



Payment Device SDK - Axium Development Guide Supplement

Document Version: 1.0.1
Date: 19th June 2026



Introduction	3
Setup for Development	4
Device Modes	4
Development	4
Production	4
Pre-Requisites	5
Integration Considerations	5
Android Library Restrictions	5
Connection	5
UI Updates	5
HEM	7
HEM Concepts	7
Users and Roles	7
Campaigns	7
Region	7
Sponsors	8
Estates	8
Terminals	8
Call Schedule	8
HEM Navigation	9
Software Library	9
Campaigns	10
Device Management	10
MDM Profiles	10
User Management	10
Sponsor Selection	11
Requesting Access	11
Device Onboarding Process	13
Partner Onboarding with a Partner Code	13
Role Access Levels	15
PGP-ADMIN	15
PGP-CAMPAIGN-MANAGER	15
PGP-DEVICE-MANAGER	15
PGP-MDM-MANAGER	16
PGP-VIEW-ONLY	16
Admin Controls	17
User Management	17
Create a new account	18
Defining Access	19
Device Manager Controls	21
Managing Estates	21

Adding Estates	22
Adding Terminal	23
Call Schedule	24
Campaign Managers	26
Upload Software	26
Campaign Creation	26
MDM Managers	28
Viewers	31
Application Signing	32
Signing	32

Introduction

This supplement provides information for integration partners who wish to develop their own applications to run on Axiom devices. It covers the steps required to set up development on an Axiom device, as well as how to access and use Ingenico's Hosted Estate Manager and E-Signing platform.

Setup for Development

Development Axiom devices operate just like a normal Android device once plugged into your development machine they will appear in Android studio. You will also use the ChipDNA Mobile SDK as you would in a standard Semi Integrated environment.

Device Modes

When selecting a device it's important to get the correct configuration for the purpose you require it for. Axiom device can come in two variants:

DEVELOPMENT

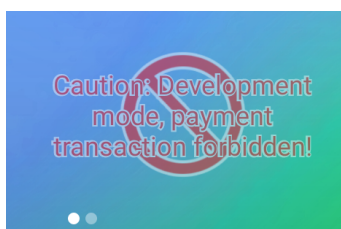
Development devices are injected with test keys and can only be used in the Test environment. They are intended for building and testing applications directly on the device.

These devices:

- Ignore application signature validation
- Can be connected to Android Studio
- Display a warning message on the home screen

Once a device has been set to Development mode, it cannot be reverted to Production mode without being returned to Ingenico.

Development devices can be identified by a flashing warning sign on the home screen:



PRODUCTION

Production devices are injected with production keys and can be used in both Test and Production environments. These are intended for standard usage where no on-device development is required.

These devices:

- Only run applications signed via Ingenico's e-signing portal
- Do not appear in Android Studio
- Cannot be used for development

Pre-Requisites

- Android SDK Target 29
- Android Studio
- ChipDNA Mobile SDK v5.2.0 or above

Integration Considerations

Developing on a development Axiom device is very similar to developing an application for standard Android. However there are some considerations to think about.

ANDROID LIBRARY RESTRICTIONS

While the version of Android running on Axiom devices is based on the standard Android distribution, some standard Android Libraries have been removed in order for the OS to meet PCI security requirements.

CONNECTION

In order to connect to the TransactionInitiatorUI application from an application running on the same device you must use the following connection properties:

- Connection Type: TCP-IP
- IP Address: 0.0.0.0
- Port No. 8088

To set this within the ChipDNA Mobile SDK it would look like the following:

```
Parameters requestParameters = new Parameters();
    requestParameters.add(ParameterKeys.PinPadConnectionType,
ParameterValues.TcpIpConnectionType);
    requestParameters.add(ParameterKeys.PinPadName, "Axiom-"+Build.MODEL);
    requestParameters.add(ParameterKeys.PinPadIpAddress, "0.0.0.0");
    requestParameters.add(ParameterKeys.PinPadPort, "8088");

ChipDnaMobile.getInstance().setProperties(requestParameters);
```

UI UPDATES

When making calls to the ChipDNA Mobile SDK, the Ingenico ARC UX application is brought to the foreground to handle transaction processing. This behaviour is controlled by Ingenico, and NMI cannot return the integrating application to the foreground automatically. While the ARC UX application is in the foreground, your application continues to run in the background and will still receive standard updates from the ChipDNA Mobile SDK.

If your application needs to regain control and return to the foreground, call the method below from your transaction listener — typically at the end of **onTransactionFinishedListener** (and, if required, on the **GetCardDetailsCompleted** transaction update).

Two points to note:

- Use an Intent with `FLAG_ACTIVITY_REORDER_TO_FRONT` as the primary approach. `moveTaskToFront` is increasingly restricted on modern Android and is used here only as a fallback.
- A short delay is recommended before bringing your application forward, so the ARC UX application can finish its own screen teardown first.

The method must be a member of the Activity you want to bring to the foreground, so that `this` and `taskId` resolve correctly:

Kotlin

```
**  
* Returns the integrating application to the foreground after a transaction  
* completes. Call from your transaction listener (e.g.  
onTransactionFinishedListener).  
*  
* @param delayMs delay before returning to the foreground, allowing the ARC  
UX  
* application to finish its screen teardown first.  
*/  
private fun bringAppToForeground(delayMs: Long = 500) {  
    Handler(Looper.getMainLooper()).postDelayed({  
        try {  
            // Preferred: re-order this app's existing task to the front.  
            val intent = Intent(this, YourActivity::class.java).apply {  
                addFlags(Intent.FLAG_ACTIVITY_REORDER_TO_FRONT or  
                    Intent.FLAG_ACTIVITY_SINGLE_TOP)  
            }  
            startActivity(intent)  
        } catch (e: Exception) {  
            // Fallback: move the task to the front via ActivityManager.  
            val activityManager =  
                getSystemService(Context.ACTIVITY_SERVICE) as ActivityManager  
            activityManager.moveTaskToFront(  
                taskId, ActivityManager.MOVE_TASK_NO_USER_ACTION)  
            }  
        }, delayMs)  
    }  
}
```

Call it from your transaction-finished handler:

Kotlin

```
override fun onTransactionFinishedListener(parameters: Parameters) {  
    // ... your existing transaction handling ...  
    bringAppToForeground()  
}
```

The following permission will also need to be added to the applications manifest file.

```
<uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
```

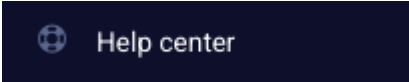
Note: From Android API 29, an application in the background is prevented from launching activities or moving its task to the foreground. The `SYSTEM_ALERT_WINDOW` permission exempts your application from this restriction, which is what allows the code above to work. This is a special permission that must be **granted** on the device — either by the user ("Display over other apps") or through your MDM profile. You can verify it at runtime with `Settings.canDrawOverlays(context)`; if it returns `false`, the calls above will silently have no effect.

HEM

This section provides a brief overview of the structure and key concepts used in HEM.

HEM is an Ingenico-owned product and may be subject to change without prior notice to NMI. The information provided here is intended as a starting point, covering basic concepts and common tasks.

For more detailed guidance, refer to Ingenico's official documentation, which is available within HEM via the navigation menu under the following tab:

A dark blue rectangular button with a white globe icon on the left and the text "Help center" in white on the right.

HEM Concepts

USERS AND ROLES

A user is a member of your organisation that you wish to give access to HEM. PGP-ADMIN is the only role allowed to add new users.

Roles define the level of access a user is granted. A user can hold multiple roles so one user can be a PGP-DEVICE-MANAGER and a PGP-CAMPAIGN-MANAGER to allow a single user to manage the devices and campaigns for those devices.

CAMPAIGNS

Campaigns allow you to assign Axiom software from the software library to devices, ensuring it is installed the next time the device connects to HEM. Within a campaign you can assign software to either individual devices or entire estates, giving you flexibility over software deployment.

REGION

NMI operates at the Region level of HEM. All sponsors, estates and terminals reside within NMI's region.

SPONSORS

Sponsors is the highest level structure accessible for partners on HEM. Sponsors are linked to a Partners ID. Depending on your integration type this will either be:

- Cardease Client ID
- Omni Platform Affiliate ID

Each sponsor holds its own software library, estates and terminals.

Devices will be assigned to your sponsor the first time it reaches out to the NMI backend. Once a device is registered on HEM it can move between sponsors by an Admin or user holding the PGP-DEVICE-MANAGER role.

ESTATES

Estates can contain Sub-Estates and Terminals. Estates are a way to group Terminals. You can create as many estates as needed and organise your Terminals within the Estate as required. Estates enable you to assign Campaigns to groups of terminals instead of needing to select terminals individually

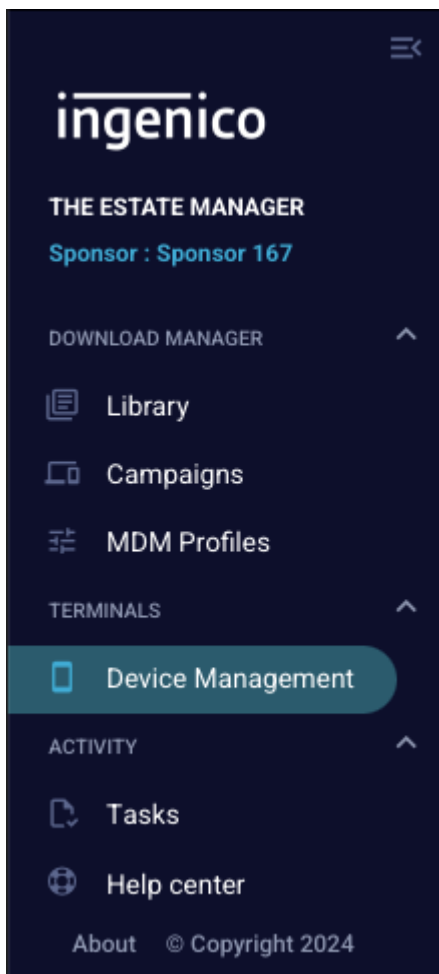
TERMINALS

Terminals align with devices. Devices are onboarded onto HEM at the distributor and sit in a holding estate until it connects to the NMI Backend. A device will be added to a Sponsors default estate when it first connects up to the NMI backend.

CALL SCHEDULE

A call schedule can be assigned to a terminal or an estate then synced to all terminals below it. By default all devices are assigned a 24 hour call schedule, meaning every 24 hours the device will make a call to HEM and run any Campaigns assigned to it.

HEM Navigation



Once access is granted the left hand bar of HEM will show the navigation options. The appearance may vary depending on your access level, as HEM only displays the options available to you.

SOFTWARE LIBRARY



The library section allows management of your software library. It allows you to upload your Axiom compatible software.

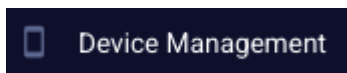
This must be in APK or UNS format and signed with a valid Ingenico e-signing card if you are intending to load it onto production devices.

CAMPAIGNS



The campaign section allows management of Campaigns. Campaigns allow you to set software uploaded to the software library to be installed onto devices within your estate.

DEVICE MANAGEMENT



From device management you can view all estates and terminals associated with your current sponsor.

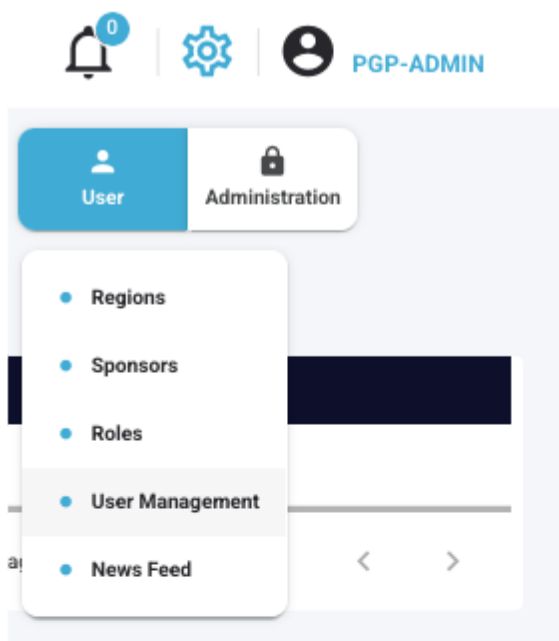
From this section you can move your devices between estates, configure call schedules

MDM PROFILES



The MDM Profiles section allows you to create and manage your MDM profiles. This section allows you to control aspects of your devices OS settings such as Wi-Fi network settings, boot launching of an application etc.

USER MANAGEMENT



User management is available under the cog wheel icon at the top right of the page. Only users with the role PGP-ADMIN have access to this section.

SPONSOR SELECTION



If your user account has access to multiple sponsors you can select which one you are viewing by clicking on the current sponsor name.

Select a Sponsor



Saving sponsor selection will reload the home page. All your unsaved changes will be lost.

Search

Region	Sponsor Name
☐ NMI UK	Original Sponsor 167
☒ NMI UK	Sponsor 167

1-2 of 2



1



Cancel

Admin Mode

Save Selection

Requesting Access

Access to HEM incurs an additional cost. To request access, please contact your Account Manager.

To ensure the correct level of access is provisioned, include the following information in your request:

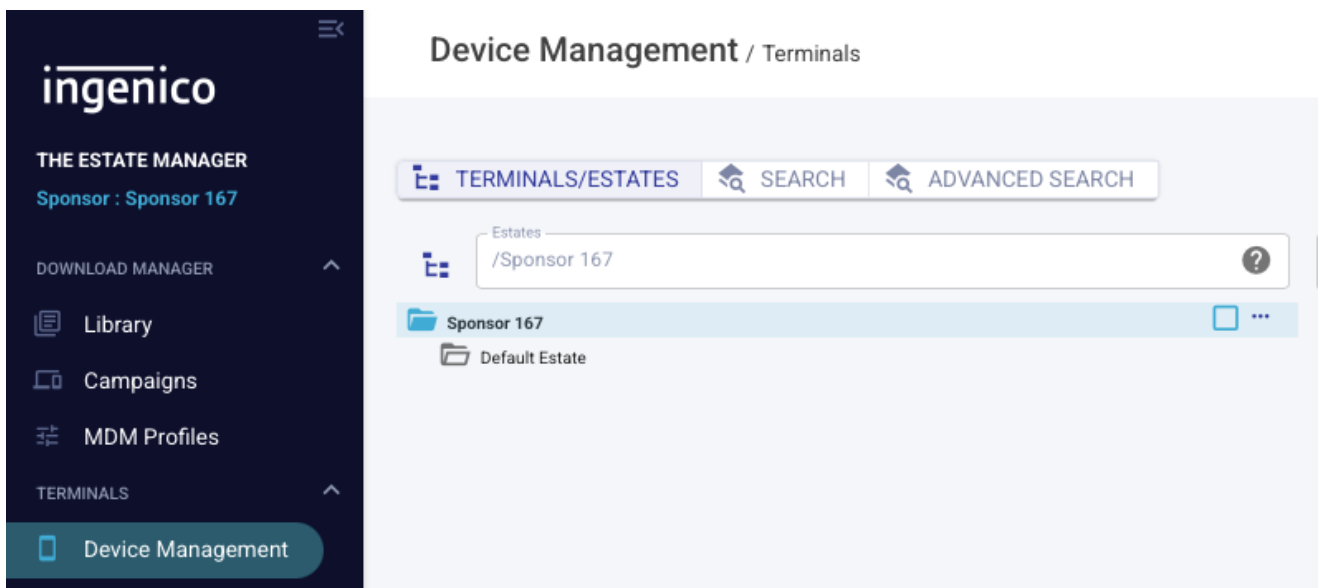
- Account Name
- Client/Affiliate ID(s) (if known), otherwise the serial number of a registered device
- Initial Admin Details:
 - Email
 - First name
 - Last name
- E-signing Portal Account Details (for Pushers and Validators):
 - Email
 - First name
 - Last name

Once provisioned, an email will be sent to the provided address to complete setup of the admin account. The admin user can then grant access to additional users as required.

Device Onboarding Process

All terminals are boarded onto HEM at the point of distribution. Until a device is first used, it remains in a holding estate that is only accessible to NMI personnel. Attempting to add a device that has already been boarded onto HEM will fail.

When the device is first registered and configured with the NMI backend, it is automatically moved to a default estate under a sponsor associated with the NMI account using the device.



A sponsor is linked to an NMI partner ID, which will be one of the following:

- Cardease Client ID
- Omni Platform Affiliate ID

If you use devices across multiple Client or Affiliate IDs, you will need access to each corresponding sponsor.

Partner Onboarding with a Partner Code

By default devices are automatically moved to your sponsor's default estate the first time they register with the NMI backend based on their Client or Affiliate ID (see Device Onboarding Process above).

The Partner Code flow provides an alternative: it allows you to direct a device into a specific onboarding estate that you control. This ensures that your custom applications and

configurations install automatically, without requiring the device to be tied to your specific Client or Affiliate ID.

At a high level, you prepare an onboarding estate and a permanent campaign in HEM, NMI links a Partner Code to that estate, and your end-users enter the code on their device using the Partner Onboarding app.

Setting up for Partner Code Onboarding

These are one-time steps you complete in HEM before distributing the code to your end users.

1. **Create an onboarding estate.** In Device Management, create an estate to act as your onboarding target (see Adding Estates). All devices that use your Partner Code will be moved into this estate.
2. **Create a permanent campaign.** In the Campaigns section, create a campaign containing the application(s) and configuration required for your all-in-one integration, and assign it to your onboarding estate (see Campaign Creation).
 - a. Important: Enable the Permanent Campaign switch to ensure the software is installed immediately whenever a device enters the estate.
3. **Share your estate ID with NMI.** Provide the ID of your onboarding estate to your Account Manager.
 - a. Tip: You can find the estate ID in the URL when viewing your estate in HEM — it appears as the `currentEstate` parameter, for example:
`https://<hem-address>/deviceManagement?currentEstate=12345678-0dc0-1234-a123-1234ac5a1e23`
4. **Receive your Partner Code.** NMI will provision a Partner Code linked to your onboarding estate and return it to you. A single code maps to one estate and can be reused across all of your devices.
5. **Distribute the Partner Code** to your end users, along with their device.

The End-User Experience

A new device is first set up using the NMI Setup App, which guides the user through Wi-Fi and, optionally, Bluetooth set up, registers the device with the NMI backend, and downloads the NMI Transaction Initiator and Device Agent applications.

To complete partner onboarding, the user then opens the **Partner Onboarding app** and enters their Partner Code.

If the user enters a valid Partner Code, the device is moved into your onboarding estate and an update is triggered immediately, installing the applications from your permanent campaign. The user can exit the app without entering a code if they do not have one; the device then remains in its default estate and can be onboarded later.

If a code is entered incorrectly, the user is prompted to check it and try again. A code that is not recognised should be reported to you, so it can be confirmed against the one NMI provisioned.



Note: The code is not case-sensitive and may be shown grouped with hyphens for readability (for example 000-019-VW); the hyphens are optional and the code can be entered with or without them.

Role Access Levels

The following is a brief summary of the predefined roles and the permissions they provide to users

PGP-ADMIN

Section	Access
Software Library	Read/Write/Update
Campaigns	Read/Write/Update
Device Management	Read/Write/Update
MDM Profile	Read/Write/Update
User Management	Read/Write/Update

PGP-CAMPAIGN-MANAGER

Section	Access
Software Library	Read/Write/Update
Campaigns	Read/Write/Update
Device Management	Read
MDM Profile	Read
User Management	None

PGP-DEVICE-MANAGER

Section	Access
Software Library	Read

Campaigns	Read
Device Management	Read/Write/Update
MDM Profile	Read
User Management	None

PGP-MDM-MANAGER

Section	Access
Software Library	Read
Campaigns	Read
Device Management	Read
MDM Profile	Read/Write/Update
User Management	None

PGP-VIEW-ONLY

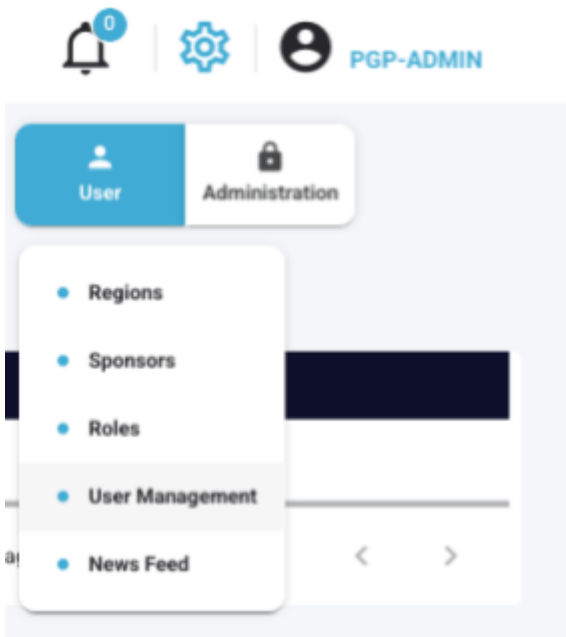
Section	Access
Software Library	Read
Campaigns	Read
Device Management	Read
MDM Profile	Read
User Management	None

Admin Controls

This section will detail Admin specific controls. Admin accounts also have the permission granted to other roles. To avoid repetition please refer to the other role section for further information on controls available to admins.

USER MANAGEMENT

User management is accessible via the cog icon in the top right corner of HEM.



From the user management screen you'll be able to see details on all the users currently added to all sponsors your own account has access to.

A screenshot of the 'User / User Management' screen. At the top, there's a breadcrumb 'User / User Management' and the same navigation icons as the previous image. Below is a search bar and a '+ New User' button. The main content is a table with the following columns: Username, Access List, Roles, Status, Api, Created By, Creation Date, Last Login Date, Locked, and 2FA. There are two rows of user data. At the bottom, there are icons for user management and a pagination control showing 'Rows per page: 10' and '1-2 of 2'.

Clicking the “...” next to the user will open the following menu:



From right to left this will allow you to perform the following actions:

- Edit user details
- Reset 2FA
- Set a new Password
- Send a reset password email
- Deactivate the account
- Delete the account

Create a new account

To create a new user account click the **+New User** button:



This will show the add user menu to input new user details and assign them their access type.

NMI does not impose any requirements around input and you only need to fill in fields that HEM requires or you would like to input. Required fields include:

- User Name
- Email - for the user being added
- Role - defines the level of access being granted

You can either set the new user's password, or have HEM send them an email to set their own password and 2FA.

This is controlled by the following toggle switch:



Defining Access

There are 2 parts to defining access:

- Sponsor Access
- User Role

By default new users will be assigned access to all sponsors that the Admin creating the user has access to. To adjust this click on the “Access List” table to begin editing. You can then click the Trash Bin icon next to a sponsor to remove it or click “Add” to add a sponsor.

☐ Full Add ^

REGION	SPONSOR	
NMI UK	Original Sponsor 167	
NMI UK	Sponsor 167	

Rows per page: 10 1-2 of 2 < 1 >

When adding you will need to select the “NMI UK” Region as all NMI partner sponsors will be under this region. You will then see a list of sponsors that your account has access to and can select ones that you wish to allow the new user access to.

Add access

Select one or several regions and/or one or several sponsors

Region

NMI UK

Sponsor

Original Sponsor 167

Cancel

Ok

To set the user's role click the roles drop down box and select the roles you wish to give the new user. You can select as many as you want. The access granted by these roles can be reviewed in the [Role Access Levels](#) section above.

Roles *

- ☐ PGP-ADMIN
- ☐ PGP-CAMPAIGN-MANAGER
- ☐ PGP-DEVICE-MANAGER
- ☐ PGP-MDM-MANAGER
- ☐ PGP-VIEW-ONLY

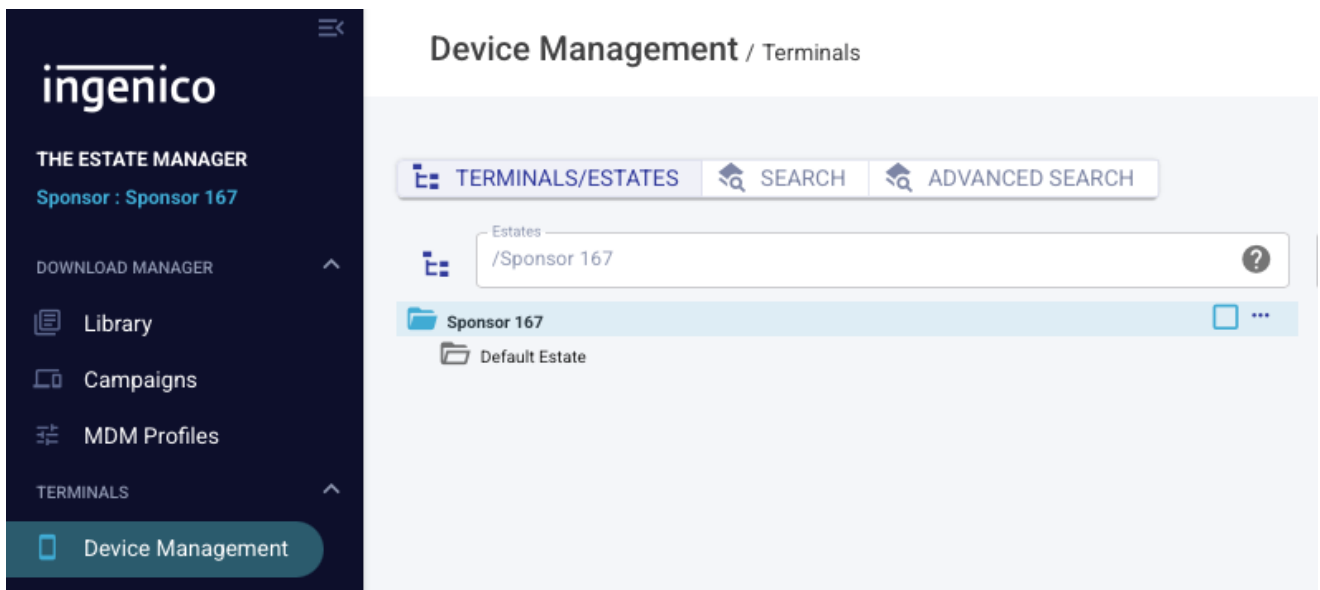
Once you're satisfied with the user's account information click the "Ok" button to complete the process of the user being added.

Device Manager Controls

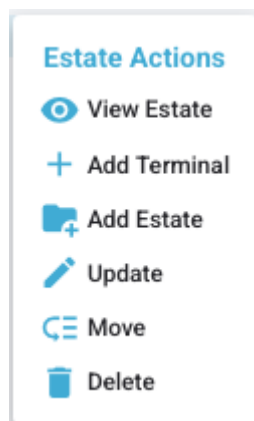
The device manager role grants access to the Device Management page of HEM. This page allows you to manage your terminals and estates, building them into a logical structure to make management easier.

MANAGING ESTATES

To add a terminal or estate within the device management section of HEM, select the parent estate you would like to add the terminal or estate to. This will reveal a “...” to the right of the estate name.



Clicking this will reveal a menu showing the operations you can perform:



- View Estate - View the details of the current estate selected
- Add Terminal - Add a new terminal to the estate
- Add Estate - Add new sub-estate

- Update - Update the details of the selected estate
- Move - Move the selected estate/terminal to a new location
- Delete - Delete the current estate/terminal

Adding Estates

GENERAL

CALL SCHEDULE

Parent Name

Sponsor 167

Signature*

com.nmi.sponsor167.newestate

Name*

New Estate

Type

Axiom

Status

☒ Enabled ☐ Disabled

Description

Merchant Id

Tags

Cancel

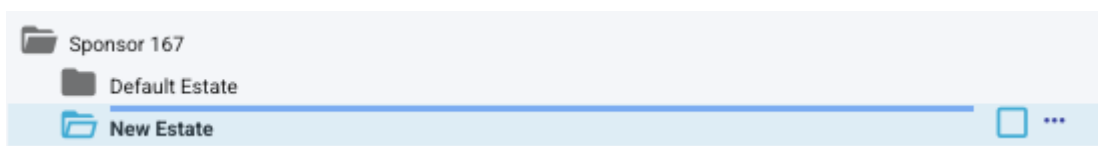
Save

To add estates the following information must be filled out:

- Estate Name - what you would like the estate to be called
- Signature - a **unique** identifier for this estate. NMI recommends using a domain based identifier as shown in the example above.

The other fields can be filled out as you feel necessary, NMI doesn't place any restrictions on content.

When you are ready click the save button. The new estate can be found under the specified parent estate.



Adding Terminal

If you have ordered your device through an NMI-approved distributor, you do not need to manually add terminals. New terminals will automatically appear in your default estate after their first registration with the NMI platform.

Attempting to add a device supplied by an NMI-approved distributor may fail, as the device is already registered within the NMI HEM region.

The following information is provided for completeness, in case manual terminal creation is required.

Add Terminal

GENERAL

CALL SCHEDULE

LOCATION

Parent Name

New Estate

Signature*

235GKD420124

Type

Axiom

Name*

Prod-DX8000-235GKD420124

Status

☒ Enabled ☐ Disabled

Description

Merchant Id

Tags

Cancel

Save

Adding a terminal is similar to creating an estate. You will be required to provide the following information:

- **Terminal Name** – The name assigned to the terminal
- **Signature** – The device's serial number

All other fields can be completed as needed. NMI does not impose restrictions on their content.

CALL SCHEDULE

The call schedule defines when a device calls home to HEM to see whether updates are required. The call schedule can be adjusted against the estate and synced to the terminals or a terminal can have its own call schedule.

GENERAL
CALL SCHEDULE
LOCATION

General

☒ Enable Call Scheduling
☐ Enable Load Balancing
☐ Protect From Parent Update

Scheduling Parameters

☐ Force Time

Frequency days
1

Retry period (hours)
1

Timezone Adjustment
No Adjustment

Window
From 00:00 to 00:00

☐ Reject Calls Outwith Window

Cancel
Save

The fields are as follows:

- **Enable Call Scheduling** - Enable or disable call scheduling. A device must call home in order for call scheduling updates to take effect.
- **Enable Load Balancing** - HEM will spread devices across the maintenance window with this enabled so they don't all call home at once.
- **Protect From Parent Update** - Enabling this will mean a terminal won't receive updates to its call schedule from its parent estates.
- **Frequency days** - How often the device will call home in days.
- **Retry Period** - If a HEM call fails how often will a device try for within the call window.

- Timezone Adjustment - Allows you to adjust the maintenance window to the Terminal Local time.
- Window - The maintenance window that a device will call home in.
- Reject calls out with Window - HEM will reject calls that are not within the maintenance window



Note: the call schedule is not pushed to the device when saved on HEM and is only updated on the terminal the next time the device calls home. If call scheduling is disabled on a device a manual HEM update must be performed to re-enable it.

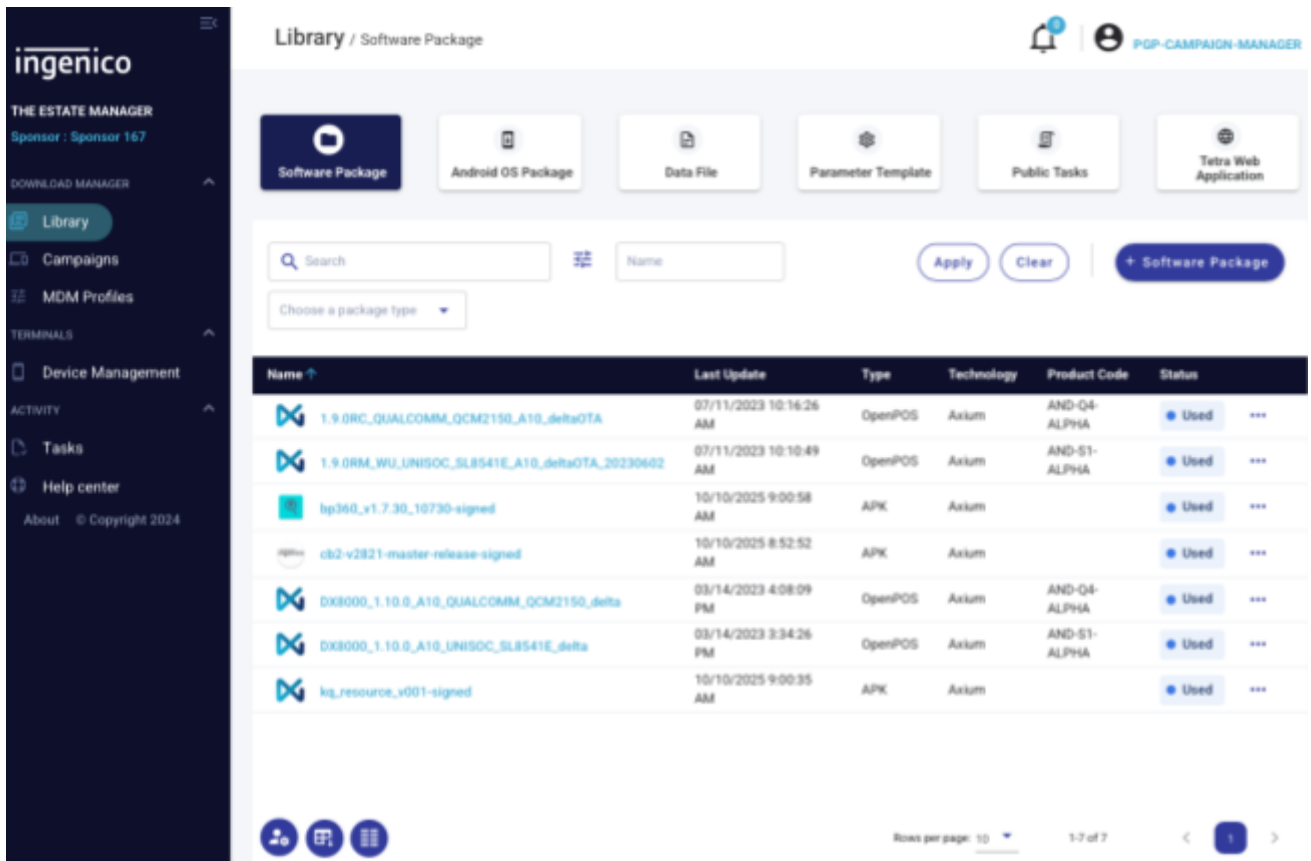
Setting the call schedule at the estate level will be applied to all devices within that estate as long as those devices don't have their own call schedules applied.

Campaign Managers

The campaign manager role grants a user access to the Software Library and the Campaign section of HEM. In the Software Library you are able to upload your APKs to HEM then in the campaign section you can choose how software will get applied to terminals.

UPLOAD SOFTWARE

You can upload your APK to HEM from the library section of HEM. From the Software Package tab click on the “+ Software Package” button



The screenshot shows the 'Library / Software Package' section of the Ingenico HEM interface. The left sidebar contains navigation options: THE ESTATE MANAGER, Sponsor: Sponsor 167, DOWNLOAD MANAGER, Library (selected), Campaigns, MDM Profiles, TERMINALS, Device Management, ACTIVITY, Tasks, and Help center. The main content area has a top bar with 'Library / Software Package' and a user profile 'PGP-CAMPAIGN-MANAGER'. Below this is a row of buttons: Software Package (selected), Android OS Package, Data File, Parameter Template, Public Tasks, and Tetra Web Application. A search bar and a 'Choose a package type' dropdown are present. A table lists software packages with columns: Name, Last Update, Type, Technology, Product Code, and Status. The table shows several packages, including '1.9.0RC_QUALCOMM_QCM2150_A10_deltaOTA', '1.9.0RM_WU_UNISOC_SL8541E_A10_deltaOTA_20230602', 'bp360_v1.7.30_10730-signed', 'cb2-v2821-master-release-signed', 'DX8000_1.10.0_A10_QUALCOMM_QCM2150_delta', 'DX8000_1.10.0_A10_UNISOC_SL8541E_delta', and 'kg_resource_v001-signed'. Each package has a status of 'Used' and a three-dot menu icon. At the bottom right, there is a 'Rows per page: 10' dropdown and a '1-7 of 7' indicator.

Name	Last Update	Type	Technology	Product Code	Status
1.9.0RC_QUALCOMM_QCM2150_A10_deltaOTA	07/11/2023 10:16:26 AM	OpenPOS	Axiom	AND-Q4-ALPHA	Used
1.9.0RM_WU_UNISOC_SL8541E_A10_deltaOTA_20230602	07/11/2023 10:10:49 AM	OpenPOS	Axiom	AND-S1-ALPHA	Used
bp360_v1.7.30_10730-signed	10/10/2025 9:00:58 AM	APK	Axiom		Used
cb2-v2821-master-release-signed	10/10/2025 8:52:52 AM	APK	Axiom		Used
DX8000_1.10.0_A10_QUALCOMM_QCM2150_delta	03/14/2023 4:08:09 PM	OpenPOS	Axiom	AND-Q4-ALPHA	Used
DX8000_1.10.0_A10_UNISOC_SL8541E_delta	03/14/2023 3:34:26 PM	OpenPOS	Axiom	AND-S1-ALPHA	Used
kg_resource_v001-signed	10/10/2025 9:00:35 AM	APK	Axiom		Used

This will bring up a file browser where you can select your APK for upload.



If you are intending to distribute your APK to production Axiom devices it must be signed with a valid ecard from Ingenico's e-signing portal.

CAMPAIGN CREATION

To create a campaign under the Campaigns section of HEM click the “+ New Campaign” button.



This will bring up a window to allow you to input your campaign details:

Define campaign type

☒ Classical - at next terminal call

Set a name and select a deployment period

Campaign name* 0 / 50

Priority (0 to 100)* 50

☐ Permanent campaign

Description 0 / 100

Start date* 03/18/2026 5:03:12 PM

End date

☒ No end date

A campaign requires the following:

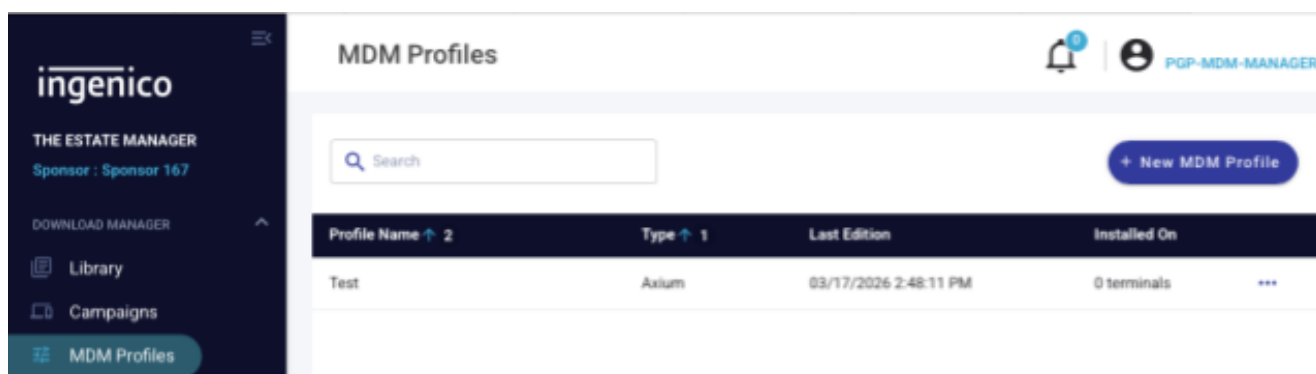
- Campaign Name - what you would like the Campaign to be called.

Useful to know:

- Permanent Campaign Switch - Will mean the campaign is applied to devices even if they have already been applied previously. Note: this will not mean the same software is installed multiple times just that it will be re-installed if removed.
- Priority - You can have multiple campaigns set against the same device or estate. These will be run in priority order with 100 being the highest priority.

MDM Managers

MDM Managers have access to the MDM Profiles section of HEM. Here they are able to create, modify and apply MDM Profiles to devices.



MDM Profiles are applied in a similar way to Campaigns. First you need to create one using the “+ New MDM Profile” button.

Create new MDM profile

Terminal Type *
Axiom

Name *
Test Profile

Cancel Ok

Set the type of profile to “Axiom” and use a name that makes sense for your needs. Then click “Ok” and HEM will allow you to fill out details for your MDM Profile

WI-FI MOBILE NETWORK MOBILE NETWORK - SIM 1 MOBILE NETWORK - SIM 2 POS SPECIFIC DISPLAY AND SOUND OTHER PERIPHERALS

Wi-Fi ☐ Activated ☐ Deactivated ...

Allow user to change Wi-fi settings ☒ ...

Wi-Fi sleep policy <null> ...

Wi-fi profile

SSID	Password	Wi-Fi Security Type
Add		

Validate Save And Apply Close

Once complete you can validate the profile using the “Validate” button and then “Save and Apply”. You’ll notice your profile is then available to be applied to devices. You will do this using the ‘...’ available at the right of the profile.

Profile Name ↑ 2	Type ↑ 1	Last Edition	Installed On
Test Profile	Axium	03/19/2026 10:32:50 AM	0 terminals    

This allows you to delete, apply or edit your profile. Clicking the cross-hairs symbol will show you the current devices/estates that are currently being targeted:

Search	+ New MDM Profile	 	+ Add Targets
Profile Name ↑ 2	Type ↑ 1	Last Edition	Installed On
Test Profile	Axium	03/19/2026 10:32:50 AM	0 terminals ...
No data available			

More targets can be added using the “+ Add Targets” button. This will allow you to explore your current estates and select any you wish the MDM Profile to apply to.

Select estates or terminals

Estates

/Sponsor 167

Sponsor 167

Default Estate

New Estate

Search for terminals in selected estate on Name, Signature

CHOOSE

SELECTED

Name	Signature	Type
No data available		

Close

OK

Targets will receive the MDM profile next time they call home.

Viewers

NMI has provided the PGP-VIEW-ONLY role which allows a user “view” access to your HEM estate. They will be able to view all pages **except** from the User Management Page.

Application Signing

Any application intended to run on a production Axiom device must be signed using a valid e-signing card provided by Ingenico.

To sign an application, you will need access to Ingenico's e-signing portal and a provisioned e-signing card. NMI will assist in enabling this via your Account Manager when access to HEM is requested.

Signing

Signing is a two-step process involving two user roles:

- Pusher
- Validator

The Pusher uploads the application (APK) to the Ingenico e-signing portal and submits it for validation.

The Validator reviews the APK to ensure it is suitable for signing and, if approved, completes the signing process.

NMI will provision four accounts for the Ingenico e-signing portal:

- Two Pushers
- Two Validators

These accounts are included in the cost of enrollment. Additional accounts can be provisioned via your Account Manager for an additional fee.