Mobile Device Management (MDM)
User Manual V 4.2

1/14/2021

Contents

Overview

The Mobile Device Management solution will allow users to remotely manage and configure their devices in the field. The solution is designed specifically for Educational institutions as well as Enterprises and small businesses. The cloud-based management platform is secured by 2 Factor authentication and industry standard security and protocols.

Login

When you first login you will need to request a One Time Pin (OTP) code. This value will be a 6-digit code sent to the cell phone of the registered owner of the email id. Once you receive the code, enter it along with your password and select LOGIN & CONTINUE.

Reset – Clears all current fields.
Recover password – This will allow you to reset your password. You will need the registered phone to be able to receive the OTP code.

Dashboard

The dashboard page will show you all the current devices loaded under your account.

You can easily search for a specific device by using the search field. Click on the device details to configure the device. You can also search based on group name as well to list all the devices within the group.

Device Version Color Codes:

Orange- A configuration has been sent but the device has not checked in yet.
Green- Device and the server have the same configuration.
No-data: The server has not received any updates from the device at all.

If the device is running MR2 (v891) the device version will only report a config version number. Devices running MR3 (v1311) will show the actual firmware version.

Data Usage is a new field only available for devices running MR3. This is based on a local counter on the device and is not provided by your Carrier or based on your rate plan. Usage limits can be set using MDM for informational purposes. The data usage available is not a real-time counter and will only update when the device is powered on or every 24 hours if on AC power. This is to help IT administrators monitor usage at a general level. If a user goes over their usage limit MDM will not stop internet access and in most cases the carrier will simply throttle down the network speed.

You can also do a quick search by typing in the last 4-digit s of the device IMEI.

Make sure to select LOAD GROUP or LOAD DEVICES before searching.
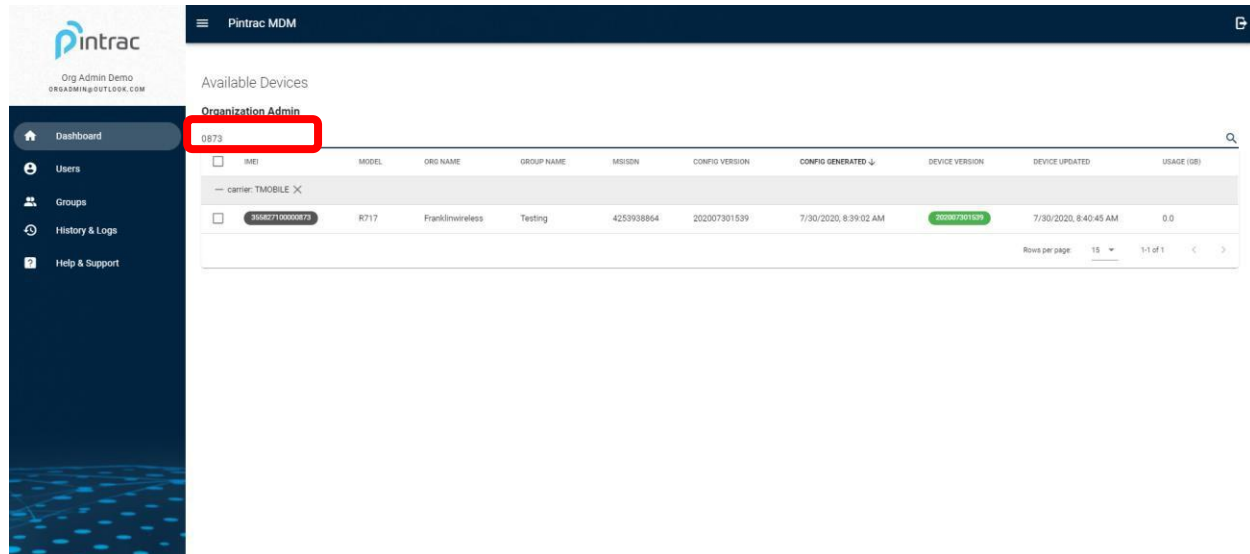
Device Settings

Once you have selected your device you can manage and make configuration setting changes.

General Information

The General Information page allows you to view or change device settings.

- IMEI – This is the hardware ID of your device.
- Product code – The is the model of the device type.
- Select Country Code- This allows to you to select your country.
- Select Carrier – The allows you to set the specific Carrier of your device.
- Organization – This shows the current organization the device is assigned too.
- Phone Number – This is the phone number of the device.
- Color – This is the device color.
- Save Config & Publish:
  This will change to Gray if one of the values in settings is not entered properly.
  Selecting this setting will save the local configuration as well as send a SMS to the device telling it to check-in with the server.
- Save Config – This saves the latest configuration to the local server settings but does not send a message to the device to check in. Instead the next time the device reboots it will retrieve the latest update.

Wireless Settings

The Wireless Settings page allows you to view or change device wireless settings.
- WiFi Name – This is the current SSID or network name of the device.
- WiFi Password – This is the current network WiFi password used to connect to the device.
- WiFi Band – This allows you to set the device band. Supported bands are 2.4GHz & 5GHz.
- Maximum Connections – This is the maximum number of users allowed to connect at one time.
- Display Name & Password – This is to turn on/off the WiFi Name and Password from the display on the device.
- Inactive Time – This is the setting used to control how long the device will be idle before going to sleep.
- SSID Stealth – This is to disable the broadcast SSID so that the network becomes hidden. You need to know the SSID name and password to be able to connect and manually enter it into your connection when this feature is enabled. Do not enable without taking note of your device details.

Mobile Settings

The Mobile Settings page allows you to view or change mobile settings.

- Connection Type – This allows you to choose your connection types. (WiFi Only, WiFi + USB, USB Only) Note: If USB Only is enabled you will not see WiFi information on the device display.
- Factory Reset – This allows you to disable the physical button that performs a factory reset.
- Time of Day Access – This allows you to set specific times of day allowed for the user to access the internet. You can set up to 3 time periods.
- Monthly Reset – This is typically the day your billing cycle restarts. The device default is calculated based on the initial activation date. If a new value is provided the initial date will be overwritten. The device will calculate 1 month based on activation date or manual update. If the activation date or manual date is set to June 18th the device will reset the data counter on July 18th.
- Usage Limit – This is the current data usage limit on your rate plan.
- Usage Unit – This is the unit values (MB, GB, Unlimited)
- Web Interface Access – This allows you to control if a user can access the local Web UI. If this is set to no or disabled a user will receive an error if they try and access the admin URL https://mobile.hotspot. This is where you could change the device settings in the local WEB UI, however if remote management is enabled and the local settings are different than what is in the MDM server, they will be updated to the latest server configuration next time the device checks in.
- Web Interface Password – This is the local Web UI login password used to make local setting changes on the device.
- **Remote Management** – **This is an important setting. If you change this to Off you will no longer be able to manage your device remotely.**
- Data Usage Info Display – This setting allows you to turn on/off the data usage meter on the LCD display.

📞 GENERAL INFORMATION	📶 WIRELESS SETTINGS	🌐 MOBILE SETTINGS	🛡 LAN + FIREWALL

Connection Type	Factory Reset Button	Time of Day Access (On/Off)
WiFi Only ▾	Disable ▾	Off ▾

Data Usage

Monthly Reset (Day of month)	Usage Limit (eg: 500, 30)	Usage Unit (GB/MB/Unlimited)
5 ▾	20	Unlimited ▾

Web Interface Settings

Web Interface Password	Confirm Password	Web Interface Access
•••••••• 🚫👁	•••••••• 🚫👁	Off ▾

Remote Management + Show Usage

Enable Remote Management	Data Usage Info Display
On ▾	WebUI Only ▾

Lan + Firewall Settings

The LAN Firewall settings page allows you to set network related settings.

- DNS Manual Mode – When enabled this allows you to set custom DNS settings. Custom DNS settings can be used to enter a DNS server of a content filtering partner. Once enabled all internet request will be sent to the custom DNS servers for resolution. For example: if you are using WEB Titan as a content filtering partner and you enter the Web Titan DNS servers that have been assigned to you all internet request will be resolved by WEB Titan.

- DNS Address 1 – Custom DNS 1
- DNS Address 2 – Custom DNS 2

☎ GENERAL INFORMATION	🛜 WIRELESS SETTINGS	🌐 MOBILE SETTINGS	🛡 LAN + FIREWALL

DNS Settings

DNS Manual Mode	DNS Address 1	DNS Address 2
On	XXX.XXX.XXX.XXX	XXX.XXX.XXX.XXX

Firewall & Filter Settings

Firewall Switch (IPv4)	Port Blacklist (IPv4)	Port Forwarding (IPv4)
On	Off	Off

Firewall Switch (IPv6)	Port Whitelist (IPv6)	WiFi MAC Filtering
On	Off	Off

- Firewall Switch (IPv4) – Turn the IP v4 firewall on/off. This protects you from external attacks.
- Port Blacklist (IPv4) – Allows you to add port blacklist rules.
- Port forwarding (IPv4) – Allows you to add mapping ports to forward.
- Firewall Switch (IPv6) – Turn the IPv6 firewall on/ff. This protects you from external attacks.
- Port Whitelist (IPv6) – Allows you to add port whitelist rules.
- WiFi MAC Filtering - Allows you to set specific MAC IDs you wish to allow to connect to your device. Meaning you can configure the hotspot to only allow access to the internet from specific devices. Make sure you use a colon ":" between each 2 characters (i.e. 12:34:56:78:90:10)

Users

The Users page will show you all the current users and their roles. You can add and delete users as needed but you cannot edit an existing user.

If you wish to delete a user you can select the user you wish to remove and select the DELETE USER button.

You can also temporarily disable the user if needed. First select the user you want to disable and confirm the change.

Groups

The groups page shows you all of the current groups within an organization. You can add new groups as needed. You currently cannot delete groups.

You can also change groups from the dashboard page. Select the device you want to move to a new group and change groups in the fields below.

History

The History page shows you the latest changes that were made to the server within your organization.

Configuration Management

The MDM platform comes with a feature to be able to apply a specific configuration to multiple devices. For example, if you have a golden device that is setup exactly how you like it and you want to copy that configuration to a set or group of other devices.

1) Setup the device you would like to be the default and select the "Set As Default Config Device" button.

2) Go back to the dashboard and select the devices you would like to copy the configuration too.
3) Scroll to the bottom of the page to select the Bulk configuration details you want to duplicate. This feature is useful if you have many devices that will have the same configuration. Devices that have unique settings should not use this feature.

1) Example: Select save config + generate file. Select the device IMEI that been selected and the default config. **NOTE: Choosing All in this scenario will generate an error**.

2) Next Apply config to selected devices. The configs will be put in a que to propagate. Updates should propagate in a few minutes.

Config Modes:

Save Config – Saved for review (No update sent to device)
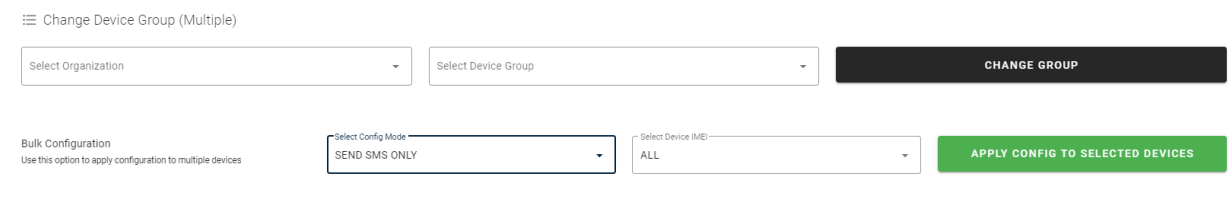
Save Config + generate file – Save config and device will retrieve when it checks in.

Save config and publish – Save config and send SMS to device to check in.

3) Send SMS only – Config file has already been created previously and you want to push to the device to request a check in. The server updates 50 devices every 10 minutes during bulk SMS pushes. In this case you should select ALL.

4) You can also select to use Group Level Actions with the button on the top right of the page. The changes made here will apply to all devices in a specific group. This could be your current group or another group.

FAQ

How often will the device check in with the server?
Every 24 hours or on every power up.

Can I bulk upload devices?
Only Franklin Admins can upload new devices to be registered. Once the devices are uploaded and registered the user can manage on their own.

Can I have more than one user assigned to a single contact phone number?
Yes, however whenever the user logs in they will need the registered phone to receive the OTP code.

Does my data traffic go through the MDM server?
No user or data traffic is sent through the MDM server. The MDM server only maintains and updates device configurations.

Can I add devices which are already deployed to MDM portal?
Yes. You can add the devices even though they are deployed. Update the configuration and push to the devices.

Can I pull the configurations from the devices which are deployed?
No. MDM will help to over-write the configuration which in on the device. MDM will not download configuration from the device.

Does Pintrac or device slowdown data speed or disconnect service if the data usage crosses the set limit?
No. MDM or Device will not be able to disconnect the service or rate plan or slow down data speeds. But, based on your contract with the network operator, they control that option.

Can MDM send alerts if a particular device reaches the data limit?
Within the MDM portal, user can login to sort on data usage to observe the data consumption on every hotspot. Those which have the limit crossed will show in RED. If the data usage is within the limit it will be GREEN. Alerts will not be sent to any users of portal or hotspot.

What does contract Expire mean?
When MDM contract expires, all of those devices which are out of contract will be removed and deleted.

Will user be able to see the devices on MDM portal?
No. User will not see those devices anymore on MDM portal.

Will the device lose its configuration or go back to factory settings?
No. Devices will have the last updated values sent from MDM portal. User will not be able to make changes anymore. Device will not go through factory reset.

What happens to those device which are not updated yet?
No updates will be pushed to those devices which are not updated yet.

Can user bring back those devices to Pintrac portal?
Yes. User can bring back those devices back to Pintrac portal anytime.

Can user pay the remaining amount to stay on Pintrac or renew contract to another term.?
Yes. It should be done before the devices are removed from the system

Demo Video Links

MDM Presentation and Demo
https://drive.google.com/file/d/1k4LqCEO1YXqUd8CI_mT_R6viYRlAweRg/view?usp=sharing

MDM Demo
https://drive.google.com/file/d/1INdg7Zt1oMpT1RX8IDbF2S3sEPSFymQ4/view?usp=sharing

Logging In
https://drive.google.com/file/d/1nJfuQ8dUsOIXz5UAteOaQgrqc0zEAsBx/view?usp=sharing

Dashboard Navigation
https://drive.google.com/file/d/1B0avOUWcIkSPExISPouihGuby-huLiqI/view?usp=sharing

Device Navigation

General Information and Wireless Settings
https://drive.google.com/file/d/1Mj4hRaZa9NkCgFg90gJz6Ado4fqCIO1G/view?usp=sharing

Mobile Settings
https://drive.google.com/file/d/1NR6rMmQahEVNaUpNJMrAZSGw6O-GBz8R/view?usp=sharing

Lan + Firewall
https://drive.google.com/file/d/1G8uLOA6fahl1C6L9RA4UacdO2mgxWfTN/view?usp=sharing

Groups, Group Level Actions, and Users
https://drive.google.com/file/d/16YCLaQkOovHDHJkikz_3q4VCcauwV79z/view?usp=sharing

History & Logs/Help & Support
https://drive.google.com/file/d/1nWHH12f8fX3dnHabuwguIXiEf18aNSfB/view?usp=sharing

Configuration Management

Master Config and Push
https://drive.google.com/file/d/1Wfl73MB04uXOhkqfEAzmtz3ZyTybpAyx/view?usp=sharing

Save Config and Publish
https://drive.google.com/file/d/1eF8hPiB665WpjFBgeFS3TZ6bUwtjULrk/view?usp=sharing