ENTERPRISE MOBILITY - FAQs

INTRODUCTION

The CommuniTake Enterprise Mobility solution empowers enterprise IT personnel to centrally manage mobile device assets, deliver high quality mobile experience, provide data security, while simultaneously maximizing employee productivity and monitoring the cost of mobile use. The CommuniTake Enterprise Mobility solution guides IT with relevant insights on the mobile devices; dynamically deploys enterprises policies and simplifies technical support via remote access. With CommuniTake Enterprise Mobility, every device holder can perform at his best within the limitations imposed in accordance to the enterprise philosophy.

ENTERPRISE MOBILITY - BUSINESS FAQ'S

What CommuniTake Enterprise Mobility is for?

The enterprise mobility environment creates new challenges for the CIO. Digital mobile devices are becoming more instrumental than ever in execution of daily tasks. As these devices become more crucial to the enterprise, they create a dual challenge:
(1) How to best control security exposure;
(2) How to maximize device capabilities across the business realities.
Enterprise Mobility resolves those challenges posed by mobile device by executing on the following directives:

- Protect the connected employee and organization by managing risk situations
- Monitor mobile assets utilization and control outlays

Enterprise Mobility allows the following salient capabilities:

Assets Management. It provides a centralized comprehensive view of the enterprise and BYOD mobile assets. One can see all of the devices, their assigned applications and their on-device hardware, software and connectivity parameters that are of importance to ensure enterprise mobile use compliance.

Policies Management. It allows the enforcement of on-device password policy, on-device data backup / restore policy, access control policy, including configuration for Exchange ActiveSync, WI-FI, VPN and APNs.

Mobile Applications Management. The Enterprise Mobility allows enterprise IT to define which on-device applications are mandatory and which are prohibited. The system constantly monitors the overall deployed applications across the enterprise's devices and provides a mechanism to define applications' status. It implements the chosen policy through automated procedures of alerting, installing and uninstalling applications.

Mass Deployments. The Enterprise Mobility facilitates mass deployment campaigns on pre-defined devices groups. Device groups are managed through organizational hierarchies as used by the system for assets management and Mobile Applications Management. Defining on-device content for a group generates an automated distribution process.

Device Data Protection. Enterprise Mobility allows enterprise IT to locate a device on a map or via its alarm; lock access to it; wipe on-device data from afar and back-up and restore device data. These functions can be also performed by the device owner through self-service portal.

Use Control. The use control in CommuniTake Enterprise Mobility provides business views of the device use. It analyses call, messaging, data and roaming usage. It presents the implied enterprise expense and the heavy users along with indications to usage by threshold.

Remote Support. The Enterprise Mobility enables IT personnel to assume complete control over the enterprise mobile devices from afar. The ability to see the device screen and operate it in real time allows quick understanding of the issue and resolving it in a fraction of the time.

How can I benefit from CommuniTake Enterprise Mobility?

Enterprise Mobility introduces benefits in several dimensions:

Shifting to new mobile devices. Enterprise Mobility allows you a simple way to shift to new devices by automated enlisting and policies definition processes.

Implementing mobile policies. There is a delicate balance between enforcing the business security and use policies and the fact that most of the devices are owned by their holders. Enterprise Mobility allows the business to set and define security; data protection and applications use policies across the employees' devices with provisioning and monitoring mechanisms but without imposing harsh reality on users. These operations reduce data security breach and increase employees' productivity.

Increase efficiency, reduce costs. Advanced support capabilities reduce idle work time and increase employees' productivity. The expense control module restraints the use cost and the roaming expenses.

How can CommuniTake software improve enterprise mobility?

CommuniTake Enterprise Mobility ensures always connected professionals; higher productivity; reduced idle work time searching for support or using non-work applications; mitigating mobile work force malfunction risks via remote guidance by a back office expert; reduced use and roaming expenses; aligning price plans to users by their actual use; resolving stolen / lost devices scenarios; allowing 24/7 support while reducing the dependency on an external support; reducing security breaches.

How can I register to the service? What is the registration flow?

After registration to the service, you will receive a welcome letter, allowing you to activate the service with your owned defined password. Once defined, you will have access to the device management and remote support capabilities. You will have a dedicated portal through which you can get more information and training material or access to the support team.

Is the solution delivered in SaaS? On-premise installation?

The solution is available both via the cloud or an on premise deployment.

Which data is kept and where?

Enterprise Mobility keeps devices attributes: User Name; Phone number; Group; Device vendor; Device model; Last seen date; Previous backups; Password policy status; OS; OS version; Firmware version; Client version; Rooted status; Country; Roaming; IMEI; IMSI; Whitelist violations status; Blacklist violations status; Remote control enablement; Wi-Fi configuration status; Exchange ActiveSync configuration status; VPN configuration; iOS restriction configuration.

In addition, the system keeps the following: the policies parameters as defined by the system administrator such as prohibited applications and mandatory applications; device users as defined by the system administrator for self-service operations; device contacts and messages based on the backup policy and its related activities; use data (calls minutes; messages; data) based on devices internal counters.

The data is stored on the system server that is located in Europe.

All private data stored in the system is fully encrypted.

Is there a limit to kept data size?

There is no limit to the data size.

Can Enterprise Mobility be used for private devices?

Yes, the limitation is as the number of licenses your organization has purchased.

Can Enterprise Mobility be used for devices that were not purchased via my operator?

Yes, the limitation is as the number of licenses your organization has purchased.

Should I use Enterprise Mobility for all the devices in my organization?

You should exercise your judgment regarding the risks. Activate Enterprise Mobility for all the devices for which you wish to control data security, activate data protection capabilities, provision application use or provide better support.

Who in my enterprise should operate Enterprise Mobility?

Enterprise Mobility is usually managed by an IT stakeholder with data security awareness. This person should take a proactive role in monitoring the policies fulfillment. This person should exercise decisiveness and assertiveness. It is recommended to align the mobility policies with the organization's human resources department. This will ensure employees buy-in to the process.

How can I gain employees' cooperation on device policies?

The system is aimed at friendly users. It assumes that the users are known and have a willingness to participate in the organizational effort for better enterprise mobility. There is a need to share with the employees the policies and the drivers for it. Continuous and open communication with the employees should build their confidence and desire to be part of the effort. When a deviation takes place, it is better to offer the employee to take a corrective action by himself and not take potentially severe, one-sided corrective measures.

Should all employees have the same mobile policies?

No, these can differ by the managerial level or by their professional department, pending their daily tasks.

How can I best use the management by groups function?

Groups allow you to define the logical audiences that require different device management approaches. It is best to utilize these groups based on the organizational logic and differences in the members' daily lives. It is best to define groups that represent different needs for applications use (such as marketing) or security risks (such as top executives). An inferior practice will be to define groups of device types. Devices are handled by the policy based on its OS capability so there is no need to define stand-alone groups such as Android devices, iPhone devices, etc. A specific device can be part of only one group and as such, it should be allocated to the best structure that reflects the needs of the organization.

Most of the system's policies and configurations can be inherited from the parent group allowing you to maintain higher group granularity but with the same policies.

What are the recommended policies for security, apps and backup?

Policies are driven by several factors such as the business's philosophies; Bring Your Own Device (BYOD); the internal inherent acceptance by employees to cooperate with the management etc. A good policy will maintain a proper balance between the interests of the organization and the freedom that employees look for.

Security: make sure to deploy a password for every device. Data protection capabilities are there once the client is installed.

Applications: consumer applications serve the professional lives of the employees. Make sure to only prohibit applications that generate real threat of data sharing or leakage without really contributing to the business. BYOD device should have more freedom in compare to enterprise liable devices.

Backup: define backups across the device. In a stolen / lost device scenario, you might be required to wipe the on-device data but you will have sufficient time to backup prior to wipe.

Self-service: grant self-service capabilities to employees. It will allow them better control over their data protection hazards while encouraging more cooperation.

Can I operate the policies equally over all the devices?

No, mobile operating systems differ regarding elements such as password complexity, the ability to remove applications and the ability the remotely takeover a device for support. The system is built in such a manner that all you need to do is to define your policy once, and the system will publish your request to the device and it will be fulfilled according to the capabilities of the operating system.

Can I remotely operate and manage a device without the awareness of the device holder?

Device management regarding policies management can be done without the awareness of the device holder. A remote takeover for support purposes requires that proactive consent of the device holder.

What self-service operation can my employees operate via the Enterprise Mobility?

Employees can perform the following: locate a device; activate device's alarm; lock a device; wipe a device directly or after a successful backup; selectively wipe a device or perform a total factory reset; activate backup policy; backup the device; view device diagnostics; deploy recommended applications from an enterprise apps portal.

How can I grant employees access to the self-service operations?

When adding a device to the system, make sure to fill in the user email in the 'Add new device' box. This will send a welcome letter to the user, allowing him to activate his self-service capabilities. You can also add this after you have enlisted a device in the system in the ownership editing screen.

Which mobile operating systems and versions are supported by CommuniTake Enterprise Mobility?

The application supports Android 2.2 and above and iOS 4.0 and above.

COMMUNITAKE ENTERPRISE MOBILITY - TECHNICAL FAQ'S

What are the prerequisites to operate Enterprise Mobility?

Internet Browser (IE 7, 8, 9; Firefox; Chrome).

Remote Care:

Each agent workstation or Citrix server must have the following software installed:

Internet Browser (IE 6, 7, 8, 9; Firefox; Chrome).

Sun Java JRE 1.6 with minimum version of 1.6.27.

Access ports: Port 80: http; Port 443: SSL-based TCP

The ports must have access to the following IP address:

Server	IP	Port	Region
support.communitake.com	46.137.110.154	80/443	World
r1.communitake.com	46.137.110.162	443 (TCP)	Europe (default)
r2.communitake.com	50.19.104.23	443 (TCP)	USA East
r3.communitake.com	212.199.177.153	443 (TCP)	Israel
r4.communitake.com	54.232.122.90	443 (TCP)	South America
r5.communitake.com	122.248.248.56	443 (TCP)	Singapore
r6.communitake.com	118.194.128.10	443 (TCP)	China
R7.communitake.com	54.251.162.183	443 (TCP)	India

How secure is the CommuniTake Enterprise Mobility Application?

All communications are encrypted using industry standard HTTPS and SSL. The private data that is stored on the system server is encrypted. There is a clear segregation between different customers and users. One customer cannot see the information from another customer. One user cannot control another user's device.

The SMS (text) message has not reached the target device, what should I do?

This is probably an SMS gateway issue. Select the device under the "fleet" tab. Click on the "Send SMS" in the pop-up located at the bottom of the screen.

You can also download the device client directly by directing the device's browser to:

http://mydevice.communitake.com/d.

(This manual process is not supported for iOS devices).

You can also select the device (or devices) which did not receive the SMS and click "resend SMS".

The on-device client installation is stuck, what should I do?

The device must have a valid SIM card in order to receive SMS messages and push notifications. On-device client installation may take a few minutes in rare cases.

For reinstalling, make sure that the client is not installed on the device. If it is, use the device's "uninstall application" mechanism to make sure that all the files that are related to client are removed.

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.

To make the client simulate a push notification, open the client on the device, click on options and click on "Sync Now".

I do not see a complete view of all my devices in the system dashboard.

If you cannot see all the devices, it might indicate that not all the devices have successfully concluded their enrollment process. You can check their status via the dashboard view.

None of the Enterprise Mobility operations are working on the target device (backups, location update, application or policy enforcement).

The speed in which a device will perform a task is directly connected 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 command that requires fulfillment time (Get location, for example), and immediately after it, the user issues a backup request, the backup will not start until the first command finishes and the device connects to the server to get the next command in line.

If the client is not properly installed on the device, the device will not publish its actual capabilities to the application server. It means that the application server is not ready to properly issue and manage requests.

Enterprise Mobility does not perform "live", "no latency" changes on multiple devices. Requests are published to the device as push notifications via a 3rd party service. Though this usually performs immediately, it might take a few minutes for requests and their driven changes to propagate to the devices.

How can I assign two devices to one employee?

Simply define another device to the user. The user doesn’t have to be in the same group. Every device will get its policies & configurations based on its group. When the user logs in to the self- service operation, he will see all of his devices.

I want to swap ownership of a device between employees.

If you want to keep the device in the same group, you can click “edit” and change the user.

You can also select the device. Once selected, click on the “move” tab in the pop-up at the bottom of the screen and select the target group.

How can I know that the inherit policy actually works?

If the parent group has an assigned policy and the inherit tab was selected, the inheritance mechanism automatically works.

In general, if the OS supports silent install/uninstall then all actions are silent. If not, a notification is displayed to the device holder which automatically directs him to the install/uninstall page of the required application.

The status can always be seen in the “fleet” table.

How can I unlock the device from afar?

If you have locked the device and now wish to unlock it, remove the assigned password, if you have assigned one, or indicate it to the device holder.

Can I define application policy via one application for all the devices?

No, as each mobile operating system (OS) has its own built application, even for the same application. For every application that you wish to define across multiple mobile OSs, you should specify and include all the relevant OS versions of this application.

Getting the device's location failed.

Getting the device's current location can fail if the device has no GPS reception and is unable to detect its location via the network.

My device location does not show the current location.

Click on the refresh tab to generate an accurate device location presentation.

I want to remove a device from the system, what should I do?

Use the remove device mechanism in the devices "fleet" view. After removing a device, the device should show an alert saying it was disconnected. The device will try to connect to the server and will fail. 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. Use the device's application manager to completely uninstall the client, instead of just deleting it.

I cannot delete a group from the groups' hierarchies.

Make sure that the group does not contain devices allocated to it. Prior to deletion, a group should be with no devices that are assigned to it.

I forgot my login password, what should I do?

You can use the "Forgot my password" link available on the login page to reset your password.

If the process was completed successfully you should receive an email with information about how to set a new password.

I added a device but forgot to add a user for that device.

Select the "Fleet" tab and click “Edit” and set a user for the devices. New users will receive a welcome email.

I want to move a device to a different group, how can I do that?

Select the "Fleet" tab and click “Move” and set the device in its new group.

I want to change the location of a group in the hierarchy. How can I do it?

At present, group change location is not supported in the system. In order to move a group location, you will have to move the devices that are allocated to it, delete the group and define it again in its new location, and re-allocate the devices.

Can I restore a backup to a different device? How can I shift data from one device to another?

We consider these backups as private user information as such restore can be done between different devices in two ways:

1. If the new device is added with the same phone number as the old device then it will see all the previous device’s backups
2. The user can see backups from all his devices.

Note: 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.

Which content is backed-up and restored?

For Android devices: Contacts and Messages.

For iOS devices: Contacts.

Are contacts being restored by their source?

No, the application restores all the contacts to the contacts book in a unified manner, without maintaining its source orientation.

The usage on the expense control is not accurate.

Expense control uses the internal device counters to present the implied usage. These counters are not as accurate as the billing system so some differences may occur. However, the numbers will be accurate enough to monitor the use and generate alerts on exceptional usage.

How can I impose policies?

If an employee does not respond to your device management requests, you can activate event driven enforcements located in the system's "setting". In addition, you can manually lock the device with your own set password, and block the device from accessing the mail server or the content container. The device holder will be forced to approach you and fix the policy based on your directive.

How can I know that an employee has uninstalled the on-device application?

The application presents a client removal KPI for both Android and iOS. The administrator can define an alert for this KPI.

Do I need to allocate a user for each enrolled device?

No, you can define a generic PIN number per group. Every device that is added to this group will be enrolled based on this PIN number. A user can be defined to this device later on.

What is the process for supporting iOS devices?

You must complete a few simple steps in order to start adding iOS devices to the system:

1. Click "settings" in the top left corner on the CommuniTake Enterprise Mobility UI.
2. Fill in the "iPhone certificate request" information and download the certificate request file
3. If you don't already have an Apple ID, please create one (for free) in the following link: http://appleid.apple.com/
4. Sign in using your Apple ID in the following link: https://identity.apple.com/pushcert/
5. Click "create certificate" and agree to the terms of use
6. Upload the certificate request file from step 2, after a few seconds your certificate will be ready for download
7. Upload this certificate in the "Settings" page

How do I add an iOS device to the system?

You start by filling in the device's information, similar to adding any other device. When opening the link from the SMS/Email, instead of downloading an application, you will download a profile. Accept the installation of the profile to complete the registration process.

What happens when you disable the camera via the iOS restrictions configuration?

When false, the camera is completely disabled and its icon is removed from the Home screen. Users are unable to take photographs.

Can I use the system for managing an iPad or an Android tablet?

Yes. Enter an email address instead of entering a phone number. The download client link will be sent by an email instead of an SMS.

I get an error when trying to add a new iOS device

This can be caused by several causes

1. You did not register your organization with CommuniTake via Apple. There are a few simple steps that must be done with Apple before you can add iOS devices to the system. Please consult the user manual for more details.
2. The date on your device is totally wrong thus rendering the certificates invalid. Make sure that the device date and year are correct.

I started an import from my LDAP but now I cannot open any group

The import process can take some time, driven by the amount of groups, users and the changes done in the LDAP from the last time an import was done.

During this time, the system blocks access to all the LDAP groups. The status of the import is displayed in the top right corner.

I connected the system with my exchange server and now new devices cannot access their mail.

This means that the exchange settings you have created block all new devices. It means that only devices which are registered to the Enterprise Mobility system can access their mail.

Once you add a new device to the Enterprise Mobility and set up the exchange account on that device, click the device in the "Fleet", go to security and change the device to "allowed" in the exchange configuration.

I want to allow/block a device from accessing the exchange server but I don't see the device in the list.

In order for the system to change the device's exchange status, the device must first try to connect to the exchange server. Once a connection has been made (even if the device is now blocked) the exchange server "recognizes" the device and the device management system will now be able to find it.

I need to send a status report regarding current system status.

The dashboard can be exported to an Excel file by clicking the "Export" button.