Installation Guide SMART Manager

Abstract

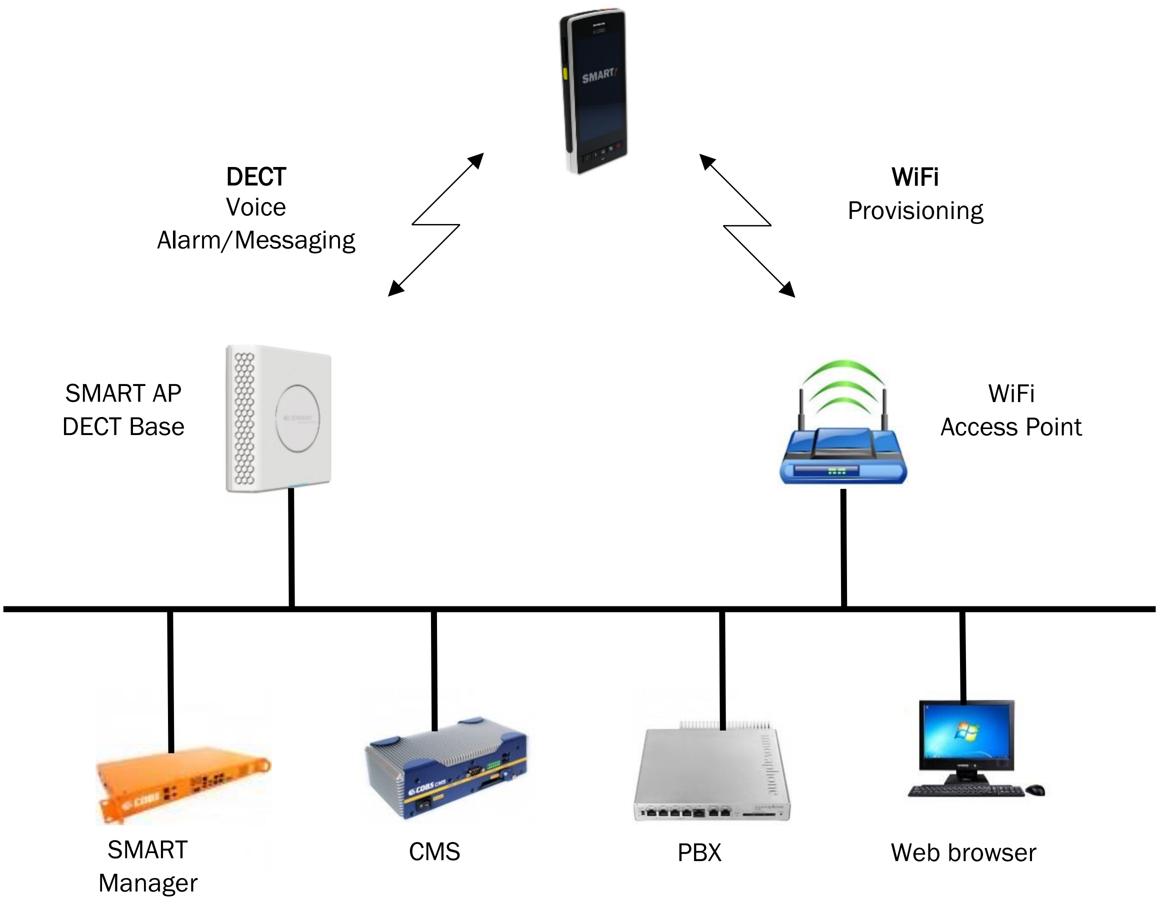
This document describes the installation and configuration of the SMART Manager.

TABLE OF CONTENTS

1 Introduction

The SMART Manager is a provisioning tool for administrating the COBS SMART1 handsets. It provisions apps, licenses and settings for the COBS.
It also handles firmware updates and updates of the apps.
The SMART Manager also has a number of different logging facilities for the handsets and other system components via syslog.

2 System Overview



The SMART system consists of a DECT system, SMART Manager, PBX, CMS and for configuration of the system we need a web browser.

The SMART1 handsets are assigned to a local number (extension) in the DECT/PBX. The local number then identifies the handset in the CMS for messaging and in the SMART Manager for provisioning.

All voice (call handling) is done in the PBX and the voice is transferred over DECT via the SMART AP base stations.

Alarm and message handling is done in the CMS and the communication is done over DECT via the SMART AP base stations (there is a possibility to use WiFi for non-critical messaging applications).

Provisioning and administration of the SMART1 handsets is done in the SMART Manager and all communication is done over WiFi.

3 Installation

The SMART Manger is distributed as a virtual application in either OVF format or as a VM Ware machine.

Virtual machine requirements:
Memory 1GB
Processors 1
HDD 20GB
Network adapters 2 (can be mapped to one physical network)

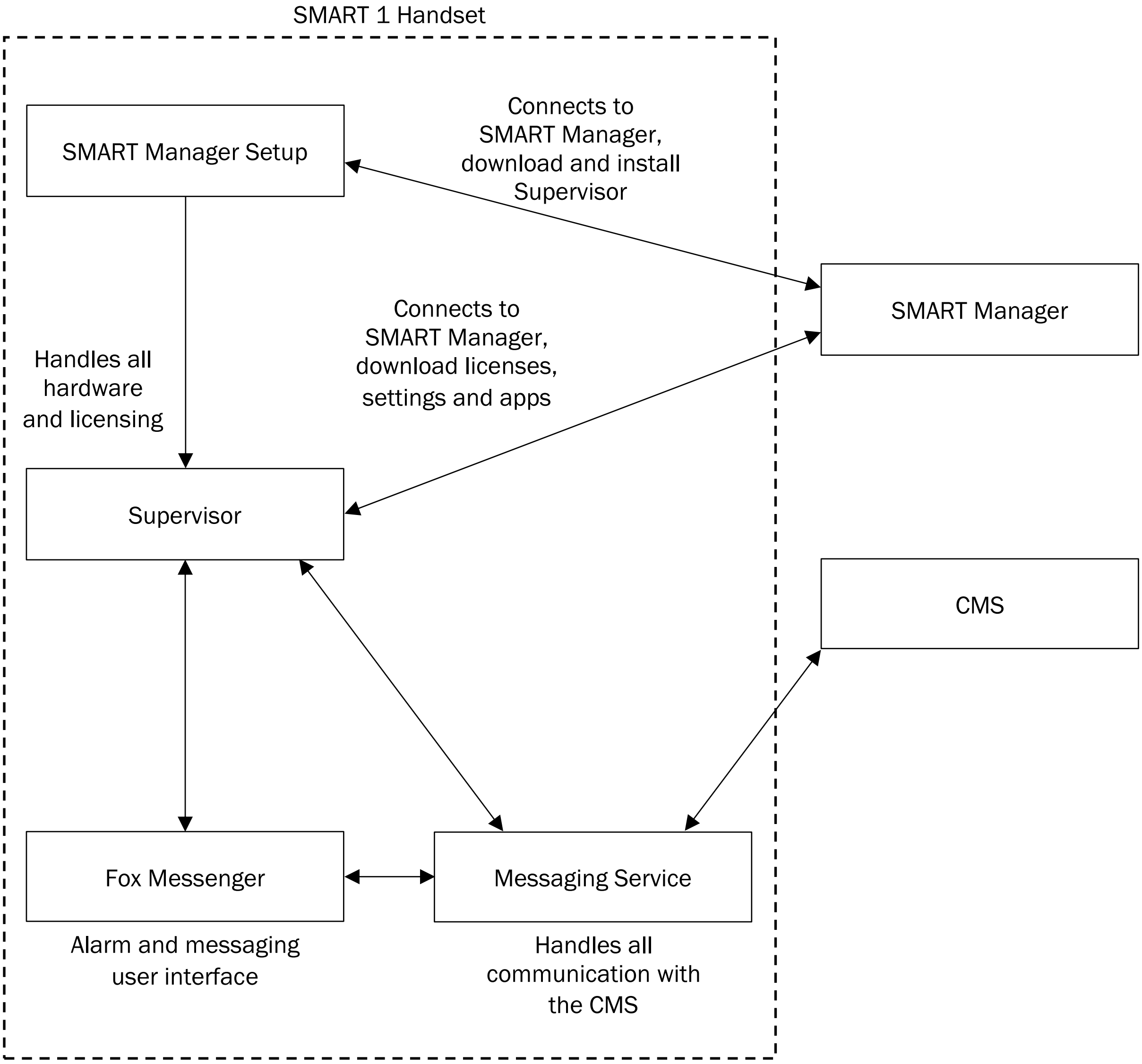
Setting up a virtual SMART Manager using the CM Ware machine files in VMWare is very simple.
Extract the files in a new separate directory.
Start VMWare Player, choose “Open a Virtual Machine”.
Select the SMART Manager “.vmx” file in the directory where the SMART Manager files where extracted.

Click on play virtual machine to start the SMART Manager.
This will start a new “empty” SMART Manager using the default IP addresses 192.168.0.1 and 192.168.1.1.
When the machine is started, start a web browser and navigate to the SMART Manager on LAN1 (192.168.0.1) or LAN2 (192.168.0.1).
The default virtual SMART Manager is supplied with a preinstalled test license that will operate for 99 hours and then needs a restart.

When using the OVF files the SMART Manager the procedure is similar but the virtual machine must be created/imported from the OVF files.

4 SMART Apps

Described here are some of the COBS SMART android apps that interact with the SMART Manager.


SMART 1 Handset
SMART Manager Setup
Connects to SMART Manager, download and install Supervisor
SMART Manager
Handles all hardware and licensing
Connects to SMART Manager, download licenses, settings and apps
Supervisor
CMS
Fox Messenger
Messaging Service
Alarm and messaging user interface
Handles all communication with the CMS

4.1 SMART Manager Setup

The SMART Manager Setup app is preinstalled in the SMART1 handsets.
It has one main purpose and that is to connect to the SMART Manager and download the Supervisor when the SMART1 handset connects to the system for the first time.
This is the only time the SMART Manager Setup is run.
Once the supervisor is downloaded and installed then the Supervisor handles all communication with the SMART Manager.

4.2 Supervisor

The Supervisor is the main controller for all SMART1 features.
It connects to the SMART Manager and identifies the handset using the local number (extension).

From the SMART Manager receives the Site data, profile configuration and licenses.
The configuration data received from the SMART Manager is stored in a local database and can be accessed by other apps through an API.

It downloads and installs the apps in the profile configuration and if configured it removes all unwanted apps.
It starts up the Messaging service and the Fox Messenger app.

During runtime it performs a number of tasks, for example:

Transfers handset debug logs to the SMART Manager.
Downloads the Firmware updates.
Monitors the battery level
Monitors the charging state

It also handles the SMART1 hardware, for example:

Alarm Key
Side Key
RFID positioning
BLE positioning
NFC Positioning (also requires the NFC Reader app)
Enable/disable the camera
Top display
LED

4.3 Messaging Service

The messaging service handles all communication with the CMS (COBS Messaging Server).
The communication is primarily over DECT but as an alternative it can also communicate over WiFi.

The messages sent from the CMS is received and acknowledged by the messaging service. Then the messaging service forwards the messages to all apps that have registered as listeners as for example the Fox Messenger.

Any app that needs to send a message to the CMS (for example the Supervisor when the alarm key is activated) will send the message to the Messaging service that forwards the message to the CMS.

4.4 Fox Messenger

The Fox Messenger is the user interface for messages received from the CMS.
It flashes the incoming messages and enables call back and user response to a message.
It organises the received messages depending on priority and reception time.
The messages are displayed with the message text, a user defined icon and colour in the main screen and a smaller icon and message text in the top display.
When a message is received the user is alerted with a user defined alert tone and/or vibration.

See document “T100366 User Guide FOX Messenger” for more information.

4.5 User Login

The User login app provides a possibility to tag messages from the handset with a user name of the user that is currently logged on to the handset. The login also controls the licenses and/or profiles downloaded by the supervisor.

The User Login app is started when the handset is taken out of the charger and the user is requested to enter a username and password (these can also be provided using an NFC tag).
The user name and password is sent to the SMART Manager and authenticated.
After a successful authentication the supervisor will update the license and profile data and all messages sent from the handset will be tagged with the user name.

The user will be logged out when the handset is placed in the charger or another user logs in.

4.6 NFC Reader

The NFC Reader app enables location features with an NFC Tag.
A NFC location tag is written using the SMART Admin app. When creating the NCF tag an id (text) is written to the tag.
When the SMART1 reads these NFC tags by holding the handset next to this tag the id is sent to the CMS.

The received NFC data is sent from the NFC Reader to the supervisor that forwards the event to the CMS via the Messaging Service.

4.7 SMART Admin

The SMART Admin app is an administration app for the SMART system.

Status Information
Status information of the handset SIP and DECT registration.

DECT Survey
Utility for deployment and troubleshooting of the DECT system.

RFID Survey
Utility for deployment and troubleshooting of RFID location beacons.

BLE Survey
Utility for deployment and troubleshooting of BLE location beacons.

SMART Man Setup NFC Tag
Reading and writing NFC Tags used with the SMART Manager Setup app.

User Login NFC Tag
Reading and writing NFC Tags used with the User Login app.

SMART Man Setup NFC Tag
Reading and writing NFC Tags used for location.

See document “T100365 User Guide SMART Admin” for more information on the SMART Admin app.

5 Site Name and Serial ID

The SMART Manager Site Name and Serial ID are essential to understand when configuring a SMART Manager.

When starting a new clean SMART Manager it does not have a Site Name or Serial ID.

The SMART Manager will run on the preinstalled “TESTLICENSE” but in order to generate real licenses we need a License Key.

The License Key is generated in the SMART Manager when a Site Name and Serial ID is save din the SMART Manager.

The Site Name is an arbitrary text that should identify the site.

NOTE!
Set a Site Name that identifies the site as this cannot be changed later on and it is this name that will identify the site when ordering new licenses, when in contact with COBS support etc.

Site Serial ID is a unique serial ID for this SMART Manager, the Serial ID must be requested from COBS. Send an email to order@cobs.se and supply the Site Name you have chosen and your customer to request a Serial ID.

Never define a serial ID of our own or reuse an old serial ID as you will not be able to order licenses or get support if the Serial ID is incorrect.

When the Site Name and Serial ID is saved in the SMART Manger it will generate a License Key. This is shown in the web interface.

When the License Key has been generated the Site Name and Serial ID cannot be changed in the SMART Manager except when clearing the Data Base.

When ordering license the Site Name and License Key must be supplied.

6 Getting Started

6.1 Setting up the SMART Manager

6.1.1 Accessing the SMART Manager

The default settings of the network interfaces are:

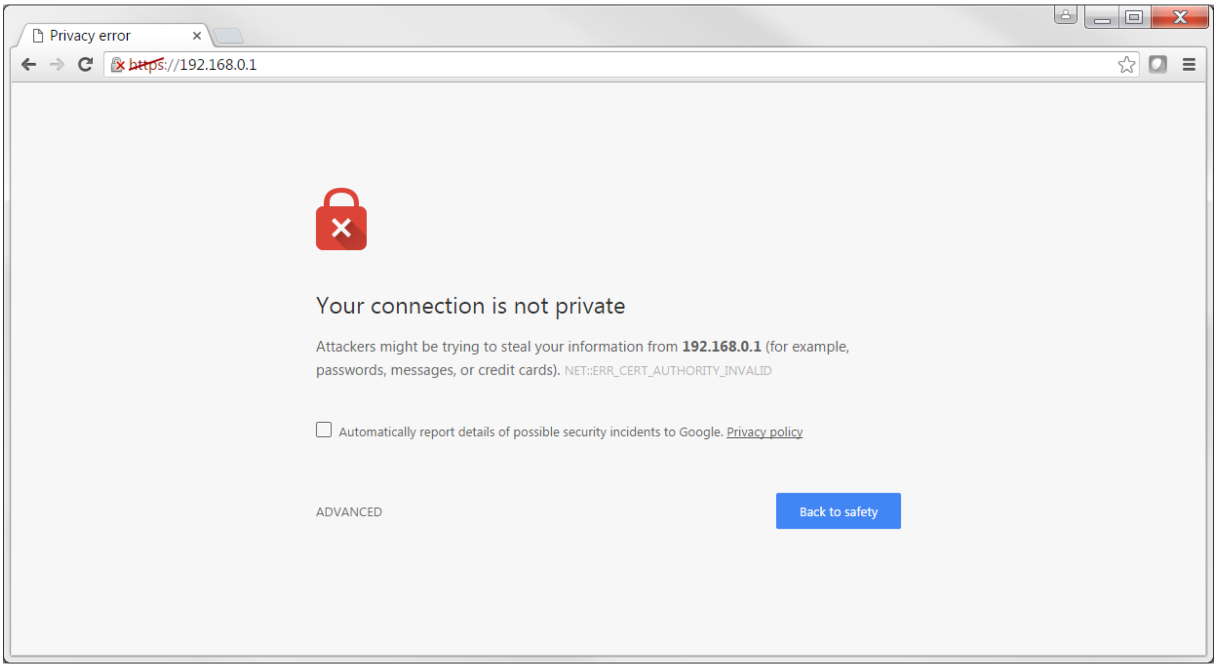
LAN1

IP:	192.168.0.1
Mask:	255.255.255.0
Gateway:	None

LAN2

IP:	192.168.1.1
Mask:	255.255.255.0
Gateway:	None

Use a web browser (Chrome or Firefox) to access the SMART Manger on either LAN1 or LAN2.
As the SMART Manager uses https you will probably get a warning in the browser accept this and proceed



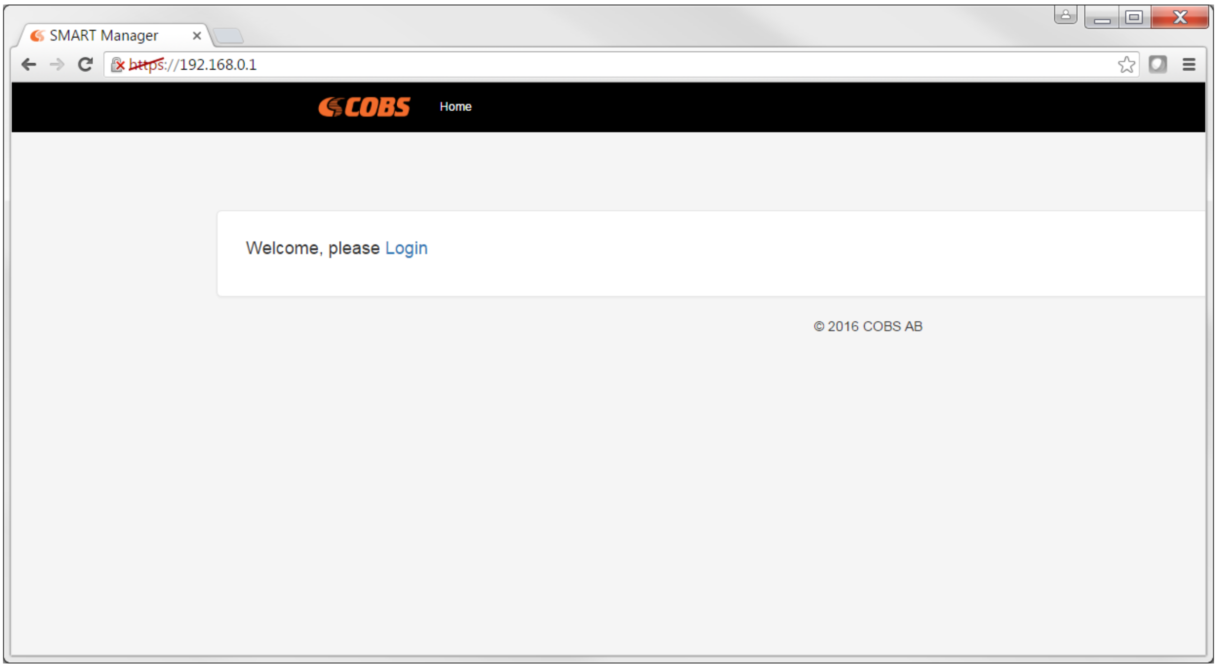
Your connection is not private

Attackers might be trying to steal your information from **192.168.0.1** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically report details of possible security incidents to Google. Privacy policy

In Chrome click on advanced and then proceed.

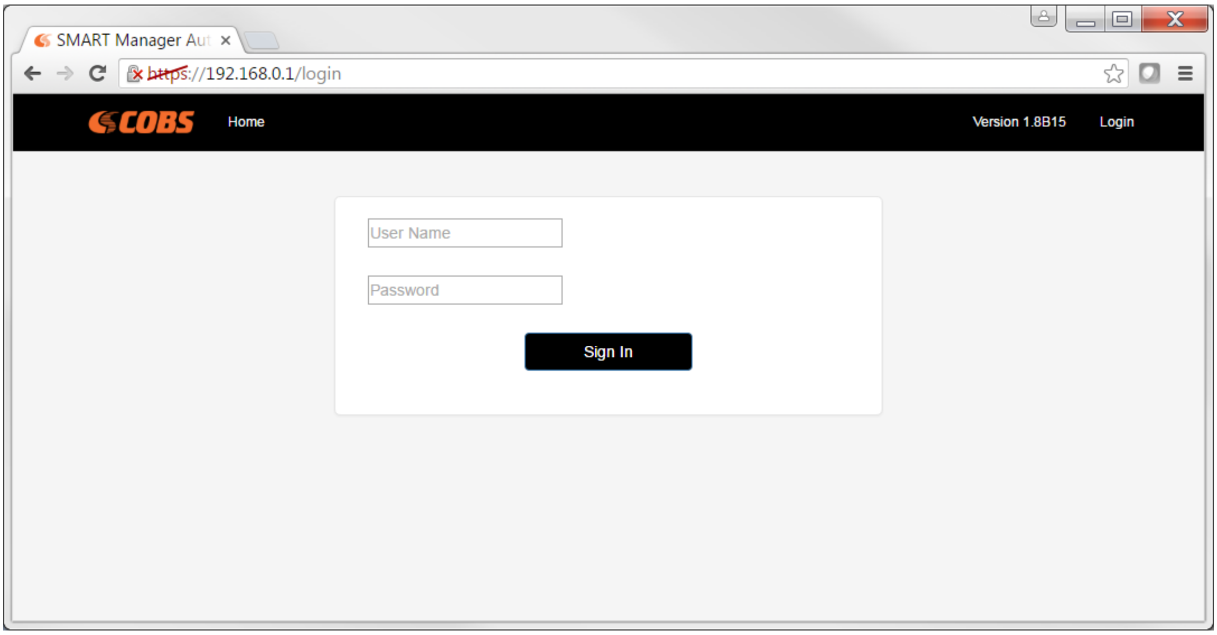
You should now see:



Welcome, please Login

© 2016 COBS AB

Click on Login to proceed to the login page:



User Name

Password

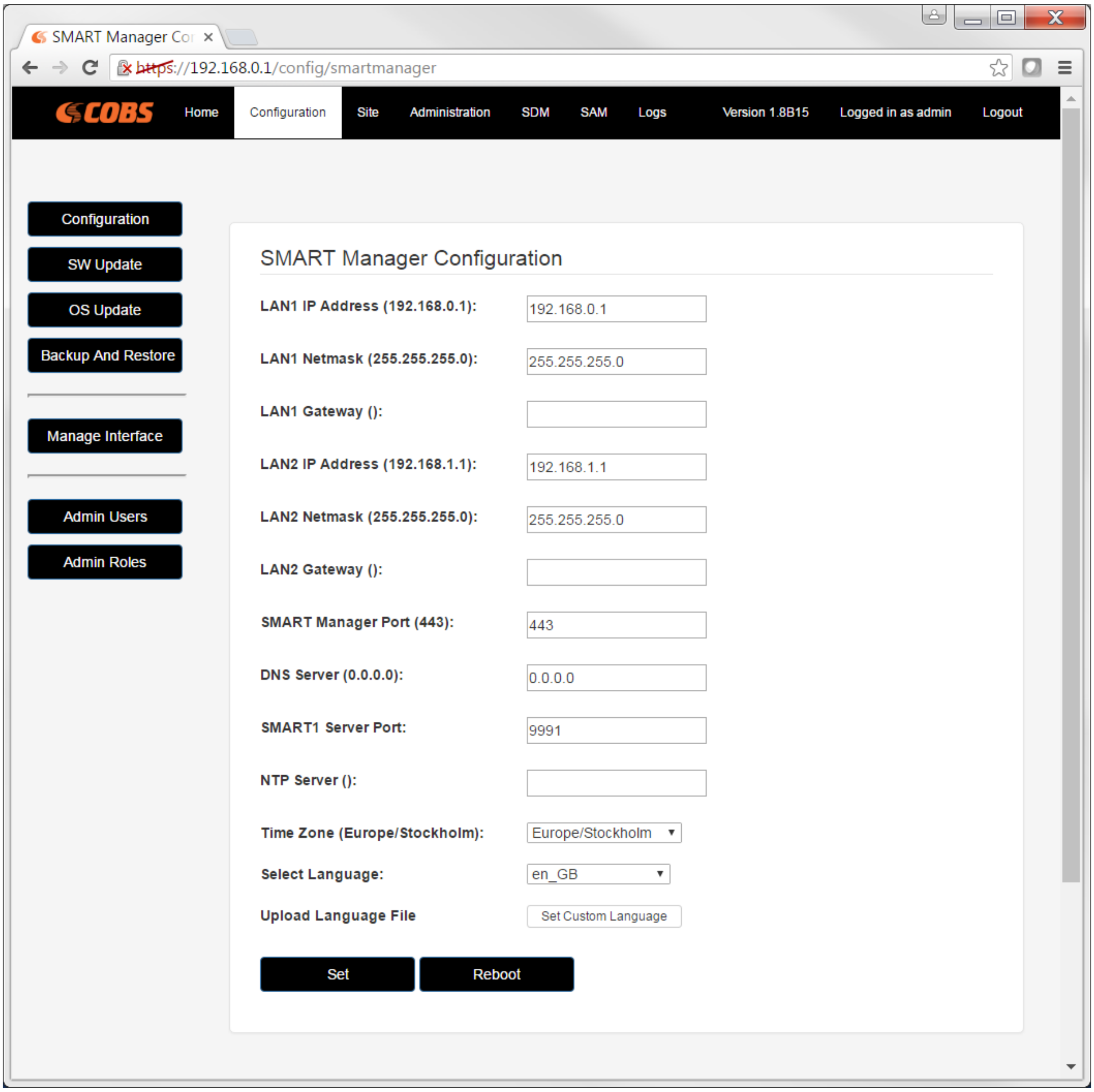
Sign In

Enter the default username “admin” and the default password “admin”.

The SMART Manager is always delivered with a TEST LICENSE which will let you run the SMART Manager for 99 hours, after that a restart is needed.
The TEST LICENSE will give you full access to all features without any limitations.

6.1.2 Configuring the SMART Manager

Click on “Configuration”:



SMART Manager Configuration

LAN1 IP Address (192.168.0.1):	192.168.0.1
LAN1 Netmask (255.255.255.0):	255.255.255.0
LAN1 Gateway ():	
LAN2 IP Address (192.168.1.1):	192.168.1.1
LAN2 Netmask (255.255.255.0):	255.255.255.0
LAN2 Gateway ():	
SMART Manager Port (443):	443
DNS Server (0.0.0.0):	0.0.0.0
SMART1 Server Port:	9991
NTP Server ():	
Time Zone (Europe/Stockholm):	Europe/Stockholm
Select Language:	en_GB
Upload Language File	Set Custom Language

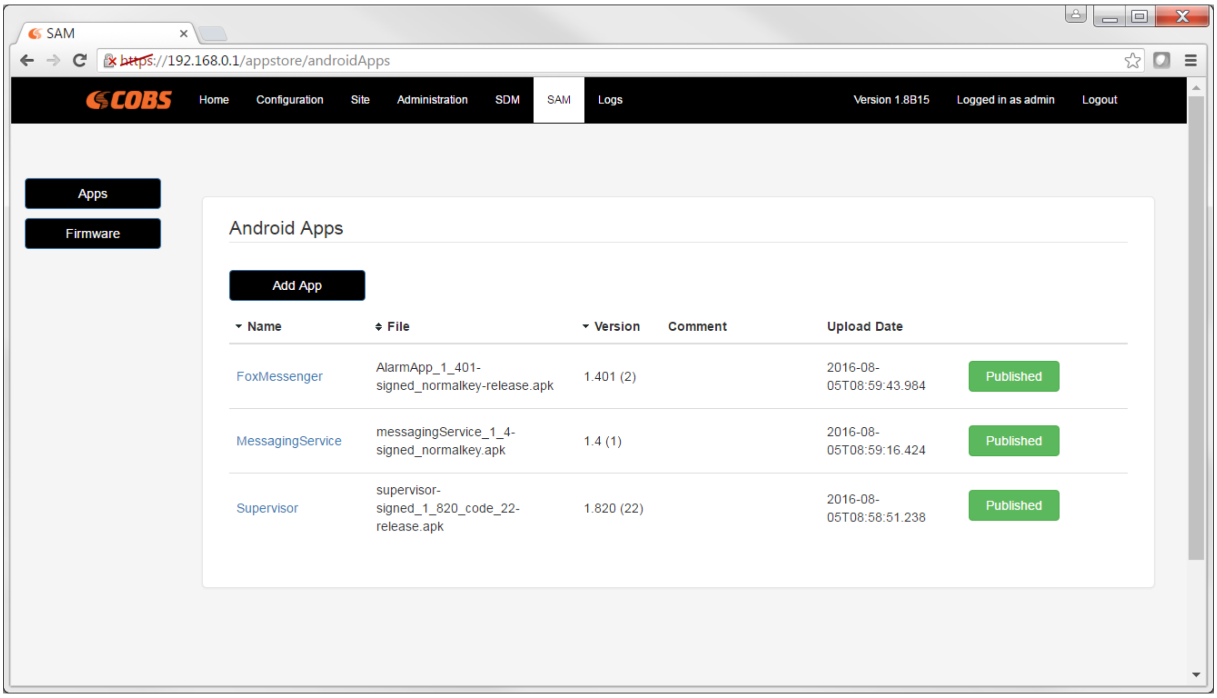
Enter the network settings for LAN1 and LAN2 as required on your network.
NOTE
There must only be one Gateway configured, either for LAN1 or LAN2.

Enter an NTP server, best practise is to set up the CMS as NTP server and then point the SMART Manager and the SMART AP to use the CMS as NTP server. Then the CMS can synchronise to an external NTP server. This way all units in the SMART System will always use the same time even if then external NTP server cannot be reached.

Press “Set” and then ”Reboot”.

After the reboot access the SMART Manager on the new IP address.
Login with “admin”/”admin”.

Click on “SAM”.
Make sure that there is a Supervisor app in the SAM and that it is published.



Android Apps

Name	File	Version	Comment	Upload Date	
FoxMessenger	AlarmApp_1_401-signed_normalkey-release.apk	1.401 (2)		2016-08-05T08:59:43.984	Published
MessagingService	messagingService_1_4-signed_normalkey.apk	1.4 (1)		2016-08-05T08:59:16.424	Published
Supervisor	supervisor-signed_1_820_code_22-release.apk	1.820 (22)		2016-08-05T08:58:51.238	Published

If not click on “Add App” and upload the Supervisor app APK file (can be downloaded from www.cobs.se). After the app is uploaded publish it by clicking on the “Unpublished” button.

6.2 Registering new handsets

Always make sure you have the Supervisor app in the SAM (SMART Application Manager) in the SMART Manager and that it is published.
Make sure there are enough free user licenses and an SSA (or a TEST LICENSE) to register a new handset.

6.2.1 Using COBS SMART AP

STEP 1:
Register the SMART1 handset to the DECT system.

STEP 2:
Connect the SMART1 to the WiFi network

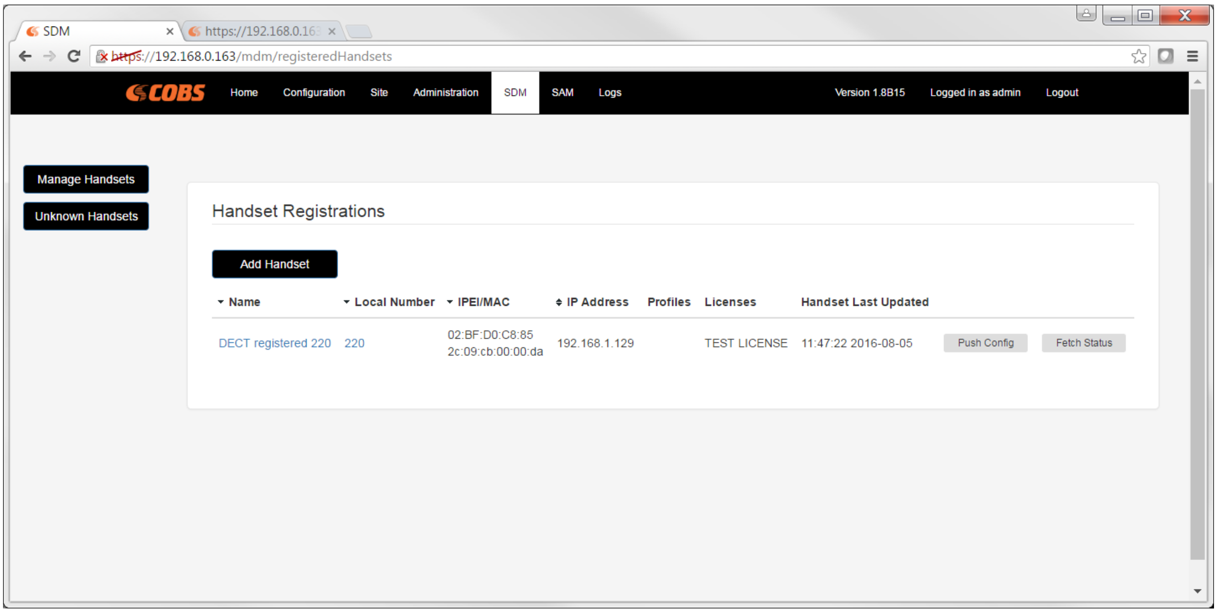
STEP 3:
Start the SMART Manager Setup app in the SMART1.
Enter the address to the SMART Manager and press “Connect”.

The SMART Manager will download, install and start the Supervisor from the SMART Manager

When started the Supervisor will register the handset in the SMART Manager using the localno (extension number) assigned from the DECT system.

Pull down the notification bar in the handset and you should see the Supervisor notification indicating that the phone is registered with the local number from the DECT.

STEP 4:
In the SDM (SMART Device Manager), the handset should now be registered with its local number and can now be associated with profiles and assigned licenses.



Handset Registrations

Name	Local Number	IPEI/MAC	IP Address	Profiles	Licenses	Handset Last Updated		
DECT registered 220	220	02:BF:D0:C8:85 2c:09:cb:00:00:da	192.168.1.129		TEST LICENSE	11:47:22 2016-08-05	Push Config	Fetch Status

6.2.2 Without DECT

STEP 1:
Connect the SMART1 to the WiFi network

STEP 2:
Start the SMART Manager Setup app in the SMART1.
Enter the address to the SMART Manager and press “Connect”.

The SMART Manager will download, install and start the Supervisor from the SMART Manager

When started, the Supervisor will add the handset in the SMART Manager as an unknown handset.
Check that the handset is listed in the “Unknown Handsets List”.

STEP 3:
Create a new handset registration under “Manage Handsets”. Use a unique name and a localno.
Assign the new registration to the handset selected from the

STEP 4:
In the SDM (SMART Device Manager), the handset should now be registered with its local number and can now be associated with profiles and assigned licenses.

6.3 Adding a profile

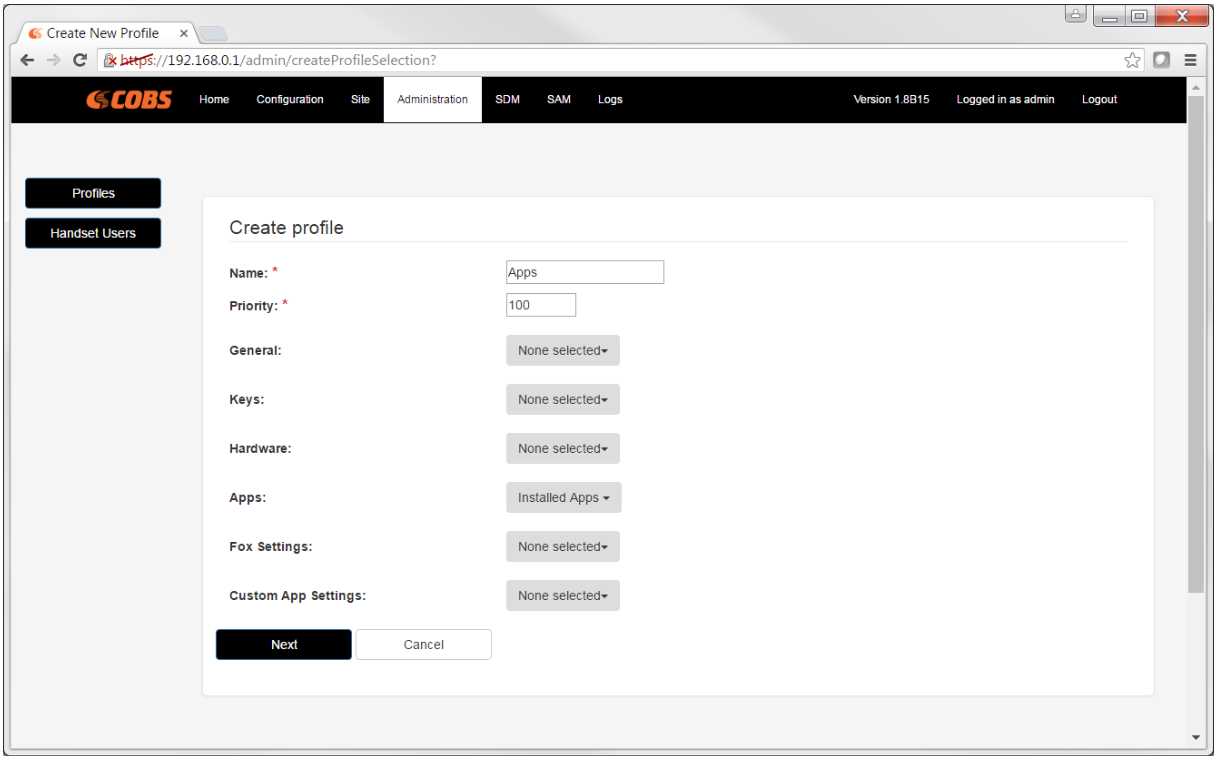
All settings and apps in the handsets are loaded into the handset using profiles.

In this example we add a profile to install some apps.
In the SAM, add the Messaging service and FOX apps and publish them (in the same way as the Supervisor was added above).

In the SMART Manager click on “Administration” and then click on “Add New Profile”.

Give the profile a name, for example “Apps” and add a priority between 1 and 1000 (1 is the highest priority).

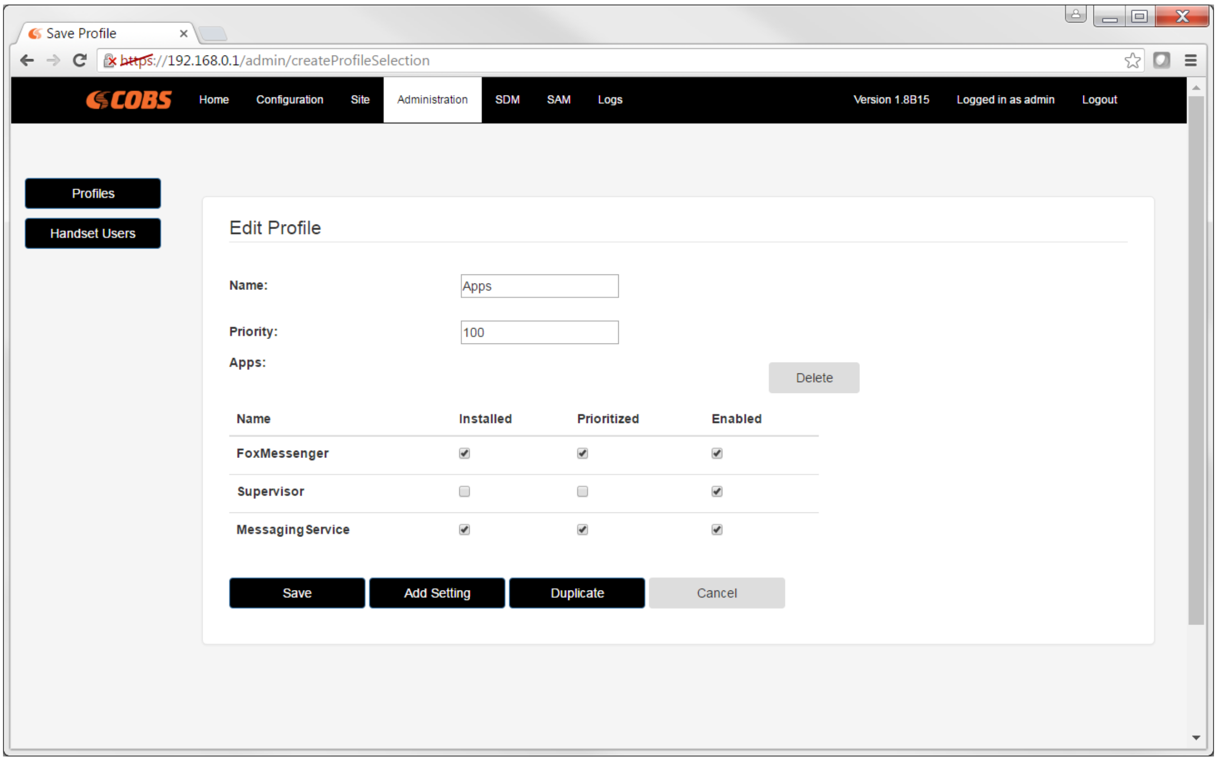
Then click on button next to “Apps” and select “Installed Apps”.



Create profile

Name: *	Apps
Priority: *	100
General:	None selected
Keys:	None selected
Hardware:	None selected
Apps:	Installed Apps
Fox Settings:	None selected
Custom App Settings:	None selected

Click on “Next” to proceed.



Edit Profile

Name: Apps

Priority: 100

Apps:

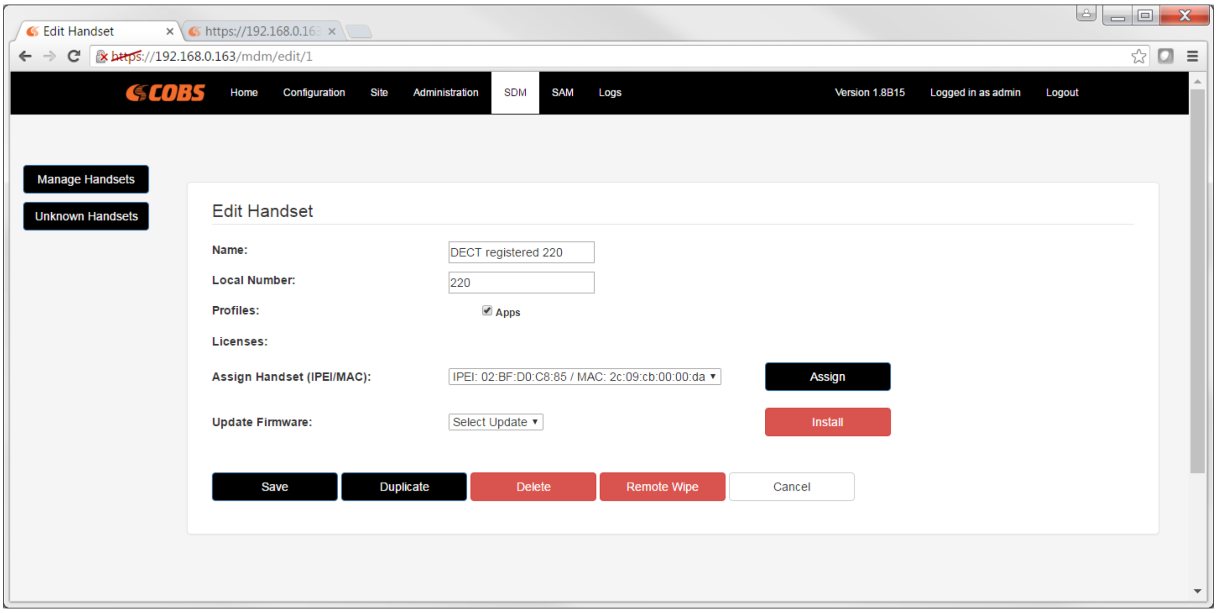
Name	Installed	Prioritized	Enabled
FoxMessenger	☑	☑	☑
Supervisor	□	□	☑
MessagingService	☑	☑	☑

Check “Installed”, “Prioritized” and “Enabled for the “Messaging Service” and the Fox Messenger” apps.

(The supervisor is installed automatically and does not need to be specified in a profile unless you have different versions of the supervisor app.)

Click on “Save”.

Click on MDM and then click a handset registration.



Edit Handset

Name: DECT registered 220

Local Number: 220

Profiles: ☑ Apps

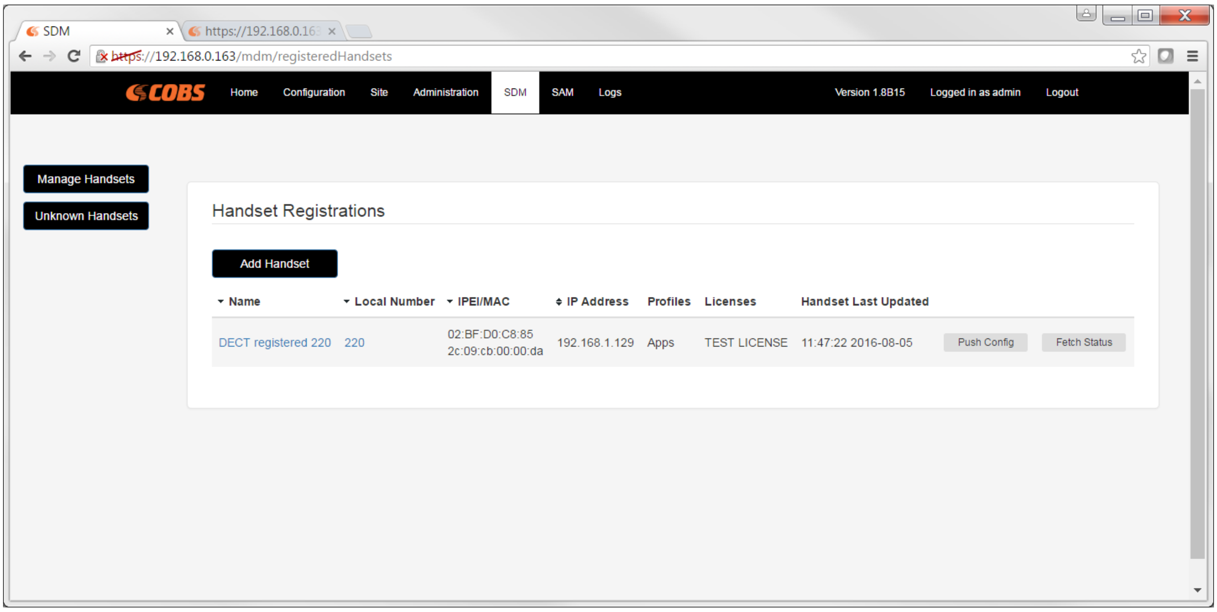
Licenses:

Assign Handset (IPEI/MAC): IPEI: 02:BF:D0:C8:85 / MAC: 2c:09:cb:00:00:da

Update Firmware: Select Update

Check the profile “Apps” that was created above and press “Save”.

Now press “Push Config” for the handset and the apps shall be installed.



Handset Registrations

Name	Local Number	IPEI/MAC	IP Address	Profiles	Licenses	Handset Last Updated		
DECT registered 220	220	02:BF:D0:C8:85 2c:09:cb:00:00:da	192.168.1.129	Apps	TEST LICENSE	11:47:22 2016-08-05	Push Config	Fetch Status

7 Handset Registration

A handset is identified in the COBS SMART system by its local number (extension number).

The CMS uses the local number for alarm and messaging, it
The DECT/PBX uses the local number for voice calls.
The SMART Manager uses the local number for licensing and provisioning.

Therefore the local number / extension number must be unique in the SMART System.
There must not be 2 handset using the same local number / extension number.

If the handset is registered to the COBS SMART AP it is assigned a local number in the DECT.

When the handset communicates with the SMART Manager it will always use this local number.
This means that if you change the local number (extension number) for a handset in the DECT system it will use another registration in the SMART Manager.

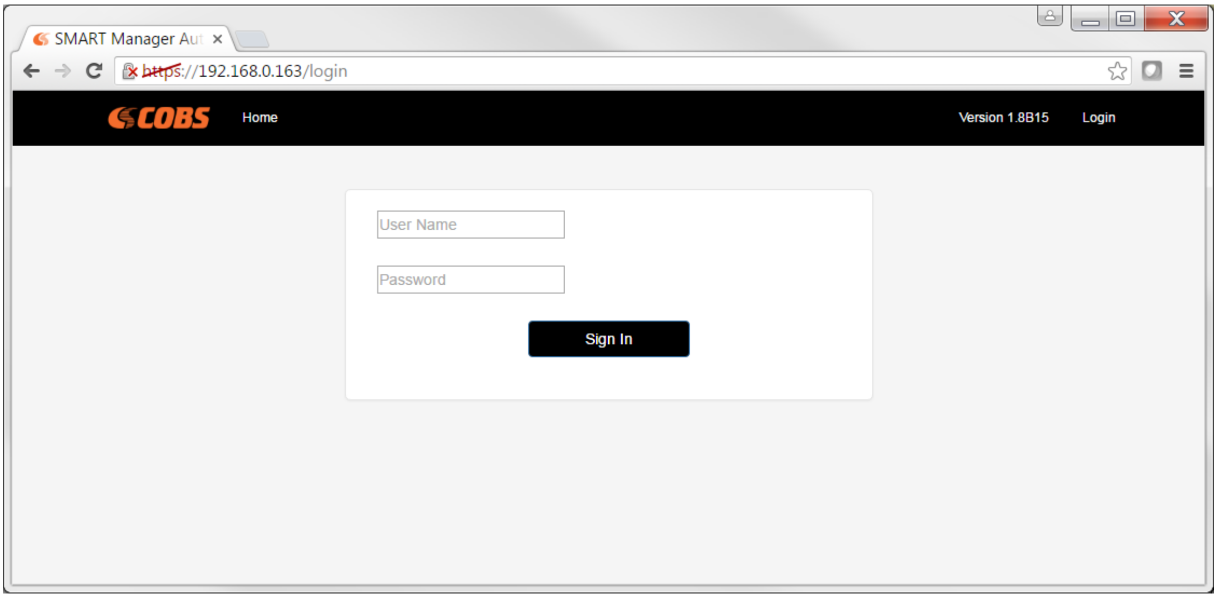
Therefore always register the handset in the COBS AP DECT before connection it to the SMART Manager.

Then the SMART Manager will assign the handset to the registration with the local number.
If there is no registration with that local no then the SMART Manager will automatically create a registration.

If the handset has not been registered to a COBS AP DECT then it has no local number so when it connects to the SMART Manager it will be shown as an “Unknown Handset”.
Then you must create a handset registration with a local number in the SMART Manager and then assign the handset to the registration.

8 Reference Manual

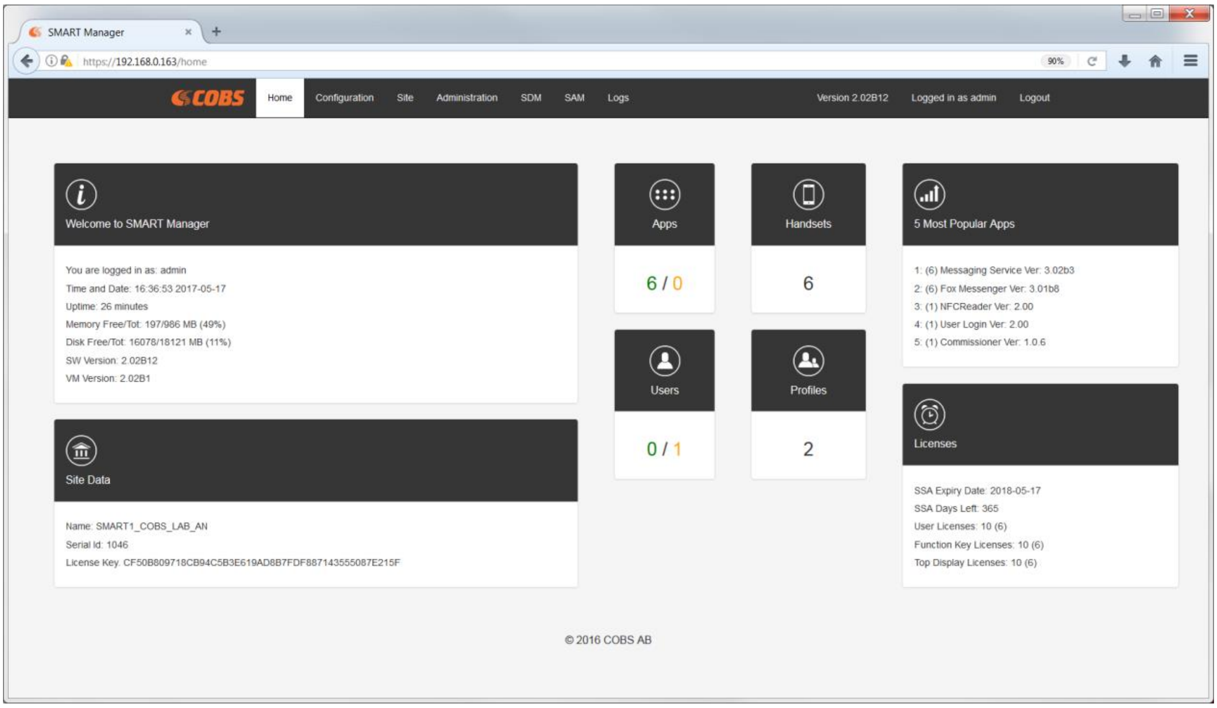
8.1 Login



To get access to the web interface you must login with an administration user.
The default user is “admin” with password “admin”.

8.2 Home

The Home tab displays some basic status information about the SMART Manager.



Welcome to SMART Manager

You are logged in as: admin
Time and Date: 16:36:53 2017-05-17
Uptime: 26 minutes
Memory Free/Tot: 197/986 MB (49%)
Disk Free/Tot: 16078/18121 MB (11%)
SW Version: 2.02B12
VM Version: 2.02B1

Site Data

Name: SMART1_COBS_LAB_AN
Serial Id: 1046
License Key: CF50B809718CB94C5B3E619AD8B7FDF887143555087E215F

Apps: 6 / 0

Handsets: 6

Users: 0 / 1

Profiles: 2

5 Most Popular Apps

1: (6) Messaging Service Ver: 3.02b3
2: (6) Fox Messenger Ver: 3.01b8
3: (1) NFCReader Ver: 2.00
4: (1) User Login Ver: 2.00
5: (1) Commissioner Ver: 1.0.6

Licenses

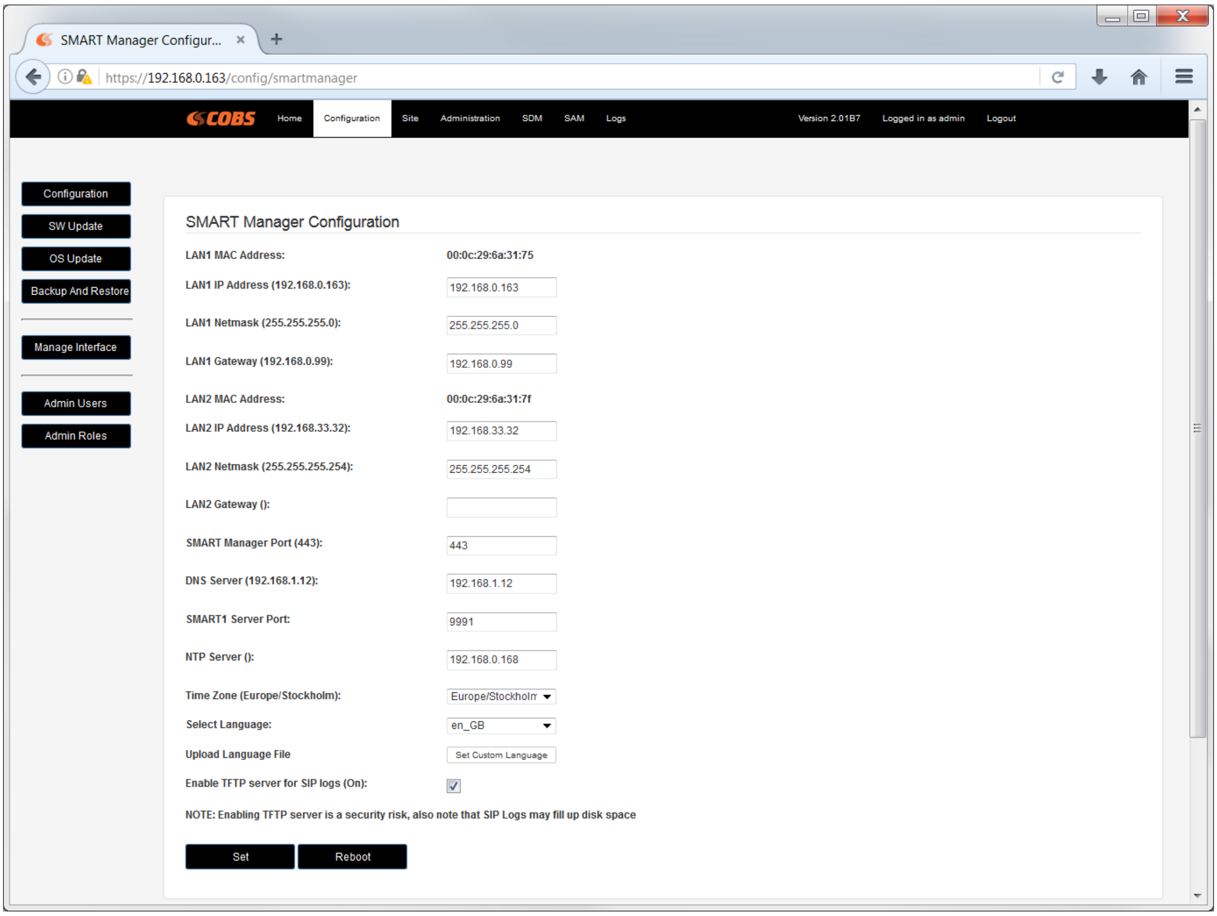
SSA Expiry Date: 2018-05-17
SSA Days Left: 365
User Licenses: 10 (6)
Function Key Licenses: 10 (6)
Top Display Licenses: 10 (6)

© 2016 COBS AB

8.3 Configuration

The Configuration tab holds configuration parameters for the SMART Manager server and the user interface.

8.3.1 Configuration



SMART Manager Configuration

LAN1 MAC Address:	00:0c:29:6a:31:75
LAN1 IP Address (192.168.0.163):	192.168.0.163
LAN1 Netmask (255.255.255.0):	255.255.255.0
LAN1 Gateway (192.168.0.99):	192.168.0.99
LAN2 MAC Address:	00:0c:29:6a:31:7f
LAN2 IP Address (192.168.33.32):	192.168.33.32
LAN2 Netmask (255.255.255.254):	255.255.255.254
LAN2 Gateway ():	
SMART Manager Port (443):	443
DNS Server (192.168.1.12):	192.168.1.12
SMART1 Server Port:	9991
NTP Server ():	192.168.0.168
Time Zone (Europe/Stockholm):	Europe/Stockholm
Select Language:	en_GB
Upload Language File	Set Custom Language
Enable TFTP server for SIP logs (On):	☑

NOTE: Enabling TFTP server is a security risk, also note that SIP Logs may fill up disk space

The value within parenthesis after the label indicates the value currently in use by the SMART Manager whereas the value in the input box is the value set in the configuration database.

To apply the values in the configuration database press “Set” and then reboot the SMART Manager.

The SMART Manager is designed to use 2 network interfaces designated LAN1 and LAN2.
In the setup of the virtual machine these can be routed to 2 physical network interfaces or to the same physical network interface.

LANX MAC Address
The MAC Address of the network interface.

LANX IP Address
The IP Address of the network interface.

LANX Netmask
The netmask of the network interface.
Note that the 2 network interfaces must be configured to 2 different subnets.

LANX Gateway
The default router/gateway.
Note that there must only be one Gateway configured on either LAN1 or LAN2.

SMART Manager Port
This is the server port that the SMART Manager listens to.
The port is used by the web configuration interface as well as the SMART1 handsets.

The SMART Manager also listens for http requests on port 80 and redirects these web browser requests to https on port 443.

IMPORTANT!
If this is changed from the default 443 port then all handsets must be reconfigured (using the SMART Manager Setup app) to access the SMART Manager on the new port

DNS Server
Server for resolving DNS names.

SMART1 Server Port
This is the port that the SMART1 handsets listens to.

IMPORTANT!
If this is changed from the default 443 port then all handsets must be reconfigured (using the SMART Manager Setup app) so that the SMART Manager can access the SMART1 handsets on the new port

NTP Server
NTP server for synchronising the time and date of the SMART Manager.

Time Zone
Time zone for the time and date of the SMART Manager.

Select Language
Selects the web interface language for the SMART Manager.
Options are “en_GB” which is the default English and “custom_CUSTOM” which is the uploaded custom language file.

Upload Language File
Uploads the custom language file.

Enable TFTP server for SIP Logs
Check to enable a TFTP server for uploading of SIP logs from the SMART AP’s.
Enabling the TFTP server is a security risk and it should only be enabled while debugging SIP issues in the SMART AP base stations.
Besides the SIP Logs contains an extensive amount of data and will fill up the SMART Manager disk space if left active and thus will result in deletion of other logs as well when disk space is filled up.
From SMART AP version 4XX the SIP logs are uploaded to the syslog so the TFTP server in the SMART Manager is not used for this purpose anymore.

8.3.2 SW Update

Upload SW Update
Uploads a new SMART Manager SW update file to the SMART Manager.

Apply SW Update
After uploading an update file to the SMART Manager it has to be applied.
When applying an uploaded SW file the SMART Manager automatically makes a backup of the configuration database before installing the new update.

After the update has been installed the SMART Manager is rebooted.

Reboot
Manually reboot the SMART Manager.

Shut Down
This will permanently shut down the SMART Manager.

WARNING!
After shutting down the SMART Manager the virtual machine must be “power cycled” in order to start up the SMART Manager again.

Only use the “Shut Down” feature when you need to power off the virtual machine or host.
Then the SMART Manager should be shut down manually before the power off.

8.3.3 OS Update

Use this feature to upload and install operating system patches supplied by COBS.

8.3.4 Backup and Restore

Listed here are the backup files stored in the SMART Manager.
A backup file consist of the configuration database and it includes all configuration except:
Android Firmware Updates
Customised web interface logotype picture.
Custom Language file

A backup is automatically performed when updating the SMART Manager SW.

Perform a Backup
To create a new backup click on the “Perform Backup” button.

Download a Backup
To download a backup to the local PC, right click on the backup file name and select “Save Link As” in your web browser.

Upload a Backup
To upload a backup file from the local PC click on the “Upload Backup” button and select the backup file.
The uploaded file will be added to the list of backup files.

Restore a Backup
Clicking on the “Restore” button next to the backup file name will apply the backup to the SMART Manager replacing the existing configuration.
After restoring a backup file, go to the “Configuration” page and click on the “Set” Button to apply the new network interface settings before rebooting the SMART Manager.
After the reboot the SMART Manager will use the new restored configuration.

NOTE!
A backup performed with a later SMART Manager software version than the version currently used in the SMART Manager might fail if the database structure has changed between the different versions.
If this is the case then the configuration will be cleared.

A backup performed using an older version than is currently used in the SMART Manager will migrate the database configuration to the currently used version.

When a backup I performed the file name will start with the SMART Manager SW Version so check that the SMART Manager version is equal or newer that the version of the backup file.

NOTE!
Do not edit the backup files manually in a text editor!

Clearing Database
Clearing the data base will restore all configuration settings to their default values but the network interfaces will remain to operate with the current settings (IP address etc.) until “Set” is pressed in the “Configuration” page and the SMART Manager rebooted.

8.3.5 Manage Interface

Under this page the web interface can be customised.

Header Logotype
The logotype can be replaced by a custom picture file (size 130px*60px).

Background Colour

This is the main work area background colour.

Button Colour
This is the colour of the left side command buttons.

Header Colours
This is the background and text colours of the top menu bar.

Reset Interface to Default
This will restore the interface settings to the default values.

8.3.6 Admin Users

The “Admin Users” are user logins for the web interface.
A user is added with a user name, a password and one or more roles.
The entered password cannot be viewed after entering it so if a user forgets his password a new password must be entered.

There must always be one User with the ADMIN role. It is possible to change the user name and password for this user but it cannot be deleted.

As default there will be one user with the name “admin”, password “admin” and with the ADMIN role.

8.3.7 Admin Roles

An admin role defines an access level. There can be many different roles with access to different pages in the web interface.

There must always be on role called ADMIN which has access to everything, this role cannot be edited or deleted.

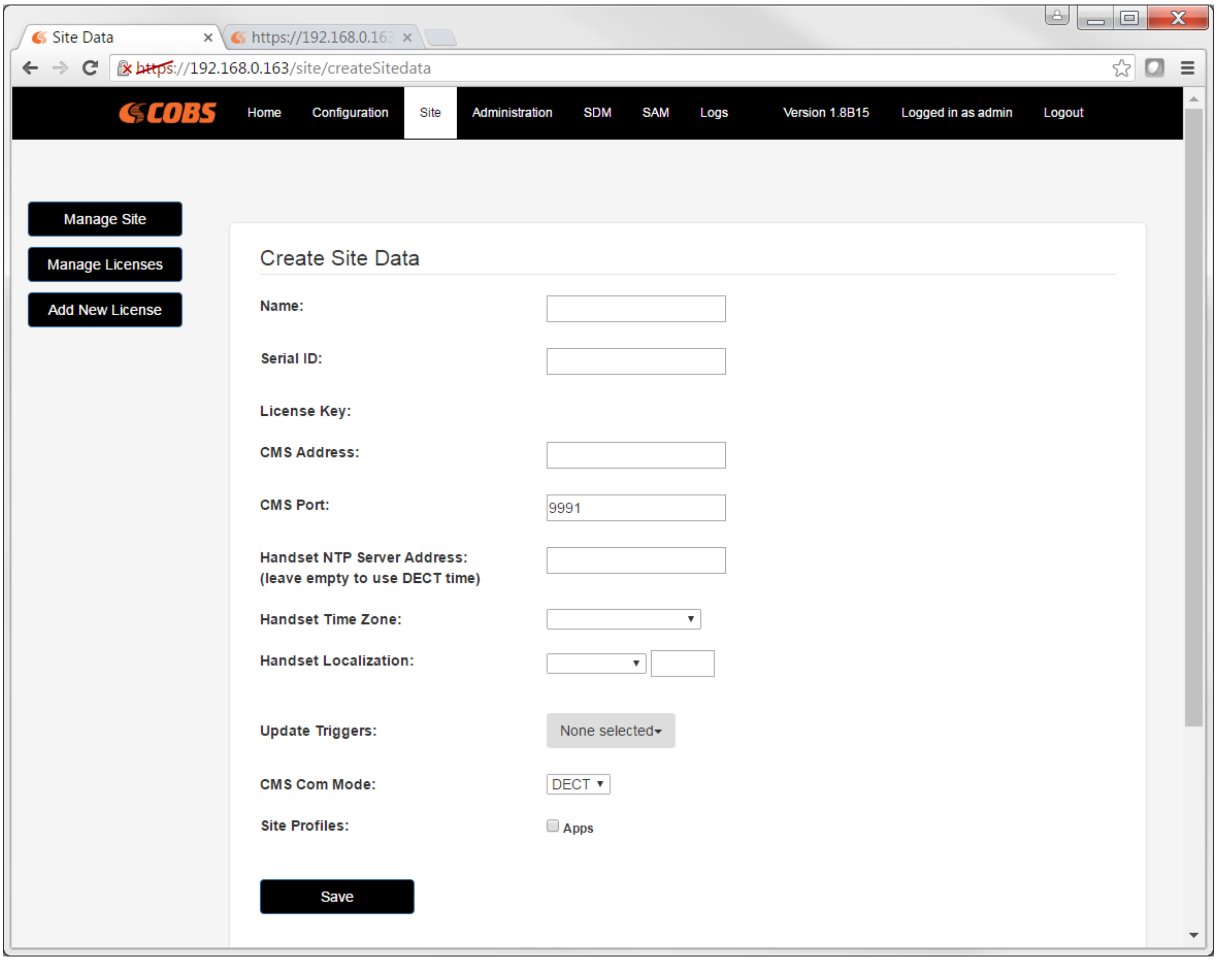
Each roles is assigned with full permission or read only permission for each web page in the SMART Manager GUI.
For read only permissions then the User cannot perform any changes to the configuration.

The permissions are divided into a number of main categories, these are the top menu items. If a user does not have permission for a main category, the menu item will not be displayed and the user can thus not access any sub-pages for this category.
Example:
If a user should have access to the “Manage Handset” page then it must also have access to the “SDM” category.

8.4 Site

The Site tab holds configuration parameters for the SMART Manager site and licenses.

8.4.1 Manage Site



Create Site Data

Name:

Serial ID:

License Key:

CMS Address:

CMS Port: 9991

Handset NTP Server Address:
(leave empty to use DECT time)

Handset Time Zone:

Handset Localization:

Update Triggers: None selected

CMS Com Mode: DECT

Site Profiles: □ Apps

Name
This is the name of the SMART Manager Site.
The name must be selected with care and should be unique as well as identifying the actual site.

NOTE!
The Site Name can only be entered once and cannot be changed except when clearing the database.
The Site name will identify the site within the COBS service and support system and must be supplied in all support tickets and also when ordering licenses.

Serial ID
This is a unique serial id that must be acquired from COBS.

License Key
When saving the Name and Serial Id for the first time the SMART Manager will calculate a License Key that will be used when ordering licenses.

CMS Address
This the IP address to the CMS used on the site.
This parameter is only applicable when using WiFi Com Mode (using WiFi for messaging).

CMS Port
This the port number that is configured in the CMS used on the site.
This parameter is only applicable when using WiFi Com Mode (using WiFi for messaging).

Handset NTP Server Address
This is the NTP server the handset will use for time and date synchronisation.
When using the COBS SMART AP DECT then the preferred solution is to leave this parameter empty, then the handsets will synchronise the Time and date with the DECT system.

Handset Time Zone
This is the Time Zone used in the handset when using an external NTP server.

Handset Localization
This is the localization setting used in the handsets. It defines for example the language used in the SMART1.
If set to "User" it is the setting in the handset menus that will define the handset localization.

Update Triggers
These are the events in the handset that will trigger the handset to update the Licenses and profiles.
As default it is only the "Charger Out" event that will trigger a handset to update the configuration.

Apart from these triggers then a User login/logout will always trigger a handset update.

CMS Com Mode
This is the communication mode the handset will use when sending/receiving alarms and messages to/from the CMS.

The options are:

WiFi:	The communication will only use WiFi (CMS Address and Port must be configured)
DECT:	The communication will only use the SMART AP DECT system.
Both:	The communication will use DECT for the first attempt, if the fails then WiFi will be used and then the attempts will switch until the message has been delivered. The handset will try 3 times to send a message to the CMS and in the CMS the number of attempts is a configuration parameter.

Site Profiles
The profiles selected here will be added to all handsets connected to the SMART Manager.

8.4.2 Manage Licenses

Active License Summary
This lists the currently active licenses, with cumulative licenses (ex. "User", "Top Display", and "Function Key") added up.
When the Used Devices adds up to the Total Devices it will be marked in red to alert that there are no more licenses available.

All Licenses
This lists all individual licenses.

License Files
This lists the license file for all licenses including the comments from the license file.
To remove a license, delete it from the License File list.

The license files can be downloaded by clicking on the license file name.

8.4.3 Add New License

A new license can be added by uploading the license file.
Select the file and click on save.
Any duplicates of the licenses in the file and the already uploaded licenses will be ignored.

8.5 Administration

Under the Administration tab you can configure the setting Profiles, Handset Users, Contact Lists and Contact Labels.

8.5.1 Profiles

The profile are essential in the configuration of a SMART system.

A profile consists of a number of settings and a profile can be assigned to the Site, a handset registration or a user.

A profile assigned to the Site (Site->Manage Site) will be added to all handsets registered in the system.

A profile assigned to a Handset Registration (SDM->Manage Handsets) will be added to that handset.

A profile assigned to a Handset User (Administration->Handset Users) will be added to a handset when that user is logged on to the handset.

When a handset updates the profiles (Site->Manage Site->Update Triggers) the SMART Manager collects all the profiles applicable to the Site, Handset and User and merges them into one profile sent to the handset. If a setting is present in more than one of the collected profiles it is the setting from the profile with the highest priority (1=highest priority) that will be used. If a setting is not present in any of the profiles the default value will be used.

Create many profiles with valid names for different settings and try to keep the number of settings in each profile as few as possible. This will make the configuration more manageable and much easier to survey.

Create a Profile
Click on “Add New Profile”.

Enter a valid name that indicates the purpose of the profile.

Enter a priority, 1-1000 where 1 is the highest priority. The priority defines the profile setting used if the same setting is present in more than one of the merged profiles.

Select the Settings (see Profile Settings) that shall be added to the profile.

Press “Next” when all settings selected.

Enter the values for the selected settings then save the profile.

Edit a Profile
Click on the profile name in the Profiles list to edit a profile.
In the edit view a setting value can be edited or setting can be added or deleted from the profile.
A profile can also be duplicated (excluding the profile name and priority which must be unique).

8.5.2 Handset Users

The User Login app uses the Handset Users to authenticate a user and to assign user defined licenses and profiles to a handset when a user is logged on to that handset.

Add a New User
Click on “Add User” to add a new user.
Enter a unique user name and a password. The password cannot be viewed once the handset has been save so if a user forgets the password a new password must be entered.

Select the profiles and licenses that shall be assigned to this user then save the user.

Edit a User
To edit a user click on the user name in the list.

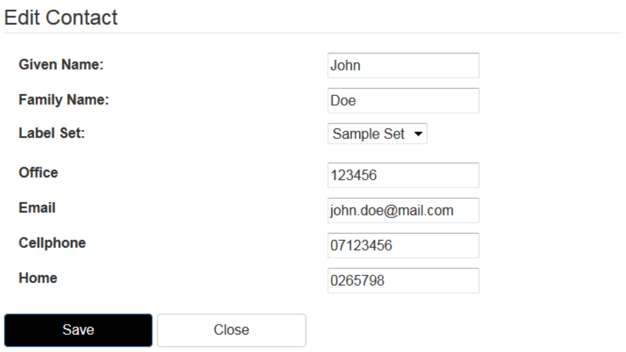
8.5.3 Contact Lists/Labels

The contact in a contact list will be added as an android contact in the SMART1 handset and can be used by any app using the android contact as for example the telephone dialler. A contact list in the SMART manager can be added in a profile and used as any other profile setting.
All contacts in the contact lists configured for the highest prioritised profile will be available as an android contact in the handset

A contact consists of a "Given Name" and a "Family Name" and a number of labels, each with a number/address.

Before creating a contact, start with defining a label set.
The labels are configured as a label set that can be reused for many contacts.

Example of a label set:
"Office"
"Email"
"Cellphone"
"Home"



Edit Contact

Given Name:	John
Family Name:	Doe
Label Set:	Sample Set
Office	123456
Email	john.doe@mail.com
Cellphone	07123456
Home	0265798

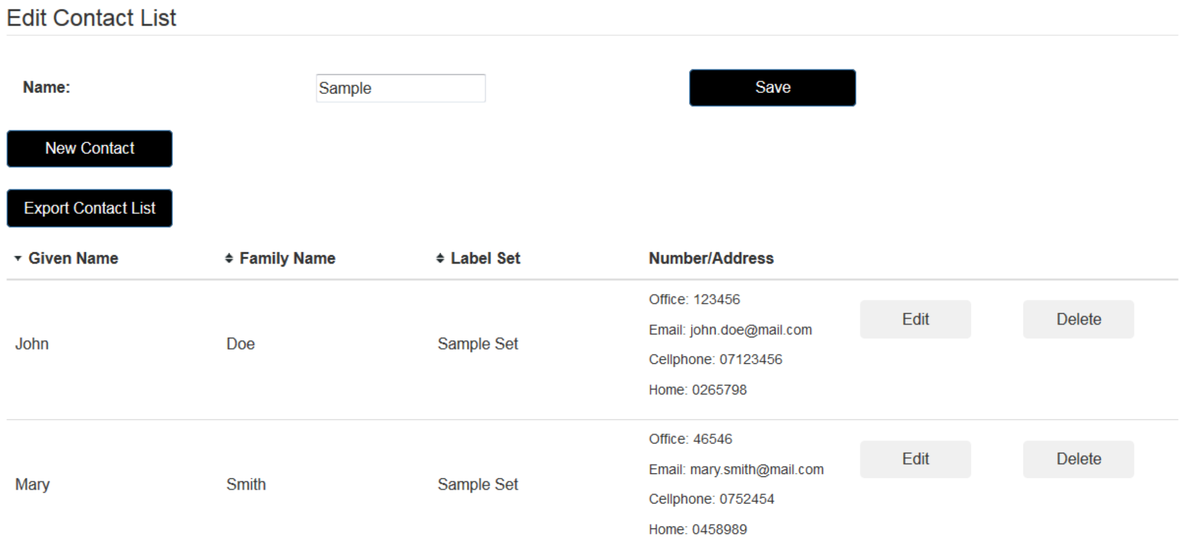
The number/address can be added as different types if addresses in the android contact.
Default are an email address in case the number/address contains an "@" character otherwise it will be added as a telephone number.

Other address types can be specified using the following prefixes:

Prefix	App	Comment
tel:	Dialler	Telephone number
mailto:	Mail client	Email address
http:	Web browser	Web address link[1]
https:	Web browser	Web address link[1]
sip:	SIP client	SIP address

[1]You must add the complete url after the prefix.
Example "http:http://www.cobs.se"

Import/Export Contact List
A contact list can be exported as a comma separated text file (csv file).
Mandatory columns are "GivenName" and "FamilyName", then the remaining columns will be the labels and their numbers.
Example:



Edit Contact List

Name: Sample

Given Name	Family Name	Label Set	Number/Address		
John	Doe	Sample Set	Office: 123456 Email: john.doe@mail.com Cellphone: 07123456 Home: 0265798	Edit	Delete
Mary	Smith	Sample Set	Office: 46546 Email: mary.smith@mail.com Cellphone: 0752454 Home: 0458989	Edit	Delete

The contact list above will be exported as:

```
"GivenName","FamilyName","Home","Cellphone","Office","Email"
"John","Doe","0265798","07123456","123456","john.doe@mail.com"
"Mary","Smith","0458989","0752454","46546","mary.smith@mail.com"
```

When importing a contact list the format is the same with the exception that you can specify the delimiter character (“,” in the example above) and if the fields are in quotations you can select the quotation character.

To import a contact list that already exists in the SMART Manager select “Replace” instead of “Import”.

8.5.4 Push To Talk

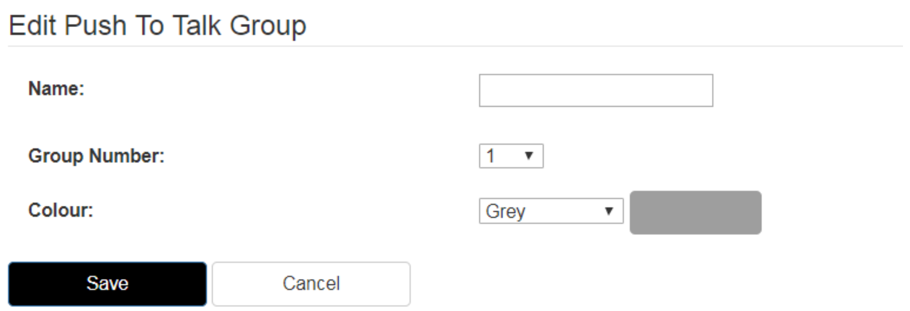
“Push To Talk” is a feature in the SMART system that allows a user to speak with a number of other users that belongs to the same “Push to Talk” group. In the receiving handsets the voice channel is opened automatically without any user action.

A SMART1 handset is configured to send and receive on a number of Push To Talk groups, the groups are configured in the SMART Manager and added as a transmit and/or receive group as a profile parameter in the handset.
The number of transmit groups is limited to 5. If a SMART1 is configured to have more than one transmit group then a double push on the yellow side key enables the user to select which group to talk to.

When “Push To Talk” is activated on one handset in the system one voice channel in the air interface is allocated on each base in the system.
So in the system there is only one “Push To Talk” channel that all groups shares.
If one handset opens a “Push To Talk” channel any other handset will get a busy signal when trying send regardless which group.

The “Push to Talk” is activated pressing the yellow side button of the handset (this button can then not be used for alarms). As long as the button is pressed the handset is sending and all other handsets configured to this group will listen.

To create a “Push to Talk” group,



Edit Push To Talk Group

Name:	
Group Number:	1 ▼
Colour:	Grey ▼

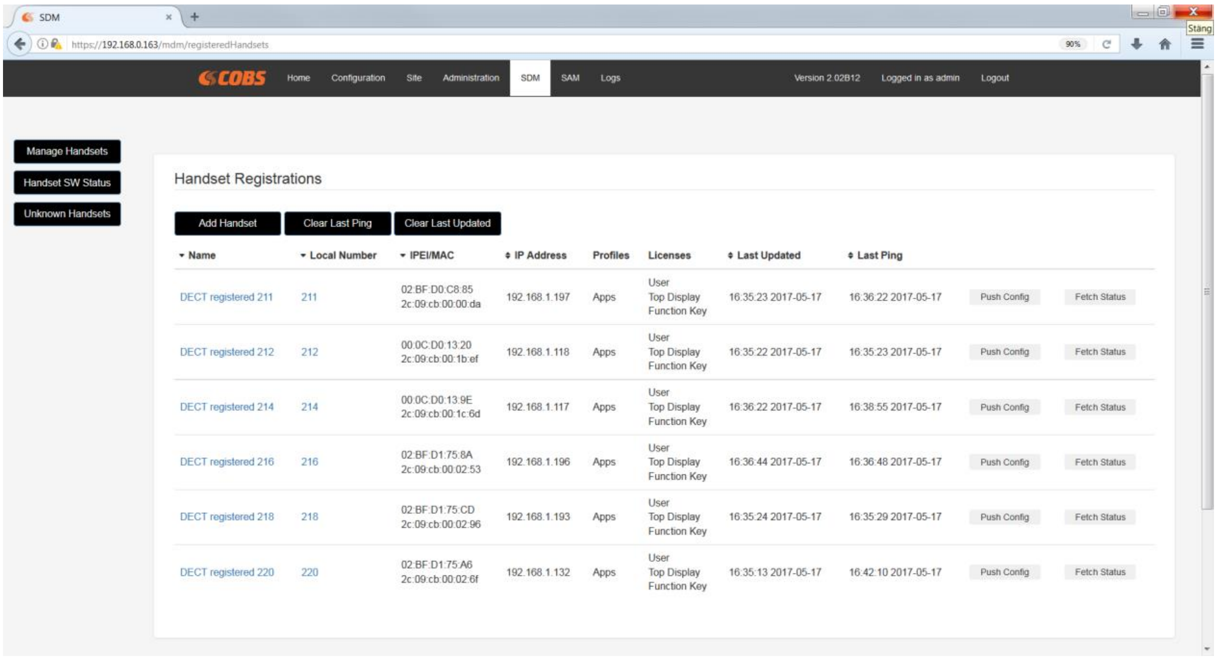
The name and colour of the group is displayed in handset when it is sending/receiving using this group. The group number is the unique identifier for the group and it can range from 1 to 254.

8.6 SDM

The SDM tab handles the handset registrations.

8.6.1 Manage Handsets

Lists all the handset registrations.



Handset Registrations

Name	Local Number	IPEI/MAC	IP Address	Profiles	Licenses	Last Updated	Last Ping		
DECT registered 211	211	02:BF:D0:C8:85 2c:09:cb:00:00:da	192.168.1.197	Apps	User Top Display Function Key	16:35:23 2017-05-17	16:36:22 2017-05-17	Push Config	Fetch Status
DECT registered 212	212	00:0C:D0:13:20 2c:09:cb:00:1b:ef	192.168.1.118	Apps	User Top Display Function Key	16:35:22 2017-05-17	16:35:23 2017-05-17	Push Config	Fetch Status
DECT registered 214	214	00:0C:D0:13:9E 2c:09:cb:00:1c:6d	192.168.1.117	Apps	User Top Display Function Key	16:36:22 2017-05-17	16:38:55 2017-05-17	Push Config	Fetch Status
DECT registered 216	216	02:BF:D1:75:8A 2c:09:cb:00:02:53	192.168.1.196	Apps	User Top Display Function Key	16:36:44 2017-05-17	16:36:48 2017-05-17	Push Config	Fetch Status
DECT registered 218	218	02:BF:D1:75:CD 2c:09:cb:00:02:96	192.168.1.193	Apps	User Top Display Function Key	16:35:24 2017-05-17	16:35:29 2017-05-17	Push Config	Fetch Status
DECT registered 220	220	02:BF:D1:75:A6 2c:09:cb:00:02:6f	192.168.1.132	Apps	User Top Display Function Key	16:35:13 2017-05-17	16:42:10 2017-05-17	Push Config	Fetch Status

Name
The “Name” is an arbitrary text describing the handset registration.
If the registration is created automatically by the SMART Manager then the name will be:
“DECT registered XXX” where XXX is the local number assigned in the DECT system.

Local Number
The local number (extension number) identifies the handset and must be unique.
It is assigned to the handset by the COBS SMART AP DECT system.
If not assigned by the DECT system a handset can manually be assigned to a registration.

IPEI/MAC
The IPEI is a unique DECT serial identifier that identifies the physical handset in DECT.
The MAC is the Ethernet MAC address of the physical handset.

IP Address
This is the IP Address of the handset.
The SMART Manager uses the IP address to communicate with the handset when pushing out configuration, new firmware, issuing a remote wipe and when fetching status information.

Profiles
Lists the profiles associated with the handset.

Licenses
Lists the licenses associated with the handset.

Last Update
The time when the handset made an update of the configuration (site data, profiles and licenses).

Last Ping
The time when the SMART Manager received a ping request from the handset. If within WiFi coverage the handset sends a ping approximately every 10 minutes.

Clicking on the time and date will display the historical ping statistics for the last 7 days. The statistics is displayed in a graph as well as a list.
The statistics can also be exported to a comma separated text file.

Push Config
Pushes the current configuration (site data, profiles and licenses) to the handset.

Fetch Status
Fetch and display the “Handset Status” information retrieved from the handset.
If the handset could not be reached then the last received status will be displayed.

Clear Last Ping
Click on this button the clear the “Last Ping” timestamp for all registered handsets.
This can be useful to check that all handsets are alive and within WiFi coverage.
Then “Clear Last Ping” and wait for at least 10 minutes and all handsets should have a new timestamp.

Clear Last Updated
Click on this button the clear the “Last Updated” timestamp for all registered handsets.
This can be useful when changing site data or a global profile.
Then “Clear Last Updated” and push the configuration to all handsets. The handsets will get a new timestamp when the update is done.

8.6.2 Add New Handset

A handset registration can manually be added to the SMART.
This can be the case when registering handsets that has not received a local number from the DECT system.

Handset registrations can also be added in advance to prepare a site configuration without having the handset available.
Then the handset registrations can be added manually. When a handset later is connected to the SMART Manager and the local number already exists it will be assigned to that registration.

8.6.3 Editing a Handset Registration

A handset registration can be edited by clicking on the handset registration name or the local number.

Name
The “Name” is an arbitrary text describing the handset registration.

Local Number
The local number (extension number) identifies the handset and must be unique.
It is assigned to the handset by the COBS SMART AP DECT system.
If not assigned by the DECT system a handset can manually be assigned to a registration.

NOTE
If the local number of a handset registration is changed then handset extension in the COBS SMART AP must also be changed.

Profile
Check all profiles that shall be associated to this handset.

License
Check all licenses that shall be applied to this handset.

Assign Handset (IPEI/MAC)
Select the physical handset from the dropdown list of unknown handsets to assign the physical handset to this registration.
Click on “Assign” to execute the new assignment.
If a handset already assigned to this registration it will be unassigned.

Update Firmware
Select a handset firmware (from all firmware uploaded in the SAM).
Click on Install to push a new firmware to the handset.

NOTE
Downloading firmware to the handset takes several minutes depending on the WiFi network and the number of ongoing firmware downloads.
Do not install firmware on more than 4-5 handsets simultaneously.
Make sure that the handset remains within good WiFi coverage during the download.

After the handset has downloaded the firmware it will automatically be installed and the handset will restart after the installation.

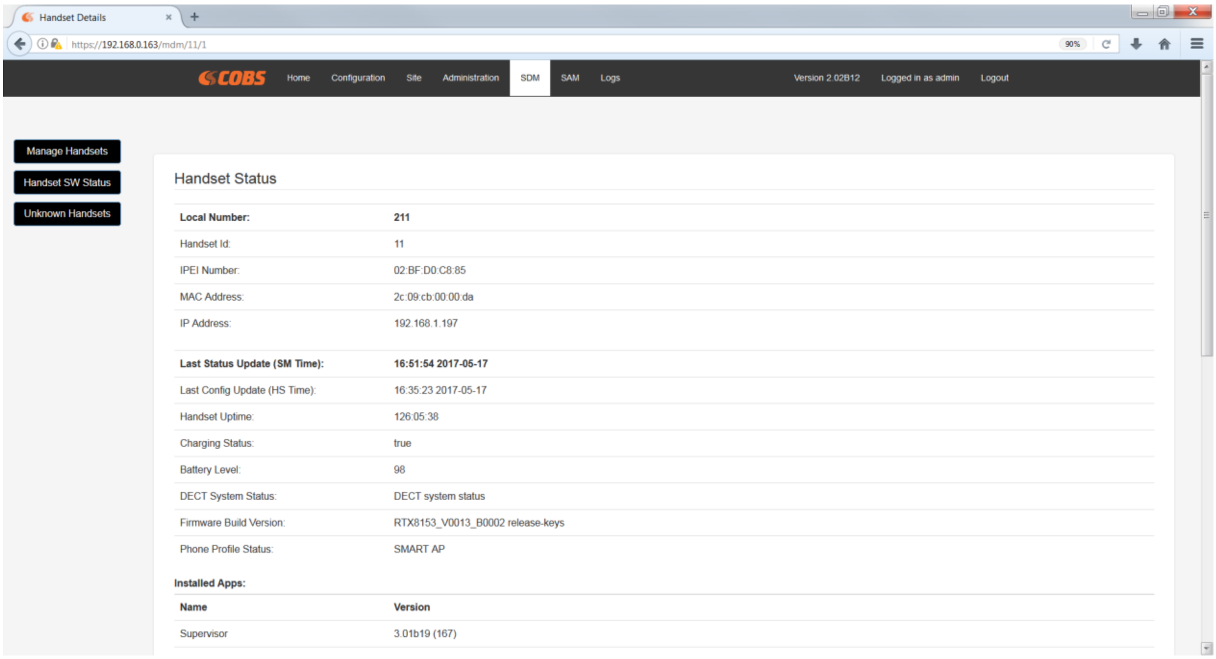
Remote Wipe
Clicking on remote wipe will erase all user data on the handset and issue a factory reset.
After a remote wipe the handset must be connected to the SMART manager manually using the SMART Manager Setup app.

8.6.4 Unknown Handsets

Lists all the unknown handset.
A handset is regarded as unknown if it has connected to the SMART Manager without a local number or if a handset has been unassigned from a registration.

8.6.5 Handset Status

This page displays the last received status information from the handset.



Handset Status

Local Number:	**211**
Handset Id:	11
IPEI Number:	02:BF:D0:C8:85
MAC Address:	2c:09:cb:00:00:da
IP Address:	192.168.1.197
Last Status Update (SM Time):	**16:51:54 2017-05-17**
Last Config Update (HS Time):	16:35:23 2017-05-17
Handset Uptime:	126:05:38
Charging Status:	true
Battery Level:	98
DECT System Status:	DECT system status
Firmware Build Version:	RTX8153_V0013_B0002 release-keys
Phone Profile Status:	SMART AP

Installed Apps:

Name	Version
Supervisor	3.01b19 (167)

Local Number
The local number (extension number) assigned to the handset.

Handset Id
This is the handset registration id in the SMART Manager database.

IPEI Number
The IPEI is a unique DECT serial identifier that identifies the physical handset in DECT.

MAC Address
The MAC is the Ethernet MAC address of the physical handset.

IP Address
This is the IP Address of the handset.

Last Status Update (SM Time)
Time and date when the status information displayed was received from the handset.
The text is marked in red if the status information is old.

NOTE:
The time stamp is in SMART Manager time.

Last Config Update (HS Time)
Time and date when the handset configuration was updated in the handset.

NOTE
The time stamp is in handset time.

Handset Uptime
The time elapsed since handset started.

Charging Status
True if handset is charging.

Battery Level
Current battery level in percent.

DECT System Status

Current status of the DECT, “In Service” or “Out of Service”.

Firmware Build Version
Version of the handset firmware version.

HW Version
The hardware version of the handset (should be 7 or higher).

Phone Profile Status
The phone profile currently used in the handset.

Rfid Pos1
Last received RFID positioning beacon.

Rfid Pos2
Second last received RFID positioning beacon.

Dect Base
RPN number of the DECT base the handset is locked to.

BLE Id 1
Last received BLE beacon.

BLE Id 2
Second last received BLE beacon.

Wifi AP MAC
The MAC address of the WiFi Access Point the handset is associated to.

Installed Apps
The apps installed in the handset

Running Apps
Apps currently running in the handset.

Forced Closed Apps
Non-prioritized apps that has been closed due to critical low battery.

PTT Receive Groups
The “Push To Talk” groups the handset is listening to.

PTT Transmit Groups
The “Push To Talk” groups the handset is sending to.

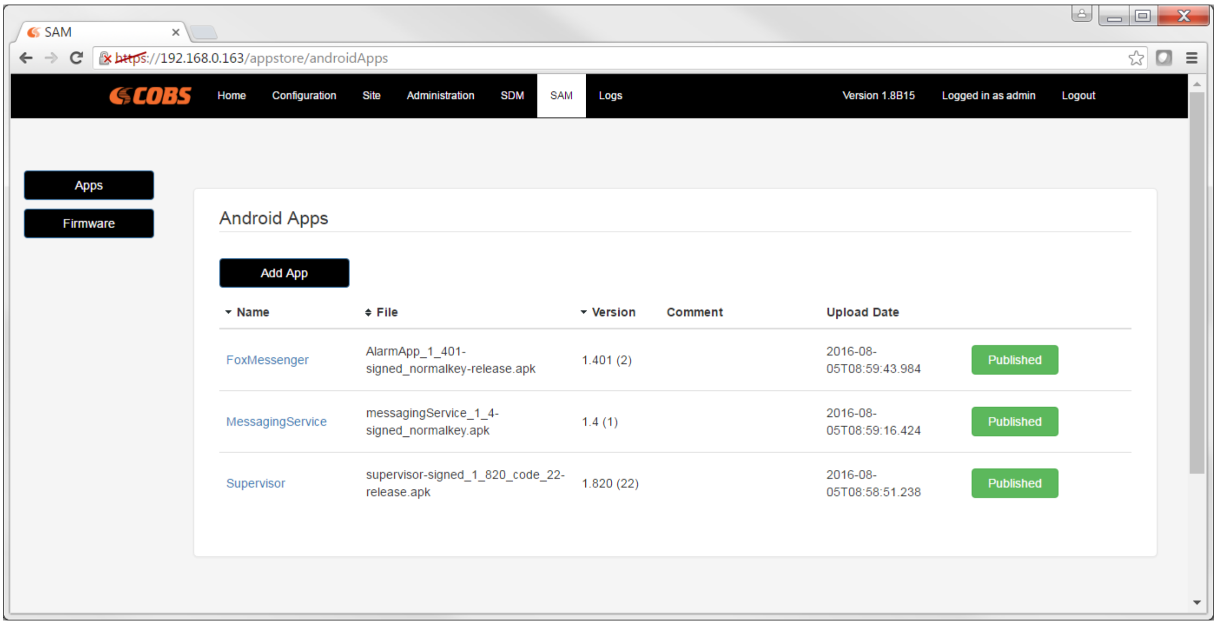
PP Status Event Mask
The PP Status Events that are masked.
That means that these events are not sent to the CMS.

8.7 SAM

The SAM (SMART App Manager) holds all apps downloaded to the handsets as well as the handset firmware updates.

8.7.1 Apps

Apps holds all apps that can be downloaded to the handsets using a profile.



Android Apps

Name	File	Version	Comment	Upload Date	
FoxMessenger	AlarmApp_1_401-signed_normalkey-release.apk	1.401 (2)		2016-08-05T08:59:43.984	Published
MessagingService	messagingService_1_4-signed_normalkey.apk	1.4 (1)		2016-08-05T08:59:16.424	Published
Supervisor	supervisor-signed_1_820_code_22-release.apk	1.820 (22)		2016-08-05T08:58:51.238	Published

The apps can have 2 status, “Published” and “Unpublished”.
Only the published apps are possible to add to a profile.
An app that is present in a profile cannot be unpublished.

NOTE
There must always be at least one published supervisor app in the SAM.
When a handset connects to the SMART Manager with the SMART Manager Setup and the handset does not have a supervisor installed it will download and install the published supervisor with the latest version.

Apps are uploaded and stored in the SAM as AKP files.

Click on “Add App” to upload a new app to the SAM.

If name is omitted it will be extracted from the APK file.
The name must be unique in the SAM.

Comment is an arbitrary text describing the app.

The app APK file can be downloaded from the SAM to the PC by clicking on the app name.

8.7.2 Firmware

Firmware holds the handset firmware update files.
The firmware can be installed in the handset from the SDM.

The firmware file can be downloaded from the SAM to the PC by clicking on the firmware name.
Make sure the handset remains within good WiFi coverage during the download.
After the firmware has been downloaded it will be installed on the handset. The handset cannot be in use during the installation.
After the installation the handset will reboot.

NOTE
Firmware files are not included in the SMART Manager Backup.

8.8 Logs

The logs are stored on the SMART Manager HDD.

At midnight todays current logs are zipped.
When the HDD reaches 80% of used space the oldest log files are deleted to make room for new log files.

Today's log file can be viewed clicking on "Current Log"/"Current Statistics", it will then be opened in a new browser window.
Or right click on "Current Log"/"Current Statistics" and select "Save As" to download it to the PC.

Click on "Clear" to delete the current log.

Click on "Archived" to view the archived zip files, then click on the filename to download it to the PC.

8.8.1 Syslog

The SMART Manger can act as a syslog server.
The SMART AP and CMS uses external syslog server for logging and these can be pointed to the SMART Manager that will save the syslog information.
The syslog server also contain syslog information from the SMART Manager itself.

The current log is stored as a text file and the archived file are named "syslog_MM_DD_YYYY.zip".

8.8.2 SMART Man. Log

This is the debug log of the SMART Manager.

The current log is stored as a text file and the archived file are named "smartmanagerlog_MM_DD_YYYY.zip".

8.8.3 Handset Log

The handset log is the android debug logcat from the handsets.
Handset debug must be activated in the handset (profile setting).

The handset will try to push the logcat every 30 min to the SMART Manager.
If the handset is out of coverage then the handset will try again after 30min.
The memory for storing the logcat information is limited so if the handset is often out of WiFi coverage then some logcat information may be lost.

The handset logs are saved separately with the handset local number as identifier.
If a handset has no local number or if it has been deleted/unassigned it will be shown under "Unknown Handsets".

When archived all handsets files are zipped in the same zip file named "handsetlog_DD_MM_YYYY.zip".

NOTE
The android logcat creates a very large amount of log data!
Only activate "Handset Debug" on a handset if there is a problem and only during trouble shooting!
Do not forget to deactivate the "Handset Debug" after troubleshooting!

8.8.4 SMART Man Stat.

The SMART Manager Statistics log is a csv file with statistics information.
The statistic information is to be used for performance monitoring of the SMART Manager.

The current statistics is stored as a csv file and the archived file are named "smartmanagerstatistics_MM_DD_YYYY.zip".

8.8.5 Handset Stat.

The handset statistics log is a csv file with statistics information.
The statistic information is to be used for performance monitoring of the SMART Manager.

The handset will try to push the statistics every 30 min to the SMART Manager.
If the handset is out of coverage then the handset will try again after 30min.

The handset statistics is saved separately with the handset local number as identifier.

If a handset has no local number or if it has been deleted/unassigned it will be shown under “Unknown Handsets”.

When archived all handsets files are zipped in the same zip file named “handsetstatistics_DD_MM_YYYY.zip”.

8.8.6 SIP Log

The SIP log are log files uploaded from the SMART AP base stations. Each log is named with the MAC address of the base and the date and time the log was uploaded. The base uploads a new SIP log file when the size of the local sip log exceeds a certain size.

The SIP logs are uploaded to the SMART Manager using TFTP and the SMART Manager TFPT Server must be enabled under “Configuration”.
In the SMART AP base station the SIP log must be activated and the Management Transfer Protocol must be set to TFTP.

When archived all base SIP log files are zipped in the same zip file named “siplog_DD_MM_YYYY.zip”.

NOTE!
The SIP logs are for debugging a certain problem on specific bases only!
Do not leave them active in a production environment as this will produce an extensive amount of log data that eventually will fill up the SMART Manager disk space resulting in deletion of other logs that might be more useful.

From SMART AP software version 4 the SIP logs are sent as syslog messages so the SIP Log in the SMART Manager is not used.

9 License Handling

9.1 Test License

The test license enables all feature without any limitations.
When a test license is added the SMART Manager will run for 99 hours. When the test license expires the SMART Manager will stop working and a reboot is required to start it again.
After the restart it will run for another 99 hours.
This can be repeated 10 times. After that the test license must be deleted and added again to regain another 99 times 10 hours.

9.2 Activation

The activation license is required to run the SMART Manager.

9.3 User

The user license is the number of handset registrations the SMART Manager can use.
Several user licenses can be accumulated to extend the number of handset registrations.

9.4 Function Key

The function key license enables the alarm key and the yellow side key on the handset.
The function key license is associated to a handset registration or a user.
Several function key licenses can be accumulated to extend the number of handset/users using the function keys.

9.5 Top Display

The top display license enables the use of the top display for messaging.
The top display license is associated to a handset registration or a user.
Several top display licenses can be accumulated to extend the number of handset/users using the top display.

9.6 Push To Talk

The “Push To Talk” license enables the use of the “push To Talk” feature in the SMART1.
The “Push To Talk” license is associated to a handset registration or a user.
Several “Push To Talk” licenses can be accumulated to extend the number of handset/users using “Push To Talk”.

9.7 SSA

The SSA is a Software Service Agreement license.
The SSA license has a number of users and an expiry date.

When adding new handset registrations the number of registrations must not exceed the user license or the users in then SSA license.

When the SSA license expires the SMART Manager will continue to operate but it will not be possible to administer the SMART Manager via the web GUI except for adding new licenses.

10 Profile Settings

10.1 General

10.1.1 Boot Animation

The boot animation is a zip file containing a series of PNG images that are displayed during the boot process. The format of the boot animation is the standard android format.
The uncompressed zip file contains a desc.txt file and folders with the PNG files.

The desc.txt define how the PNG files are displayed and the folders that contain the files.

desc.txt format:

width height frame-rate
p loops pause folder-sequence-1
p loops pause folder-sequence-2
…
p loops pause folder-sequence-#

- “width” and “height” equal the resolution of the PNG images
- “frame-rate” is the number of images played per second
- “p” indicates they are part of the animation
- “loops” is the number of times the sequence will loop (0 indicates the sequence will loop infinitely).
- “pause” the number of frames the scene will pause on the last image before continuing with the next sequence.
- “folder-sequence” is the name of the folder that holds the PNG files

Example:
480 215 25
p 1 0 part0
p 0 0 part1

Here the 480 x 215 PNG images are played at 25 fps.
The first scene is played once and no pause before playing the next scene and the PNG files are located in the folder “part0”.
The second scene loops until the boot sequences is finished and the PNG files are located in “part1”.

The PNG image files in the folders may have a common prefix but must end with a whole number incremented by one.

Example:
boot_0000.png

boot_0001.png
boot_0002.png
...
boot_0085.png

10.1.2 Admin Password

This is the password for the settings app to access the settings of the handset.
Default Value: 1234

10.1.3 Handset Debug

If handset debug is activated the android logcat information is continuously saved in the handset and every 30 minutes it is sent to the SMART Manager if within WiFi coverage. If it could not be sent then it will be stored and sent again after 30 min.
Default Value: Off

NOTE!
Activating this log will cause a lot of debug data stored the SMART Manager!
It should only be activated on a handset when troubleshooting/debugging a specific issue.

10.1.4 Handset Phone Profile

The phone profile changed telephony features depending on the DECT infrastructure used.

SMART AP:	This profile should be used when the handset is registered on the COBS SMART AP.
Profile 1:	This profile should be used when the handset is registered on the COBS CWS 2500/8000/400/6500*.

*Messaging over DECT will only work with SMART AP.

NOTE!
The handset will automatically reboot when the phone profile is changed.

10.1.5 Broadcast Group

These are the broadcast messaging groups (1-254) the handset will listen to. Broadcast messages are sent from the CMS as a “fire and forget” message broadcasted on all base stations in the DECT system. Each message is tagged with a broadcast group address and if the handset is configured to listen this the broadcast group the message is forwarded by the messaging service to for example the Fox Messaging app. All handsets will always listen to group 255.
Default: None (255 is always active)

10.1.6 Low Battery Threshold

This is the battery level in percent when the handset shall issue a battery low warning.
Default Value: 20%

10.1.7 Low Battery Warning Tone Level

The volume of the warning tone when the handset battery level is below the “Low Battery Threshold”.
Default Value: “Use Ring Volume”

10.1.8 Critical Battery Threshold

This is the battery level in percent when the supervisor will start to shut down non-prioritised apps running.
Default Value: 5%

10.1.9 Silent in Charger

If this is activated the handset will enter silent mode automatically when placed in the charger. When removed from charger it will resume the settings it had before placed in the charger.
Default Value: Off

10.1.10 License Warning

Defines the type of warning (On, Silent or Off) when the licenses are not updated from the SMART Manager.
Default Value: On

10.1.11 PP Status Event Mask

The PP Status Event Mask can be used to minimise the amount of messages sent from a handset. The reasons for this can be to save handset battery and to minimise the traffic load.
The events are still fired in the handset and can be detected by apps in the handset but the message sent to the CMS is masked.
Default Value: No events masked

10.2 Keys

10.2.1 Alarm Key Timeout

Defines the time the alarm key must be pressed to activate a long press event.
When activating a double press event this defines the time between the presses.
Default Value: 3s

10.2.2 Alarm Key Hot Dial

This telephone number is dialled when the alarm key long press is activated.
Default Value: None

10.2.3 Side Key Timeout

Defines the time the yellow side key must be pressed to activate a long press event.
When activating a double press event this defines the time between the presses.
Default Value: 3s

10.2.4 Side Key Hot Dial

This telephone number is dialled when the yellow side key long press is activated.
Default Value: None

10.3 Hardware

10.3.1 RFID Enabled

Enables the RFID location receiver.
Default Value: Off (RFID disabled)

10.3.2 RFID Auto Send Limit Low/High

If an RFID beacon with an ID between the “Limit Low” and “Limit Hi” is detected then a “Beacon Received” event is triggered and a message is sent to the CMS.

Limit Low Default Value:	944
Limit High Default Value:	1007

10.3.3 RFID Auto Send All Beacons

If this is checked then a “Beacon Received” event is triggered and a message is sent to the CMS when the RFID receiver detects a new RFID beacon ID
Default Value: Off

10.3.4 Block BLE Beacons

If this is checked then BLE for location is disabled.
Default Value: On (BLE for location disabled)

10.3.5 BLE Beacon Whitelist

This is a list of the MAC addresses of the BLE beacons that shall be used for location.

Use wildcard character * to add a range of MAC addresses from one manufacturer.
Click on “COBS Eddy” to add a wild card for COBS Eddy BLE Beacon MAC addresses.

If the list is empty (parameter omitted) then all BLE Beacons received are handled as location beacons.

Default Value: Whitelist empty

10.3.6 BLE Scanning Interval

This is the interval in seconds that the handset will scan for new BLE beacons (for location).
Default Value: 10s

10.3.7 BLE Scan Time

This is the time in seconds each scan will be searching for new BLE beacons (for location).
Default Value: 2s

10.3.8 BLE RSSI Threshold

Any BLE beacon with a received signal strength (RSSI) in dBm below this threshold will be ignored.
Default Value: -60dBm

Note that the value is negative!

10.3.9 BLE Low Battery Threshold

When a battery level below this threshold in mV is received from a BLE beacon a BLE Low Battery event is sent to the CMS.
Default Value: 2800mV

10.3.10 Bluetooth Mode

Controls the Bluetooth Mode in the handset.

Off: Bluetooth is disabled in the handset.
On: Bluetooth is always activated in the handset.
User: Bluetooth mode is controlled in the handset settings menu.

Default Value: User

10.3.11 NFC Mode

Controls the NFC Mode in the handset.

Off: NFC is disabled in the handset.
On: NFC is always activated in the handset.
User: NFC mode is controlled in the handset settings menu.

Default Value: User

10.3.12 Enable Camera

If not checked the camera is blocked and cannot be accessed.
Default Value: Off (Camera disabled)

10.3.13 WiFi Mode

Controls the WiFi Mode in the handset.

Off: WiFi is disabled in the handset.
On: WiFi is always activated in the handset.
On in Charger: WiFi is only activated when the handset is placed in the charger.*
User: WiFi mode is controlled in the handset settings menu.

*This option can be selected to increase the battery lifetime.
If selected then the update trigger must be set to "Charger In".

Default Value: User

10.3.14 WiFi SSID List

Controls which WiFi SSID the handset can connect to (must also be configured in the handset).

If the list is empty (parameter omitted) then the handset can be connected to any WiFi SSID.

Default Value: WiFi SSID List empty

10.3.15 Keep WiFi During Sleep

Controls the WiFi handling when the handset goes in sleep mode.

Always:	WiFi is always on when the handset is in sleep mode.
Never:	WiFi is never on when the handset is in sleep mode
Only when plugged in:	WiFi is only on in sleep mode when the handset is placed in the charger.
User:	Controlled in the handset settings menu.

Default Value: User

10.3.16 WiFi Tweak

Controls a "WiFi Tweak" mode that can improve WiFi connectivity under certain conditions.
If set to "On" then the WiFi is restarted if the SMART Manager cannot be reached at a ping request and/or configuration update.

10.4 Apps

10.4.1 Block Unknown Apps

If checked then the any apps installed from another source than the SMART Manager will be uninstalled.
Default Value: Off

10.4.2 End Apps at Ch. Out

If checked then all apps are closed when the handset is removed from the charger.
Default Value: Off

10.4.3 Apps

Select from the published apps in the SAM.

Merge Apps
If checked then the apps in this profile are merged with the apps in a profile with lower priority.
In not checked then the apps in a profile with lower priority are not applied.

Installed
If checked then the app will be installed.
If not checked and the app has previously installed from the SMART Manager it will be uninstalled (regardless of the "Block Unknown Apps" setting).

Prioritized
If not checked then the app will be closed when the battery level goes below the "Critical Battery Threshold".

Enabled
If not checked then the app icon will be removed from the launcher but is will not be uninstalled.
That means that the use will not be able to launch (start) an app that is not enabled.

NOTE!
If several profiles containing apps associated to the handset then it is the apps in the profile with highest priority (1=highest priority) that are applied, i.e. the apps are not merged from different profiles.

Default Value: No Apps (Supervisor will not be uninstalled)

10.5 Push To Talk

10.5.1 Groups

The groups are defined under “Push To Talk” and here you select which of the groups the handset shall listen to and be able to transmit to.
The handset can transmit to up 5 groups. If more than one groups is selected for transmission the user makes a double push on the yellow side key to select which group transmit to.
The number of receive groups is unlimited.

10.5.2 Max Transmit Time

The max time (in seconds) for a “Push To Talk” transmission. As all handsets share one PTT channel the transmit time should be limited to avoid one user from blocking the channel.
Default Value: 10s

10.5.3 Min Call Volume

The volume of a received PTT call.
Default Value: Use Voice Call Volume

10.6 Fox Settings

10.6.1 Main Display Icons

Main Display Icons are the icons displayed on the screen together with a received message from the CMS.
They are numbered from 1 to 255 that corresponds to the Icon Id in the message from the CMS.
It is possible to replace the default icons as well as add new icons to the Icon Id’s that are not assigned to a default icon.
Recommended format is a 202px x 202px png file but the Fox will try to convert/scale other formats too.
Default Value: None

10.6.2 Top Display Icons

Top Display Icons are the icons displayed in the top display when receiving a message from the CMS.
They are numbered from 1 to 255 that corresponds to the Icon Id in the message from the CMS.
It is possible to replace the default icons as well as add new icons to the Icon Id’s that are not assigned to a default icon.

The SMART1 top display requires a bitmap (.bmp) file format. Bitmap colours are limited to black (hex #000000) and white (hex #FFFFFF).
Custom top display images are allowed to be 16 pixels height and 16 pixels width (16x16 pixels).
Images larger than 16x16 pixels will be resized to fit the 16x16 format. When designing a top display image and have it displayed as designed, i.e. achieve pixel perfect image reflection, and keep the 16x16 dimensions for all your icons.

Note that a 1 pixel border will be added to each side of the bitmap when rendered in the handset top display. The extra pixels is for padding the text and icon number for a clear overall view.

Bitmaps can look something like this ( ).

Default Value: None

10.6.3 Alert Tones

Alert Tones are the tones played when receiving a message from the CMS.

They are numbered from 1 to 255 that corresponds to the Alert Tone in the message from the CMS.
It is possible to replace the default Alert Tones as well as add new tones to the Alert Tones that are not assigned to a default tone.

The format of a custom alert tone can be any of the following:

- MP3 files: Mono or stereo 8- 320kbps CBR or VBR.
- Wav files: 8 or 16 bit linear PCM with sampling rates 8000. 16000 or 44100 Hz.
- Ogg files.

More information on the supported audio formats can be found at:
https://developer.android.com/guide/topics/media/media-formats.html

Default Value: None

10.6.4 Top Display Show Icon

If this is checked then the Top Display Icon is displayed in the top display together with the message text.
If not checked then the message text will use the whole width of the top display.
Default Value: On

10.6.5 Top Display Orientation

If this is checked then the Top Display is rotated 180 degrees.
Default Value: Off

10.6.6 Use Alarm List Lock screen

If checked then the Fox Alarm List will be used as lock screen.
Default Value: Off

10.6.7 Authenticated Custom Menus

If checked then it will not be possible to reply on an alarm using the Custom menus in the alarm if there is no user logged on the handset (using the “User Login” app).
This is to prevent a user from acknowledging an alarm without a user id tagged to the response.
Default Value: Off

10.6.8 Lock Screen Display Timeout

This is the timeout before the Alarm List Lock screen will lock the handset (if “Use Alarm List Lock screen” activated).
Default Value: 15s

10.6.9 Messaging Logo

It is possible to replace the COBS logo in the Fox app with a custom logo.
The original Fox logo is a 156px x 60px png file but the Fox will try to convert/scale other formats too.
Default Value: None

10.6.10 Background Colour

This is the background colour of the header in the Fox app.
Default Value: #000000 (Black)

10.6.11 Help File URL

In the Fox menu there is a “Help” item. When the user click the “Help” item the web browser is opened and directed to this URL. The URL can be pointed to any web server that can contain customised help information. The SMARTCOM process in the CMS has a built in webserver with a customisable help web site.
Default Value: The CMS IP Address using port number 8085.

10.6.12 Disable Erase All Messages

When checked the option to erase all messages is removed.

An individual message can still be removed if it is allowed in the message information, otherwise messages can only be removed from the CMS.
Default Value: Off

10.6.13 Alert Tone Level

This is the volume level for the alert tones used in the FOX app. The volume can be set between 1 and 10 or set to use the media volume in Android that configured in the handset.
Default Value: Use Media Volume

10.6.14 Alert Tone In Call Level

This is the volume level and/or vibrator for the alert tone in the FOX app if a message is received during a voice call. The volume can be disabled or set between 1 and 10 or set in combination with the vibrator.
Default Value: 7

10.7 Contact Settings

10.7.1 Contact Lists

Select from the configured Contact lists.
The selected contact lists will be merged and added to the handset android contacts.

NOTE:
The contact lists from different profiles are not merged, it is the contact lists from the highest prioritised profile that are merged and added.

To remove all SMART manager contact from a handset create an empty contact list and enable this in the highest prioritised profile.

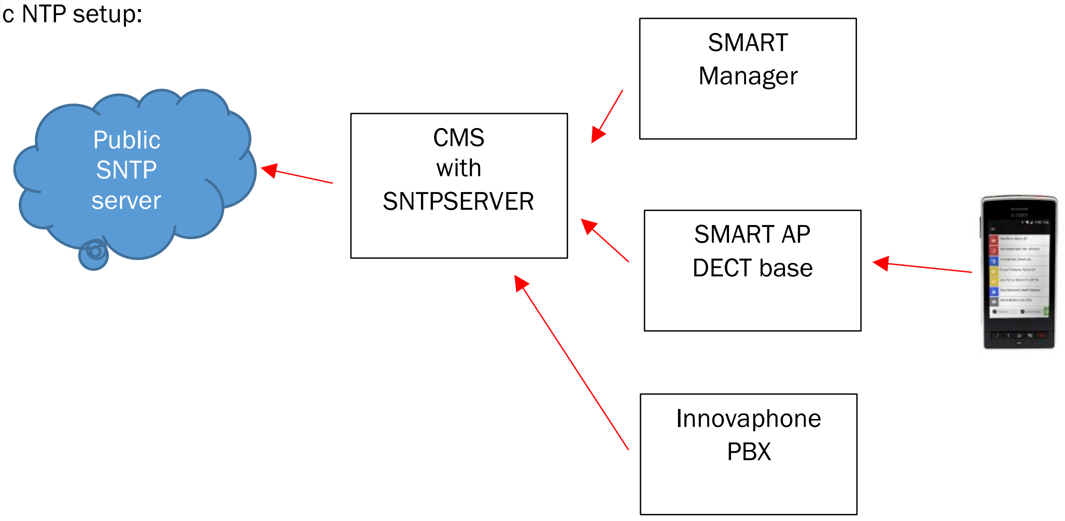
10.8 Custom App Settings

This is an arbitrary data file that can be used for third party apps.
It can for example contain settings for an app.
Default Value: None

11 Time configuration

The time synchronisation can be configured in a number of different combinations depending on the system design.

Basic NTP setup:



Basic setup configuration:

The CMS should be configured with the SNTPSERVER process to enable the other units, like SMART Manager, SMARTAP (DECT bases) and PBX to have a common time source.

Then the CMS should synchronise to an external SNTP server to get the correct time that will be distributed to all other units.

The SMART1 handsets will use the DECT system to synchronise the time from the SMARTAP base.

This setup will ensure that all units will have the same time and that logs/messages can be synchronised.

NOTE:
If SPEAK handset are used on the same site as the SMART1 the SMART AP must be configured to use timezone and daylight saving. In this case the SMART1 should be configured to use a NTP server directly and not use DECT time.

11.1 Configuration of the basic setup

11.1.1 CMS Configuration

Under “System”->”Time”, configure the CMS to synchronise the time with the external NTP server.
Add an SNTP Server process (license needed) using the default configuration.
See “T100200 Installation Guide CMS SNTPSERVER” for more information on how to setup the CMS.

11.1.2 SMART Manager Configuration:

Under “Configuration” enter the CMS as NTP server and set the appropriate Time Zone.
Under “Site” leave the “Handset NTP Server Address” **empty** and set the appropriate Time Zone.

11.1.3 SMART1 Configuration:

All SMART1 settings for this setup are done by the supervisor.

11.1.4 SMART AP Configuration

Under “Time” enter the CMS as “Time Server”.
Uncheck “Set timezone by country/region”.
Uncheck “Set DST by country/region”.
Set “Daylight Saving Time (DST)” to “Disabled”.
NOTE!
The SMART AP web GUI will display the GMT on the “Welcome” page but the syslog messages sent to the SMART Manager will be tagged with the correct time zone and daylight adjustment.

12 Default Ports

The SMART Manager and SMART1 uses the following default server ports:

SMART Manager Server Ports (incoming):

80 TCP	Web browser -> SMART Manager	Redirects to https on port 443 (optional)
443 TCP	Web browser -> SMART Manager	Configuration GUI
443 TCP	SMART1 -> SMART Manager	Registration and profile updates
514 TCP/UDP	Syslog -> SMART Manager	Incoming syslog messages (optional)

SMART1 Handset Server Ports (incoming):

9991 TCP	SMART Manager -> SMART1	Registration and profile updates

13 Troubleshooting

13.1 Apps/Services running

13.1.1 Supervisor

The supervisor must always be running in the handset.
In the status bar of the handset the icon for the supervisor should always be visible.

When pulling down the status bar the notification for the supervisor should display the local number and that the handset is registered.

13.1.2 Messaging Service

If using messaging then the messaging service must always be running in the handset.
In the status bar of the handset the icon for the messaging service should always be visible.

When pulling down the status bar the notification for the messaging service should display the communication mode, DECT or WiFi.

13.1.3 Fox Messenger

If using the Fox Messenger for displaying alarms and messages then the Fox Messenger must always be running in the handset.
In the status bar of the handset the icon for the Fox Messenger should always be visible

When pulling down the status bar the notification for the Fox Messenger should display “Ready to receive messages”.

13.2 Factory reset of a SMART1 handset

A handset can be factory reset in the following ways:

Remote Wipe
A “Remote Wipe” can be sent from the SDM in the SMART Manager to the handset over WiFi.

Boot Menu
Turn then handset off.
Press “Vol up” + “Home” and keep then pressed while pressing the “Power On” key.
Keep them pressed until the handset vibrates twice.
The handset will then start in the android boot mode.
Press the “Home” key to enter the boot menu.
Select the “wipe data/factory reset” menu option by pressing “Vol up/down” and press the “Power”.
Step down to the “Yes – delete all user data” option and press the “Power” key.
Select “reboot system now” and press the “Power Key”.

14 Abbreviations

In this document the following abbreviations are used.

CMS	COBS Message Server
SDM	SMART Device Manager
SAM	SMART App Manager
Local number	Extension Number
APK	Android Application Package
AP	Access Point
PTT	Push To Talk

15 Document History

161014	RA	First edition
170125	RB	Added new features in SMART Manager 2.01.
170522	RC	Added new features in SMART Manager 2.02.
171006	RD	Added Contact Lists and Labels.
180413	RE	Added new features in SMART Manager 2.04.