Device Management Portal Integrator DMP GUIDE

Version V1.3 Aug 04, 2020

FREEDOMPAY

NEXT LEVEL COMMERCE

Document Version History

VERSION	DATE	AUTHOR	REASON FOR CHANGE
1.3	2020-08-04	Minesh Patel	• Rebranded
1.2	2019-07-16	Steve Pickard	• Updated
1.1	2019-03-25	Daniel Profico	• Updated
1.0	2019-01-01	Daniel Profico	• Initial Version

© 2020 FreedomPay | www.freedompay.com

Contents

1.0 Device Management

1.1 Document Purpose

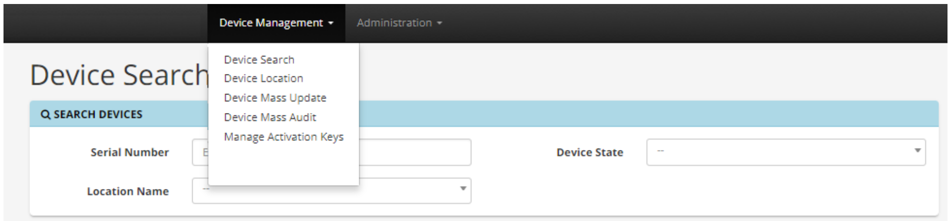
The primary purpose of this document is to describe the usage and management of the activation keys for DMP. Device Management portal will allow clients to self-manage their card scanning P2PE devices by providing options to track device statuses, location, create audits and run reports. As the integrating POS it is partly your responsibility to manage the activation keys per enterprise to ensure the correct keys are used during installation of the POS. There are currently four modules under Device Management that a user can see, Manage Activation Keys is the section of topic.

Device Search	Allows user to manage device information
Device Location	Allows user to manage device location configurations
Device Mass Audit	Allows user to perform mass audits
Manage Activation Keys	Allows user to generate activation key required for FCC installation

2.0 Enterprise Portal

The Merchant can control all of this through the enterprise portal depending on the permission of the users. As a POS provider this will either be managed by the client or merchant directly or it can be managed by the POS provider, depending on the agreement.

All the features mentioned above are accessed through the enterprise portal under the Device Management Tab across the top.



3.0 Manage Activation Keys

To connect the enterprise to the devices to enable the DMP to work as intended, a DMP activation key(s) will be needed. These can be obtained from the enterprise portal under Manage Activation Keys. Keys are currently good for up to 50,000 installs of the FCC. A new key is NOT needed for each install that is being performed. The Activation Key will be used on a fresh install or when *updating the FCC. If the current version of the FCC that is installed supports this. If, during the FCC installation, registering an activation key process was skipped, please refer to the FCC API guide on how to use command line to add the Activation Key for registering this installation of the FCC.

Please Note: The primary purpose of an activation key is to associate the installation to an Enterprise, within FreedomPay's portal and ecosystem. A different key must be used for merchants in different enterprises. You should be very careful and consult with the merchant you are installing your software with, to ensure a key was created from within that merchant's enterprise**. Using the wrong key will result in devices being registered under the wrong enterprise in the portal.**

*NOTE: Adding the Activation Key during an update will only need to be done on the first upgrade. This will not need to be done every time you choose to upgrade the FCC.

3.1 FCC Installation

Before the FCC installer application installs files, machine's registry is checked to see if the install was already performed on the hardware. If it wasn't, user is prompted for an Activation Key.

Once the Activation Key is entered, user clicks 'Next' on the installer application.

The installer application will then make a call to the DMP WebAPI supplying the Activation Key. The DMP WebAPI will then verify/validate the Activation Key, and if good create new account credentials (A GUID to be used as FCCIdentifier and a GUID to represent a password). It will then return the account credentials to the FCC installer application along with a Success response. The FCC installer application will then store the GUIDs in the registry. These registry entries are what the FCC installer application will check for if run again on the same hardware. The credentials will then be used for all future FCC communication with the DMP WebAPI. The accounts created by the DMP WebAPI for the FCC instances will be granted the single Role/Permission of 'FCCInternal'. All DMP WebAPI endpoints to support the FCC communication will require this role/permission. Refer User Management section for details on user roles and permissions

***NOTE: If the network the POS is connected to requires whitelisting for the FCC to communicate to FreeWay, then the DMP URL will also need to be whitelisted.**

Each machine where FCC instance is installed, requests new passwords at a set at a default interval of 24 hours and can be updated as needed. If this time threshold has been passed, the FCC instance will submit a new password along with its normal request. The presence of this additional Password Key will tell the DMP Web API to perform a password update for the given Machine/User Key.

If successful, everything goes on as normally expected and a success response is sent to the FCC instance. If it fails for an invalid Password Key supplied (original Key, not new Key), then it still returns a success response. However, when this condition is encountered (password not valid for Machine Key), the DMP functionality will be disabled until a valid set of credentials are obtained. This does not affect normal card processing.

3.2 Activation Key

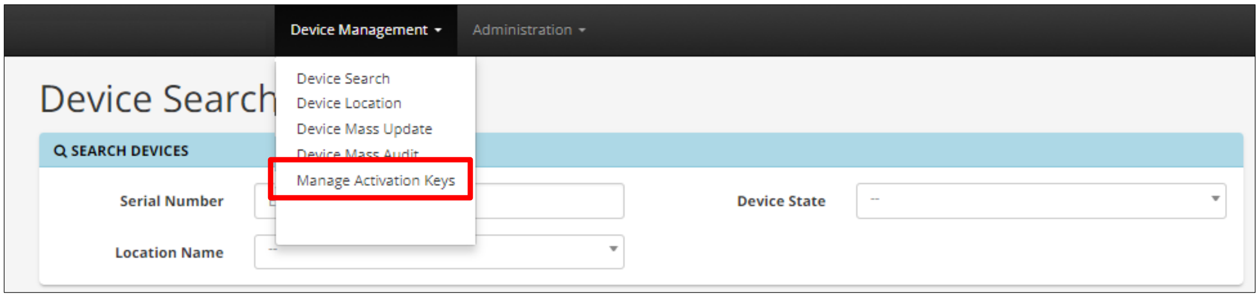
When an Activation Key is created, it will be associated with an Enterprise. When the Activation Key is used to create credentials, those credentials will also be associated with the Enterprise.

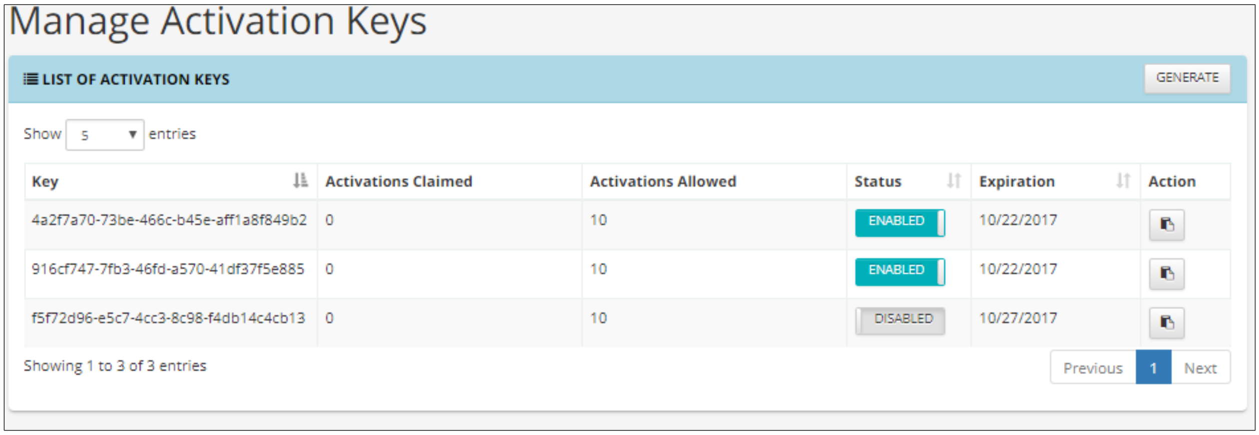
3.3 Authenticating/Authorizing Requests

All calls to the DMP Web API will require the Machine/User Key and the Password Key (the credentials created when an Activation Key is submitted/used). When the DMP Web API calls to the Authentication Server, it will return the associated Enterprise if the authentication/authorization are successful.

3.4 Password Key Change Grace Periods

To prevent a rare condition that can occur when FCC Client and FCC Server instances on the same machine and both may make calls requesting password change, the original Password Key will be valid for a grace period of 60 seconds.





Manage Activation Keys

LIST OF ACTIVATION KEYS

Show 5 entries

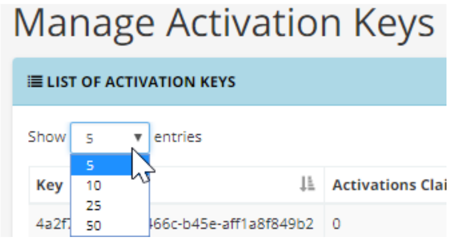
Key	Activations Claimed	Activations Allowed	Status	Expiration	Action
4a2f7a70-73be-466c-b45e-aff1a8f849b2	0	10	ENABLED	10/22/2017	
916cf747-7fb3-46fd-a570-41df37f5e885	0	10	ENABLED	10/22/2017	
f5f72d96-e5c7-4cc3-8c98-f4db14c4cb13	0	10	DISABLED	10/27/2017	

Showing 1 to 3 of 3 entries

This section allows user (with required permissions) to manage activation keys **within a specific enterprise**. User will be able to generate activation keys required for FCC installation. The activation key will have a limited configurable lifetime and number of uses.

Generate — On selecting 'Generate' option, a new activation key is generated

Show Entries — Allows the user to select the number of search results



Manage Activation Keys

LIST OF ACTIVATION KEYS

Show 5 entries

Key — Activation key generated for FCC installation

Activations Claimed — Number of times the activation key is used

Activations Allowed — Maximum number of times the activation times can be used for the given enterprise

Status — Allows user to enable/disable activation key. New activation keys are 'enabled' by default

Expiration — Expiration date of the activation key. This does not affect the related credentials that were created by the key.

Action — Allows use to copy the activation key so that it can be used for FCC installation