INTACTPHONE

COMMUNITAKE TECHNOLOGIES

INTACTPHONE USER GUIDE

Powered by CommuniTake Technologies

COMMUNITAKE

Contents

1

PRELIMINARIES

WHAT IS COMMUNITAKE INTACTPHONE

CommuniTake IntactPhone allows businesses to protect against cybercrime attacks and advanced eavesdropping techniques while centrally governing their mobile devices covering inventory, security, policies and analytics. IntactPhone can be deployed in two security levels:

1. IntactPhone Device Level: a hardened device locked with custom firmware and enhanced secured mobility services. This solution is deployed on the CommuniTake device or on a commercial Android, as selected by the customer.
2. IntactPhone Application Level: secured mobility services including, secured voice calls and messaging, central administration, and care tools. This solution is deployed on commercial Android and iOS devices.

All deployments contain a central device management system.

CommuniTake IntactPhone Application Level comprises:

- Secure voice calls.
- Secure messaging.
- System dashboard.
- Mobile device inventory management.
- Grouping by organizational hierarchy.
- Password policy enforcement.
- Mobile applications management (Blacklist; Whitelist).
- Internal enterprise app store.
- Granular use restrictions management.
- Browsing control.
- Location and time driven policies.
- Secure file container (SharePoint files view).
- Usage monitoring and reporting.
- Mobile configurations (Exchange ActiveSync; Wi-Fi; VPN).
- Device branding.
- Device launcher.
- Device data protection: locate; lock; alarm; wipe.
- Device data backup and restore (contacts and messages).
- Enterprise wipe for selective business data.
- Antimalware (optional).
- Remote support for mobile devices (optional).

- Self-troubleshooting application (optional).
- Self-service portal for managing data protection.

CommuniTake IntactPhone Device Level comprises the following features:

- All the Application Level capabilities.
- Security-rich use restrictions management.
- App permissions management.
- Internal phonebook management.
- FOTA updates.

CommuniTake IntactPhone is intuitive and easy to manage, allowing system administrator to perform quickly and effectively without the need for extensive training.

ABOUT THIS DOCUMENT

The document refers to the IntactPhone Device Level solution. It presents step-by-step guidelines for using CommuniTake IntactPhone.

This document presents CommuniTake IntactPhone features. Please refer to the CommuniTake Remote Care Manual for guidance on the remote support feature-set.

2

GETTING STARTED FOR ADMINISTRATORS

CommuniTake IntactPhone is mobile security solution of the CommuniTake Mobility solutions suite for businesses.
An account has been defined for your organization. All you need to do is activate the account and begin using it for managing your organization's mobile devices.

SYSTEM COMPONENTS AND BEHAVIOR

There are four main components that facilitate system operation: custom Android-like firmware, on-device client; cloud based server; User Interface (UI). The solution can be deployed without the custom firmware for application level only security – based on the specific deployment.

Two processes occur when an on-device client is properly installed on a device:

1. The on-device client publishes the device's Secured Device Management capabilities to the cloud-based server. These capabilities will vary as custom firmware supports different capabilities in compare with commercial firmware.

2. The system will automatically alter the Graphical User Interface (GUI) to allow each device to show its specific supported features as operational components in the system UI. For this reason, not all operations are available in the UI for some devices.

Based on policies, settings and other actions taken by system users, the UI creates tasks for the device and generates requests for push notifications to be sent to the device. When the push notification reaches the device, the device will connect to the cloud services and it will read and perform the next task in line.

The speed in which a device will perform a task is directly related to the speed in which it receives push notifications. Furthermore, a device with no SIM card or an Android device that is not registered, will not receive any push notifications.

The device client handles requests one at a time. If a device has received a task that requires fulfillment time (Get location, for example), and immediately afterward , the user issues an action like backup request, the action will not start until the first task finishes and the device connects to the server to get the next one in line.

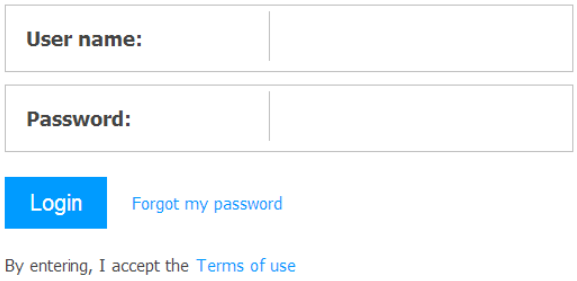
If the client is not properly installed on the device, the device will not publish its actual capabilities to the cloud service. In such a case, the cloud service will not be able to properly perform requests.

IntactPhone is not designed to perform "live", "no latency" changes on multiple devices. Requests are published to the device via push notifications service. Whereas the system usually performs immediately, there are times that it might take a few minutes for requests and their driven changes to propagate to the devices.
The system deployment can vary based on your specific environment. Fulfill the following procedures based on your requirements:

Process	Directive
Activating account	Account activation is mandatory to start using the system.
Manage Customer	Manage the system name, system logo, default prefix and system language
Two step verification	Set two-factor authentication for enhanced security
Settings	Various across-account configurations for defining frameworks for use policies, security controls, integration with external elements, enrollment, and updates.

ACTIVATE YOUR ACCOUNT

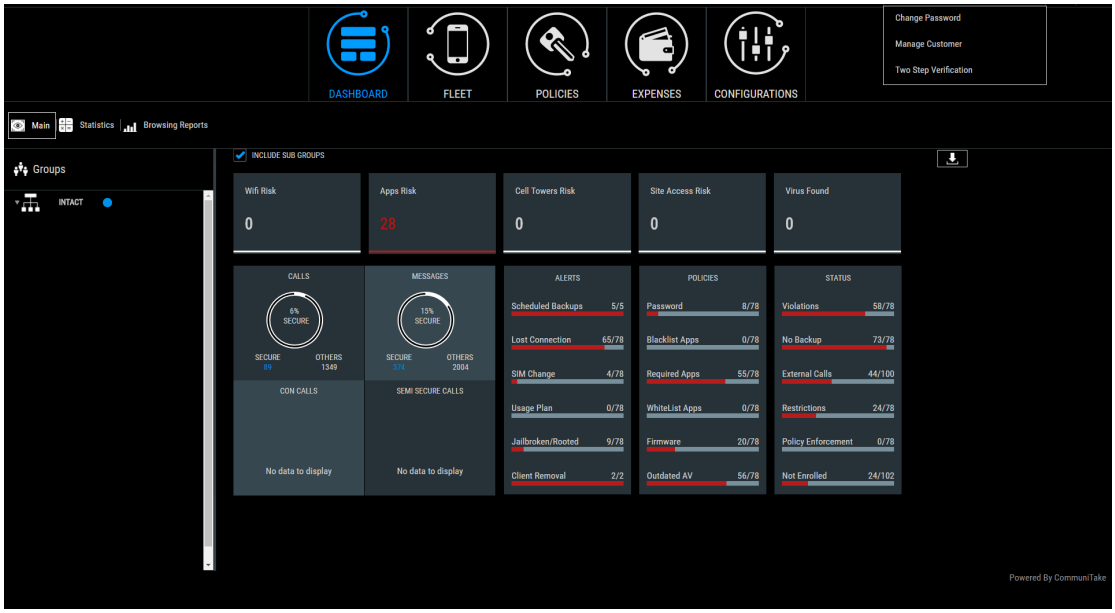
1. Click on the **'Activate Account'** link in the welcome email you have received from us.
2. You will be directed to a login page. Your user name has been defined to be your email address.
3. Define your password to the IntactPhone system.
4. Usernames and passwords in IntactPhone system are case sensitive.
5. Click the '**Login**' button.



Once you are logged-in, you will be directed to the system dashboard.

Important The system allows you to add several business administrators with equal administration rights. Please see the **"System Users**" module under the **"Fleet"** tab.

MANAGE ACCOUNT

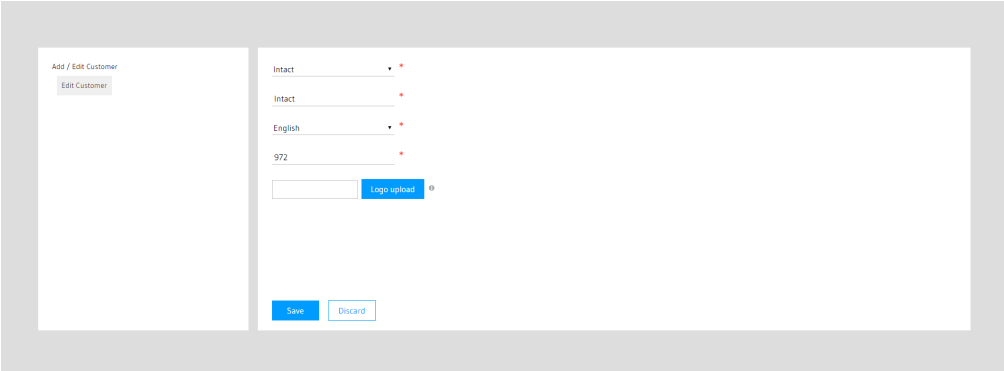


The IntactPhone administration system allows you to self-define the following system parameters:

- System/account name;
- System language;
- System default phone numbers prefix;
- System logo.

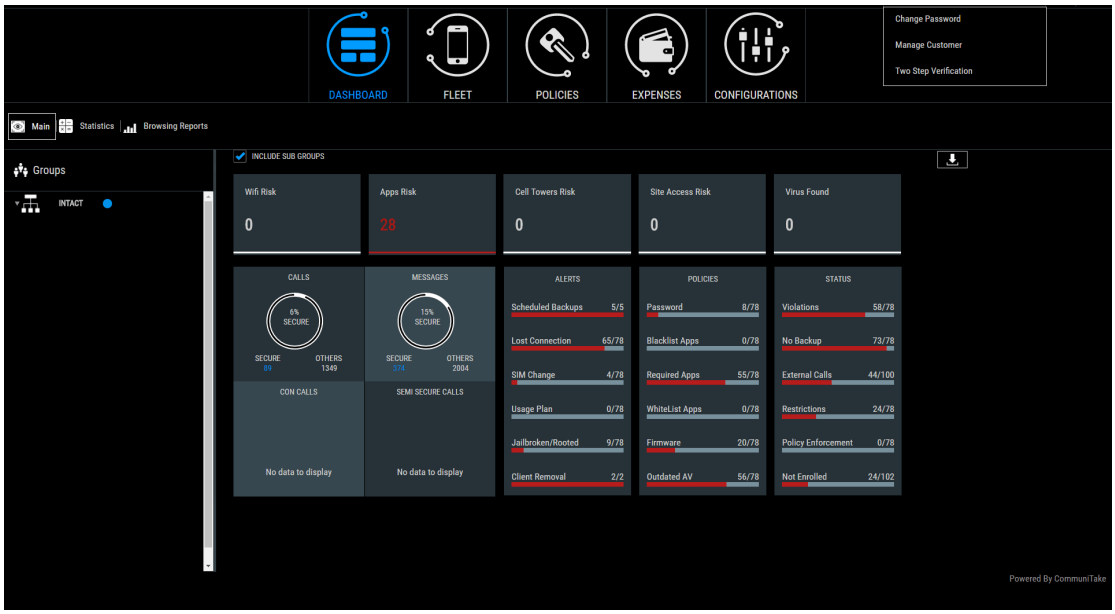
TO MANAGE AN ACCOUNT

1. Log-in to you administration account.
2. Click on the small rectangle button near the administrator name in the upper right corner.
3. Select “Manage Customer”
4. Name your account.
5. Define your system language.
6. Set your system default phone numbers prefix.
7. Upload your desired logo.
8. Click on “Save”.



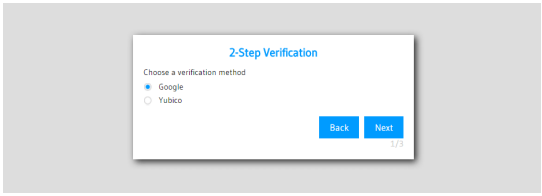
SET TWO STEP VERIFICATION

IntactPhone enables two-factor authentication for the system administrator.



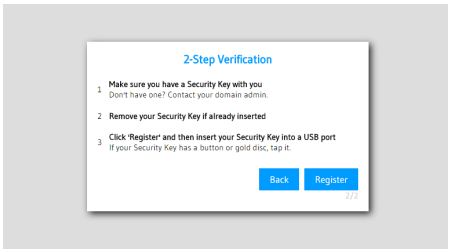
TO ACTIVATE TWO STEP VERIFICATION

1. Log-in to you administration account.
2. Click on the small rectangle button near the administrator name in the upper right corner.
3. Click on "**Two Step Verification**".
4. Turn on "**Two Step Verification**".
5. Select "**Google**" or "**Yubico**" and click on "**Next**". (Note that Yubico is a 3rd party security key. It operates only with a Chrome browser for both authentication set-up and on-going use).

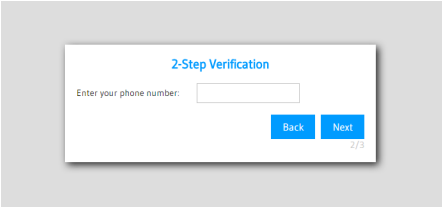


6. Follow the instructions based on your selection.

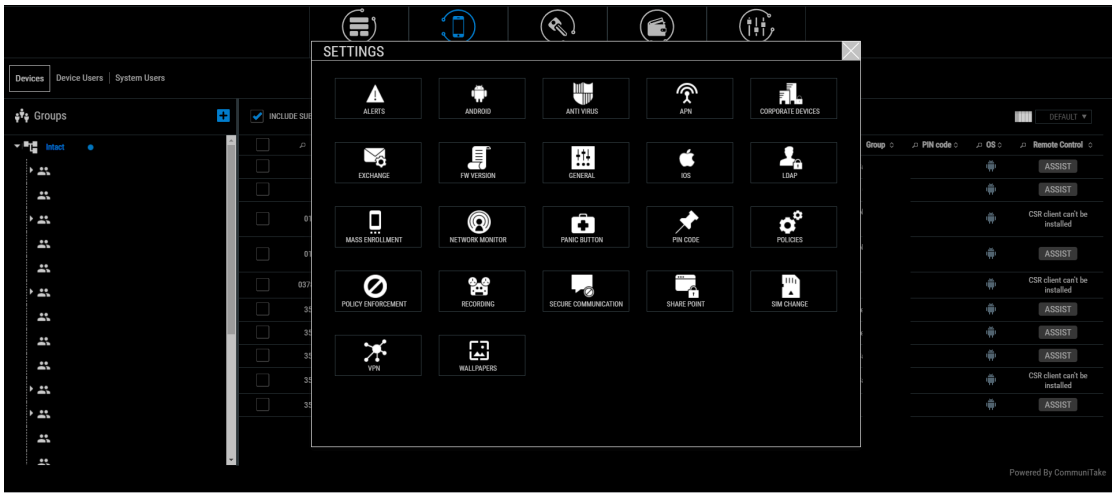
   For "**Yubico"**



For “**Google**”



DEFINE SYSTEM SETTINGS



The “Settings” area allows you to define various generic settings that will apply for all the devices that are defined in the system. Settings allows you to configure the following directives:

Process	Directive
Alerts	The system “**Alerts**” module allows you to send alerts when a policy or use violations occur. We recommend you to set it by your system management requirements.
Android	“**Android**” settings allow you to choose enforcement when the device administrator app is removed from the device (for non-IntactPhone devices)
Antivirus	Both application-level and device level IntactPhone consist of a built-in Antivirus. These settings define the way by which the Antivirus runs in the device and impacts the user experience.
APN	“**APN**” settings allow you to add or remove APN data that will be pushed to the devices under the mass APNs policy.
Corporate Devices	The “**Corporate Devices**” enable you to generate a QR code to enroll new devices as Android Enterprise controlled devices. This a generic Google enrollment process.
Exchange	The “**Exchange**” tab allows you to define the Exchange server through which the device will access emails and contacts and its generic ActiveSync settings. The

	Exchange Settings enables the system user to block/allow device accessing the exchange server. Define these setting to activate these capabilities.
FW version	For custom firmware only IntactPhone: The system consists of custom Android-like firmware. The system support over-the-air firmware updates that are crucial for up-to-date security. These settings define the firmware updates method.
General (General system settings	"**General"** settings define various timeframes by which the system operates. It also establishes the system's data collection operations. These are mandatory for settings.
iOS	"**iOS**" settings allow you to define a certification to enroll in iOS devices.
LDAP	The "**LDAP"** integration enables you to manage device groups by the definitions in the LDAP. This is a mandatory procedure if you intend to unify the IntactPhone groups with your pre-configured LDAP groups.
Mass Enrollment	"**Mass Enrollment**" settings provide you with the ability to enroll many devices in a simple structured process (please see the "Enrolling Devices" section). It simulates Google's Zero-Touch Enrolment process but does not require Google services to run on the device.
Network Monitor	The system enables you to define the time in days for displaying network monitoring KPIs data.
Panic Button	"**Panic Button**" settings allow you to define which actions the device holder will be able to select on panic button activation.
PIN code	The system enables a global enrollment process before allocating Android devices to actual users. It allows you to get a global PIN code for a specific group. Devices that will enter this PIN will be registered to this group. Utilize it only if required for your particular operation.
Policies	**"Policies"** define the inheritance mechanisms between the system groups. These are mandatory settings.
Policy Enforcement	The system enables to define of automated actions on compromised devices. We recommend you set it by your system management requirements to enforce your mobility policies (please see "Policy Violations Driven Enforcement" section).
Recording	The system enables to define recording on instant communications – both voice calls and messages. The customer solely maintains the encryption keys.
Secure Communication	The "**Secure Communication"** settings enable enrolled devices to access a contained environment to perform secure messaging. The settings define two enhancements to exchanging messages: (1) ability to send files as part of the encrypted messages; (2) requirement to key-in additional password before accessing the contained messages area.

Share Point	The "**Share Point"** settings enable enrolled devices to access content maintained in the organizational SharePoint system. Authorized device holders will have view-only access to SharePoint content.
SIM Change	The system enables to define of automated actions on SIM change events. We recommend you set it by your system management requirements to enforce your mobility policies (please see "SIM Change Driven Enforcement").
VPN	"**VPN**" settings provide you with the ability to select the operation method of the system VPN.
Wallpaper	"**Wallpaper**" setting allows you to manage the wallpapers that will be available for home screen definitions.

Click on the "**Setting**" icon to navigate to the "**Settings**" page. Click on the required settings icon in the "**Settings**" page to perform granular configurations.

DEFINE GENERAL SYSTEM SETTINGS ("GENERAL")

GENERAL CONNECTION INTERVALS

The "**General**" settings tab provides you with the flexibility to define the connection intervals between the system server and the device as follows:

Parameter	Description	Default
Device connection interval	The time interval in which the system connects with the device.	30 minutes
Device not seen interval	The amount of time which must pass with no connection to the device after which the system will report the device as "not seen".	48 hours

Device SIM change interval	The amount of time the system will report a device SIM change.	7 days
Device Client Removal Interval (Hours)	The amount of time which must pass with no connection to the device after which the system will report "device client removal". This time window is valid for Android devices. For iOS devices, the indication will be immediate on client removal.	168
Device Periodic Location Interval (Minutes)	The time interval in which the system connects with the device and gets the device location.	

If no new settings are defined, the system will use the default time intervals.

DEFINE PRIVACY RESTRICTIONS ("GENERAL")

Privacy restrictions contain two elements:

"Collect Usage Statistics": Usage is anonymous, but still the system allows the administrator to eliminate the ability to track the general use per device regarding use in general. The "**Collect Usage statistics"** function allows you to collect usage data per device for call minutes, messages and data – local and roaming. This is valuable for usage monitoring and expense control. The system provides you with the option to disable this function as may be required by the organizational privacy policy. The default system state is active usage collection. Uncheck it if you wish to halt the system from collecting usage data.

"Enable BYOD privacy": Once BYOD privacy is activated, a 'BYOD' checkbox is added to the new device attributes in the enrollment process. If a device is marked as BYOD, the administrator cannot view its location, its backups and its applications. The default BYOD setting is inactive.

"Check Battery Level": Once "**Check Battery Level**" is activated, the system will monitor the device's battery level. The system will generate an alert to defined recipients, once the battery level reaches the set threshold.

"**Disable Push**": Once "Disable Push" is activated, on-device clients will be receiving new notifications during the pre-set connection intervals and not in real-time. This feature provides more data cost control capabilities as less data traffic will occur between the device and the system application server.

"**Retrieve Location From BYOD Devices**": The "Retrieve Location From BYOD Devices" allows you to collect device locations by setting time intervals. The system provides you with the flexibility to enable or disable this function as required by the organizational privacy policy.

Important	Once "**Disable Push**" is activated, all instant actions (such as wipe, locate, etc.) will be delayed and will not happen immediately.

Note: Violations driven policies enforcement, Actions on SIM change and action on Device Administrator removal are discussed under the policy section of this document.

PERFORM BUSINESS REGISTRATION FOR IOS DEVICES (“IOS”)

For application level only IntactPhone deployment that consists of iOS devices:

Apple requires a one-time procedural step to allow the IntactPhone Command Center to manage your iOS devices.

1. If you do not already have an Apple ID, you should create one via the following Apple site link: http://appleid.apple.com
2. Click on the **“Settings”** icon located on the upper right corner of the system user interface and click **“iOS”**.
3. Download the Certificate **request** and save the file.
4. Using the above certificate, request a certificate from Apple. Go to the following Apple site link https://identity.apple.com/pushcert/ and log in using your Apple ID.
5. Click **“Create a Certificate”** and agree to the terms of use.
6. Upload your certificate request (which you have saved in step 4). After a few seconds, your certificate will be ready for download. Download and save the certificate.
7. Click “**Settings”** again on the system user interface. Upload the certificate that you have downloaded from Apple.
8. You are now ready to add iOS devices to the IntactPhone system.

FULFILL LDAP INTEGRATION (“LDAP)

Devices are managed in the system via groups. Devices are allocated to logical groups with similar use policies. These groups are built and populated manually or via integration with an LDAP that already contains groups and devices. The **“LDAP”** tab allows you to create LDAP integration for defining and populating the system's devices groups via the organizational LDAP.

Accessing the **“LDAP”** integration interface is done through the system **“Setting”** located on the upper right corner of the screen.

The system enables LDAP integration for performing the following:

1. Populating the system with groups and users from the LDAP
2. Defining which groups should be synchronized
3. On-demand synchronization of groups and /or users

Integrating with your organizational LDAP will facilitate rapid creation of the organizational groups in the IntactPhone Command Center system.

To complete LDAP integration:

1. Set the following definitions:
    a. Username – This user must have, at minimum, LDAP read permissions.
    b. Password.
    c. Secured LDAP (Checked / Unchecked).
    d. Secured LDAP parameters:
        i. Upload the certificate.
        ii. Certificate password.
        iii. Certificate type.
    e. Primary Host Port (mandatory parameter).
    f. Secondary Host Port.
    g. Root Context.
    h. Users Organizational Unit (mandatory parameter).
    i. Groups Organizational Unit (mandatory parameter).
    j. Domain Alias.
    k. LDAP Field Mapping
        i. User ID.
        ii. User Display Name.
        iii. User Email.
        iv. Group ID.

v. Group Display Name.
vi. User Object Class.
vii. Group Object Class.

l. Check the "**Enabled Periodic Sync"** for periodic updates.
m. Define the "**Periodic Sync Interval**" in hours.
n. Define if you want the device to be deleted from the system when its owner is deleted from the LDAP. Otherwise, the device will remain attached to the group.

2. Once defined, click on **"Save Configurations**".
3. Click "**Choose Groups to import**" to select which groups to import.
    a. You will be presented with the groups that are currently available for import from the LDAP (the default is to import all).
    b. Select the groups that you wish to import into the system.
    Please note that if a child group is selected, its parent group will also be selected.
    c. Click **"Import"** to initiate the import process.
    The process will import the selected groups and all their valid users. A valid user is a user that has an email address.
    d. The status of the import process is displayed in the top right corner.
    During the import process, all the LDAP groups are locked and cannot be accessed.
4. Click on "**Import Users Only"**, if you wish to refresh the users in the groups that were imported.
The status of the import process is displayed in the top right corner. During the import process, all LDAP groups are locked and cannot be accessed
5. Click on **"Test Connection**", if you wish to verify proper connection without an actual population of the system groups.

The end result of this process is a group structure and their allocated users present in the system. All you have to do is add the device to the user (MSISDN or Email), define the display name for the device in the system and define the self-service access.

Important

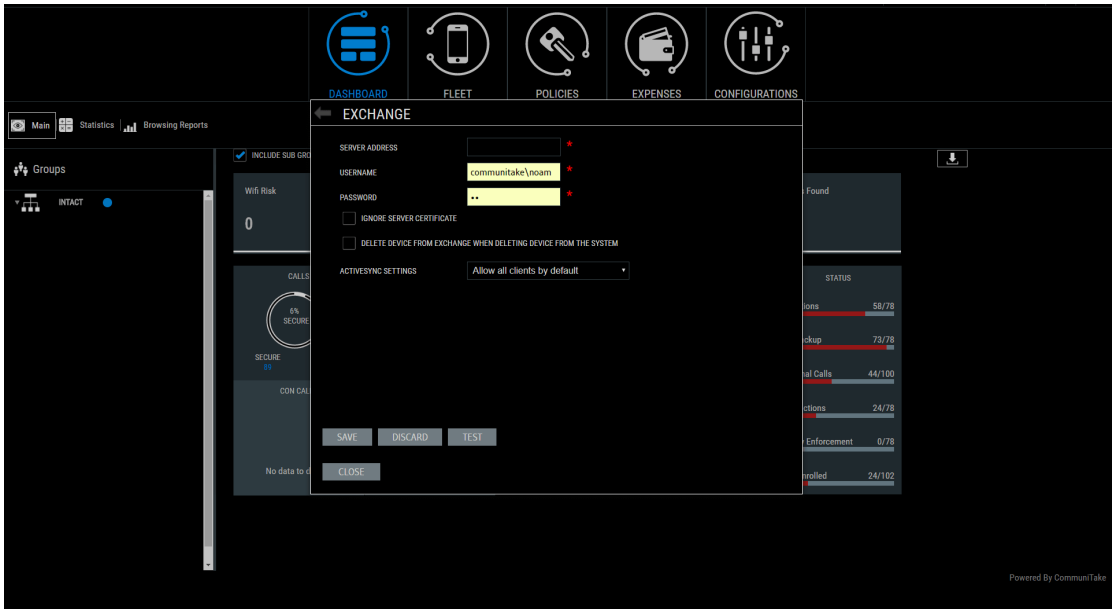
- If a user is removed from the LDAP, the user will be also removed from the system along with all his related devices.
- If a group is deleted from the LDAP, all the users in that group that were not moved to another group which was imported to the system, will be deleted along with their related devices.
- If a group is deleted from the LDAP, all the devices that are directly attached to the group will be deleted.
- When a user is moved between different LDAP groups, his device remains in the original group.
- When a group is moved in the LDAP to a different location, all the users and the devices that are attached to this group will also move. It means that the group's policy could potentially change if a policy is "inherited".
- In order to perform an import from the LDAP, the IntactPhone Command Center system servers must be able to access the LDAP servers. Once the import is

completed, you can close the access connection until next time it is needed for an import or sync.

- A device can only be attached to a user that is defined in the LDAP group.

SET EXCHANGE CONFIGURATION ("EXCHANGE")

The **"Exchange"** tab allows you to define the Exchange server through which the device will access emails and contacts and its generic ActiveSync settings. Accessing the **"Exchange"** configuration interface is done through the system **"Setting"** located on the upper right corner of the screen.



The Exchange Settings enables the system user to block / allow devices accessing the exchange server;
Use cases for connecting the exchange server with the IntactPhone system:

1. Only devices attached to the IntactPhone system can access the Exchange server.
2. Blocking a device from accessing the Exchange server if it has outstanding policy violations.

The IntactPhone system utilizes the remote configuration capabilities of the Exchange server to manage different settings directly on the Exchange.

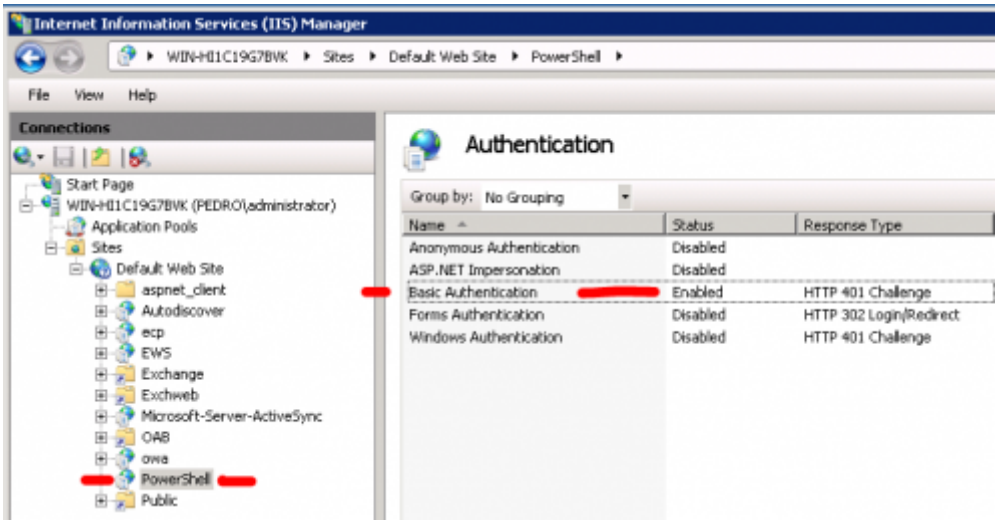
PRECONDITIONS FOR ACCESSING THE EXCHANGE SERVER USER

- The Exchange connection uses port 443.
- Currently, only Exchange 2010 is supported.
- Exchange integration requires a username and password for accessing the Exchange server.
- The user must be a part of a Role Group that has Mail Recipient Creation rights. To perform this, make the run as user that is part of the **"Recipient Management"** Role Group. You can achieve it by going to **"Exchange Management Console"** → **"Microsoft Exchange"** → **"Microsoft Exchange On-Premises"** → "**Toolbox"** → "**Role Based Access Control (RBAC) User Editor**".
- The user name must have Remote PowerShell rights. Gain these rights by going to the **"Exchange Management Shell'** and running the following cmdlet:

Set-User UserNameHere-RemotePowerShellEnabled:$true

- The Exchange server must be configured to allow remote management.

- The Exchange 2010 server must allow basic authentication. To allow Basic Authentication perform the following: **"IIS Manager"** → **"Sites"** → **"Default Website"** → "**Powershell**". Select the **"Authentication"** feature and enable **"Basic Authentication"**. If **"Basic Authentication"** is not an option on the **"Authentication"** feature page, you should install it: navigate to the **"Server Manager"**; select the **"Web Server"** role; select **"Add Role Services"**, under the **"Security"** node in the tree view; select **"Basic Authentication"**.



TO PERFORM EXCHANGE CONFIGURATION

1. Define the following parameters:
    a. Server Address (mandatory parameter).
    b. Username (mandatory parameter).
    c. Password (mandatory parameter).
    d. Ignore server certificate (checked / unchecked).
    e. Delete device from exchange when deleting device from the system (checked / unchecked).
    f. ActiveSync Settings (select between **"Allow all clients by default"** or **"Block all clients by default"**).
2. Click **"Save"** to perform the configuration.
3. Click **"Test"** for verifying the validity of your settings without activating it.

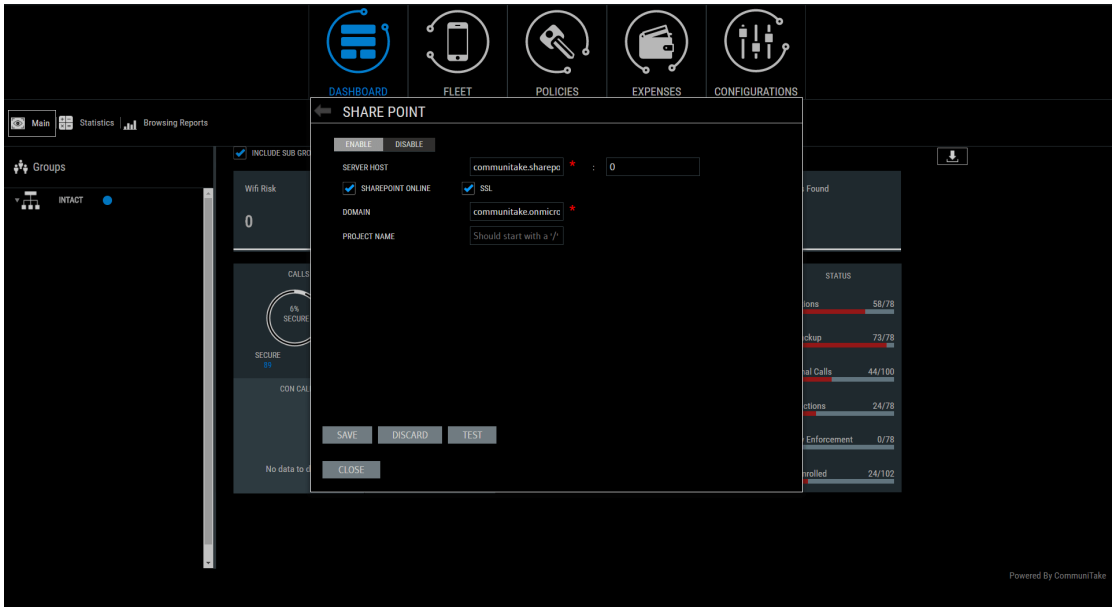
Important

- In order to manage the Exchange settings, the IntactPhone system servers must be able to access your Exchange servers.
- Currently, if you have configured the Exchange to block all clients, when you add a new device to the IntactPhone system, it is not automatically allowed in the Exchange. You must click the device in the IntactPhone system, go to the Security tab and move the device to Allow.
- All the settings that are done by the IntactPhone system can be done directly on the Exchange server itself; for example, you can change the configuration in the Exchange

from “Block all clients” to “Allow all clients”. The next time you log into the system and check the Exchange settings page, you will see that the settings have changed.

SET ACCESS TO THE SHAREPOINT CONTAINER (“SHAREPOINT”)

The SharePoint Container enables enrolled devices to access content that is maintained in the organizational SharePoint system. Authorized device holders will have a view-only access to SharePoint content.



Perform the following steps to set Secure File Container access:

1. Click on "**Settings**".
2. Click on "**Share Point**".
3. Check the "**Enable SharePoint**" checkbox.
4. Define the server host IP address (mandatory).
5. Check the "**SSL**" checkbox to define encrypted connectivity.
6. Fill in the Domain name (mandatory).
7. Fill in the Project name (optional).
8. Click on "**Test**" to test the connectivity.
    a. Enter valid SharePoint credentials and click “**Test**”.
    b. Test results will be displayed when the test completes.
9. Click on "**Save**".

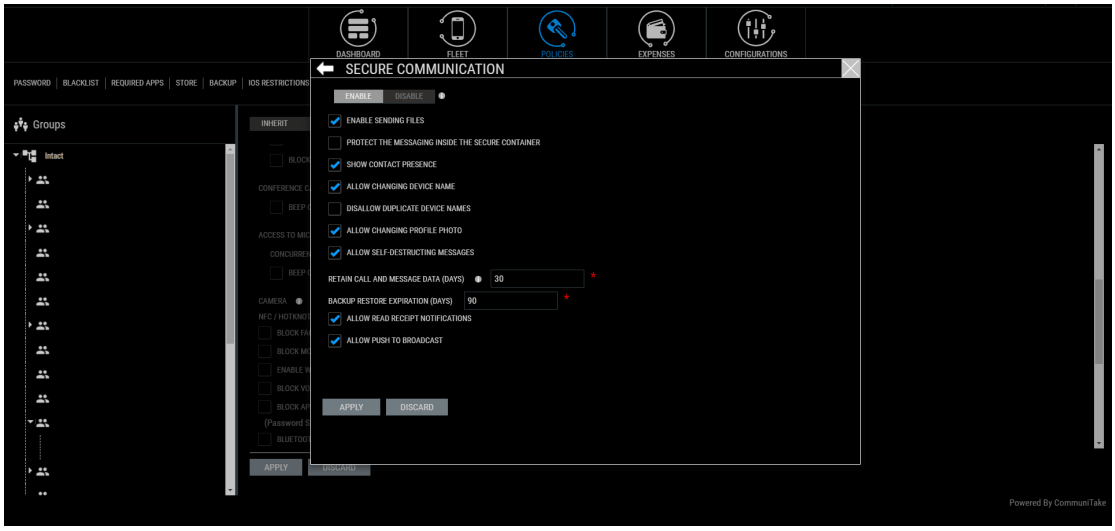
The SharePoint Container operates according to the following guidelines:

- Integrates with SharePoint.
- Enables accessing the SharePoint content via the IntactPhone on-device client.
- Allows access to users which have SharePoint access.
- Automatically uses the SharePoint's permission scheme.
- Uses the device holders SharePoint credentials in order to access the content.

- Enables content browsing by the SharePoint directory structure.
- Provides file status view - not downloaded; downloaded; newer version available.
- Enables the device holder to perform on-demand download of files to the device by the following restrictions:
    - Stores encrypted content.
    - Device encryption by using a user provided password which is also used to access the container.
    - Displays content only inside the client.
    - Prevents cut / copy of document content.
- Provides control to block / allow device to access the files.
- Allows deletion of the on-device files when the device is deleted from system or as part of the enterprise wipe.

SET SECURE COMMUNICATIONS ("SECURE COMMUNICATION")

Secure Communication is activated for the account as part of the deployment process. The Secure Communication module provides users with a safe environment in which they can exchange safe voice calls and textual messages. The system allows you to define granular use elements.



Perform the following steps to set Secure Messaging access:

1. Click on "**Settings**".
2. Click on "**Secure Communication** ".
3. Select "**Enable**".
4. Check "**Enable sending files**". This enables the device holder to send PDF and image files within the secure messages to enrolled devices, and share any file with external contacts.
5. Check **"Protect the messaging inside the secure container".** This enables the device holder to exchange messages with enrolled devices only after keying-in a password to the contained environment.

6. Check “**Show contact presence**”. This enables the device holder to define his presence status for other system users.
7. Check “**Allow changing device name**”. This allows the device user to define the name by which he will be displayed in the system.
8. Check “**Disallow duplicate device names**”. This allows you to allow only different names across the account. The device holder will not be able to set a device name that already exists in the account.
9. Check “**Allow changing profile photo**”. This enables the device holder to select the image by which he will be displayed to other users in the system.
10. Check “**Allow self-destruct messages**”. This enables the device holder to define a self-destructing time spanning from 5 seconds to one week after which the sent message will be removed from the device.
11. Set the number of days in “**Retain call and message data (days)**”. This will define the number of days for which the system will present users calls and messages data. The default is set for 30 days.
12. Set the number of days in “**Backup expiration time**”. This will define the number of days for which the system performs backup and restoration of calls and messages. The restoration expiration time is only applicable to attached files and voice messages. Text messages have no expiration time.
13. Check “**Allow read receipt notifications**”. This enables the device holder to ask for read receipt notifications.
14. Check “**Allow push to broadcast**”. This enables the device holder to perform push- to- broadcast, and vocally burst to system users’ phones.
15. Click on "**Save**".

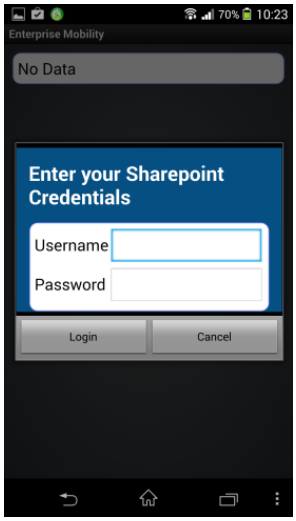
Important The system can send an email alert for brute force attempts on the container password. The system blocks the container after ten bad password attempts.

Important Self-destruct messages: the message is automatically removed on the recipient side from the opening time by the set time frame, and also on the sender side from the sending time by the set time frame.

GRANT DEVICE ACCESS TO THE CONTAINER

1. Check the "**Secure Container**" checkbox when adding a device to the IntactPhone. (You can define access after device enrollment via the "**Edit**" function in the devices table).
2. The device holder launches the IntactPhone application on his device.
3. The device holder is prompted to select a password for the container.

4. The device holder is prompted to enter his SharePoint credentials.



5. The application checks the credentials via the server and the SharePoint credentials are stored encrypted.

REMOVE DEVICE ACCESS TO THE SECURE CONTAINER

1. Disable the device's Secure Container access via the "**Edit**" function or by selecting the device and clicking "**Block**" on the action bar.
2. Remove Secure Container access message is sent to the device.
3. Once received, the device performs the following actions:
    a. Deletes all on-device stored files.
    b. Erases the SharePoint's stored credentials.
    c. Erases the password.
    d. Removes the "**Container**" button from the on-device application UI.

SET MOBILITY POLICIES INHERITANCE ("POLICIES")

The system allows you to define the default inheritance mechanism across policies.

The inheritance settings alternatives are as follows:

- **Password Policy**: **inherit**; disable.
- **Blacklist**: enable; **inherit**; adopt.
- **Whitelist**: enable; **inherit**; adopt.
- **Recommended** (apps): enable; **inherit**; adopt.
- **Backup Policy**: **inherit**; disable.
- **iOS Restrictions**: **inherit**; disable.
- **Android Restrictions**: **inherit**; disable.
- **Web Control**: enable; **inherit**; adopt; disable.
- **File Distribution**: enable; **inherit**; adopt.
- **Home screen**: **inherit**; disable.
- **Launcher**: **inherit**; disable.
- **Secure Contacts**: **inherit**; enable.
- **Applications Permissions**: **inherit**; disable.

The default inheritance is set for **"inherit"**.

SET DEFAULT INHERITANCE FOR NEW GROUPS

1. Click on the **"Settings"** icon.
2. Click on the **"Policies"** icon.
3. Mark the required inheritance for the target policy.
4. Click on **"Apply"**.

SET SYSTEM ALERTS (“ALERTS”)

The system alerts module allows the system administrator to send alerts when policy or use violations occur.

The drive for this alert will be to inform system administrators and managers of violations for increased awareness and as acceleration for resolution. The system enables you to granularly set alerts so that recipients will receive various alerts for various events with different alerts timing.

Alerts can be set for the following parameters:

Required Apps; Blacklist; Exclusive Apps; Password Policy; Not Enrolled; Client Removal; Roaming; Usage Plan; Violation; Sim Changed; Lost Connection; Rooted; Battery Level; SW Monitoring; Wi-Fi Monitoring; Cellular; Tower Monitoring; FW Version; Virus Detection; Container Security.

SEND SYSTEM ALERTS

1. Click on the “**Settings”** icon at the upper right of the application screen.
2. Click on “**Alerts”**.
3. Click on the plus icon to add and define an alert.
4. Click on the plus icon next to “**Send alerts for”** to define the initiation for the alert. Alerts causes can be the following violations: Required Apps

Blacklist; Exclusive Apps; Password Policy; Not Enrolled; Client Removal; Roaming; Usage Plan Violation; Sim Changed; Lost Connection; Rooted; Battery Level; SW Monitoring; Wi-Fi Monitoring; Cellular Tower Monitoring; FW Version; Virus Detection; Container Security; Site Browsing

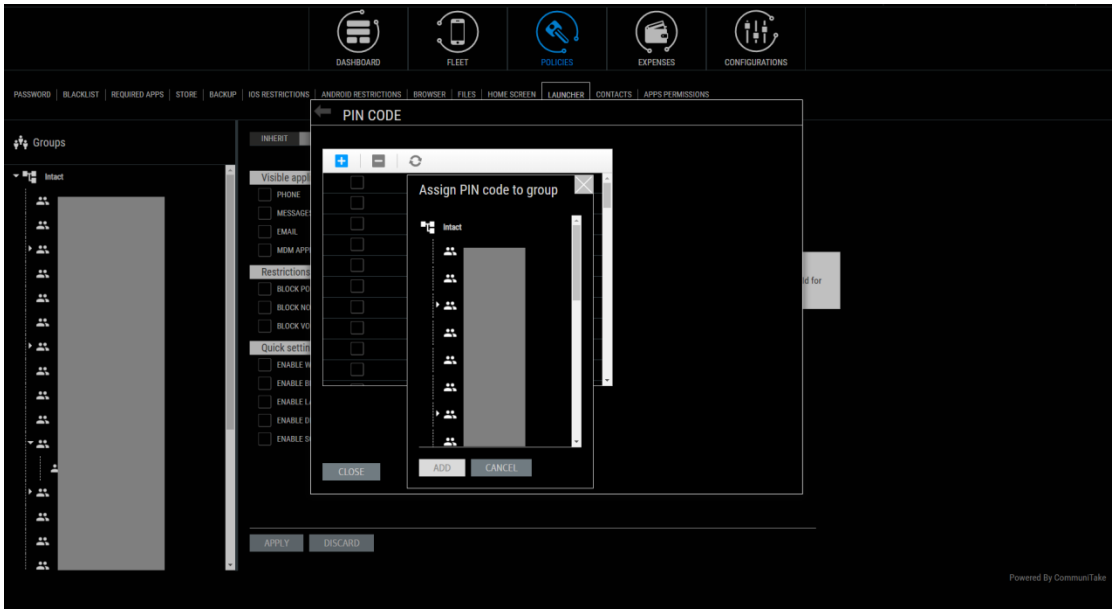
5. Click on the **OK** icon to approve the selection.
6. An alert will be sent as soon as possible, once defined and activated.
7. Check the following activation options are required:
    a. **“Send alert even if resolved”.**
    b. **“Then send an alert every <number> Hours”** (can be every 15 minutes; every 30 minutes; every one hour; every six hours; every twelve hours; and once a day).

c. **“And stop after <number> Day”** (can be every day; every two days; every three days; once a week).

8. Key-in the recipient’s email address in the “**Send To”** data field. Click on the plus icon near this field for adding more recipients.
9. Click on “**Apply**” to activate the alerts mechanism.

PERFORM GLOBAL ENROLLMENT PROCESS (“PIN CODE”)

The system enables a global enrollment process prior to allocating Android devices to actual users.
It allows administrators to get a global PIN code for a specific group. Devices which will enter this PIN will be registered to this group.



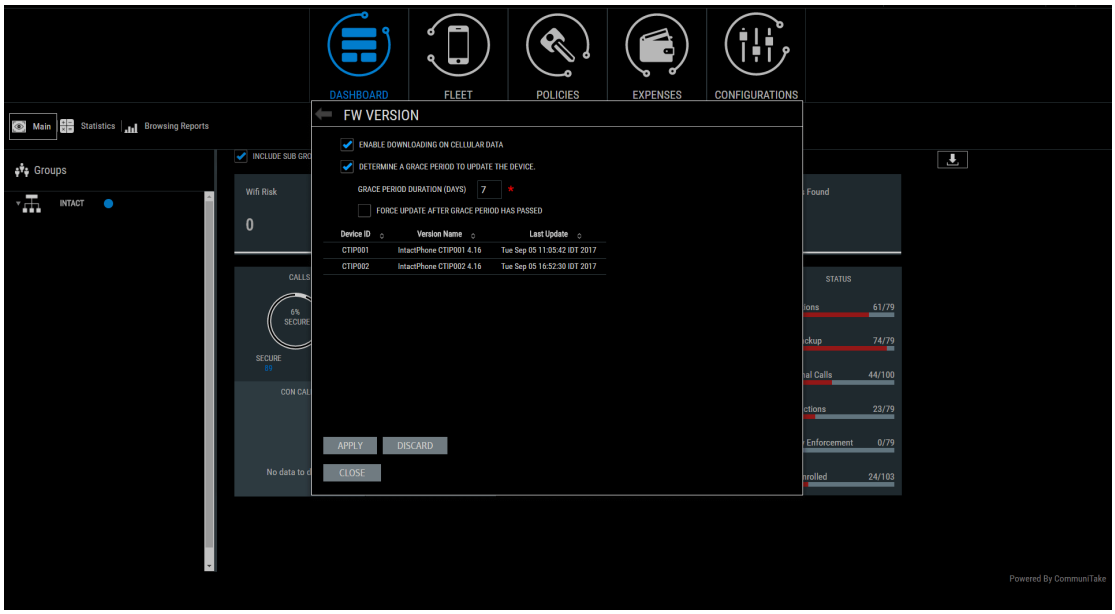
Perform the following steps to set a global enrollment process:

1. Click on "**Settings**".
2. Click on the "**PIN code**".
3. Click on the Add Group icon. 
4. Select the group / groups to which you wish to add devices.
5. Once added, the system will automatically assign a PIN code to this group.
6. Any device which enters this PIN code will be registered to this group.

Important The global enrollment process is only applicable to Android devices.

SET FIRMWARE VERSION ("FW VERSION")

The IntactPhone solution provides frequent over-the-air security updates to add improved functionality, to better address new cybercrime threats, and to deploy the on-going security improvements. The system enables you to define the parameters by which the IntactOS firmware over-the-air deployment will be fulfilled.



Perform the following steps to manage IntactOS firmware over-the-air updates:

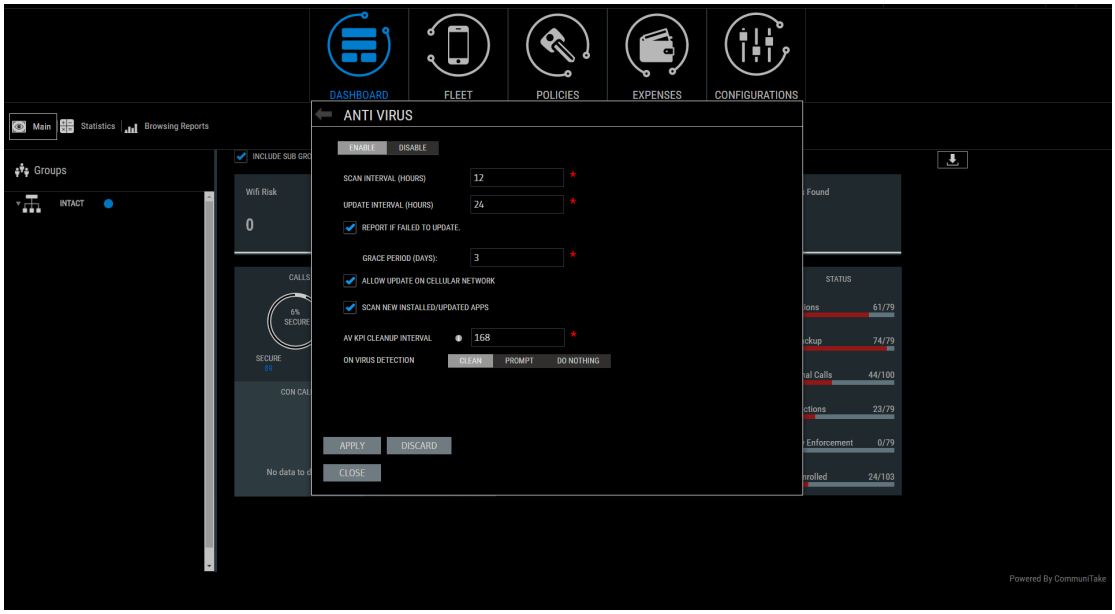
1. Click on the "**Settings"** icon at the upper right of the application screen.
2. Click on "**FW Version"**.
3. Check "Enable downloading on cellular data" if you wish to allow antivirus file updates via both Wi-Fi network and cellular network.
4. Determine a grace period to update the device. The grace period duration is set in days.
5. Check "Force update after grace period has passed", if you wish to enforce the new IntactOS deployment after the grace period.
6. Click on "**Apply**".

Important The firmware over-the-air update process is only applicable to IntactPhone devices that run the IntactOS firmware.

Some over-the-air updates are large. You should consider whether to enable downloading them over a cellular network.

SET ANTIVIRUS (“ANTIVIRUS”)

The IntactPhone solution contains an integrated antivirus application. The antivirus application is embedded in the Android on-device IntactPhone client.



Perform the following steps to manage the antivirus application behavior

1. Click on the “**Settings”** icon at the upper right of the application screen.
2. Click on “**Antivirus”**.
3. Check to “**Enable**” or “**Disable**” the antivirus scan process.
4. Set the “**Scan interval**” in hours. The default scan interval is set to 12 hours.
5. Set the “**Update interval**” in hours. The “**Update interval**” refers to the antivirus file update re new threats. The default update interval is set to 24 hours.
6. Check “**Report if failed to update**” to report on antivirus file update failures. Set the “**Grace period**” in days. This time period stands for the timeframe in which the system will still ignore failed updates.
7. Check “**Allow update on cellular network**” if you wish to allow antivirus file updates via both Wi-Fi network and cellular network. The default is set to only Wi-Fi network, and an antivirus file update will occur only once the device has access to a Wi-Fi network.
8. Check “**Scan new installed/updated apps**” to define a real-time scan on every installation or update of on-device mobile application.
9. Set the “**AV KPI cleanup interval**” in hours. This feature defines the time in which the system will clean up the indications on found virus, as presented in the system dashboard.
10. Define the “**Antivirus KPI cleanup interval**” to set the period in days after which a KPI on malware detections will be removed. The default period is set to 168 hours.
11. Define “**On virus detection**” for what will happen once a virus is tracked. Select one of the following options: “**Uninstall app**” for an immediate uninstallation once the virus is detected; or “**Prompt**” to only alert on the virus detection; or “**Do nothing**”.

DEFINE APNS (“APN”)

The Intact Command and Control system enables you to define the available APN addresses to device holders.

Perform the following steps to define APNs:

1. Click on the “**Settings”** icon at the upper right of the application screen.
2. Click on “**APN”**.
3. Click the Add icon. 
4. Define the mandatory APN data fields: NAME; APN; MCC; MNC; APN TYPE.
5. Define the optional data fields by your preference.
6. Click “**Add**”.

The added APN addresses will be available for selection by the system administrators when setting APN policy.

DEFINE ACTIONS ON DEVICE ADMINISTRATOR REMOVAL (“ANDROID”)

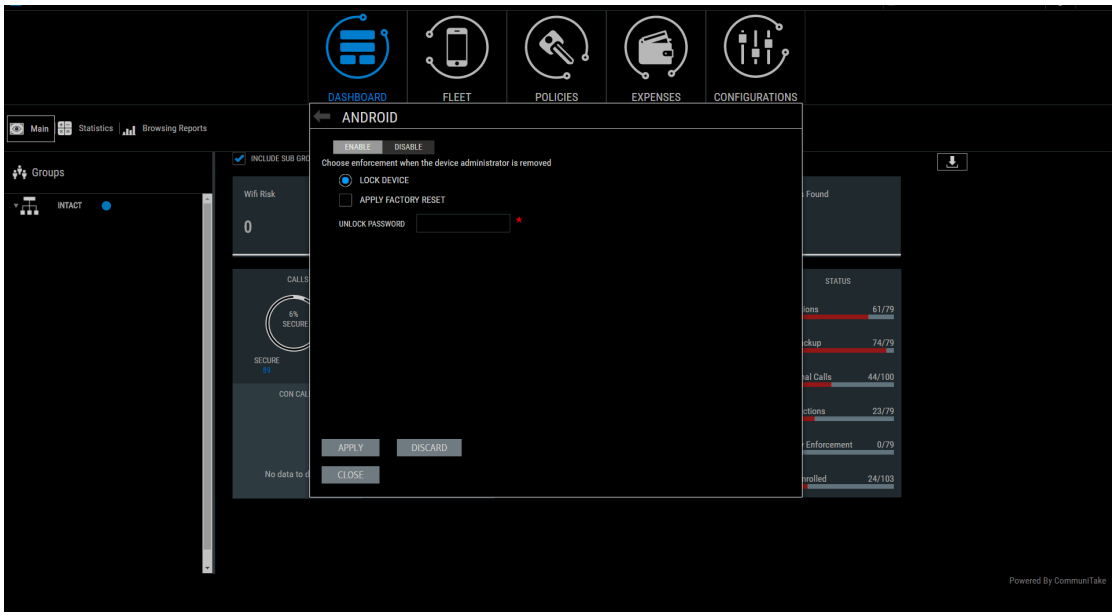
The IntactPhone solution provides use limitations when the administration client is removed from the device.

Note: client removal is possible only for IntactPhone application level solution. For IntactPhone devices that use the IntactOS, the administration client is fused in the operating system.

Perform the following steps to activate use limitations on client removal:

7. Click on the “**Settings”** icon at the upper right of the application screen.
8. Click on “**Android”**.
9. Check to “**Enable**” or “**Disable**” the client removal actions.
10. Check “**Lock device**” if you wish to activate this sanction on client removal.
11. Check “**Factory reset**” if you wish to activate this sanction on client removal.
12. Key-in the unlock password (mandatory).

13. Click on “**Apply**”.

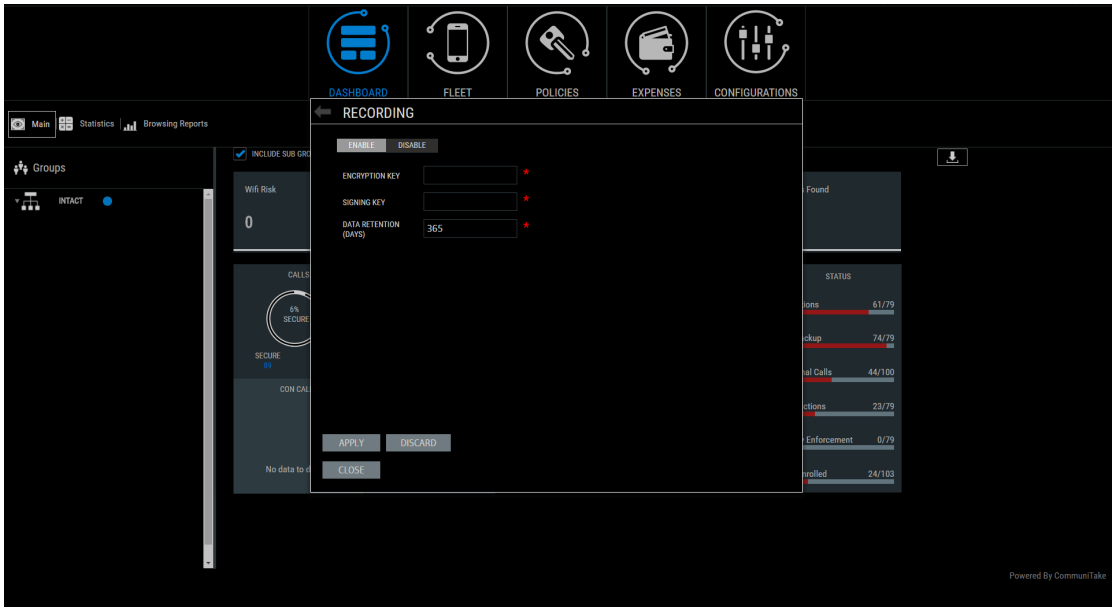


SET RECORDINGS (“RECORDING”)

INTRODUCTION

The IntactPhone enables you to store all the IntactPhone communications in an encrypted state. Recordings are aimed at regulated organizations that might be required to provide their communications content to governmental agencies. Encrypted recordings require a specific deployment request and a dedicated set-up. The communications encryption was designed by the following directives:

- Only the private keys holder can decrypt the communications files.
- No external user (including CommuniTake) is able to decrypt the communications files.
- CommuniTake does not have access to the encryption private keys.
- Every communications element (message, file, call recording) is encrypted using AES 256bit with its own random 256bit key.
- The random 256bit key is encrypted using the public key. As such, only the private keys holder can decrypt the actual communications.
- The communications element is sent from the device to the server fully encrypted.
- CommuniTake can disclose the encrypted communications files under a legal court order; however it cannot decrypt the files.



Perform the following steps to activate the communications recording:

1. Click on the "**Settings"** icon at the upper right of the application screen.
2. Click on "**Recording"**.
3. Key-in an "**Encryption Key**" (mandatory).
4. Key-in a "**Signing Key**" (mandatory).
5. Define the "**Data Retention**" period (days)
6. Click on "**Apply**".

Note The following definitions require password.

Recordings related actions: Enable; Disable; Data retention changes.

The recordings feature will be shown only if this feature was activated for your account.

HOW TO COMPILE THE CODE

The following section illustrates how to compile the encryption code:

1. Make sure you have Java and Eclipse installed on your machine.
1. Open the provided project in Eclipse and export it or use it directly from Eclipse.
    a. Alternatively, copy the code to your own project and use it.

HOW TO GENERATE AND USE THE ENCRYPTION KEYS

The following section illustrates how to generate and use the encryption keys:

1. Run the IntactEncryption program with the "-generate" modifier

   "*java -jar intactenc.jar -generate*"
2. The output:
    a. Private and public keys for the encryption key.
    b. Private and public keys for the signing key.

3. Conduct this process only once.
4. Upload the public keys to the system under "**Settings"** → "**Recording**".
5. Store the private keys in a secure manner.
6. Storing of the communications will only commence once the public keys are uploaded to the system.

HOW TO RECOVER FROM LOST PRIVATE KEYS SCENARIO

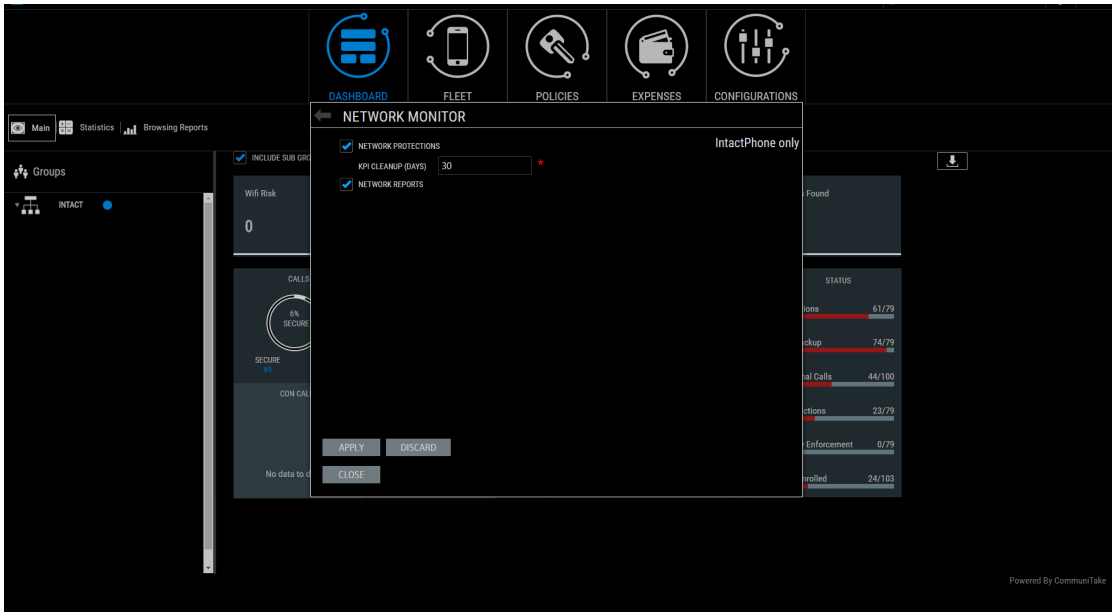
If you lose your private keys, act by the following guidelines:

1. There is no way to get the lost private keys back.
2. There is no way to decrypt the stored communications without the lost private keys.
    a. You must generate and upload a new pair of keys - you will be able to decrypt the communications which accrue from this time point onward.

HOW TO DECRYPT A STORED COMMUNICATION

1. Find the communications you wish to decrypt in the "**Fleet"** → "**Recording"** table.
2. Click on the record details
    a. Download the encrypted file to your machine.
    b. Copy the encryption key.
3. Run the IntactEncryption program with the following command line:
   "*java –jar intactenc.jar –rsaEncPriv { your encryption private key } –key {the key used to encrypt the file} –inFile { full path to the file downloaded from the system } –outFile { full path to where you want to store the decrypted file }*"
4. To easily open the file on your machine, based on the communications type, choose the following outFile suffix:
    a. Message – ".txt"
    b. Image – ".jpg"
    c. Movie – ".mov"
    d. Call – ".mp3"

SET NETWORK MONITORING (“NETWORK MONITOR”)

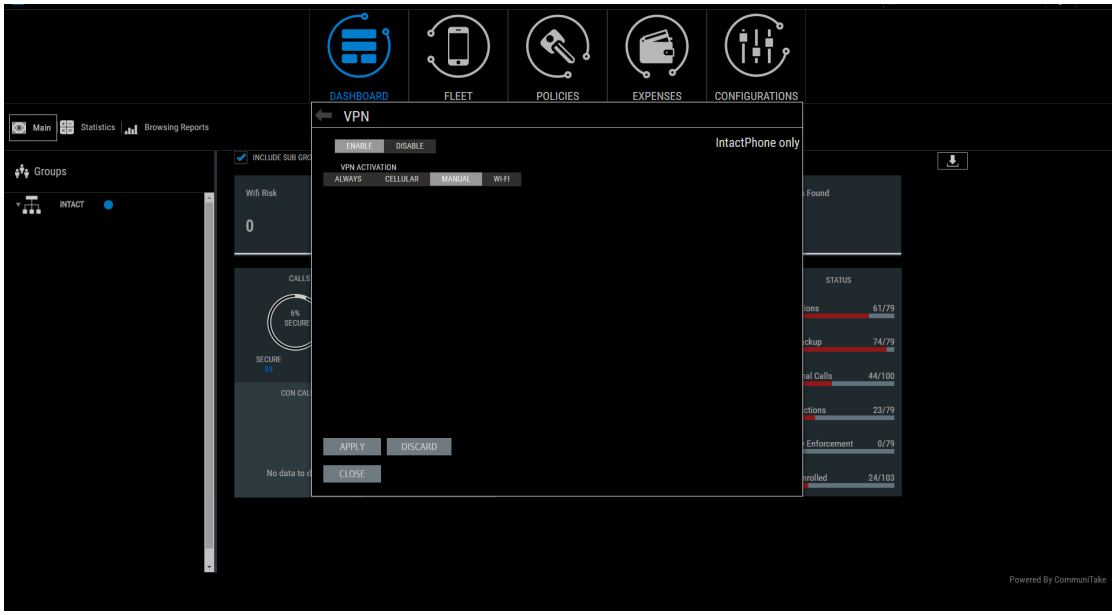


Network Monitoring settings feature provisions attempts by on-device applications to access internet addresses that are defined or suspected as suspicious sites by external listing.

Perform the following steps to activate network monitoring:

1. Click on the “**Settings”** icon at the upper right of the application screen.
2. Click on “**Network Monitor”**.
3. Check “**Network Protection**”. This will activate the monitoring operation.
4. Select the number of days in which the Network Monitoring KPI will display deviating devices.
5. Check “**Network reports**” to activate network monitoring reports display on the main screen.
6. Click on “**Save**”.

DEFINE VPN (“VPN”)



VPN settings define the activation type of the persistent APN across the IntactPhone environment. The VPN is tunneling all device communications, including emails.

Perform the following steps to activate VPN:

1. Click on the “**Settings”** icon at the upper right of the application screen.
2. Click on “**VPN”**.
3. Select “**Enable**” or “**Disable**”.
4. Select the “**VPN activation**” type:
    a. **Always**: the VPN is always active.
    b. **Cellular**: the VPN is always active on a cellular connection.
    c. **Manual**: the device holder can manually activate/deactivate the VPN from the device.
    d. **Wi-Fi**: the VPN is always active on a Wi-Fi connection.
5. Click **“Apply”.**

Note If the VPN button is missing from the settings menu, it was not enabled as a “feature to display” in the central accounts management system under. Verify that it was activated by your account manager.

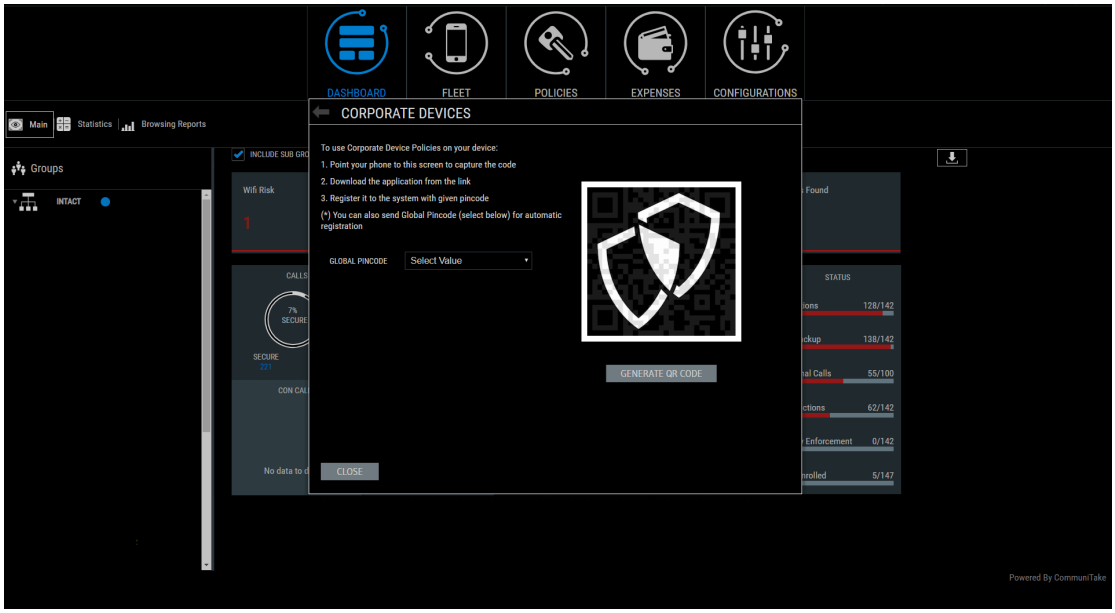
SET PANIC BUTTON (“PANIC BUTTON”)

Panic Button settings define automated device configurations that are performed once the device holder activates Panic Button. This activation is expected to occur once the device holder faces dangerous situation in which the device may physically be obtained by malicious others. Panic Button activation occurs by rapidly clicking three consecutive times on the Panic Button icon.

Perform the following steps to activate Panic Button:

1. Click on the “**Settings”** icon at the upper right of the application screen.
2. Click “**Enable**”.
3. Check the following Panic Button actions (one or more):
    a. **“Allow factory reset”.**
    b. **“Allow delete contacts”.**
    c. **“Allow delete SMS”.**
    d. **“Allow clear applications data”.**
    e. **“Allow uninstall applications”.**
    f. **“Allow send location”.**
4. Click “**Apply**”.

SET CORPORATE DEVICES ("CORPORATE DEVICES")



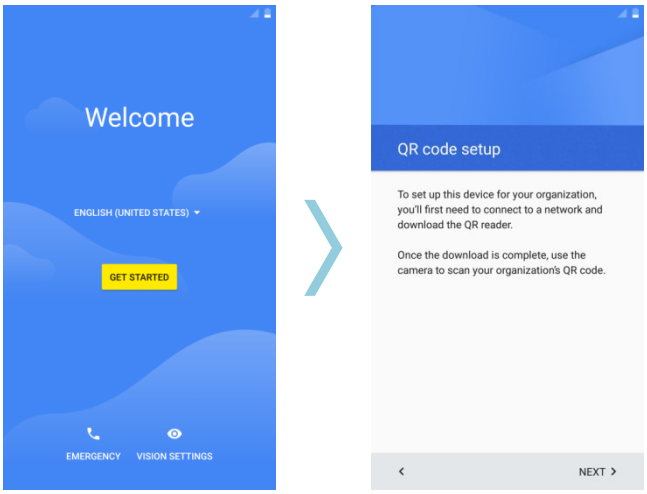
Corporate Devices settings enable you to deploy additional device restrictions as part of Android built-in capabilities. Corporate Devices support installation and provisioning of a device without registering the device to a Google account.

IntactPhone devices that are running IntactOS automatically support Corporate Devices restrictions once enrolled in the central administration system.

Non-IntactPhone devices require the following provisioning process to download and install the app on the device. Please note that devices that will not use the following procedure to install the app will not gain the Corporate Devices privileges and capabilities.

To install the APK on a commercial Android mobile device:

1. Make sure that the mobile device is in its factory state (e.g., new device or post factory reset action).
2. Validate that the target mobile device runs Android 7.0 OS or higher.
3. After factory reset, on the **Welcome / Start** screen >> tap six (6) times on the **Welcome / Start** text.
4. On the **QR Code Set-up Screen** >> tap "**Next".**

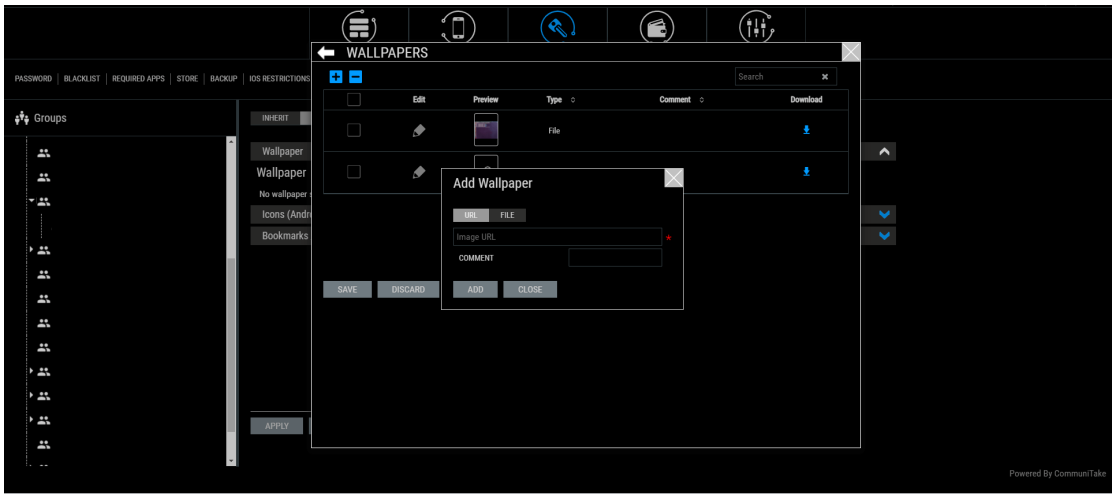


5. You may be asked to connect to a WI-FI network and install the QR code app (will be done automatically)
6. At this point, you can enroll the device in two forms:
    - Enroll in the target account with no allocation to a specific group. For this choose "**Select Value"** in the **Global PIN code** data field.
    - Enroll in the target account to a specific group. For this choose a target group PIN code from the dropdown list in the "**Global Pincode"** data field
7. Click on "**Generate QR Code" button.** A QR code will be generated**.**
8. Point the phone to the on-screen QR to capture the code.
9. Download the APK from the link.
10. At this phase, act by the selected PIN code type:
    - If you have selected the **Global Pincode**, on first app activation tap on the IntactPhone app, and key in a PIN code that was generated for that account via the in general Global Enrollment Process (Perform Global Enrollment Process).
    - If you have selected a group related PIN code, the device will run by this PIN code, and there is no need to key in a PIN code on first app activation. The device will automatically enroll in the target group and will inherit its pre-defined policies.

MANAGE WALLPAPERS LIBRARY ("WALLPAPER")

One of the system's policy is device home screen management. The policy allows you to define the device's home screen. You can pre-define the home screen images librabry to facilitate running this policy smoothly.

TO MAMANGE WALLPAPERS



1. Click on the "**Settings"** gear icon at the upper right of the application screen.
2. Click the "**Wallpaper**" button.
3. Click the Plus icon. 

4. Select a source "**URL"** and key-in the link or select "**File**" and upload the source file.
5. Click "**Add**".
6. Click "**Save**".
7. To edit a Wallpaper, click on the Pencil icon, and repeat the Add actions.
8. To remove a Wallpaper, check the box near the target Wallpaper and click the Minus icon.
9. Click "**Save**".

When required to manage the Homescreen policy, the Wallpaper library will be available for you to download the image needed.

Note Home screen wallpaper: wallpaper retrieval via an external URL allows HTTPS only links.

3

ENROLLING DEVICES

INTACTPHONE APPLICATION INSTALLATION

The IntactPhone application can be installed on the device in three methods:

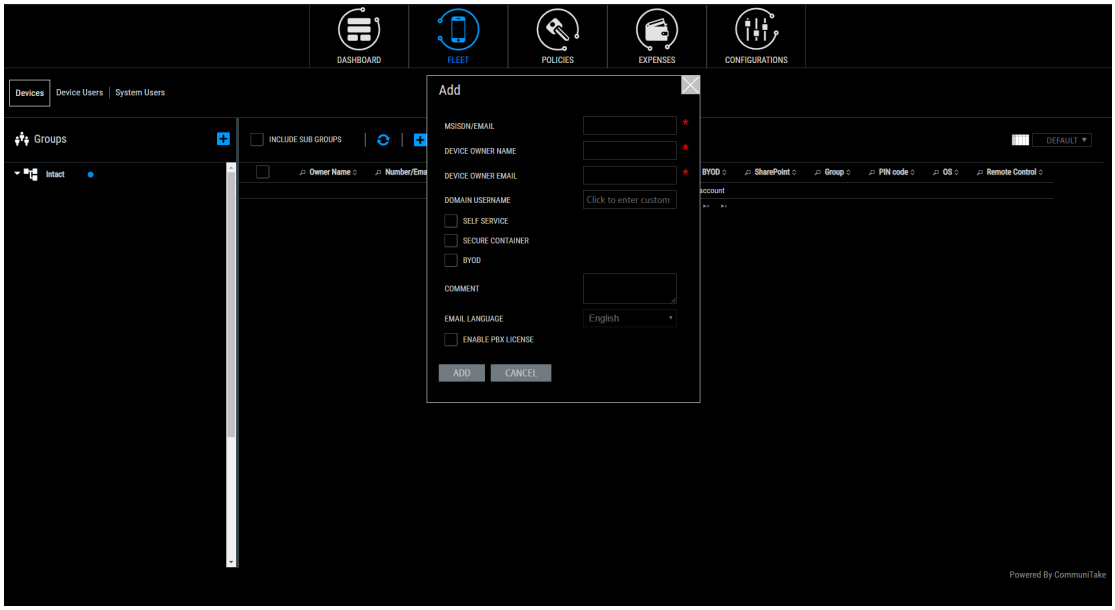
1. SMS/Email invite based installation.
2. Self-registration using Active Directory / LDAP credentials.
3. Global enrollment via PIN codes.
4. Mass enrollment process.

The enrollment method will be defined by the system administrator.

SMS/EMAIL INVITE

The enrollment via an SMS invite occurs as follows:

You manually add the user and his / her device to the system (one by one or via bulk upload). Note to select Self Service access and / or Secure Container access and / or BYOD policy.



Once added, the system automatically sends an invite, containing a download link, to install the IntactPhone application.

ENROLL AN INTACTPHONE DEVICE

IntactPhone devices are delivered with a built-in command and control app.

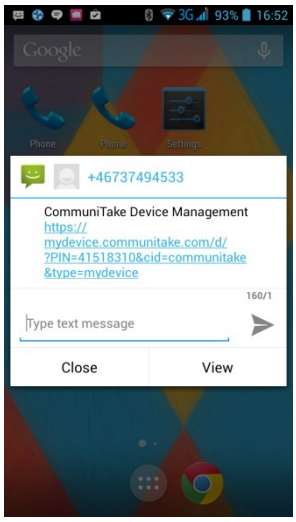
All you have to do is tap on the "**Intact**" app icon that resides on the apps menu screen and key in the enrollment Pine code that you have set under the Global Enrollment process (Global Enrollment) or that was set for you by us.

Note: Make sure to connect the device via SIM Card or Wi-Fi prior to this procedure. Ensure that the device is connected by ratifying its displayed date and time.

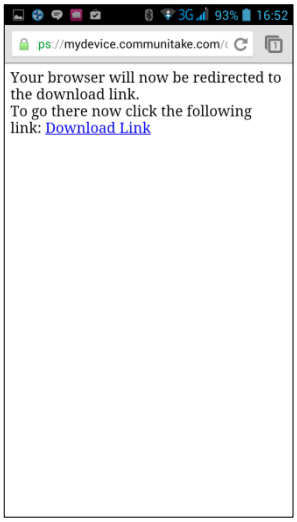
ENROLL AN ANDROID DEVICE (WITHOUT INTACTOS)

The device holder should click the link, install the IntactPhone application and follow the directives during the installation:

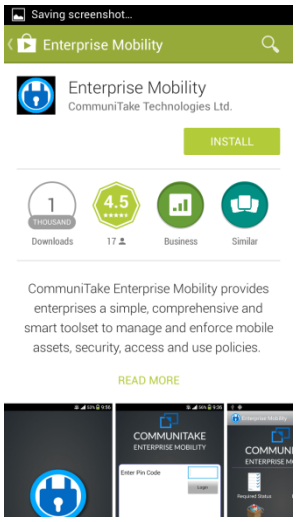
Open the SMS



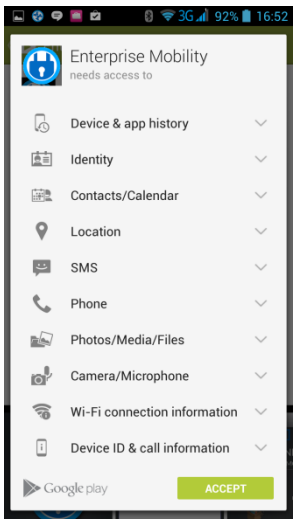
Download starts automatically



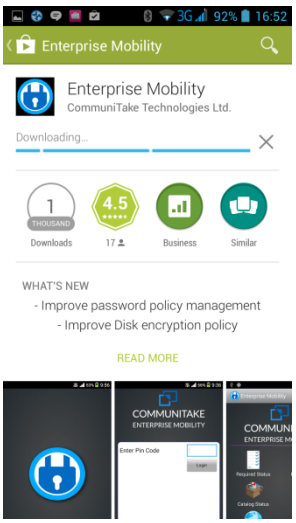
Click 'Install'



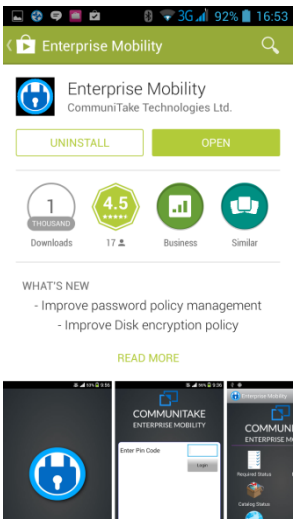
Click 'Accept'. You may be presented with a PIN code screen at first launch



Downloading



Click 'Open'

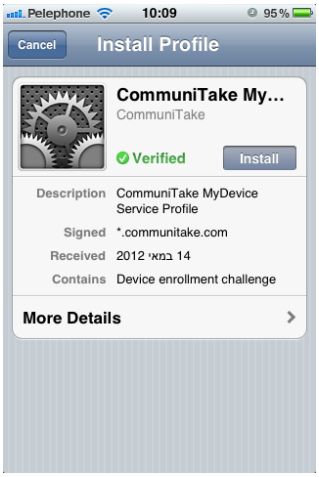


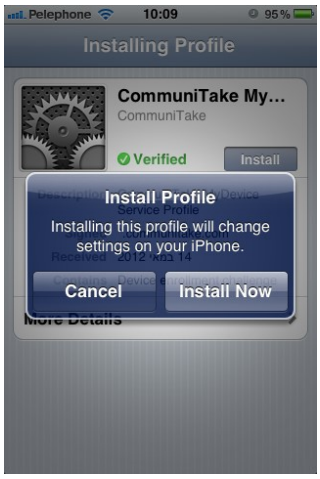
ENROLL AN IOS DEVICE

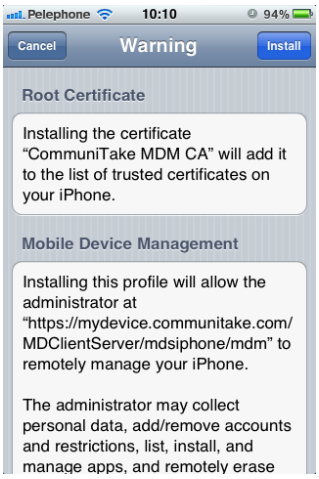
For application level only IntactPhone deployments that consist iOS devices:

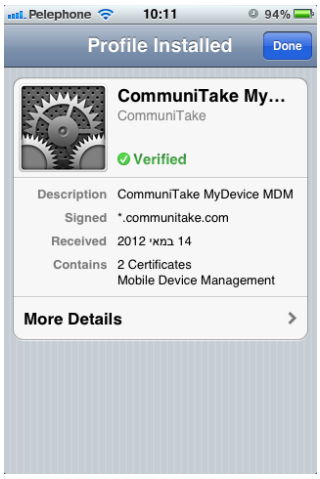
Prior to enrolling an iOS device, conclude the process of the registration for iOS devices. Apple requires a one-time procedural step to allow the IntactPhone EMM system to manage your iOS devices. Requesting and uploading the iOS certificate is done through the system **'Setting'** located on the upper right corner of the screen. Once you have completed the generic iOS registration process, you can enroll new iOS devices in the system.

1. Follow the steps of adding a device.
2. An SMS will reach the device. The device holder should open it and click on the link. A profile will be automatically downloaded.
3. The device holder should install the profile. On completion, the device is registered.



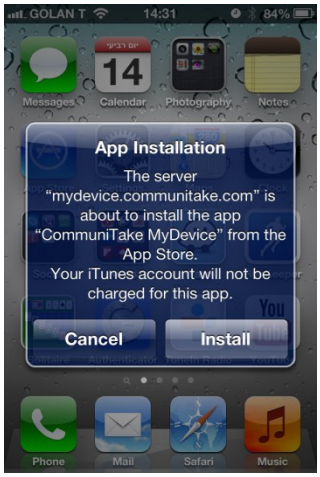




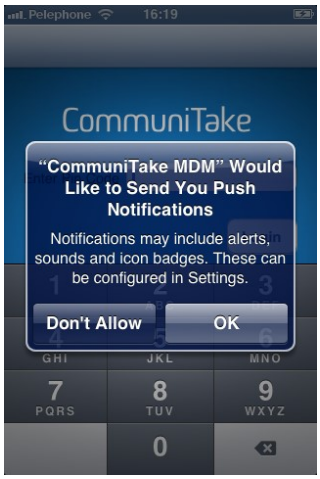


In order to allow more iOS device management capabilities such as contacts backup and restore, sound alarm, get location, web browser control and data usage tracking, there is a need to complete the installation process with the following:

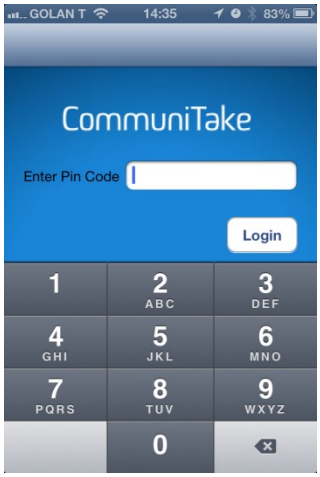
Once the profile was installed, you are required to install the IntactPhone application that is displayed on the device.



1. Install the application from the Apple store.
2. Launch the application.
3. Accept the following three requests (you must accept all three):
    a. Use of current location.
    b. Access contacts.
    c. Receive push notifications



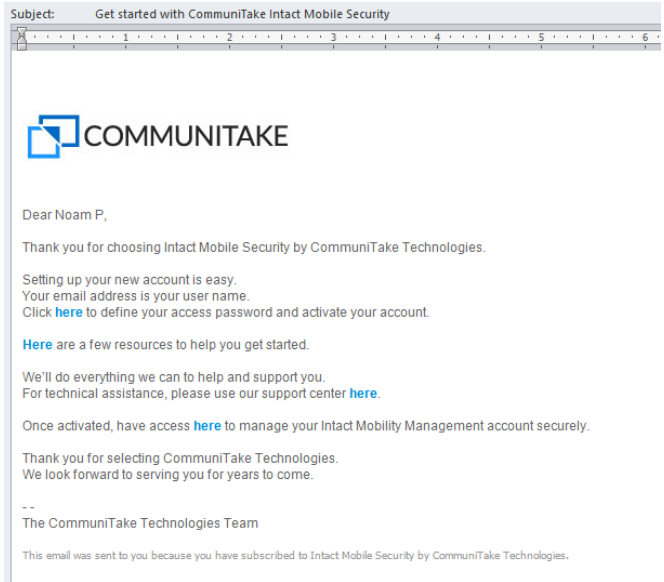
4. The application then requests a PIN code. The PIN code is the same for both the profile installation and the application installation. It remains in the "Devices table" until the complete installation of the profile and the application.



5. Key-in the PIN code.
6. Verify to receive a "**Registered Successfully**" notification. This is the indication that the application connects to the server and finishes syncing with it.

7. Close the application.

If you have marked the self-service access and / or the Secured Container access, the user will receive email for each module access.


Subject: Get started with CommuniTake Intact Mobile Security

COMMUNITAKE

Dear Noam P,

Thank you for choosing Intact Mobile Security by CommuniTake Technologies.

Setting up your new account is easy.
Your email address is your user name.
Click here to define your access password and activate your account.

Here are a few resources to help you get started.

We'll do everything we can to help and support you.
For technical assistance, please use our support center here.

Once activated, have access here to manage your Intact Mobility Management account securely.

Thank you for selecting CommuniTake Technologies.
We look forward to serving you for years to come.

--
The CommuniTake Technologies Team

This email was sent to you because you have subscribed to Intact Mobile Security by CommuniTake Technologies.

For accessing the Secure Container and performing secure messaging or secure SharePoint files view, the user should click on the Secure Container icon and enter the temporary password as sent in the email. Then the user will be directed to replace the password with a new password.

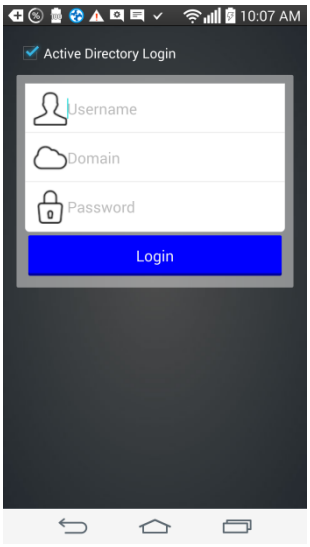
PERFORM SELF-REGISTRATION

1. The system integration with Active Directory / LDAP structures the hierarchical groups in the system.
2. Each group contains the users that are attached to it, without the allocated devices.
3. Once the integration process is concluded, you can initiate the self-registration process.
4. Send an email to users, inviting them to register.
5. The invite should contain the link to download the application: https://mydevice.CommuniTake.com/d
6. Direct the users to download the IntactPhone application and install it.
7. After installation, users are required to check the Active Directory Login checkbox and enter their Active Directory / LDAP credentials in order to complete the enrollment.
8. On registration completion, the device is being automatically added to the user's group and obtains all the policies that were defined for it.

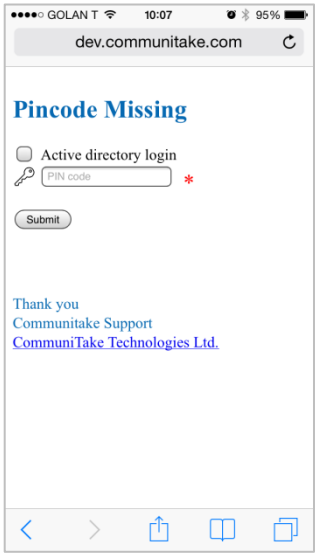
Important For devices running pre iOS 7.0:
When entering the Active Directory / LDAP credentials, a PIN code is displayed at the bottom of the screen. This PIN is also displayed in the system portal fleet view.
The user should enter this PIN code when the registration process requires it.

For Android devices:
Once the download link is selected, the device holder will be presented with this screen. The user should check the Active Directory Login checkbox.

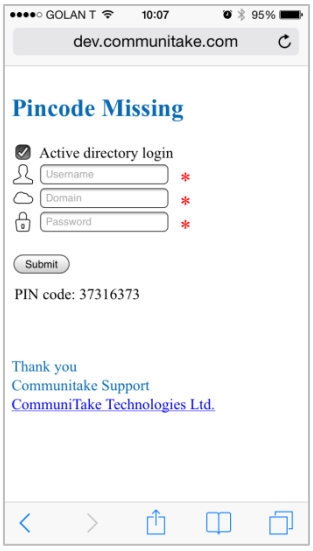
For Android devices:
Once checked, the user will be presented with this screen. The user should enter the credentials. On completion, the device will be enrolled in the IntactPhone Command Center.



For iOS devices:
Once the download link is selected, the device holder will be presented with this screen. The user should check the Active Directory Login checkbox.



For iOS devices:
Once checked, the user will be presented with this screen. The user should enter the credentials. On completion, the device will install the IntactPhone profile and enroll in the IntactPhone Command Center.



SET GLOBAL ENROLLMENT VIA PIN CODES

The system allows you to allocate devices to groups without allocating them to specific users. These devices are allocated to pre-defined groups via a group's PIN code. (Please refer to the section named 'Global Enrollment Process').
For enrolling a group related device, you should send the user an invite email / SMS with a link to download the device administrator app. You should also indicate in the invite email / SMS the pre-defined PIN code of the user's group.

The user will be required to enter the specific PIN code during the enrollment process.

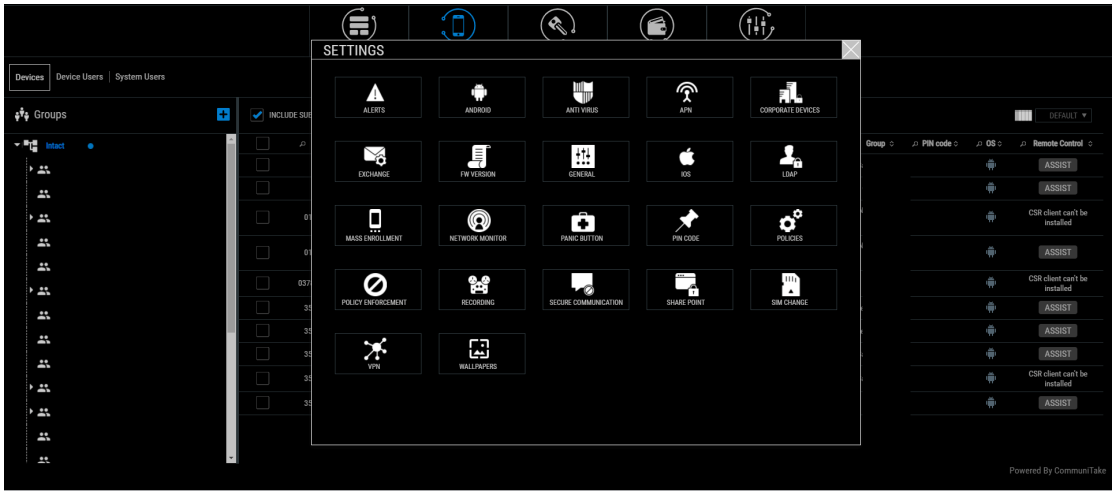
Important The global enrollment process is only applicable to Android devices.

PERFORM MASS ENROLLMENT

The proprietary mass enrollment process is similar to the Google Zero Touch enrollment. It applies to IntactPhone devices that are not enrolled in the IntactCC system.
The process: The IntactCC admin uploads an Excel/CSV file containing IMEI numbers, Serial numbers, and Group Names. On the first device activation, the device connects to the system server and receives an on-the-fly group pin code, which is used to enroll in the group.

TO PERFORM MASS ENROLLMENT

1. Click on the "**Settings"** gear icon at the upper right of the application screen.



2. Click on the "Mass Enrollment" tab. Make sure to be on the "Process" tab.
3. Upload an Excel or a CSV file in the described structures.

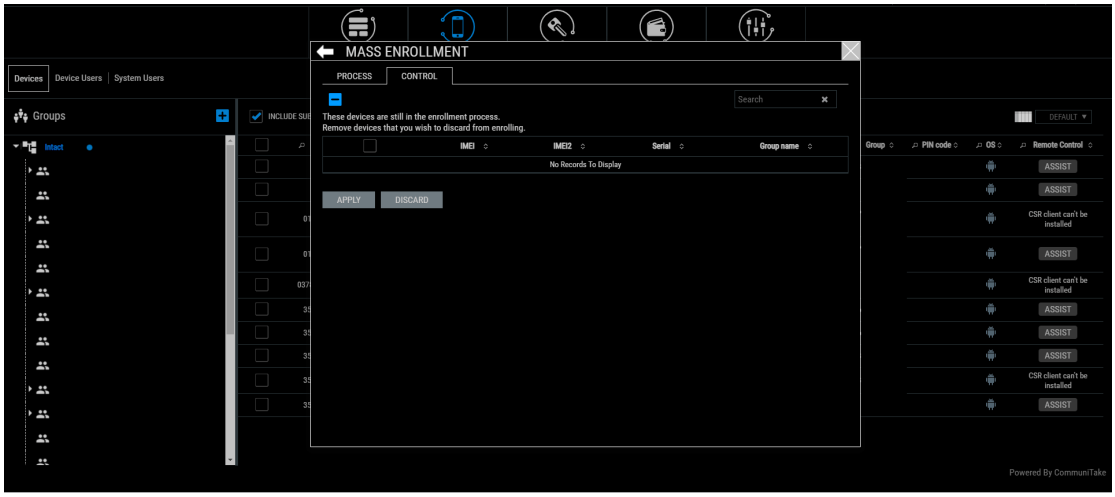
The system will display valid device data. The system will display invalid information in Red. The system will mass enroll devices with correct entries only.

4. Click "**Submit**".

The system will display the devices that are ready to complete the enrollment process.

Device holder experience: the device holder should activate the device for the first time, link it to Wi-Fi or data connectivity, and tap the "**Intact**" app icon. The device will seamlessly enroll in the IntactCC system. An ICOM device holder should activate the device for the first time and follow the Welcome screen guidance - link the device to Wi-Fi or data connectivity, tap on the enrollment button. The device will seamlessly enroll in the IntactCC system.

5. Click the "**Control**" tab to view devices that are ready for registration, but the device holders have not yet completed the process.



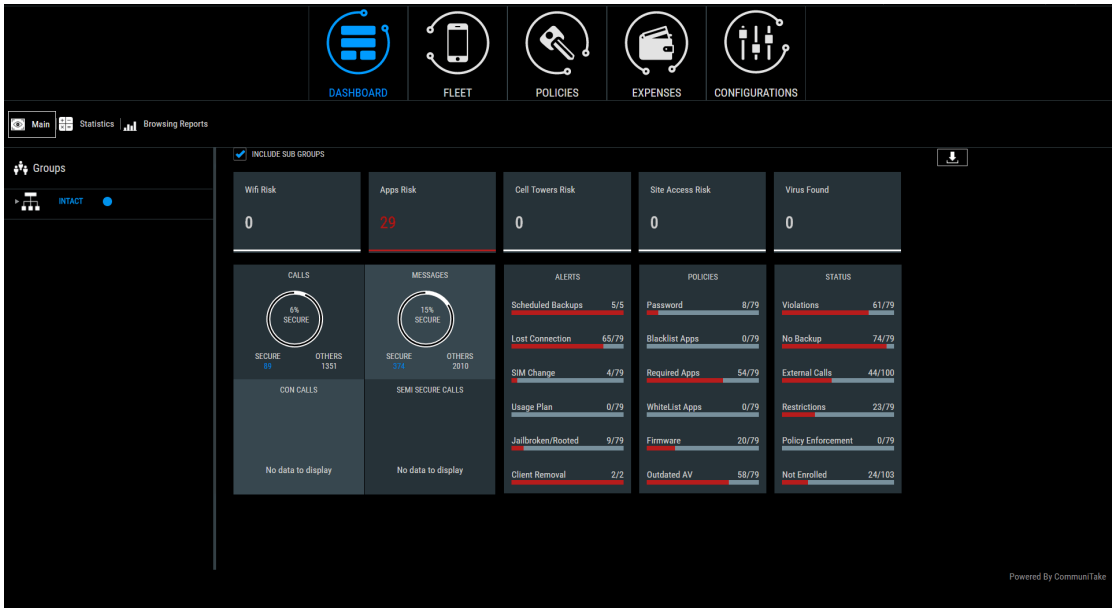
Note: It is best to send the application APK file to already active devices before the Mass Enrollment process. Once received, the device holder should tap the Intact icom and key in the PIN code as given by the system administrator.

4

DASHBOARD MANAGEMENT

DASHBOARD DATA AND KEY PERFORMANCE INDICATORS (KPIS)

The initial view presented when accessing the system is the system dashboard. The system dashboard provides an instant overview of the state of the enterprise's devices.



You can select to view information for current group or current group along with its subgroups. The Dashboard components that are displayed and the order of their display can be customized to your personal preference. This order and filtering is maintained between sessions, allowing you to choose the KPIs you wish to see.
The system dashboard contains the following information:

Presentation	Description
Risks	
Wi-Fi Risk	The number of devices for which the IntactPhone's threat intelligence system has detected anomalies in Wi-Fi connectivity parameters that may indicate a cyber-attack.
Apps Risk	The number of devices for which the IntactPhone's threat intelligence system has detected anomalies in one or more application that may indicate a cyber-attack.

Cell Tower Risk	The number of devices for which the IntactPhone's threat intelligence system has detected anomalies in Cell-Towers' connectivity parameters that may indicate a cyber-attack.
Site Access Risk	The number of devices for which the IntactPhone's network monitoring system has identified an attempt by one or more on-device application to access internet addresses that are defined or suspected as suspicious sites by external listing. (The app that attempts this access is being automatically shut down).
Virus Found	The number of devices for which the IntactPhone's antimalware application has detected a known malware that may indicate a cyber-attack.

Presentation	Description
Calls graph	
Secure calls	The total IntactPhone-to-IntactPhone calls number.
Other calls	The total non IntactPhone-to-IntactPhone calls number (e.g., IntactPhone-to-IntactDialog calls; IntactDialog-to-IntactDialog calls; IntactPhone-to-regular phone).
% secure	% of IntactPhone-to-IntactPhone calls number out of the total calls.

Presentation	Description
Messages graph	
Secure messages	The total IntactPhone-to-IntactPhone messages number.
Other messages	The total non IntactPhone-to-IntactPhone messages number (e.g., IntactPhone-to-IntactDialog calls; IntactDialog-to-IntactDialog).
% secure	% of IntactPhone-to-IntactPhone messages number out of the total messages.

Presentation	Description
Semi-secure calls graph	
Semi-secure calls	The total IntactPhone-to-regular phone calls number.
Other calls	The total non IntactPhone-to-IntactPhone voice calls number (e.g., IntactPhone-to-IntactDialog calls; IntactDialog-to-IntactDialog calls; IntactPhone-to-regular phone).
% secure	% of IntactPhone-to-regular phone calls number out of the total calls.

Presentation	Description
Conference Calls	
Secure Con Calls	The total IntactPhone-to-IntactPhone conference calls number.
Other Con Calls	The total non IntactPhone-to-IntactPhone conference calls number (e.g., IntactPhone-to-IntactDialog con calls; IntactDialog-to-IntactDialog con calls; IntactPhone-to-regular phone con call).
% Secure Con Calls	% of IntactPhone-to-IntactPhone conference voice calls out of the total con calls.

Presentation	Description
Alerts	
Scheduled backups	The number of devices that have a backup policy but the periodic backup has failed.
Lost connection	The number of devices which have exceeded the time configured in the system for connecting to the cloud service.
SIM change	The number of devices that have replaced their SIM card.
Usage Plan	The number of devices which have exceeded one or more usage thresholds set in the system. These thresholds include items defined in the Usage plans such as calls minutes, SMSs and data.
Jailbroken / Rooted	Number of devices that are jailbroken or rooted.
Client removal	The number of devices in which the user disabled the Android device administrator for the Command Center application or an iOS Command Center profile was deleted.
Policies	
Password Policy	The number of devices that are not aligned with their assigned password policy. This policy may present four states: **"OK"**: the device has received the Password Policy and is in compliance. **"Not Supported"**: the device cannot fulfill the Password Policy due to OS limitations. **"Pending"**: the device has not yet received the Password Policy from the system server. **"Failed"**: the device has received the Password Policy but is not in compliance.

Blacklist Apps	The number of devices that are not aligned with their assigned prohibited applications policy. This policy may present three states: **"OK"**: the device has received the Blacklist Apps policy and is in compliance. **"Pending"**: the device has not received yet the Blacklist Apps policy from the system server. **"Failed"**: the device has received the Blacklist Apps policy but is not in compliance (the device has an application installed that appears in the blacklist).
Required Apps	The number of devices that are not aligned with their assigned mandatory applications policy. This policy may present three states: **"OK"**: the device has received the Required Apps policy and has installed all required applications. **"Pending"**: the device has not received yet the Required Apps policy from the system server. **"Failed"**: the device has received the Required Apps policy but has not yet installed all required applications.
Whitelist Apps	The number of devices that have installed applications that are not in their whitelist. This policy may present three states: **"OK"**: the device has received the Whitelist Apps policy and is in compliance. **"Pending"**: the device has not received yet the Whitelist Apps policy from the system server. **"Failed"**: the device has received the Whitelist Apps policy but is not in compliance (the device has an application installed that does not appear in the Whitelist apps list).
Firmware	The number of devices that have not yet installed the latest firmware version. This policy may present two states: **"OK"**: the device has received the firmware updates and is in compliance. **"Failed"**: the device has received the updated firmware but is not in compliance.
Not Updated AV	The number of devices that do not have the recent antivirus definition updates. This policy may present two states: **"OK"**: the device has received the antivirus updates and is in compliance. **"Failed"**: the device has received the updated antivirus, but is not in compliance.
Status	
Violations	The number of devices that have deviated from a policy / restriction out of the devices in the selected group.

No backup	The number of devices that do not have an assigned backup procedure out of the devices in the selected group.
External calls	The number of devices that are enabled to perform midway secure voice calls via specially allocated subscription number in the mobile network out of the total allocated midway secure voice calls licenses to the account.
Restrictions	The number of devices that have violated either iOS or Android restrictions out of the devices in the selected group.
Policy enforcement	The number of devices which have exceeded the allowed grace period for policy violations and the system has activated enforcement measurements against them out of the devices in the selected group..
Not enrolled	The number of devices that have been registered in the system but have not yet completed the enrollment process and their attributes are not yet available to the system.

Clicking on one of the presentation areas in the dashboard will show further details such as the list of devices that is in violation or details on the device distribution:

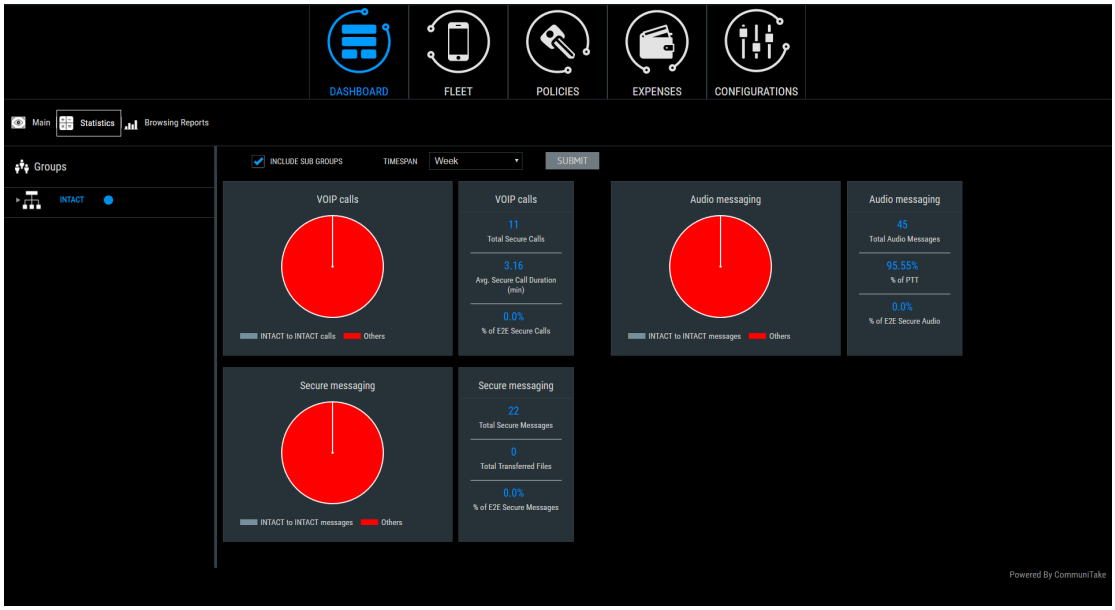
Important The device status is presented in the default table views. Please refer to section 5.

DASHBOARD DATA EXTRACTION

The dashboard data can be exported to an Excel file for further processing. To export the data, click on the "**Export"** button located in the upper right corner of the dashboard page. An Excel file will be created.

Each KPI will have its own sheet in the Excel file and only the KPIs which have data are exported.

DASHBOARD SECURE COMMUNICATIONS STATISTICS



To view the encrypted communications statistics, click on the "**Statistics**" button above "**Groups**".

The dashboard presents statistics on the use of the encrypted communications.

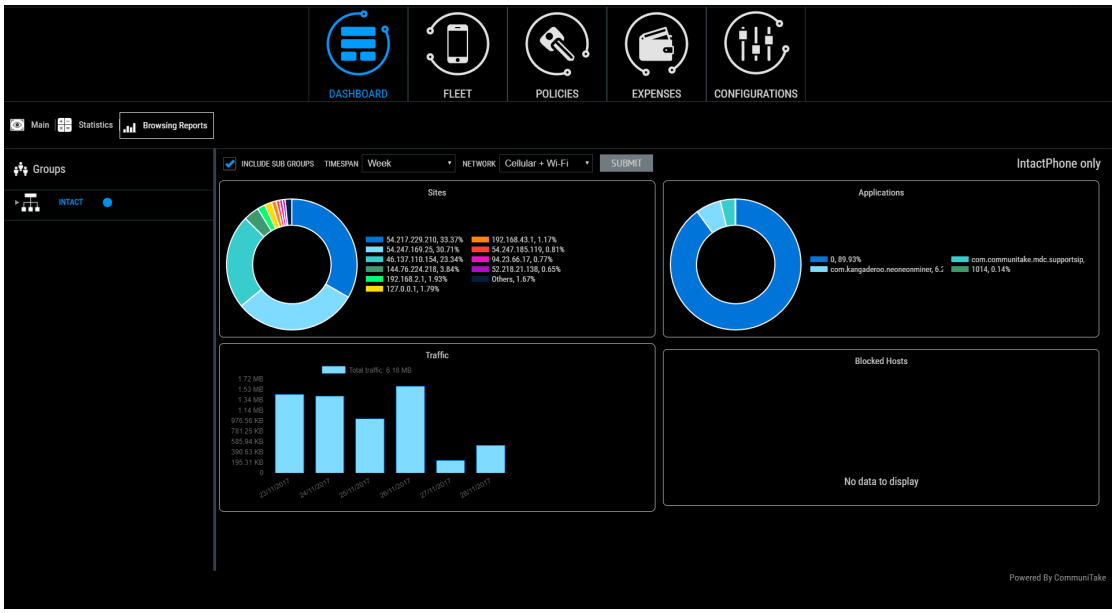
It presents the following data items:

- VoIP calls:
  - Total IntactPhone-to-IntactPhone calls number.
  - Total non IntactPhone-to-IntactPhone calls number.
  - Average duration time of IntactPhone-to-IntactPhone calls .
  - % of IntactPhone-to-IntactPhone calls out of the total voice calls.
- Secure messaging
  - Total IntactPhone-to-IntactPhone messages number.
  - Total non IntactPhone-to-IntactPhone messages number.
  - Total in-messages transferred files number.
  - % of IntactPhone-to-IntactPhone messages out of the total messages.
- Broadcast calls
  - Total broadcast calls number.
  - % of broadcast calls out of the total voice calls.
  - % of IntactPhone-to-IntactPhone broadcast calls out of the total voice calls.

The data can be filtered by group and by time:

- Day.
- Week.
- Month.
- Custom dates.

DASHBOARD BROWSING REPORTS



To view the browsing monitoring reports, click on the “browsing reports” button above “Groups”. The dashboard presents statistics on devices/applications attempts to access malicious sites.

It presents the following data items:

- Sites: sites which were visited by IntactPhone devices.
- Applications: applications that have accessed the internet and their relative browsing percentage out of the total browsing.
- Traffic: the total browsing data in MBs.
- Blocked hosts: sites’ hosts that were blocked due to suspicious behavior.

The data can be filtered by group and by time:

- Day (today).
- Week.
- Month.
- Custom dates.

Filter capabilities:

- Network type: Wi-Fi; Cellular; Both.
- Include sub-groups.

5

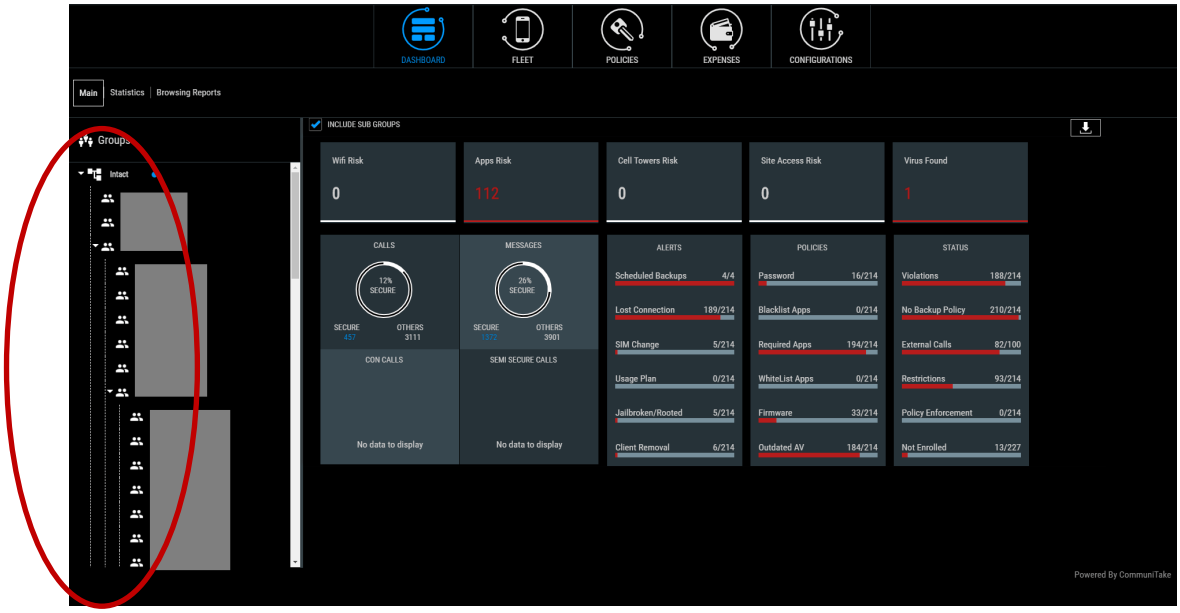
DEVICE FLEET MANAGEMENT

The **“Fleet”** tab provides a view of the enterprise's devices. Device assets are viewed and managed by groups.

ENTERPRISE GROUPS

Enterprise groups appear in the left section of the console screen. Every device holder must be part of a group. The top level group will be the overall enterprise. Below this, you can define sub-groups according to any logical structure that suits your needs. These groups can be by device type, by organizational role, by device holder location, by department etc. The enterprise groups are the basis for implementing any kind of activity on the device such as enforcing password policy, implementing backup policy and conducting mass deployment campaigns.

The small rectangle identifies a parent group on its left side. Clicking it will display the subgroups that are related to it. A group icon without a rectangle will mark a group that does not have subgroups linked to it without the rectangle on its left side.



In the initial group set-up, you will see only the top level group, representing your organization. From this point, you should build the group hierarchies that best serve you in managing your enterprise devices. You can add devices from different operating systems and different vendors to the same group.

Actions and definitions made in the device management areas will be valid for the selected group at the time of definition and activation. It is recommended to select the upper group, representing the entire enterprise for generic actions that need to take place across the organization.

Important A Group's hierarchical location has significance since it is possible to indicate an inheritance mechanism for policies. This mechanism activates on the child group the same policy as defined for its parent group. Make sure to locate groups under the proper parent group through which you want to define identical policies.

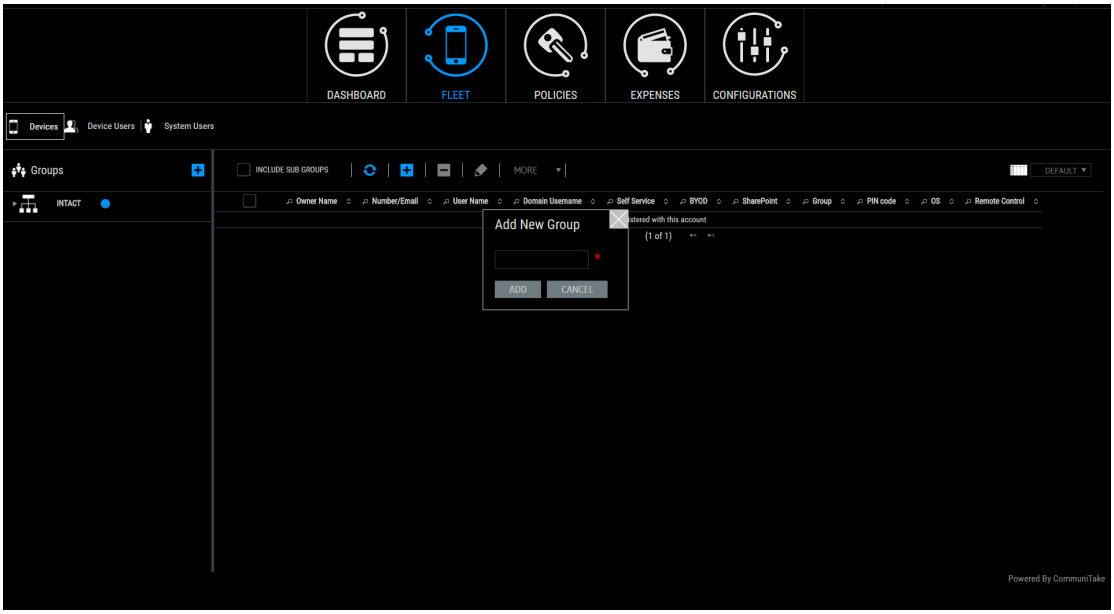
Tip The triangle on the left side of the group name appears when it is a parent group that has child groups. No such triangle will appear if it is a group with no child groups.

Clicking on this Triangle will display all the child groups connected to the parent group.

Important Business groups represent logical clusters of devices that have similar policies but differentiated policies as compared to other groups. As an initial step, it is highly recommended to carefully and thoughtfully build the business structure and allocate the policies to each and every group and only then add the devices to the groups.

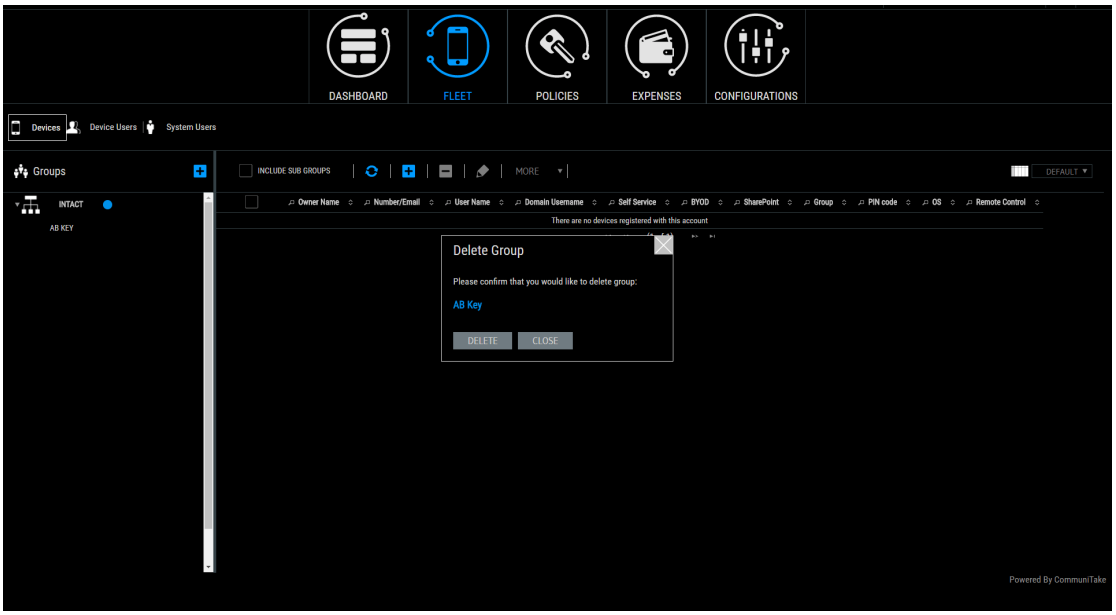
TO CREATE A GROUP

1. Click on the group for which you want to create a child group.
2. Click on the "**Add Group"** button.
3. A pop-up box appears for entering the new group name. Enter the new group name.
4. Click the **"Add"** button in the pop-up box.
5. The new group will be added under the group that you have selected.



TO DELETE A GROUP

1. Click on the group which you want to delete.
2. Click on the "**Delete Group**" button .
3. The group will be deleted from the groups' hierarchy tree.



Important You cannot delete a group that contains devices, users or child groups. You must delete all the devices, users and child groups associated with the group prior to deleting it.

DEVICES

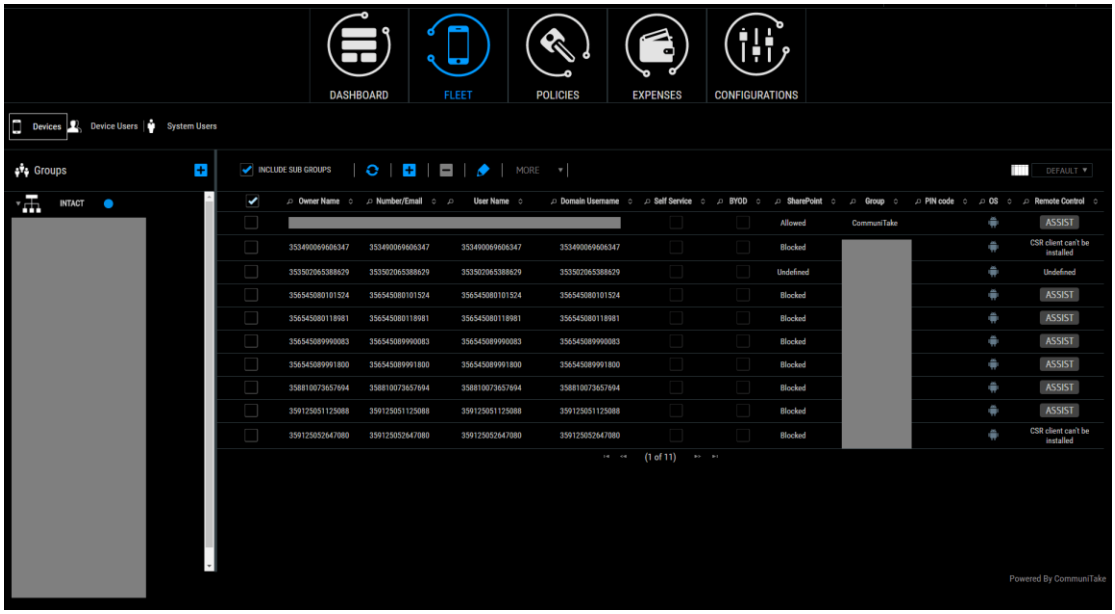
The '**Fleet**' section presents the enterprise device inventory along with device attributes

DEVICES INVENTORY VIEW

Select the '**Fleet**' tab and then click on the '**Devices**' tab.

Note This is the default presentation when clicking the "**Fleet"** tab. The system will present a table showing all the devices that are assigned to the selected group at the time of selection.

You can select to see devices only from the current group or the devices from the current group and all its subgroups.



The device table presents a default view with following attributes:

Item	Description
Device Owner Name	Device holder name as defined when the device was added to the system.
Number/Email	The MSISDN or the email address as defined when the device was added to the system.
User name	Device user email address. It will be used for Exchange configuration such as blocking the user from accessing the Exchange server as well as the IntactPhone Command Center user name for device holders who are given self-service access.
Self-service access	Checkbox for defining the device user as a self-service user.
Group	The organizational group to which the device is assigned.

PIN code	The PIN code identifies the device in the enrollment process. It might be required by the device holder in order to conclude the enrollment process. Once connected to the IntactPhone Command Center, this PIN code will no longer be necessary and will not appear in the table.
OS	Device mobile operating system.
Remote Control	One-click remote access to the device for support.

All columns contain filters or search capabilities.

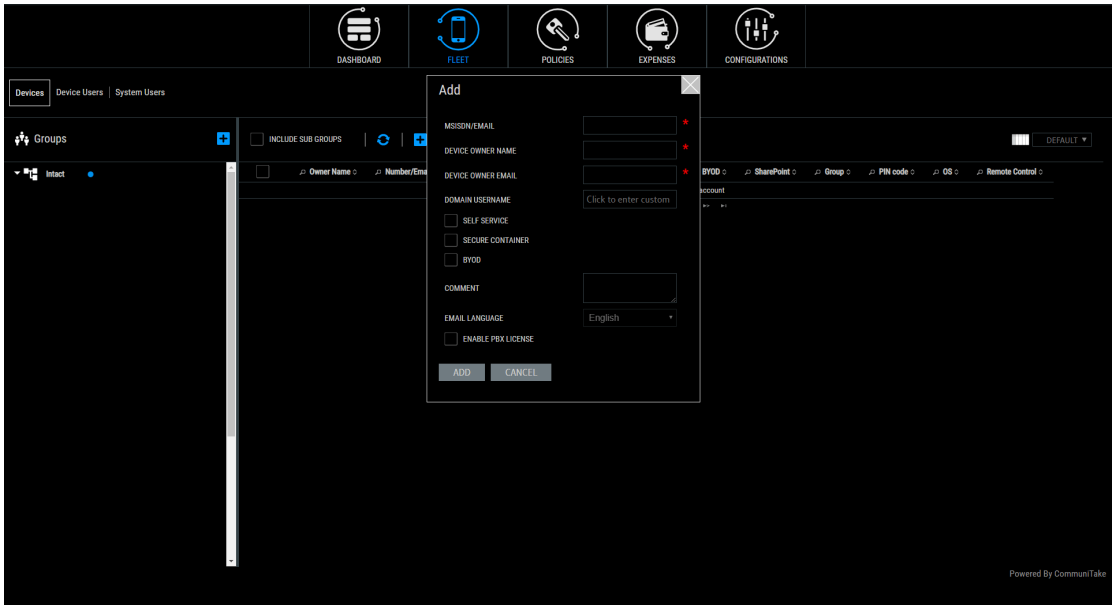
The device table icons:

Icon	Description
	Policy setting has failed.
	Policy setting is not supported.
	Policy setting is pending.
	Policy setting has succeeded.
	Policy not set.
	Policy is violated.
	Roaming is not viable.
	Roaming is viable.
	The device is not rooted.
	The device is rooted.

INCLUDING SUBGROUPS

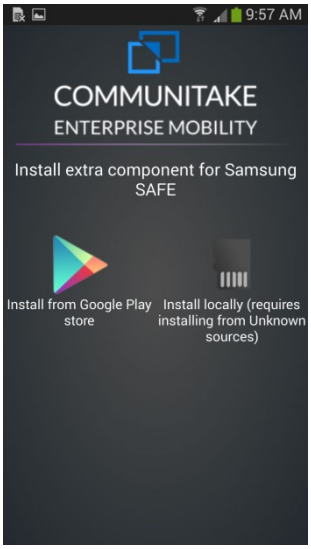
Including subgroups allows you to see and manage all the groups that are under the selected group. Once "**Include Sub Groups"** is checked, the devices table will present all the devices that are under the selected hierarchy group. If it is not checked, the system will show only the devices that directly associated with the selected group.

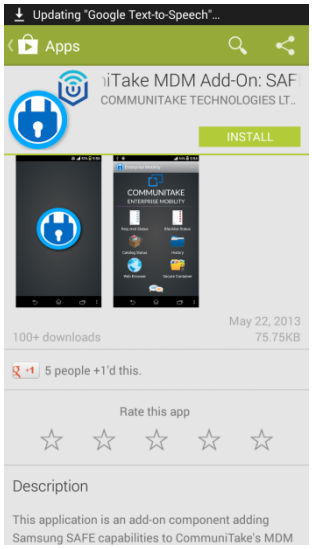
TO ADD A DEVICE



1. Click on the group to which you want to add a device.
2. Click on the **"Add"** button.
3. A pop-up box appears for entering the new device attributes. Enter the following:
    a. The new device MSISDN (phone number for a mobile phone) or an email address (for tablets).
    b. Define the device owner name as you wish it to appear in the system. Device owner name serves only for display.
    c. The device owner email. The Email address will be used for Exchange configurations and as the user name for the device owner to access the self-service device protection features.
    d. Domain username. For some enterprises, the domain username is different than the email address. For this reason, this data field must also be filled. This will allow proper operation of configurations such as Exchange and VPN.
    e. Self-service access. This access will allow the device user to access the self-service device protection features. Checking this option will generate a welcome email to the device user for activating his access.
    f. BYOD. This will appear only when the "**Enable BYOD Privacy"** is checked in the general settings. It prohibits system administrator from viewing the device location; the device backups; and the on-device applications attributes.
    g. Secure container access. This access will allow the device user to access the SharePoint files via the device client. This is only available for a Secure Container that is configured in the Settings.
    h. Email language. The selected welcome email language that will be sent to the device user.

4. Make sure that the MSISDN/email is not used elsewhere in the system.
5. If a device with the same SIM is used, you will be prompted by an alert indicating that the number is in use.
6. Click the "**Add"** button in the pop-up box. A PIN code is assigned to the device.
7. The new device will be added to the devices table under the group that you have selected.
8. An SMS is sent to the device with a client download link. The assigned PIN code is embedded in the SMS thus ensuring accurate device identification. The device must have a valid SIM card in order to receive SMS messages and push notifications.
9. The device holder should install the device client as follows:
    a. Open the SMS / Email.
    b. Activate the link and download the device client.
    c. Once the download was completed, activate the client. Device registration is completed only after the device holder downloads and activates the on-device client.
10. Once the client has finished installing, the device will show "**Successfully Registered**" message. If there was no such message, the device did not yet register. (In Android devices, the message is presented in the upper status bar).
11. Samsung SAFE and Android Enhanced devices are required to install an extra component that empowers the additional capabilities. The device holder can install the extra component from the Google Play store or locally - for Samsung SAFE or just locally – for Android Enhanced (requires allowed installation from unknown sources). It is recommended to install the extra component via the Google Play store if the user has access to it.





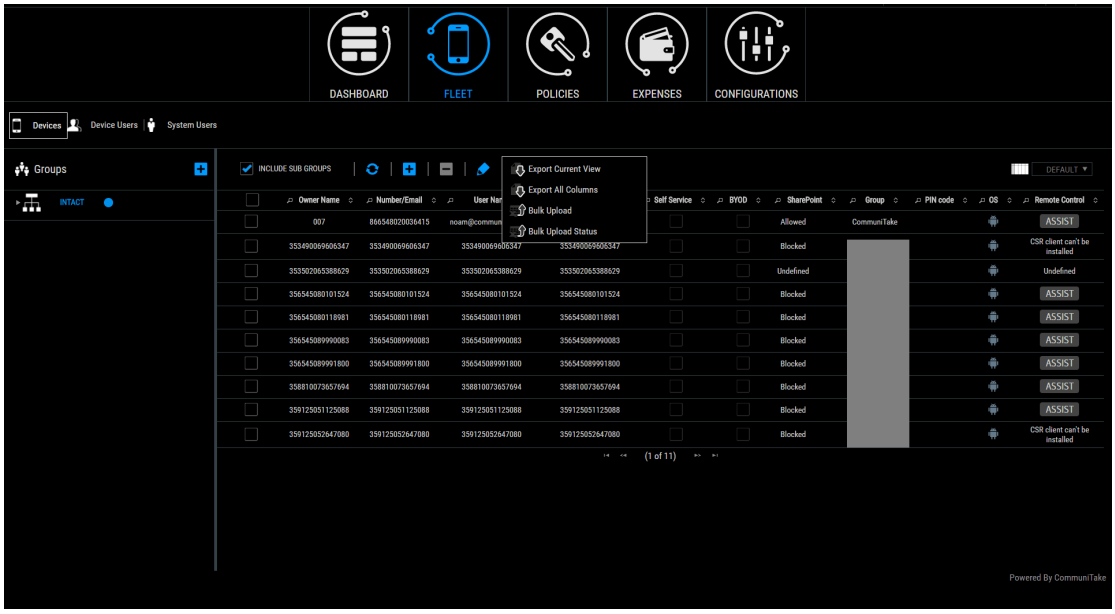
12. You can check if your device is Samsung SAFE enabled in the following link: http://www.samsung.com/us/business/samsung-for-enterprise/index.html?cid=omc-mb-cph-1112-10000022

13. You might be prompted to enter a PIN code in order to complete the device registration. Please use the PIN that was created when the device was added.
14. Make sure that there are no network issues. The client will try to reconnect every few seconds as long as it is running. It will update the capabilities when connected.
15. For every action instance made in the web page and that needs to be updated in a device, a push notification will be sent.
16. If there is no SIM card or if the device is an Android device that was not correctly registered with an account (user and password), the device will not be able to receive a push notification and it would seem as if the action did not take place. In this case, the message will reach the device the next time it periodically connects to the system.
17. To make the client simulate a push notification, open the client on the device, click on options and click on "Sync Now".
18. An email is sent to the device holder enabling him to define an access password for self-managed device protection features. The device holder user name for the system is his email address as specified in the device addition process.

Important Email address on the third field is a mandatory data field. The self-service access is optional.

If the installation SMS / email does not reach the device, you can download and install the client by manually launching the device's web browser to the following URL: http://mydevice.CommuniTake.com/d

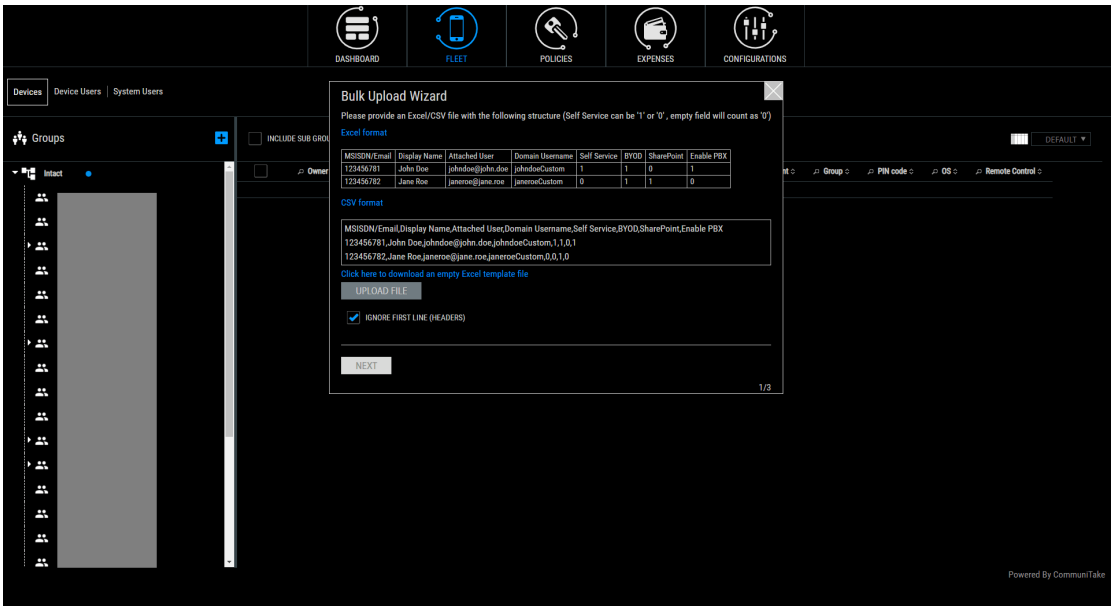
TO ADD DEVICES VIA BULK UPLOAD



The system allows you to add devices via bulk upload. Bulk upload populates a group by importing an external Excel / CSV file that contains device holders details.

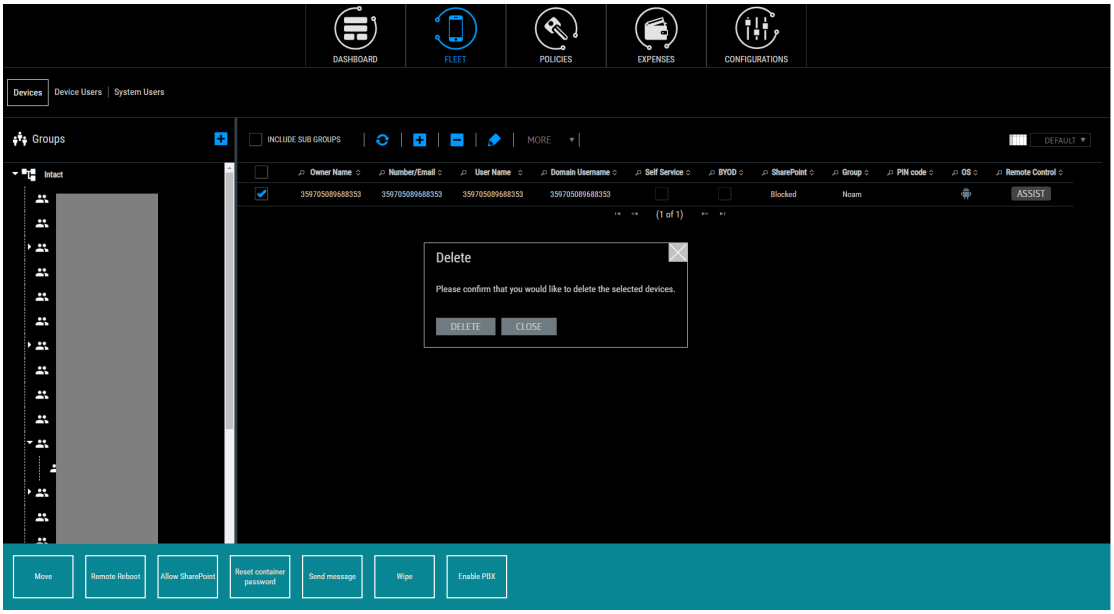
To add device holders via bulk upload:

1. Click on the **“Fleet”** tab.
2. Click on **“Devices”** tab.
3. Select the group which should be populated.
4. Click on the **“More”** tab.



5. Select **“Bulk Upload”** in the dropdown list.
6. Download the Excel file template.
7. Populate the Excel file with details by the template. Make sure to build this file in the right order. Align the data to the upper left corner of the spreadsheet.
8. Upload the file with the device holders details.
9. Click on **“Next”**.
10. Once uploaded, the system verifies that the file is in the proper structure.
11. Click on **“Next”**.
12. The system provides view of details and upload status. Verify completion for the new devices.
13. Click “**Close”**.

TO REMOVE A DEVICE



1. Click on the group from which you wish to delete a device.
2. Select the device or devices to be deleted in the table.
3. Click on the **“Remove”** button (you must select a device to see this button).
4. The device will be deleted from the system and from the table.
5. The device will display a message stating that it has been deleted. If you wish to reconnect the device to the system, you must first uninstall the on-device client and reinstall it via a new SMS.

Important After removing a device, the device should show an alert saying it was disconnected. If no alert is shown, open the client on the device; click on options and then on **“Sync Now”**. After the device is successfully disconnected, it can no longer connect to the server. If you try to manually launch the application at this point it will automatically quit. Use the device's application manager to completely uninstall the client, instead of just deleting it.

Important To remove an on-device client: Delete the device from the group it is in. Once removed from the group, a message on the device should inform the device holder that the device was disconnected successfully. An attempt to reconnect with the same device (performed by starting the client on the device) should return an error message.

Use the device's "uninstall application" mechanism to make sure that all the files that are related to client are removed.

Use the device's remove application program in **“Options”** → **“Device”** → **“Application Management”**.

TO ADD/REMOVE AN IOS DEVICE

To add an iOS device, see the flow in the subsection "**To Enroll an iOS Device"**.

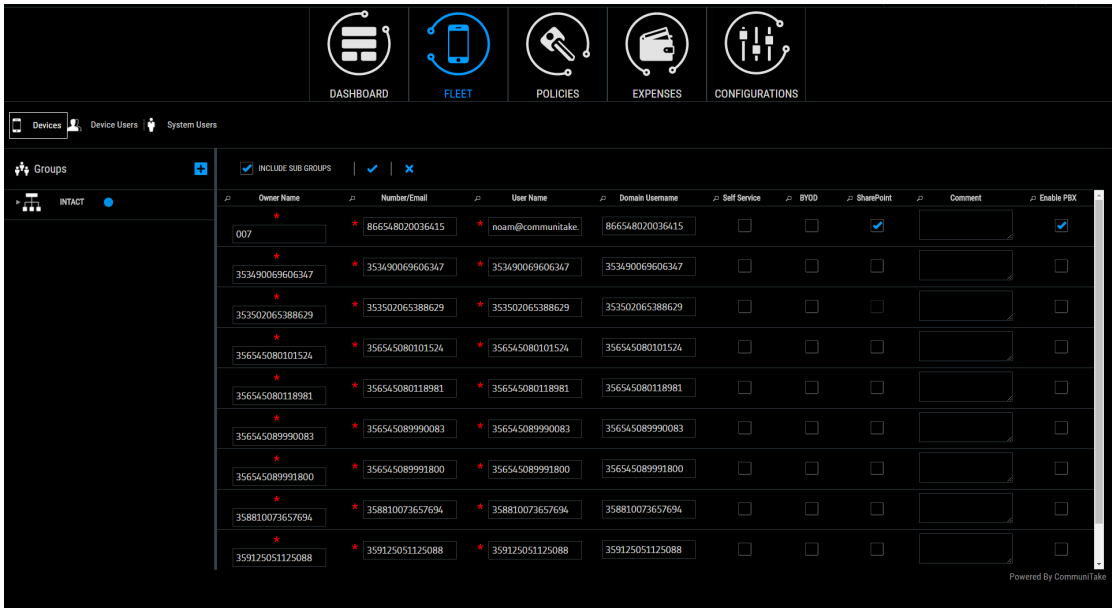
Delete the device from the IntactPhone system, in the same way you would remove any other device. On the device, do the following:

1. Select the system **"Settings".**
2. Select **"General".**
3. Select **"Profile"**.
4. Select **"CommuniTake MyDevice"** and click **"Remove"**.
5. Delete the "**CommuniTake MyDevice**" application (long press on it and click the "X").

TO EDIT DEVICE ATTRIBUTES

1. Click on the group in which you want to edit a device.
2. Click on the **"More"** tab.
3. Click on the **"Edit"** Device.
4. An editable table will be opened with Device Owner Name; Number/Email; User Name, for all the devices in the selected group.
5. You can edit the following device details:
    a. Phone number / email address.
    b. Device owner name.
    c. User name (e.g., user email address).
        i. Attach a device to a user.
        ii. Remove a user from a device, leaving just the device in the group Switch the device between users.

        If the device is attached to a new user, the user will receive a welcome email inviting him to the system.
    d. Self-service access.
    e. Secure Container access.
6. Click Save to save your changes.



Important If there was an error while changing device's details, you will remain in the edit mode with only the devices that require details completion.

TO REFRESH DEVICE DATA

The devices table is refreshed via user generated events. Clicking on the **'Refresh'** button generates an immediate update of the table data with the recent data that resides in device management system server.

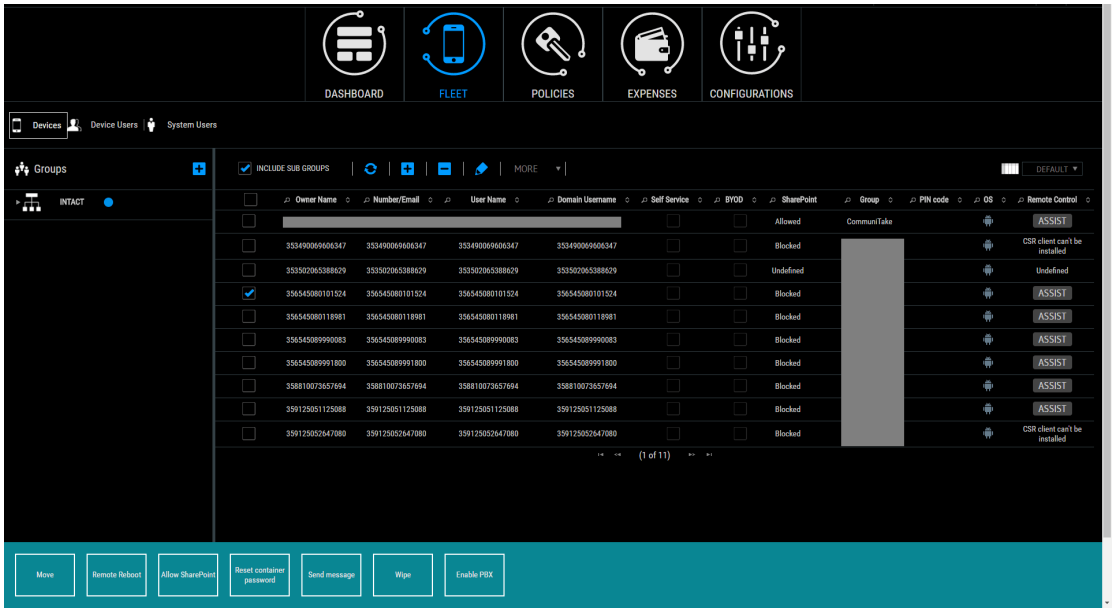
TO RESEND SMS

Device enrollment process requires sending an installation SMS. Through this SMS, the device holder downloads and installs the on-device management client. If the enrollment process was not concluded or the device holder accidently deleted the SMS, the system enables a resend procedure.

1. Click on the group in which you want to edit a device.
2. Select the device / devices for which you wish to resend an SMS.
3. Click on the **"More"** tab.
4. Click on the **"Resend SMS"**.
5. You will be displayed with a list of the devices for which the SMS is being re-sent to, along with the current PIN code and the SMS sending status.

   SMS status and PIN code presence are refreshed automatically as they become available.

TO SEND A MESSAGE

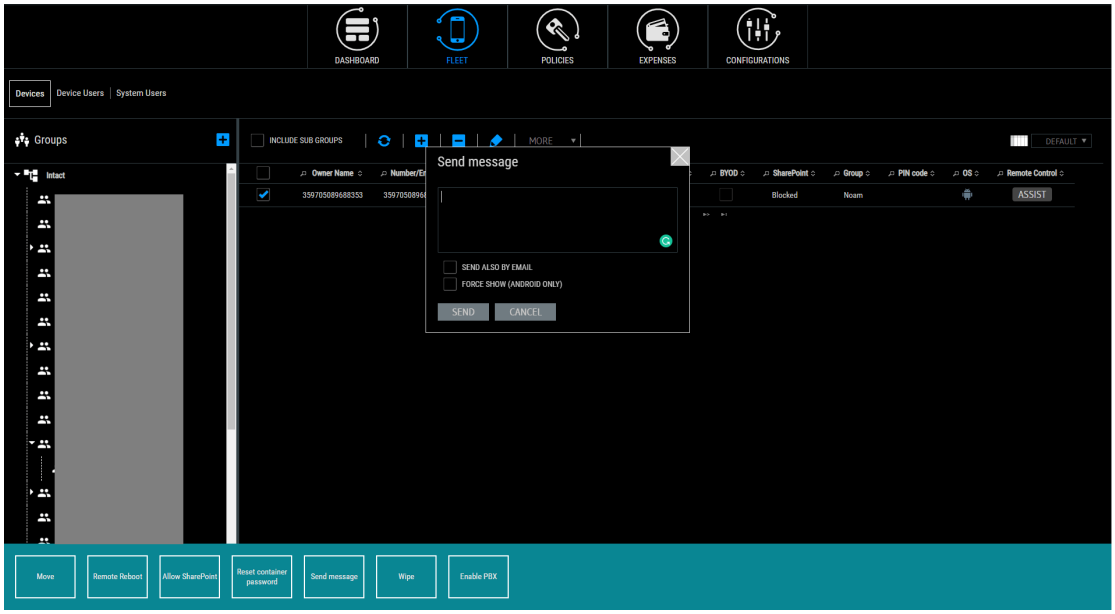


A message can be sent to a group of devices or to a single device. The message can be a notification from the IntactPhone application or an email.

1. Click on the 'Fleet' tab.
2. Click on the devices group to which you wish to send a message.
3. Check the checkbox to select all the devices that are presented on the screen. A notification will appear above the devices' table headers indicating the number of the checked devices. If you wish to send to all the group's devices, click on the link 'Click here to select all <number> devices' next to the notification about the checked devices. Once clicked, you will be notified that 'All <number> devices are selected'. Click on the 'Clear selection', if you wish to cancel your selection.
4. If you wish to send a message to a single device, check only this device in the table.
5. If you wish to send a message only to a number of devices, check the devices you wish to send the message to.
6. Click on the 'Send message' at the left bottom part of the screen.
7. Write the message in the pop-up message screen.
8. Check 'Send also by email' if you wish to send the message as an email as well. The email will be sent to the defined "device's owner email".
9. Check 'Force Show' (applicable for Android devices) if you wish that the message will pop on the recipient device screen.
10. Click on 'Send'.

Note You can also send messages to devices from:

- The KPI drill down popup.
- From the device's location tab.

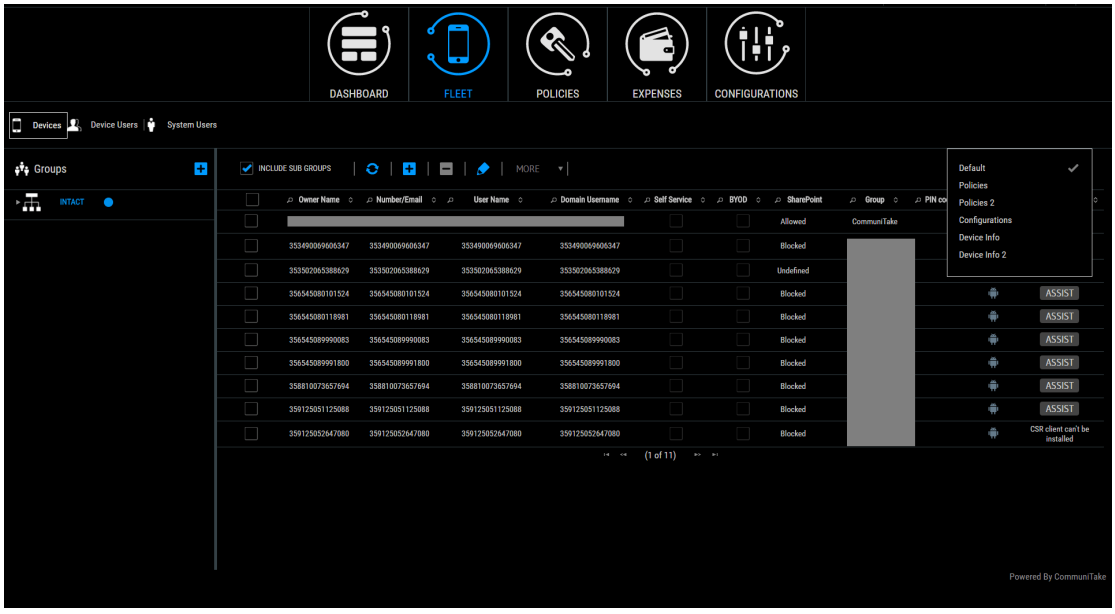


TO EXPORT DATA TO EXCEL

Devices table data can be extracted to an Excel file for further processing:

1. Click on the devices group for which you want to export its attributes.
2. Click on the **“More”** tab.
3. Select either to **“Export Current View”** or **“Export All Columns”**
4. Click on “**Export”**. The requested table will be exported to Excel.

DEVICE TABLE BUSINESS VIEWS



There are five pre-defined views of the devices' data:

Table view	Attributes
Default	Item Device Owner Name; Number/Email; User name; Self-service access; Group; PIN code; OS; Remote Control.
Policies	Device Owner Name; Number/Email; Password policy; OS; Required Apps Violation; WhiteList Violations; BlackList Violations; Restrictions Violations; Last Seen; Last Backup.
Policies 2	Device Owner Name; Number/Email; Cell Tower Violations; Wi-Fi Violations; SW Violations.
Configurations	Device Owner Name; Number/Email; OS; Exchange Violations; Wi-Fi Violations; VPN Violations.
Device Info 1	Device Owner Name; Number/Email; Vendor; Model; OS; OS Version; Firmware; Client Version; Rooted; FOTA.
Device Info 2	Device Owner Name; Number/Email; FOTA; Comment; Operator; Country; Roaming; IMSI; IMEI; Firmware.

To select a pre-defined table view:

1. Select the devices' group.
2. Click on the Views filter icon on the right area in the sub tabs area.
3. Check in the drop down views the desired view.
4. The table view will be changed in real time by the selected view.

The following table describes the content of each parameter:

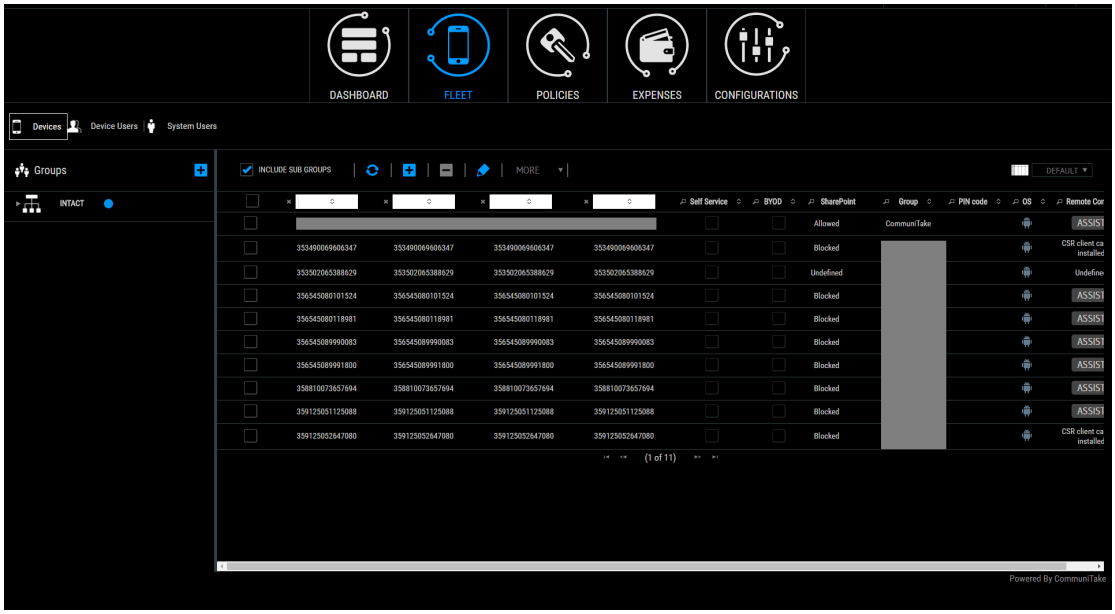
Parameter	Description
Device Owner Name	Device holder name as defined when the device was added to the system.
Phone number	MSISDN as defined when the device was added to the system.
User name	Device user email address. It will be used for Exchange configuration such as blocking the user from accessing the Exchange server as well as the IntactPhone Command Center user name for device holders who are given self-service access.
Self-service access	Checkbox for defining the device user as a self-service user.
Secure container	Device’s Secure Container access status. This is only available when secure container is defined.
PIN code	The PIN code identifies the device in the enrollment process. It might be required by the device holder in order to conclude the enrollment process. Once connected

	to the IntactPhone Command Center system, this PIN code will no longer be necessary and will not appear in the table.
Group	The organizational group to which the device is assigned.
Device vendor	Device manufacturer name.
Device Model	Device brand model name.
Last seen	The last time the device was connected to the system cloud service.
Last backup	Last backup date.
Password policy status	Yes / no indication whether there is a defined and active password policy on the device.
OS	Device mobile operating system.
OS version	Device mobile operating system version.
Firmware version	Device firmware version (not available for all operating systems).
Client version	Version of the On-device device management client that is currently installed and operating.
Rooted	Yes / no indication whether the device is rooted or jailbroken.
Country	The country as identified by Mobile Country Code (MCC) to uniquely identify a network operator.
Roaming	Yes / no indication whether the device is roaming enabled.
IMEI	The International Mobile Equipment Identity is a unique number identifying GSM, WCDMA, iDEN and some satellite phones. The IMEI number is used by the GSM network to identify valid devices.
IMSI	An International Mobile Subscriber Identity is a unique number associated with all GSM and UMTS network mobile phone users. It is stored in the SIM inside the phone and is sent by the phone to the network.
Required Apps Violation	Yes / no indication whether the device is fulfilling the mandatory applications' policy.
Whitelist Violations	Yes / no indication whether the device is fulfilling the only allowed applications' policy.
Blacklist Violations	Yes / no indication whether the device is fulfilling the prohibited applications' policy.
Wi-Fi violations	Yes / no indication whether the device installed the configuration (if supported).
Exchange violations	Yes / no indication whether the device installed the defined configuration (if supported).

VPN violations	Yes / no indication whether the device installed the defined configuration (if supported).
Restriction violations	Yes / no indication whether the device installed the defined policy (if supported).
Cell Tower violations	Yes / no indication whether the device contains a deviation from the expected Cell Tower parameters based on crowd analysis. This deviation might indicate a malicious attack.
Wi-Fi violation	Yes / no indication whether the device contains a deviation from the expected Wi-Fi connectivity parameters based on crowd analysis. This deviation might indicate a malicious attack.
SW violation	Yes / no indication whether the device contains a deviation from the expected installed applications parameters based on crowd analysis. This deviation might indicate a malicious attack.
Remote Control	One-click remote access to the device for support.
Comment	Textual description of the device / device holder.
FOTA	The date of the last Firmware over-the-air update.

SORTING AND SEARCHING DEVICES TABLE ATTRIBUTES

The system allows you to filter the devices table according to column attributes.



To select a filtered table view by column parameter:

1. Select the devices' group.
2. Click on the magnify glass icon to the left of the desired column heading.
3. Select the parameter from the drop down list or write your search item. Search is case sensitive.
4. The table view will be changed in real time showing only the devices by the selected parameter.
5. Click on the refresh icon or close the filter to resume the original table view.

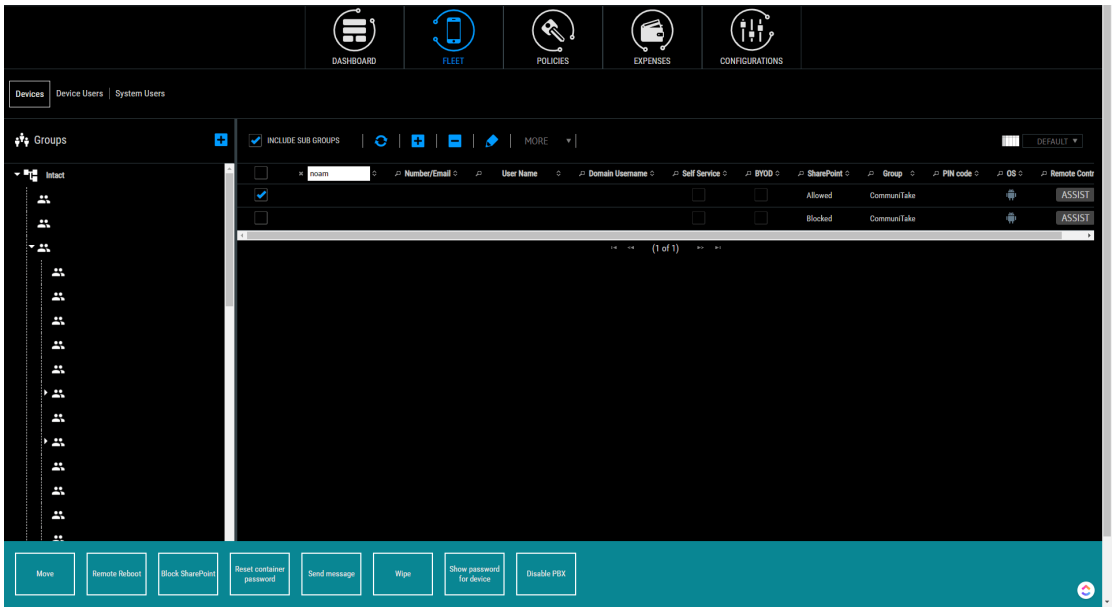
6. Click on the small arrows near the column headline to sort the column data by descending and ascending order.

The table parameters filtering options are as follow:

Parameter	Filter
Device Owner Name	A specific or partial name.
Phone number	A specific or partial number.
User name	A specific or partial name.
Self-service access	Yes / No selection.
PIN code	A specific or partial number.
Group	A specific or partial name.
Device vendor	A specific or partial name.
Device Model	A specific or partial name / number.
Last seen	A specific or partial date item.
Last backup	A specific or partial date item.
Password policy status	Success; violated; pending; unsupported; undefined.
OS	Dropdown selection: Android; iOS; WP (pending validity).
OS version	A specific or partial number.
Firmware version	A specific or partial number.
Client version	A specific or partial number.
Rooted	Yes; No; Unknown.
Country	A specific or partial name.
Roaming	Yes; No; Unknown.
IMEI	A specific or partial number.
IMSI	A specific or partial number.
Required Apps Violation	Success; violated; pending; unsupported; undefined.
Whitelist Violations	Success; violated; pending; unsupported; undefined.
Blacklist Violations	Success; violated; pending; unsupported; undefined.
Wi-Fi violations	Success; failed; pending; unsupported; undefined.
Exchange violations	Success; failed; pending; unsupported; undefined.
VPN violations	Success; failed; pending; unsupported; undefined.

Restriction violations	Success; failed; pending; unsupported; undefined.
Cell Tower violations	Success; failed; pending; unsupported; undefined.
Wi-Fi violation	Success; failed; pending; unsupported; undefined.
SW violation	Success; failed; pending; unsupported; undefined.
Remote Control	CSR Available; CSR Client Not Installed; CSR Client Not Supported; Undefined.
Comment	Free text.
FOTA	Free text.

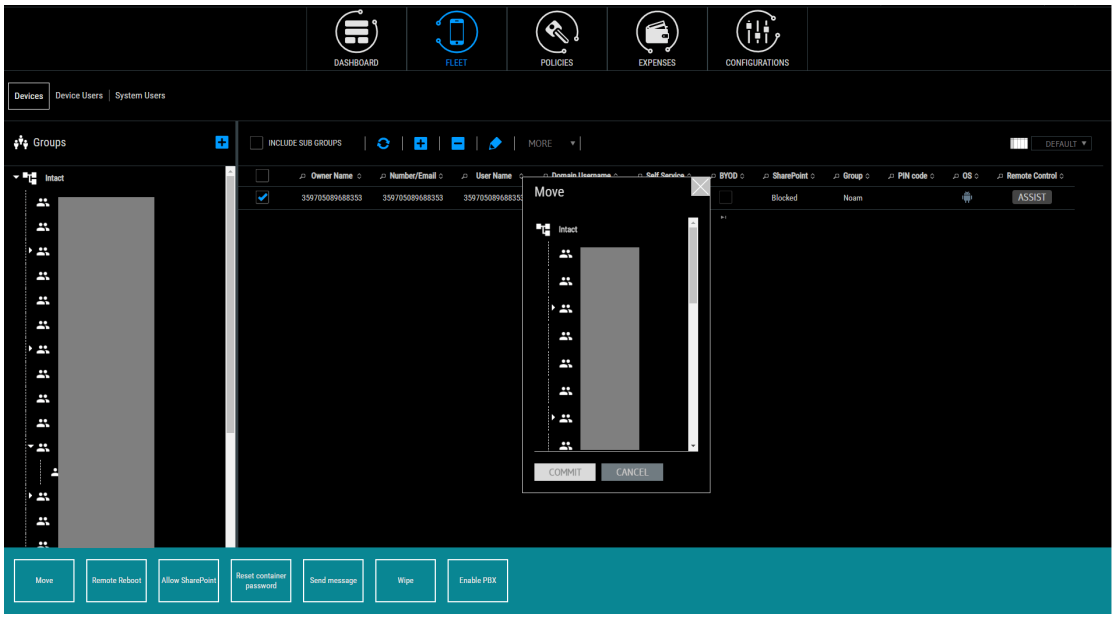
SPECIFIC DEVICE MANAGEMENT



Checking one or more device checkboxes in the devices table allows you quick links to up to four actions:

1. **“Move”** (devices / users).
2. **“Remote Reboot**.”
3. **“Allow / Block SharePoint”** (container access; case sensitive – applicable when a container is defined).
4. **“Reset container password”** (case sensitive – applicable when a SharePoint is defined).
5. **“Send message**.”
6. **“Wipe**.”
7. **“Show password for the device**.” (For revoking APN addresses and enabling APN settings for the user).
8. “**Enable PBX**” (midway secured calls; parent customer admin should enable the service).

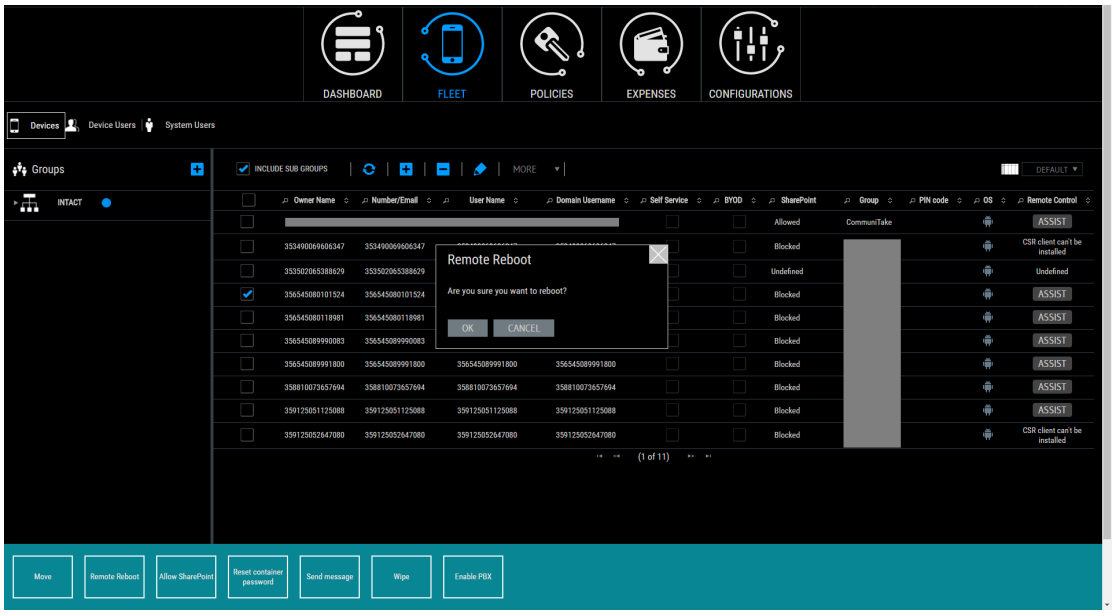
MOVE DEVICES / USERS



"**Move**" allows you to edit the location of devices in the group:

1. Check the device which you wish to edit.
2. Click on the **Move Devices / Users**" at the bottom of the screen.
3. Select the group to which you wish to move the device.
4. Click on "**Commit**".

REMOTE REBOOT



"**Remote Reboot**" allows you to reboot the device from afar:

1. Check the device which you wish to reboot.
2. Click on the "**Remote Reboot**" at the bottom of the screen.

ALLOW SHAREPOINT

"**Allow SharePoint**" enables the device to access the Secure File Container:

1. Check the device which you wish to edit.
2. Click on the **Allow SharePoint**" at the bottom of the screen.
3. The action will generate the process of Secure File container Access enablement.

BLOCK SHAREPOINT

"**Block SharePoint**" removes the device access to the Secure File Container:

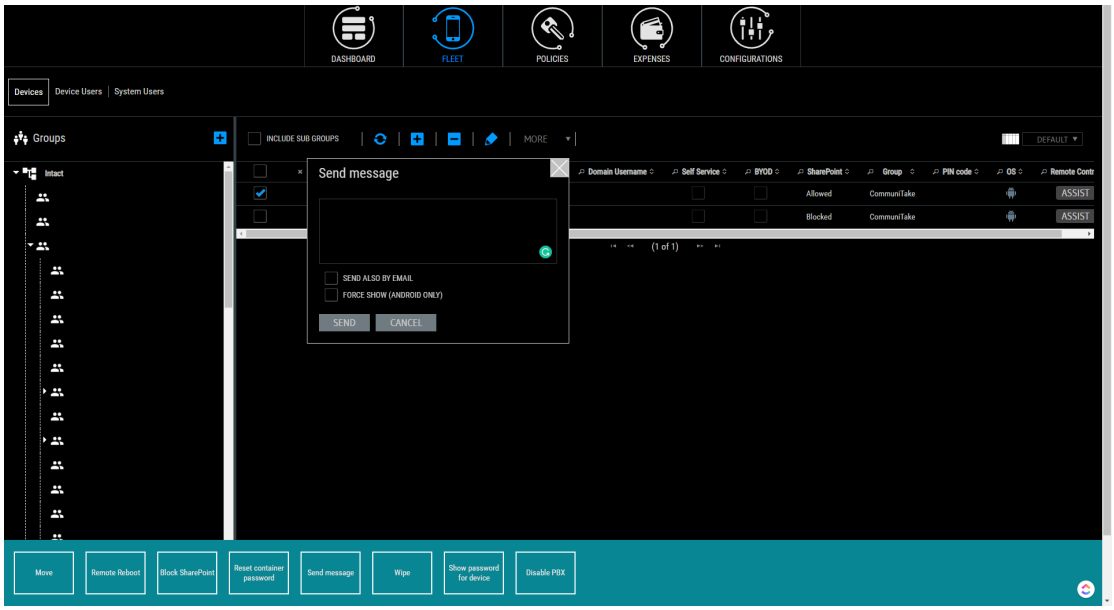
1. Check the device which you wish to edit.
2. Click on the "**Block SharePoint**" at the bottom of the screen.
3. The action will generate the process of removing Secure File container Access.

RESET DEVICE CONTAINER PASSWORD

"**Reset Device Container Password**" initiates new password settings for accessing the Secure File Container:

1. Check the device which you wish to edit.
2. Click on the "**Reset Device Container Password**" at the bottom of the screen.
3. The action will generate the process of resetting the access password to the Secure File Container.

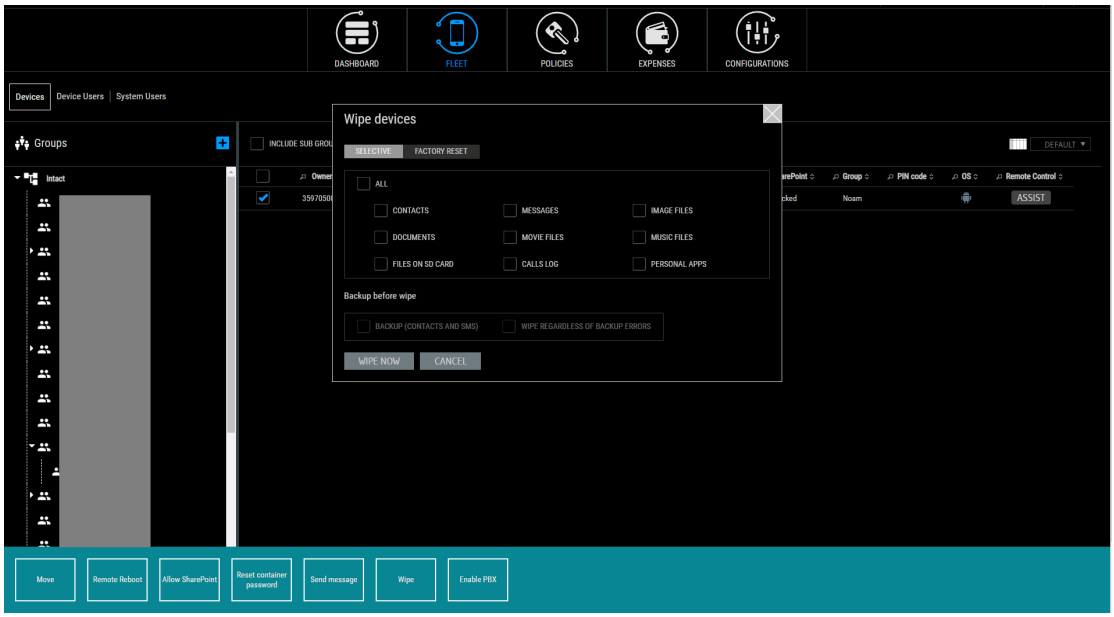
SEND MESSAGE



"**Send Message**" sends a text message to one or more devices:

1. Check the devices to which you wish to send a message.
2. Write the message in the message data field.
3. Select "**Send also by email**" if you wish to send also as an email.
4. Select "**Force show**" if you wish to display the message as a pop-up (For Android only).
5. Click "Send."

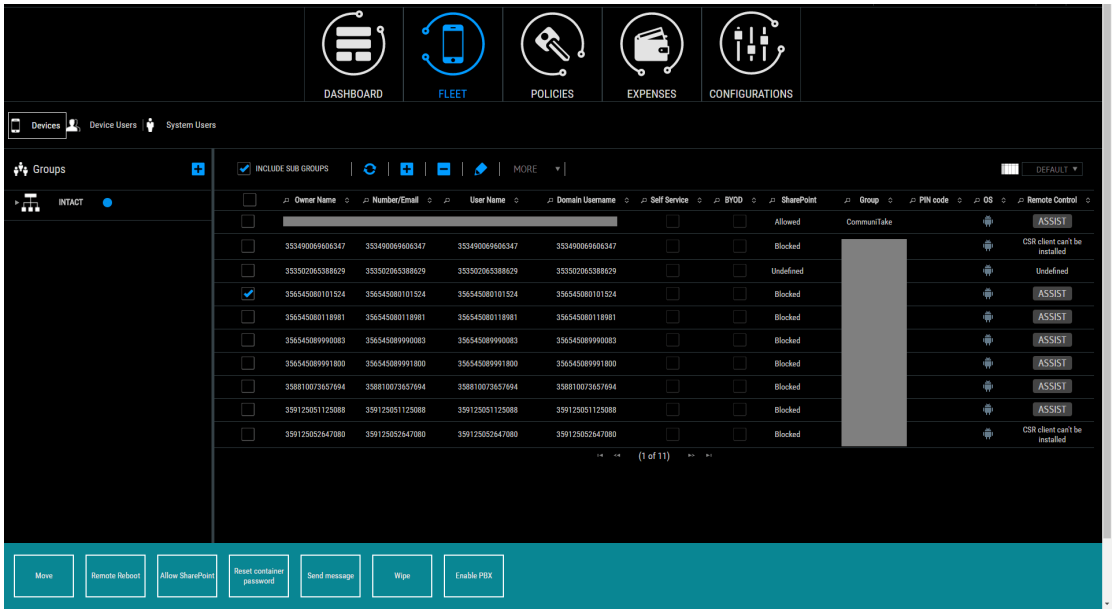
WIPE



"**Wipe**" allows wipe of the device content – complete or selective wipe:

1. Check the device which you wish to wipe.
2. Click on the "**Wipe**" at the bottom of the screen.
3. Check the wipe procedure – either "all" or selected items.
4. Check the requested "**Backup before wipe**" procedure.
5. Click "**Wipe now**". The action will generate the process of resetting the access password to the Secure File Container.

ENABLE PBX

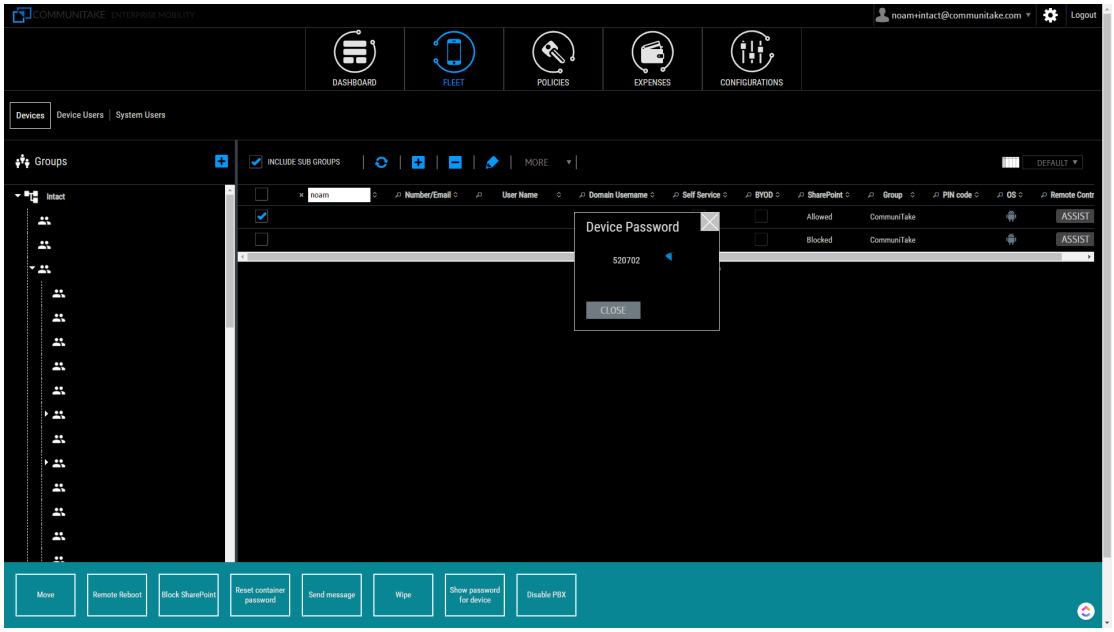


"**Enable PBX**" allows you to perform an outgoing call to any number and the call will be from an unknown or with other number until a number will be attached to that device. It is possible to link the device with a pre-defined MSISDN. This will enable the receiving device to see a calling phone number.

To enable PBX:

1. Check the device which you wish to enable PBX.
2. Click on the "**Enable PBX**" at the bottom of the screen.

SHOW PASSWORD FOR THE DEVICE



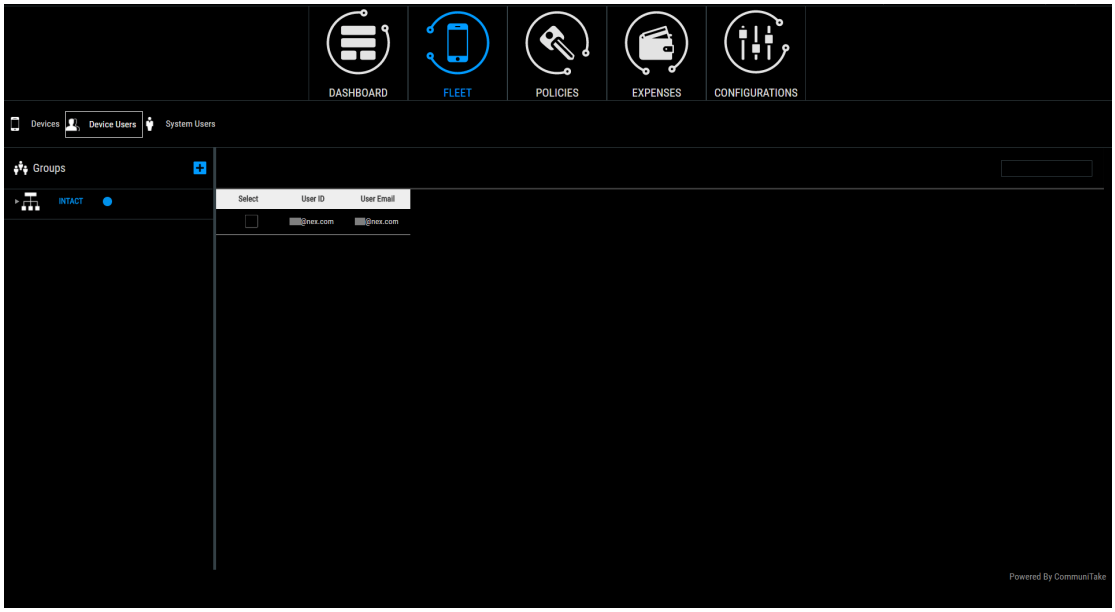
"**Show password for the device**" enables you to recover from a situation where the target device lacks connectivity. Still, the user cannot set a new APN address since the APN policy is blocking the new address

definition. The mechanism behind "**Show password for the device"** allows accessing the on-device Intact app even when there is no connectivity. When the device holder enters the password that is generated via this mechanism, it revokes the APN addresses from the target device and reactivates the APN settings.

To generate a password for the device:

1. Check the device for which you wish to generate a password.
2. Click on the "**Show password for the device"** at the bottom of the screen.
3. The system will automatically generate a password. You are required to communicate this password to the device holder. The device holder will key the password after selecting "**Revoke APNs**" in the Intact app three-dot menu.

DEVICE USERS



Device users are device holders that are allowed to operate device data protection procedures via the system. These procedures include: locate a device on a map; activate a device alarm; lock a device; wipe device data; backup device data.

Once a device is added to a group, its holder is added to the system as a user.

Once a user is defined in the system, he can be identified and authorized to run these procedures. A user is defined in the system by the email address that was defined in the device addition process.

TO DELETE A DEVICE USER

1. Select the device group in which the user is defined.
2. Click on the **"Users"** tab.
3. Check the user line.
4. Click on **"Delete Users"** button.
5. You can select to delete just the user or the user and his/her devices.
6. Deleting the user but not his/her device will result in the device remaining in the group and only the administrator can access it (same as adding a device with no user).

Tip You can add a user after the initial enrollment process. If you wish to enable self-service for device protection, check the "**Self-service access"** box in the devices table or in the edit devices table. This will generate the process to send a welcome email to the device holder through which he can activate his access to self-manage the device protection features.

SYSTEM USERS

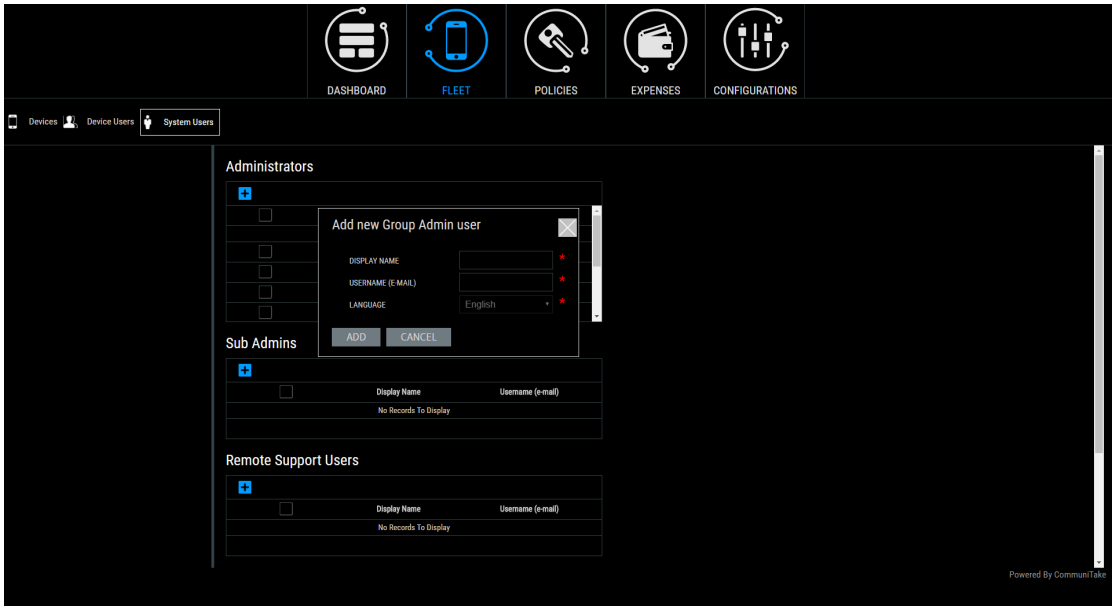
The System **Users** module allows you to add system administrators and Customer Service Representatives (CSR) to the system. Once added, the system will generate for every user a similar account activation process, including sending a welcome letter and a requirement to set a password.

ADMINISTRATORS

Administrators are additional administrators who can manage the system. Administrators have complete administration rights equal to the administrator who has activated the account for the first time.

TO ADD ADMINISTRATORS

1. Select **"System Users"** under the **"Fleet"** tab.
2. Click **"Add"** under the Admin users section.
3. Define the **"Display name"** for the user.
4. Write the **"Username"** (the user's email address).
5. Select the preferred **"Language"**. This will define the welcome letter language.
6. Click **"Add"**.



The new administrator will receive a welcome letter that includes links to the device management application and to the remote support application. Once the newly added user will activate his account by setting his unique

password, he will be able to enter the system with his user name (email address) and the password and perform complete administration tasks.

TO DELETE ADMINISTRATOR

Select "**System Users"** under the "**Fleet"** tab.

1. Select the Administrator you wish to remove.
2. Click on **"Delete"** user.
3. Confirm the action.

SUB ADMINISTRATORS

Sub administrators are additional administrators with lower access privileges who can manage the system. Sub administrators can only view policies and configurations but they cannot change them.

TO ADD SUB ADMINISTRATORS

1. Select **"System Users"** under the **"Fleet"** tab.
2. Click **"Add"** under the Sub Admin users section.
3. Define the **"Display name"** for the user.
4. Write the **"Username"** (the user's email address).
5. Select the preferred **"Language"**. This will define the welcome letter language.
6. Click **"Add"**.

The new sub administrator will receive a welcome letter that includes links to the device management application and to the remote support application. Once the newly added user will activate his account by setting his unique password, he will be able to enter the system with his user name (email address) and the password and perform administration tasks.

TO DELETE SUB ADMINISTRATOR

1. Select "**System Users"** under the "**Fleet"** tab.
2. Select the Sub Administrator you wish to remove.
3. Click on **"Delete"** user.
4. Confirm the action.

TO ADD A REMOTE SUPPORT USER

Remote Support Users are additional users that can perform remote support via device takeover. Remote Support Users have complete device takeover rights but no system administration rights.

1. Select **"System Users"** under the **"Fleet"** tab.
2. Click **"Add"** under the Remote Support users section.
3. Define the **"Display name"** for the user.
4. Write the Username (the user's email address).
5. Select the preferred **"Language"**. This will define the welcome letter language.
6. Click **"Add"**.

The new Remote Support user will receive a welcome letter that includes a link to the remote support application. Once the newly added user will activate his account by setting his unique password, he will be able to enter the system with his user name (email address) and the password and perform remote support tasks.

TO DELETE REMOTE SUPPORT USER

1. Select **"System Users"** under the "**Fleet"** tab.
2. Select the Remote Support user you wish to remove.
3. Click on **"Delete"** user.
4. Confirm the action.

GROUP ADMINISTRATORS

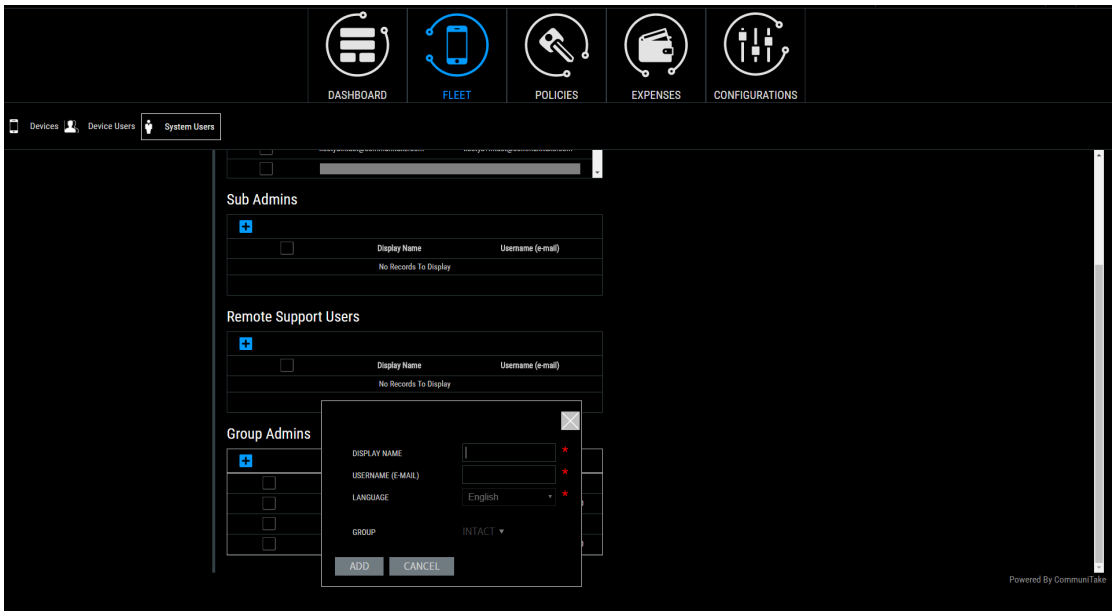
The power system administrator can define administrators for a specific group.

Group administrators can perform the following functionality:

1. Manage the assigned group and its subgroups and members.
2. Define additional group administrators for the group .
3. Manage enterprise mobility features only for the groups that are managed by the administrator.

Group administrators cannot add system or sub-system administrators.

Device users are "read-only" parameter for group administrators.



TO ADD GROUP ADMINISTRATORS

1. Select **"System Users"** under the **"Fleet"** tab.
2. Click **"Add"** under the Group Admins section.
3. Define the **"Display name"** for the user.
4. Write the **"Username"** (the user's email address).
5. Select the preferred **"Language"**. This will define the welcome letter language.
6. Select the group.
7. Click **"Add"**.

The new sub administrator will receive a welcome letter that includes links to the device management application and to the remote support application. Once the newly added user will activate his account by setting his unique password, he will be able to enter the system with his user name (email address) and password and perform group administration tasks.

TO DELETE GROUP ADMINISTRATOR

1. Select "**System Users"** under the "**Fleet"** tab.
2. Select the Group Administrator that you wish to remove.
3. Click on **"Delete"** user.
4. Confirm the action.

Important You cannot delete yourself as an administrator. You can remove only other administrators.
Both the administrator and the Remote Support user can also be device owners. You should simply put in their usernames when adding their device to a group.
A group with an assigned group administrator cannot be deleted.

6

USE POLICIES MANAGEMENT

Device management policies are courses of action and procedures conforming to the philosophy by which the enterprise regards its employees' mobile experience. The system allows the following policies:

1. Password policy: enforcement of on-device password in accordance to the OS capabilities.
2. Blacklist Applications policy: enforcement of on-device prohibited applications.
3. Required Applications policy: enforcement of on-device mandatory applications.
4. Whitelist Applications policy: enforcement of on-device only allowed applications (Android/WP8).
5. Catalog (Recommended Applications) policy: recommended on-device applications.
6. Backup policy: periodic backup of on-device contacts and messages.
7. iOS restrictions.
8. Android restrictions.
9. Browser Control policy.
10. Files Distribution policy.
11. Home Screen policy.
12. Launcher policy.
13. Secure Contacts policy.
14. Application Permissions policy.

PASSWORD POLICY

A password policy defines the following attributes:

Feature	Description
Inherit policy	Automatically implements the parent group password policy on the selected group.
Enable	Enable / disable the password policy.
Minimum password length	The minimum characters number for setting a password.
History length	How many former passwords the system will remember and deny reuse.
How many days between changing passwords	The number of days after which the device holder will be required to change the password.

Number of failed attempts before wiping the device	Number of failed attempts before the device will undergo a factory reset deleting all its data.
How long before the device locks (seconds)	How many seconds of device inactivity before the device is locked.
Complex policy	Automatically implements the complex policy enabled by the device operating system.
Disk encryption	Encrypts the on-device disk data. The device encrypts the user's files, contacts, emails and messages, both on the internal drive and the SD card (if available) using the device's lock password. The encryption key is the device's lock password. The encryption is handled by the operating system itself.

Important Disk encryption requires the following:

- The device should have an access password of at least 8 characters and complex (letters and numbers).
- The device should have 80% battery level or more.
- The device should be wired to a charger.

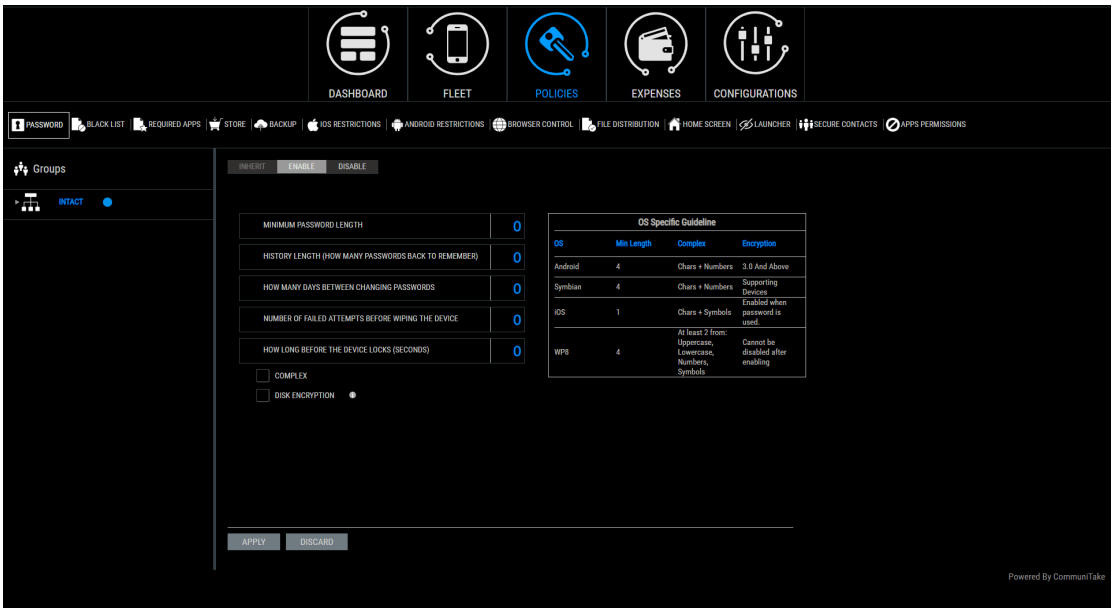
Once activated, the policy will always be active without the ability to stop it.

Once activated, the user will be asked to reboot the device and after reboot, he will be required to key-in a new disk encryption password.

For iOS devices, disk encryption is done automatically when a password is set on the device.

TO DEFINE A PASSWORD POLICY

1. Select the group for which you wish to deploy the password policy.
2. Click on the "**Password Policy"** tab.
3. Define the password attributes parameters.
4. Click on the "**Apply"** button.



TO DISCARD A PASSWORD POLICY

1. Select the group for which you wish to discard the password policy.
2. Click on the **"Password Policy"** tab.
3. Uncheck the "**Enabled"** checkbox.
4. Click the **"Apply"** button.

PASSWORD POLICY ENFORCEMENT

The password policy enforcement varies by the mobile OS:

Criteria / OS	Android	iOS
Minimum length	4	4
History length	Supported	Supported
Expiration	Supported	Supported
Max attempts before wipe	Supported	Supported
Lock timeout	Supported	Supported
Complex	Letters and numbers	Letters, numbers and one symbol which is neither.
Disk encryption	Android 3.0 and above	Enabled automatically when the password is defined.
Enforcement	The user is forced to change the password as soon as the policy reaches the device.	The user is granted a one hour grace period for setting a password. After the

		hour expires, the user is forced to set a password.
Status change in the portal	Status is updated when the password is set.	Device status is queried after an hour. By then the user must set a password.

Important

- Samsung SAFE enabled devices enforce the password via the Samsung SAFE services.
- Adding a device to a group on which a password policy is deployed, will automatically implement the set password policy on the new device.
- The "**Inherit Policy**" check box will be disabled for a group if it does not have a parent group with a set password policy.
- **"Inherit Policy"** always works regardless of the **"Enabled"** status of the parent group. If the parent group password policy is disabled then so will be the child group password policy.
- **"Complex"** relates to the most complex password as defined by the device operating system. This will vary by the operating systems. The device owner will be directed to define the most complex password in the event of password definition.
- Password expiration is supported for Android 3 and above.
- Disk encryption is supported for Android 3.0 devices and above.
- **"OS Specific Guideline"** provides guidelines re possible password complexity, password components and encryption support by the device OS version.

MOBILE APPLICATIONS POLICY

Mobile applications management is conducted via the system application policies. The system allows defining which application must not reside in the device (Blacklist applications); which applications must reside in the device (Whitelist applications); which applications are recommended to reside in the device (Recommended applications).

Mobile applications policy is managed by the enterprise groups. There are three states for managing this policy:

1. **"Inherited":** inherit the parent group applications policy as is.
2. **"Adopt":** inherit the parent group applications policy but allow adding more applications.
3. **"Enable":** do not inherit any policy and allow setting the policy from the very beginning.

To fulfill these policies, the system activates a smart content management mechanism that constantly scans the devices' state and automatically removes or deploys applications by the policies definitions.

BLACKLIST APPLICATIONS POLICY

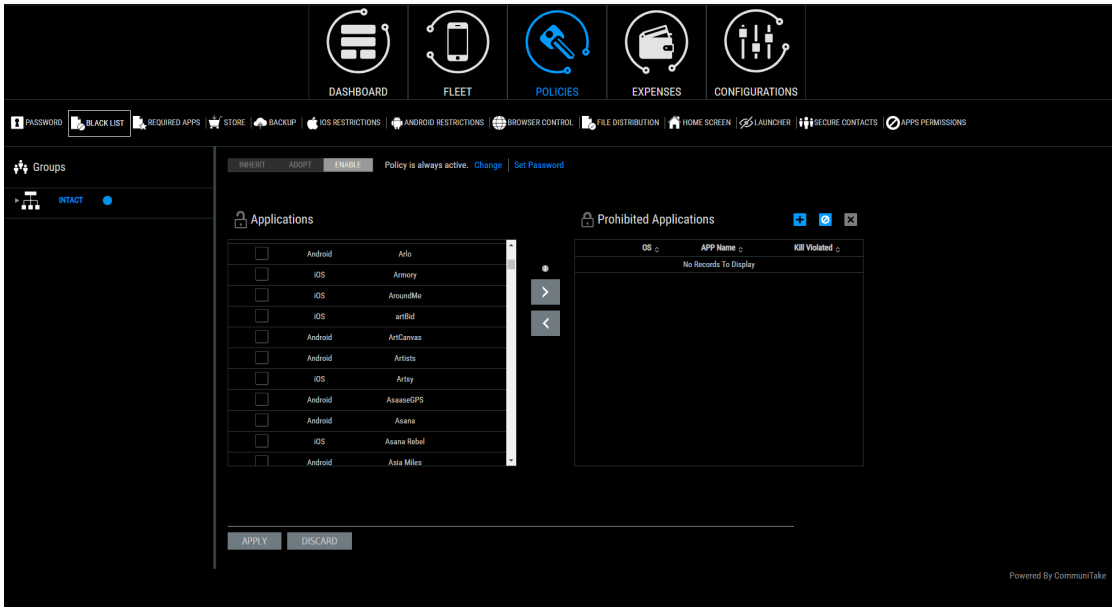
Blacklist applications are on-device applications that are prohibited on the device.

Selecting and defining a prohibited application can be done in two ways:

1. Selecting an application from a pre-built applications list.

2. Manually defining a prohibited application.

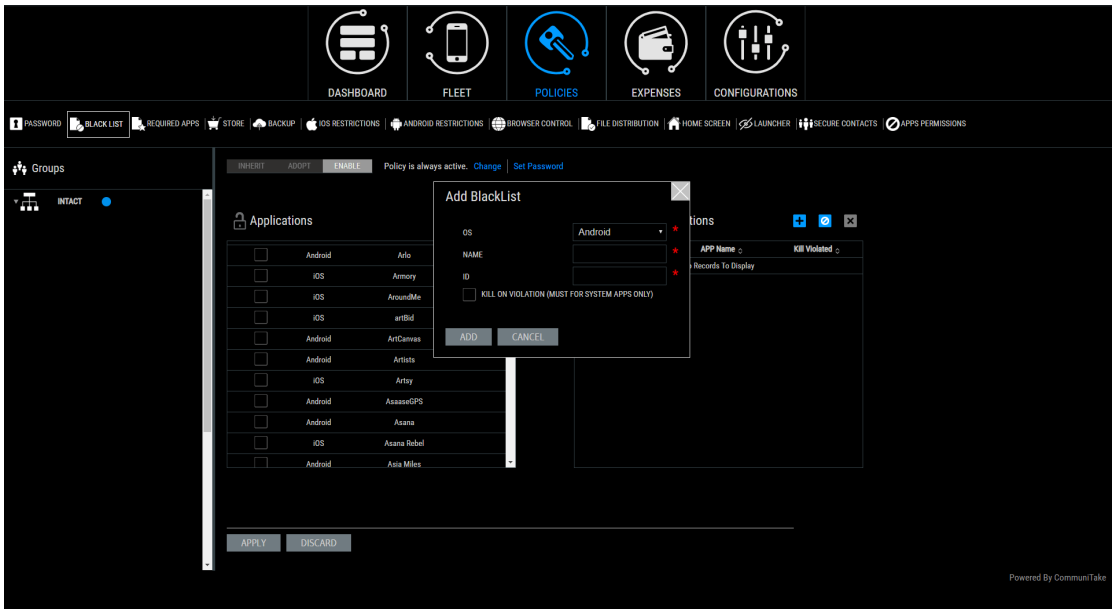
The pre-built applications list is automatically generated by the system as it reviews and collects all the applications that reside on the enterprise devices which are enrolled in the system.



TO DEFINE PROHIBITED APPLICATIONS FROM THE PRE-BUILT APPLICATIONS LIST

1. Select the **“Blacklist”** tab.
2. Select the heritage state. Note that only when selecting **“Do not inherit”** or **“Adopt Inherited”**, the system will present the available applications.
3. Check the selected application checkbox in the applications list.
4. Click on **“Add”** to shift the applications to the prohibited application list.
5. Click **“Submit”**.

TO MANUALLY DEFINE PROHIBITED APPLICATIONS



1. Select the **"Blacklist"** tab.
2. Click on the "**Add Manually"** button.
3. Select the mobile OS from the OS list.
4. Enter the application name.
5. Enter the application ID.
6. Click **"Add"**.
7. Click **"Submit"**.

You have the flexibility to shift between two prohibited applications states:

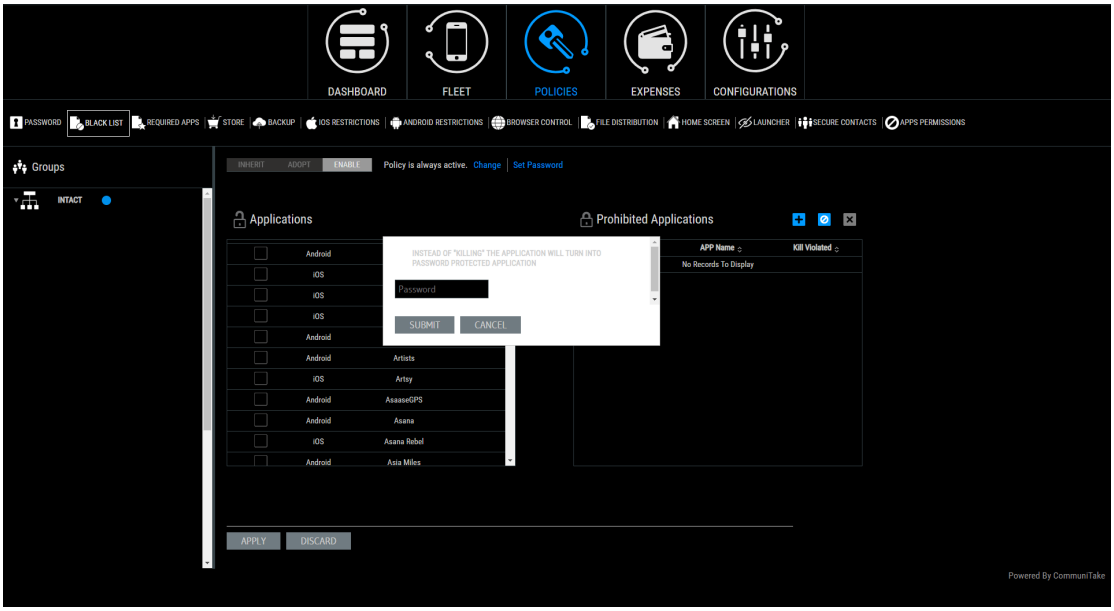
1. Totally prohibited applications.
2. Time / location driven prohibited applications.

To shift between these two states act as follows:

1. Define Blacklisted applications.
2. Define the time or location policy.
3. Click on "**Kill**" to prohibit the application from running by the time / location but allow it to reside on the device. 
4. Click on "**Uninstall**" to totally block the application from running on the device, regardless of time / location policy. 
5. Verify that the "**Kill Violated**" indicate "**Yes**" for kill only and "**No**" for blocking.
6. Click on "**Apply**".

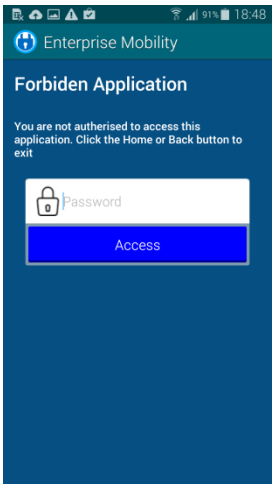
TO DEFINE PASSWORD PROTECTED APPLICATIONS

This module allows you to restrict the activation of on-device applications via a password. The device holder will be required to key-in the password prior to running these applications.

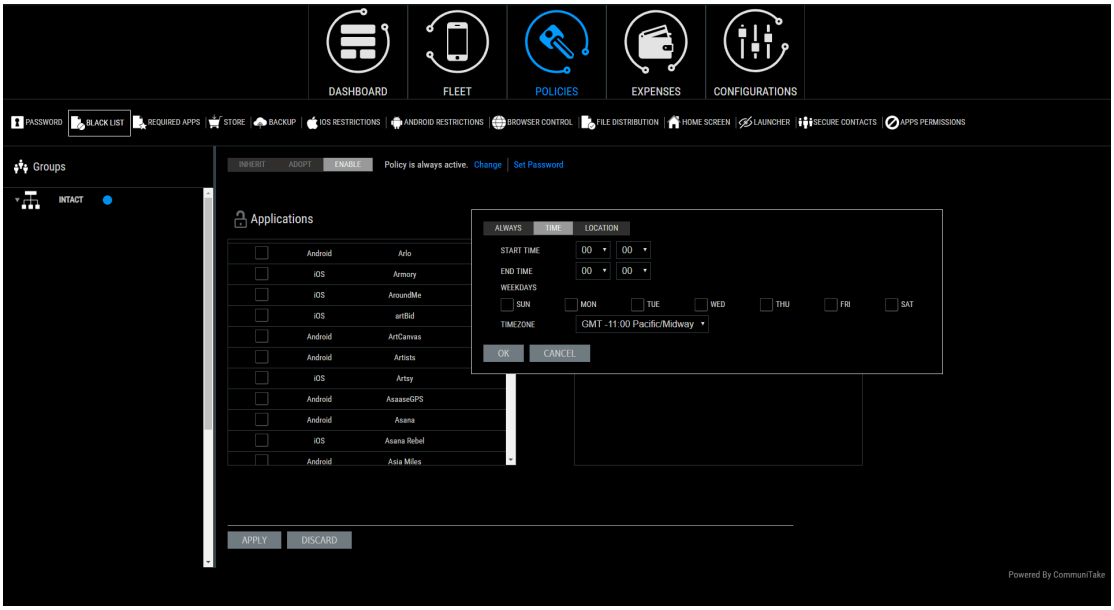


1. Define prohibited applications, as described above.
2. Click on "**Kill**" to prohibit the application from running by the time / location but allow it to reside on the device. 
3. Click on the 'Edit Password' button.
4. Define the password.
5. Click "**Submit**".
6. Click "**Apply"**.
7. To remove the application and switch back to "Kill" mode, you should enter an empty password in step 4.

Device holder's screen for approving a password protected application:



TO ACTIVATE ANDROID BLACKLIST POLICY BY TIME



The default Blacklist policy state is always active, by your definitions. However, you can selectively activate the policy by a specific time of day and week. In this time period and only at this time period, the Blacklist policy will be viable thus allowing prohibited applications to reside on the device but not run under the time policy restrictions. This definition provides you with the flexibility to allocate various policies to devices with different ownership addressing BYOD challenges.

To define time driven Blacklist policy:

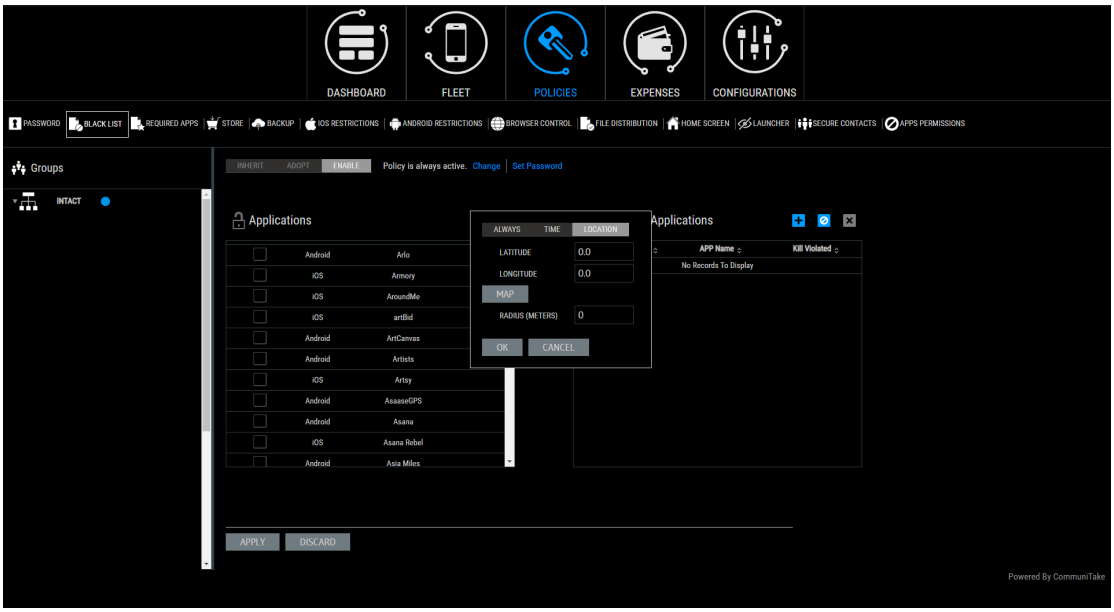
1. Define Blacklist applications.
2. Click on the "**Change**" link near the "**Policy is always active**".
3. Select "**Time**" in the pop-up.
4. Select the start time and the end time in hours and minutes.
5. Select the days of the week.
6. Select the time zone.
7. Click on "**Submit**". Verify that your selection summary appears on the upper Blacklist bar.
8. Click on "**Change**" near the summary if you wish to alter it.
9. Click on the "**Kill**" icon to activate the policy. Verify that the "**Kill Violated**" has turned to "**Yes**".
10. Click on the "**Block**" icon if you wish to uninstall the prohibited application once the policy is violated, regardless of the time policy.
11. Click on "**Apply**".

TO ACTIVATE ANDROID BLACKLIST POLICY BY LOCATION

The default Blacklist policy state is always active, by your definitions. However, you can selectively activate the policy by a specific device location. In this location and only at this location, the Blacklist policy will be viable. To define location driven Blacklist policy:

1. Define Blacklist applications.
2. Click on the "**Change**" link near the "**Policy is always active**".

3. Select "**Location**" in the pop-up.



4. You can define the location in two ways:
    a. Define specifically the latitude and the Longitude
    b. Click on the "**Map**".
        i. You will be shown New York City location as the starting point. Navigate to the desired location and click on the map. The latitude and the Longitude fields will be populated in accordance.
        ii. Define the desired radius in meters in the "**Radius**" field for the selected point location.
5. Click on "**Submit**".
6. Click on "**Apply**".

Important The system by its nature is not a real time system and it depends on the data transmitted by the devices to the cloud service. As such, you may not see immediately all the applications that reside across all the enrolled devices once you log-in to the system. To view all these applications, log-out and log-in again to refresh this view and create a more up-to-date applications list.

Applications are managed by OS. Make sure to define the applications per OS.

Blacklist policy by time and location is valid only to Android devices.

You can define Blacklist viability by location or by time – not by both.

ENFORCEMENT OF PROHIBITED APPLICATIONS

Once an application is defined as a prohibited application, the policy enforcement varies by the mobile OS:

OS	Blacklist enforcement
Android	The system administrator is notified through the violation status in the devices table. For Intact devices, Android Enhanced devices (devices for which CommuniTake has enhanced management capabilities) and Samsung SAFE devices, the application will be automatically removed. This is applicable for most Samsung, LG and HTC devices. For non-Android Enhanced devices, a notification is displayed in the devices notification center prompting the device holder to uninstall the application. The device holder is blocked from using the application. The application should be manually removed by the device holder. This can be done either by clicking the notification or by clicking the application inside the IntactPhone Command Center application under “Blacklist Status”. For Samsung SAFE enabled devices, the prohibited applications will be silently uninstalled.
iOS	The system administrator is notified through the violation status in the devices table. The application should be manually removed by the device holder.

The user can see the Blacklist application status in the on-device application.

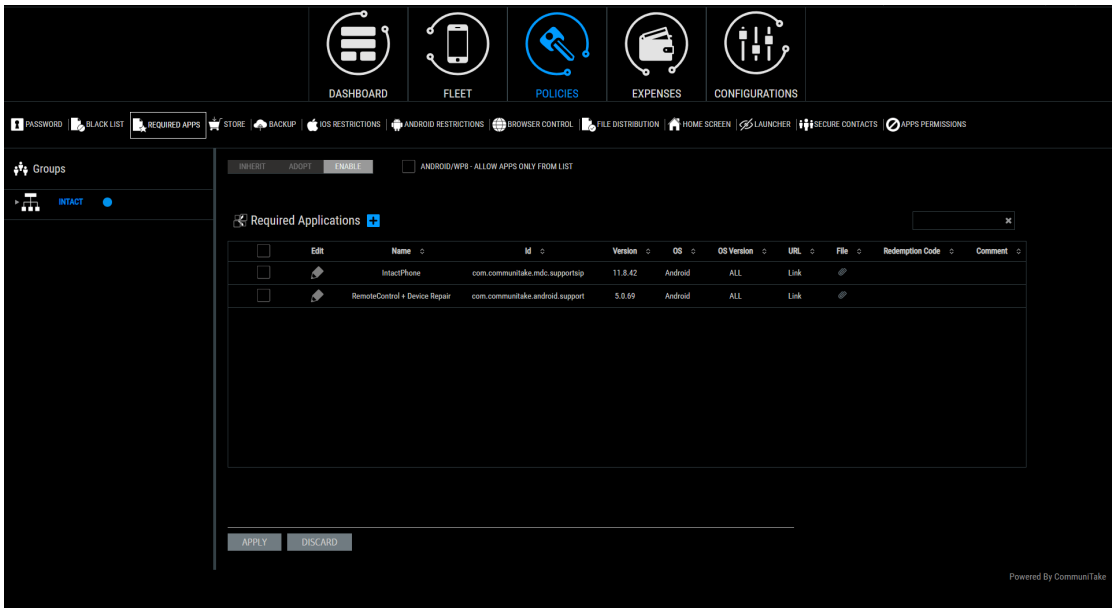
REQUIRED APPLICATIONS POLICY

Required applications policy defines all the mandatory applications that the enterprise expects to have on the device. The Device Management Required Applications function also acts as a smart mechanism for mass deployments and patch management.

The system deploys the mandatory application in two possible ways:

1. Installing the application files on the device.
2. Installing the application via a link to its location in the web / app store.

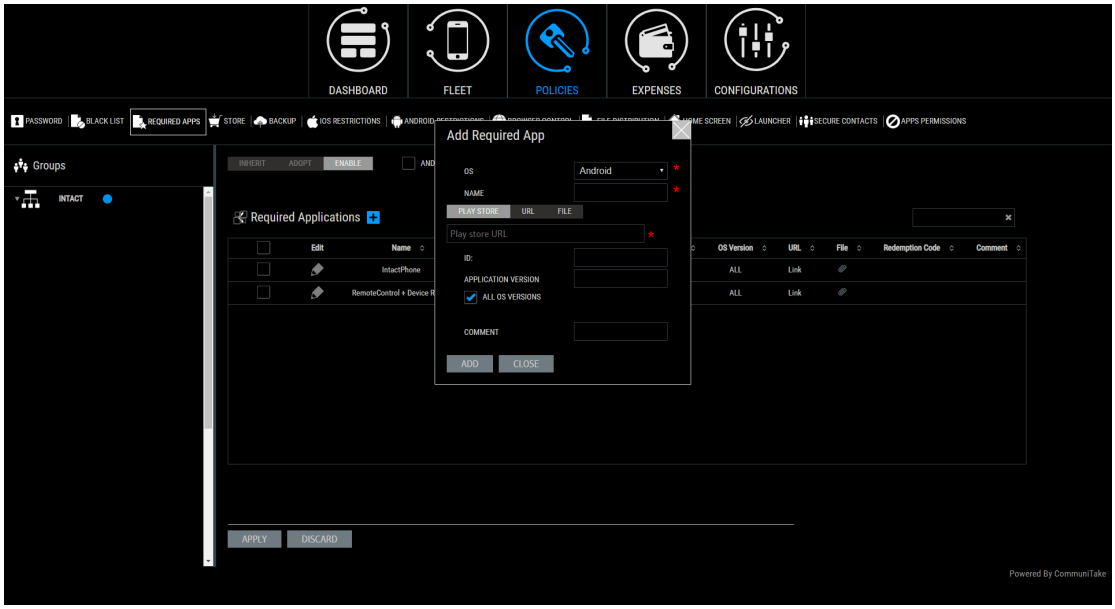
There is a need to indicate in the system one of these two data sources.



Note Required apps: apps retrieval via an external URL allows only HTTPS links.

TO DEFINE MANDATORY APPLICATIONS

1. Select the **"Required Apps"** tab.
2. Click on the **"Add"** button.
3. Select the application OS.
4. Enter the application name.
5. Select the deployment method: Application store; direct download URL; File.
6. Add the deployment parameter by the selected method (Store URL; URL; File).
7. Select the application versions. (The Default is set to All OS Versions).
8. In Android, if selected otherwise, define with the slider the OS versions for which the installation should occur.
9. Add comments (optional).
10. Click **"Add"**.
11. Click on the edit icon near the app for corrections, once required .



Note When adding required apps, the system automatically detects the ID and the version number for Android APKs uploaded to the system. The system automatically detects ID from the Google Play links or from the iOS App Store links.

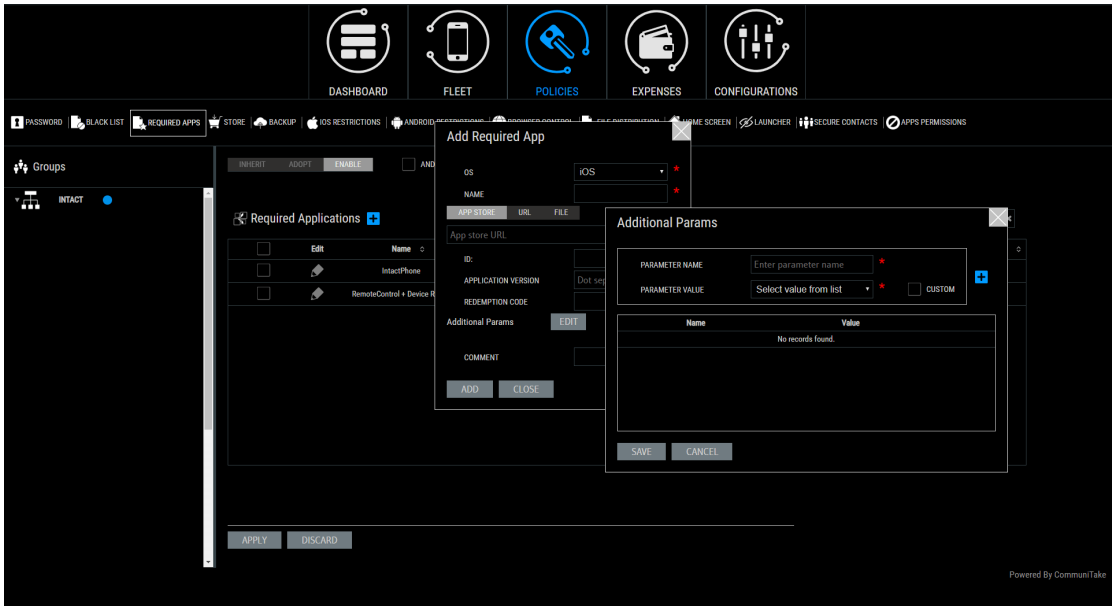
ADDING REQUIRED IOS APPLICATIONS

When adding an iOS application, the system allows you to pass additional parameters as follows:

- System parameters: UDID, Wi-Fi MAC, Bluetooth MAC, Ethernet MAC, MSISDN, IMEI and IMSI.
- User defined static values such as server to connect with, PIN code and more.

To add parameters:

1. Click on the "**Policies**" tab.
2. Click on the "**Required Apps**" tab.
3. Select iOS as the OS.
4. In the process of adding an app, click on the "**Edit**" button.
5. Key-in the parameter name.
6. Select the parameter value.
7. Click on the "**Add**" button.
8. Click on "**Save**".



Note iOS added parameters are also applicable when adding recommended apps.

ENFORCEMENT OF MANDATORY APPLICATIONS

Once an application is defined as a mandatory application, the policy enforcement will vary by the mobile OS:

OS	Required Apps enforcement
Android	The system administrator is notified through the violation status in the devices table. A notification is displayed on the device's notification center prompting the user to install the application. The application should be manually installed by the device holder. This can be done either by clicking the notification or by clicking the application inside the IntactPhone Command Center application under "Required Apps Status". For Intact devices, Samsung SAFE enabled devices, and Android Enhanced devices (devices for which CommuniTake has improved management capabilities), required APK files will be silently installed. The files should be uploaded to the system or should contain direct download links. In any case, Google Play applications must be manually installed by the user.
iOS	The system administrator is notified through the violation status in the devices table. The application is automatically installed on the device. The user may be prompted to enter his / hers iTunes password.

IOS 'IN-HOUSE' APPLICATIONS DISTRIBUTION

The system allows distribution of Ad-Hoc in house applications to iOS devices. These devices must be managed inside the provisioning profile used to sign the application. Once built and signed, the iApp file can either be uploaded directly to the system or a link can be provided to an internet location where the file can be downloaded from.

ANDROID WHITELIST APPLICATIONS POLICY

Whitelist applications policy defines the applications that the enterprise allows to run on an Android device.

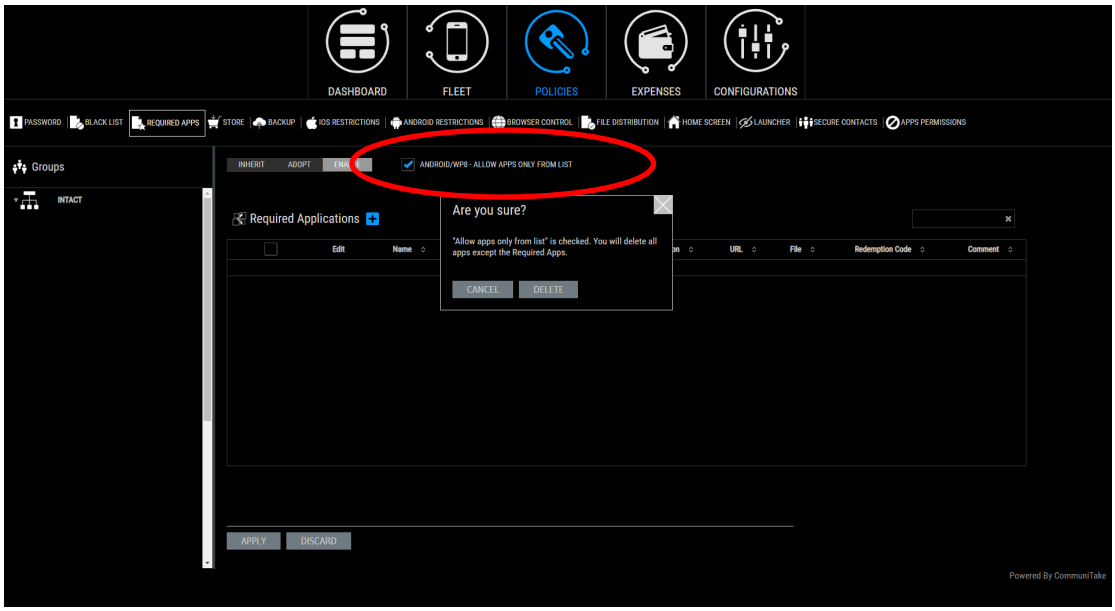
No other applications can run on the device once this policy is set.

TO ENABLE WHITELIST MODE FOR ANDROID DEVICES

1. Check the checkbox "**Android – allow apps only from whitelist".**
2. Click **"Apply".**

Once applied, all Android "required" applications now define the Whitelist apps:

- These applications are mandatory on the device.
- These applications are the only 3rd party applications which are allowed to run on the device.



ENFORCEMENT OF WHITELIST APPLICATIONS

The system administrator is notified through the violation status in the devices table. A notification is displayed in the devices notification center prompting the device holder to uninstall the not allowed application. The device holder is blocked from using applications that were not defined as allowed. The system will 'kill' any not allowed application from running. The prohibited application should be manually removed by the device holder.

This can be done either by clicking the notification.

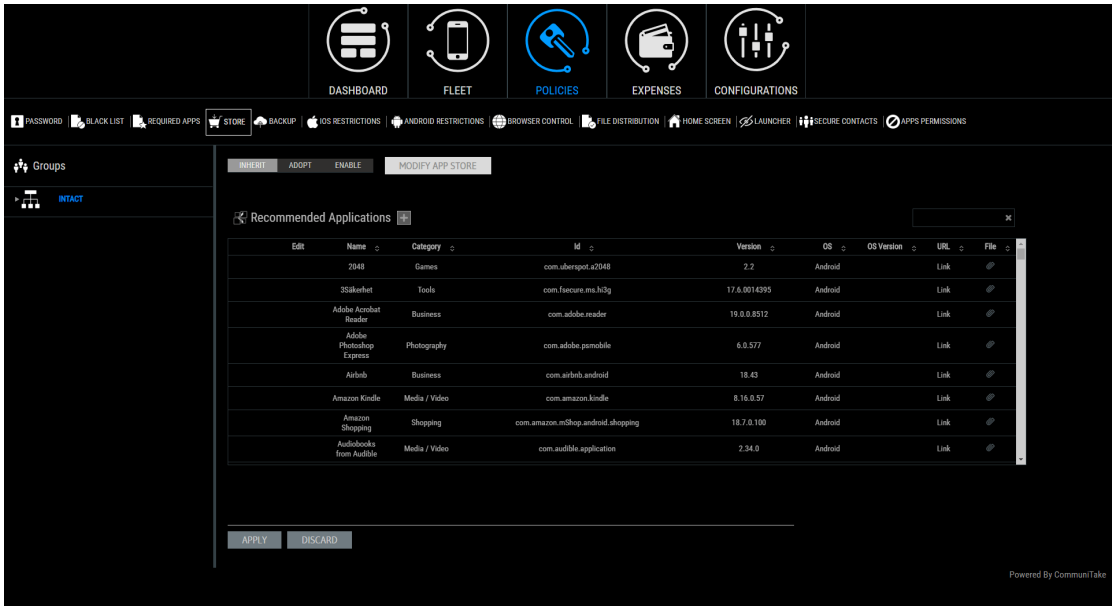
On Samsung SAFE and Android Enhanced devices, applications which are not part of the whitelist will be silently uninstalled.

STORE POLICY

CommuniTake Technologies centrally defines the Global App Store. The Global App Store comprises default applications that have been inserted by CommuniTake Technologies. Store policy enables system admins to determine the recommended applications which the business wishes to allow on the devices without enforcing their presence.

CommuniTake Technologies, per customer's directives, can initially customize global App Store. Once defined, the customer can manage the app store content and its sync with the central app store uploads.

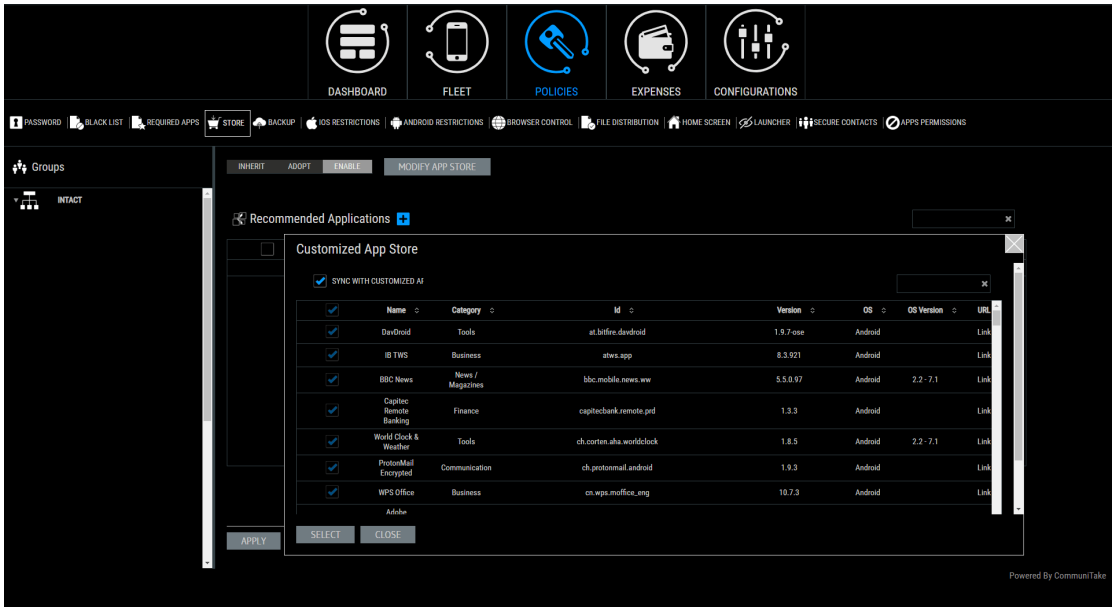
An on-device enterprise app store displays the available applications from which device holders can download and install them.



The system administrator can select from the Global App Store the custom store apps that will be available for his organization.

To custom your organizational app store from the global app store:

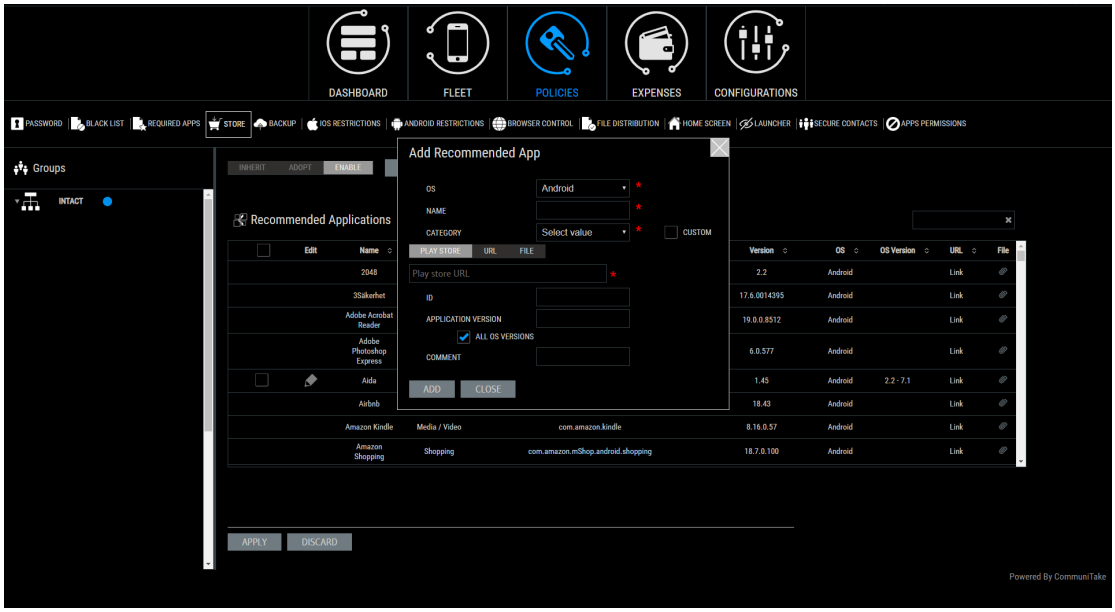
1. Select the "**Store**" tab.
2. Click on "**Modify App Store**" tab.
3. Check the required applications that you wish to make available to employees.
4. Click on "**Select**"
5. Click on "**Apply**"



System admin can define automated synchronization between the Global App Store and the custom organizational app store. The automatic sync feature seamlessly adds apps to the organizational App Store, once CommuniTake Technologies adds apps the central app store, without the need to proactively add them.

To enable automated synchronization between the Global app store and the custom organizational app store:

1. Click on the "**Store**" tab.
2. Check "**Modify App Store**"
3. Check "**Sync with Global App Store**."
4. Check the required applications, if needed.
5. Click on "**Select**"
6. Click on "**Apply**."



To add a new recommended app to the app store that does not exist in the Global App Store:

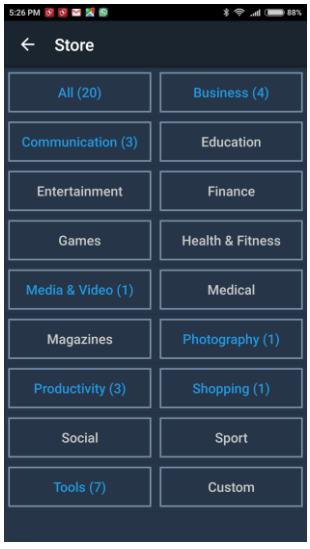
1. Select the "**Store**" tab.
2. Click on the "**Add**" (plus) button.
3. Select the application OS.

4. Enter the application name.
5. Select the deployment method: Application store; direct download URL; File.
6. Add the deployment parameter by the selected method (Application store URL; URL; File).
7. Select the application versions. (The Default is "All OS Versions").
8. In Android, if selected otherwise, define with the slider the OS versions for which the installation should occur.
9. Add comments (optional).
10. Click "**Add**."

Note Note The system automatically detects the ID, and the version number for Android APKs uploaded to the store when adding catalog apps. The system automatically detects ID from the Google Play links or from the iOS App Store links.
Recommended apps: apps retrieval via an external URL allows HTTPS only links.
Click on the Edit icon near the app for corrections, once required.

Once the recommended application is defined, the device holder will be able to view all the recommended application on his / her device via the application client. The user can select to install the apps directly from the on-device apps list.

User view of the on device app store

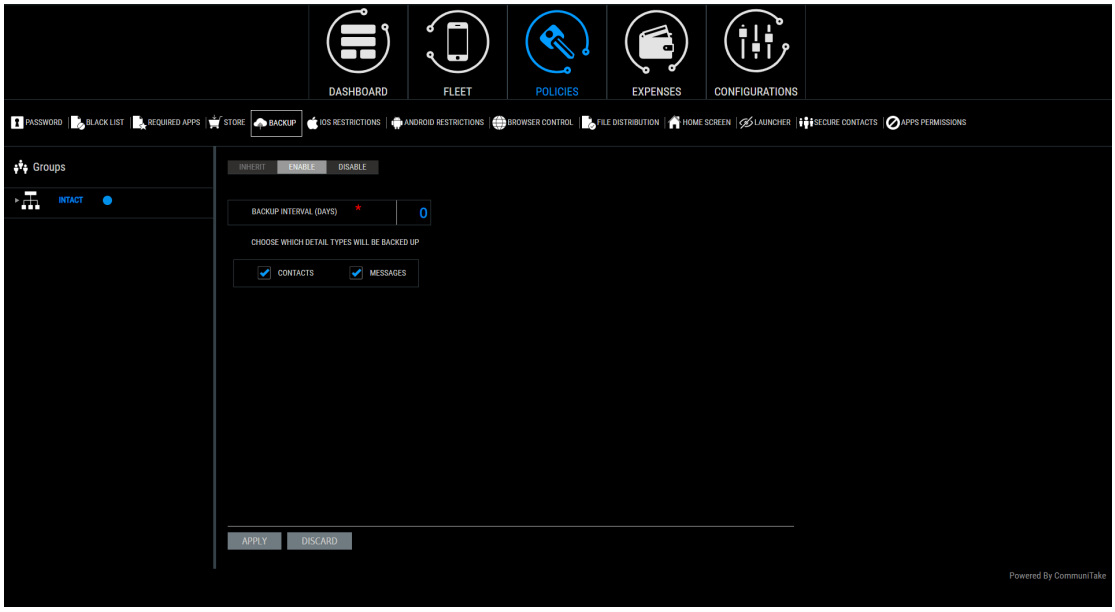


BACKUP POLICY

TO DEFINE BACKUP SETTINGS

1. Select the device group for which you wish to deploy the backup settings.
2. Click on the "**Backup"** tab.
3. The default selection is **"Inherit Backup Settings"**.
4. Check the **"Enable Periodic Backup"** checkbox (uncheck the default settings).

5. Define the number of days for the **“Backup Interval**”.
6. Select which data detail types will be backed up: Contacts; Messages; Note that Contacts and Messages are pre-defined once you mark the Enable Periodic Backup checkbox.
7. Click on **“Commit Changes”**.

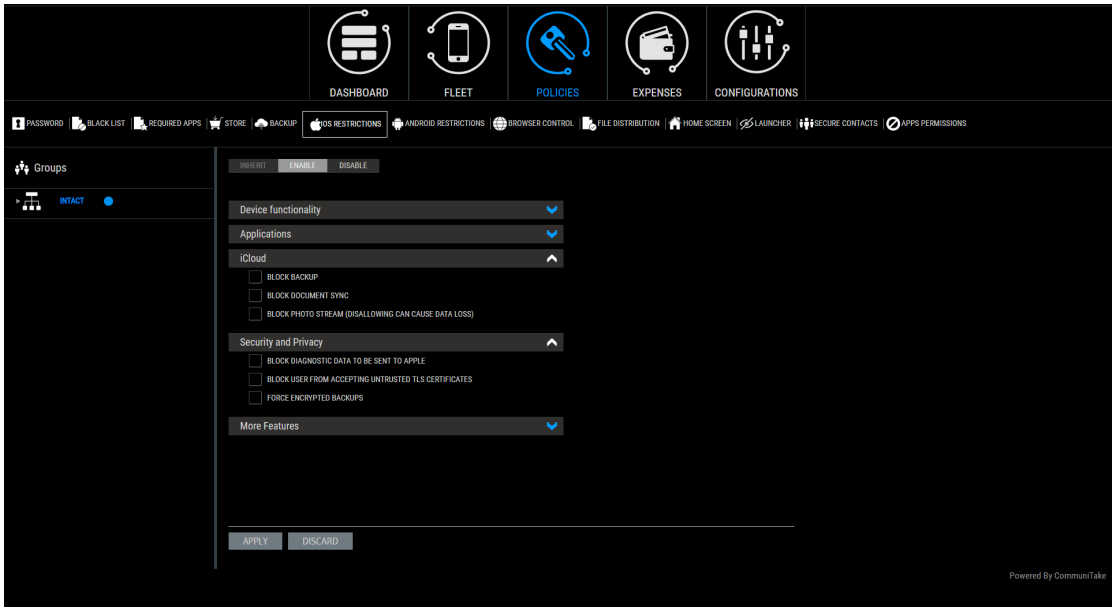


TO REMOVE BACKUP SETTINGS

1. Select the device group for which you wish to remove the backup settings.
2. Click on the **“Backup”** tab.
3. Uncheck the **“Enable Periodic Backup”** checkbox.
4. Click on **“Commit Changes”**.

Tip The default policy is the inherit policy by the parent group. In order to select another policy, first uncheck the inherit checkbox and then check the enable checkbox and define the policy parameters.

IOS RESTRICTIONS CONFIGURATION



The iOS restrictions module allows you to limit user's access to services.

Optional configuration for iOS restrictions:

Device functionality

- Block Installing Apps
- Block Camera
    - Block Facetime
- Block Screen Capture
- Block Automatic Sync While Roaming
- Block SIRI
- Block Voice Dialing
- Block In-App Purchase
- Do Not Force User To Enter Itunes Store Password For All Purchases
- Block Multiplayer Gaming
- Block Game Center Friends
- Block Assistant While Device Is Locked
- Block Installing UI Configuration Profile
- Block Using of Shared Streams

Applications

- Block use of Itunes store
- Blocks Use of Safari
    - Enable Autofill
    - Do Not Force Fraud Warning
    - Block Javascript
    - Block Pop-Ups
    - Do Not Accept Cookies (Never; From visited sites; Always)
- Block User From Using Passbook While Device Is Locked

- Block User From Using GameCenter
- Block User From Using Bookstore
- Block User From Accessing Erotica In Bookstore

iCloud

- Allow backup.
- Allow document sync.
- Allow Photo Stream (disallowing can cause data loss).

Security and Privacy

- Allow diagnostic data to be sent to Apple.
- Allow user to accept untrusted TLS certificates.
- Force encrypted backups.

More Features

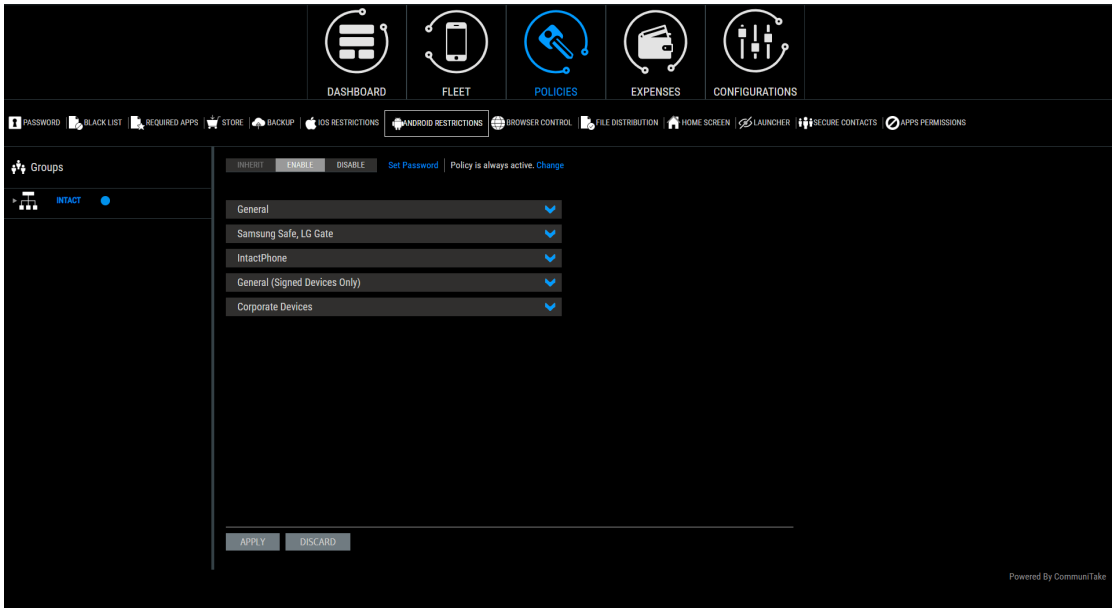
- Block Account Modification
- Block Air Drop
- Block App Cellular Data Modification
- Block Assistant User Generated Content
- Block Find My Friends Modification
- Block Fingerprint For Unlock
- Block Host Pairing
- Block Lock Screen Control Center
- Block Lock Screen Notifications View
- Block Lock Screen Today View
- Block Open From Managed To Unmanaged
- Block Open From Unmanaged To Managed
- Block OTA PKI Updated
- Do Not Force Limit Ad Tracking

To define iOS restrictions:

1. Select the devices group for which you wish to define iOS restrictions.
2. Click on the **"Policies"** tab.
3. Click on the "**iOS Restrictions"** tab.
4. Select the heritage behavior.
5. Check the required restrictions.
6. Click on **"Apply"**.

Important The implication of activating a restriction: for example, disabling the camera will cause the camera application to disappear from the device.

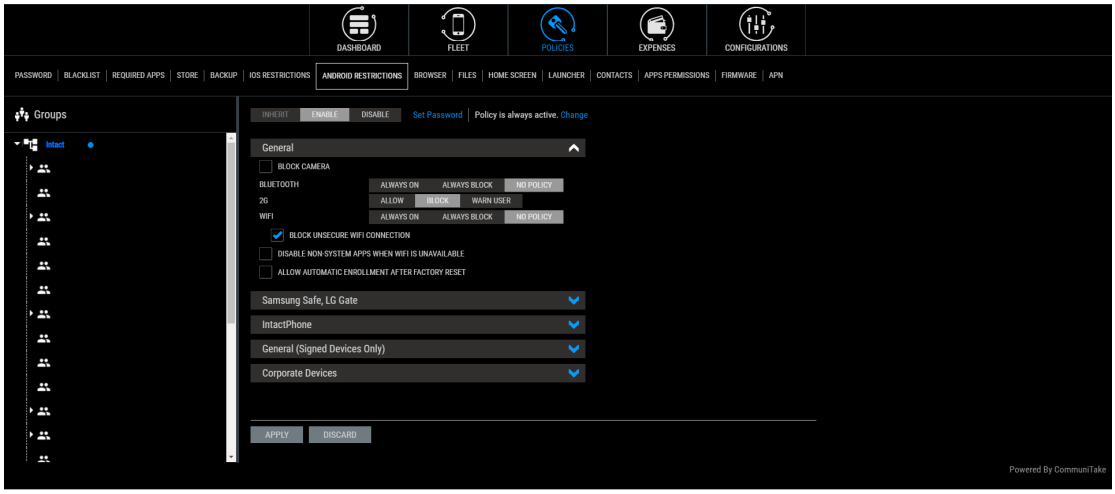
ANDROID RESTRICTIONS CONFIGURATION



The Android restrictions module allows you to limit user's access to services. These limitations defer by device type. There are five different device types which allow distinctive restrictions:

1. Generic Android devices.
2. Samsung SAFE, LG Gate devices.
3. Devices containing the IntactPhone secure firmware (IntactOS).
4. Devices containing enhanced management capabilities – namely non-SAFE Samsung, LG, HTC and newest Sony devices (Samsung SAFE does not require downloading the extra component).
5. Corporate Devices - Devices containing the IntactPhone secure firmware (IntactOS) seamlessly support these restrictions. Commercial non-IntactOS devices require installing a dedicated APK.

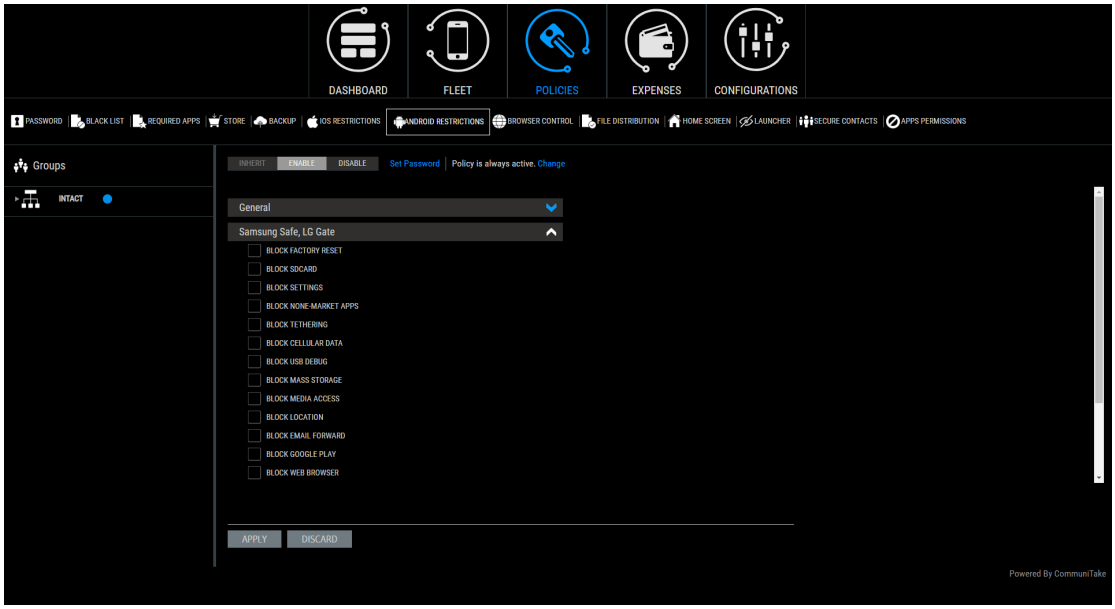
GENERIC ANDROID DEVICE RESTRICTIONS



Optional configuration for generic Android restrictions:

- Block Camera.
- Bluetooth: “**Always on”** or “**Always block”** or “**No policy”**.
- 2G: “**Allow”** or ‘**Block’** or “**Warn user”**.
    - The 2G policy prevents or warns the device holder once a voice call (incoming or outgoing) is conducted over an unsecure 2G network. It can allow the device, or totally block a call once on 2G or warn the user through pop-up message and a beep sound during the call.
- Wi-Fi: “**Always on”** or “**Always block**” or “**No policy”**.
- “**Block unsecured Wi-Fi connections**”. Block connections to Wi-Fi networks which are not encrypted. Unencrypted Wi-Fi networks allow easy interception of data sent to / from the device.
- “**Disable Non-System Apps when Wi-Fi is not available**”.
- **“Allow automatic enrollment after factory reset”.** Automatic enrollment of the device after a factory reset procedure without any need to proactively re-enroll the device.

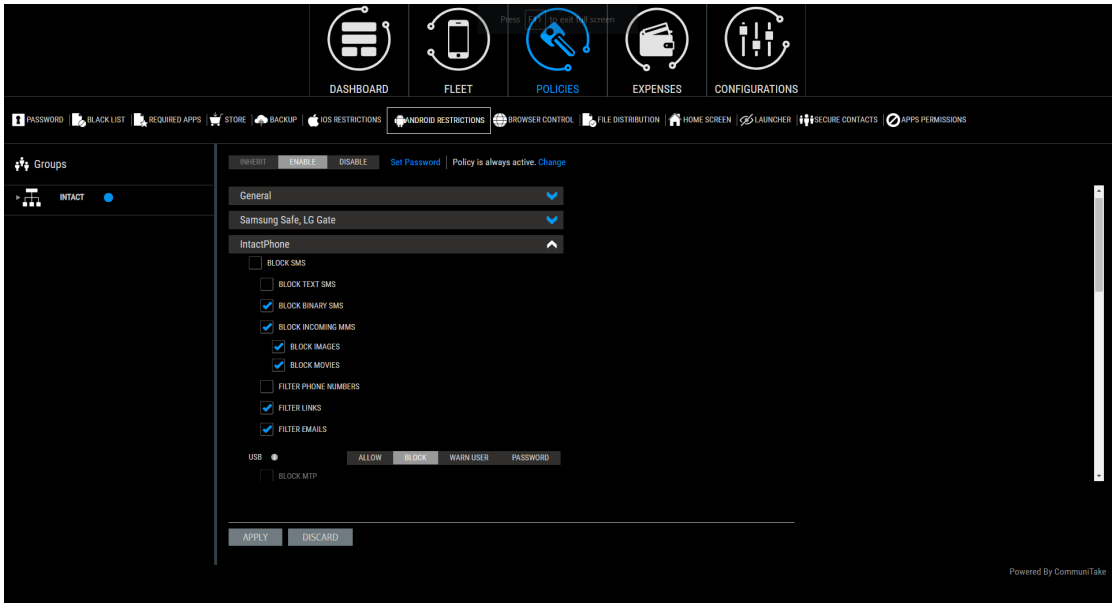
SAMSUNG SAFE LG GATE DEVICE RESTRICTIONS



Optional restrictions for Samsung SAFE and LG Gate devices:

- Block Factory Reset
- Block SDcard
- Block Settings
- Block None-Market Apps
- Block Tethering
- Block Cellular Data
- Block USB Debug
- Block Mass Storage
- Block Media Access
- Block Location
- Block Email Forward
- Block Google Play
- Block Web Browser
- Block YouTube

INTACTOS FIRMWARE RESTRICTIONS



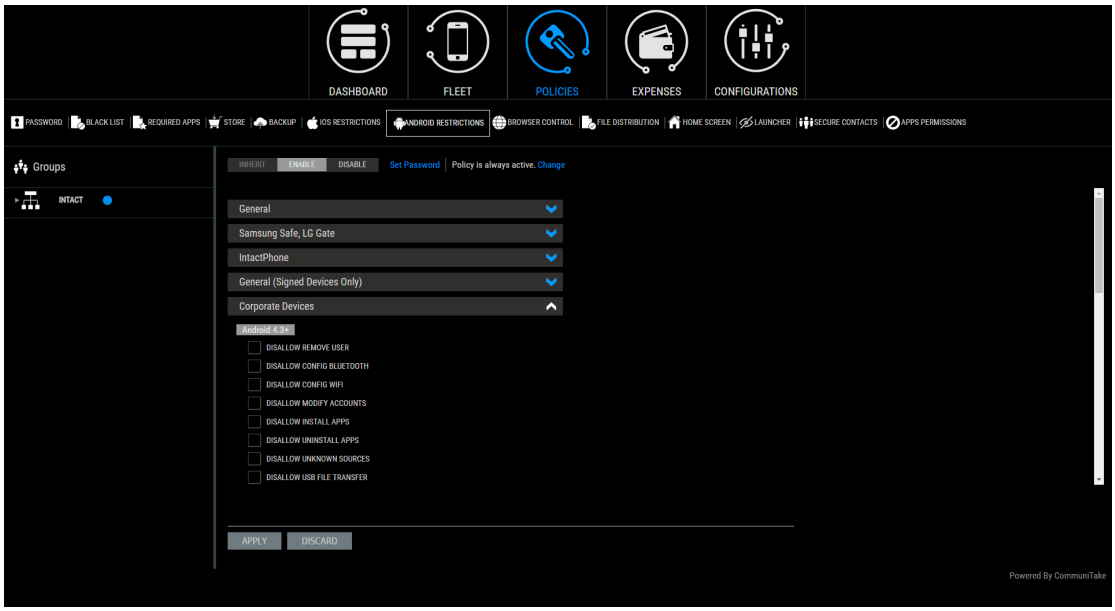
Android use restrictions for the IntactOS consist of the following protection feature-set:

- Lock SMS
  - Block Text SMS
  - Block Binary SMS
- Block Incoming MMS
  - Block Images
  - Block Movies
- Filter Phone Numbers
- Filter Links
- Filter Emails
- USB access: **“Allow”; “Block”; “Warn user”; “Password”**
  - Block Media Transfer Protocol (MTP).
  - Block Picture Transfer Protocol (PTP).
  - Block Android Debug Bridge (ADB).
- Conference Call: **“Allow”; “Block”; “Warn user”.**
  - Beep on conference call.
- Access to Microphone: **“Allow”; “Block”; “Warn user”.**
  - Concurrent application access (to microphone): **“Single”; “Multiple”**.
    - Beep on microphone access.
- Camera: **“Allow”; “Block”; “Warn user”. (**The application that uses the camera has no indication that the camera is blocked).
- NFC / HotKnot: **“Allow”; “Block”; “Momentary”.** The momentary state disables the NFC immediately after it was used.
- Block Factory Reset.
- Block Mobile Data.
- Block Voice.
- Enable Wi-Fi MAC Address Spoof.

- Block App Installation (Password Supported).
- Bluetooth Whitelist. Allowing the device to connect only to explicitly approved Bluetooth devices.
- Block adding device administrators.
- Block installing root certificate Authority (CA) certificates.
- Screen capture control (Enable; Disable; Ask user).
- SD Card encryption (Allow; Block; Encrypted only).
- Block Accessibility.
- Disable access to OS codecs / parsers
    - Block images (config.).
    - Block audio (config).
    - Block video (config).
- Google Play (Always On; Always Block; No Policy)
- Block notifications.

Important When activating the encryption on the SD card, all existing on-card data will be erased. The encryption will be applicable only for data that was added to the SD card after the encryption act. On-SD card encrypted data will only be readable via the device. The same restrictions are applicable when the SD card is decrypted: when activating the decryption on the SD card, all existing on-card data will be erased. The decryption will be applicable only for data that was added to the SD card after the decryption act.

ANDROID ENHANCED DEVICE RESTRICTIONS



Android Enhanced devices are devices for which CommuniTake has obtained improved management capabilities. This is applicable for most Samsung, LG, HTC and the newest Sony devices.

Optional configuration for Android Enhanced devices include:

- Block GPS: **“Always on”; “Always block”; “No policy”.**
- Roaming: **“Always on”; “Always block”; “No policy”.**
- Unknown sources: **“Always on”; “Always block”; “No policy”.**

- Block USB Debug.
- Block Airplane Mode.
- Mobile Data: **“Always on”; “Always block”; “No policy”.**

ANDROID CORPORATE DEVICES RESTRICTIONS

Corporate Devices-derived restrictions leverage generic Android built-in capabilities. Supported features differ between Android OS versions hence the restriction differences between operating system versions. The commercial Android device should run version 7.0 and higher to support Corporate Devices restrictions.

For devices running Android 7+ operating system:

- Disallow Remove User.
- Disallow Config Bluetooth.
- Disallow Config Wi-Fi.
- Disallow Modify Accounts.
- Disallow Install Apps.
- Disallow Uninstall Apps.
- Disallow Unknown Sources.
- Disallow USB File Transfer.
- Disallow Add User.
- Disallow SMS.
- Disallow Config Mobile Networks.
- Disallow Config Tethering.
- Disallow Config VPN.
- Disallow Debug Features.
- Disallow Factory Reset.
- Disallow Mount Physical Media.
- Disallow Outgoing Calls.
- Disallow Apps Control.
- Disable Accessibility Services.
- Disallow Safe Boot.
- Disable Status Bar.
- Disallow Data Roaming.
- Disallow Set Wallpaper.

For devices running Android 8+ operating system

- Disallow Bluetooth.
- Disallow Bluetooth Sharing.

For devices running Android 9 operating system+

- Disallow Airplane Mode.
- Disallow Config Brightness.
- Disallow Config Date Time.
- Disallow Config Locale.

- Disallow Config Location.
- Disallow Config Screen Timeout.
- Disallow Printing.

TO DEFINE ANDROID RESTRICTIONS

1. Select the devices group for which you wish to define Android restrictions.
2. Click on the **"Policies"** tab.
3. Click on the "**Android Restrictions"** tab.
4. Select the heritage behavior.
5. Select the restrictions by the Android device type.
6. Check the required restrictions and define the passwords, once required.
7. Click on **"Apply"**.

For Samsung SAFE enabled devices, the Android restrictions are implemented via the SAFE services.

TO DEFINE ANDROID RESTRICTION BY TIME

The default Android Restrictions policy state is always active, by your definitions. However, you can selectively activate the policy by a specific time of day and week. In this time period and only at this time period, the Android Restrictions policy will be viable. This definition provides you with the flexibility to activate security restrictions that are viable to work hours for example. To define time driven Android Restrictions policy:

1. Define Android Restrictions policy.
2. Click on the "**Change**" link near the "**Policy is always active**".
3. Select "**Time**" in the pop-up.
4. Select the start time and the end time in hours and minutes.
5. Select the days of the week.
6. Select the time zone.
7. Click on "**Submit**". Verify that your selection summary appears on the upper policies bar.
8. Click on "**Change**" near the summary if you wish to alter it.
9. Click on "**Apply**".

TO DEFINE ANDROID RESTRICTION BY LOCATION

The default Android Restrictions policy state is always active, by your definitions. However, you can selectively activate the policy by a specific device location. In this location and only at this location, the Android Restrictions policy will be viable. This can be valuable when you wish to block security breaches of unauthorized data collection in the organization premise. To define location driven Android Restrictions policy:

1. Define Android Restrictions policy.
2. Click on the "**Change**" link near the "**Policy is always active**".
3. Select "**Location**" in the pop-up.
4. You can define the location in two ways:

a. Manually define the latitude and the Longitude
b. Or click on the "**Map**" to locate your location.
    i. You will be shown New York City location as the starting point. Navigate to the desired location and click on the map. The latitude and the Longitude fields will be populated in accordance.

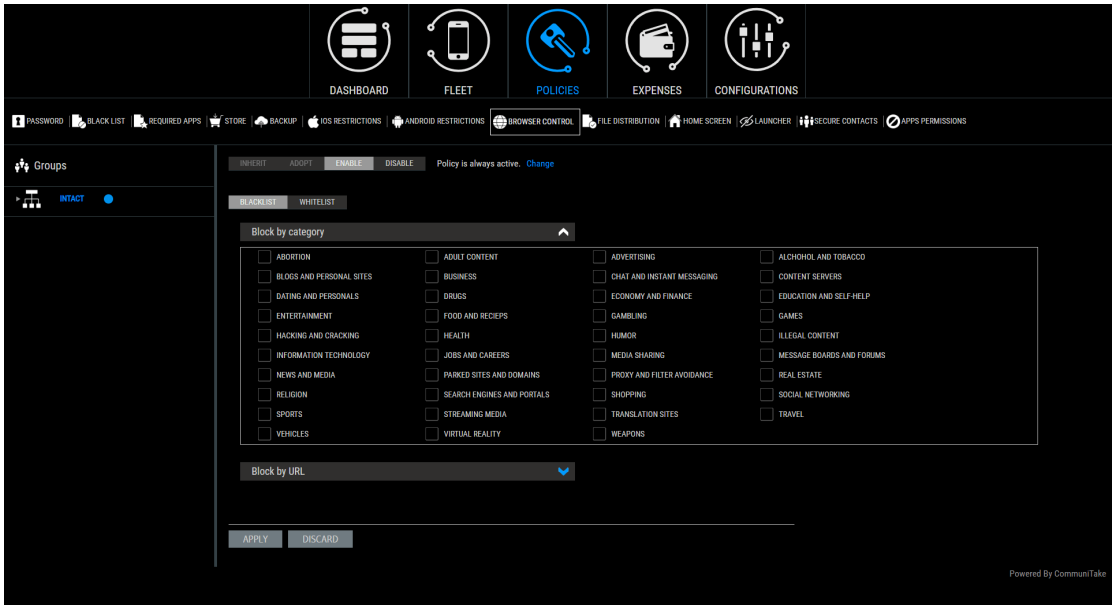
5. Define the desired radius in meters in the "**Radius**" field for the selected point location.
6. Click on "**Submit**".
7. Click on "**Apply**".

BROWSER CONTROL

Web browser control has two deployments:

1. Blacklist:
    a. Allows you to block sites by their category.
    b. Allows you to block certain domains / URLs from access by the device.
2. Whitelist: allows you to define domains / URLs that the device will be able to navigate to.

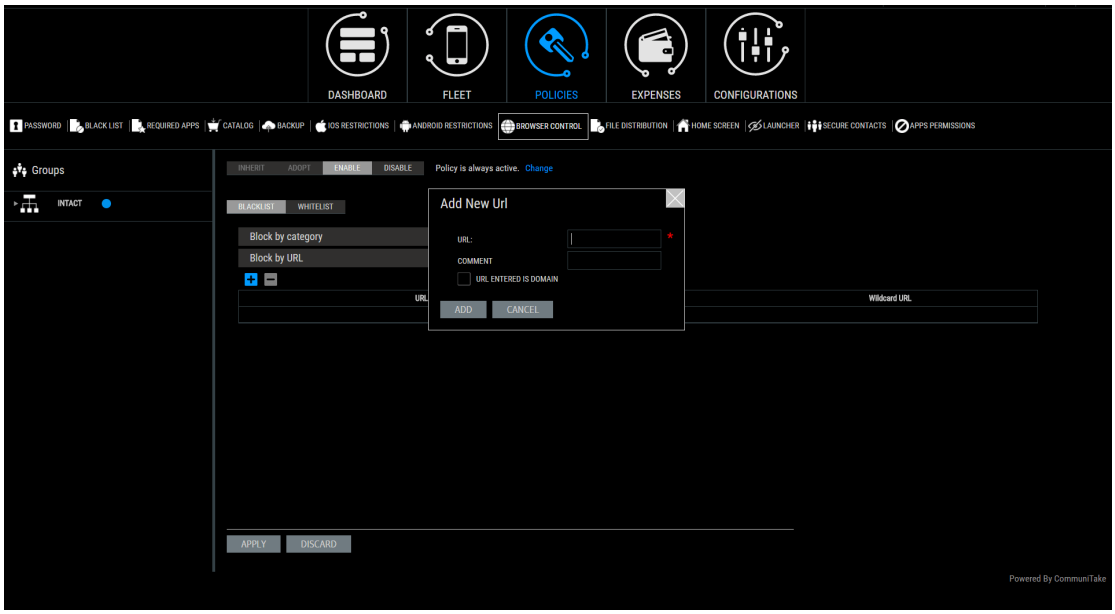
The control over the web use is fulfilled via a dedicated COMMUNITAKE browser. URLs are also black listed using Google's safe browsing.



TO ACTIVATE BROWSER CONTROL

1. Select the group for which you wish to define browser control.
2. Click on the "**Policies"** tab.
3. Click on the **"Browser Control"** sub tab.
4. Select the preferred action: **"Disable"** or **"Enable"** or **"Inherit"** or **"Adopt"**.
5. Select **"Blacklist"** or "**Whitelist"**.
6. When selecting "**Blacklist**", click "**Block by category**" or "**Block by URL**".
7. When "**Block by category**" is selected, check the desired site content categories to be blocked.

8. When selecting “**Blacklist**” “**Block by URL**” or selecting “**Whitelist**”, click on “**Add URL**”.



9. Enter the URL in the designated data field.
   The URL is required to have a legal format (for example: http://).
10. Select Domain to block the entire domain, or uncheck to block only the specific URL
11. Click “**Add**”.

Important If the required URL (for whitelist or blacklist) is accessible with and without WWW then you must add both options.
The default selection is that all categories are unselected (e.g. all are allowed).
The Blacklisted web categories policy is automatically inherited, and it cannot be modified in an “Adopt” mode.

TO REMOVE DOMAIN/URL IN BROWSER CONTROL

1. Select the group for which you wish to remove browser control.
2. Click on the **“Policies”** tab.
3. Click on the **“Browser Control”** sub tab.
4. Select the preferred action: “**Disable”** or **“Enable”** or **“Inherit”** or **“Adopt”**.
5. Select “**Blacklist**” or “**Whitelist**”.
6. When “**Blacklist**” and “**Block by category**” are selected, uncheck the blocked category.
7. When “**Blacklist**” and **“Block by URL”** are selected or “**Whitelist** is selected, Select the URL you wish to remove.
8. Select the URL you wish to remove.
9. Click on **“Delete URL”**.
10. Click “**Delete”** on the pop-up.

When Browser Control is activated, the “Browser” button will appear in the on-device application client.
All popular browsers are automatically disabled ('killed') when launched.
Additional browsers can be handled via application blacklist.

TO ACTIVATE BROWSER CONTROL BY TIME

The default Browser Control policy state is always active, by your definitions. However, you can selectively activate the policy by a specific time of day and week. In this time period and only at this time period, the Browser Control policy will be viable. This definition provides you with the flexibility to activate productivity enforcement during work hours for example. To define time driven Browser Control policy:

1. Define Browser Control policy.
2. Click on the "**Change**" link near the "**Policy is always active**".
3. Select "**Time**" in the pop-up.
4. Select the start time and the end time in hours and minutes.
5. Select the days of the week.
6. Select the time zone.
7. Click on "**Submit**". Verify that your selection summary appears on the upper policies bar.
8. Click on "**Change**" near the summary if you wish to alter it.
9. Click on "**Apply**".

TO ACTIVATE BROWSER CONTROL BY LOCATION

The default Browser Control policy state is always active, by your definitions. However, you can selectively activate the policy by a specific device location. In this location and only at this location, the Browser Control policy will be viable. This definition provides you with the flexibility to activate productivity enforcement when on the organization premise for example. To define location driven Browser Control policy:

1. Define Browser Control policy.
2. Click on the "**Change**" link near the "**Policy is always active**".
3. Select "**Location**" in the pop-up.
4. You can define the location in two ways:
    a. Manually define the latitude and the Longitude.
    b. Or click on the "**Map**" to find the required location.
        i. You will be shown New York City location as the starting point. Navigate to the desired location and click on the map. The latitude and the Longitude fields will be populated in accordance.
5. Define the desired radius in meters in the "**Radius**" field for the selected point location.
6. Click on "**Submit**".
7. Click on "**Apply**".

Important iOS: The application cannot disable the browser on iOS devices. This will be done via iOS restrictions (blocking default browser) and Blacklist (which only notifies the application administrator).
In order to block the Safari browser, and iOS restrictions policy which disables the Safari browser must be applied to the devices' group. All other browsers must be handled via Blacklist management.

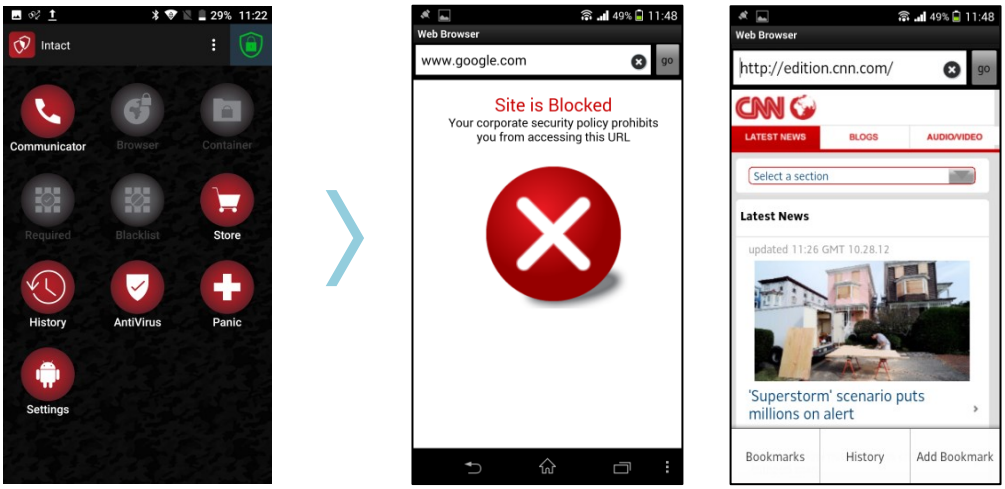
DEVICE USER EXPERIENCE

The on-device web access is conducted only via the on-device application client.

Once the web browser is activated, the device holder is required to enter the domain / URL

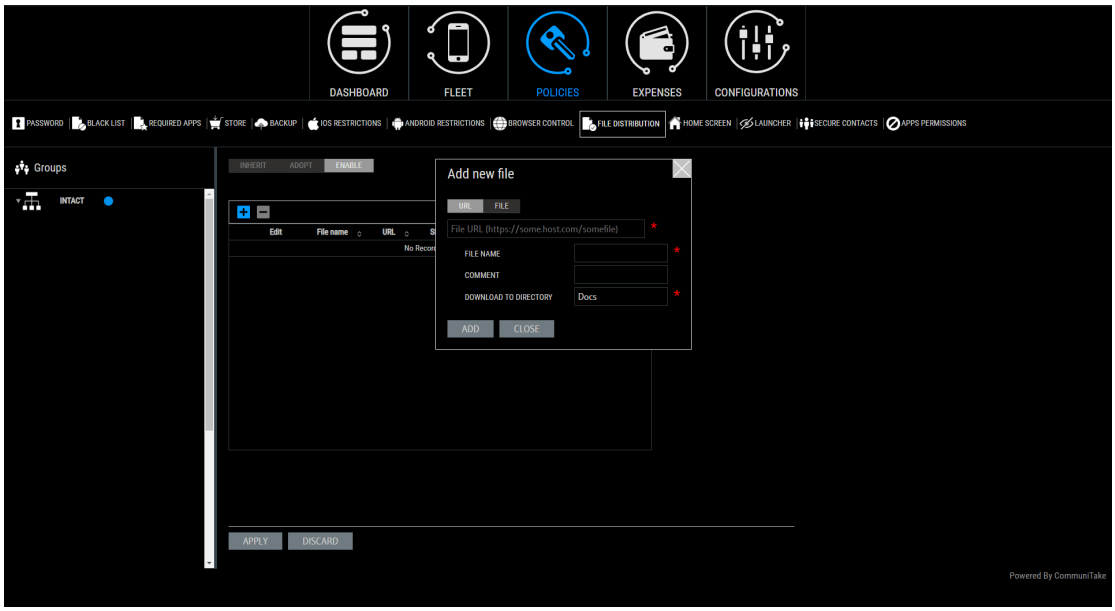
When trying to access a prohibited domain / URL, the access will be blocked.

When accessing the web, the device user can leverage Bookmarks, History and Add bookmarks.



FILE DISTRIBUTION

The file distribution module allows you to send files to groups of devices. The files are defined in the system for distribution and the devices pull them once they connect to the system. If a distributed file already resides on the device, the new file will overwrite it. In iOS devices, the files are viewed via the on-device Command Center application but can be exported to external applications. In Android devices, the files are visible in the device file system.



Note File distribution: files retrieval via an external URL requires HTTPS only links.

TO DISTRIBUTE FILES TO DEVICES

1. Select the **"Files distribution"** tab.
2. "**Inherit"** is the default state. Change the inheritance status to "**Adopt"** or "**Enable".**
3. Click on the **"Add"** button.
4. Select "**URL"** for a file pull via a URL or "**File"** to upload a file.
5. For "**URL"** enter the **"File URL"** address (mandatory).
6. For "**File"**, click "**Upload File**" and select the file you wish to upload.
7. Enter the **"File name"** (mandatory).
8. Enter **"Comment"** (optional). Note that this comment will be displayed inside the iOS application.
9. Enter the **"Download to directory"** location to which the files will be downloaded (mandatory).
10. Click on "**Add"** to activate the procedure.
11. Click "**Apply**" when you finish adding all the files.

TO EDIT AN EXISTING FILE

1. Select the **"Files distribution"** tab.
2. Click the edit button  near the file you wish to edit.
3. Change one or more of the following:
    a. Update the file by either changing the download URL or uploading a new file. You can also switch between the two modes.
    b. Update the file name.
    c. Update the comment.
    d. Change the download directory.
4. Click "**Save"** to save the changes.
5. Click "**Apply"** to finalize the process and activate the changes.

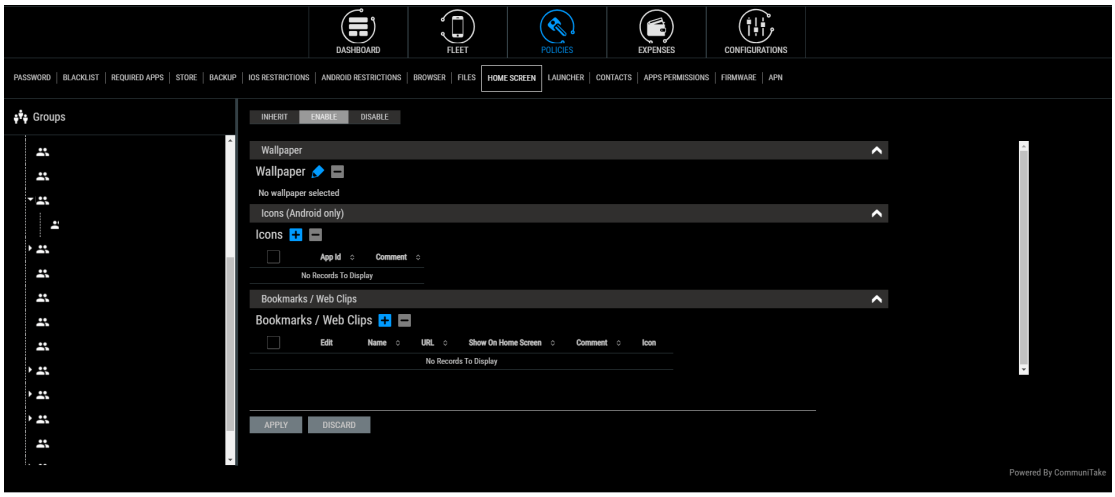
Note

- There is a 100 MB size limit for uploading a file to the system.
- Not all edit operations result in the file being re-downloaded.
- If the download fails due to on- device memory limit, the system will attempt to re-distribute the file until a successful distribution.
- In Android, the system does not track if the user deleted, moved or renamed the file.

HOME SCREEN

The 'Home screen' policy allows you to define the elements that appear on the device's home screen. These elements contain Wallpaper (Android only), Icons (Android only) and Bookmarks / Web clips.

Note **"Inherit"** is the default state. Change the inheritance status to "**Adopt"** or "**Enable"** prior to specific configuration.



TO ADD WALLPAPER

1. Select the **"Home screen"** tab.
2. Under "**Wallpaper"**, select the "**Edit"** (pencil) icon.
3. Check the checkbox near the target Wallpaper and click "**Apply**".
4. You can download the file for your records by clicking the Download arrow in the checked line.
5. To remove a Wallpaper, click the Minus icon.
6. Under "**Delete wallpaper**" Click "**Delete**".
7. Click "**Apply**".

Note Home screen wallpaper: wallpaper retrieval via an external URL allows HTTPS only links.

TO ADD ICONS

1. Select the **"Home screen"** tab.
2. Under "I**cons"**, click on the add button to add an icon.
3. Enter the **"App ID"** (mandatory).
4. Enter **"Comment"** (optional).
5. Click "**Add"**.
6. Check the checkbox near the icons that you wish to add.
7. Click "**Apply"**.
8. To delete an icon, check the checkbox near its name.
9. Click on the minus button .
10. Click on "**Delete"**.

TO ADD BOOKMARKS / WEB CLIPS

1. Select the **"Home screen"** tab.
2. Under "**Bookmarks / Web clips"** click on the add button to add a bookmark.
3. Enter the bookmark's name (mandatory).
4. Enter the bookmark's URL (mandatory).
5. Enter **"Comment"** (optional). Note that this comment will be displayed only in the web portal
6. Upload a file for the bookmark's icon (optional).
7. Click "**Add"**.
8. Check the checkbox near the icons that you wish to add.
9. Click "**Apply"**.
10. To delete a bookmark, check the checkbox near its name.
11. Click on the minus button .
12. Click on "**Delete**".

LAUNCHER

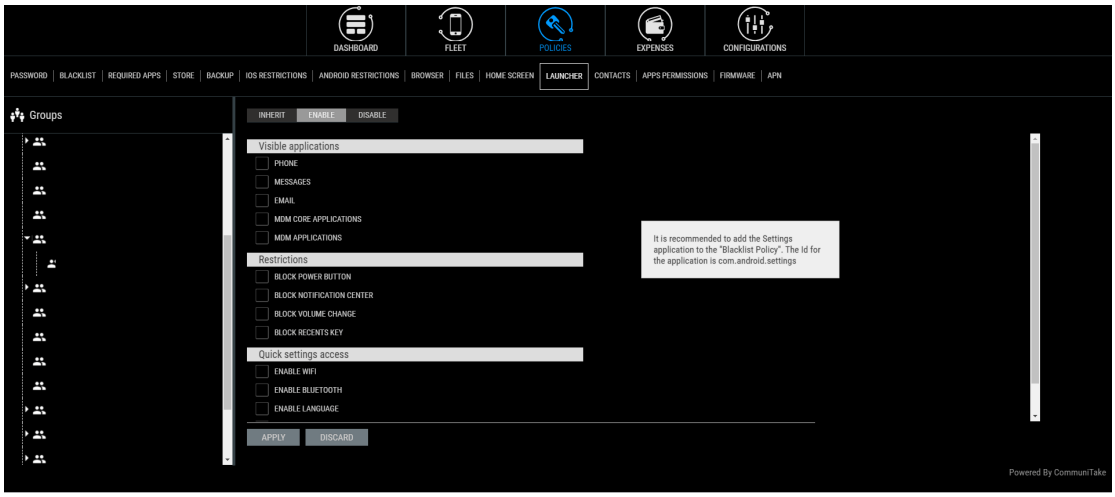
The 'Launcher' policy allows you to lock the use of the device to only specified services.

By default, the launcher will show (1) applications defined as Required Apps where the "ANDROID - ALLOW APPS ONLY FROM LIST" was checked (2) applications that were installed in the past as Recommended Apps from the internal enterprise store (3) icons that were added to the home screen as part of Home Screen policy management.

The device 'settings' application will also be only available via the Launcher's menu. It is recommended to define the Settings application as a prohibited application to block device holders from changing it. You block the Settings app but still authorize device users to configure policy-allowed only settings such as Wi-Fi and Bluetooth.

You can choose to add more common applications:

- Phone.
- Messaging.
- Email.
- MDM core applications: the IntactPhone applications including, the Intact Command Center, Secure Intact browser, Intact communicator, and the Intact store.
- MDM: the applications that were defined as Required Applications.

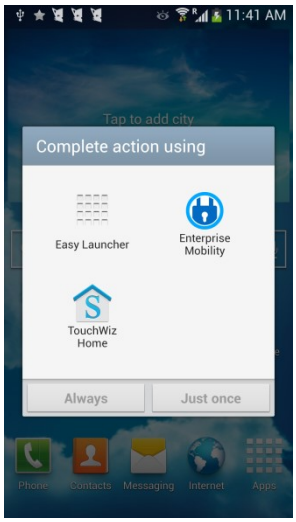


TO DEFINE LAUNCHER

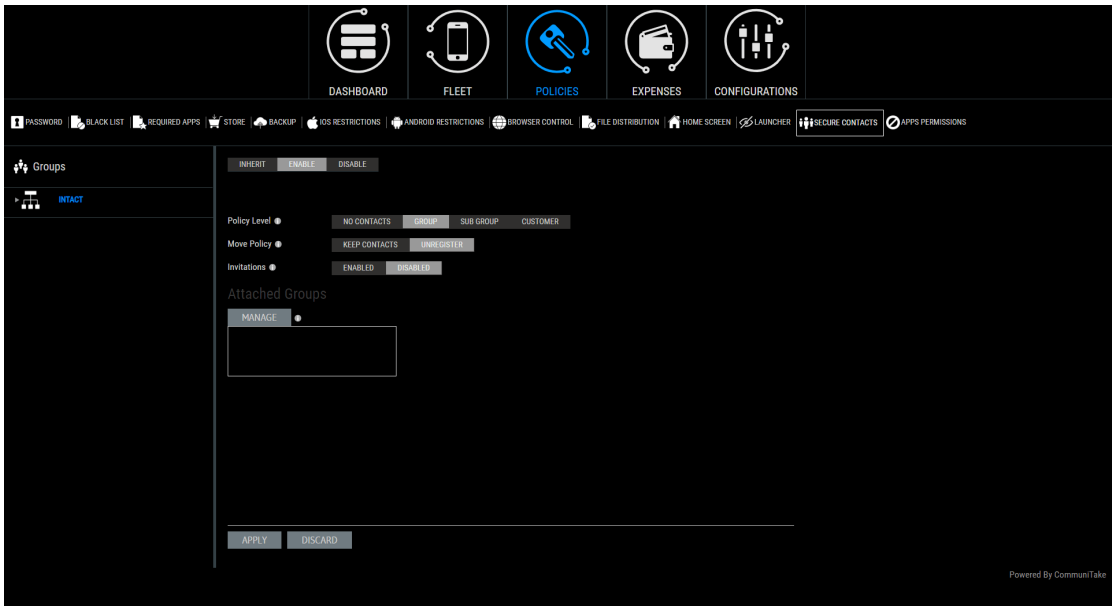
1. Select the **“Launcher”** tab.
2. “**Inherit”** is the default state. Change the inheritance status to “**Adopt”** or “**Enable.”**
3. Click the Launcher’s tab.
4. Check the desired Launcher’s services by your preference:
    a. Phone.
    b. Messages.
    c. Email.
    d. MDM core applications. Check this box if you wish to display these generic applications to device holders. If it is not checked, device holders will not see these applications. The MDM core applications feature generates a more clean display for devices holders that are not intended to use the Intact generic applications, but only use organizational applications or other desired applications.
    e. MDM Applications. Check this box if you wish to display the following applications:
        i. Required applications, when "allow apps only from list" is checked.
        ii. Applications installed from the Intact Store.
        iii. Home screen bookmarks.
5. Check the restrictions by your preference:
    a. Block Power button.
    b. Block notification center.
    c. Block Volume change.
    d. Block Recents key

6. Check Quick Settings access by your preference (enabled Settings for the device holder even when Settings is blocked)
    a. Enable Wi-Fi
    b. Enable Bluetooth
    c. Enable Language
    d. Enable Display
    e. Enable Sound
7. Click "**Apply.**"

Once defined, the device holder will be required to complete the action when trying to access device services.



SECURE CONTACTS



The Secure contacts feature enables you to define the accessible contacts for a device holder. The device holder will be able to conduct secure voice calls and secure messages with these contacts.

You can manage the following capabilities:

Policy Level: (the contacts with whom the device holder will be able to communicate with)

- **No contacts**: The device holder will not see any other contacts.
- **Group**: The device holder will only be able to see the contacts in his group.
- **Sub-Group**: The device holder will only be able to see the contacts in his group and its sub-groups
- **Customer**: The device holder will be able to see all the contacts in the organization.

Move Policy: (the contacts with whom the device holder will be able to communicate with when switching groups)

- Keep Contacts: the device holder will be able to view his previous group's contact when moving to a different group.
- Unregister: the device holder will not be able to view his previous group's contact when moving to a different group.

Invitations: (the policy to invite other devices)

- **Enabled**: the device holder can invite other contacts.
- **Disabled**: the device holder cannot invite other contacts.

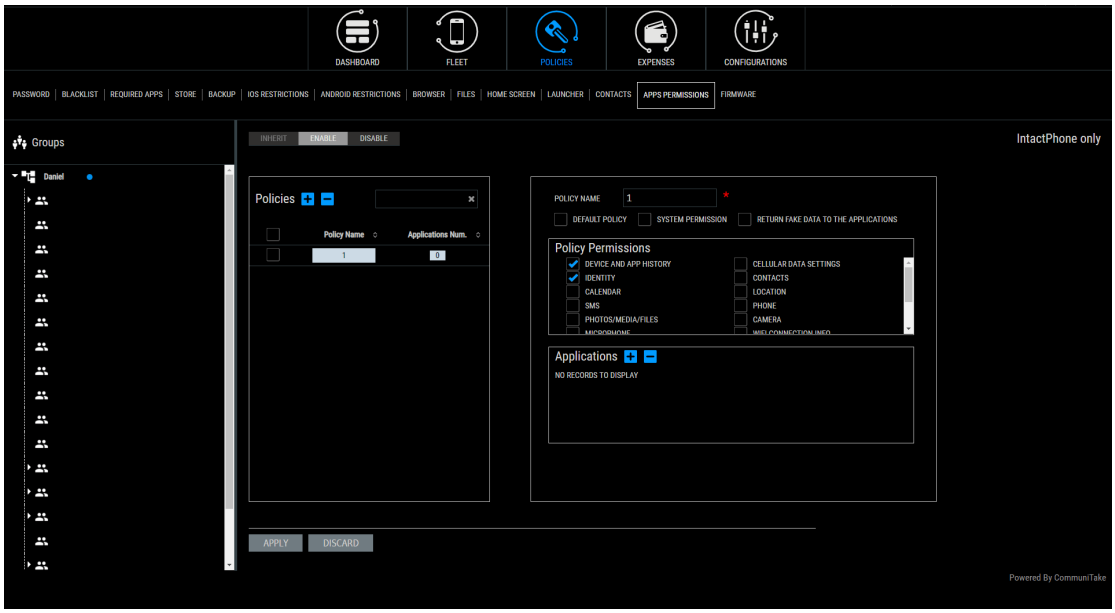
Attached groups: enables granular visibility of specific groups to other groups beyond the pre-defined view policy. The device holder will be able to view all the contacts from groups that were defined as visible for him, on top of the generic view policy.

APPLICATIONS PERMISSIONS

The 'Applications Permissions' feature enables you to define the permissions for every on-device application.

To define the permissions act as follows:

1. Click on the Apps Permissions tab under Policies.
2. Add a policy and name it.



3. Check the enabled permission for applications for this policy. Available permissions:
    a. Device and App history.
    b. Cellular data settings.
    c. Identity.

d. Contacts.
e. Calendar.
f. SMS.
g. Phone.
h. Photos/Media/Files.
i. Camera.
j. Microphone.
k. Bluetooth connection info.
l. Wearable sensors/activity data.
m. Device ID & Call info.
n. In-app purchases.
o. Other.

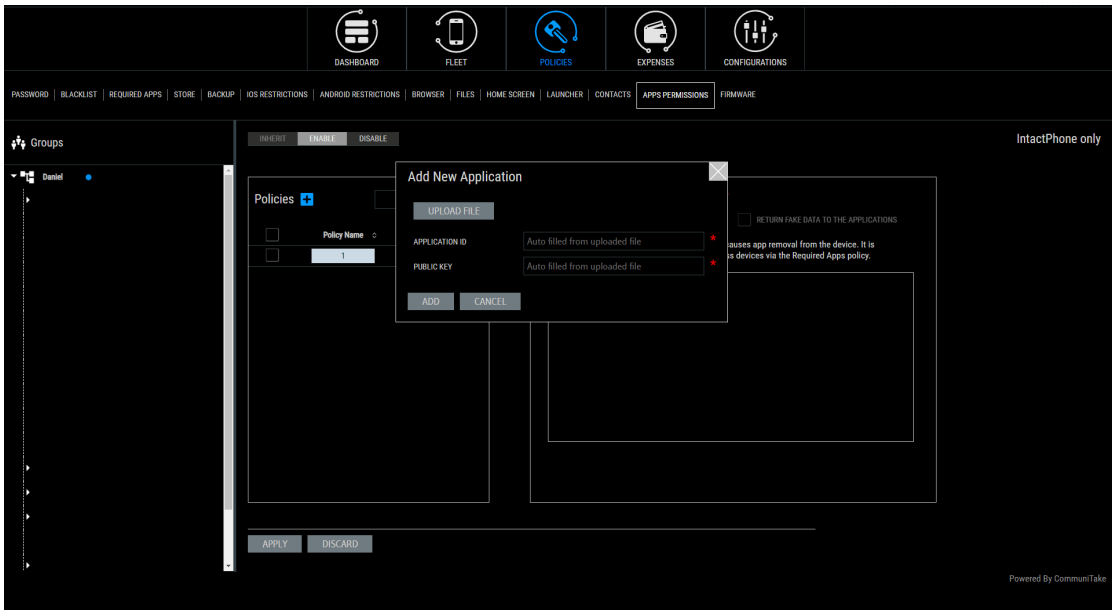
4. Attach the applications to the selected policy.
5. You can check the Default Policy checkbox to define a generic policy across all applications, without the need to attach specific applications to it.
6. Click 'Apply'.

Note The "**Default policy"** refers to all 3rd party applications which do not have a specific policy assigned to them.

Note You can assign specific policy to system applications, though this can cause irregular behavior on the device. It is suggested you check such policy before deploying it.

SYSTEM PERMISSIONS APPLICATIONS

The permissions management policy enables you to define system permission to apps. A system permission app can get all the system permission when it operates on the device. It provides complete flexibility for apps' developers to achieve the exact app function and user experience.



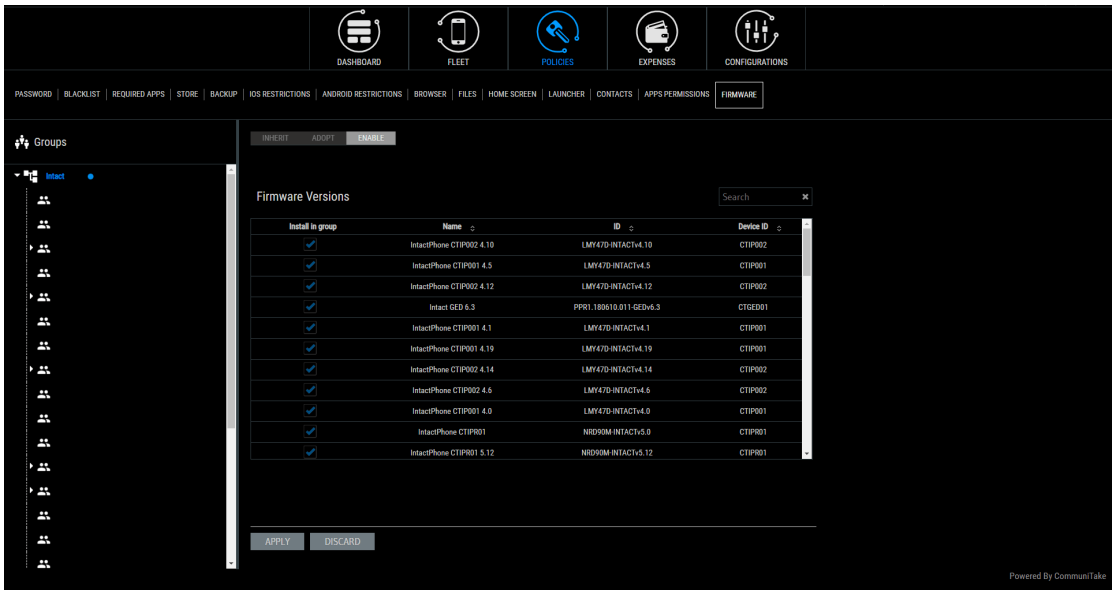
To define an app as a system permissions app:

1. Click on the "**Policies**" tab.
2. Click on the "**Apps Permissions**" tab.
3. Check the "**System Permission**" checkbox.
4. Click on the Add app icon .
5. Click "**Upload file**" and upload the APK to the system.
6. Click "**Add**" then click "**Apply**".

Note: Assigning system permissions to an application causes app removal from the device. It is recommended to distribute the applications across devices via the Required Apps policy.

Note: System Permissions management may not operate on all firmware versions. Please consult before applying the policy.

FIRMWARE MANAGEMENT



Firmware management enables you to control the firmware version that runs the device as follows:

- The administrator of your parent account defines the allowed firmware versions.
- You can select which firmware version should be deployed on devices by their group.
- Devices in a group can only run the same firmware.
- Firmware updates cannot skip firmware versions. If you wish to force a firmware upgrade, you must make sure to select all the firmware versions that were published before the target firmware.
- Device firmware can only be upgraded to a newer version. It cannot be downgraded to a previous version.

To force a firmware version upgrade:

1. Select the target group.
2. Click the "**Policies**" tab.

3. Click the “**Firmware**” tab.
4. Check the firmware version you wish to force. Make sure to select all the versions that were forced after the base version and up to the target version.
5. Click on “**Apply**”.

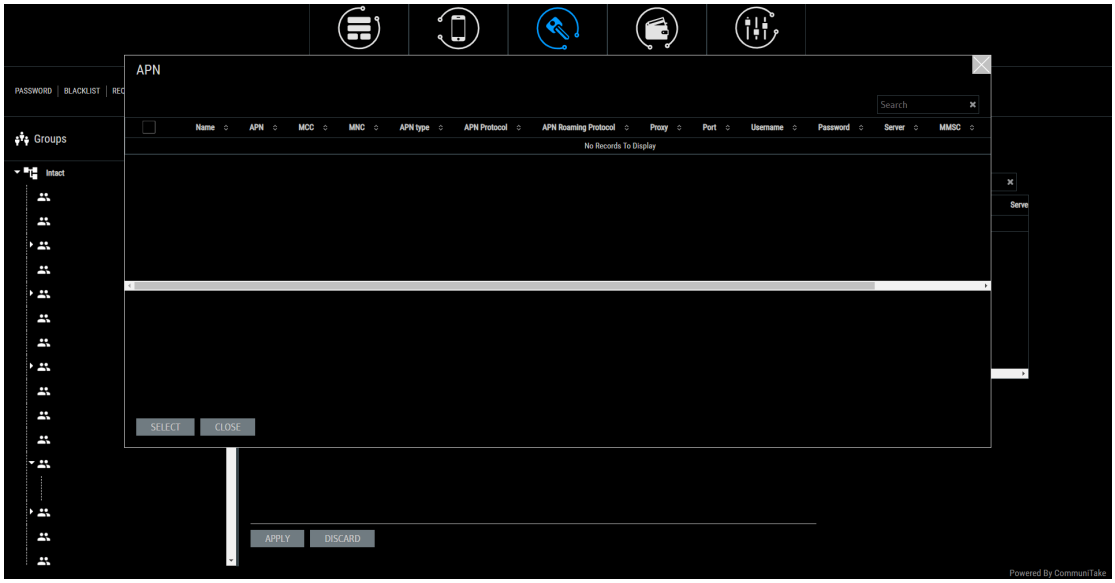
APN MANAGEMENT

APN management enables you to define a set of APN addresses that will be deployed on the account devices.

APN management policy behavior is as follows:

The customer level system administrator defines the available set of APN addresses.

The system/group administrator can select the APN addresses to be deployed from the pre-defined set.



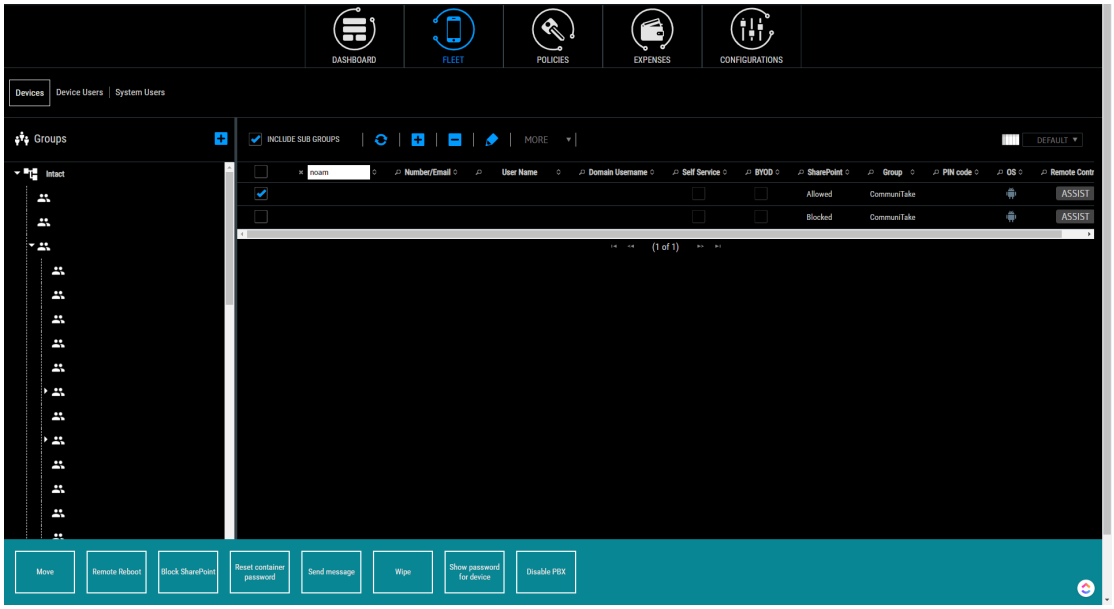
Once the system/group admin activates the APN policy, device holders do not have direct access to APN settings.

If several APN addresses are set on the device, the device will automatically select the APN by the inserted SIM card.

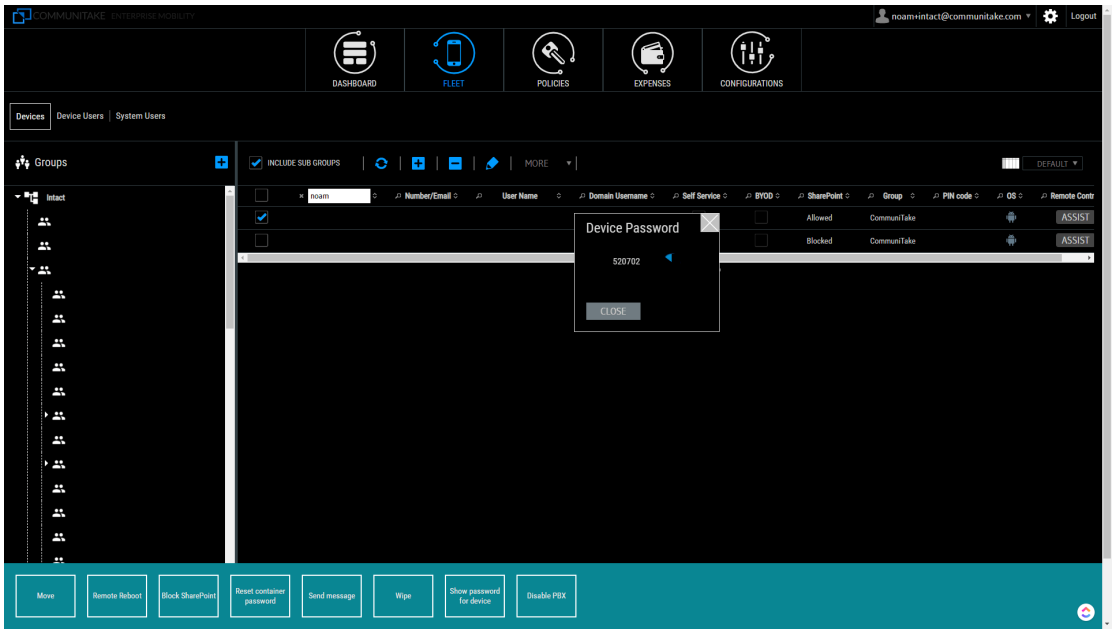
If the device lacks connectivity, but there is a need to redefine access points, you can revoke the APN policy and alter the device to its original APN settings.

To revoke APN policy settings:

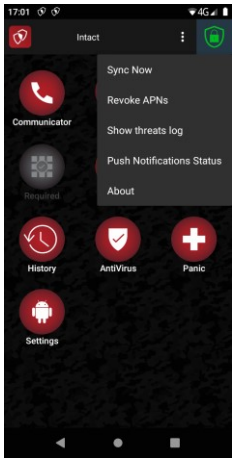
1. Click the “**Fleet**” tab.
2. Check the target device.
3. Tap on the “**Show password for the device.**”

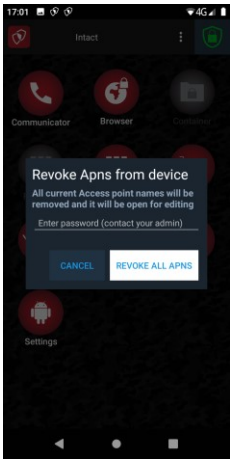


4. The system will display you with a code.



5. Direct the device holder to tap on the Intact icon, then on the three-dot menu in the upper right corner of the app screen, then on "**Revoke APNs.**"



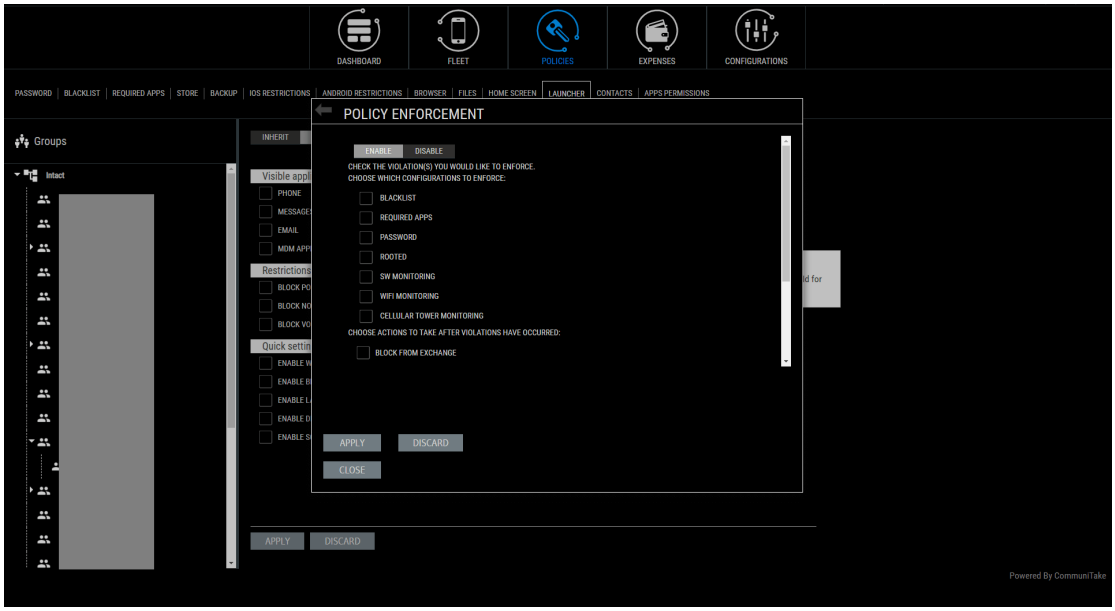


6. Direct the device holder to key-in the password code.
7. The app will delete the current APNs, and the APN settings will be active, allowing the device holder to define any APN.

Note: revoking APNs password changes every 30 seconds. Direct the device holder to key the displayed password before it changes to another password.

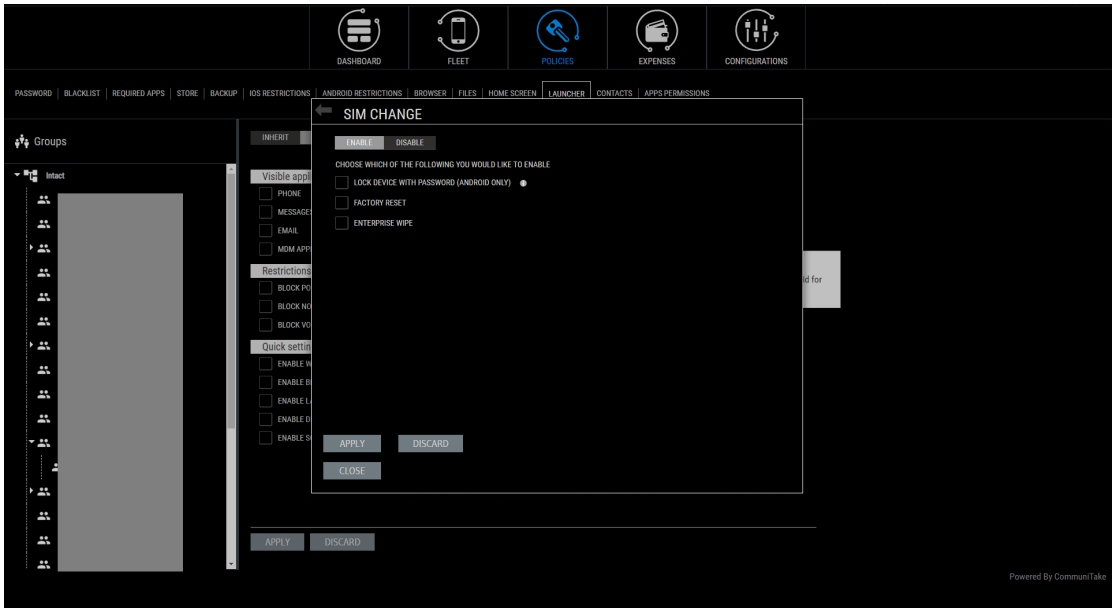
POLICY VIOLATIONS DRIVEN ENFORCEMENT

The system allows you to enable enforcement actions once a policy violation occurs.



1. Click on **"Settings"** on the upper right corner of the screen.
2. Click on the "**Policy Enforcement"** icon.
3. Select "**Enable**".
4. Check the policies violations events for which you wish to activate enforcement:
    a. **"Blacklist".**
    b. **"Required apps".**
    c. **"Password**".
    d. **"Rooted".**
    e. "SW Monitoring".
    f. "Wi-Fi Monitoring".
    g. "Cell Tower Monitoring".
5. Choose actions to take after violations have occurred:
    a. **"Block from Exchange"** (this is only available if the Exchange server is properly configured).
    b. **"Lock the device with a password (Android only)".**
    c. "Enterprise Wipe".
    d. "Disconnect internet connectivity".
    e. "Factory reset".
    f. "Block SharePoint".
6. Define the grace period in days for the enforcement activation. The default time is set to 168.

SIM CHANGE DRIVEN ENFORCEMENT



For action on a SIM Change event:

1. Click on **“Settings”** on the upper right corner of the screen.
2. Click on “**SIM Change”**.
3. Select “**Enable**”.
4. Enable one of the following actions once the device SIM card is changed:
    a. **“Lock device with password (Android only)”.**
    b. “Factory Reset”.
    c. “Enterprise Wipe”.
5. Click **“Apply”**.

7

USAGE MONITORING

The Expense Control module allows the user to monitor usage across the enterprise's devices that are enrolled in the system. Usage monitoring is governed by two factors:

1. Enterprise's groups as defined in the system.
2. The usage plans that are defined in the system and that are associated to groups. A device usage will be examined in accordance to its group's plan.

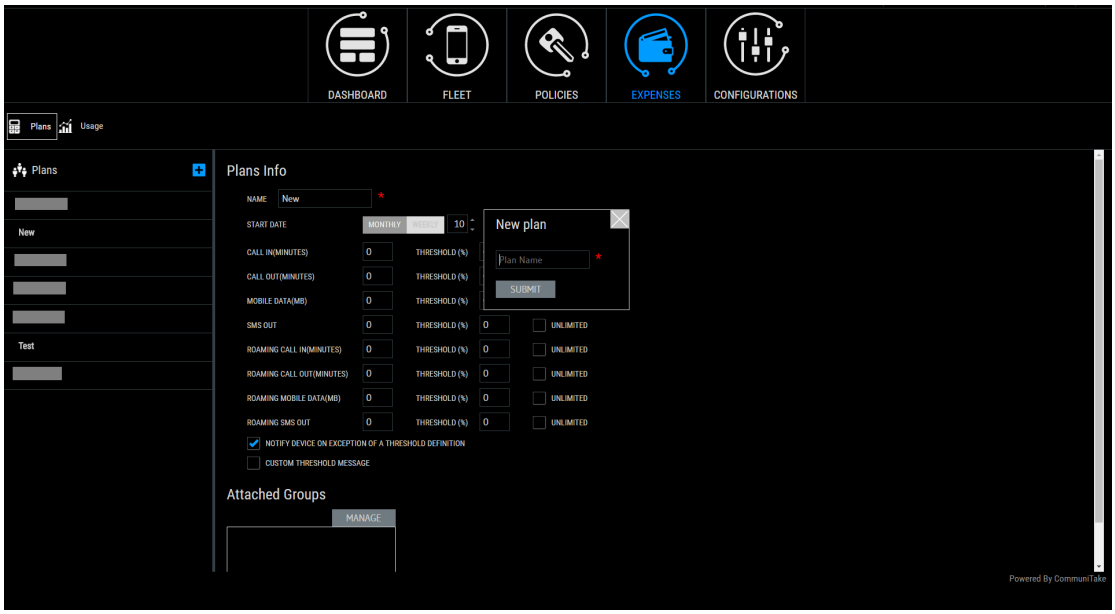
USAGE PLANS

Usage plans are set in the system by the user.

TO MANGE USAGE PLANS

TO ADD A NEW PLAN

1. Click on the **"Expense"** tab.
2. Click on the **+** near **"Plans"**.
3. Enter the plan name.
4. Click **"Submit"**.

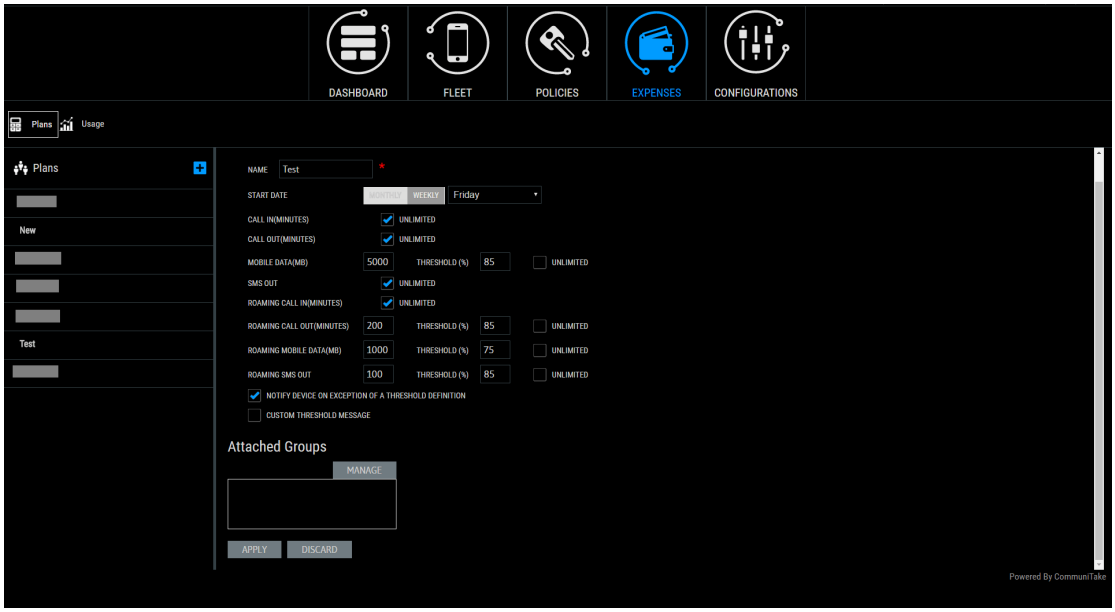


TO REMOVE AN EXISTING PLAN

1. Click on the **"Expense"** tab.
2. Click on the "–" (minus sign) near the plan you wish to remove.
3. Click **"Submit**".

TO DEFINE PLAN ATTRIBUTES

You can allocate usage parameters to a new plan or amend usage parameters to an existing plan.



Supported usage parameters by mobile operating system:

Usage Parameter	Android	iOS
Call In (Seconds)	Yes	No
Call Out (Seconds)	Yes	No
Data (KB)	Yes	Yes
SMS Out	Yes	No
Roaming Call in (Seconds)	Yes	No
Roaming Call out (Seconds)	Yes	No
Roaming Data (KB)	Yes	Yes
Roaming SMS out	Yes	No

1. Select the plan which you wish to define.
2. Set the timeframe for which you wish to monitor the usage. It can be on a monthly basis or a weekly basis. For a weekly basis, define the first day of the week.
3. Define the usage level for each plan parameter:
    a. Call In (Seconds).
    b. Call Out (Seconds).

c. Data 3G (KB).

d. SMS Out.

e. Roaming Call in (Seconds).

f. Roaming Call out (Seconds).

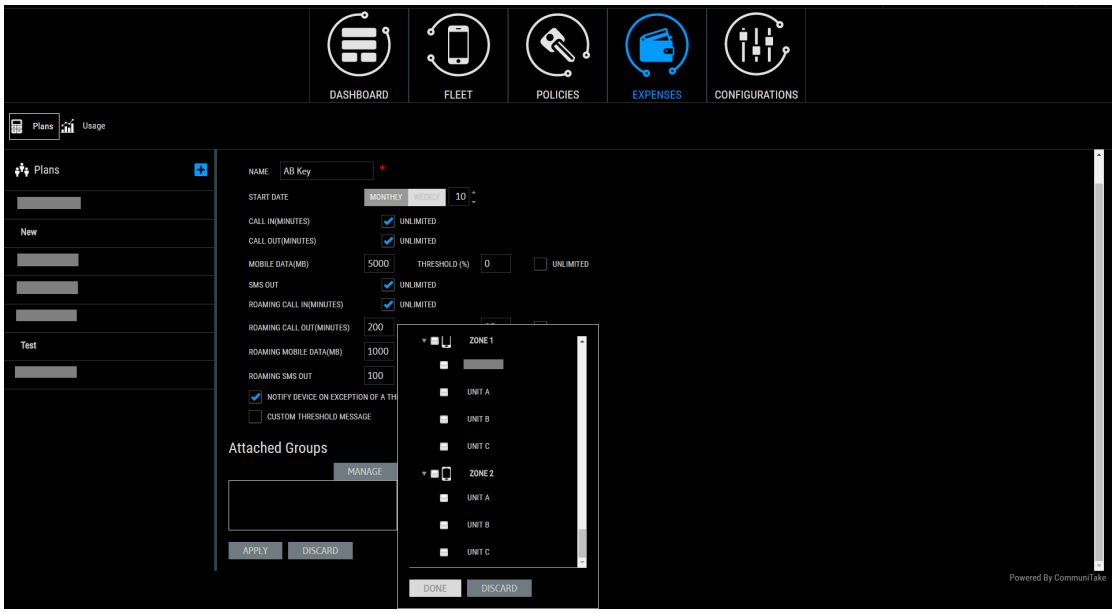
g. Roaming Data 3G (KB).

h. Roaming SMS out.

4. Define for each parameter the monitoring mechanism:
   a. **"Unlimited"** use will not generate monitoring procedure.
   b. A "**Threshold"** defines the percentage of the limit for that parameter by which you wish to create an alert mechanism. The alert will be performed in accordance to the threshold percentage and the plan attribute.
5. Check **"Notify Device on Exception of a Threshold Definition"** if you wish the system to generate a notification to the device holder when the threshold is reached.
6. Define the "**Message to send to device on threshold exception".**
7. Attach the groups to the plan:
   a. Click on the **"Manage"** button the **"Attached Groups"** table.
   b. Select the groups you wish to attach the plan.
   c. Click **"Done"**.

   Please note that adding a group does not automatically adds its subgroups. You will be prompted to select the behavior.

   If the selected group is already attached to a different plan, you will be requested to override the attachment.
8. Click **"Apply"**.



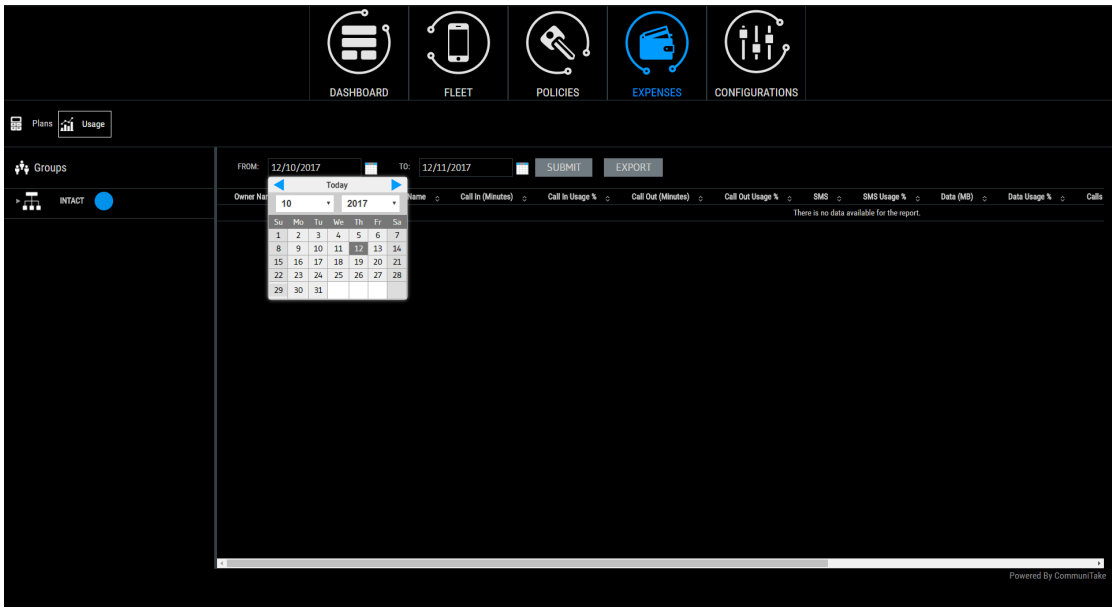
USAGE REPORT

Usage report provides you with an approximate usage view based on the parameters that were set in the usage plans.

The report provides data for the following parameters:

1. Device Number (MSISDN).
2. Device User Name.
3. Call In (Minutes).
4. Call In % of defined Usage.
5. Call Out (Minutes).
6. Call Out % of defined Usage.
7. SMSs.
8. SMSs % of defined Usage.
9. Data (MBs).
10. Data % of defined Usage.
11. Calls In Roaming (minutes).
12. Calls Out Roaming (minutes).
13. SMSs Roaming.
14. Data Roaming (MBs).

The % of usage relates to the parameter level in the price plan.



TO RUN USAGE REPORT

1. Select the devices group.
2. Click the **“Expenses”** tab.
3. Click the “**Usage Report”** tab.
4. Select the time period for which you wish to see the usage data.
5. Click on **“Submit”**.

Important The system presents an approximate usage based on the device's counters. This usage presentation does not replace the usage calculated by the billing system and cannot be considered as accurate as the billing system calculations.

The system collects usage once the device in enrolled. It cannot present historic usage data that has occurred prior to the device enrollment.

TO EXPORT USAGE DATA TO EXCEL

1. Usage data can be exported to an Excel file for further processing.
2. Select the devices group.
3. Click the Expenses tab.
4. Click the Usage Report tab.
5. Select the time period for which you wish to see the usage data.
6. Click on Submit. This is a mandatory step prior to exporting.
7. Click on the Export button.

8

REMOTE SUPPORT

REMOTE SUPPORT

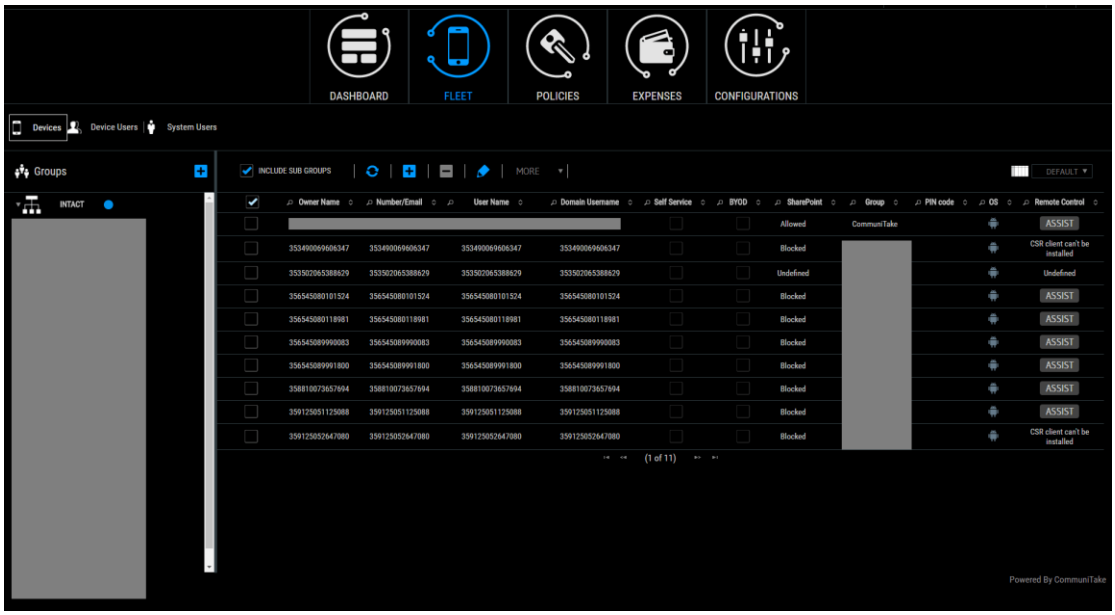
The '**Support**' module enables the system user to remotely assume complete control over the mobile device. It enables technical experts to take over a mobile phone or tablet through an Internet connection, regardless of the phone's actual location. After installing a small device client with the active participation of the phone holder, the system user can remotely view and operate the phone as if he is holding it in his hands, while simultaneously talking with the device holder.

Remote Support includes the following features:

- A fully operational device replica.
- On-device screen drawing in real time for guiding on "How Do I?" queries.
- Automated resolution macros for resolving operational problems.
- Extensive device diagnostics.
- Device data management for managing device files and content.
- Operations to manage device applications.
- Permission solicitation mechanism for device access authorization by device user.
- Remote iOS configuration without complete takeover.
- Remote iOS screen captures view.
- Pause Remote access due to privacy constraints.
- Automated reconnect after device restart.
- One-click screen capture and recording.
- Textual chat.

ACTIVATING REMOTE SUPPORT

Activating the remote takeover for a device is performed via the devices table under the **“Fleet**” tab.



Once activated, the system launches the remote support module under a new **“Support**” tab:

1. Select the **“Fleet”** tab and then the “**Devices”** tab below it.
2. Select the **“Default”** view.
3. Select the device for which you wish to conduct remote takeover.
4. Click on **“Assist**” at the line of the selected device. (You can shift to the Remote Support table view for an easy access to the remote support request).
5. The system will deflect you to a new tab where the remote support application will be launched.
6. If needed, the remote support application will automatically send the support client download SMS to the target device by the number indicated in the devices table.
7. Proactively guide the device holder how to install the remote support client.
8. Once the client is installed and the device holder has approved the terms of use, the remote takeover will take place.
9. At the end of the remote support session, disconnect from the device by clicking the disconnect icon in the remote support application.

9

MASS CONFIGURATIONS

The system enables three configuration settings:

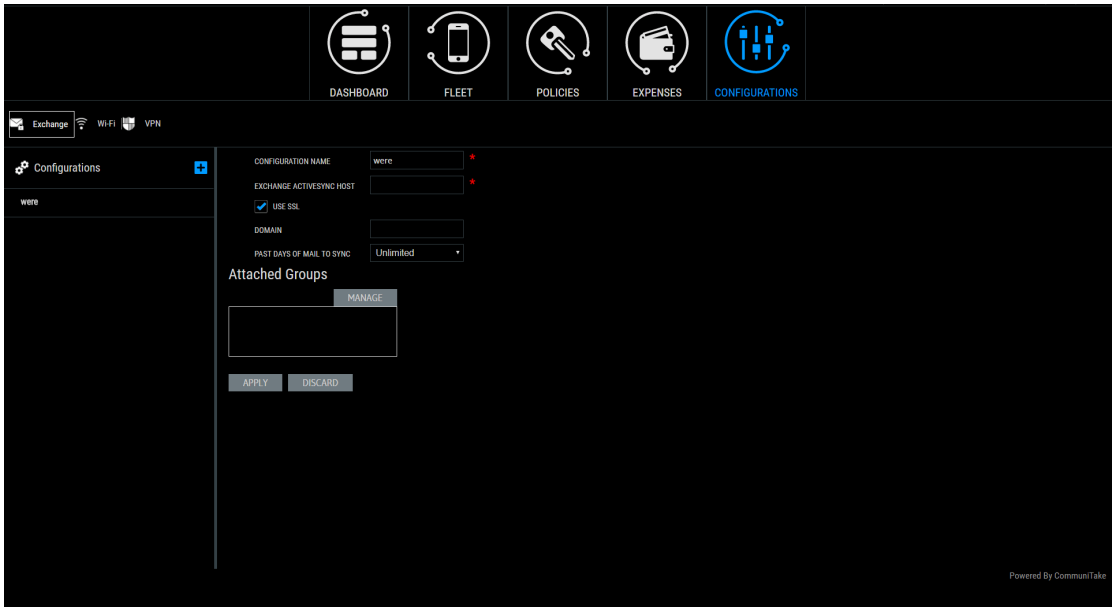
1. Exchange ActiveSync.
2. Wi-Fi.
3. VPN.

SETTING CONFIGURATIONS

Setting a configuration is performed using the same flow for all configurations:

1. Select the **"Configurations"** tab.
2. Select the configuration type out of the options: Exchange ActiveSync; Wi-Fi; VPN. The system indicates the mobile OSs for which the configuration is valid.
3. Click on the plus icon near the **"Add configuration"**.
4. Define the Configuration name in the "**Add new configuration"** box.
5. Click on **"Submit"**.
6. Define the configuration parameters as presented for the configuration type. Make sure to define the mandatory parameters marked in *.
7. Under the **"Attach Groups"** click on **"Manage**".
8. Select the groups for which you wish to deploy the configuration.
9. Click on **"Apply"**.

ADDING EXCHANGE ACTIVESYNC CONFIGURATION

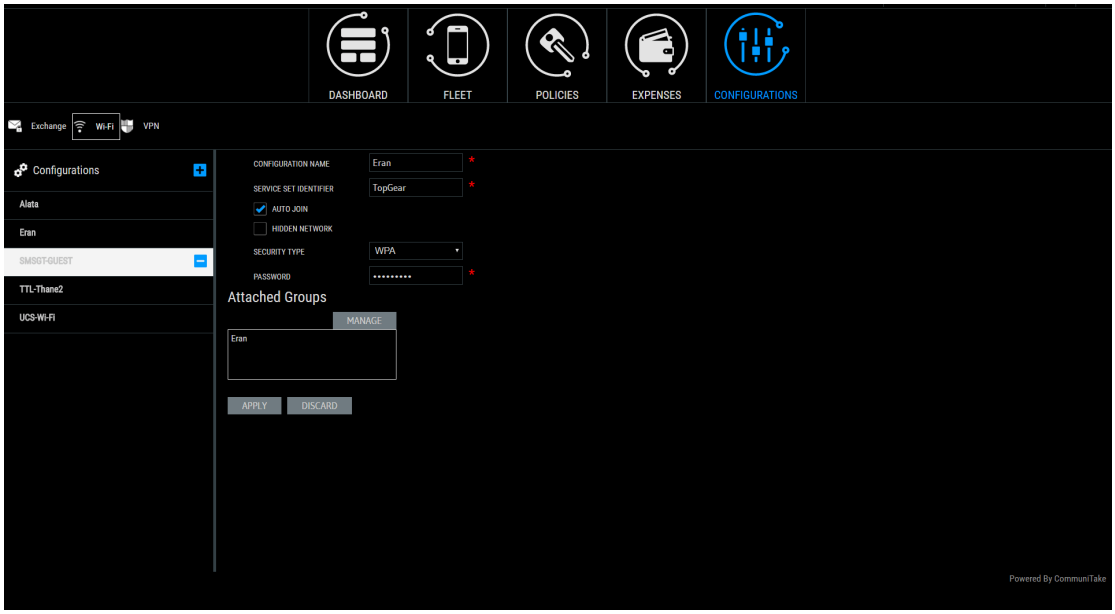


For Exchange ActiveSync configuration make sure to define the following mandatory parameters:

1. Name.
2. Exchange ActiveSync Host.

Important This configuration is supported for the following Android devices: Samsung SAFE, Motorola EDM, HTC Pro and Sony MDM Version 4.0 and above devices.

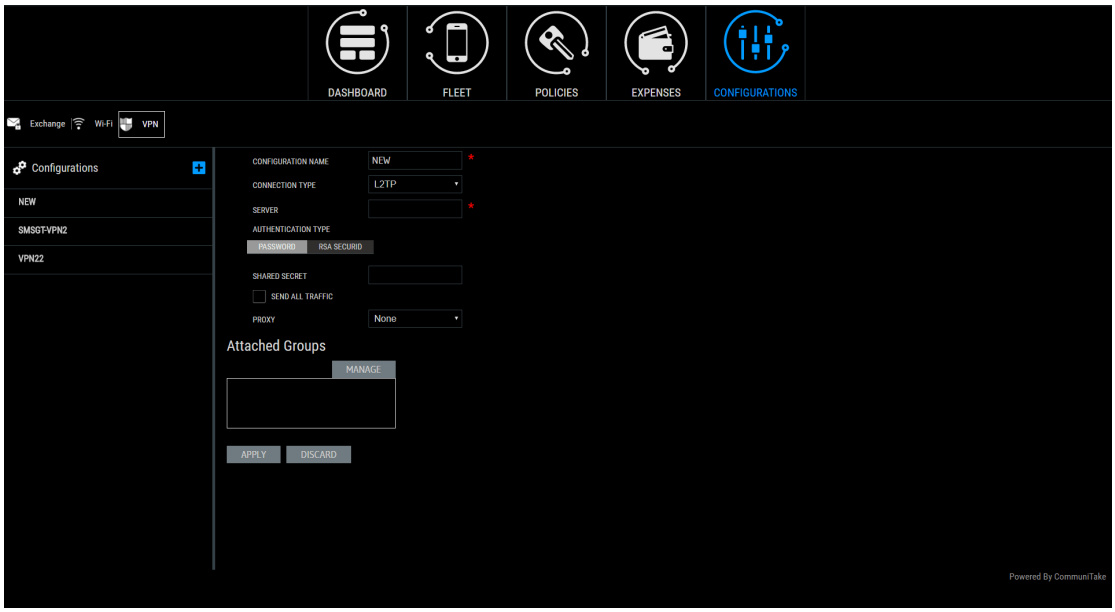
ADDING WI-FI CONFIGURATION



For Wi-Fi configuration make sure to define the following mandatory parameters:

1. Name.
2. Service Set Identifier.

ADDING VPN CONFIGURATION



For VPN configuration make sure to define the following mandatory parameters:

1. Name.
2. Server.
3. Account.

Important This configuration is supported for the following Android devices: Samsung SAFE, Motorola EDM, HTC Pro and Sony device management Version 4.0 and above devices. For Android 2.2 – 2.3.6 devices, activating the IntactPhone Command Center defined VPN connection, is done via the on-device IntactPhone application, under VPN.

10

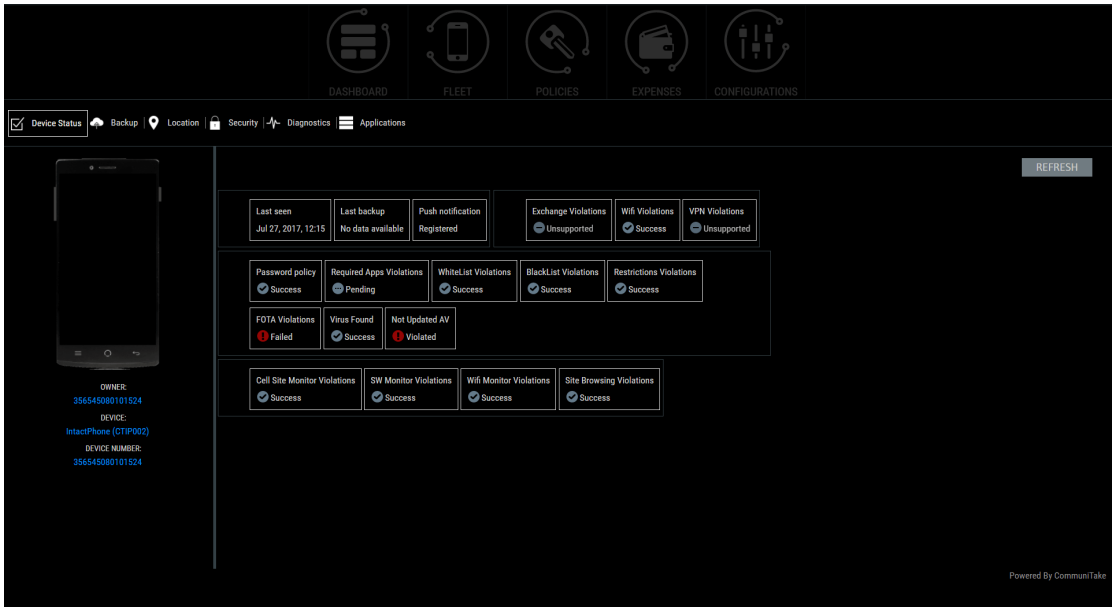
SINGLE DEVICE MANAGEMENT

DEVICE STATUS

The system provides quick device status with the following parameters:

Parameter	Description
Dates	
Last seen	The last date in which the device has connected with the application.
Last backup	The last date in which the device has performed data backup.
Push notifications	Push notifications status: connected; not connected.
Policies	
Password policy	The device password policy status: 'Success'; 'Not Supported'; 'Pending'; 'Failed'.
Required Apps violations	The device Required Apps policy compliance status: 'Success'; 'Pending'; 'Failed'.
Whitelist violations	The device Whitelist policy compliance status: 'Success'; 'Pending'; 'Failed'.
Blacklist violations	The device Blacklist policy compliance status: 'Success'; 'Pending'; 'Failed'.
Restrictions violations	The device restrictions policy compliance status: 'Success'; 'Pending'; 'Failed'.
Firmware	The device Firmware policy compliance status: 'Success'; 'Pending'; 'Failed'.
Virus Found	The Virus Found policy compliance status: 'Success'; 'Pending'; 'Failed'.
Not Updated AV	The Not Updated AV policy compliance status: 'Success'; 'Pending'; 'Failed'.
Configurations	
Exchange violations	The device Exchange configuration status: 'OK'; 'Not Supported'; 'Pending'; 'Failed'.
Wi-Fi violations	The device Wi-Fi configuration status: 'OK'; 'Not Supported'; 'Pending'; 'Failed'.
VPN violations	The VPN configuration status: 'OK'; 'Not Supported'; 'Pending'; 'Failed'.
Deviations	
Cell Site Monitor Violations	The Cell Site Monitor Violations status: 'Success'; 'Pending'; 'Failed'.

SW Monitor Violations	The SW Monitor Violations status: 'Success'; 'Pending'; 'Failed'.
Wi-Fi Monitor Violations	The Wi-Fi Monitor Violations status: 'Success'; 'Pending'; 'Failed'.
Site Browsing Violations	The Site Browsing Violations status: 'Success'; 'Pending'; 'Failed'.



The system provides device protection features that allow the enterprise system administrator or the device holder to resolve lost or stolen device situations. Device protection includes:

- Locate the device on a map.
- Activate device alarm from afar.
- Lock the device (with or without a password).
- Wipe on-device data.
- Backup and restore on-device data.

The system user can navigate to these features by clicking on the selected device from the devices table under the 'Fleet' tab.

LOCATE THE DEVICE

There are two ways to locate a device: on map position and via activating its alarm.

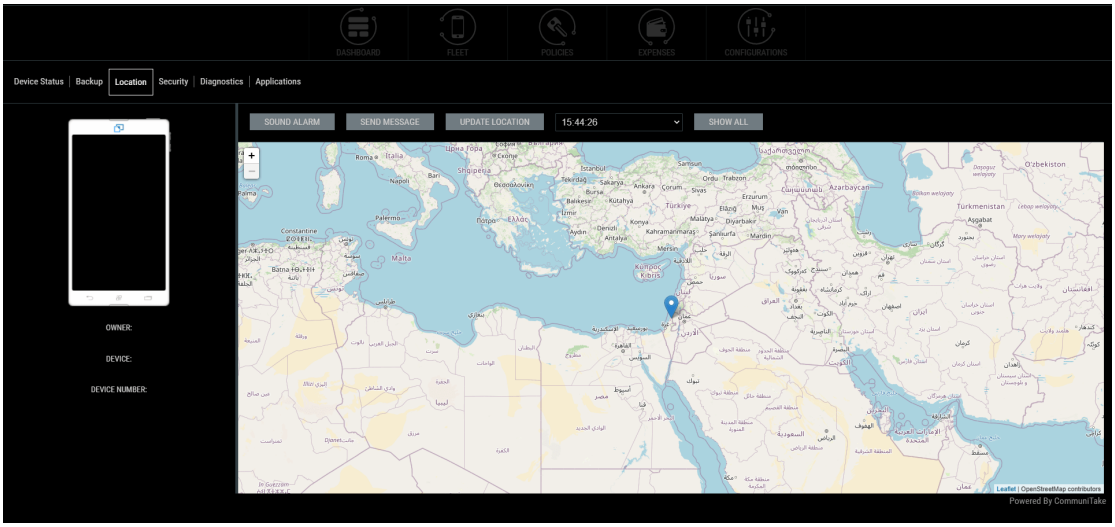
Based on your country's regulation, you may or may not be able to track other users' devices.

LOCATE DEVICE POSITION ON A MAP

1. Select the group to which the device is assigned.
2. Click once on the device line in the devices table.
3. Click on the **'Location'** button.

4. A map with device location indicator will be presented. This is the last known location as perceived by the system based on the level of accuracy that the device itself achieves (either via GPS location or via nearest cell location).
5. Click the **'Update Location'** button if you wish to see the device's current location after a time shift.
6. You can select a specific location date from the locations dropdown list.
7. You can choose "**Show All**" and the system will display the last 30 locations of the device on the map.

Important Push notifications in iOS devices do not wakeup the application without the user consent. If the user doesn't click on the notification, the action will only be performed when the device wakes up the app in the background. It may take a while for this to happen.



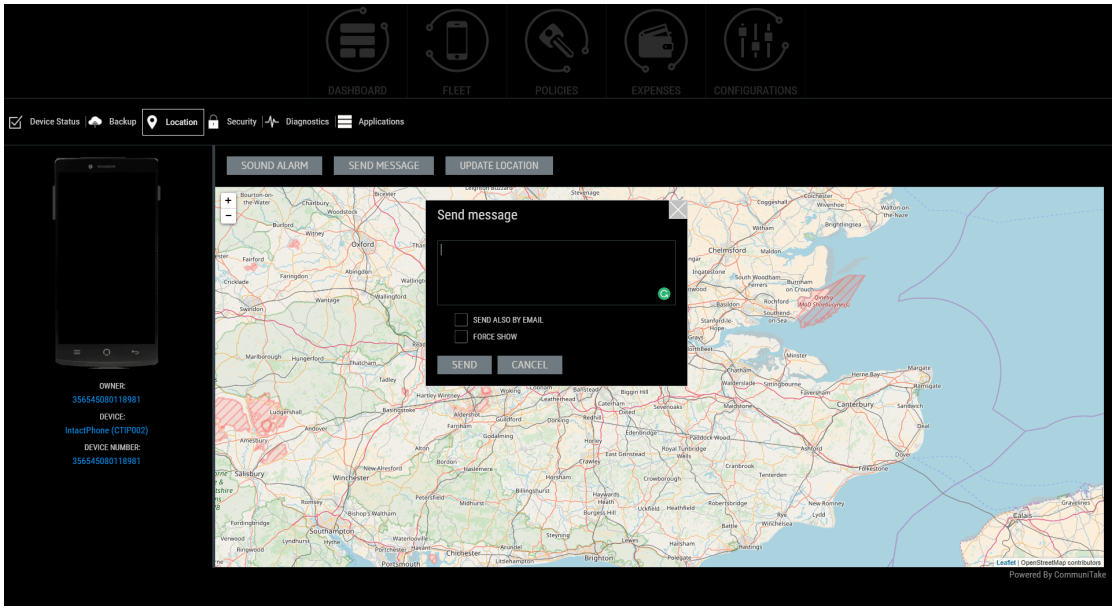
LOCATE DEVICE VIA ALARM

1. Select the group to which the device is assigned.
2. Click once on the device line in the devices table.
3. Click on the "**Location"** button.
4. A map with device location indicator will be presented. This is the current location as perceived by the system.
5. Click on the **"Sound Alarm"** Button for activating an alarm even if the device in on silent.

Important You can activate the device alarm from afar even if the device is set to silent mode.

SEND A MESSAGE TO THE DEVICE

1. Select the group to which the device is assigned.
2. Click once on the device line in the devices table.
3. Click on the "**Location"** button.
4. A map with device location indicator will be presented. This is the current location as perceived by the system.
5. Click on the **"Send Message"** Button.
6. Select whether you wish to send also an email with the message.
7. Select whether you wish to force the message as a poip-up on the target device.
8. Click on "**Send**".



LOCK THE DEVICE

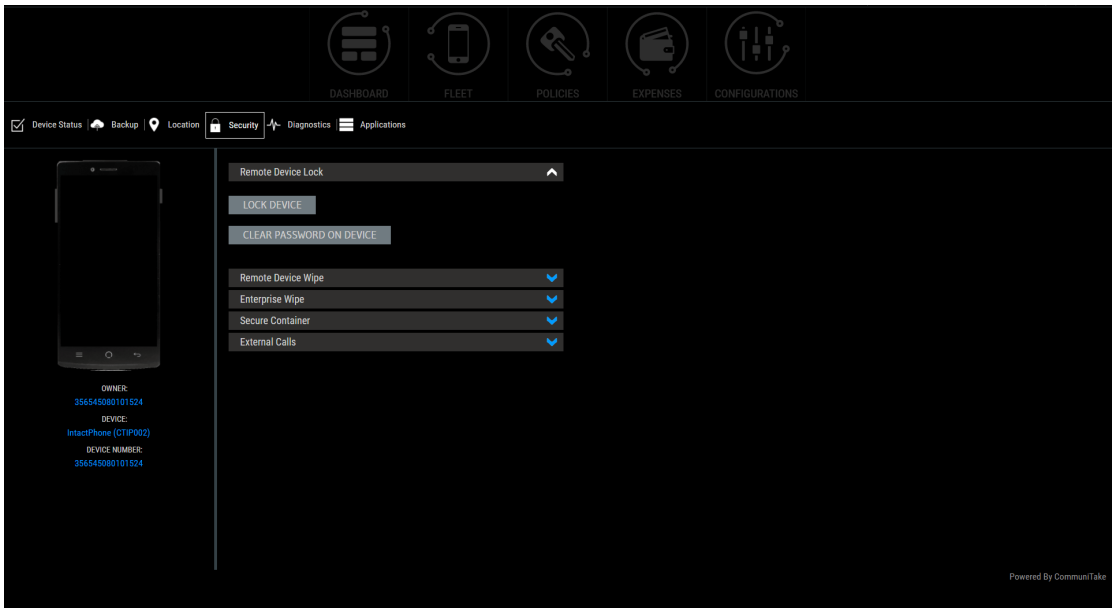
Locking a device from afar will require from the device holder to enter a set password prior to operating it.

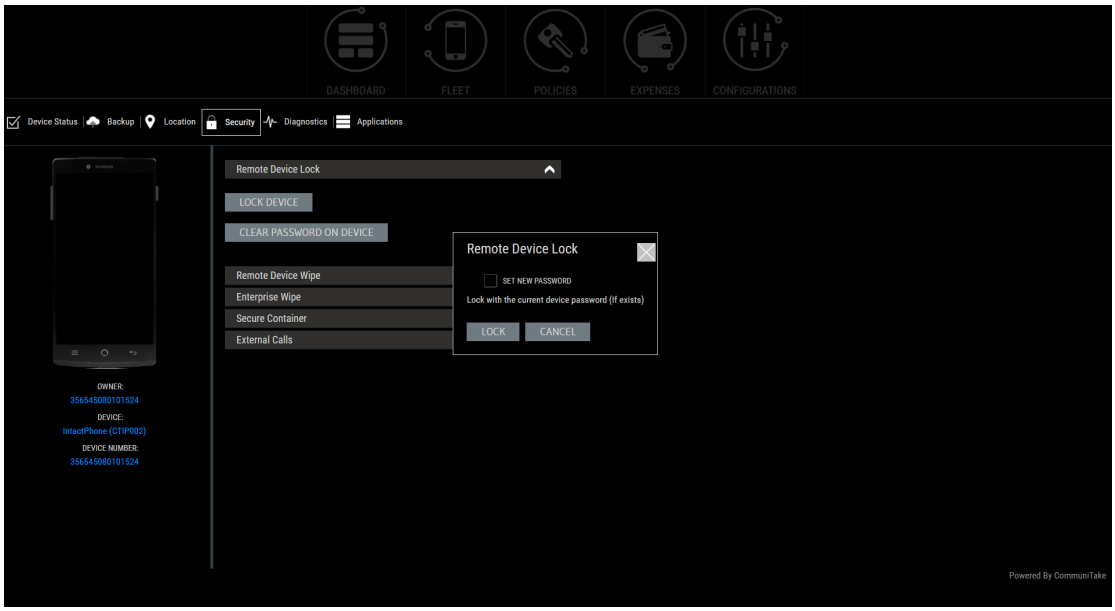
Lock device features:

Feature	Description
Lock device	Lock with the current device password (If exists): Locks the device with the password that was defined Or, Set New Password.
Set lock password	Defines the password for the lock without activating the lock.
Clear on-device password	Clears the on-device password that is used to lock the device.

TO LOCK A DEVICE

1. Select the group to which the device is assigned.
2. Click once on the device line in the devices table.
3. Click on the **"Security"** button.
4. Click on the "**Lock Device"** Button.





Tip You should define a minimum of four (4) characters password on an Android device. Lock password is not supported on all mobile operating systems.

Important When setting a new lock password, the password must be compliant with current password policy - otherwise it might fail.

TO UNLOCK A DEVICE

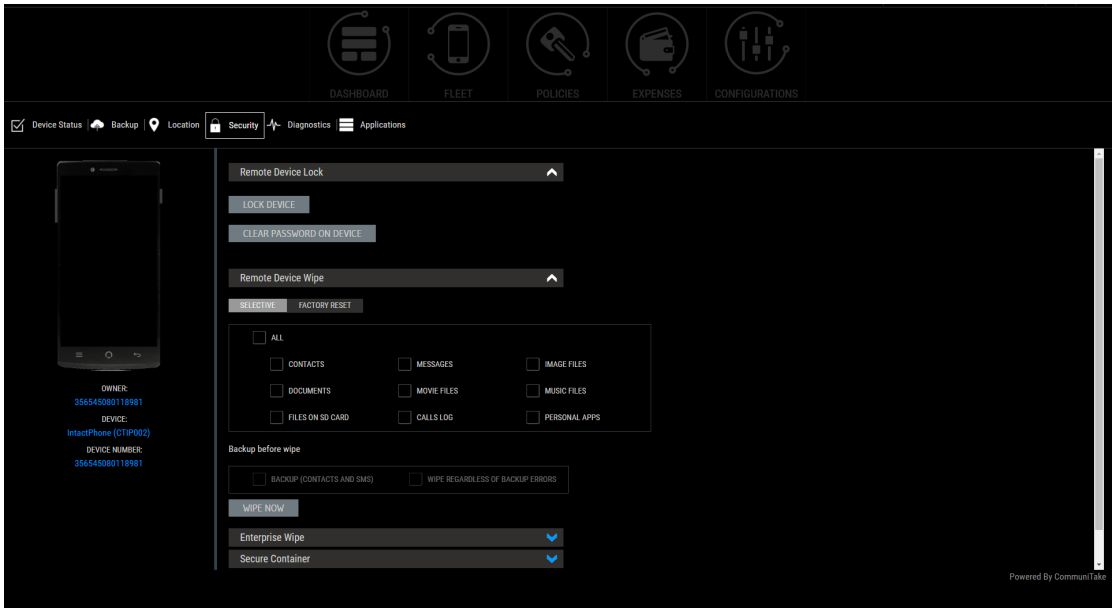
Unlocking the device is done by the device holder: once activating the locked device, the device holder will be requested to key-in the unlock password. Entering the password will unlock the device.

Another option is to clear the on-device password thus no password will reside on the device.

WIPE ON-DEVICE DATA

Wipe on-device data has two dimensions:

1. Choosing the on-device data that should be wiped:
    a. Complete wipe via factory reset.
    b. Selective wipe through which the device holder can select to wipe only portions of that data stored on the device.
2. Under which conditions will the wipe data function be activated:
    a. Only after a successful backup.
    b. Regardless of a successful backup.



Note Device Wipe operation requires to key-in a password prior to completion

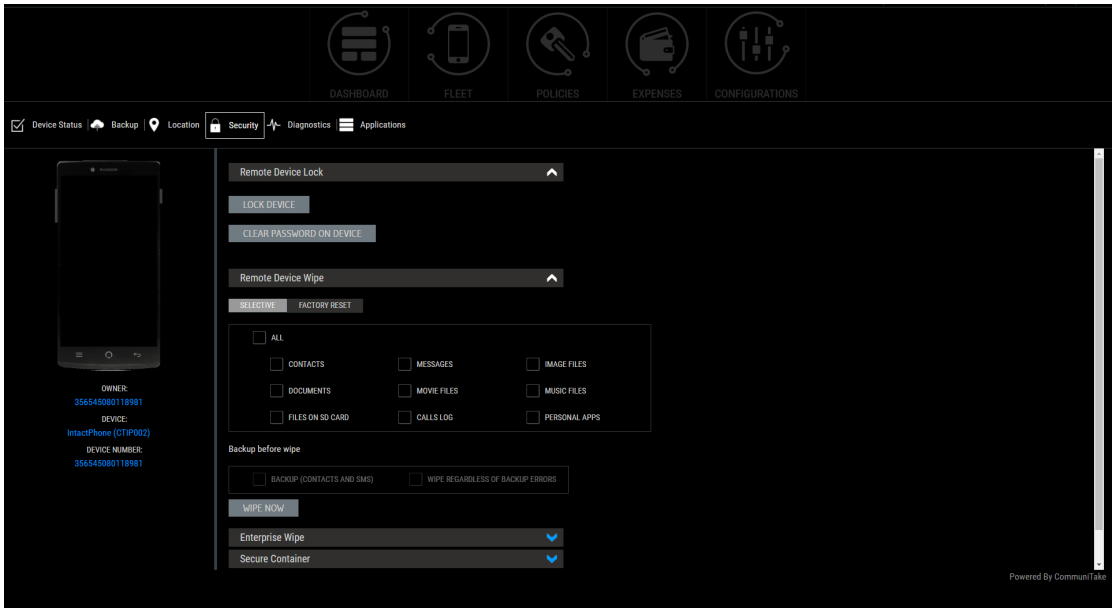
TO ACTIVATE A COMPLETE WIPE

1. Select the group to which the device is assigned.
2. Click once on the device line in the devices table.
3. Click on the **“Security”** button.
4. Check the **“Complete Wipe Factory Reset”** checkbox.
5. Check a backup before wipe checkboxes by your preference. Checking the **“Backup”** checkbox will require a complete successful backup prior to on-device data wipe. Checking **“Wipe regardless of backup errors”** will activate a wipe even if the back was not completed successfully.
6. Click the **“Wipe Now”** button.

Important Not all the devices support Factory Reset. Factory Reset also deletes the SD card data.

Factory Reset status might not be updated when the device goes through a reset process. This is driven by the fact that at times, the device reboots before it manages sending back the reset status.

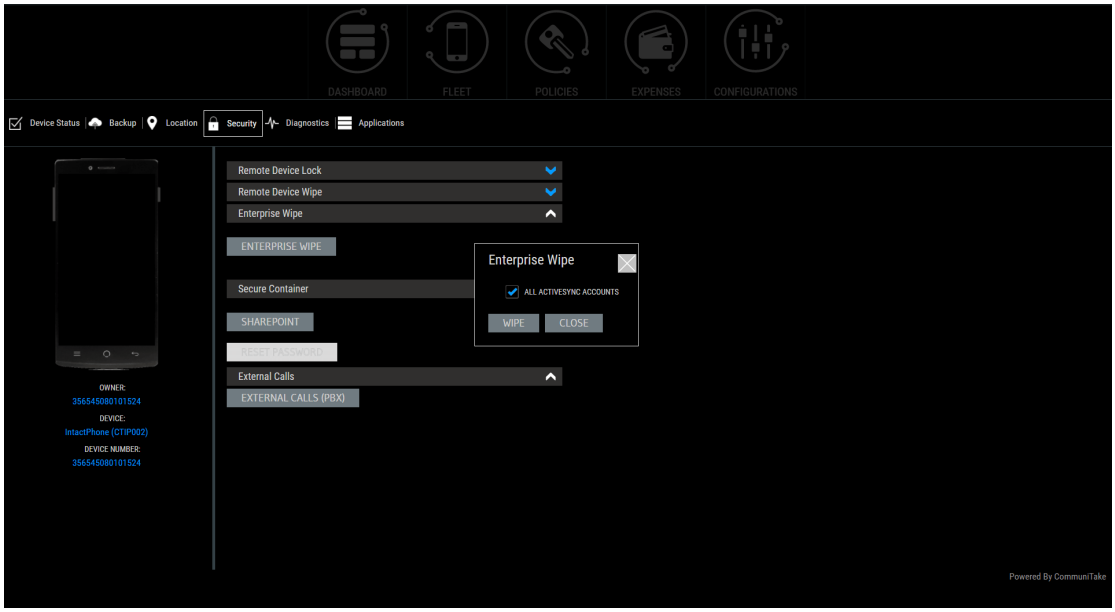
TO ACTIVATE A SELECTIVE WIPE



1. Select the group to which the device is assigned.
2. Click once on the device line in the devices table.
3. Click on the "'**Security"** button.
4. Check the data items checkboxes of your choice in the selective wipe area. You can select one or many of the data items: **Contacts; Messages; Image Files; Documents; Movie Files; Music Files; Files on the SD Card; Call Logs**.
5. Check a backup before wipe checkboxes by your preference. Checking the **"Backup**" checkbox will require a complete successful backup prior to on-device data wipe. Checking **"Wipe regardless of backup errors"** will activate a wipe even if the back was not completed successfully.
6. Click the **"Wipe Now"** button.

ENTERPRISE WIPE

Enterprise Wipe allows the system user to delete the on-device Exchange email configuration.

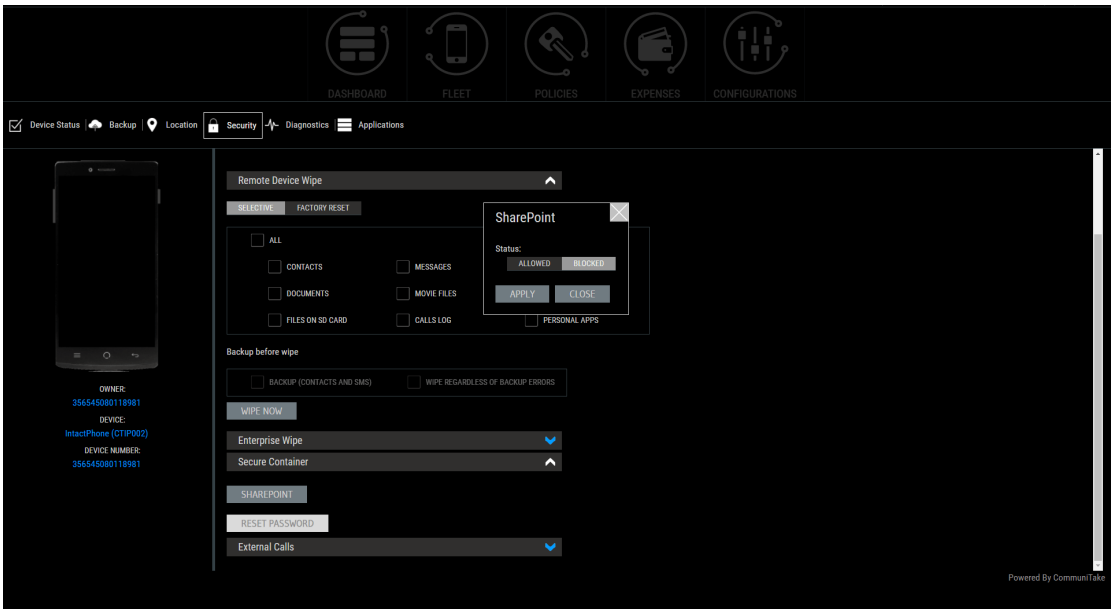


TO WIPE ENTERPRISE DATA

1. Select the devices group.
2. Select the required device from the devices table.
3. Click on the **“Security”** tab.
4. Click on **“Enterprise Wipe”**.
5. You can choose to either delete all the exchange configurations from the device or to selectively define which email account to delete by providing their email addresses.

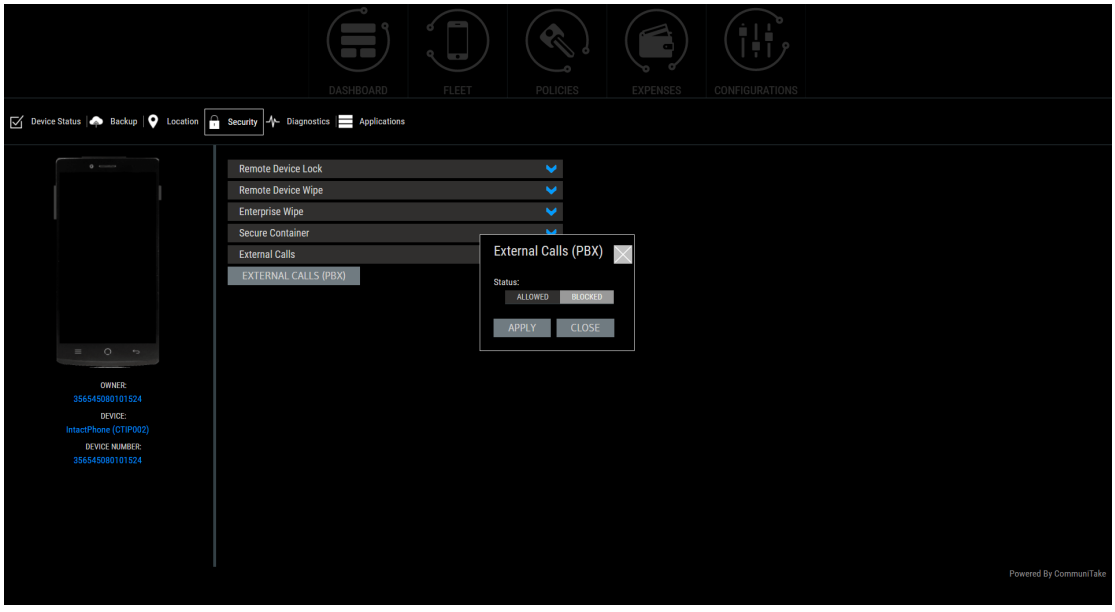
Important iOS devices can only delete Exchange configurations which were created via the **“Exchange Configuration”**.

TO ALLOW / BLOCK SECURE CONTAINER ACCESS



1. Select the devices group.
2. Select the required device from the devices table.
3. Click on the **"Security"** tab.
4. Click on **"Secure Container"**.
5. You can choose to either allow or block access to the container or set the access password.

TO ALLOW / BLOCK EXTERNAL CALLS (PBX) ACCESS



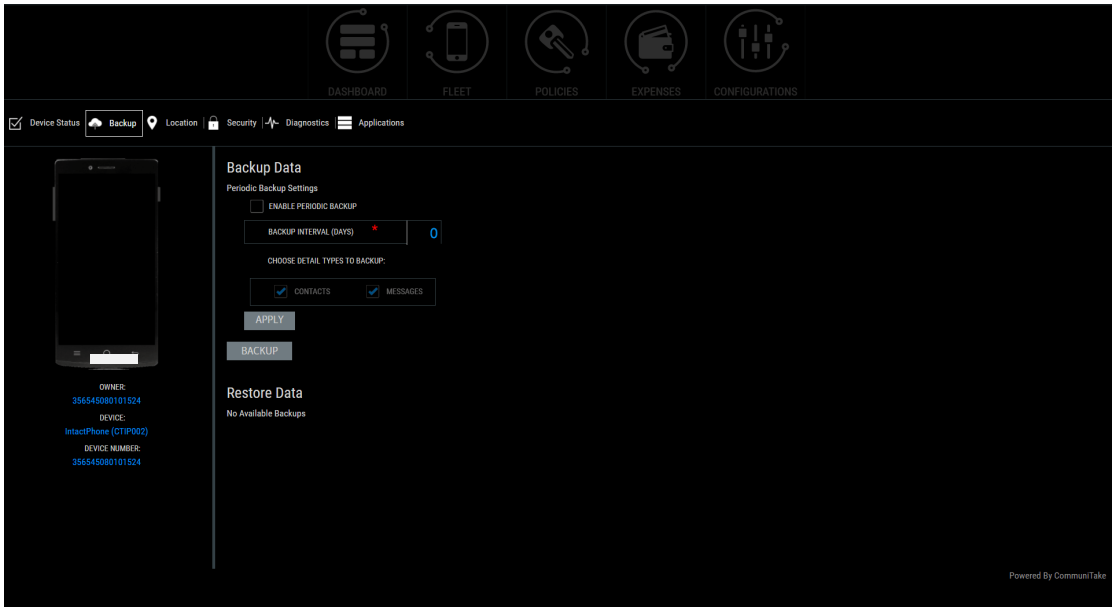
1. Select the devices group.
2. Select the required device from the devices table.
3. Click on the **"Security"** tab.
4. Click on **"External Calls (PBX)"**.

5. You can choose to either allow or block access to External Calls.

BACKUP ON-DEVICE DATA

TO BACK UP ON-DEVICE DATA

1. Select the group to which the device is assigned.
2. Click once on the device line in the devices table.
3. Click on the "**Backup"** tab.
4. There are two backup alternatives: periodic backup and on-demand backup.
    a. For periodic backup:
        i. Check the **"Enable periodic backup"** button.
        ii. Define the **"Backup Intervals"** in days.
        iii. Check which data items should be backed-up: **Contacts; Messages;**
    b. For on-demand backup
        i. Click on the **"Backup"** button. The system will back up now the data.



TO RESTORE DEVICE DATA

Restoring device data allows you to restore backed up data from one device to another device:

1. Select the group to which the device is assigned.
2. Click once on the device line in the devices table.
3. Click on the **"Backup"** tab.
4. Select the required backup from the **"Available Backups"** under Restore Data.
5. Click on the "**Restore"** button. The backed up data will be restored on the device in context.

Important Restore can generate duplicated Contacts and Messages.

Different devices support different contact attributes. Contacts might be slightly altered and may lose parameters if restored to a different device.

A user can restore data to a new device. If the user has a new device in the system defined for him, replacing a previous device, then the restore data procedure can be apply to the new device thus transforming previous device data to the new device.

EXCHANGE ACTIVESYNC POLICY

Exchange ActiveSync settings enable to block or allow a device to access the Exchange server.

TO MANAGE EXCHANGE ACTIVESYNC POLICY

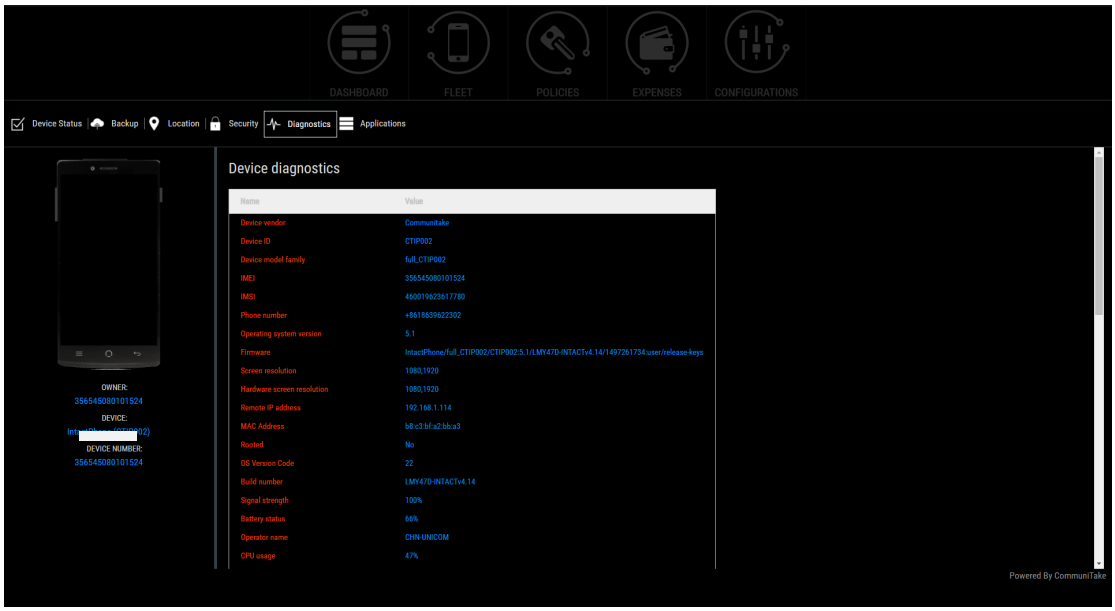
1. Click **"ActiveSync Policy"**.
2. If the device is not automatically detected in the Exchange:
    a. Enter the email which is defined on the device and click **"Show devices for this email**".
    b. Select the device from the list.
3. The current status of the device in the Exchange server is displayed.
4. Set a new status by selecting the required status radio button.

Important The device must try to connect to the Exchange server at least once before its status can be set.

If a device has more than one Exchange email account, the status will be set for all the email accounts.

DIAGNOSTICS

Device diagnostics provides insights on the device' hardware, software and connectivity parameters.
It can provide an initial directive to problems or drivers for malfunctions.



Diagnostics Criteria	Description
Device vendor	Device manufacture name.
Device ID	A unique identifier for the device. The device ID is used when accessing the IntactPhone database and other device management services.
Device model family	The family of manufacture models to which the device is related
IMEI	The International Mobile Equipment Identity is a unique number identifying GSM, WCDMA, iDEN and some satellite phones. The IMEI number is used by the GSM network to identify valid devices.
IMSI	An International Mobile Subscriber Identity is a unique number associated with all GSM and UMTS network mobile phone users. It is stored in the SIM and is sent by the phone to the network.
Operating system version	The version of the system that runs the device.
Screen resolution	The current actual screen resolution on the device.
Hardware screen resolution	The maximum screen resolution possible on the device.
Rooted	Device status whether rooted.
Signal strength	Device's connection strength.
Battery status	Device's battery charging state.
Operator name	The name of the service provider.
RAM free memory	The free device's Random Access Memory (RAM) in which information can be accessed in any order.
User profile	User permission scheme to self-operate the system.
Ringtone volume	As is.
Network type	The type of wireless network by which the device operates such as GSM, UMTS etc.
Speaker	An indication whether the speaker is on or off.
Speaker volume	As is.
UI language	Language used across device's user interface.
MCC | Mobile Country Code	Mobile Country Code (MCC) is used in identifying mobile stations in wireless telephone networks, particularly GSM and UMTS networks. An MCC is often combined with a Mobile Network Code in order to uniquely identify a network operator. The MCC is part of the International Mobile Subscriber Identity (IMSI) number, which

	uniquely identifies a particular subscriber, and is stored on a removable SIM card.
MNC | Mobile Network Code	A Mobile Network Code (MNC) is used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile phone operator/carrier using the GSM, CDMA, iDEN, TETRA and UMTS public land mobile networks and some satellite mobile networks.
APN | Access Point Name	Access point name (APN) identifies an IP packet data network (PDN), that a mobile data user wants to communicate with. An APN consists of two parts: Network Identifier and Operator Identifier.
Client version	The Intact client version installed on the device.
Cell ID	A GSM Cell ID (CID) is a unique number used to identify each Base transceiver station (BTS) or sector of a BTS within a Location area code (LAC) if not within a GSM network.
Cell location area code	A "location area" is a set of base stations that are grouped together to optimize signaling. To each location area, a unique number called a "location area code" is assigned.
RSSI | Received signal strength indication DB	Received signal strength indicator (RSSI) is a measurement of the power present in a received radio signal.
Roaming	An indication whether the device in a roaming state.

APPLICATIONS

The **“Applications”** section presents all the applications that reside on the device. Selecting a specific application will show its related details such as name, version and location URL.