the KMS administration portal, and eliminating the need to develop a server-side database application.

Lilitab HX Pro with Verifone e355

Barcode Reading

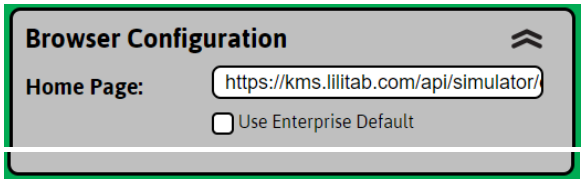
KMS offers two grades of integrated barcode reading for you to use inside your web application.

Lilitab KMS supports both free consumer-grade barcode scanning (as provided by the Apple AVCaptureMetadataOutput method), and advanced commercial-grade decoding with enhanced recognition speed and additional format support.

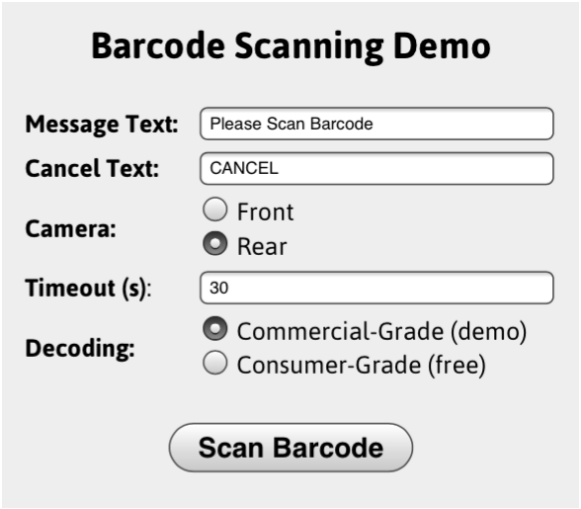
Consumer-Grade Decoding (free with KMS)	**Commercial-Grade Decoding (subscription)**
Formats: Aztec, Code 25, Code 39, Code 93, Code 128, Data Matrix, EAN, Interleaved 2of5, ITF14, PDF417, QR Code, and UPC	**Formats:** All consumer formats, at enhanced recognition speed, plus Codabar, Code 11, DotCode, GS1 Databar, MaxiCode, MSI Plessey, and Postal Barcodes

Barcode Reading Setup

Step 1: To set up the demo page as your browser home page, go the Group Setup page, open the Browser Configuration tab and specify https://kms.lilitab.com/api/simulator/cardReadDemo as your Home Page.

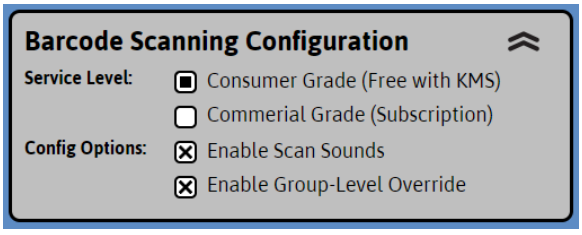


Step 2: Exiting the KMS portal will return you to your newly-specified home page, as shown below.



Step 3: On the web page, specify the desired options, then press the "Scan Barcode" button. This will bring up the barcode scanning UI. When a barcode is visible to the camera, it will capture and decode the barcode, returning the result to the web application.

Step 4: After using the demo page to test your intended barcode format, you may wish to enable commercial grade encryption. Production commercial-grade encryption (no asterisks) requires that a valid payment method be established in your KMS account.



Note that when you select commercial grade decoding in the demo page, you will see asterisks (*) in the scan result. Asterisks will be present until you begin a subscription for commercial grade encryption. Commercial-grade encryption provides faster decoding and many more decode types.

How it Works

Lilitab KMS provides a managed browser in which your web application runs. Your web application can invoke supported tablet functions and accessories through simple javascript calls. In the case of barcode scanning, the salient portions of the HTML and javascript source for the demo page are as follows:

```
<table>
<tr>
    <td><b>Message Text:</b></td>
    <td><input type="text" id="message" eXcize="27" value="Please Scan Barcode"></td>
</tr><tr>
    <td><b>Cancel Text:</b></td>
    <td><input type="text" id="cancel" eXcize="27" value="CANCEL"></td>
</tr><tr>
    <td><b>Camera:</b></td>
    <td>
        <input type="radio" name="camera" value="Front" id="camera_r1" checked><label
for="camera_r1"> Front</label><br>
        <input type="radio" name="camera" value="Rear" id="camera_r2"> <label
for="camera_r2">Rear</label></td>
</tr><tr>
    <td><b>Timeout (s)</b>:</td>
    <td><input type="text" id="timeout" eXcize="27" value="30"></td>
</tr><tr>
    <td><b>Decoding:</b></td>
    <td>
        <input type="radio" name="sdk" value="Manatee" id="sdk_r1" checked> <label
for="sdk_r1">Commercial-Grade (demo)</label><br>
        <input type="radio" name="sdk" value="Apple" id="sdk_r2"> <label
for="sdk_r2">Consumer-Grade (free)</label>
    </td>
</tr><tr>
    <td colspan=2><br></td>
</tr><tr>
    <td colspan=2 align="center">
    <button onclick="lilitabBarcodeScan()"><b>Scan Barcode</b></button></td>
</tr><tr>
    <td colspan=2><br><br></td>
</tr><tr class="results">
    <td><b>Result:</b></td>
    <td><input type="text" id="result" eXcize="27"></td>
</tr><tr class="results">
    <td><b>Barcode Type:</b></td>
    <td><input type="text" id="barcodeType" eXcize="27"></td>
</tr><tr class="results">
    <td><b>Barcode:</b></td>
    <td><input type="text" id="barcode" eXcize="27"></td>
</tr><tr class="results">
    <td colspan=2><br></td>
</tr><tr class="results">
    <td colspan=2 align="center">
        <button onclick="clearResults()"><b>Clear Results</b></button></td>
</tr>
</table>

<script>

    function lilitabBarcodeScan()
```

```
    {
        setResultsView(false);

        document.getElementById("barcodeType").value = "";
        document.getElementById("barcode").value = "";

        var dict = {
            "action":"scanBarcode",
            "kmsResultMethod":"lilitabBarcodeScanned"
        };

        dict["message"] = document.getElementById("message").value;
        dict["cancel"] = document.getElementById("cancel").value;
        dict["camera"] = document.querySelector('input[name="camera"]:checked').value;
        dict["sdk"] = document.querySelector('input[name="sdk"]:checked').value;
        dict["timeout"] = document.getElementById("timeout").value;


window.webkit.messageHandlers.lilitabAppExecute.postMessage(JSON.stringify(dict));
    }

    function lilitabBarcodeScanned(bcObj)
    {
        document.getElementById("result").value = bcObj.result;
        document.getElementById("barcodeType").value = bcObj.type;
        document.getElementById("barcode").value = bcObj.barcode;
    }
```

You can access the complete HTML and javascript source code electronically at https://kms.lilitab.com/api/simulator/barcodeDemo.

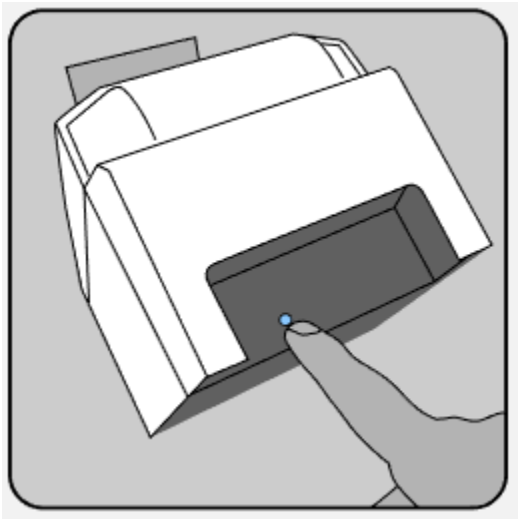
Receipt Printing

KMS supports Bluetooth receipt printing using Star Micronics thermal receipt printers, such as the TSP650, with Bluetooth module (Star Micronics P/N 39449870). For other Star printers and printers from other manufacturers, please contact Lilitab support to confirm that your printer is supported.

Printer Setup

Step 1: First plug your Star Micronics printer in and verify that the greet printer power light in front is illuminated.

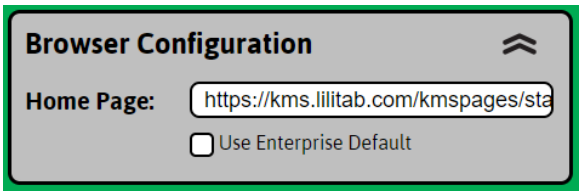
Step 2: In the back of the printer, next to the power inlet, is the pairing button (see picture below). Press and hold the pairing button for at least 6 seconds. When the button is released, the pairing light should start blinking.



Step 3: On your tablet, go to the Bluetooth section of iPad Settings. Turn Bluetooth on. In the "Other Devices" section, you should see a device called "Star Micronics". Tap on that device to pair the printer with the tablet. When paired, the printer will show in the "My Devices" section.

Step 4: You can verify successful pairing by executing a test print from the KMS menu. If the test print is not successful, you may need to repeat the pairing process. Consult the printer manual for additional information and printer troubleshooting.

Step 5: To set up the demo page as your browser home page, go the Group Setup page, open the Browser Configuration tab and specify https://kms.lilitab.com/kmspages/static/print.html as your Home Page.



Step 6: Exiting the KMS portal will return you to your newly-specified home page, which looks like the image below:

Step 7: The large form area in the middle of the demo page receives the text that your web app would generate for printing. Follow the example on the demo page to create your own receipt. The Lilitab KMS app sends the commands entered into this form to the printer, following the syntax as outlined in the StarPRNT iOS SDK User's Manual.

Supported Printer Commands

Lilitab KMS provides a managed browser in which your web application runs. Your web application can invoke supported tablet functions and accessories through simple javascript calls. In the case of receipt printing, the salient portions of the HTML and javascript source for the demo page are as follows:

To send a job for printing, the web application sends a JSON object containing the print commands and data to the starPrint action using the LilitabAppExecute method. The JSON print data object has two top-level parameters, “emulation” and “data”. The “data” object can be an array of objects, each of which contains a supported starPrint method and any associated arguments.

The supported starPrint methods are as follows:

appendCodePage

appendCodePage is used to enable special character sets. Refer to the StarPRNT iOS SDK manual for details. For standard character set use:

```
{"appendCodePage":"SCBCodePageTypeUTF8"}
```

appendInternational

appendInternational is used to enable international character sets. Refer to the StarPRNT iOS SDK manual for details. For USA character set use:

{"appendInternational":"SCBInternationalTypeUSA"}

appendFontStyle

Sets the font style for printing:

SCBFontStyleTypeA (7x9 on 12x24 spacing)
SCBFontStyleTypeB (5x9 on 9x24 spacing)

Sample:

```
{"appendFontStyle":"SCBFontStyleTypeB"},
{"appendData":"Font Style Type B\n"},
{"appendFontStyle":"SCBFontStyleTypeA"},
{"appendData":"Font Style Type A\n"}
```

appendCharacterSpace

Sets the character spacing to a specified number of dots.

Sample:

```
{"appendCharacterSpace":8},
{"appendData":"Wide Spacing\n"},
{"appendCharacterSpace":0},
{"appendData":"Default Spacing\n"}
```

appendAlignment

Sets the line alignment to one of the following:

SCBAlignmentPositionLeft
SCBAlignmentPositionCenter
SCBAlignmentPositionRight

Sample:

```
{"appendAlignment":"SCBAlignmentPositionLeft"},
{"appendData":"Left Alignment\n"},
{"appendAlignment":"SCBAlignmentPositionCenter"},
{"appendData":"Center Alignment\n"},
{"appendAlignment":"SCBAlignmentPositionRight"},
{"appendData":"Right Alignment\n"}
```

appendInvert

When sent with “YES” begins printing of inverted text; continues until appendInvert with “NO”:

Sample:

```
{"appendInvert":"YES"},
{"appendData":"Inverted\n"},
{"appendInvert":"NO"},
{"appendData":"Not Inverted\n"}
```

appendDataWithInvert

Prints associated data with inverted style.

Sample:

```
{"appendDataWithInvert":"Inverted\n"},
{"appendData":"Not Inverted\n"}
```

appendDataWithEmphasis

Prints the associated data with underline style:

Sample:

```
{"appendDataWithEmphasis":"Emphasis\n"},
```

appendDataWithUnderLine

Prints the associated data with underline style:

Sample:

```
{"appendDataWithUnderLine":"Underline\n"}
```

appendLineFeed

Prints a single line feed.

Sample:

```
"appendLineFeed"
```

appendMultipleWidth

Changes the width of printed characters to the specified multiple of regular width.

Sample:

```
{"appendMultipleWidth":2},
{"appendData":"Double Width\n"},
{"appendMultipleWidth":1},
{"appendData":"Single Width\n"}
```

appendMultipleHeight

Changes the height of printed characters to the specified multiple of regular height.

```
{"appendMultipleHeight":2},
{"appendData":"Double Height\n"},
{"appendMultipleHeight":1},
{"appendData":"Single Height\n"}
```

appendDataWithMultiple

Prints a specified data string with specified width and height, without changing the general width and height of subsequent printing.

Sample:

```
{"appendDataWithMultiple":{"data":"Wide and
Tall\n","width":2,"height":"2"}}
```

appendLineSpace

Uses the specified amount of space between lines, in dots, for any printed text that follows. The following prints the lines at 32-dot spacing spacing, and then changes to 24-dot line spacing.

Sample:

```
{"appendLineSpace":32},
{"appendData":"32 Dot\n"},
{"appendData":"Line Spacing\n"},
{"appendLineSpace":24}
{"appendData":"24 Dot\n"},
{"appendData":"Line Spacing\n"},
```

appendCutPaper

Cuts the paper at the current location in one of the following styles:

SCBCutPaperActionFullCut
SCBCutPaperActionPartialCut
SCBCutPaperActionFullCutWithFeed
SCBCutPaperActionPartialCutWithFeed

Sample:

```
{"appendData":"Cut Paper Here\n"},
{"appendCutPaper":"SCBCutPaperActionPartialCut"}
```

appendPeripheral

Sends a pulse of duration “time” to peripheral “channel”. Most commonly, this can be used to release a cash drawer, usually on channel 1.

Sample:

```
{"appendPeripheral":{"channel":"1","time":"1000"}},
{"appendPeripheral":{"channel":"2","time":"1000"}}
```

```
<textarea rows="30" cols="100" Id="printJSON">
{
    "emulation":"StarIoExtEmulationStarLine",
    "data": [
        {"appendCodePage":"SCBCodePageTypeUTF8"},
        {"appendInternational":"SCBInternationalTypeUSA"},
        {"appendFontStyle":"SCBFontStyleTypeB"},
        {"appendData":"Font Style Type B\n"},
        {"appendFontStyle":"SCBFontStyleTypeA"},
        {"appendData":"Font Style Type A\n"}
        {"appendCharacterSpace":8},
        {"appendData":"Wide Spacing\n"},
        {"appendCharacterSpace":0},
        {"appendData":"Default Spacing\n"}
        {"appendAlignment":"SCBAlignmentPositionLeft"},
        {"appendData":"Left Alignment\n"},
        {"appendAlignment":"SCBAlignmentPositionCenter"},
        {"appendData":"Center Alignment\n"},
        {"appendAlignment":"SCBAlignmentPositionRight"},
        {"appendData":"Right Alignment\n"}
        {"appendInvert":"YES"},
        {"appendData":"Inverted\n"},
        {"appendInvert":"NO"},
        {"appendData":"Not Inverted\n"}
        {"appendDataWithInvert":"Inverted\n"},
        {"appendData":"Not Inverted\n"}
        {"appendDataWithEmphasis":"Emphasis\n"},
        {"appendDataWithUnderLine":"Underline\n"}
"appendLineFeed"
        {"appendMultipleWidth":2},
        {"appendData":"Double Width\n"},
        {"appendMultipleWidth":1),
        {"appendData":"Single Width\n"}
        {"appendMultipleHeight":2},
        {"appendData":"Double Height\n"},
        {"appendMultipleWidth":1},
        {"appendData":"Single Height\n"}
        {"appendDataWithMultiple":{"data":"Wide and Tall\n","width":2,"height":"2"}}
        {"appendLineSpace":32},
        {"appendData":"32 Dot\n"},
        {"appendData":"Line Spacing\n"},
        {"appendLineSpace":24}
        {"appendData":"24 Dot\n"},
        {"appendData":"Line Spacing\n"},
        {"appendData":"Cut Paper Here\n"},
        {"appendCutPaper":"SCBCutPaperActionPartialCut"}
        {"appendPeripheral":{"channel":"1","time":"1000"}},
    ]
}
</textarea>
<br>
<button style="height:50px;width:100px" onclick="starPrint()">Print</button>
<br>
<br>
Result:
<textarea rows="3" cols="100" Id="printJSONResult">
</textarea>
<br>
<script>
    function starPrint()
    {
        var printJSON = document.getElementById("printJSON").value;
        var obj = {'action':'starPrint',"kmsResultMethod":"starPrintCompletion"};
        obj['printData'] = printJSON;
```

```
        var jsonString = JSON.stringify(obj);
        window.webkit.messageHandlers.lilitabAppExecute.postMessage(jsonString);
    }

    function starPrintCompletion(printObj)
    {
        document.getElementById("printJSONResult").value = printObj.result;
    }
</script>
```

You can access the complete HTML and javascript source code electronically at https://kms.lilitab.com/api/simulator/print.html.

Appendix A: SmartDOCK Troubleshooting

If the SmartDOCK won't lock or unlock

- Be sure the USB cable is plugged into the power supply, the power supply is plugged into the wall, and the wall outlet has power. The SmartDOCK motor will not operate unless the SmartDOCK is plugged in.
- Make sure the correct PIN is being used. If a user PIN isn't working or has been forgotten, please see "if a PIN is forgotten or not working" below.
- If needed, the key may be used to lock or unlock the SmartDOCK at any time.

If a PIN or Password is forgotten or not working

- If new users are set up, they will enter and confirm their PIN the first time they use the PIN Pad.
- If a user forgets their PIN, it can be renewed by the Group Owner or a Group Manager from the user's detail page in the Local Group Admin interface. After PIN Renew, the user will be asked to enter and confirm a new PIN the next time they log in.
- If a Group admin forgets their password, it can be recovered by clicking "forgot password" on the portal login screen and completing the password recovery process.

To reset the SmartDOCK

- Remove the head unit with the key by inserting the key, pushing inward, and turning it counterclockwise 90 degrees. **Return the key to the center position before removing the key.** Remove the head unit.
- With the head removed, unplug the SmartDOCK USB connector from the power supply.
- Wait at least 10 seconds.
- Plug the USB connector back into the power supply. Wait until the SmartDOCK resets.
- Replace the head unit onto the SmartDOCK. The SmartDOCK should lock normally.

If more help is needed, please call Lilitab Product Support at (888)705-0190
or http://www.lilitab.com/pages/support

Appendix B: App Settings

App settings can be accessed via the System Settings interface on the tablet. To access Settings, tap on the Settings icon on the Home Page, then scroll down in the left hand column until you see the Lilitab KMS icon. Tap this icon to access KMS settings.

At the top of the screen are the access settings:

Setting	Purpose	Recommended Setting
Location	Used to provide tablet location to service. **Must be enabled to use geofence.**	On
Camera	Used on the PIN Pad screen to capture QR Code badge.	On
Notifications	Used to notify for app updates	On
Background App Refresh	Used to allow app to monitor geofence and continue updating server when in background	On

Below the access settings are the tablet coordinates, which allow the user to identify the tablet and assign it to an enterprise and group.

Setting	Purpose	Recommended Setting
Enterprise ID	Use to specify or change Enterprise ID for device configuration in company network	Enterprise ID
Group ID	Use to specify or change Group ID for device configuration in company network	Group ID
Tablet ID	Use to specify or change Tablet ID for device configuration in company network	Tablet ID

Any changes to the tablet coordinates will launch the Registration wizard next time the app is returned to. If settings changes would require the tablet to change groups, an owner/admin (with owner or higher permission) from the originating group, as well as an owner/admin from the destination group, will be required to approve. If admin approval fails, the previous settings will be restored. If the tablet will change TabletID but stays in the same group, then only an owner/admin from that group is required to approve.