# Contents

1. Glossary .............................................................................................................................................................. 3
2. About Sophos Mobile Control.......................................................................................................................... 4
3. Prerequisites....................................................................................................................................................... 6
4. Login ................................................................................................................................................................... 7
5. Overview ............................................................................................................................................................. 8
6. Common elements........................................................................................................................................... 16
7. Wizards............................................................................................................................................................. 22
8. Task view .......................................................................................................................................................... 23
9. Inventory .......................................................................................................................................................... 26
10. Provisioning ..................................................................................................................................................... 34
11. Applications ................................................................................................................................................... 36
12. Configurations ................................................................................................................................................ 39
13. Command bundles ........................................................................................................................................ 41
14. Backup ........................................................................................................................................................... 43
15. Task bundles ............................................................................................................................................... 44
16. Traffic counter ............................................................................................................................................... 45
17. The Sophos Mobile Control Self Service Portal .......................................................................................... 46
18. Troubleshooting .......................................................................................................................................... 48
19. Technical support .......................................................................................................................................... 49
20. Legal notices ................................................................................................................................................ 50
# Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPRS network</td>
<td>Mobile network for packet-oriented data transmission</td>
</tr>
<tr>
<td>UMTS/3G network</td>
<td>Mobile network for packet-oriented data transmission</td>
</tr>
<tr>
<td>IMEI</td>
<td>International Mobile Equipment Identity, unique serial number of a mobile device</td>
</tr>
<tr>
<td>OTA</td>
<td>Over-The-Air</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service</td>
</tr>
<tr>
<td>APNS</td>
<td>Apple Push Notification Service</td>
</tr>
<tr>
<td>BES</td>
<td>RIM BlackBerry Enterprise Server</td>
</tr>
<tr>
<td>OMA DM</td>
<td>Open Mobile Alliance Device Management</td>
</tr>
<tr>
<td>OMA DS</td>
<td>Open Mobile Alliance Data Synchronization</td>
</tr>
<tr>
<td>MDM</td>
<td>Mobile Device Management</td>
</tr>
<tr>
<td>PDA</td>
<td>Personal Digital Assistant</td>
</tr>
</tbody>
</table>
2 About Sophos Mobile Control

Sophos Mobile Control is a device management solution for mobile devices like smartphones and tablets. 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.

With Sophos Mobile Control you can keep corporate data safe by managing apps and security settings. The Sophos Mobile Control client is easily installed and managed with over-the-air setup and configuration through the Sophos Mobile Control web console. With the Sophos Mobile Control Self Service Portal for your users, you can reduce IT efforts by allowing them to register their own devices and carry out other tasks without having to contact the helpdesk.

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. For a matrix of the features supported for the different platforms, refer to the *Sophos Mobile Control technical guide*.

This administrator guide describes the Sophos Mobile Control administrator web console.
2.1 Terminology

In this manual, the following terms are used:

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

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.

Usually the following roles exist:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Is allowed to perform all actions.</td>
</tr>
<tr>
<td>User</td>
<td>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).</td>
</tr>
<tr>
<td>Helpdesk</td>
<td>This role is intended for support purposes and has the fewest rights (for example installation of software packages), but no access to critical functions.</td>
</tr>
</tbody>
</table>
3 Prerequisites

To use the web console, 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)
- Mozilla Firefox 3.0 (or higher)
- Google Chrome
- Apple Safari

For the web console, JavaScript has to be activated.
4 Login

To log in to the web console:
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 console is granted. If the information is incorrect, an error message is shown and access is denied.

Note: Depending on the password policies defined for your account, the account may be locked after a defined number of failed login attempts. In this case, contact your system administrator.

4.1 Password recovery

If you have forgotten your password for logging in to the Sophos Mobile Control web console, you can reset it to receive a new password.

1. In the Login dialog, click Reset password.
   The Reset password dialog is displayed.
2. Enter your Customer and User information and click Reset.
   You receive an email with a link for resetting your password.
3. Click the link.
   The login dialog is displayed with a message that an email with a new password has been sent to you. This second email contains a randomly generated password.
4. Enter the password to log in.

You are logged in to the Sophos Mobile web console and prompted to change your password.
5 Overview

After login the web console displays the home page with the Dashboard 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.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="filter_inactive.png" alt="Inactive filter" /></td>
<td><strong>Inactive filter</strong> – 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 20).</td>
</tr>
<tr>
<td><img src="filter_active.png" alt="Active filter" /></td>
<td><strong>Active filter</strong> – 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 20).</td>
</tr>
<tr>
<td><img src="home.png" alt="Home" /></td>
<td>The <strong>Home</strong> button opens the homepage with the Dashboard view.</td>
</tr>
<tr>
<td><img src="help.png" alt="Help" /></td>
<td>This button opens a link to the administrator guide as a .pdf.</td>
</tr>
<tr>
<td><img src="logout.png" alt="Logout" /></td>
<td>This button logs off the currently logged in user.</td>
</tr>
</tbody>
</table>
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 Dashboard view

The Dashboard view shows information about the user currently logged in (for example customer, user name and role), the total number of devices, the number of licensed devices and the validity period for licenses.

Above this information, the following buttons are shown:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="gear.png" alt="Settings" /></td>
<td>Opens the Settings dialog.</td>
</tr>
<tr>
<td><img src="lock.png" alt="Change Password" /></td>
<td>Opens the Change password dialog.</td>
</tr>
<tr>
<td><img src="user.png" alt="User Management" /></td>
<td>Opens the user management for managing users of the Sophos Mobile Control web console.</td>
</tr>
</tbody>
</table>
| ![Internal User Management](user.png) | Opens the internal user management for managing Self Service Portal users.  
Note: This button is only displayed for customers, for which the internal user management has been defined. For further information, see Internal user management (page 13). |
| ![Tech Contact](phone.png) | Opens the Technical contact dialog. |
| ![Compliance Settings](gear-check.png) | Opens the Compliance settings dialog. |
| ![Graphical Report](chart.png) | Opens a graphical report on the inventory state. This report shows the following information in pie charts:  
Compliant/non-compliant devices  
Corporate/employee devices  
Device by OS type  
Device by OS version per OS type. |
In addition, a dashboard view of the managed devices is shown:

- **Device Status:**
  Shows the status of registered devices: the number of devices that are compliant/not compliant, managed/not managed, the number of devices with SSP configuration completed/pending/failed and the number of corporate/employee devices.

  For iOS devices, the number of checked out devices is shown. These are devices from which users have manually removed the MDM profile. In this case, the iOS device notifies the MDM server. **Note:** The iOS feature Checkout is supported as of iOS 5.

- **Device 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.

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

  This tab also offers a table for assigning phones to groups and profiles based on the user Active Directory/LDAP membership. In this table, you can define specific SSP configurations for Active Directory groups for users. When a user logs on to the Self Service Portal, the Active Directory groups specified in this table are evaluated from top to bottom for the specific user. If the user belongs to one of the groups, the defined SSP configuration applies.

  Click the **Add** button above the table to add a new group. In the **Edit SSP configuration view**:

  - Enter a **Name** for the SSP configuration group.
  - In the **Directory group** field, enter the Active Directory group. You can use the * wildcard to specify several groups.
  - Under **Platform** select the platforms that should be available in the Self Service Portal.
Under Add to device group, select the group the device should be added to.

Under Task bundle, select the task bundles to be executed.

You can also configure a mobile policy, disclaimer or agreement text to be displayed as a first step when users register their devices. Self Service Portal users have to confirm that they have read this text to be able to continue.

Besides this text, you can define a post install text to be displayed after the automatic installation steps in the Self Service Portal to give the user guidance for the next required steps, for example configuring the server in the iOS app or configuring the Android Mail client. HTML formatting tags are supported for the texts. They will be displayed in the Browser accordingly.

In addition, you can specify the maximum number of devices a user can register through the Self Service Portal. By defining a maximum number here, you can avoid that available licenses are exceeded.

You can also define which functions should be available for users in the Self Service Portal. For example, you may want to disable the wipe function as a lost phone is a major compliance risk and requires additional actions with helpdesk assistance.

- Provisioning via email
  In this tab, you can define an email template for the initial provisioning of devices by email. With initial provisioning by email, devices are registered by sending an email to an account (personal or corporate email account) available on the relevant device instead of SMS. You need to specify an Originator and a Subject. In the text field, you need to predefine the email content. For the download link, you must use the placeholder _DOWNLOAD_LINK_ which will be replaced by the actual link in the email sent to devices.
  For further information, see Provisioning by email (page 34).

- Password Policies
  In this tab, you can define rules for passwords defined or changed for users in Sophos Mobile Control.

  You can define a password change interval, reuse restrictions and a maximum number of failed login attempts. For the passwords themselves, you can define a minimum password length and minimum numbers for letters (lower case and upper case), special characters and digits a password must contain.

  Under Reset password settings, you define the emails to be sent to users after they have requested a password reset. You need to specify an Originator and a Subject. In the text fields, you need to predefine the email content. The placeholders _NEW_PASSWORD_ and _RESET_TOKEN_LINK_ will be replaced by the corresponding values in the emails.

- SSP welcome mail
  In this tab, you define the welcome email to be sent to Self Service Portal users to inform them about their login credentials. You need to specify an Originator and a Subject. In the text field, you need to predefine the email content, including a link (by using the placeholder _RESET_TOKEN_LINK_) for generating a password for the user.
  The placeholders _RESET_TOKEN_LINK_, _LOGINNAME_, _FIRSTNAME_ and _LASTNAME_ will be replaced by the corresponding values in the email.
After you have configured the Self Service Portal welcome email here, the field Send welcome mail is available in the internal user management, see Creating Self Service Portal users with internal user management (page 13).

- **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).

- **RIM BES (BlackBerry Enterprise Server)**
  In this tab, you can specify the BES URL and account configured to be used for Sophos Mobile Control.

### 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 (for users of the Sophos Mobile Control web console)

User management gives you a quick overview of all registered users of the Sophos Mobile Control web console. 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 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, Last name, First name and Email.

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 Internal user management (for users of the Sophos Mobile Control Self Service Portal)

For customers, for which internal management of Self Service Portal users is defined, the Internal user management button is available in the Dashboard. Click it to open internal user management.

Note: Whether a customer uses internal user management or LDAP user management for Self Service Portal users is defined when the customer is created. For further information, see the Sophos Mobile Control super administrator guide.

5.3.4.1 Creating Self Service Portal users with internal user management

1. In the Dashboard view, click the Internal user management button.

2. Click the Create new user button showing a plus sign.
   The Edit user view is displayed.

3. Enter the following information for the new Self Service Portal user:

   - Make sure that the Send welcome mail field is selected.
     This field is available, if you have configured a welcome mail in the SSP welcome mail tab in Settings, see Settings (page 10). If the field is not displayed, configure a welcome mail first.
     The welcome mail has to include all required login credential information.

   - User name
   - Last name
   - First name
   - Email
   - Phone number (optionally).

The new Self Service Portal user is displayed in the Show users view. An email with the Self Service Portal URL and the user credentials is sent to the new user.
5.3.4.2 Importing Self Service Portal users with internal user management

If internal user management is used for a customer, you can add new users by importing a .csv file with up to 300 users.

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.

1. In the Dashboard view, click the Internal user management button.

2. Click the Import users button showing a small arrow symbol pointing downwards. The Import users view is displayed.
   If you do not have a .csv file with users yet, you can download a sample file now and use it for creating your import file.

3. Make sure that the Send welcome mails field is selected.
   This field is available, if you have configured a welcome mail in the SSP welcome mail tab in Settings, see Settings (page 10). If the field is not displayed, configure a welcome mail first. The welcome mail has to include all required login credential information.

4. 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.

5. If all entries are correct, click the blue Finish button.

5.3.5 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, Email, Phone number and Mobile number.

In the text field Additional information, you can enter any additional information required.

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

5.3.6 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.

You can define the following compliance settings for rules:

- **Min. client version**: Enter the minimum Sophos Mobile Control client version required.
- **Allow jailbreak** (iOS): Yes/No
- **Allow root rights** (Android): Yes/No
- **Passcode required** (iOS): Yes/No
- **Allow non-market apps** (Android): Yes/No. If users change this setting on devices, they are no longer compliant.
- **Allow debug bridge** (ADB) (Android): 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.
- **Data roaming allowed** (Android, iOS): Yes/No
- **Blacklisted apps/Whitelisted apps**: By using this field, you can allow or disallow apps on devices. Select **Blacklisted apps** and click **Edit**, to define a list of apps that users must not install on devices. Select **Whitelisted apps** and click **Edit**, to define a list of user-installed apps that users may install on devices.

To add an app to the list, click the **Add** button and enter the **App name** and the **App identifier** in the **Edit App** view.

**Note**: If you use whitelisted apps, only the ones on the list can be installed on the device. All other apps are not allowed.

- **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 Active Sync** in case of non-compliance. If the device does not comply with the rule, email access will automatically be denied.

For each option you can define the action **Notify admin** to get notified by email, if devices are no longer compliant. For notification by email, specify the relevant recipients in **Admin mail recipients** and define a notification schedule under **Admin mail timetable**. The email sent to the defined recipients at the specified time contains all devices that no longer comply with the rule for which the **Notify admin** check box has been selected.

For each option, you can select a task bundle that will be automatically executed, if a device no longer complies with the relevant rule. For example, you can create a task bundle that will automatically apply a profile with a number of restrictions, if a device is no longer compliant. Select the task bundle from the **Transfer task bundle** dropdown list next to the compliance rule options.

**Note**: The task bundle must be created under **Task bundles > Bundles** first. For further information, see **Task bundles** (page 44).

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

For Android and iOS devices, a notification is sent to the device user if their device is no longer compliant.

For further information, see the *Sophos Mobile Control user guides for Android and Apple iOS*.
6 Common elements

6.1 Buttons

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

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="#" alt="Next arrow" /></td>
<td>Navigates to the next view of a wizard.</td>
</tr>
<tr>
<td><img src="#" alt="Back arrow" /></td>
<td>Navigates to the last view of a wizard.</td>
</tr>
<tr>
<td><img src="#" alt="Information icon" /></td>
<td>Provides further information on a specific topic.</td>
</tr>
<tr>
<td><img src="#" alt="Duplicate icon" /></td>
<td>Duplicates a profile/command bundle.</td>
</tr>
<tr>
<td><img src="#" alt="Confirmation icon" /></td>
<td>Confirms an action.</td>
</tr>
<tr>
<td><img src="#" alt="Cancel icon" /></td>
<td>Cancels an action.</td>
</tr>
<tr>
<td><img src="#" alt="Select device group" /></td>
<td>Switches to the Select device group(s) view.</td>
</tr>
<tr>
<td><img src="#" alt="Select device" /></td>
<td>Switches to the Select device(s) view.</td>
</tr>
<tr>
<td><img src="#" alt="Finish wizard" /></td>
<td>Finishes a wizard and executes an action.</td>
</tr>
<tr>
<td><img src="#" alt="Change settings" /></td>
<td>Enables you to change settings or information.</td>
</tr>
<tr>
<td><img src="#" alt="Save settings" /></td>
<td>Saves changed settings.</td>
</tr>
<tr>
<td><img src="#" alt="Reload table" /></td>
<td>Reloads the content of a table.</td>
</tr>
<tr>
<td><img src="#" alt="Add entry" /></td>
<td>Adds an entry.</td>
</tr>
<tr>
<td><img src="#" alt="Delete entry" /></td>
<td>Deletes a selected entry.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;</td>
<td>Jump to first page.</td>
</tr>
<tr>
<td>&lt;&lt;</td>
<td>Jump back five pages.</td>
</tr>
<tr>
<td>&lt;</td>
<td>Jump back one page.</td>
</tr>
<tr>
<td>1 2 3 4 5 6</td>
<td>Jump to a specific page.</td>
</tr>
<tr>
<td>&gt;</td>
<td>Jump forward one page.</td>
</tr>
<tr>
<td>&gt;&gt;</td>
<td>Jump forward five pages.</td>
</tr>
<tr>
<td>&gt;</td>
<td>Jump to the last page.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>Activated process</td>
</tr>
<tr>
<td></td>
<td>Leave process unchanged</td>
</tr>
<tr>
<td>❌</td>
<td>Deactivated process</td>
</tr>
</tbody>
</table>

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 console 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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Filtering device names/parts of device names.</td>
</tr>
<tr>
<td>IMEI</td>
<td>Filtering IMEI.</td>
</tr>
<tr>
<td>Phone number</td>
<td>Filtering phone number.</td>
</tr>
<tr>
<td>Managed</td>
<td>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.</td>
</tr>
<tr>
<td>Compliant</td>
<td>Filtering according to compliance.</td>
</tr>
<tr>
<td>Device wiped</td>
<td>Filtering wiped or non-wiped devices.</td>
</tr>
<tr>
<td>Package</td>
<td>Filtering software packages/parts of software packages. You can use wildcards for both fields.</td>
</tr>
<tr>
<td>Device group</td>
<td>Device groups whose members are not to be displayed can be deactivated.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Devices which are equipped with a certain operating system can be deactivated.</td>
</tr>
<tr>
<td>Device property</td>
<td>Filtering a specific device property</td>
</tr>
</tbody>
</table>
6.3.2 Device group filter

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Filters by name of the device group.</td>
</tr>
</tbody>
</table>

6.3.3 Software filter

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Filters by name of the package</td>
</tr>
<tr>
<td>Version</td>
<td>Filters by version of the package</td>
</tr>
<tr>
<td>Operating System</td>
<td>Packages which are applicable for certain operating systems can be filtered by selecting the check box next to the operating systems.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Filters by device name.</td>
</tr>
<tr>
<td>Package</td>
<td>Filters by package name.</td>
</tr>
<tr>
<td>State</td>
<td>Tasks in a specific state can be deactivated. The states are grouped in five groups for easier handling.</td>
</tr>
<tr>
<td>Group</td>
<td>Device groups whose members are not to be displayed can be deactivated.</td>
</tr>
</tbody>
</table>
7 Wizards

The concept of wizards guiding through task creation is a common feature in the web console. 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 console 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:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄</td>
<td>Installation</td>
</tr>
<tr>
<td>🔄 tà</td>
<td>Uninstallation</td>
</tr>
<tr>
<td>🔄 ✓</td>
<td>Process activation/deactivation</td>
</tr>
<tr>
<td>🔄 ✓</td>
<td>Explicit refresh of device data</td>
</tr>
<tr>
<td>📩</td>
<td>Text SMS</td>
</tr>
<tr>
<td>📲</td>
<td>Windows Mobile profile transfer</td>
</tr>
<tr>
<td>📲</td>
<td>iOS profile transfer</td>
</tr>
<tr>
<td>📲</td>
<td>Command bundle transfer</td>
</tr>
<tr>
<td>📲</td>
<td>Bootstrap</td>
</tr>
<tr>
<td>📲</td>
<td>Command transfer</td>
</tr>
<tr>
<td>📲</td>
<td>Windows Mobile security settings</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accepted</td>
<td>The task has been created.</td>
</tr>
<tr>
<td>Retry</td>
<td>The task will be retried later.</td>
</tr>
<tr>
<td>Started</td>
<td>The task has been started.</td>
</tr>
<tr>
<td>In progress</td>
<td>The execution of the task is being prepared.</td>
</tr>
<tr>
<td>Sending notification</td>
<td>The client is being notified.</td>
</tr>
<tr>
<td>Waiting for delivery</td>
<td>The server is waiting for a confirmation of the notification by the client.</td>
</tr>
<tr>
<td>Notified</td>
<td>The client has received the notification.</td>
</tr>
<tr>
<td>Exported</td>
<td>The client has received the package and/or the commands.</td>
</tr>
<tr>
<td>Result evaluation started</td>
<td>The client has answered and the evaluation of the result has been started.</td>
</tr>
<tr>
<td>Result incomplete</td>
<td>The result evaluation showed that not all commands’ results have been received by now.</td>
</tr>
</tbody>
</table>
| 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.                                                       |

*Note:* You can manually retry a task in case it failed by clicking the **Execute now** button in the **Task history**. This is only possible for tasks that have not failed completely.
8.2 Task history

In the Task view, the magnifier icon besides a task 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.

To manually retry failed tasks, click the Execute Now button available for failed tasks in this view.

Note: This is only possible for tasks that have not failed completely.
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.

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 email you can also enter an email address. You can define the email to be sent under Settings. For further information, see Provisioning by email (page 34).

4. In the Owner field, select Corporate device or Employee device.
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.

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

2. In the message displayed, select the data source **CSV file**.
   The **Import devices** view is displayed.
   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.

3. 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.

4. 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** view 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 **Email**.

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 report takes any filters currently set into consideration. If the report does not contain the expected results, check the current filters.

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. At the top of the view the following information is shown: Name, Description, Device group, Phone number, Owner (corporate device or employee device), Email address (for Android and iOS devices), Operating system, Device ID and Last synchronization. For iOS devices, the Last iOS App synchronization 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.

The Show device/Edit device view offers a number of buttons for administrating devices. Below the buttons, the following tabs show detailed device information:

- **Device properties**
  Shows device properties, for example properties for model, model name, OS version.
  For Android devices, rooted smartphones are detected and the relevant property is shown.
  For Apple iOS devices, jailbroken smartphones are detected and the relevant property is shown.

- **Custom properties**
  Shows the custom properties. These are properties you can create yourself. Custom properties can for example be used in placeholders if no Active Directory connection is available. You can also add user-specific information here.

- **Internal properties**
  Shows internal device properties, for example ActiveSync traffic allowed, IMEI.
- **Compliance violations**
  This tab is only displayed for non-compliant devices. It shows the compliance violations of the non-compliant device.
  Click the **Show** (magnifier) icon next to a compliance violation to view the violation **History**.
  Click the **Edit** icon in the Compliance violations tab or the **Add new action** icon in the History view 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 email.

- **Installed Software**
  Shows the software installed on the device.

  For Apple iOS devices, the **Managed** column in the Installed software tab indicates managed apps.
  Managed apps are a new functionality introduced with iOS 5.0. With Sophos Mobile Control you can push such apps to iOS devices and also silently remove them.

  **Note:** Sophos Mobile Control supports the managed apps functionality as of iOS 5.1.

  For Android devices, Sophos Mobile Control differentiates between system apps and apps that the user has installed on the device.

  For Android devices, the data size used by the individual apps on the device is shown.

  For iOS devices, the space used by an app after installation is shown as well as additional space that may be required for downloads, configuration, or settings and the like.

  In this tab, an **Install app** button is available in the upper corner on the left. With this button you can install software on the device. You can also remove managed apps from the device by clicking the **Delete** icon displayed next to the relevant app.

- **Installed profiles (iOS)**
  Shows the profiles installed on iOS devices.

  In this tab, an **Install profile** button is available. With this button you can install software on the device. You can also remove profiles from the device by clicking the **Delete** icon displayed next to the relevant profile.

  This tab also lists provisioning profiles.

- **System software (Android)**
  Shows Android system software on the device.

- **Certificates (iOS)**
  Shows the certificates in use on the iOS device.
### 9.1.5.1 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.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Button" /></td>
<td>Click this button to set the name and the IMEI of the specific device in the Device filter.</td>
</tr>
<tr>
<td><img src="image" alt="Button" /></td>
<td>Shows the installed software packages, version numbers and processes.</td>
</tr>
<tr>
<td><img src="image" alt="Button" /></td>
<td>Shows the installed profiles. In this dialog, you can also delete profiles.</td>
</tr>
<tr>
<td><img src="image" alt="Button" /></td>
<td>Use this button to add an ActiveDirectory link to the device.</td>
</tr>
<tr>
<td><img src="image" alt="Button" /></td>
<td>Use this button to remove an ActiveDirectory link to the device.</td>
</tr>
<tr>
<td><img src="image" alt="Button" /></td>
<td>Use this button to refresh the data.</td>
</tr>
<tr>
<td><img src="image" alt="Button" /></td>
<td>Opens the traffic counter details for the device.</td>
</tr>
</tbody>
</table>
| ![Button](image) | Indicates that email access is denied. An additional icon on the button indicates whether email access was denied:  
  - manually 👎 or  
  - automatically ⏳.  
If you click this button, a window opens where you can allow email access or set it to automatic mode. |
| ![Button](image) | Indicates that email access is allowed. An additional icon on the button indicates whether email access was allowed:  
  - manually 👍 or  
  - automatically ⏳.  
If you click this button, a window opens where you can deny email access or set it to automatic mode. |
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:

- 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.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="lock" /></td>
<td>Locks the device remotely.</td>
</tr>
<tr>
<td><img src="image" alt="unlock" /></td>
<td>Unlocks the device remotely.</td>
</tr>
<tr>
<td><img src="image" alt="reset" /></td>
<td>Use this button to reset the passcode/password of a device.</td>
</tr>
<tr>
<td><img src="image" alt="delete" /></td>
<td>Deletes all synchronization data of the device. Sophos Mobile Control client needs to be reinstalled.</td>
</tr>
<tr>
<td><img src="image" alt="sms" /></td>
<td>Use this button to send a text SMS message to a specific device.</td>
</tr>
<tr>
<td><img src="image" alt="locate" /></td>
<td>Use this button to locate a device.</td>
</tr>
<tr>
<td><img src="image" alt="backup" /></td>
<td>Restores the data for the device from backup.</td>
</tr>
<tr>
<td><img src="image" alt="delete" /></td>
<td>Use this button to delete the device.</td>
</tr>
<tr>
<td><img src="image" alt="tasks" /></td>
<td>Use this button to display all tasks for this device.</td>
</tr>
</tbody>
</table>
This button is available for devices where the registration through the Self Service Portal has failed. With this button you can reset the SSP registration failed status after you have fixed the relevant issues.

**Note:** Use this button only, if you are sure that the device will nevertheless synchronize with the Sophos Mobile Control Server.

Use this button to decommission an iOS or Android device, see *Decommissioning Android and iOS devices* (page 32).

**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.

### 9.1.6 Decommissioning Android and iOS devices

You can decommission managed Android and iOS devices that will no longer be used, for example if a user leaves the company or gets a new device.

To decommission a device, click the **Device decommissioning** button in the **Show device/Edit device** view of the relevant device.

This results in the following:

**Android devices:**
- The Sophos Mobile Control Client device administrator is disabled.
- The server login data and all other data received from the server are removed.

**iOS devices:**
- All profiles are removed.
- All managed apps are removed (from iOS 5.1).
- The Sophos Mobile Control iOS client app is removed, if it was installed through managed apps (from iOS 5.1).
- All certificates are removed.
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.

10.3 Provisioning by email

Android and Apple iOS devices can be initially provisioned by email instead of SMS. This provisioning method can be used for devices which do not support SMS, for example iPads.

Prerequisites:

- A mail server needs to be configured during Sophos Mobile Control installation. For further details, see the Sophos Mobile Control installation guide.
- An email account (personal or corporate email account) needs to be available on the devices to be provisioned
- The email addresses must be specified when the devices are added to Sophos Mobile Control manually or by import.

Note: For provisioning by email, the device phone number must be 0.
For provisioning, an email configured in the admin user interface is sent to the specified email accounts.

You can configure the email to be sent under Settings in the Provisioning via email tab. In this tab, you specify Originator, Subject and the email content. For download and configuration links, the placeholders _DOWNLOADLINK_ and _CONFIG_LINK_ are available. They are obligatory and are replaced by the actual link in the email sent to devices. In addition, the placeholders _DEVICENAME_ and _DEVICEDESCRIPTION_ are available.
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”, “apk” or “ipa”).

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.

Once you have uploaded a software package to the system, you can download it again to check it, so you do not need to manage the files separately. To download a software package, click the Edit icon in the Software Packages view and click the Download icon next to the software package in the Edit package view.

If you want to delete a software package, you must first delete all active tasks referencing it. To delete a software package, click the Delete icon next to the relevant package in the Software Packages view.

Note: A software package cannot be deleted if it was inherited from the super administrator. For further information, see the Sophos Mobile Control super administrator guide.

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.

Once you have uploaded a profile for an iOS device to the system, you can download it again to check it, so you do not need to manage the files separately. To download a profile for an iOS device, click the Edit icon in the Apple iOS Profiles view and click the Download icon next to the profile in the Edit profile view.
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:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄️</td>
<td>Move up one row.</td>
</tr>
<tr>
<td>🔄️</td>
<td>Move to the top of the list.</td>
</tr>
<tr>
<td>🔄️</td>
<td>Move down one row.</td>
</tr>
<tr>
<td>🔄️</td>
<td>Move to the end of the list.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value type</th>
<th>Value range</th>
<th>Default</th>
<th>WM</th>
<th>AND</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdminSMS</td>
<td>Administrator SMS phone number for IMSI change.</td>
<td>String</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ImsiChange</td>
<td>Delay for the check for IMSI change in seconds (-1: off, &gt;=0: on).</td>
<td>Number</td>
<td>-1 - 1800</td>
<td>-1</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>MaxSyncGap</td>
<td>Automatic sync interval in minutes (0: off)</td>
<td>Number</td>
<td>0 - 2147483647</td>
<td>0</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

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.

Note: Backups are platform-specific.

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 (for example managed apps for iOS devices)

You can also include wipe commands in task bundles to automatically wipe non-compliant (for example jailbroken or rooted) devices.

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 (page 41).

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.
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. Users have to open their Browser on the device, enter the Self Service Portal URL there and register their device with the Sophos Mobile Control system.

- 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:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Customer (Tenant)</th>
<th>AD Server</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>The user login is sufficient to authenticate against the system. The DNS name of the default domain will automatically be extended. The customer for which the AD has been configured has to be specified. <em>Note:</em> This is only possible if the setting of the default domain has been configured accordingly during setup.</td>
</tr>
<tr>
<td>2</td>
<td>N</td>
<td>1</td>
<td>For each of the clients a separate group in AD must be available to achieve a unique assignment</td>
</tr>
<tr>
<td>3</td>
<td>N</td>
<td>N</td>
<td>If more AD servers are used, a qualified user name must be given in one of the two options shown here: 1.) <code>&lt;NetBIOS name&gt; \&lt;login name&gt;</code> 2.) <code>&lt;login name&gt;@&lt;DNS name&gt;</code> <em>Note:</em> The domain only has to be specified, if no SSP login template has been defined during configuration.</td>
</tr>
</tbody>
</table>
## Troubleshooting

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible reason</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>I cannot log in.</td>
<td>Login data is incorrect.</td>
<td>Check the data and try again.</td>
</tr>
<tr>
<td>I cannot register devices.</td>
<td>The Sophos Mobile Control installation does not use a valid license.</td>
<td>Check with your System Administrator whether a valid license has been used for Sophos Mobile Control installation. For further information refer to the section <em>Licenses</em> in the <em>Sophos Mobile Control installation guide</em>.</td>
</tr>
<tr>
<td>Item tables are empty.</td>
<td>The filter is too restricted. There are no items that match the criteria.</td>
<td>Edit criteria or reset filter.</td>
</tr>
<tr>
<td>The provisioning task to install Sophos Mobile Control client stays in state “successful”.</td>
<td>The device has been switched off.</td>
<td>Wait until it is switched on.</td>
</tr>
<tr>
<td></td>
<td>The installation has failed.</td>
<td>Ensure that the correct Sophos Mobile Control client package has been selected for installation.</td>
</tr>
<tr>
<td></td>
<td>The wrong package has been installed.</td>
<td>Delete the task and retry using the correct package.</td>
</tr>
</tbody>
</table>
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 – 2012 Sophos Group. 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.