

Sophos Mobile Control Administrator guide

Product version: 2

Document date: December 2011



Contents

- 1 Glossary 3
- 2 About Sophos Mobile Control..... 4
- 3 Prerequisites..... 6
- 4 Login 7
- 5 Overview..... 8
- 6 Common elements..... 13
- 7 Wizards..... 19
- 8 Task view 20
- 9 Inventory 23
- 10 Provisioning 28
- 11 Applications 29
- 12 Configurations 32
- 13 Command bundles 34
- 14 Backup 36
- 15 Task bundles 37
- 16 Traffic counter 38
- 17 The Sophos Mobile Control Self Service Portal 39
- 18 Troubleshooting 40
- 19 Technical support 41
- 20 Legal notices 42

1 Glossary

Term	Explanation
GPRS network	Mobile network for packet-oriented data transmission
UMTS/3G network	Mobile network for packet-oriented data transmission
IMEI	International Mobile Equipment Identity, unique serial number of a mobile device
OTA	Over-The-Air
SMS	Short Message Service
APNS	Apple Push Notification Service
C2DM	Google Android Cloud-to-Device-Management Push Notification Service
BES	RIM BlackBerry Enterprise Server
OMA DM	Open Mobile Alliance Device Management
OMA DS	Open Mobile Alliance Data Synchronization
MDM	Mobile Device Management
PDA	Personal Digital Assistant

2 About Sophos Mobile Control

Sophos Mobile Control is a device management solution for mobile devices like smartphones and PDAs. It allows configuration and software distribution as well as security settings and many other device management operations on mobile devices. The Sophos Mobile Control system consists of a server and a client component which communicate through data connections and SMS messages. This manual describes the Sophos Mobile Control web interface.

Sophos Mobile Control currently supports the following mobile device platforms:

- **Android**
- **Apple iOS**
- **Windows Mobile**
- **BlackBerry (through BlackBerry Enterprise Server)**
Note: For BlackBerry devices only the following functions are supported: show devices in Sophos Mobile Control, Lock, Wipe, show software inventory, show device properties. The Self Service Portal does not support BlackBerry devices.

Due to the nature of the different platforms supported features vary.

2.1 Terminology

In this manual, the following terms are used:

Term	Explanation
Device	The device to be managed (smartphone, PDA, etc.).
Client	The Sophos Mobile Control client installed on the device, built-in MDM client iOS4.
End user	The end user of the device.
Server	The central component in the Sophos Mobile Control architecture.
Web interface	The web interface of the server which is used to manage the devices.
Administrator	The person who uses the web interface.
Customer	The tenant whose devices are managed with Sophos Mobile Control.
Provisioning	The process of equipping the device with the Sophos Mobile Control client.

2.2 Concept of different user roles

Because of the rights concept of Sophos Mobile Control not every module/action described in this guide is necessarily visible. Also, some buttons shown in screenshots may not be visible. The rights assigned to different modules and actions are defined in user roles. These roles may change and are fully adjustable with a special tool.

Usually the following roles exist:

Role	Description
Administrator	Is allowed to perform all actions.
User	Is allowed to perform all actions concerned with installing and administrating a device, but not with essential settings (for example modifying a user, client package or template).
Helpdesk	This role is intended for support purposes and has the fewest rights (for example installation of software packages), but no access to critical functions.

3 Prerequisites

To use the web interface, you need a Sophos Mobile Control user account. These accounts consist of the following information:

- Customer
- User
- Password

In addition, a computer connected to the internet is necessary. It has to be equipped with one of the following internet browsers. We recommend that you use the newest version of the relevant browser.

- Microsoft Internet Explorer 6 (or higher), SVG-Viewer for the charts
- Mozilla Firefox 1.0 (or higher)
- Google Chrome
- Apple Safari

For the web interface, JavaScript has to be activated.

4 Login

To log in to the web interface:

1. Enter the Sophos Mobile Control server URL in your preferred internet browser.
2. Enter your account information.
3. Click **Login** to send the data to the server.

If the information is correct, access to the web interface is granted. If the information is incorrect, an error message is shown and access is denied.

5 Overview

After login the web interface displays the home page with the welcome view.

The home page consists of the header, the menu bar and the view. The header and the menu bar are static. The view is dynamic and changes its content depending on the relevant topic.

5.1 Header

The upper part of the interface shows the **Filter**, **Home**, **Help** and **Logout** buttons.



Button	Description
	Inactive filter – This button opens the filter function. With the filter function, you can restrict the number of items shown in lists. For further details, see Filters (page 17).
	Active filter – This button opens the filter function. With the filter function, you can restrict the number of items shown in lists. For further details, see Filters (page 17).
	The Home button opens the welcome view.
	This button opens the administrator guide as pdf.
	This button logs off the currently logged in user.







5.2 Menu

The menu on the left side of the interface is used to navigate to modules and functions. Click on a main module to open the sub items with a brief description. You can also open sub items directly.

5.3 Welcome view

The welcome view shows information about the user currently logged in (for example user name and role), information about the server version and buttons for the standard settings.

The following table offers a brief description of the buttons:

Icon	Description
	Opens the Settings dialog.
	Opens the Change password dialog.
	Opens the User management dialog.
	Opens the Technical contact dialog.
	Creates a report of all customers' devices (CSV file).
	Opens the Compliance settings dialog.

In addition a dashboard view of the managed devices is shown:

- **Status:**
Shows the status of registered devices: for example compliant/not compliant, managed/not managed.
- **Platforms:**
Shows the number of devices for each platform.
- **Device groups:**
Shows device groups with the number of devices they contain.

Click on a table row to open a details view of this dashboard item.

5.3.1 Settings

The **Settings** dialog shows the following tabs:

- **Personal**

In this tab, you can specify the platforms you want to use and limit the maximum data sets you want to display per page. You can choose between 20 and 100 Data sets per table page. If you select specific platforms, you can only use those specific platforms with Sophos Mobile Control. All other platforms are hidden. In addition, all modules and functions that are not needed for a specific platform are hidden.

Note: These settings are user-specific. They have to be made separately for each user.
- **Provisioning via E-mail**

In this tab, you can define an E-mail template for the initial provisioning of devices by E-mail. With initial provisioning by E-Mail, devices are registered by sending an E-Mail to an account (personal account or Google Mail account) available on the relevant device instead of SMS. You need to specify an Originator and a Subject. You can also predefine the E-mail Content. For the download link, you can use the placeholder `_DOWNLOAD_LINK_` which will be replaced by the actual link in the E-mail sent to devices.
- **iOS APNS (Apple Push Notification Service)**

In this tab, you can upload the “Apple Push Notification keystore” (which is needed to be able to use the APNS).
- **Android C2DM (Cloud-to-Device Management)**

In this tab, you can specify the account to be used for sending Google Push Notifications. Possible types are **Google**, **hosted** and **Google or hosted**. You need to register this account for C2DM and specify the Sophos Mobile Control client package.
- **RIM BES (BlackBerry Enterprise Server)**

In this tab, you can specify the BES URL and account configured to be used for Sophos Mobile Control.
- **Self Service Portal**

With the Sophos Mobile Control Self Service Portal, end users can register their devices themselves. In this tab, you can specify for which platforms registration through the Self Service Portal should be active, the relevant device template, default group and task bundle. You can also configure a mobile policy, disclaimer or agreement text to be displayed as a first step when users register their devices. For the text, HTML formatting tags are supported. The text will be displayed in the Browser accordingly.

5.3.2 Change password

In this dialog, you can change your user password. Enter the **Old password**, a new one and confirm the **New password**.

5.3.3 User management

User management gives you a quick overview of all registered users. To display all user information, click the magnifier button. You can sort the table by login name or last name. You can also add, edit or delete users.

For further details on tables, see [Tables](#) (page 14).

For users, the relevant user details and - most importantly - passwords need to be specified. In addition, you must specify the user role. In a standard installation there are three user roles:

- Administrator
- User
- Helpdesk

To add a new user, click the **Create new user** button. Now the **Edit user** dialog is shown. In this dialog, you enter all relevant user information: **Login name**, **Role**, **Password**, **Last name**, **First name**, **E-mail** and optionally a **Description**.

Most people registered should have the role **User**. This role allows everything by default except for the right to modify:

- User management
- Sophos Mobile Control client packages
- Device templates

5.3.4 Technical contact

The **Technical contact** information refers to the customer's IT staff who can be contacted if there are any questions or problems. To add a technical contact, click the **Edit** button and enter the **First name**, **Last name**, **E-mail**, **Phone number** and **Mobile number**.

Note: Only users with the user role **Administrator** can edit the **Technical contact** information.

5.3.5 Compliance settings

In the **Compliance settings** dialog, you can configure a compliance check for devices. The function checks if devices are still managed by SMC and comply with your corporate rules for mobile access. For the compliance check, you can define one set of rules per customer. You can enable/disable any platform. Click on the tab for the relevant platform to specify the rules per device type.

The following compliance settings are available for rules:

- **Managed required:** Yes/No
- **Allow Jailbreak:** Yes/No
- **Allow root access:** Yes/No
- **Passcode required:** Yes/No
- **Allow Non-Market Apps:** Yes/No
- **Min. os version:** Select the minimum operating system version required.
- **Max. synchronization gap:** Select the maximum time span between synchronization processes of devices.
- **Max. iOS app synchronization gap:** Select the maximum time span between synchronization processes of the iOS Sophos Mobile Control App. For further information, refer to the Sophos Mobile Control user guide for Apple iOS.
- **Blacklist:** Click **Edit** to define a blacklist of apps that must not be installed on devices.
- **Mandatory apps:** Click **Edit** to define a list of apps that must be installed on devices.















For each option, you can define the action **Disallow ActiveSync** in case of non-compliance. If the device does not comply with the rule, E-mail access will automatically be denied.



The **Status** table of the **Welcome** view shows how many devices are non-compliant. Click on the **Not compliant** row to show a list of all non-compliant devices.

6 Common elements

6.1 Buttons

This chapter gives a brief overview of all buttons throughout the web interface and their functions.







Button	Description
	Navigates to the next view of a wizard.
	Navigates to the last view of a wizard.
	Provides further information on a specific topic.
	Duplicates a profile/command bundle.
	Confirms an action.
	Cancels an action.
	Switches to the Select device group(s) view.
	Switches to the Select device(s) view.
	Finishes a wizard and executes an action.
	Enables you to change settings or information.
	Saves changed settings.
	Reloads the content of a table.
	Adds an entry.
	Deletes a selected entry.

	Imports entries.
	Creates a device report (CSV file).

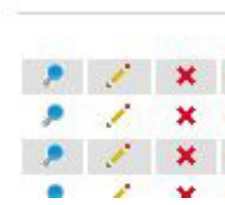
6.2 Tables




To make the interface easier to use and to enhance responsiveness, all items shown in tables are grouped to usually 20 items per page. To browse table pages, use the table controls below the corresponding table.

These controls allow the following actions:

Control	Description
	Jump to first page.
	Jump back five pages.
	Jump back one page.
1 2 3 4 5 6	Jump to a specific page.
	Jump forward one page.
	Jump forward five pages.
	Jump to the last page.

Most tables allow actions regarding the listed items. The action icons are shown next to the items. They trigger the following actions:



Icon	Description
	Show details of this item.
	Edit this item.
	Delete this item.

In some tables, you can also select one or several items for an action. To do so, select the check box next to the items. To select all items currently displayed, select the check box in the table header.



For selecting exactly one item, tables may also include radio buttons.






The next two tables are based on each other. They are used when setting up specific functions as applications or system components of more than one device or device groups. The first table is only shown, if more than one device or a group of devices was selected during device/group selection. This table shows all devices selected or all devices included in the selected group/s, so you can specify a device as data source. Selecting a device as data source makes it easier to find the right function as only the functions available on the specific device are shown. But changing one of the settings will affect all of the devices or device groups selected, if they provide the same functions.

Settings can be activated, left unchanged, or deactivated. Remember that different devices may be configured differently. Activating or deactivating a function activates/deactivates the function on all selected devices. If you choose to leave the previous setting unchanged, the different settings of the devices are maintained.



Use the radio buttons to toggle the state to the desired value. The following symbols indicate activated/unchanged/deactivated processes:

Symbol	Description
	Activated process
	Leave process unchanged
	Deactivated process

In many tables, you can sort items. Fields that can be used for sorting show small arrows. Click the arrows to sort the items according to the selected field.

6.3 Filters

By using filters you can restrict the number of items shown in lists according to defined criteria. To open the filter, click the **Filter** button located in the header. The Sophos Mobile Control web interface offers four different filters:

- **Device filter**
- **Device group filter**
- **Software filter**
- **Task filter**

The filters are not only valid for the function currently displayed, but for all functions where items of this type are listed. Filters are shown as drop-down menus. A status message indicates whether filters are active and restrict the results display at the top. After you have selected the required criteria, click the **Filter** button to activate the filter and reload the list of items. To reset a filter, click the **Reset** button, which is displayed if a filter is active. The different criteria options provided by the filters are described in the following sections.

6.3.1 Device filter

The device filter allows filtering lists of devices. It offers the following options:

Option	Description
Name	Filtering device names/parts of device names.
IMEI	Filtering IMEI.
Phone number	Filtering phone number.
SMC client	With this option, you can show all provisioned devices or all devices that are not provisioned. Note: If you use this option in combination with the IMEI/Phone number option, the result set is not restricted further, but extended.
Package	Filtering software packages/parts of software packages. You can use wildcards for both fields.
Device group	Device groups whose members are not to be displayed can be deactivated.
Operating System	Devices which are equipped with a certain operating system can be deactivated.

6.3.2 Device group filter

The device group filter restricts the results in lists of device groups. It offers the following option:

Option	Description
Name	Filters by name of the device group.

6.3.3 Software filter

The software filter is used to restrict the results in lists of software packages. It offers the following options:

Option	Description
Name	Filters by name of the package
Version	Filters by version of the package
Operating System	Packages which are applicable for certain operating systems can be filtered by selecting the check box next to the operating systems.

6.3.4 Task filter

With the task filter, you can filter tasks displayed in both the task view and the task archive. It offers the following options:

Option	Description
Device	Filters by device name.
Package	Filters by package name.
State	Tasks in a specific state can be deactivated. The states are grouped in five groups for easier handling.
Group	Device groups whose members are not to be displayed can be deactivated.

7 Wizards

The concept of wizards guiding through task creation is a common feature in the web interface. This chapter first describes the basic procedure of creating a task. Afterwards, module-specific aspects are described.

1. As a first step, you select the target devices for the task. Under **Select Devices** or **Select device group(s)**, you can select one or more devices or device groups.

Note: Due to the different objects to select for the task it is usually not wise to select devices with different operating systems, for example Android and Windows Mobile.

2. In the next step, you select the task object. This can for example be a software package to install or uninstall. In the final step under **Set execution date**, you schedule the task.

Now is pre-selected, but you can also select date and time. The task will be started on the given date. This makes it for example easy to have tasks running at night when the users do not use their devices.

3. Click **Finish** to start task creation.

Depending on how many devices are selected, this may take some time. A progress bar shows task creation progress. The server creates a separate task for each selected device, no matter if it was selected by adding a group or as a single device. Any events during task creation are listed in a table with a description and the corresponding device. This is for example the case, if a device already has the selected package installed. Tasks for devices listed in this table are not created. All other devices remain unaffected. Their tasks are created.












The tasks appear in the task view after the server has finished creating them. Depending on the scheduled date, they are not necessarily started immediately.

All wizards work this way. Later chapters just describe aspects to consider regarding the specific modules.

8 Task view

In the **Task view**, you can monitor all existing tasks in the system. In contrast to the task archive, the **Task view** only lists unfinished and failed tasks. For user convenience, it also displays the finished tasks of the last few days. Older tasks are automatically moved to the task archive. The **Task view** is refreshed automatically, so you can watch the states of the tasks evolve. The task archive does not have this auto-refresh feature. All tasks created using the web interface are listed in the task view (installations, process activations, text SMS etc.). It does not matter which user created the task, all users see all tasks of the customer.

The icons of the task item categorize the respective task. They have the following meaning:

Icon	Description
	Installation
	Uninstallation
	Process activation/deactivation
	Explicit refresh of device data
	Text SMS
	Windows Mobile profile transfer
	iOS profile transfer
	Command bundle transfer
	Bootstrap
	Command transfer
	Windows Mobile security settings

The delete icon removes the item next to it. The task is deleted. If the task is not finished at the time of deletion, it may still be carried out depending on the current task progress.

8.1 Explanation of task states

	State	Description
●	Accepted	The task has been created.
●	Retry	The task will be retried later.
●	Started	The task has been started.
●	In progress	The execution of the task is being prepared.
●	Sending notification	The client is being notified.
●	Waiting for delivery	The server is waiting for a confirmation of the notification by the client.
●	Notified	The client has received the notification.
●	Exported	The client has received the package and/or the commands.
●	Result evaluation started	The client has answered and the evaluation of the result has been started.
●	Result incomplete	The result evaluation showed that not all commands' results have been received by now.
●	Successful	The package has been installed or the commands have been successfully executed. Note: For the initial provisioning of the Sophos Mobile Control client the task must finish with the state "installed".
●	Installed	The Sophos Mobile Control client has been installed successfully. The device is provisioned now.
●	Result evaluation failed	The result evaluation could not be executed.
●	Result evaluation aborted	The result evaluation has been aborted.
●	Task partly failed	Not all commands of the task could be executed successfully.
●	Delayed	The task will be restarted later.
●	Failed (retry queued)	The task has failed and will be retried later.
●	Task failed	The task has failed and no further retries are queued.
●	Completely failed	The task has failed.

8.2 Task history

The magnifier icon opens the **Task history**. Besides general information on the task (for example **Device**, **Package name**, **Creation date** etc.) it shows the states a specific task went through including timestamps and error codes.

If there are commands to be executed by the device, an additional **Details** button appears in the **Task history**. Click the **Details** button to open the **Commands** view. The commands sent to the device are part of the task. They are executed by the client. Results indicating the success or failure are transferred back to the server. If there was no error, the error code is “0”. If a command has failed, the error code is displayed. In most cases there is also a description of what may have caused the command to fail.

9 Inventory

If you click **Inventory** in the menu, you get a quick overview of the sub items **Devices** and **Device groups** and a brief description of their functions. In addition, a circular chart of all devices and the different platforms registered is shown.

Click on one of the platforms in the chart to open a second chart showing a breakdown of the versions installed on the devices.

Note: The Internet Explorer must have an SVG-Viewer plug-in installed to display the chart.

9.1 Devices

The **Devices** view lists all devices known for the customer with their **Name**, **Operating System** and the **Group** they belong to.

The **Managed** column shows whether the device is controlled by Sophos Mobile Control (green icon: Yes, red icon: No). The **Compliant** column shows whether the device complies with the compliance check rules defined (green icon: Yes, red icon: No).

The **Synchronized** column shows when the devices have last synchronized with the server.

9.1.1 Creating a new device

1. To create a new device, click the **Create new device** button.
2. In **Select device template**, you select the appropriate device template.
New device templates can be added by updates supplied by Sophos.
3. In **Edit device**, specify the device details. You must at least specify the device **Name**, **Description** and **Phone number**. It is important to enter the phone number in international format, for example “+491701234567”.

For registering the device by E-mail you can also enter an E-Mail address. You can define the E-Mail to be sent under **Settings**.

9.1.2 Importing devices

You can add new devices by importing a .csv file with up to 500 devices. A sample file with the correct column names and column order is available for download from the import page.

Note: Use a text editor for editing the .csv file. If you use Microsoft Excel, values entered may not be resolved correctly. Make sure that you save the file with the extension .csv.

Click the **Import devices** button showing a small arrow symbol pointing downwards.

1. In the message displayed, select the data source **CSV file**.
The **Import devices** page is displayed.
Note: If you do not have a .csv file with devices yet, you can download a sample file now and use it for creating your import file.
2. Select the .csv file you want to import and click **Upload file**.
The entries in the .csv file are checked for errors and displayed on the import page.
Note: If there are any errors in the .csv file, it cannot be imported. An error message is displayed next to the relevant entries. Edit the .csv file accordingly and try again.
3. If all entries are correct, click the blue **Finish** button.

The devices listed in the .csv file are imported and displayed in the **Devices** view.

9.1.3 Importing BlackBerry devices through BlackBerry Enterprise Server

You can import BlackBerry devices through BlackBerry Enterprise Server to show them in the Sophos Mobile Control **Devices** view.

1. Click the **Import devices** button showing a small arrow symbol pointing downwards.
2. In the message displayed, select the data source **BlackBerry Enterprise Server**.
The **Import devices** page is displayed.
3. Click the **Query** button to display a list of all devices registered with BlackBerry Enterprise Server. You can also specify a filter for the list of devices in the fields **User name** and **E-mail**.
4. Select the devices to import and click the blue **Finish** button.
A message is displayed.
5. In the message, select if all or only selected devices should be imported, specify the template and device group to be used.
6. Confirm your selection by clicking the blue button.

The selected BlackBerry devices are imported and displayed in the **Devices** view.

Note: For BlackBerry devices only the following functions are supported: show devices in Sophos Mobile Control, Lock, Wipe, show software inventory, show device properties. The Self Service Portal does not support BlackBerry devices.

9.1.4 Creating a device report

To export device information from the **Devices** view:

1. Click the **Export** button showing an arrow symbol pointing upwards.
A file download dialog is displayed.
2. Click **Save** to save the export file to the required file location.

Note: The device report format is different from the device import spreadsheet format and contains significantly more information. An export can therefore only be imported after major adjustments.

9.1.5 Show device/Edit device view

To view/edit the details of individual devices, click the magnifier symbol/pen symbol next to the relevant device in the **Devices** view.





In the **Show device/Edit device** view, all relevant information for an individual device is displayed: **Name, Description, Device group, Operating System, Phone number, Last synchronization**. The table at the bottom shows all properties for the device. For Android devices, rooted smartphones are detected and the relevant property is shown in this view. For Apple iOS devices, jailbroken smartphones are detected and the relevant property is shown.













Note: Before a device has been registered, the **Operating System** information displayed here originates from the operating system you have selected when you added the device. After the device has been registered, the operating system is detected automatically. The **Show/Edit device** view then shows the more detailed operating system information received from the mobile device.






For non-compliant devices, click the **Compliance/Violations** button to show a table of all violations occurred. Click the **Show** icon in the table to view the **History** of violations for the device. Click the **Edit** icon to display the **Add action** dialog. In this dialog, you can enter information on the action taken due to the compliance violation. For example: Notified user by E-Mail.

9.1.6 Buttons for administrating devices

There are many different buttons to help administrating the devices and viewing device information. Certain buttons are shown depending on device platform and configuration.

Button	Description
	Click this button to set the name and the IMEI of the specific device in the Device filter .
	Shows the installed software packages, version numbers and processes.
	Shows the installed profiles. In this dialog, you can also delete profiles.
	Use this button to add an ActiveDirectory link to the device.

Button	Description
	Use this button to remove an ActiveDirectory link to the device.
	Use this button to refresh the data.
	Opens the traffic counter details for the device.
	<p>Indicates that E-Mail access is denied. An additional icon on the button indicates whether E-Mail access was denied</p> <ul style="list-style-type: none"> ▪ manually  or ▪ automatically . <p>If you click this button, a window opens where you can allow E-Mail access or set it to automatic mode.</p>
	<p>Indicates that E-Mail access is allowed. An additional icon on the button indicates whether E-Mail access was allowed</p> <ul style="list-style-type: none"> ▪ manually  or ▪ automatically . <p>If you click this button, a window opens where you can deny E-Mail access or set it to automatic mode.</p>
	<p>Indicates that the Active Sync ID for the device is unknown. Settings do not have any effect. How to get the Active Sync ID for a device depends on the device type:</p> <ul style="list-style-type: none"> ▪ For Apple iOS and Windows Mobile Devices, the Active Sync ID is known as soon as the device is managed by the SMC profile/client. ▪ For Android devices, the ID is resolved when the device connects with the Exchange Server for the first time. Devices are identified by the Exchange user name. The Active Sync ID is then entered. Note: This is only possible if just one device is found.
	Locks the device remotely.
	<p>Unlocks the device remotely. For Apple iOS devices, this icon also resets the passcode/password on the device. The user is prompted to define a new one. For Android devices, the administrator can replace the passcode/password with a new one. It must comply with the passcode/password rules.</p>

Button	Description
	Deletes all synchronization data of the device. Sophos Mobile Control client needs to be reinstalled.
	Use this button to wipe the device remotely in case of loss.
	Use this button to send a text SMS message to a specific device.
	Note: This function is only available for Android devices. Use this button to locate a device.
	Note: This function is only available for Android and Windows Mobile devices. Restores the data for the device from backup.

Note: Property changes only become valid after you have clicked **Save**. If you do not save the changes you have made, they do not have any effect.

When you delete a device its tasks are automatically deleted too. The server deletes everything that is related to the device, including synchronized information. The client side is not affected by the server side deletion. If the client is to be reinstalled, the Sophos Mobile Control client has to be removed from the client manually.

9.2 Device groups

With device groups, you can categorize devices. A device always belongs to exactly one device group. Using different groups makes it easy to work with the system because most modules allow the selection of complete groups as well as single devices.

Note: We recommend to only group devices which have the same operating system. This makes it easier to use them for installations and other operating system specific tasks.

Deleting device groups moves the group's devices to another group that has to be specified. If there is no other group left to move the devices to, the group cannot be deleted. Before a group is deleted, a warning message is displayed. To delete the group, confirm this message.

10 Provisioning

10.1 Sophos Mobile Control client packages

This function lists the Sophos Mobile Control client packages available for provisioning new devices. New packages can be added by updates supplied by Sophos. You can also use the **Create new package** button.

10.1.1 Create new Sophos Mobile Control client package

To create a new Sophos Mobile Control client package, specify a **Name**, **Version number** and compatible **Operating systems**. In addition, specify how the setup is to be provided: **Upload package** or **Link to package**.

10.2 Sophos Mobile Control client installation

This function is used for provisioning new devices. This is usually done only once per device. The function creates basic data for the device and sends a short message (SMS) with an installation link for downloading the selected Sophos Mobile Control client package. The type of the message depends on the device template used, because devices with different operating systems support different ways to install the client. For further information on how to install the Sophos Mobile Control client on the device, refer to the *Sophos Mobile Control user guides for Android, Apple iOS and Windows Mobile*.

Note: If the Sophos Mobile Control client needs to be reinstalled because the device has been reset/formatted, the Sophos Mobile Control client flag in the device's properties has to be reset before entering the wizard. This causes the server to remove all data of previous synchronizations.

11 Applications

11.1 Software packages

With the software packages function, you can create new packages to be installed on the devices. Packages may consist of several files although they are usually packaged as an operating system specific file (for example “cab” or “apk”).

As an administrator, you can upload new packages by clicking the **Create new package** button.

Under **Edit package**, enter the **Name** and the **Version** of the software package and select the **Operating system** the package applies to. In addition, specify how the setup is to be provided: **Upload package** or **Link to package**.

For the provisioning of software through the Enterprise App Store, you can define software packages as **Required** or **Recommended**. The software package is then listed in the Enterprise App Store of the SMC agent for download and users can select it for installation. The installation process runs unattended or with very little user interaction.

If you want to delete a software package, you must first delete all active tasks referencing it.

11.2 Install

With the **Install** function, you can install software packages on the devices. If the device is provisioned, installation is performed by the Sophos Mobile Control client. In this case, the operation is silent. The end user cannot interfere.

The software packages available for installation have to be created by using the software packages function before they are available in the object selection step.

In the date selection step, you can set the **Enforce** flag for this task. In this function, the **Enforce** flag specifies if the task is to be created although the device already has the selected package installed. If it is not selected and the server notices that the device already has the package installed, it will output a notice and will not create a task for this device.

11.3 Uninstall

With the **Uninstall** function, you can remove packages from the clients. The object selection step lists packages installed on the clients. If more than one device has been selected, the list shows all packages for all devices. In this function it is likely to get a notice when creating the tasks because usually not all devices have the selected package installed.

Uninstallation is carried out silently. The end user cannot interfere. If the application to be uninstalled is currently running, Sophos Mobile Control closes it before uninstalling it.

11.4 Enable/disable

With this module, you can activate or deactivate processes on the device. Deactivated processes are not allowed to run. The Sophos Mobile Control client monitors all processes running on the device and immediately kills deactivated processes. This allows you as an administrator to disable certain applications. Activated processes are unaffected and can be started.

Note: If software packages are installed on the device manually (not via Sophos Mobile Control), the included processes are deactivated by default. If the package has been installed using Sophos Mobile Control, they are activated automatically.

Note: If a package that contains activated processes is uninstalled, the processes remain activated. This means that once the same application is installed again the processes are still activated, regardless of whether the installation is done by Sophos Mobile Control or manually.

Processes can be activated or deactivated for single or multiple devices. The common wizard is used to create the tasks. When you set up multiple devices, one additional step called **Base device selection** is added after device/group selection.

Note: For Windows Mobile, the enabling and disabling of processes is deactivated by default. You can activate this functionality with the setConfig command (ProcessSecurityOn).

11.4.1 Single device

For some devices, system processes are also defined. You define them when creating the device from a template or with the **Create new property** function (under **Edit device**).

If the state of a process that is not listed is to be changed, you can enter it manually. To do so, you need to know the name and the ID of the process. In case of Windows Mobile processes, the ID is the file size in bytes as shown under **Show installed software**. In this case, it is necessary to have a device that lists these processes and retrieve the ID this way.

1. To enter new processes, use the menu to navigate to **Devices** and edit the specific device.
2. Click the **Create new property** button. The **Edit property** dialog is displayed. The syntax must be as in the following example:
 - **Name:** SystemProcess2
 - **Value:** Internet;10008d39,BrowserNG.exe

The name is always “SystemProcess” followed by an index starting at “0”. Spaces are not allowed. When you create another process always use the subsequent index, for example “SystemProcess1”, “SystemProcess2”.

The value is <display name>;<UID of the process>,<name of the process>.

Multiple processes can also be combined, for example <display name>;<UID of the process>,<name of the process>;<UID of the process>,<name of the process>.

We recommend that you change the default display name to a more meaningful name describing the goal of the process state changes. Created processes are shown under **Properties**.

11.4.2 Multiple devices

The device selected in **Base device selection** serves as the process information basis. Only the processes for this device are listed for activation/deactivation. But all devices selected during device/group selection will be affected by the change if they provide the same processes.

In contrast to the single device states function, all states are displayed as unchanged. So by default, no process is changed and the specific settings for each device will be kept. You can select each state separately. If a target device does not have the process to be changed installed, it is not affected by the change.

All processes not selected for activation or deactivation remain in their current state.

12 Configurations

With this module, you can create and transfer setting profiles for Windows Mobile, Android and Apple iPhone/iPad devices.

12.1 Profile templates

With this module you can manage templates for setting profiles. They define the setting options available for the Sophos Mobile Control user. New templates supplied by Sophos have to be uploaded manually by an administrator using the **Create new template** button.

Note: Profile templates are only available for Windows Mobile devices. To create an Apple iPhone/iPad profile, you need to install the Apple iPhone configuration utility.

1. Navigate to **Apple iPhone** in the menu to get a short overview of the functions of the utility.
2. Click the **Profile creation** button to get to the download links and a short description on how to create an Apple iPhone/iPad profile.

12.2 Profiles

This module manages settings profiles for Windows Mobile and Android devices. Apple iPhone/iPad profiles created previously have to be uploaded with this module.

Before creating a new profile, you have to upload at least one profile template. The selected template defines the set of settings available to the Sophos Mobile Control user. You can create any number of different profiles.

Note: Each function has to be applied separately. Settings will be lost, if you do not apply the function. Settings will also be lost, if you do not save them before leaving the **Edit profile** dialog.

Since creating a profile can be time-consuming, created profiles can be duplicated with the **Duplicate this bundle** button. This function is helpful if you need to create several extensive profiles with similar settings. Then only few settings need to be changed.

Note: Profiles can only be duplicated, if you are not editing the profile at the time. Copies are named “Copy of” plus the name of the original, but can be renamed.

12.2.1 Placeholders for profiles

Generic profiles may contain placeholders which are replaced by user data at the time of task execution. The following placeholders can be used in profiles:

ActiveDirectory placeholders:

- `_%EMAILADDRESS_%`
- `_%USERNAME_%`
- `_%PHONENUMBER_%`

Device property placeholder:

`_%DEVPROP(property-name)_%`

This placeholder can for example be used to specify the IMEI of the device: `_%DEVPROP(IMEI)_%`

12.3 Transfer

With this module, you can transfer profiles to specific devices or device groups. The common wizard is used to create the task.

13 Command bundles





13.1 Bundles

With this module, you can combine various commands to command bundles. So you can configure many different functions with only one transfer. This is especially helpful, if many devices are to be configured the same way. Command bundles are only available for Windows Mobile and Android devices. When you create a new bundle, you must select a name, a version, at least one operating system and at least one command.

Note: Improperly used commands may lock or even damage the devices. Therefore only experienced users should use this function. We highly recommend that you test the commands on a single device before you distribute them.

Standard commands are supported on all available platforms. Commands of platform-specific categories are only supported by the specific platforms. The columns AND (Android) and WIN (Windows Mobile) alongside the commands indicate for which platform(s) the commands are available. If various platforms have been selected and a platform-specific command has been added, devices that do not support the specific function refuse the command.

You can set the order of installation for selected commands by using the sort arrows on the right-hand side of the list. The arrows trigger the following actions:

Icon	Description
	Move up one row.
	Move to the top of the list.
	Move down one row.
	Move to the end of the list.

Since creating a command bundle can be time-consuming, finished command bundles can be duplicated with the **Duplicate this bundle** button. This function is helpful, if several extensive command bundles with similar commands need to be created. Then only few commands need to be deleted or added.

Note: Command bundles can only be duplicated, if you are not editing the bundle at the same time. Copies are named “Copy of” plus the name of the original, but can be renamed.

13.2 Parameters for the setConfiguration command

With the command setconfiguration, you set values in the configuration of the Sophos Mobile Control Client. The command offers the following parameters:

Parameter	Description	Value type	Value range	Default	WM	AND
AdminSMS	Administrator SMS phone number for IMSI change.	String			✓	✓
ImsiChangeNotifyDelay	Delay for the check for IMSI change in seconds (-1: off, >=0: on).	Number	-1 - 1800	-1	✓	✓
MaxSyncGap	Automatic sync interval in minutes (0: off)	Number	0 - 2147483647	0	✓	✓

13.3 Transfers

With this module, you can transfer command bundles to specific devices or device groups. The common wizard is used to create the task.

14 Backup

With the **Backup** module you can configure data backups for Android and Windows Mobile devices. The backups handle SMS messages, bookmarks and user defined directory paths. After backups have been created, you can restore data for devices by clicking the **Restore data from backup** button in the **Show device** or **Edit device** view.

14.1 Profiles

You can configure backups by selecting **Profiles** under **Backup** from the Sophos Mobile Control menu.

Under **Edit backup configuration** you specify a **Name** and a **Version** for the new backup configuration and select the operating systems the configuration applies to. To specify a **Schedule** for the backup, select the required weekdays and time.

You can select the following to be backed up:

- SMS
- Bookmarks of system browser
- Paths to backup

14.2 Transfer

With this module, you can transfer backup configurations to specific devices or device groups.

15 Task bundles

With the **Task bundles** module, you can bundle several tasks for mobile devices in one transaction. So you can bundle all tasks necessary to have a device fully registered and running:

- **Provision the device**
- **Apply required policies**
- **Install required applications**

15.1 Bundles

You create a new task bundle by selecting **Bundles** under **Task bundles** from the Sophos Mobile Control menu.

When adding new tasks, you can specify your own meaningful task names for the tasks selected.

You can set the order of installation for selected commands by using the sort arrows on the right-hand side of the list (see **Command bundles**).

Finished task bundles can be duplicated with the **Duplicate this bundle** button.

15.2 Transfer

With this module, you can transfer task bundles to specific devices or device groups.

After you have transferred the task bundle to the relevant devices, the tasks in the bundle are executed in the order you have defined.

16 Traffic counter

In the **Traffic counter** module, the data traffic used for the current and previous month is shown. It gives a rough overview of all devices. Select a specific device to view information about the traffic during the past twelve months or a detailed overview for each day of a specific month. When a device reaches the configured limit, the server sends a short message (text SMS) or a message box including a warning message.

Note: The traffic counter is only available for Windows Mobile and Android devices.

Note: The **Traffic counter** module does not restrict data traffic usage, even if the limit is reached. It only informs the user of the device.

In the **Traffic counter** view, several values are marked in red if traffic appears. This function provides a better overview on wanted and unwanted traffic. Therefore, Wi-Fi traffic is never going to be marked in red. GSM traffic is only marked in red if the limit is exceeded. GSM roaming traffic is going to be marked in red as soon as any traffic appears.

Click on a specific device to show the annual survey. You can restrict traffic counter detail information to specific communication media. You can also set the limit for data traffic use in this dialog.

Select a specific month to display the month chart. It shows the detailed data traffic use for each day.

Note: The Internet Explorer must have an SVG-Viewer plug-in installed to display the chart.

17 The Sophos Mobile Control Self Service Portal

With the Sophos Mobile Control Self Service Portal, end users can register their devices themselves.

Self registration is supported for

- Android
- Apple iOS

Note: As iPads cannot receive SMS messages with installation links, iPad users have to use the Self Service Portal to register their devices and to install the Sophos Mobile Control client.

- Windows Mobile

You can define settings for the Self Service Portal under **Settings** in the tab **Self Service Portal**.

For further information on how to use the Self Service Portal, refer to the *Sophos Mobile Control user guides for Android, Apple iOS and Windows Mobile*.

17.1 Login at the Self Service Portal

The Self Service Portal supports multiple clients and ActiveDirectory (AD) servers. For successful authentication, the Self Service Portal needs to resolve the client and connected ActiveDirectory. The following table shows the options you have here:

Scenario	Customer (Tenant)	AD Server	Explanation
1	1	1	The user login is sufficient to authenticate against the system. The DNS name of the default domain will automatically be extended.
2	1	N	If more AD servers are used, a qualified user name must be given in one of the two options shown here: 1.) <NetBIOS name> \<login name> 2.) <login name>@<DNS name>
3	N	1	For each of the clients a separate group in AD must be available to achieve a unique assignment
4	N	N	If more AD servers are used, a qualified user name must be given in one of the two options shown here: 1.) <NetBIOS name> \<login name> 2.) <login name>@<DNS name>

18 Troubleshooting

Problem	Possible reason	Solution
I cannot log in.	Login data is incorrect.	Check the data and try again.
I cannot register devices.	The Sophos Mobile Control installation does not use a valid license.	Check with your System Administrator whether a valid license has been used for Sophos Mobile Control installation. For further information refer to the section <i>Licenses</i> in the <i>Sophos Mobile Control installation guide</i> .
Item tables are empty.	The filter is too restricted. There are no items that match the criteria.	Edit criteria or reset filter.
Software packages are always installed via sms link (should be silent).	The device is not provisioned. The Sophos Mobile Control client is not installed on the device.	Install Sophos Mobile Control client (“provisioning”).
The provisioning task to install Sophos Mobile Control client stays in state “successful”.	The device has been switched off.	Wait until it is switched on.
	The installation has failed.	Ensure that the correct Sophos Mobile Control client package has been selected for installation.
	The wrong package has been installed.	Delete the task and retry using the correct package.

19 Technical support

You can find technical support for Sophos products in any of these ways:

- Visit the SophosTalk forum at <http://community.sophos.com/> and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at <http://www.sophos.com/support/>.
- Download the product documentation at <http://www.sophos.com/support/docs/>.
- Send an email to support@sophos.com, including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

20 Legal notices

Copyright © 2011 Sophos Ltd. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos is a registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

Powered by DIALOGS Software GmbH