

## mySync Management - product features

mySync Management Service enables total mobile device life-cycle management from the initial setup to the final device wipe when the device is restored to factory condition. mySync Management is a true mobile device management (MDM) solution. The most common managed features are listed below in section "Device features which can be remotely managed".

mySync Management Service is a separate and independent service from other mySync Services. mySync Management can be purchased with or without mySync Express Service.

### Common mySync architecture features

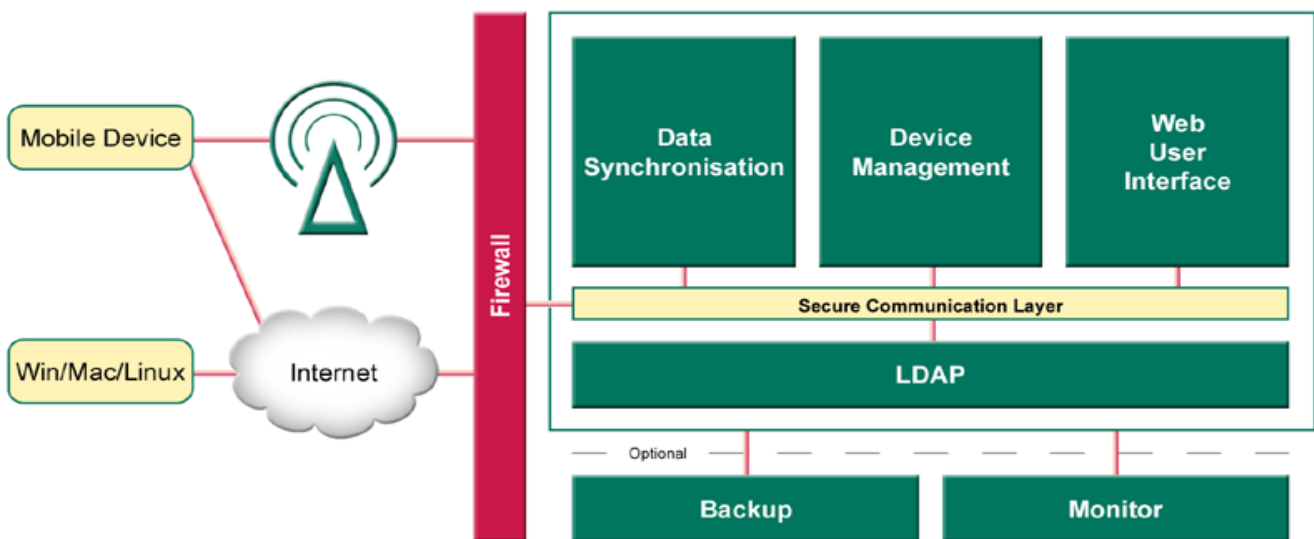
mySync extend the featureset way beyond comparable products on the market by adding the following:

- ▶ ISP-style, true firewalled multi-organisation architecture on single host
- ▶ optional HA implementation, and optional scaled-to-millions implementation
- ▶ Role-based architecture: supervisor, vendor, organisation manager, and end user
- ▶ Users with roles have rights assigned to them for more fine-tuned settings
- ▶ Web service interface for managing the system from external system
- ▶ Secure web portal for full synced data and settings management, and reporting
- ▶ All of the above makes mySync SaaS-ready; actually SaaS is the preferred mySync delivery method
- ▶ End user interface localisable in few days to any language; currently English and Finnish
- ▶ SMS-capability supports GSM modems, and true operator/carrier SMSC connections, or both
- ▶ One user can have more than one devices in his/her account at any one time
- ▶ mySync is available as an while label product, so it is easily re-brandable
- ▶ There is also support for over 500 operators/carriers world-wide for automated settings delivery

### Compatibility

- ▶ S60 3<sup>rd</sup> Edition and 5<sup>th</sup> Edition devices from Nokia, Samsung, and many others
- ▶ UIQ3 devices from Sony Ericsson, Motorola, and others
- ▶ *if required:* Windows Mobile devices, Nokia S40 5<sup>th</sup>, and 6<sup>th</sup> Edition devices

mySync Management Service requires an OMA DM capable device. There are over 150 supported models.



Above: Full mySync architecture schema with both device management and data synchronisation. HA features are not shown.

*continued...*

## Setup mySync Management

mySync Management sends the initial settings to a new device. With those settings the device is tied to be part of the service, an organisation and its standardised settings. In short, it is managed.

The setup is done by sending a text message to the device. When the message is opened, the settings are accepted, and mySync is set as a trusted service which can remotely and unattended manage settings on the device. Management is done by organisation manager, and optionally by the user.

Setup phase normally takes only few minutes, and it includes typing in some core user and device data. It is possible to setup (and manage) organisations, users and devices via web service, too.

## Using mySync Management

mySync Management Service is always used over SSL-secured connection with a web browser. Each organisation has its own manager, which manages devices and users for the organisation. There can be more than one manager, and the management can be outsourced fully or partly.

All users may optionally be allowed to logon to mySync portal to manage their own device(s). On the portal they can lock a lost device, or unlock a found device. Optionally they can also change device brand/model, send new settings, etc. mySync Management integrates to mySync Express.

## Device features which can be remotely managed

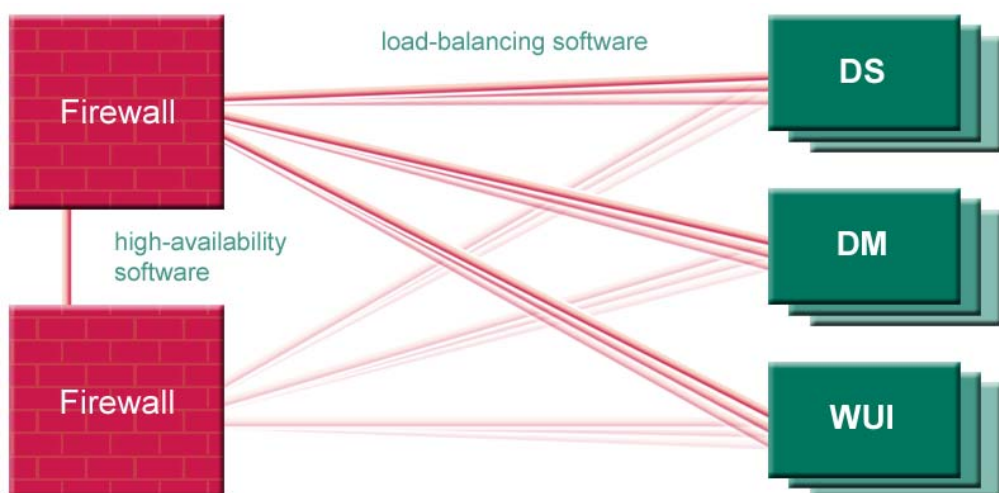
There are over 100 item to be managed, so listing them all here is not feasible.

The number of manageable settings is also growing rapidly as the devices get smarter.

Next list contains the most important settings segments which are manageable:

- ▶ General settings, security settings, data sync settings, email settings, camera activation
- ▶ Operator/carrier access points
- ▶ All settings for Nokia Mail for Exchange v2.0+
- ▶ All settings and AV updates for F-Secure Mobile Security (antivirus and firewall) v4.0+
- ▶ Passwords for device and any supported program installed in the device (manager and user, both)
- ▶ Device security code (currently only S60 3<sup>rd</sup> Edition and later devices)
- ▶ Internet telephony VoIP and SIP settings (S60 3<sup>rd</sup> Edition and later devices)
- ▶ Install and update installed programs; some programs also support full provisioning

Managing settings also include locking (some) settings, and repairing settings erroneously changed by the end-user to keep TCO down.



*Left:  
High-available and  
load-balancing  
implementation  
architecture.  
High-availability also  
optionally scale-up  
the system.*

*continued...*

## **Sending commands to the devices remotely**

It is possible to send a command to the device to lock it with a 100+ character password. This makes it nearly impossible for anyone to unlock the device without mySync Management Service.

Obviously locked device can be unlocked. In addition to locking/unlocking, a device can be wiped to factory default settings.

Devices with F-Secure Mobile Security (antivirus and firewall) installed can be sent a command to: activate, start/stop the service, update virus signature files, and make a full virus scan on the device.

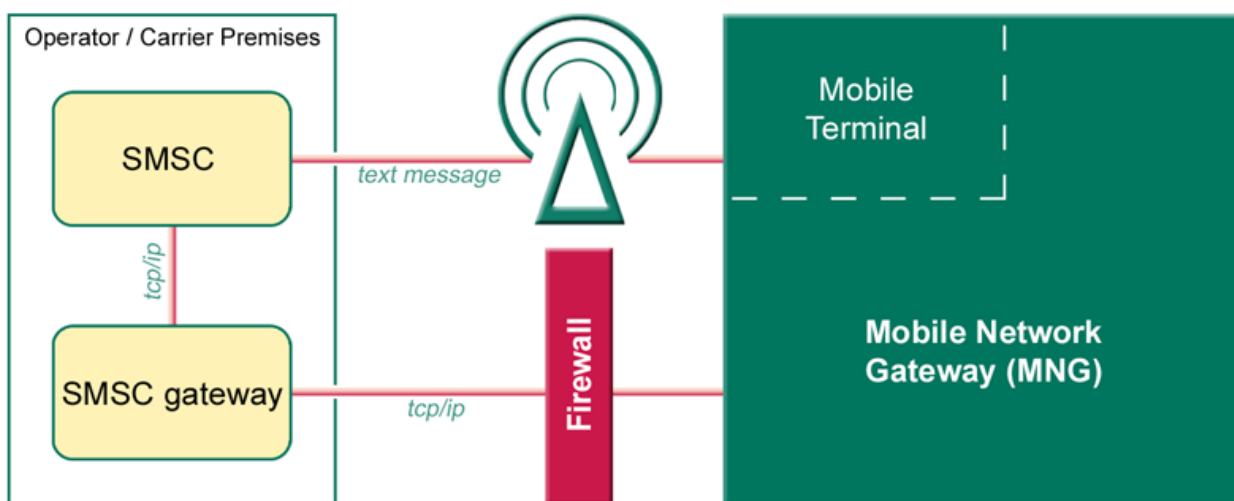
These are just few examples of what mySync Management can do with OMA DM. Additional OMA DM compatible software can easily be added.

## **Auxiliary information**

mySync Management also includes device and software inventory with reporting. There is also optional support for high security remote data erase compatible with requirements by banks, insurance companies, and military. Any OMA DM compatible software is compatible with mySync Management.

mySync Management has a complementary side, mySync Express, which is a data synchronisation service product. It is completely normal to have both, or only one side of mySync implemented.

Disclaimer: All advanced features are unfortunately not available in all mobile devices.



Top: Two routes to send text messages. MNG is a server role which can be multiplied for HA and scalability purposes.