



Features Document

MERCHANT MANAGER SYSTEM

VERSION: 2.5

REVISION DATE: 05/24/2026

Contents

Introduction 4

System Overview..... 5

Feature Overview 6

1. Login & User Authentication..... 6

2. App Manager 8

 2.1. Manage Apps 8

 2.2. Assign Applications 9

3. Cloud Security 12

 3.1. Cloud Security Template..... 12

 3.2. Assign Cloud Security - Restrict Access..... 14

4. Stakeholders (Person, Company, Merchant...) 16

 4.1. Person 16

 4.2. Company 18

 4.3. Merchant 21

 4.4. Charities 25

 4.5. Processors 26

5. Device Manager 28

 5.1. Device Registry 28

 5.2. Device Manager 30

 5.3. Hardware Management 49

6. Global Setup..... 50

 6.1 Settings 50

 6.2 Timeouts 52

 6.3 Industry Categories 53

7. Audit Log 55

8. Bulk Changes 57

 8.1. Template Amendments 57

 8.2. Base Template Assign 57

Introduction

This document provides an overview of the **Merchant Management System (MMS)**, including existing features, features currently under development, and planned enhancements, together with their current status and estimated delivery timelines.

The system is designed to manage and operate payment terminals in a centralized manner. It supports the management of terminals, merchants, and companies, and allows administrators to configure and deploy data to terminals efficiently.

Key capabilities of the system include terminal configuration, application and firmware deployment, template-based setup, and centralized control of terminal-related data. The system also supports role-based access control, allowing users to be assigned permissions based on company, role, and organizational responsibilities.

This document is intended for project stakeholders and business users to gain a high-level understanding of the system's capabilities and current delivery status. Detailed technical specifications and implementation details are out of scope for this document.

System Overview

The **Merchant Management System (MMS)** is a centralized platform used to manage payment terminals across multiple companies and merchants.

The system enables administrators to register, configure, and maintain terminals, as well as manage merchant and company structures. It allows operational data and configurations to be prepared centrally and deployed to terminals in a controlled and consistent manner.

At a high level, the system supports:

- Terminal lifecycle management, including setup, configuration, and maintenance
- Company and merchant management with hierarchical relationships
- Centralized deployment of applications, firmware, and configuration templates to terminals
- Role-based access control, allowing user permissions to be defined by company and job role

The system is accessed through a web-based interface and is intended for administrators and operational users responsible for terminal operations and system configuration.

At the time of this document, the system includes core terminal and user management capabilities, with additional features being actively developed and enhanced.

Feature Overview

This section provides a high-level overview of system features with brief descriptions and reference images. Each feature includes its current status and, where applicable, estimated delivery timelines.

1. Login & User Authentication

Description

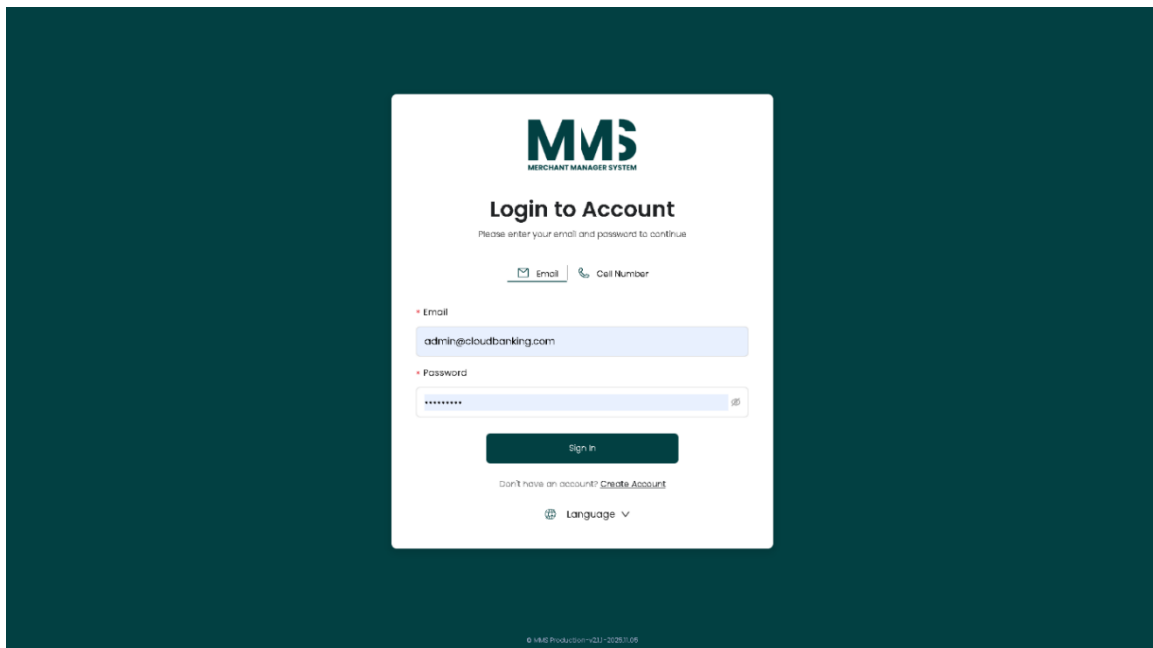
Allows users to securely access the system using admin-provided credentials. The login process includes email/password authentication, OTP verification via email, and company/merchant selection based on the user's assigned permissions. Access to system functions is restricted according to the user's role and company scope.

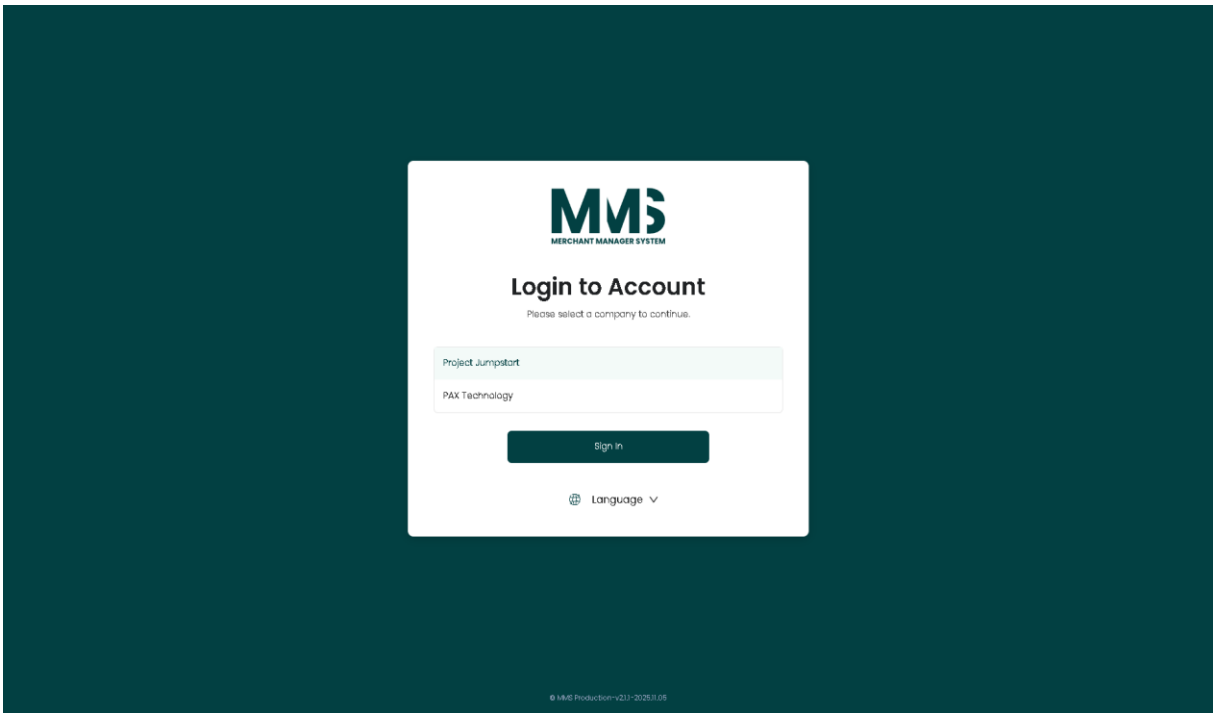
Key Capabilities

- Authenticate users using admin-provided credentials
- Verify user identity through OTP email verification
- Support access to multiple companies and merchants based on assigned permissions
- Enforce role-based access control across system features

Status: **Completed**

Reference Images:





2. App Manager

2.1. Manage Apps

Description

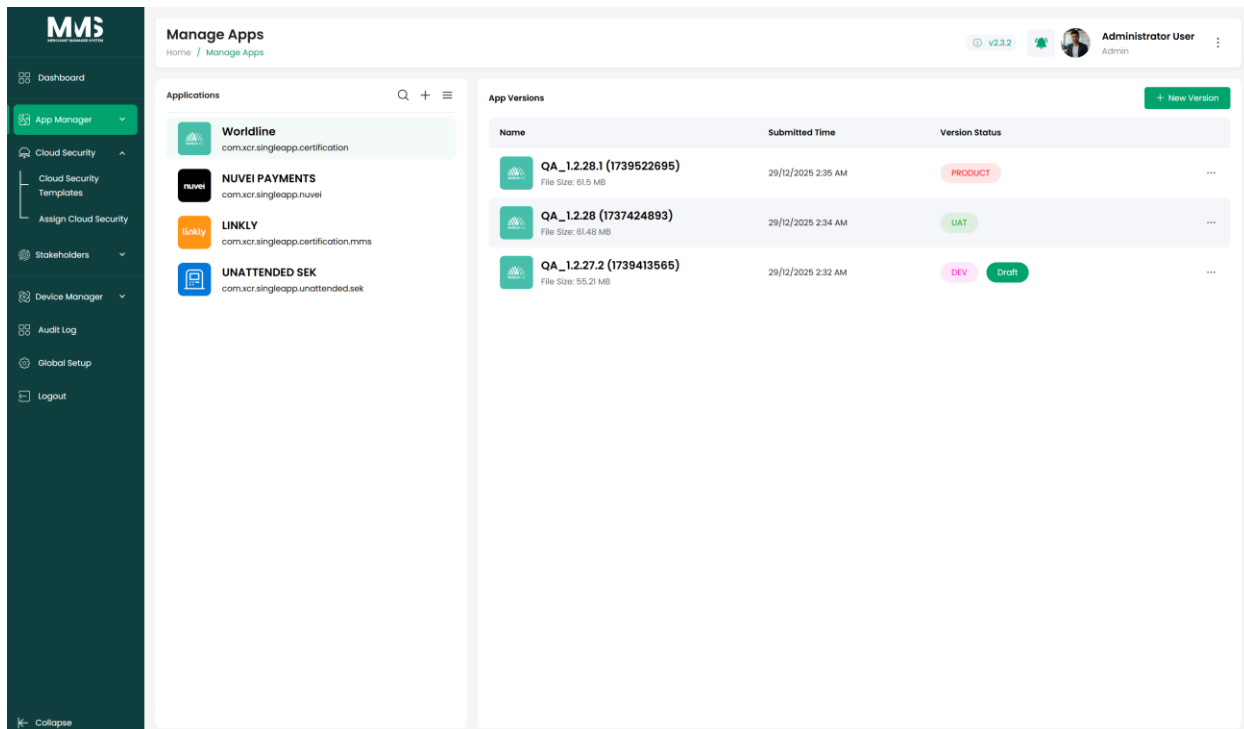
Provides centralized management of applications used on terminals, allowing administrators to create applications and upload multiple APK versions. The system automatically reads and displays application metadata to support version control and deployment management.

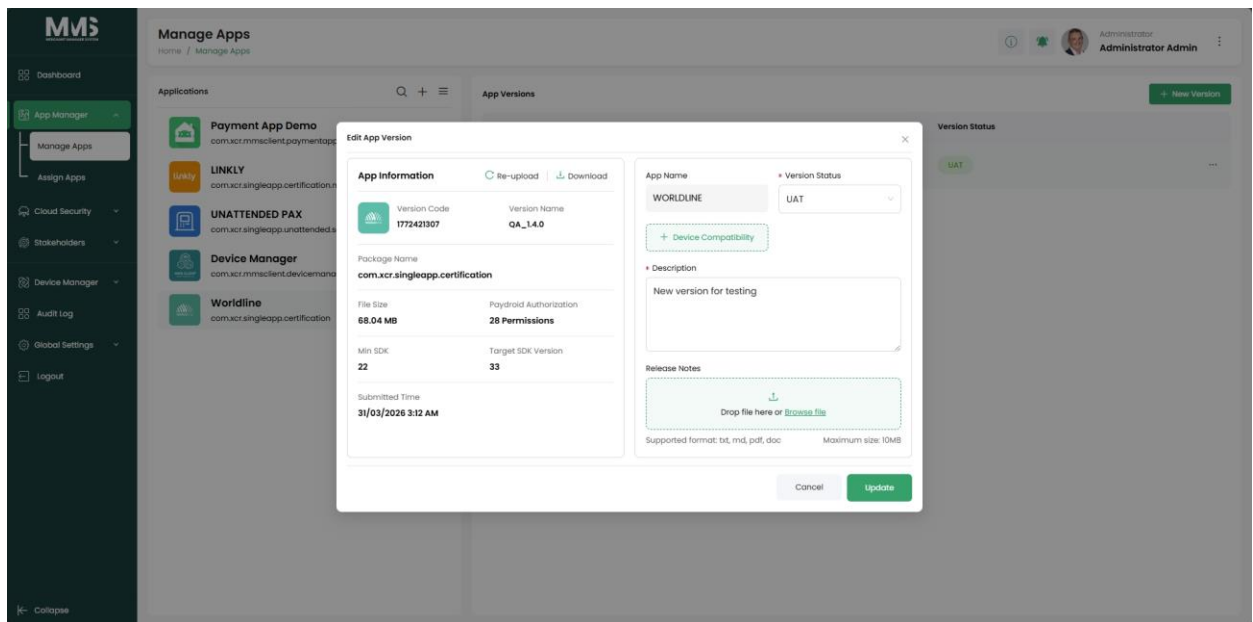
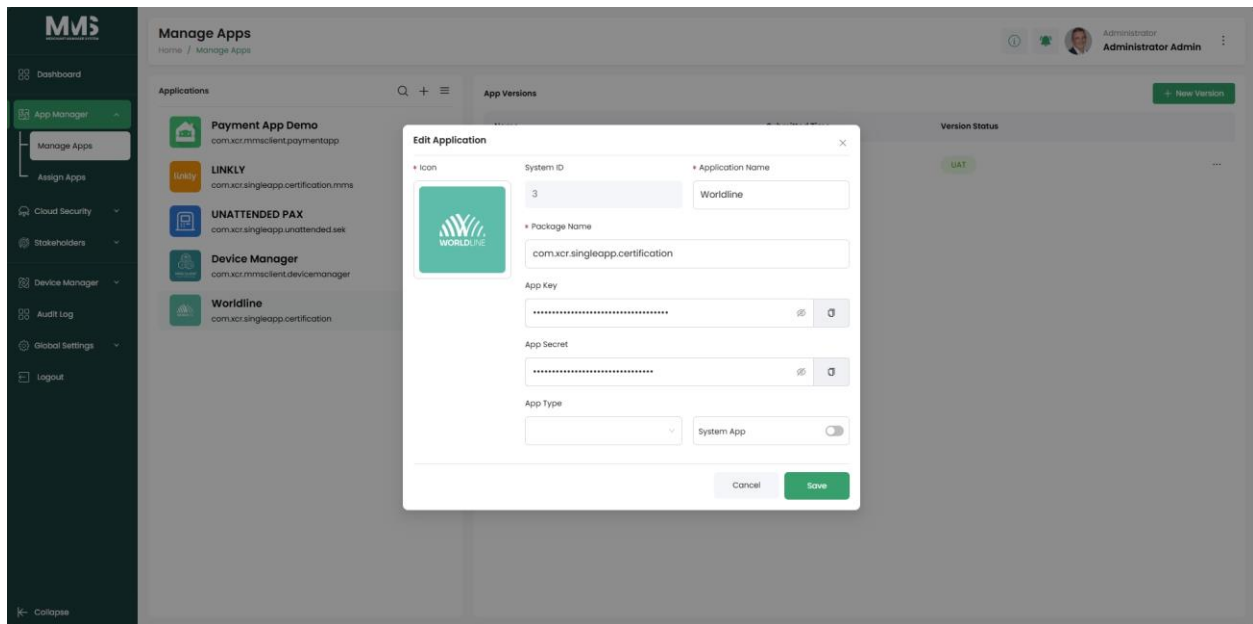
Key Capabilities

- Create and manage applications within the system
- Upload and manage multiple APK versions per application
- Automatically extract and display application metadata, including:
 - Package name
 - Application name
 - Version and build number
 - Application icon
 - ...

Status: Completed

Reference Images:





2.2. Assign Applications

Description

Allows administrators to assign specific applications and application versions to companies or company groups. Based on the assigned app version, administrators can create and manage base templates to define standardized configuration settings that are applied consistently across merchants and terminals.

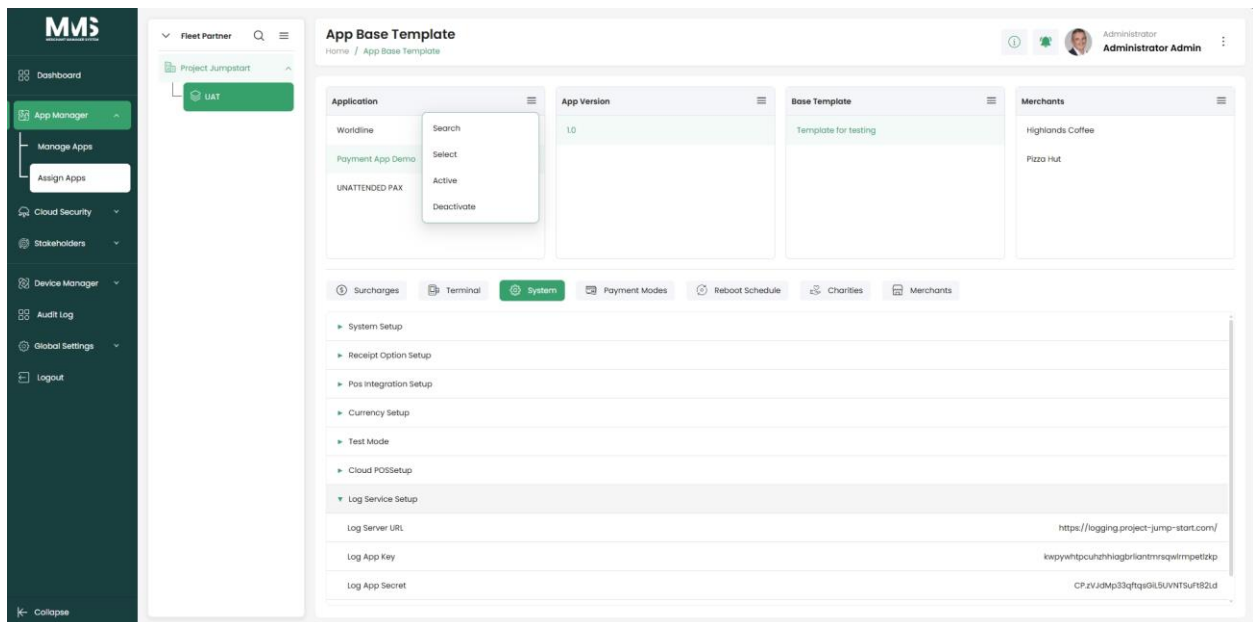
Base templates act as dynamic configuration models, enabling flexible setup of system behavior, security, and functional modules without being constrained by fixed layouts. These configurations can be reused, activated, or adjusted as needed, and are propagated to merchants and devices within the assigned scope.

Key Capabilities

- Assign applications and specific app versions to companies or company groups
- Create and manage base templates derived from assigned app versions
- Configure company-level settings such as system setup, security, modules, and operational parameters
- Support dynamic template structures that adapt to application requirements
- Apply base templates globally to merchants and automatically propagate settings to associated terminals
- Enable activation, deactivation, and version control of base templates

Status: **Completed**

Reference Images:



MMS
MERCHANT MANAGER SYSTEM

- Dashboard
- App Manager
- Organizations
- Cloud Security
- Management
- Devices
- Settings
- Logout

⌵ Collapse

App Base Template Setup

Home / App Base Template / App Base Template Setup

v2.1.0
Administrator User
Admin

Export
Import (Json/XML)
Copy Template
Save Changes

Template Name	Company Name	Application	Application Version
	Project Jumpstart	Payment wf	QA_1.4.0

Categories

- Surcharges
- Terminal
- System
- Payment Modes
- Reboot Schedule
- Chorties
- Merchants

Edit Mode

Terminal

Contactless Enabled

CPIN Characters

ActiveAccessDate

DeActiveDate

TerminalInstallTime

Contactless Time Delay Enabled

id

ActiveAccessTime

DeActiveTime

TimeZoneMasterid

Contactless Time Delay

TerminalSerialNumber

TerminalServiceDetails

TerminalInstallDate

BusinessStartTime

MMS Document

Page 11 of 57

3. Cloud Security

3.1. Cloud Security Template

Description

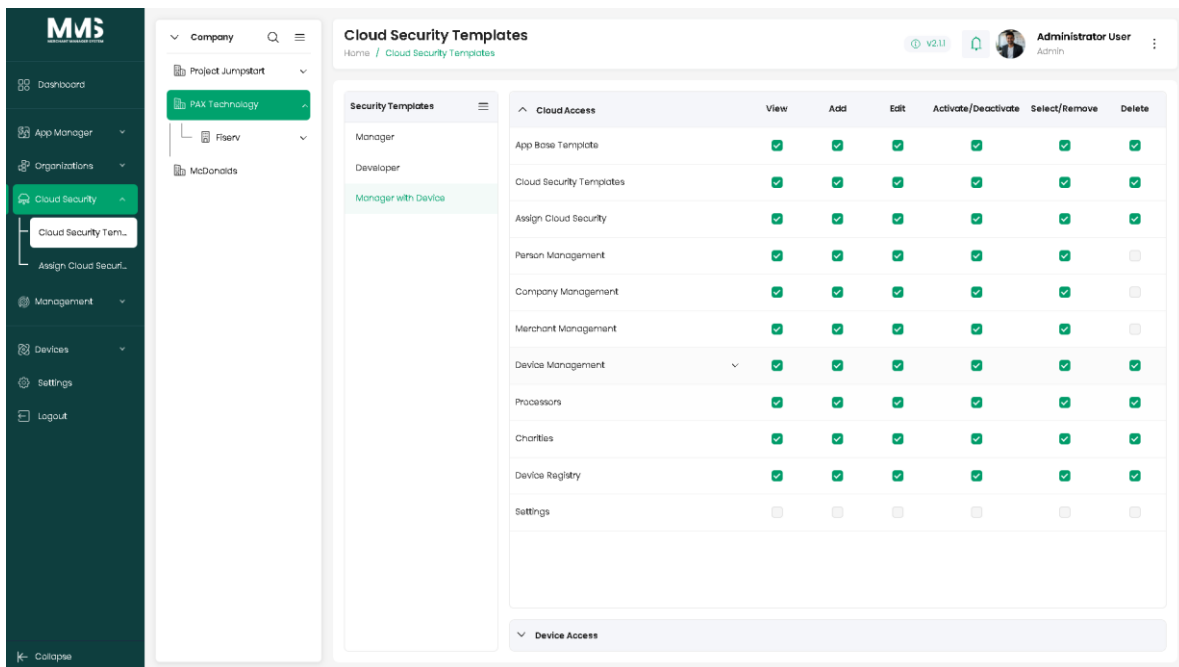
Allows administrators to define reusable permission templates that represent roles within a company, such as managers or operators. Each template specifies what actions users can perform in the cloud system and which devices they are allowed to manage. These templates can be applied to multiple users at once, ensuring consistent access control without configuring permissions individually for each user.

Key Capabilities

- Create role-based permission templates at the company or group level
- Define allowed actions across cloud modules and system functions
- Restrict or grant access to specific devices within the assigned scope
- Simplify user onboarding and permission management through reusable templates

Status: **Completed**

Reference Images:



Template Details
Home / Cloud Security Templates / Template Details

Administrator User Admin

Security Template

Company Name: PAX Technology | Template Name: Manager with Device | Access to All Devices:

Cloud Access	View	Add	Edit	Activate/Deactivate	Select/Remove	Delete
Device Access <input type="checkbox"/> SN Search by SN + Assign Device						
SN	Brand/Model	Merchant	Status			
<input type="checkbox"/> TLLI000000	Pax A920	Highlands Coffee	Activated	...		
<input type="checkbox"/> TLLI000001	Pax A920	Highlands Coffee	Activated	...		
<input type="checkbox"/> TLLI000002	Pax A920	Highlands Coffee	Activated	...		

10 Items | Showing 1-3 of 3

Assign Device Access

Device Manager Filter

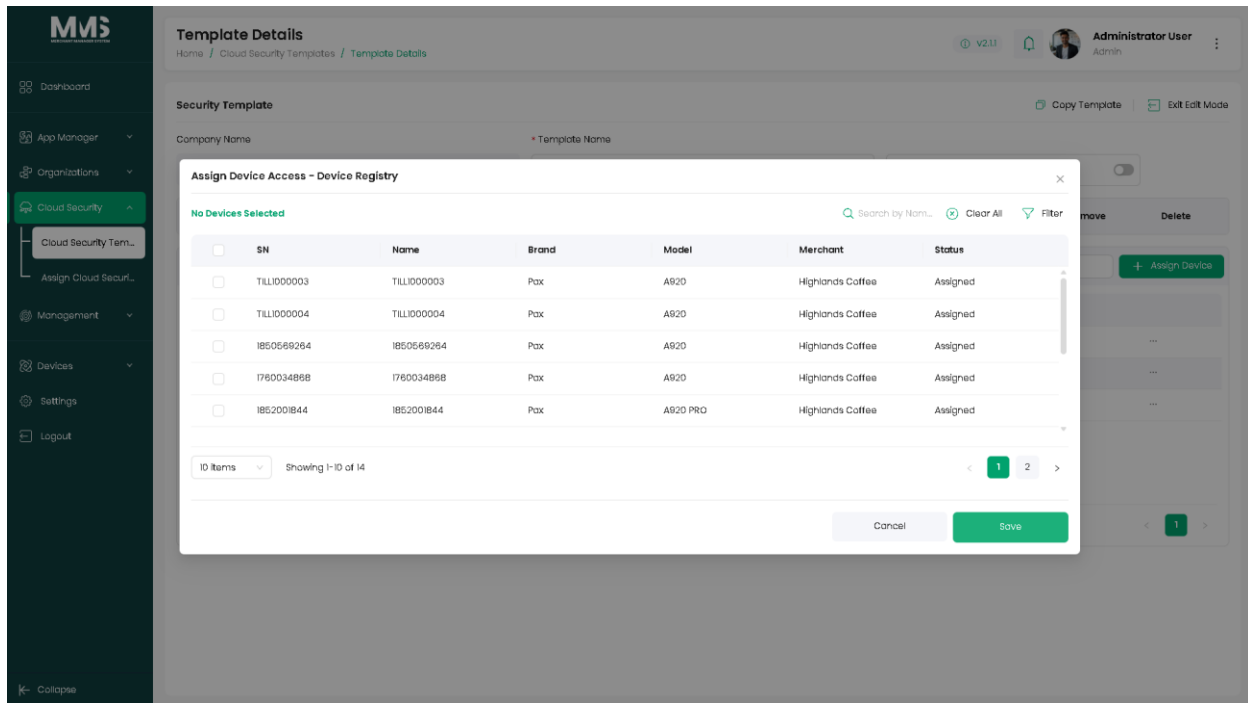
Company: Project Jumpstart | Group: DEV | Merchant: Highlands Coffee

Region	Country	State	City	Suburb	Location Area	Merchants
All	All					All
Asia Pacific	Australia					Highlands Coffee
East Asia	Japan					
Oceania	New Zealand	No data	No data	No data		
South Asia	Singapore					
Southeast Asia						

Device Registry Filter

Owner: All | Group: All | Status: All

Cancel Save



3.2. Assign Cloud Security - Restrict Access

Description

Allows administrators to assign company- or group-specific security templates to users, enabling consistent and role-based access control across the system. Assigned users automatically inherit all permissions defined in the selected security template upon login.

Key Capabilities

- Assign security templates to users within a selected company or group
- Apply predefined role-based permissions across cloud modules and device management
- Support bulk user assignment to simplify access management
- Automatically enforce template permissions when users access the system

Status: **Completed**

Reference Images:

MMS

- Dashboard
- App Manager
- Organizations
- Cloud Security
- Cloud Security Tem...
- Assign Cloud Secur...
- Management
- Devices
- Settings
- Logout

Assign Cloud Security

Home / Assign Cloud Security

v2.1.1
Administrator User
Admin

Security Templates

- Manager
- Developer
- Manager with Device

User Access

Duc Dang

Cloud Actions

- View
- Add
- Edit
- Activate/Deactivate
- Select/Remove
- Delete

Cloud Access	View	Add	Edit	Activate/Deactivate	Select/Remove	Delete
App Base Template	✓	✓	✓	✓	✓	✓
Cloud Security Templates	✓	✓	✓	✓	✓	✓
Assign Cloud Security	✓	✓	✓	✓	✓	✓
Person Management	✓	✓	✓	✓	✓	✓
Company Management	✓	✓	✓	✓	✓	✓
Merchant Management	✓	✓	✓	✓	✓	✓
Device Management	✓	✓	✓	✓	✓	✓
Processors	✓	✓	✓	✓	✓	✓

MMS

- Dashboard
- App Manager
- Organizations
- Cloud Security
- Cloud Security Tem...
- Assign Cloud Secur...
- Management
- Devices
- Settings
- Logout

Edit Assign Cloud Security

Home / Assign Cloud Security / Edit Assign Cloud Security

v2.1.1
Administrator User
Admin

Security Template

Company Name: PAX Technology

Template Name: Manager

User Name: Duc Dang

Discard Changes
Save Changes

Cloud Access	View	Add	Edit	Activate/Deactivate	Select/Remove	Delete
App Base Templates	□	✓	✓	✓	✓	✓
Cloud Security Templates	□	✓	✓	✓	✓	✓
Assign Cloud Security	□	✓	✓	✓	✓	✓
Person Management	□	✓	✓	✓	✓	✓
Company Management	✓	✓	✓	✓	✓	✓
Merchant Management	✓	✓	✓	✓	✓	✓
Device Management	✓	✓	✓	✓	✓	✓
Processors	✓	✓	✓	✓	✓	✓
Charities	✓	✓	✓	✓	✓	✓
Device Registry	✓	✓	✓	✓	✓	✓

4. Stakeholders (Person, Company, Merchant...)

4.1. Person

Description

Provides centralized management of system users, allowing administrators to create, update, and maintain user accounts within the cloud system. Person Management supports user information management, access control, and account security across companies and assigned device scopes.

Key Capabilities

- Create, edit, and delete user (person) accounts
- Manage user profile information such as name, email, and account status
- Lock and unlock user accounts to control system access
- Configure user access settings, including roles and security templates
- Manage user authentication settings, including password configuration
- View user activity details such as last login information
- Monitor operational scope, including the number of devices managed by each user

Status: **Completed**

Reference Images:

The screenshot displays the 'Person Details' page in the MMS interface. The page is divided into several sections:

- Person Info:** Includes System ID (1), Profile Picture, and Risk Score Rating (37% Risk Age).
- Personal Information:** Fields for Preferred Name (Admin), Surname (Admin), Date of Birth (01 January 2020), Gender (Female), Email Address, and Phone Number.
- Access and Security:** Includes an 'Enable' toggle, 'Add User Roles Filter', 'MMS Security Access', 'Person Address', 'Associate Linking', 'Device User Access', and 'MMS User Access' buttons.
- Person Dashboard:** A summary section with three charts:
 - Devices:** A donut chart showing 50 Active (18%), 24 Inactive (27%), and 16 Failed (56%) devices.
 - Transactions:** A donut chart showing 50 Approved (18%), 24 Declined (27%), and 16 Refunds (56%) transactions.
 - AI Shield:** A bar chart showing activity levels from Monday to Sunday.
- Security Metrics:** A small table showing ID Proof (80%), Compliance (93%), Fraud (0.003%), Credit Rating (56%), and Chargebacks (0.05%).

MMS

- Dashboard
- App Manager
- Cloud Security
- Stakeholders
- Person
- Company
- Merchant
- Charities
- Processors
- Device Manager
- Audit Log
- Global Settings
- Logout

MMS Security Access - Administrator Admin

Home / Person Management / Person Details / MMS Security Access - Administrator Admin

Administrator Admin
Administrator Admin

Access Security Edit

Administrator Access

MMS Login ID: admin@cloudbanking.com

MMS Password: *****

Feature Access Code:

Multifactor Access

Access Activation

Activate Date / Time: Deactivate Date / Time: Suspend Access:

Activate Logon Date: 01/01/2020 Deactivate Logon Date: 01/01/2020

Activate Logon Time: 10:13 AM Deactivate Logon Time: 10:13 AM

Security Dashboard View All

Persons Active Deactive

Devices

18% Active (50 Devices)
27% Inactive (24 Devices)
56% Failed (16 Devices)

Transactions

18% Approved (50 Transactions)
27% Declined (24 Transactions)
56% Refunds (16 Transactions)

Collapse

MMS

- Dashboard
- App Manager
- Cloud Security
- Stakeholders
- Person
- Company
- Merchant
- Charities
- Processors
- Device Manager
- Audit Log
- Global Settings
- Logout

Person Details

Home / Person Management / Person Details

Administrator Admin
Administrator Admin

Person Info
MMS Access
Device Access
Onboarding Details
Filter
Edit

Partner Fleet

All

No data

Merchants

No data

Location

No data

Location Areas

No data

Merchant Device

All

No data

Security Access Level

No data

Device Security Access

Use Default Access:

Device Login ID:

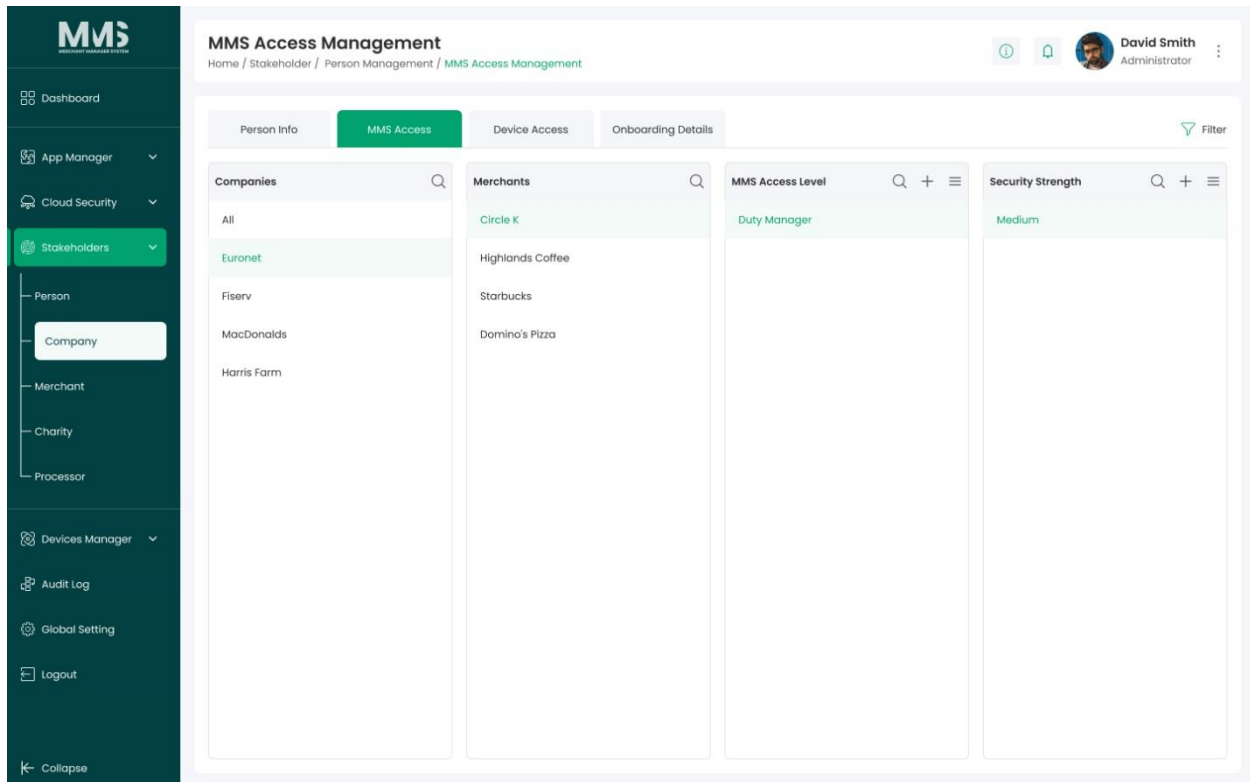
Device Password:

Device Feature Access Code:

Feature Access Code:

Use Default Access:

Collapse



4.2. Company

Description

Provides centralized management of companies within the system, allowing administrators to create, maintain, and control organizational entities. Company Management defines the organizational scope used for user access, security templates, and terminal operations.

Key Capabilities

- Create, update, and delete company records
- Manage company profile information such as name, contact details, and status
- Lock or unlock company accounts to control system access
- Assign users (persons) to companies to enable company-specific access

Status: **Completed**

Reference Images:

MMS

- Dashboard
- App Manager
- Cloud Security
- Stakeholders
- Person
- Company
- Merchant
- Charity
- Processor
- Devices Manager
- Audit Log
- Global Setting
- Logout

Company Management

Home / Stakeholder / Company Management

Company List Filter | Name | Search by Name | + Add Company

Merchant Name	Status	Devices	Users	AI Shield	Action
Euronet	Active	6	14	3	
Fiserv	Active	12	26	6	
Project Jumpstart	Active	10	19	5	
Worldline Global	Active	2	5	1	
McDonalds	Active	8	18	4	
Haris Farms	Active	7	16	3	

Showing 1-10 of 20

Companies Dashboard

Companies Active Deactive

Devices

Active: 50 Devices
Inactive: 24 Devices
Failed: 16 Devices

Transactions

Approved: 50 Transaction
Declined: 24 Transaction
Refunds: 16 Transaction

MMS

- Dashboard
- App Manager
- Cloud Security
- Stakeholders
- Person
- Company
- Merchant
- Charities
- Processors
- Device Manager
- Audit Log
- Global Settings
- Logout

Company Details

Home / Company Management / Company Details

Company Details | Company Employees | Company Devices | MMS Access | Onboarding Details

MMS System ID: 3

Company Logo:

Risk Score Rating: **37%** Risk Ave

ID Proof: 80% | Credit Rating: 56%
Compliance: 93% | Chargebacks: 0.05%
Fraud: 0.003%

80% AI Approval

Company Number: 3 Enable

Company Name: Project Jumpstart | Trading Name: Project Jumpstart

Company Registration ID: | Tax ID: 123456

ABN ID: | ACN ID: |

Approval ID: 123456 | Parent Company: |

[Contact Details](#) | [Smart Address](#)

[Associate Linking](#)

Company Dashboard

Devices: 4 Active, 0 Inactive, 0 Failed

Transactions: 50 Approved, 24 Declined, 16 Refunds

AI Shield:

MMS Document

Page 19 of 57

The screenshot shows the 'Company Details' page in the MMS interface. A 'Smart Address' modal is open, allowing the user to enter address information. The modal has tabs for 'Street', 'Shipping', and 'Billing'. The 'Street' tab is active, showing fields for Region, Country, State, City, Suburb, and Suburb Area, all currently set to 'None'. Below these are fields for Zip/Post Code, Street Type, Street Name, and Street Number. Further down are fields for Zone, Building Number, Apartment/Suit No, and Floor Number. At the bottom of the modal are text areas for 'Delivery instructions' and 'Comment', along with 'Cancel' and 'Save' buttons.

The screenshot shows the 'Company Details' page with the 'Company Employees' tab selected. The page displays a list of employees for the company 'Dung Pham'. The list includes a search bar, a menu icon, and three columns: 'Cell' (containing the phone number '+8486824405'), 'Email' (containing 'dung.pham@jugotechs.com'), and 'AI Score' (containing '0' and '0%').

Company Details
Home / Company Management / Company Details

Administrator
Administrator Admin

Company Details | Company Employees | **Company Devices** | MMS Access | Onboarding Details

Merchants	Locations	Location Areas	Company Devices
All Highlands Coffee Starbucks Pizzo Hut	No data	No data	No data

Company Details
Home / Company Management / Company Details

Administrator
Administrator Admin

Company Details | Company Employees | Company Devices | **MMS Access** | Onboarding Details

Company Employees	Merchants	MMS Access Level	Security Strength
Dung Pham	No data	No data	No data

4.3. Merchant

Description

Provides centralized management of merchants within the system, enabling administrators to maintain merchant profiles, control account status, and monitor operational performance. Merchant Management serves as the primary layer for organizing terminals, users, and merchant-level configurations.

Key Capabilities

- View and manage a centralized list of merchants
- Create, update, and maintain merchant profiles
- Activate or deactivate merchant accounts
- Search and filter merchants by defined criteria
- View comprehensive merchant details and related entities
- Monitor operational metrics, including:
 - Number of assigned devices
 - Number of associated users
 - Status of AI-enabled features
- Access visual insights and reports, such as:
 - Merchant activity overview
 - Device distribution
 - Transaction statistics

Status: **Completed**

Reference Images:

The screenshot displays the Merchant Management interface. On the left is a dark green sidebar with navigation options: Dashboard, App Manager, Cloud Security, Stakeholders (selected), Person, Company, Merchant (highlighted), Charity, Processor, Devices Manager, Audit Log, Global Setting, and Logout. The main content area is titled 'Merchant Management' and includes a breadcrumb 'Home / Stakeholder / Merchant Management' and a user profile for 'David Smith, Administrator'. Below this is a 'Merchant List' table with columns for Merchant Name, Status, Devices, Users, AI Shield, and Action. The table lists 10 merchants, with 9 active and 1 inactive (Adidas). To the right of the table is a 'Merchant Dashboard' with three charts: a bar chart for 'Merchants' showing activity over a week, a donut chart for 'Devices' (50 Active, 24 Inactive, 16 Failed), and another donut chart for 'Transactions' (50 Approved, 24 Declined, 16 Refunds). A pagination bar at the bottom indicates 'Showing 1-10 of 20'.

Merchant Name	Status	Devices	Users	AI Shield	Action
Circle K	Active	6	14	3	[Lock] [Edit] [Delete]
Highlands Coffee	Active	12	26	6	[Lock] [Edit] [Delete]
Starbucks	Active	10	19	5	[Lock] [Edit] [Delete]
Domino's Pizza	Active	2	5	1	[Lock] [Edit] [Delete]
Pizza Hut	Active	8	18	4	[Lock] [Edit] [Delete]
ExxonMobil	Active	7	16	3	[Lock] [Edit] [Delete]
Nike	Active	5	12	2	[Lock] [Edit] [Delete]
Adidas	Inactive	9	21	5	[Lock] [Edit] [Delete]

Merchant Details

Home / Merchant Management / Merchant Details

Administrator Admin

Merchant Details | Merchant Employees | Merchant Devices | Employee Access | Onboarding Details

MMS System ID: 3 | Merchant ID: 3 | Enable:

Merchant Name: Pizza Hut | Parent Company: [Dropdown]

Company ID: [Field] | Tax ID: [Field]

Industry Type: Restaurant | Industry Categories: Steak House

Risk Score Rating: 37% (Risk Ave)

ID Proof: 80% | Credit Rating: 56% | Compliance: 93% | Chargebacks: 0.05% | Fraud: 0.003%

Merchant Dashboard: 100% Active (2 Devices), 0 Inactive, 0 Failed

Transactions: 50 Approved, 24 Declined, 16 Refunds

AI Shield: [Bar Chart]

Merchant Management

Home / Stakeholder / Merchant Management

David Smith Administrator

Smart Address

Region	Country	State	City	Suburb	Location	Location Area	Merchants
Africa	Australia	NSW	Berry	Bankstown	Store 1	Section 1A	Army Surplus
America	Indonesia	NT	Bowral	Bondi	Store 2	Section 1B	Harry's Hobbies
Asia Pacific	New Zealand	QLD	Eden	Bronte	Paddy's Market	Section 2A	Sally's Homeware
Europe	Singapore	SA	Merimbula	CBD	Store 4		
Middle East		VIC	Newcastle	Edgecliff	Store 5		
		WA	Sydney	Newtown			
			Woollongong	Parramatta			

Zip/Post Code: [None] | Street Type: [None] | Street Name: [None] | Street Number: [0]

Zone: [Field] | Building Number: [0] | Apartment/Suit No: [0] | Floor Number: [Field]

Buttons: Cancel, Save

MMS Merchant Details
Home / Merchant Management / Merchant Details

Administrator Administrator Admin

Merchant Details Merchant Employees Merchant Devices Employee Access Onboarding Details Filter

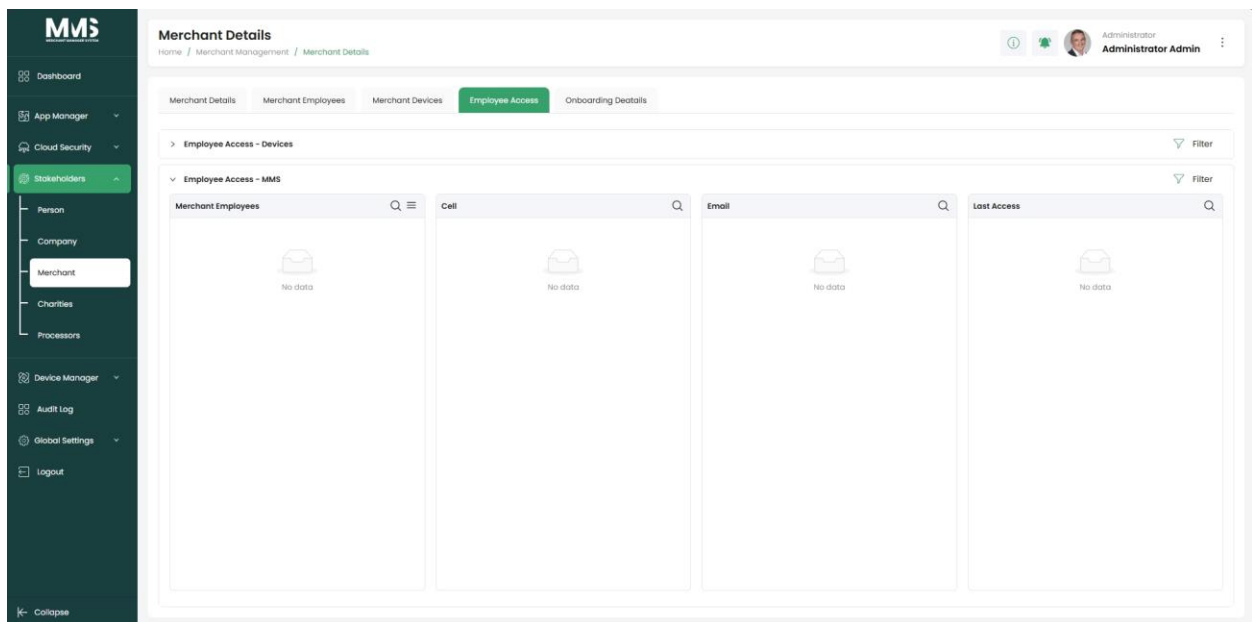
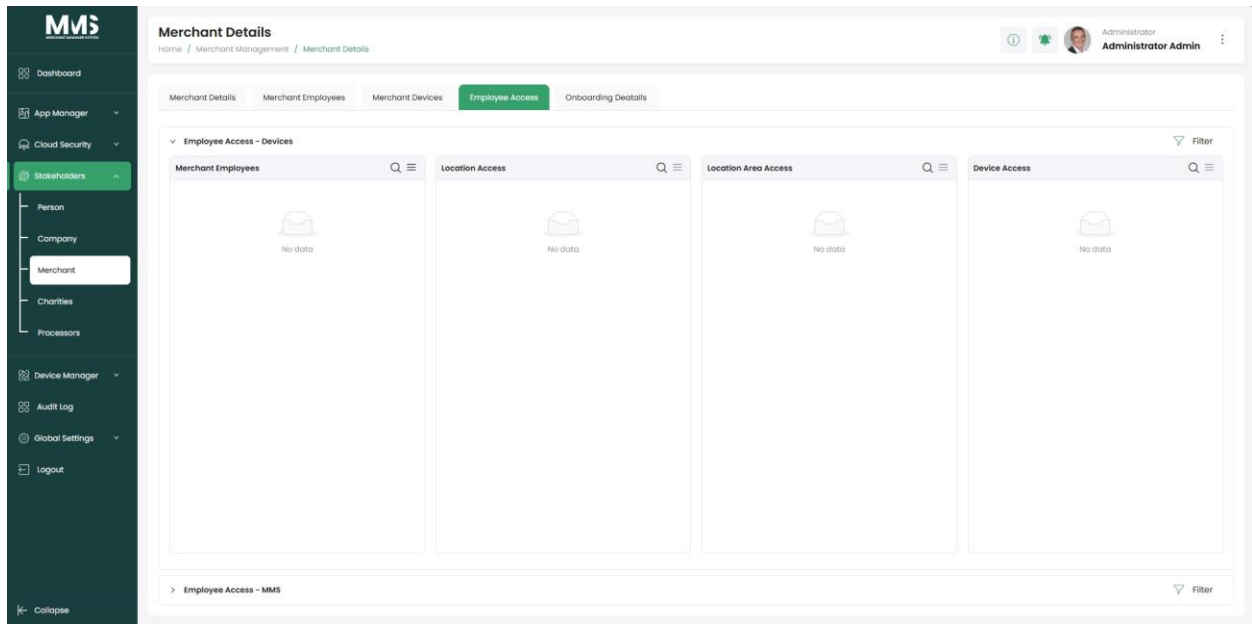
Merchant Employees	Call	Call	AI Score
No data	No data	No data	No data

MMS Merchant Details
Home / Merchant Management / Merchant Details

Administrator Administrator Admin

Merchant Details Merchant Employees Merchant Devices Employee Access Onboarding Details

Locations	Location Areas	Merchant Devices	Merchant Linking Group
All Bellevue Plaza	All Specialist Rooms	dc-4e59d02565bba 1850589200	No data



4.4. Charities

Description

Provides centralized management of charity records that can be used as a global data source for base templates. Charity configurations can be applied consistently across templates or customized at the template level to support company-specific requirements.

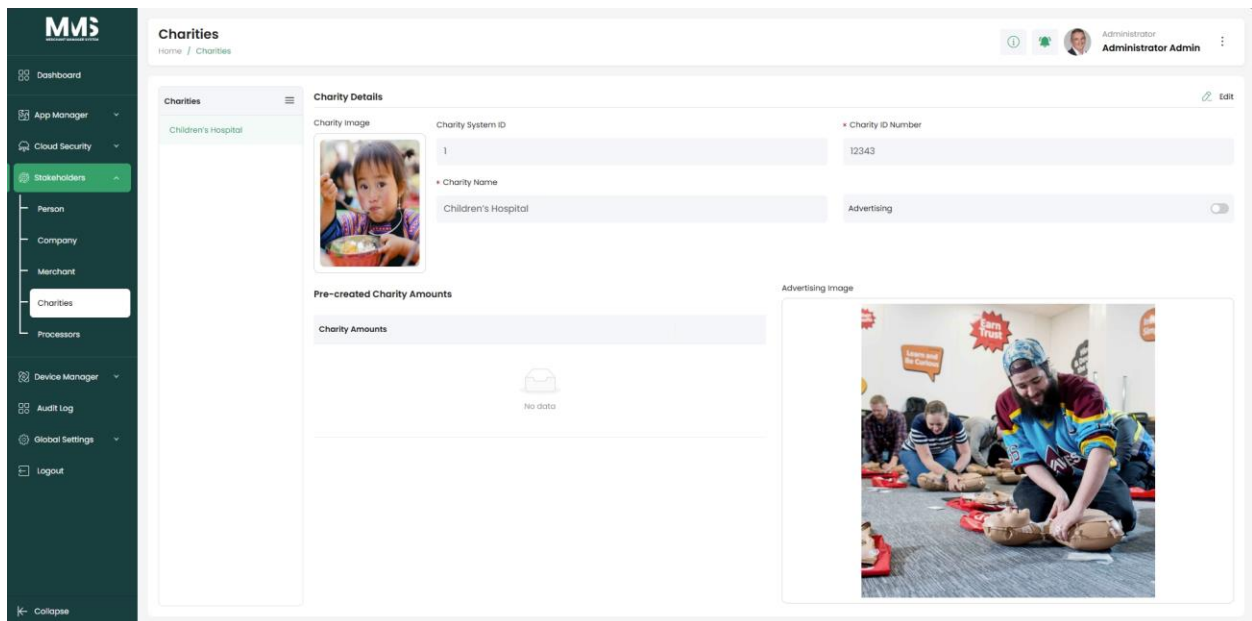
Key Capabilities

- Manage a centralized list of charity records for reuse across base templates

- Use global charity data directly within templates
- Override charity settings per template for company-specific customization
- Configure charity-related attributes, including:
 - Charity name and reference number
 - Charity images and advertising visuals
 - Donation amounts
 - Advertising enablement

Status: **Completed**

Reference Images:



4.5. Processors

Description

Provides centralized management of payment processor configurations that serve as a global data source for base templates. Processor records and interfaces can be applied directly within templates or overridden at the template level to support company-specific payment routing, libraries, and device compatibility.

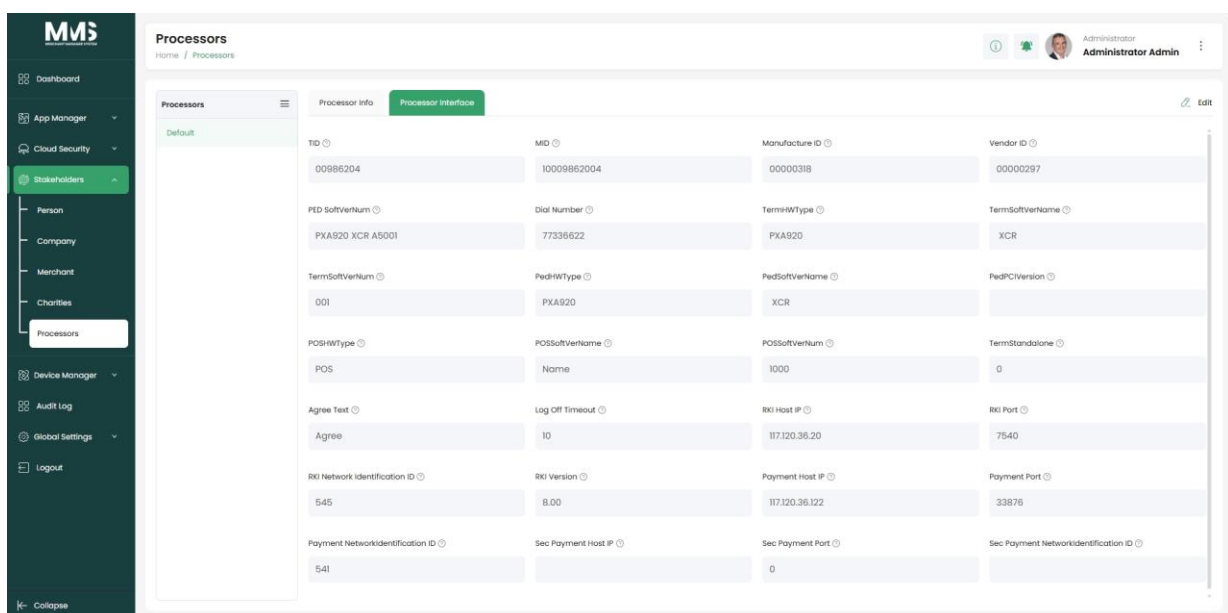
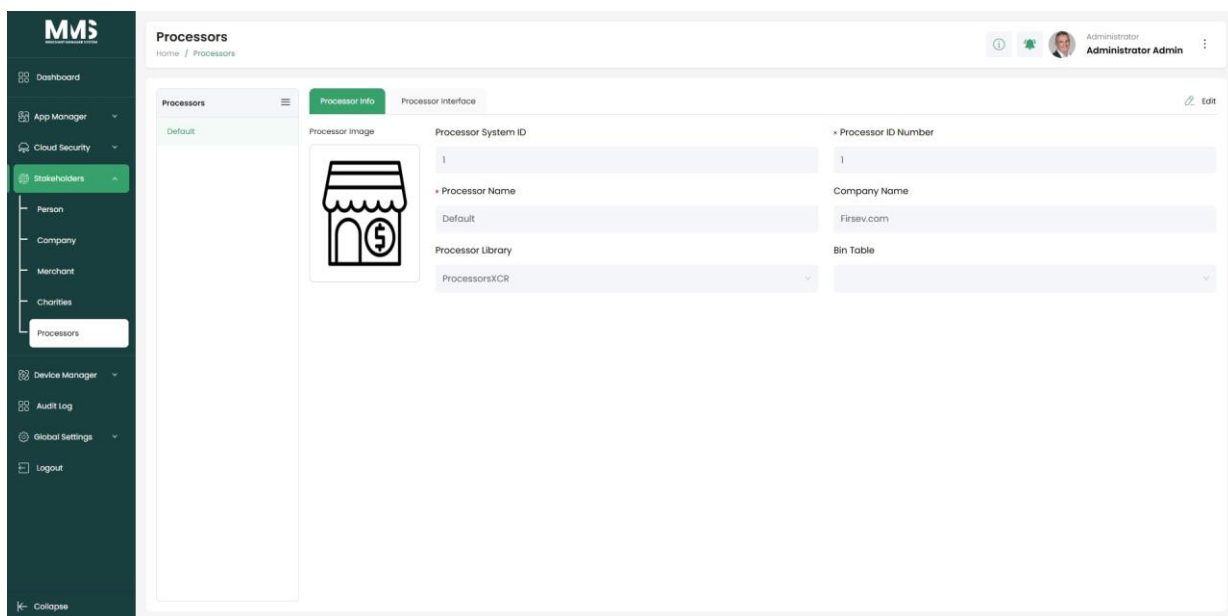
Key Capabilities

- Manage a centralized list of payment processor records for reuse across base templates
- Configure processor identity and integration attributes, including:

- Processor name, system ID, and company name
- Processor libraries and processor numbers
- BIN tables for card routing
- Processor logos and reference images
- Define and manage processor interface configurations, including network, software, and terminal settings

Status: Completed

Reference Images:



5. Device Manager

5.1. Device Registry

Description

Provides a centralized registry for creating and maintaining device records within the system. Devices are registered under specific owners and serve as the foundational inventory before being assigned for operational deployment and management.

Key Capabilities

- Register and manage devices under designated owners or organizations
- Maintain core device information, including serial number, brand, and model
- Track registered devices prior to assignment and activation
- Enable subsequent assignment of devices to companies, groups, locations, or merchants through Device Manager
- Support import devices using MAXSTORE API or CSV files

Status: **Completed**

Reference Images:

The screenshot displays the 'Device Registry' page in the MMS application. The interface includes a sidebar with navigation options like Dashboard, App Manager, Cloud Security, Stakeholders, Device Manager (selected), and Hardware. The main content area shows a table of device records with columns for SN, Brand, Model, Owner, Merchant, Created, and Status. The status for all devices is 'Assigned'. There are also buttons for 'Import Devices' and '+ Add Device'.

SN	Brand	Model	Owner	Merchant	Created	Status
TILL1000000	Pax	A920	Project Jumpstart	Multi-Merchant	30/09/2025 1:17 PM	Assigned
TILL1000001	Pax	A920	Project Jumpstart	Highlands Coffee	30/09/2025 1:17 PM	Assigned
TILL1000002	Pax	A920	Project Jumpstart	Highlands Coffee	30/09/2025 1:17 PM	Assigned
TILL1000003	Pax	A920	Project Jumpstart	Highlands Coffee	30/09/2025 1:17 PM	Assigned
TILL1000004	Pax	A920	Project Jumpstart	Highlands Coffee	30/09/2025 1:17 PM	Assigned
185058264	Pax	A920	Project Jumpstart	Highlands Coffee	07/10/2025 4:20 AM	Assigned
1780034868	Pax	A920	Project Jumpstart	Highlands Coffee	07/10/2025 9:44 AM	Assigned
1852001844	Pax	A920 PRO	Project Jumpstart	Highlands Coffee	14/10/2025 2:37 AM	Assigned
1780034810	Pax	A920	Project Jumpstart	-	24/10/2025 2:32 AM	Assigned
1780034811	Pax	A920	Project Jumpstart	Highlands Coffee	24/10/2025 2:32 AM	Assigned

Device Registry
Home / Device Registry

Administrator User
Admin

Device List

SN Search by SN + Add Device

Create a New Device

Device Owner: Project Jumpstart

Serial Number Range:

Serial Number Range (Start): PJ1001

Serial Number Range (End): PJ1050

Brand: Pax

Model: A920

OS Type: Android

OS Version: 10.0

Firmware Version: v1.0.0

SDK Version: SDK-v1.0.0-build-456

Batch Number:

Tag ID:

Cancel Save

SN	Merchant	Created	Status
TILL1000000	Highlands Coffee	30/09/2025 1:17 PM	Unassigned
TILL1000001	Highlands Coffee	30/09/2025 1:17 PM	Assigned
TILL1000002	Highlands Coffee	30/09/2025 1:17 PM	Assigned
TILL1000003	Highlands Coffee	30/09/2025 1:17 PM	Assigned
TILL1000004	Highlands Coffee	30/09/2025 1:17 PM	Assigned
1850569294	Highlands Coffee	07/10/2025 4:20 AM	Assigned
1760034868	Highlands Coffee	07/10/2025 9:44 AM	Assigned
1852001844	Highlands Coffee	14/10/2025 2:37 AM	Assigned
1760034810	-	24/10/2025 2:32 AM	Unassigned
1760034811	Highlands Coffee	24/10/2025 2:32 AM	Assigned

10 Items Showing 1-10 of 17

Device Registry
Home / Device Registry

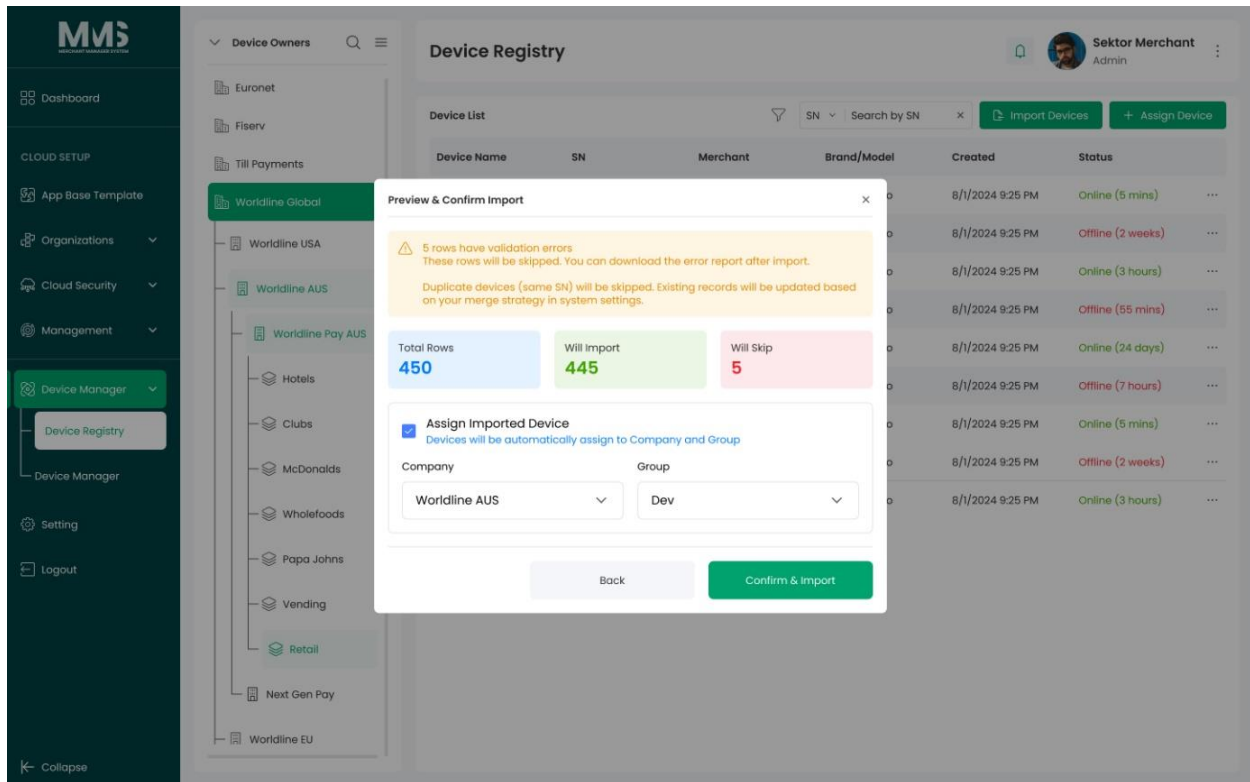
Administrator User
Admin

Device List

SN Search by SN Import Devices + Add Device

SN	Brand	Model	Owner	Merchant	Created	Status
TILL1000000	Pax	A920	Project Jumpstart	Multi-Merchant	30/09/2025 1:17	...
TILL1000001	Pax	A920	Project Jumpstart	Highlands Coffee	30/09/2025 1:17 PM	Assigned
TILL1000002	Pax	A920	Project Jumpstart	Highlands Coffee	30/09/2025 1:17 PM	Assigned
TILL1000003	Pax	A920	Project Jumpstart	Highlands Coffee	30/09/2025 1:17 PM	Assigned
TILL1000004	Pax	A920	Project Jumpstart	Highlands Coffee	30/09/2025 1:17 PM	Assigned
1850569294	Pax	A920	Project Jumpstart	Highlands Coffee	07/10/2025 4:20 AM	Assigned
1760034868	Pax	A920	Project Jumpstart	Highlands Coffee	07/10/2025 9:44 AM	Assigned
1852001844	Pax	A920 PRO	Project Jumpstart	Highlands Coffee	14/10/2025 2:37 AM	Assigned
1760034810	Pax	A920	Project Jumpstart	-	24/10/2025 2:32 AM	Assigned
1760034811	Pax	A920	Project Jumpstart	Highlands Coffee	24/10/2025 2:32 AM	Assigned

10 Items Showing 1-10 of 17



5.2. Device Manager

Description

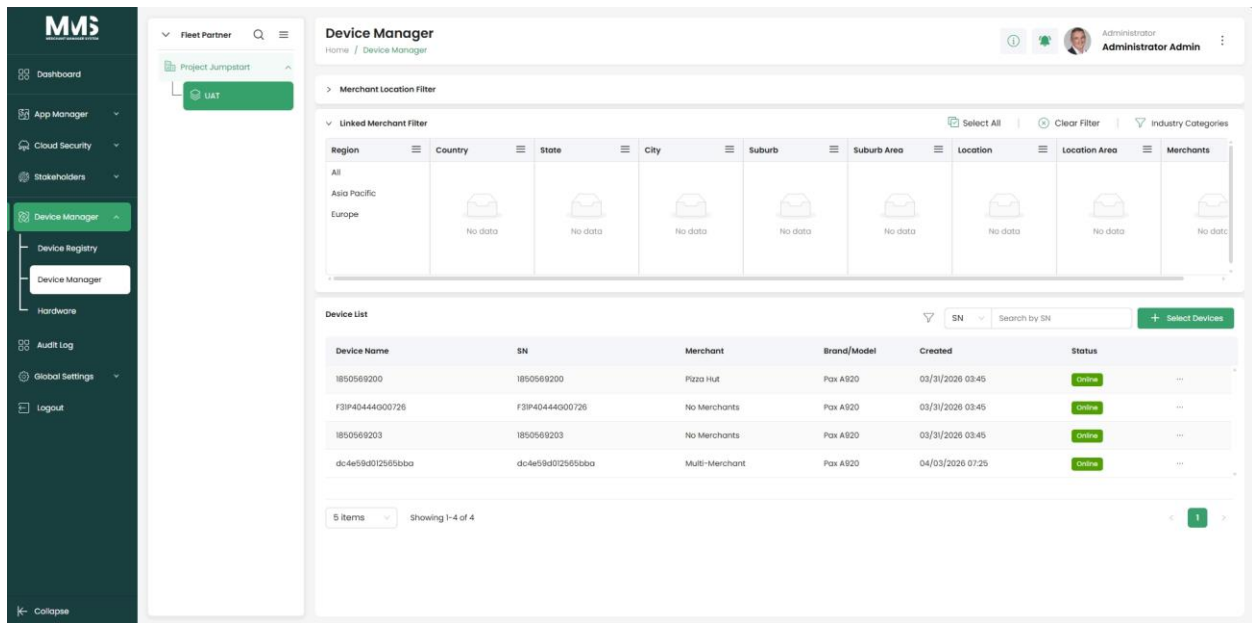
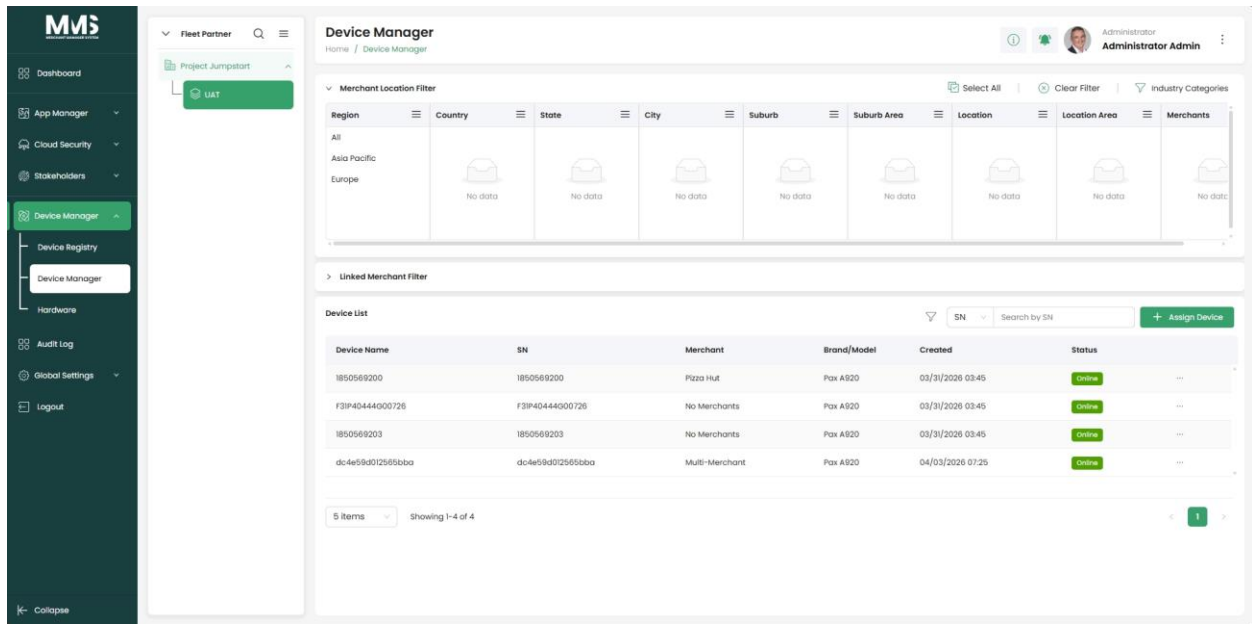
Provides centralized management of devices after registration, enabling administrators to assign devices from the Device Registry to companies, groups, locations, or merchants. Device Manager supports ongoing monitoring and management of assigned devices through a structured and hierarchical view.

Key Capabilities

- Assign registered devices to companies, subsidiaries, groups, locations, or merchants
- Manage devices after assignment, including viewing and updating assigned device information
- Navigate and select locations using a hierarchical location tree
- View and filter devices based on organizational hierarchy and assignment scope
- Support ongoing device monitoring and operational management within the assigned context.

Status: Complete

Reference Images:



5.2.1. Company Tree

Description

Provides a hierarchical structure for organizing companies, subsidiaries, and groups within the system. The company tree defines organizational relationships that are used to manage access, visibility, and device assignment in a structured and scalable manner.

Key Capabilities

- Assign registered devices to companies, subsidiaries, groups, locations, or merchants

- Manage devices after assignment, including viewing and updating assigned device information
- Navigate and select locations using a hierarchical location tree
- View and filter devices based on organizational hierarchy and assignment scope
- Support ongoing device monitoring and operational management within the assigned context

Status: **Completed**

Reference Images:

The screenshot displays the MMS Device Manager interface. On the left is a dark sidebar with navigation options: Dashboard, CLOUD SETUP (App Base Template, Organizations, Cloud Security, Management), Device Manager (highlighted), Setting, and Logout. A secondary sidebar shows a 'Company' dropdown menu with a search icon and a tree view of locations including Euronet, Fiserv, Till Payments, Worldline Global (highlighted), Worldline USA, Worldline AUS, Worldline Pay AUS, Hotels, Clubs, McDonalds, Wholefoods, Papa Johns, Vending, Retail (highlighted), Next Gen Pay, and Worldline EU. The main content area is titled 'Device Manager' and shows a 'Merchant Location Filter: Restaurant'. Below this is a table with columns: Region, Country, State, City, Suburb, Location, Location Area, and Merchants. The table lists various global locations. Below the location filter is a 'Device List' section with a search bar and a '+ Assign Device' button. The device list table has columns: Device Name, SN, Merchant, Brand/Model, Created, and Status. It contains eight rows of device information, including SN numbers and status indicators like 'Online (5 mins)' or 'Offline (2 weeks)'.

5.2.2. Location Tree

Description

Provides a hierarchical structure for organizing physical or logical locations within the system. The location tree enables administrators to group devices by location, supporting clear visibility, structured management, and location-based device operations.

Key Capabilities

- Create and manage hierarchical location structures
- Organize devices under defined locations and sub-locations
- Support device assignment and management based on location hierarchy
- Enable location-based visibility and filtering of devices
- Integrate with Device Manager for efficient device monitoring and operations

Status: In Progress (Merchant Location Filters)

Reference Images:

The screenshot displays the MMS Merchant Manager System interface. On the left is a dark green sidebar with navigation options: Dashboard, Cloud Setup (App Base Template, Organizations, Cloud Security, Management), Device Manager (highlighted), Setting, and Logout. The main content area is titled 'Device Manager' and shows a user profile for 'Sektor Merchant Admin'. A red box highlights a 'Merchant Location Filter: Restaurant' table with the following data:

Region	Country	State	City	Suburb	Location	Location Area	Merchants
Africa	Australia	NSW	Berry	Bankstown	Store 1	Section 1A	Army Surplus
America	Indonesia	NT	Bowral	Bondi	Store 2	Section 1B	Harry's Hobbies
Asia Pacific	New Zealand	QLD	Eden	Bronte	Paddy's Market	Section 2A	Sally's Homeware
Europe	Singapore	SA	Merimbula	CBD	Store 4		
Middle East		VIC	Newcastle	Edgecliff	Store 5		
		WA	Sydney	Newtown			
			Woollongong	Parramatta			

Below the filter table is a 'Device List' section with a search bar and an '+ Assign Device' button. The device list table contains the following data:

Device Name	SN	Merchant	Brand/Model	Created	Status
Counter Terminal 1	9876524637	Multi-Merchant	PAX A920 Pro	8/1/2024 9:25 PM	Online (5 mins)
Counter Terminal 1	9876524637	Army Surplus	PAX A920 Pro	8/1/2024 9:25 PM	Offline (2 weeks)
Counter Terminal 1	9876524637	Multi-Merchant	PAX A920 Pro	8/1/2024 9:25 PM	Online (3 hours)
Counter Terminal 1	9876524637	Army Surplus	PAX A920 Pro	8/1/2024 9:25 PM	Offline (55 mins)
Counter Terminal 1	9876524637	Army Surplus	PAX A920 Pro	8/1/2024 9:25 PM	Online (24 days)
Counter Terminal 1	9876524637	Army Surplus	PAX A920 Pro	8/1/2024 9:25 PM	Offline (7 hours)
Counter Terminal 1	9876524637	Multi-Merchant	PAX A920 Pro	8/1/2024 9:25 PM	Online (5 mins)

Device Manager

Merchant Location Filter

Region	Country	State	City	Suburb	Location	Location Area	Merchants
All	All	All	All	All	All	All	All
					Store 1	Section 1A	Army Surplus
					Store 2	Section 1B	Harry's Hobbies
					Paddy's Market	Section 2A	Sally's Homeware
					Store 4		
					Store 5		

Created Status

8/1/2024 9:25 PM	Online (5 mins)
8/1/2024 9:25 PM	Offline (2 weeks)
8/1/2024 9:25 PM	Online (3 hours)
8/1/2024 9:25 PM	Offline (55 mins)
8/1/2024 9:25 PM	Online (24 days)
8/1/2024 9:25 PM	Offline (7 hours)
8/1/2024 9:25 PM	Online (5 mins)

Add Region

Name: Report Name:

Default Data: Currency:

Decimal Used: 1000 Separator:

Sort: Language:

Buttons: Cancel, Done

Device Manager

Merchant Location Filter

Region	Country	State	City	Suburb	Location	Location Area	Merchants
All	All	All	All	All	All	All	All
					Store 1	Section 1A	Army Surplus
					Store 2	Section 1B	Harry's Hobbies
					Paddy's Market	Section 2A	Sally's Homeware
					Store 4		
					Store 5		

Created Status

8/1/2024 9:25 PM	Online (5 mins)
8/1/2024 9:25 PM	Offline (2 weeks)
8/1/2024 9:25 PM	Online (3 hours)
8/1/2024 9:25 PM	Offline (55 mins)
8/1/2024 9:25 PM	Online (24 days)
8/1/2024 9:25 PM	Offline (7 hours)
8/1/2024 9:25 PM	Online (5 mins)

Select Region

5 Items Selected

- Region
- Asia Pacific
- East Asia
- Oceania
- Southeast Asia
- South Asia

Showing 1-5 of 20

Buttons: + Add, Cancel, Upload

Add Location

Location System ID: Multi Merchant Location:

Merchant: Location Name:

Zip/Past Code: Street Type: Street Name:

Street Number: Zone: Building Number: Apartment/Suit No:

Floor Number:

GEO Location & Fencing

Contact Name: Contact Number: Contact Email Address:

Worldline NZ	Counter Terminal 1	9876524637	Army Surplus	PAX A920 Pro	8/1/2024 9:25 PM	Online (5 mins)
	Counter Terminal 1	9876524637	Army Surplus	PAX A920 Pro	8/1/2024 9:25 PM	Offline (2 weeks)
	Counter Terminal 1	9876524637	Multi-Merchant	PAX A920 Pro	8/1/2024 9:25 PM	Online (5 mins)

GEO Location & Fencing

GEO Location:

GEO Fencing:

VPN AI Warning:

VPN AI Block:

Latitude:

Longitude:

Radius (Meters):

Device Manager

GEO Location & Fencing

GEO Location | **GEO Fencing**

GEO Fencing

Polygon Geofence

VPN AI Warning

VPN AI Block

Point 1
-33.8688, 151.2093

Point 2
-33.8688, 151.2093

Point 3
-33.8688, 151.2093

+ Add Point

Cancel | Save

Device ID	Device Name	Model	Status	Last Update
Counter Terminal 1	9876524637	Army Surplus	PAX A920 Pro	8/1/2024 9:25 PM
Counter Terminal 1	9876524637	Multi-Merchant	PAX A920 Pro	8/1/2024 9:25 PM

Device Manager

GEO Location & Fencing

GEO Location | **GEO Fencing**

GEO Fencing

Polygon Geofence

VPN AI Warning

VPN AI Block

IP Address/Range

ISP/Network Provider

ASN (Autonomous System Number)

Country

Region/State

City

Cancel | Save

Device ID	Device Name	Model	Status	Last Update
Counter Terminal 1	9876524637	Army Surplus	PAX A920 Pro	8/1/2024 9:25 PM
Counter Terminal 1	9876524637	Multi-Merchant	PAX A920 Pro	8/1/2024 9:25 PM

5.2.3. Device Setup

Description

Provides a centralized workspace for configuring and managing assigned devices. Device Setup enables administrators to control applications, firmware, templates, and operational settings, as well as monitor device status, history, and location.

Key Capabilities

- **Dashboard:** View an overview of device status, key information, and recent activities
- **App & Firmware:** Manage application and firmware versions applied to devices
- **Update Tasks:** Schedule and monitor application and firmware update tasks
- **App Templates:** Apply configuration templates to standardize device setup
- **Geo Location:** Track and manage device location information
- **Backups:** Manage device configuration backups and restore points
- **Logs:** View device activity and operational logs
- **Settings:** Configure device-specific operational and system settings

a. Dashboard

Status: **Completed**

Reference Images:

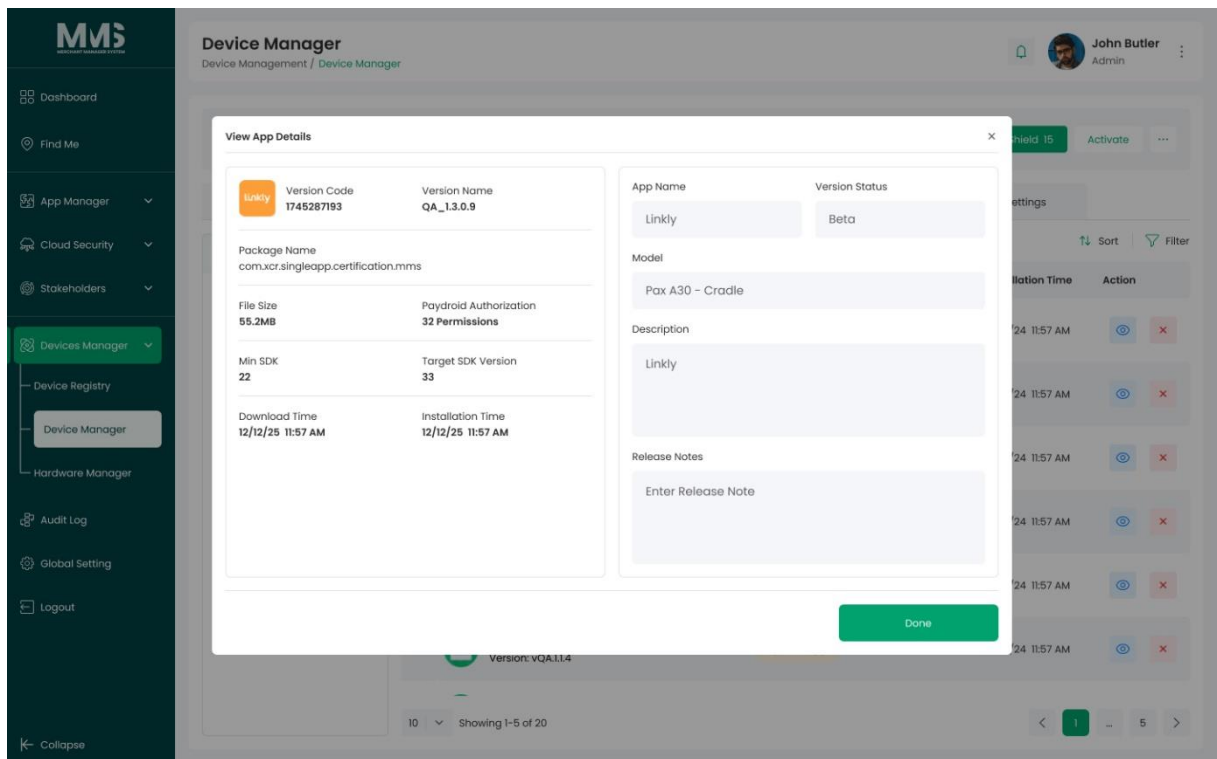
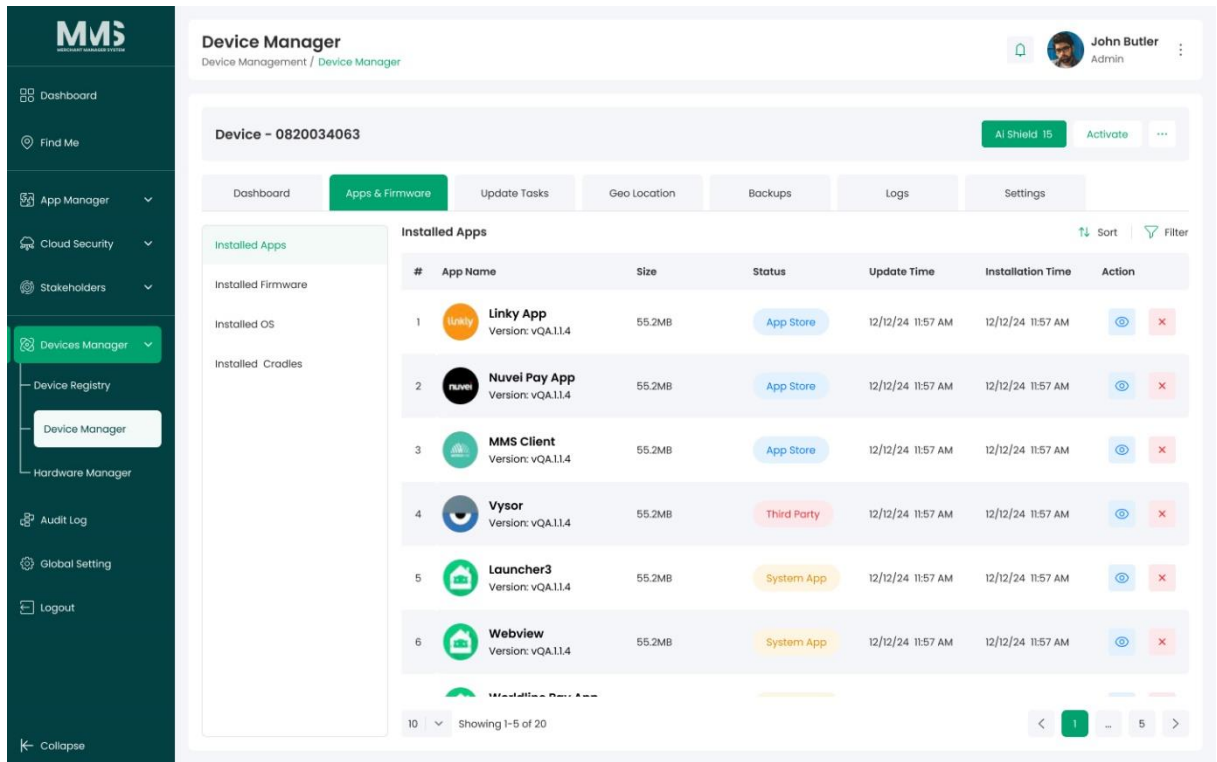
The screenshot displays the MMS Device Manager interface. On the left is a dark green sidebar with navigation options: Dashboard, Find Me, App Manager, Cloud Security, Stakeholders, Devices Manager (highlighted), Device Registry, Device Manager, Hardware Manager, Audit Log, Global Setting, and Logout. The main content area is titled 'Device Manager' and shows details for a specific device (ID: 0820034063). The device status is 'AI Shield 15' and 'Activate'. Below this are tabs for Dashboard, Apps & Firmware, Update Tasks, App Template, Geo Location, Backups, Logs, and Settings. The 'Dashboard' tab is active, showing a map of the device's location on 'Illarangi St'. To the right of the map is a 'Device Information' section with a 'View Details' link. It lists: Device Name (Counter TOP 1), Serial Number (981298273913719), Model (Pax A920 Pro), Ram (39.79%), CPU (19.00%), Battery (55%), and Storage (1.75GB/4.5GB). A small smartphone icon shows 'On-line'. Below the map and information is a 'Device Logs' section with a 'View More' link, showing three 'Create Terminal' events. At the bottom right is an 'Update Tasks' section with a 'View More' link, showing a table of tasks:

Task Name	Type	Status	Push Time
Worldline Pay App Version: vQA.11.4	Template Upgrade	In Progress	12/12/24 11:57 AM
Worldline Pay App Version: vQA.11.4	Template Upgrade	Failed	12/12/24 11:57 AM
Worldline Pay App	Template	Failed	12/12/24 11:57 AM

b. App & Firmware

Status: **Completed**

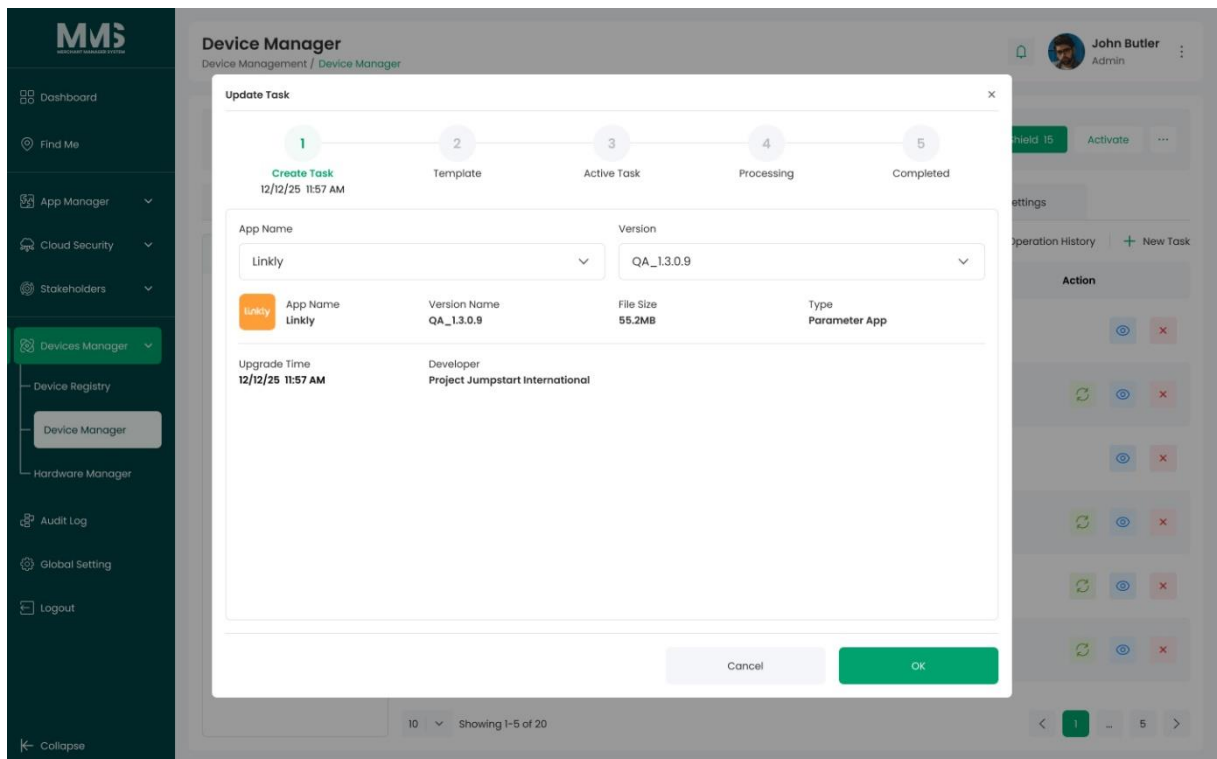
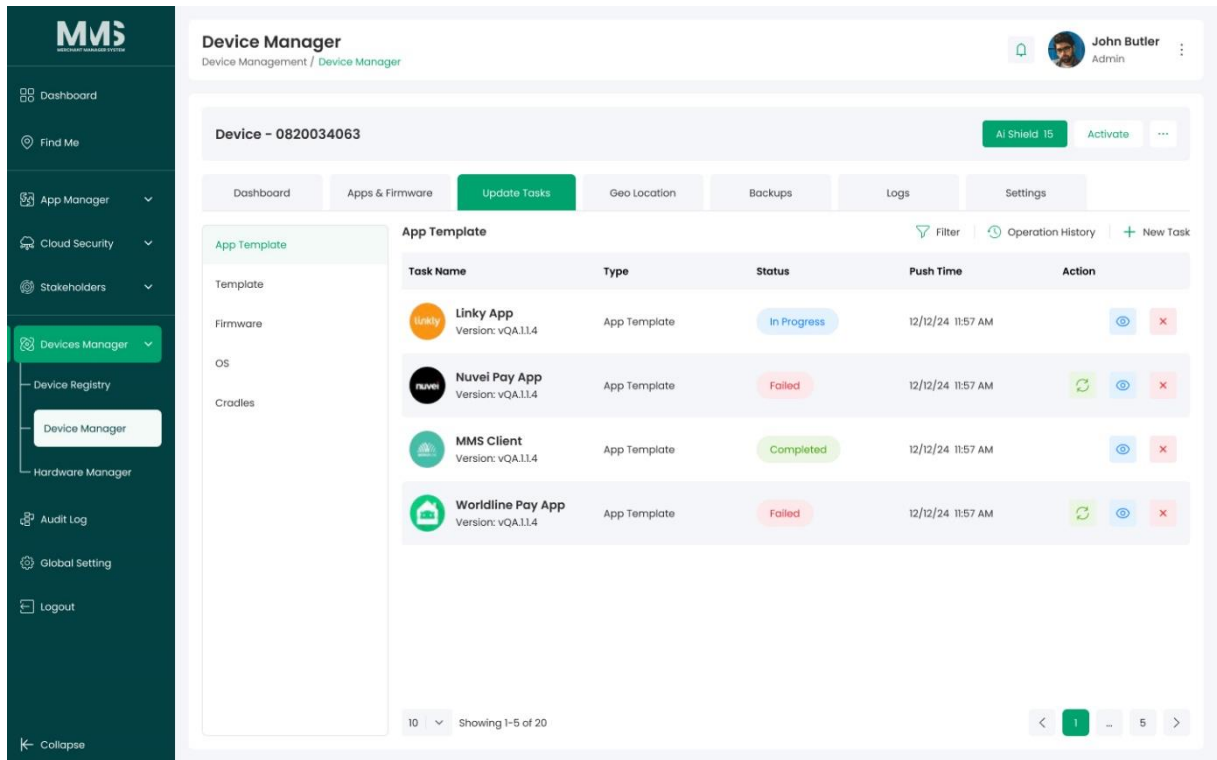
Reference Images:



c. Update Tasks

Status: **Completed**

Reference Images:



Device Manager
Device Management / Device Manager

Update Task

1 Create Task 12/12/25 11:57 AM
2 Template 12/12/25 11:57 AM
 3 Active Task
 4 Processing
 5 Completed

Linkly Version: QA_1.3.0.9
 Type: Parameter App
 Update Time: 12/12/25 11:57 AM
 Package Name: com.xcr.singleapp
 File Size: 55.2MB

Existing Templates

- Template Name - 305002011225
- Template Name - 305002011226**
- Template Name - 305002011227

Category

- System Setup**
- POS Integration Protocol
- Test Mode
- Operation Schedule
- Network Settings
- Card Reader Mode

Settings:

- Contactless Enabled: **Enabled**
- Contactless Time Delay Enabled: **Disabled**
- Contactless Time Delay: 0
- PIN Characters: 23
- ID: 857
- Terminal Serial Number: 9VBGNHGTX6
- Active Access Date

Buttons: Back, Cancel, **Next**

Device Manager
Device Management / Device Manager

Update Task

1 Create Task 12/12/25 11:57 AM
 2 Template 12/12/25 11:57 AM
3 Active Task 12/12/25 11:57 AM
 4 Processing
 5 Completed

Linkly Version: QA_1.3.0.9
 Type: Parameter App
 Update Time: 12/12/25 11:57 AM
 Package Name: com.xcr.singleapp
 File Size: 55.2MB

Template selected:
 Template Name: Linkly 305002011226
 Last Modified: 2025-02-13 14:23:15
 Modified By: admin@worldline.com

Update Configuration:

- Wi-fi Only:** Do not update using the cellular network
- Force Reboot:** The device will reboot after update to apply changes
- Update Immediately:** Will force an update
- Scheduled Update:** Use scheduled date & time

Download Date: mm/dd/yyyy | **Download Time:** hh:mm

Upgrade Date: mm/dd/yyyy | **Upgrade Time:** hh:mm

Upgrade Type: Update Type | **Retry Amount:** 3 | **Time Zone:** (GMT+07:00) Indochina Time - Bangkok

Buttons: Back, Cancel, Save Draft, **Update**

d. App Template

Status: **Completed**

Reference Images:

Device Manager
Home / Device Manager / Device Setup: (SN - TILLI000000)

Dashboard | Apps & Firmware | Update Tasks | **App Template** | Geo Location | Backups | Logs | Settings

App Name: UNATTENDED SEK | App Version: QA_13.35 (1764583018)

Existing Template | Schedule Upgrade | + New Template

Search Template History

- Template Name - 445702010126 (QA_13.35)
- Template Name - 104001030126 (QA_13.35)
- Template Name - 302905030126 (QA_13.35)
- Template Name - 205405030126 (QA_13.35)
- Template Name - 480006030126 (QA_13.35)
- Template Name - 294602050126 (QA_13.35)

Terminal Configuration:

- Contactless Enabled: Enabled
- Contactless Time Delay Enabled: Disabled
- Contactless Time Delay: 0
- PINCharacters: 23
- Id: 857
- Terminal Serial Number: 9V8GNHGTX6
- Active Access Date:
- Active Access Time:
- Terminal Service Details: 31
- De Active Date:
- De Active Time:
- Terminal Install Date:
- Terminal Install Time:

New Template
Home / Device Manager / Device Setup: (SN - TILLI000000) / New Template

Serial Number: TILLI000000 | App Name: UNATTENDED PAX | App Version: QA_13.35

Merchants: 7-Eleven, Amazon Go, Circle K, Costco

Template Name: Link to - System Standard Configuration - 202601080912

Template Description: This template is linked to the System Standard Configuration. It dynamically inherits all configuration changes from the parent template. When the System Standard Configuration is updated, this template will automatically reflect those changes.

Base Template Options: Template Selected: SYSTEM STANDARD CONFIGURATION

Buttons: Template Setup, Save Template

e. Backups

Status: **Completed**

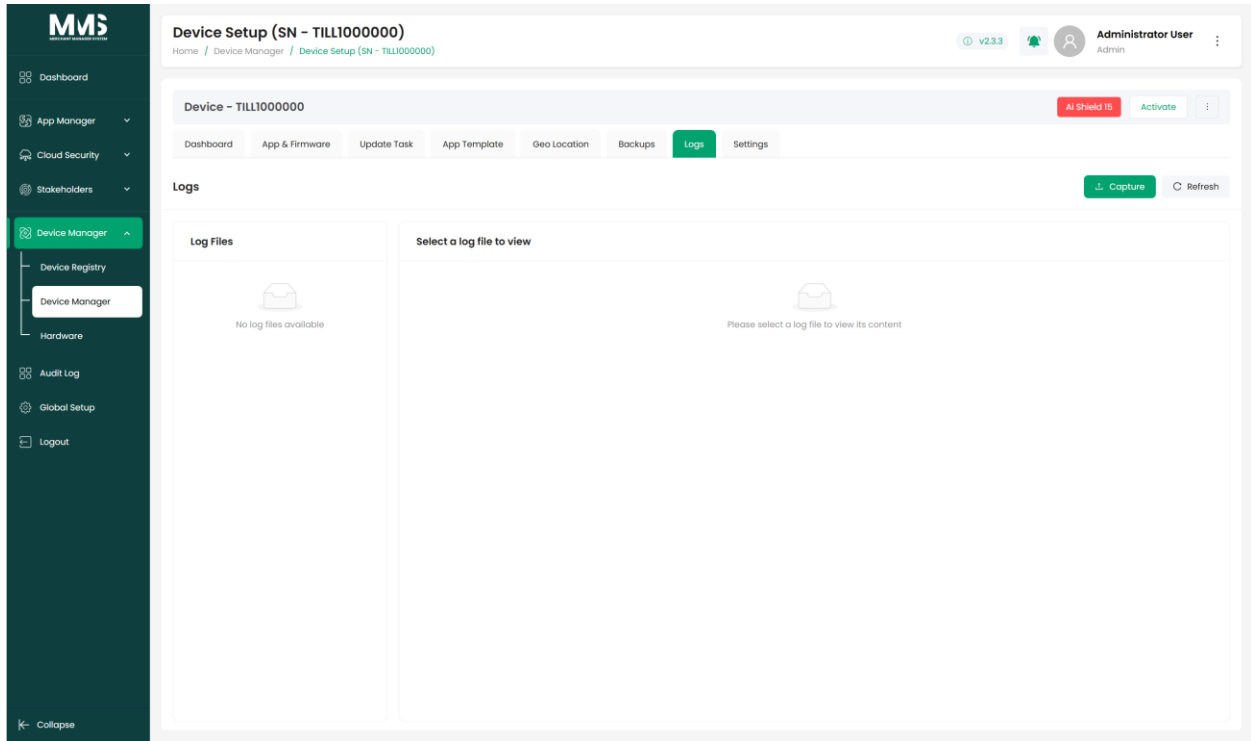
Reference Images:

TIMESTAMP (UTC)	FILE NAME	PACKAGE NAME / VERSION	SIZE	CRC CHECK	COMPLETED (UTC)	STATUS
2026-02-12 01:59:22	capturelog.txt	com.xcr.singleapp.certification.mms 1745287193	1.01 MB	Verified	2026-02-12 01:59:22	Succeed
2026-02-12 01:59:12	data.json	com.xcr.singleapp.certification.mms 1745287193		Failed	2026-02-12 01:59:12	Failed
2026-02-11 09:22:16	capturelog.txt	com.xcr.singleapp.certification.mms 1745287193	1.01 MB	Verified	2026-02-11 09:22:16	Succeed
2026-02-11 09:19:19	capturelog.txt	com.xcr.singleapp.certification.mms 1745287193	1.01 MB	Verified	2026-02-11 09:19:19	Succeed
2026-02-11 02:52:51	capturelog.txt	com.xcr.singleapp.certification.mms 1745287193	1.01 MB	Verified	2026-02-11 02:52:51	Succeed

f. Logs

Status: **Completed**

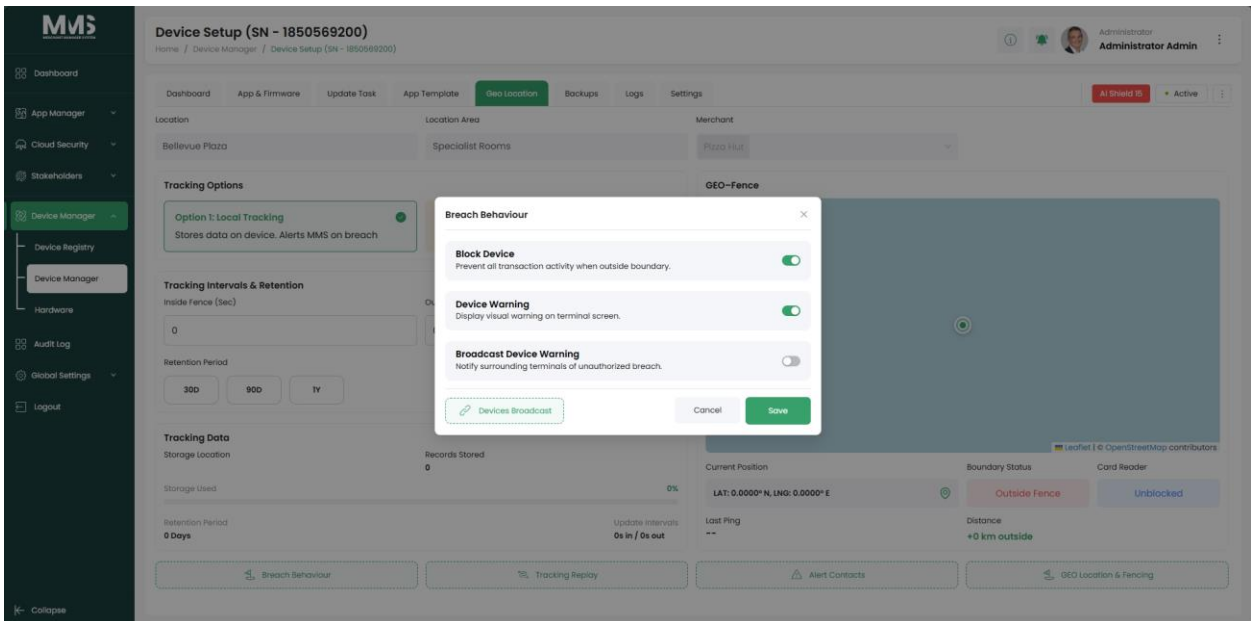
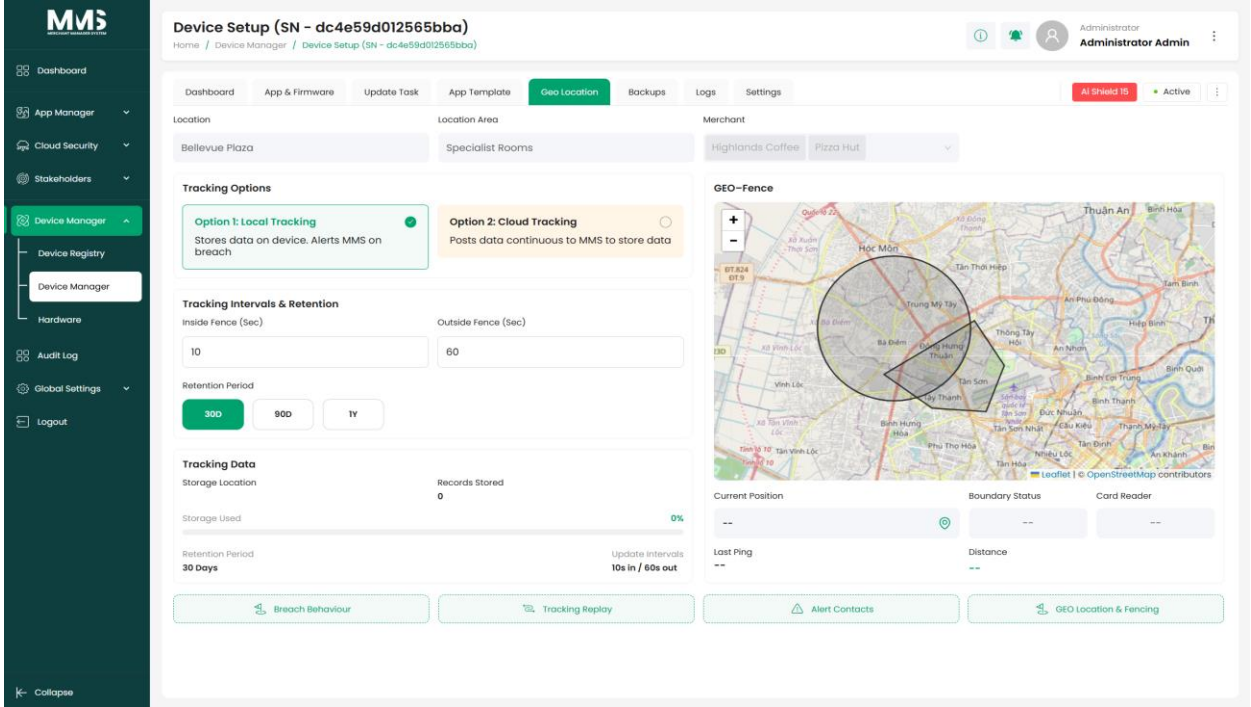
Reference Images:



g. Geo Location

Status: **Completed**

Reference Images:



Device Setup (SN - 1850569200)

Location: Bellevue Plaza | Location Area: Specialist Rooms | Merchant: Pizza Hut

Tracking Options

- Option 1: Local Tracking (Selected) - Stores data on device. Alerts MMS on breach.
- Option 2: Cloud Tracking - Posts data continuously to MMS to store data.

Tracking Intervals & Retention

Inside Fence (Sec): 0

Retention Period: 30D, 90D, 1Y

Tracking Data

Storage Location: [Empty] | Records Stored: 0 | Storage Used: 0%

Retention Period: 0 Days | Update Intervals: 0s in / 0s out

Tracking Replay Modal:

From: mms/2021/01/01 | To: mms/2021/01/01

Buttons: Cancel, Request Batch Playback

Device Setup (SN - dc4e59d012565bba)

Location: Bellevue Plaza | Location Area: Specialist Rooms | Merchant: Pizza Hut

Tracking Options

- Option 1: Local Tracking (Selected) - Stores data on device. Alerts MMS on breach.

Tracking Intervals & Retention

Inside Fence (Sec): 10

Retention Period: 30D, 90D, 1Y

Tracking Data

Storage Location: [Empty] | Storage Used: [Empty]

Retention Period: 30 Days

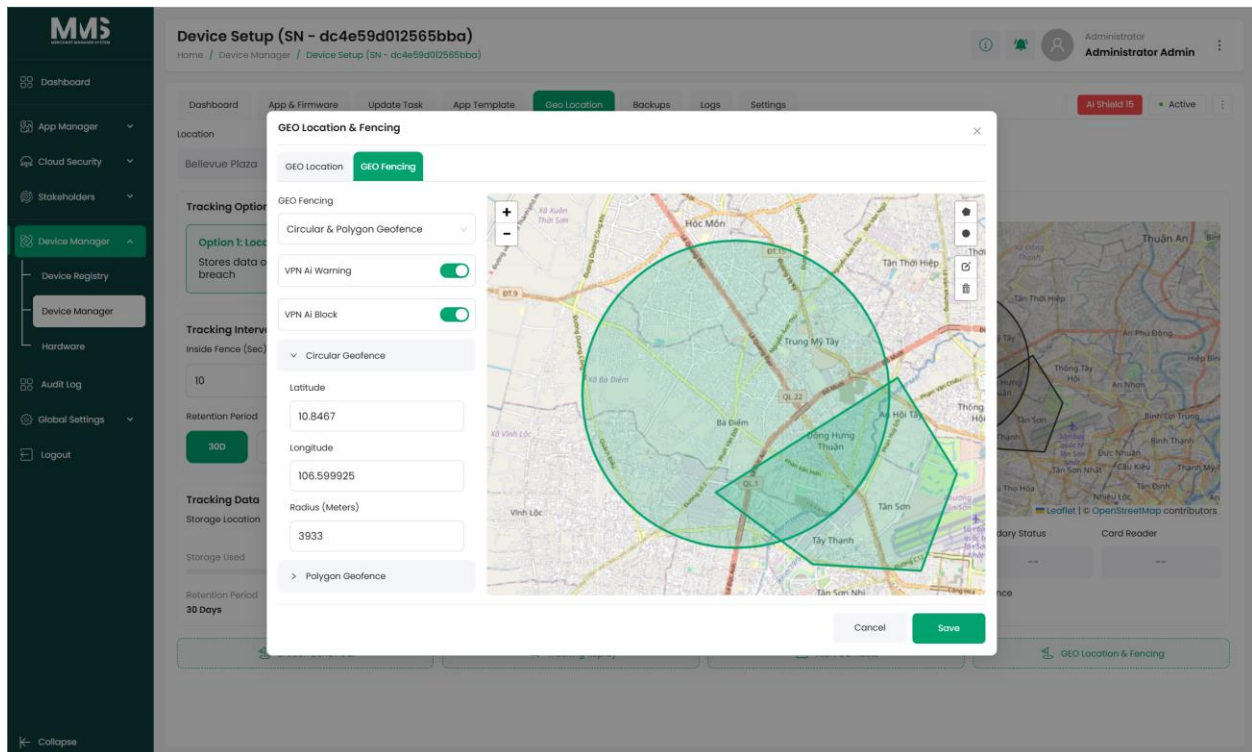
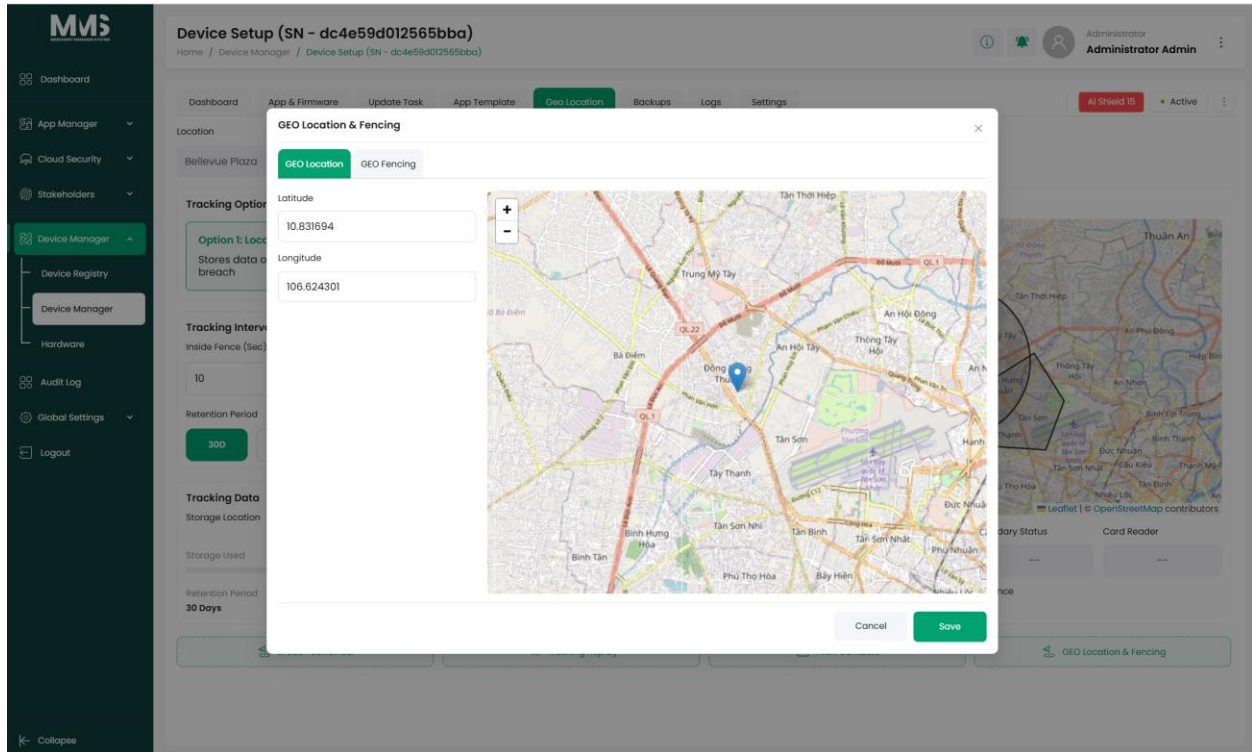
Alert Contacts Modal:

Add emails, name, or cell number

Who has alerts:

- Dung Pham (84868324405 - dung.pham@ugotech.com) - SMS: Off, Email: On

Buttons: Cancel, Save



h. Settings

Status: **Completed**

Reference Images:

The screenshot displays the 'Device Setup' interface for a terminal with SN - dc4e59d012565bba. The interface is divided into two main sections: 'Hardware Components' and 'Device Settings'.

Hardware Components: This section lists various hardware features, each with an 'Enabled' status and a toggle switch. The components shown are:

- PICC: Enabled (Toggle: On)
- Printer: Enabled (Toggle: On)
- Bluetooth: Enabled (Toggle: Off)
- Ethernet: Enabled (Toggle: Off)
- Gravity Sensor: Enabled (Toggle: Off)
- ID Card Reader: Enabled (Toggle: Off)
- SM: Enabled (Toggle: Off)
- PED: Enabled (Toggle: On)
- PED MODE: Enabled (Toggle: On). Below this, three modes are selected: 'Share Mode', 'Isolation Mode', and 'Mixed Mode'.

Device Settings: This section contains system-level configurations:

- GPS Location: Allowed the device to report GPS coordinates (Toggle: On)
- Screen Brightness: Set to 22% (Slider: 22%)
- Device Volume: Set to 75% (Slider: 75%)
- System Language: Set to VietNam (Dropdown)
- Time Zone: Set to Adak (UTC-10) (Dropdown)
- Sleep Timeout: Set to 10 minutes (Input: 10, Unit: s)

The interface includes a top navigation bar with tabs for Dashboard, App & Firmware, Update Task, App Template, Geo Location, Backups, Logs, and Settings (active). A 'Save' button is located in the top right corner of the settings panel. The left sidebar contains navigation options: Dashboard, App Manager, Cloud Security, Stakeholders, Device Manager (active), Device Registry, Device Manager, Hardware, Audit Log, Global Settings, and Logout.

5.3. Hardware Management

Description

Provides a centralized management module for defining and maintaining hardware specifications used within the system. Hardware Manager controls the master data of brands, models, OS versions, and firmware versions, ensuring consistency and standardization across all registered devices.

This module serves as the reference layer for device configuration. All devices created in the Device Registry must align with hardware definitions maintained here.

Key Capabilities

- **Brand:** Create and manage supported hardware brands (e.g., Pax, Verifone, Ingenico).
- **Model:** Define and maintain device models under each brand.
- **OS Version Control:** Register and manage supported OS versions per model.
- **Firmware Version:** Maintain firmware versions associated with specific hardware models.
- **Cradle Firmware Version:** Track and manage cradle firmware versions where applicable.

Status: **Completed**

Reference Images:

Brands	Models	OS Version	Firmware Version	Cradles Firmware Version
Pax	A920	1.0.0	v1.0.0	Cradles L1
Verifone	A920 PRO	1.0.1	2025.09.30	
Ingenico	A77	1.0.2		
Castles Technology	A800	1.1.1		
Newland Payment Technology				
Sunmi				

6. Global Setup

6.1 Settings

Description

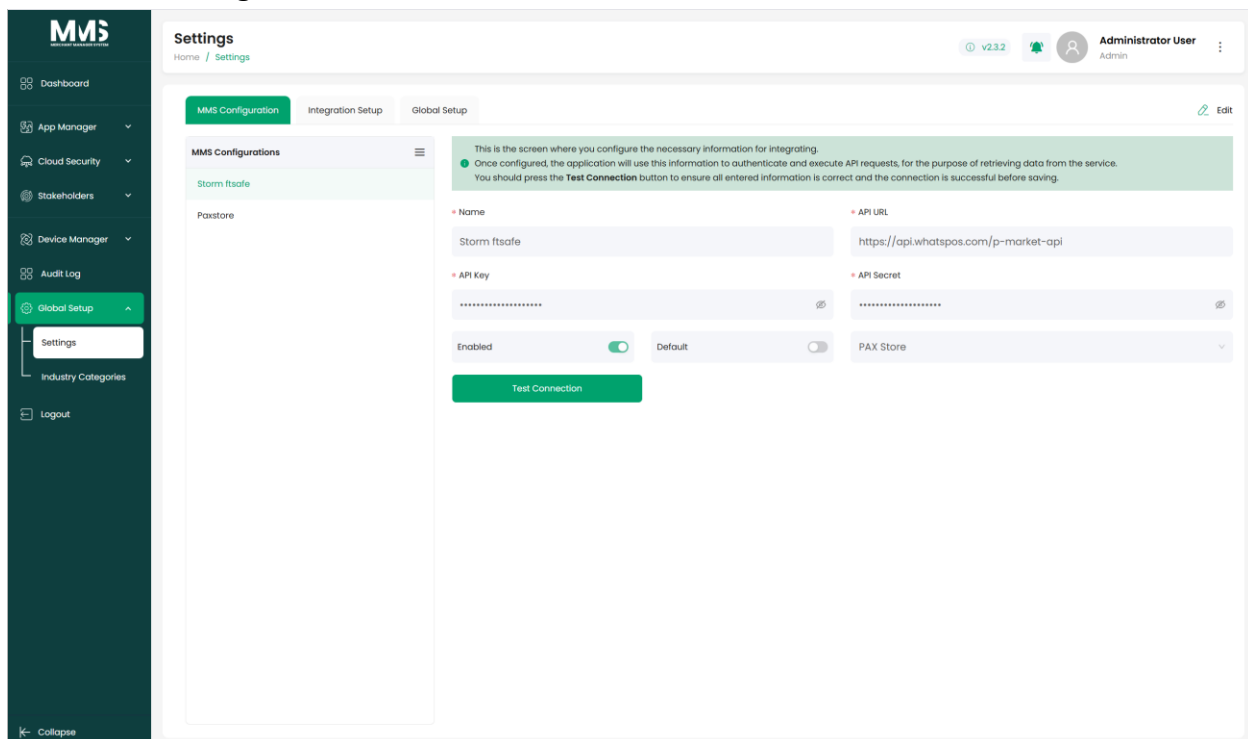
Provides centralized configuration options for managing system-wide and integration-related settings. The Settings module allows administrators to control global behavior, integrations, and core MMS configurations from a single location.

Key Capabilities

- **MMS Configuration:** Configure core system settings that control overall MMS behavior and operational rules
- **Integration Setup:** Manage and configure integrations with external systems and services
- **Global Setup:** Define global parameters
- **File Cleanup Settings:** Manage your file retention and automatic cleanup policies. (for backups and logs file)

Status: **Completed**

Reference Images:



MMS

- Dashboard
- App Manager
- Cloud Security
- Stakeholders
- Device Manager
- Audit Log
- Global Setup
- Settings
- Industry Categories
- Logout

⌵ Collapse

Settings

Home / Settings

v2.3.2

Administrator User
Admin

MMS Configuration

Integration Setup

Global Setup

Reset Key

Configure your external system integration settings below. These credentials will be used to authenticate API requests to your external service.

● Please ensure these credentials are kept confidential.

If you require a new key, you may generate one by clicking the **Reset Key** button above.

Server URL

http://localhost:5173/api

App key

App secret

MMS

- Dashboard
- App Manager
- Cloud Security
- Stakeholders
- Device Manager
- Audit Log
- Global Setup
- Settings
- Industry Categories
- Logout

⌵ Collapse

Settings

Home / Settings

v2.3.2

Administrator User
Admin

MMS Configuration

Integration Setup

Global Setup

Global Setup Types

Version Status

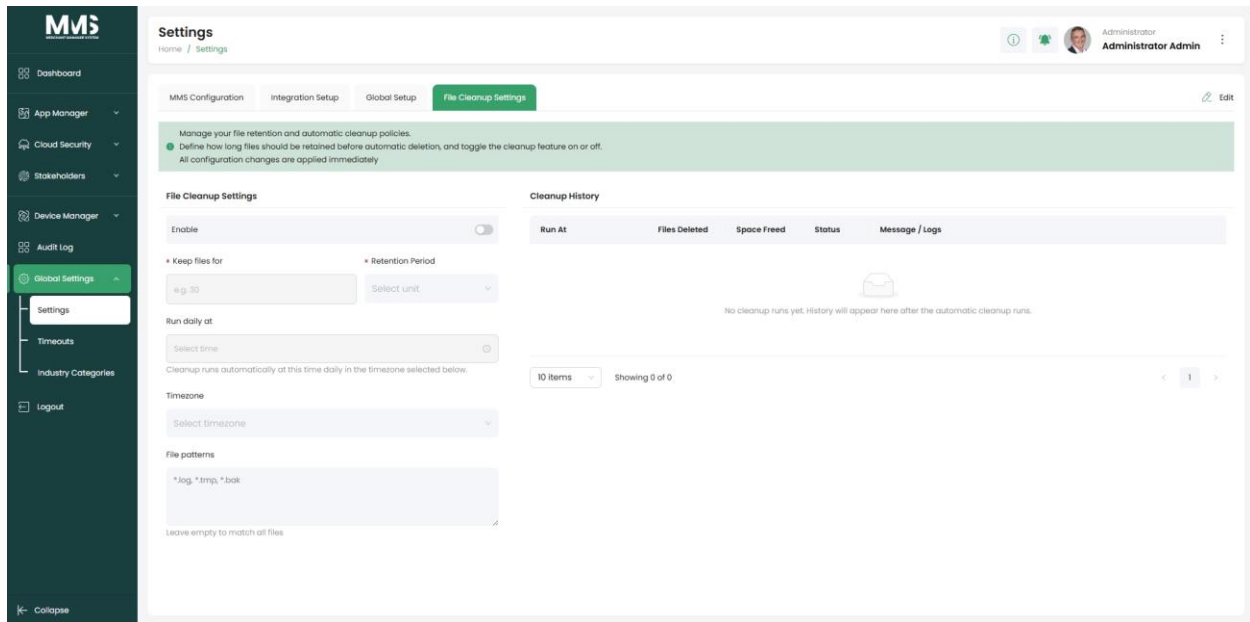
Version Status

+ Add New

Name	Code	Color	Enabled	
BETA	BETA	■ #0824F2	Enable	...
PRODUCT	PRODUCT	■ #FF0808	Enable	...
UAT	UAT	■ #0CAFA0	Enable	...
DEV	DEV	■ #FC058E	Enable	...

MMS Document

Page 51 of 57



6.2 Timeouts

Description

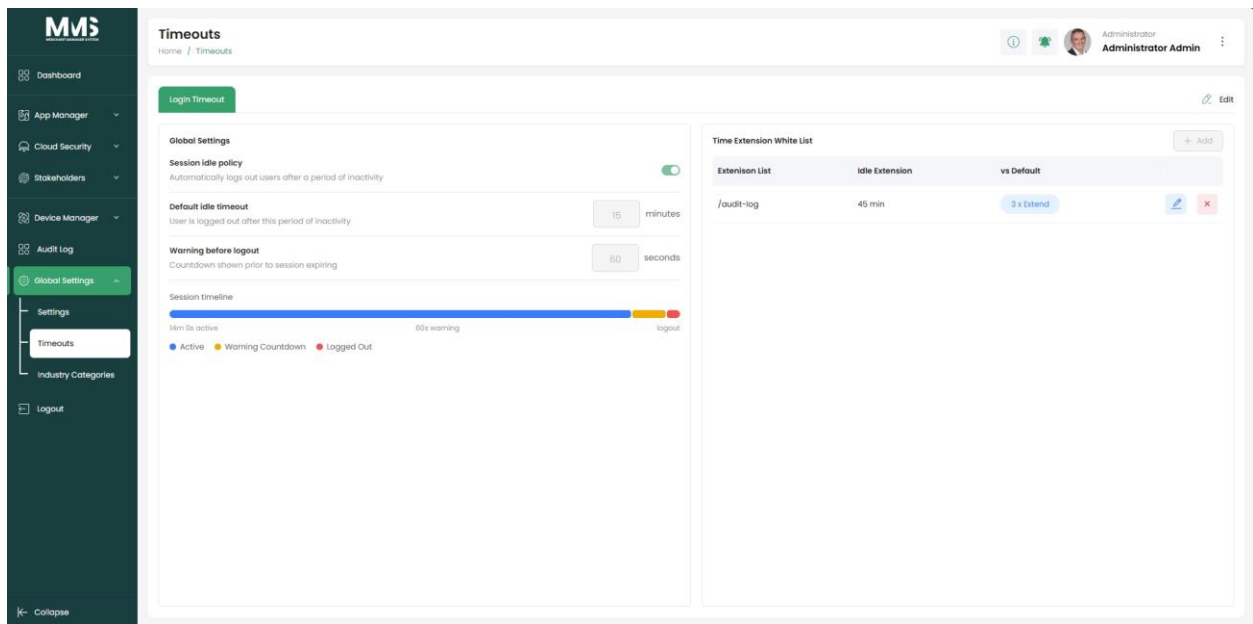
Provides centralized session timeout management to control user inactivity behavior across the system. The Timeouts module enables administrators to define default idle session durations, warning countdowns before automatic logout, and exception-based timeout extensions for specific pages or modules. This helps improve platform security while maintaining usability for operational workflows that require extended active sessions.

Key Capabilities

- Configure a global session idle policy for automatic logout after inactivity
- Define default idle timeout duration for all users and sessions
- Configure warning countdown duration before session expiration
- Display session activity timeline including active, warning, and logout states
- Manage Time Extension White List for specific modules or pages requiring longer session duration
- Configure extended timeout values for selected routes or system functions (e.g., Audit Log)
- Support centralized editing and maintenance of timeout configurations across the platform

Status: Completed

Reference Images:



6.3 Industry Categories

Description

Provides a standardized classification framework for defining industry types and industry categories within the system. Industry Categories are used to consistently classify merchants, enabling better organization, configuration, reporting, and industry-specific behavior across the platform.

Key Capabilities

- Manage a centralized list of **Industry Types** (e.g., Retail, Hospitality, Restaurant, Hotel)
- Manage a centralized list of **Industry Category** (e.g., Cocktail Bar, Wine Bar, Fashion, Hardware)

Status: Completed

Reference Images:

MMS
MERCHANT MANAGER SYSTEM

Dashboard

App Manager

Cloud Security

Stakeholders

Device Manager

Audit Log

Global Setup

Settings

Industry Categories

Logout

← Collapse

Industry Categories

Home / Industry Categories

v2.3.2

Administrator User
Admin

Industry Type	Industry Category
Retail	Cocktail Bar
Supermarket	Wine Bar
Hospitality	Fasion
Motel	Hardware
Restaurant	Accommodation
Pub	Steak House
Bar	Pizza
QSR	Burgers
Hotel	Fish & Chips
Cinema	Coffee
Liquor	Ice Cream
Club	Store
Café	
Car	

7. Audit Log

Description

Provides centralized audit logging and activity tracking across the system. The Audit Log module records user actions, configuration changes, system events, and operational activities to ensure traceability, accountability, and security monitoring. It enables administrators to review historical activities, monitor system usage, and support compliance and troubleshooting processes.

Key Capabilities

- Capture and maintain detailed records of user and system activities
- Track configuration changes, updates, and operational actions performed within the platform
- Record user information, IP address, accessed resource URL, and event timestamp for each activity
- Provide separate views for Operation Logs and System Logs
- Enable filtering and searching of audit records for easier investigation and analysis
- Support export of audit log data for reporting, compliance, and external review purposes
- Provide chronological tracking of activities to support troubleshooting and security investigations

Status: **Completed**

Reference Images:

Audit Log
Home / Audit Log

Administrator Administrator Admin

Operation Log System Log Refresh Export Filter

Operation	User	Resource URL	Timestamp
Test Connection for MMS Configuration	User: Administrator Admin IP: 172.19.0.8	Resource Url: http://mms.project-jump-start.site/setting/test-connection	2026-05-22107:0752
Test Connection for MMS Configuration	User: Administrator Admin IP: 172.19.0.9	Resource Url: http://mms.project-jump-start.site/setting/test-connection	2026-05-22107:0752
Test Connection for MMS Configuration	User: Administrator Admin IP: 172.19.0.9	Resource Url: http://mms.project-jump-start.site/setting/test-connection	2026-05-22106:5311
Update MMS Configuration	User: Administrator Admin IP: 172.19.0.9	Resource Url: http://mms.project-jump-start.site/setting/update-setting/1	2026-05-22106:5309
Copy Template For Terminal	User: Administrator Admin IP: 172.19.0.7	Resource Url: http://mms.project-jump-start.site/application-setup/copy-template-for-terminal	2026-05-21101:3638
Update Base Template	User: Administrator Admin IP: 172.19.0.7	Resource Url: http://mms.project-jump-start.site/app-template/update-template/6	2026-05-18101:2342
Upsert Device Geo Location	User: Administrator Admin IP: 172.19.0.7	Resource Url: http://mms.project-jump-start.site/device-manager/geo-location/12	2026-05-14107:5842
Upsert Device Geo Fence	User: Administrator Admin IP: 172.19.0.7	Resource Url: http://mms.project-jump-start.site/device-manager/geo-fence/12	2026-05-14107:5842
Create Push Task	User: Administrator Admin IP: 172.19.0.7	Resource Url: http://mms.project-jump-start.site/push-task/create-push-task	2026-05-14104:0231
Select Location Item	User: Administrator Admin IP: 172.19.0.7	Resource Url: http://mms.project-jump-start.site/location/select-location-item	2026-05-14101:1850

10 Items Showing 1-10 of 396

Audit Log
Home / Audit Log

Administrator Administrator Admin

Operation Log System Log Refresh Export Filter

Update Device settings	User: Administrator Admin		2026-05-24117:0149
Update Device settings	User: Administrator Admin		2026-05-24116:5453
Update Device settings	User: Administrator Admin		2026-05-24116:3748
Update Device settings	User: Administrator Admin		2026-05-24116:3745
Update Device settings	User: Administrator Admin		2026-05-24116:3554
Update Device settings	User: Administrator Admin		2026-05-24116:3548
Update Device settings	User: Administrator Admin		2026-05-24116:3530
Update Device settings	User: Administrator Admin		2026-05-24116:3004
Update Device settings	User: Administrator Admin		2026-05-24116:3002
Update Device settings	User: Administrator Admin		2026-05-24116:2929

Audit Log Details

Title	Update Device settings
User Name	Administrator Admin
Login Name	-
Action Time	2026-05-24117:0149
IP Address	172.19.0.9
HTTP Method	PUT
Response Status	No Content
Resource URL	https://localhost:7096/device-setup/terminal-setting/12

Request Body

```
{
  "type": "application/json",
  "length": 2419,
  "value": {
    "hardwareComponentList": [
      {
        "id": 1,
        "hardwareName": "Magnetic Stripe Card",
        "iconType": "magnetic_card",
        "status": "enabled",
      }
    ]
  }
}
```

Close

10 Items Showing 1-10 of 364

8. Bulk Changes

8.1. Template Amendments

Description

The Template Amendments module provides centralized management for updating, modifying, and applying configuration changes to device templates across the platform. It enables administrators to create and manage amendment rules for device configurations, application settings, transaction parameters, and operational behaviors in bulk. The module supports structured amendment workflows, template version tracking, scheduled deployment, and device-level monitoring to ensure consistent and controlled configuration management across merchant environments.

Key Capabilities

- Capture and maintain detailed records of user and system activities
- Create, edit, activate, deactivate, and remove template amendment configurations
- Manage amendment rules for application parameters, transaction settings, fees, limits, and device behaviors
- Apply bulk configuration changes to groups of devices or merchant environments through centralized templates
- Support scheduled updates and controlled deployment of template amendments to target devices
- Provide device filtering and saved filter options to simplify device selection and amendment targeting

Status: Progress - EST (05/31/2026)

8.2. Base Template Assign

Status: Design UI - EST (05/31/2026)