<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>Managing Sophos Mobile Security from Sophos Mobile Control</td>
<td>109</td>
</tr>
<tr>
<td>27</td>
<td>Appendix: Common web console buttons</td>
<td>114</td>
</tr>
<tr>
<td>28</td>
<td>Technical support</td>
<td>116</td>
</tr>
<tr>
<td>29</td>
<td>Legal notices</td>
<td>117</td>
</tr>
</tbody>
</table>
1 About Sophos Mobile Control

Sophos Mobile Control is a device management solution for mobile devices like smartphones and tablets. Sophos Mobile Control helps to keep corporate data safe by managing apps and security settings. 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 text messages.

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 selected functions are supported. 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.

1.1 Sophos Mobile Control on premise and as a Service

We offer two delivery models for Sophos Mobile Control:

- **Sophos Mobile Control for on-premise installation**

  With an on-premise installation, you keep all your data in-house on your own server. It caters for a large number of users and offers extended device management features, for example:

  - Management of access to corporate email
  - Use of your directory to automatically assign devices to your existing groups
  - Customer management with the super administrator customer, see the Sophos Mobile Control super administrator guide
  - BlackBerry support (through BlackBerry Enterprise Server) in addition to device management for iOS, Android and Windows Mobile
Configuration of backups for Android and Windows Mobile devices

Sophos Mobile Control as a Service

For our software as a Service version, no hardware is necessary on your part. Sophos Mobile Control is not installed on site. Sophos Mobile Control as a Service is the ideal choice in case of restricted IT resources. No resources are required for installing and maintaining Sophos Mobile Control. As with an on-premise installation, an administrator manages devices through the web console. With Sophos Mobile Control as a Service you can get smaller groups of users up and running in no time.

Differences between on-premise installations and Sophos Mobile Control as a Service are marked in this guide.

1.2 About this guide

This guide describes how to use the Sophos Mobile Control administration web console.

For a description of Sophos Mobile Control installation, see the Sophos Mobile Control installation guide.

Note: The installation procedure described in this guide is not relevant for Sophos Mobile Control as a Service.

For information on how to use the Sophos Mobile Control web console as a super administrator for customer management, see the Sophos Mobile Control super administrator guide.

Note: This guide is not relevant for Sophos Mobile Control as a Service. Super administrators are not supported for Sophos Mobile Control as a Service.

For a description of the key steps for initial configuration, see the Sophos Mobile Control and Sophos Mobile Control as a Service startup guides.

For information on the Sophos Mobile Control Self Service Portal, see the Sophos Mobile Control user guides for Android, Apple iOS and Windows Mobile.

1.2.1 Terminology

In this guide, the following terms are used:

<table>
<thead>
<tr>
<th>Term</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>The mobile device to be managed (for example smartphone or tablet).</td>
</tr>
<tr>
<td>Sophos Mobile Control client</td>
<td>The Sophos Mobile Control client component that is installed on the device.</td>
</tr>
<tr>
<td>Term</td>
<td>Explanation</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</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 that is used to manage devices.</td>
</tr>
<tr>
<td>Customer</td>
<td>The tenant that manages devices.</td>
</tr>
<tr>
<td>Provisioning</td>
<td>The process of equipping devices with the Sophos Mobile Control client.</td>
</tr>
<tr>
<td>Self Service Portal (SSP)</td>
<td>The Sophos Mobile Control web interface that allows end users to register their own devices and carry out other tasks without having to contact the helpdesk.</td>
</tr>
<tr>
<td>Sophos Mobile Security</td>
<td>A security app for Android phones and tablets that can be managed from Sophos Mobile Control. The Sophos Mobile Security management functionality is an optional Sophos Mobile Control module. For managing the Sophos Mobile Security app from Sophos Mobile Control, a license needs to be available and activated in the Sophos Mobile Control web console.</td>
</tr>
<tr>
<td>SMSec</td>
<td>Abbreviation for Sophos Mobile Security used in the Sophos Mobile Control web console user interface.</td>
</tr>
</tbody>
</table>
2 About the Sophos Mobile Control web console

The Sophos Mobile Control web console is the central instrument for managing devices with Sophos Mobile Control. It is the web interface of the server used for device management. With the web console you can implement a corporate policy for the use of mobile devices and apply it to the devices registered with Sophos Mobile Control.

Note: Due to the nature of different mobile device operating systems supported features vary. For a matrix of the features for the different device types, refer to the Sophos Mobile Control technical guide.

In the Sophos Mobile Control web console you can:

- Configure the system
- Register devices with Sophos Mobile Control
- Provision new devices
- Install software packages on registered devices
- Define configurations (profiles) and security policies for devices
- Create task bundles to bundle several tasks for mobile devices and transfer them in one transaction
- Define custom Sophos Mobile Control client command bundles to be transferred to devices in a single task
- Carry out administrative tasks on devices, for example reset the passcode of devices, lock or wipe devices if they are lost or stolen, decommission devices
- Configure data backups for Android and Windows Mobile devices
  
  Note: Backups are not supported for Sophos Mobile Control as a Service.

- Create and view reports and monitor the data traffic of devices
- Send messages to devices

2.1 Prerequisites

The following prerequisites apply for using the Sophos Mobile Control web console:

- You need a computer connected to the internet and equipped with a web browser. For information on supported browsers and the relevant versions, refer to the Sophos Mobile Control release notes.

- A customer (a tenant whose devices are managed in Sophos Mobile Control) needs to be available in the web console. Customers are created by super administrators. For further information, see the Sophos Mobile Control super administrator guide.
**Note:** For Sophos Mobile Control as a Service, a customer is predefined. Super administrators are not supported for Sophos Mobile Control as a Service.

- You need a Sophos Mobile Control user account and the relevant credentials for logging in to the web console. The credentials consist of customer, user and password. For further information, see *First login* (section 4.1).

## 2.2 User roles

The users of the web console can have different user roles. You can assign these roles when you create new users in the web console, see *Create new web console users* (section 7).

The modules/functions available in the web console depend on the user role.

You can assign the following user roles:

<table>
<thead>
<tr>
<th>User role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Has the rights to perform all available actions.</td>
</tr>
<tr>
<td>User</td>
<td>Is allowed to perform all actions required for installing and administrating a device, but cannot specify essential settings (for example modify a client package or a template).</td>
</tr>
<tr>
<td>Helpdesk</td>
<td>This role is intended for support purposes. It has only limited rights (for example installation of software packages). This role does not have access to critical functions, for example defining settings and creating, deleting or editing devices/device groups, packages and profiles.</td>
</tr>
</tbody>
</table>

If you require further user roles, please contact Sophos Support.
3 Key steps for managing devices with the web console

Sophos Mobile Control offers a wide range of Mobile Device Management functions depending on mobile device types, corporate security policies and specific requirements in your company. The key steps for managing mobile devices with Sophos Mobile Control are:

- Configure platform-specific settings.
- Configure compliance settings for devices in the web console.
- Configure provisioning by email for devices that do not support text messages, for example iPads.
- Create device groups.
  Device groups are used to categorize devices. They make administration easier as in most device management functions you can select a complete group or single devices.
- Register and provision devices.
  Devices can either be registered and provisioned by administrators through the web console or by device end users through the Self Service Portal. You can configure settings for the Self Service Portal and manage Self Service Portal users in the web console.
- Set up configurations and security settings for devices in the web console.
- Create task bundles for Self Service Portal configuration.
- Configure Self Service Portal use for end users.
- Apply new or updated configurations and security settings to registered devices.
4 Login to the Sophos Mobile Control web console

4.1 First login

**Prerequisite:** A user account has been created for you in the Sophos Mobile Control web console and you have the user credentials (customer, user and one-time password) for this account. The user account may have been created by the super administrator during Sophos Mobile Control installation or by another administrator user of the web console. For further information on the super administrator, refer to the Sophos Mobile Control super administrator guide. For further information on how to create new web console users, see Create new web console users (section 7).

**Note:** Super administrators are not supported for Sophos Mobile Control as a Service. For further information on first login for Sophos Mobile Control as a Service, see the Sophos Mobile Control as a Service startup guide.

1. Open the web console.
   
   The web console login dialog is displayed.

2. Enter your **Customer**, **User** name and the one-time **Password** and click **Login**.

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

3. Enter a new password, confirm it and click the **Save** button.

   A message confirms that the changes have been saved. You can now use the new password for login.

4.2 Login

1. Open the web console.
   
   The web console login dialog is displayed.

2. Enter your **Customer**, **User** name and **Password** and click **Login**.

   You are logged in to the web console. The **Dashboard** of the customer you are logged in to is displayed.
### 4.3 Password recovery

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

1. In the **Login** dialog of the web console, click **Forgot 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 web console and prompted to change your password.

### 4.4 Logout

To log out from the web console, click the blue **Logout** button in the header.
5 The web console user interface

The web console user interface consists of the header on top, the menu bar at the left-hand side and the relevant view in the center:

■ Header

In the header, the following buttons are available.

Note: Hover over the button with your mouse pointer to display a tooltip with the button name or further information.

<table>
<thead>
<tr>
<th>Button</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
|       |      | Opens the filter function. With the filter function you can restrict the number of items shown in lists. Different filters are available depending on the view you open the filter function from. Available filters are: device filter, device group filter, software filter and task filter. For further information, see Filters (section 5.3).
|       | Filter | Note: This button is only shown, if a view can be filtered. |
|       | Reset  | This button is displayed after you have set a filter. It resets an active filter. |
|       | Home   | Opens the homepage with the Dashboard view. |
|       | Help   | Opens a link to the Sophos Mobile Control documentation web page. On this page, all manuals for Sophos Mobile Control are available. |
|       | Logout | Logs off the currently logged in user. |

■ Menu bar

The menu bar on the left-hand side of the user interface shows all available Sophos Mobile Control modules (for example Inventory) and their functions (for example Devices under Inventory). Use the menu bar to navigate between modules and functions. Click a module to open a view showing the module functions with a short description. Click a function to open it directly.

■ View
The view of the web console changes depending on the module and function you are working with. When you log in to the web console, the Dashboard view for the customer you have logged in to is displayed. For further information, see Using the Dashboard (section 6).

**Note:** The functions, modules and buttons available on the web console user interface depend on the role of the logged in user, see User roles (section 2.2). For super administrators, the web console shows a specific view for the super administrator customer. For further information, see the Sophos Mobile Control super administrator guide. Super administrators are not supported for Sophos Mobile Control as a Service.

## 5.1 Tables

The web console user interface is for the most part based on tables with items you can carry out administrative tasks on. To make these tables easier to use, all items shown are by default grouped into 20 items per page. You can change this setting according to your requirements, see Configure personal settings (section 9).

You can browse the table pages with the controls shown below the 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.

In most tables you can carry out actions regarding the listed items by using the action icons shown next to them. The icons shown depend on the selected table and, in some cases, also on the status of the relevant item.

The action icons trigger the following actions:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Show details" /></td>
<td>Show details of this item.</td>
</tr>
<tr>
<td><img src="image" alt="Edit" /></td>
<td>Edit this item.</td>
</tr>
<tr>
<td><img src="image" alt="Delete" /></td>
<td>Delete this item.</td>
</tr>
<tr>
<td><img src="image" alt="Download" /></td>
<td>This icon is shown for software packages. Click it to download the software package from the web console, see Download uploaded software packages (section 16.2.1).</td>
</tr>
</tbody>
</table>

## 5.2 Buttons

Throughout the web console a number of common function buttons are used. Hover over the button with your mouse pointer to display a tooltip with the button name or further information. In this administrator guide, the button names shown in the tooltips are used. For an illustrated
list of all function buttons with their button names, see Appendix: Common web console buttons (section 27).

5.3 Filters

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

■ Device filter, see Use the device filter (section 21.2.1).
■ Device group filter, see Use the device group filter (section 21.2.2).
■ Software filter, see Use the software filter (section 16.6)
■ Task filter, see Use the task filter (section 22.3).

The filter is not only valid for the function currently displayed, but for all functions where items of this type are listed.

Note: Remember to reset filters manually when they are no longer needed. Otherwise lists or reports may not include the results you expect.
6 Using the Dashboard

The Dashboard is the initial view that is displayed when you log in to the web console. The Dashboard gives you an overview on the customer you have logged in to and the devices registered for this customer. It also provides direct access to the devices. In addition, a number of function buttons are available on the Dashboard.

To return to the Dashboard view from other views, click the Home button in the web console header.

6.1 Using the Dashboard buttons

The Dashboard offers a number of function buttons for accessing important management functions. If you hover your mouse pointer over the button, a tooltip with the button name is displayed.

- **Settings**
  
  Click this button to define a number of settings for the use of Sophos Mobile Control, for example personal settings, password policies, or Self Service Portal settings.

- **Change password**
  
  Click this button to change your password for logging in to the web console.

- **User management**
  
  Click this button to manage the users of the Sophos Mobile Control web console. For further information, see Create new web console users (section 7).

- **Internal user management**
  
  **Note:** This button is only available for customers for which internal management of Self Service Portal users has been configured. Whether a customer uses internal user management or LDAP user management for Self Service Portal users is defined for on-premise installations when the customer is created. For further information on how to create customers for Sophos Mobile Control on-premise installations, see the Sophos Mobile Control super administrator guide. Super administrators are not supported for Sophos Mobile Control as a Service. For Sophos Mobile Control as a Service, customers are predefined and internal user management is used. Click this button to manage the users of the Sophos Mobile Control Self Service Portal. For further information, see Manage Self Service Portal users (section 20.3).

- **Technical contact**
  
  Click this button to display the technical contact information. This information refers to IT staff who can be contacted if there are any questions or problems. Users with the role
Administrator can edit the technical contact information. For further information, see Configure technical contact (section 8).

- **Device compliance criteria**
  Click this button to configure compliance checks for devices. For further information, see Configure compliance settings (section 12).

- **Reports**
  Click this button to open a graphical report on the inventory state. For further information, see Create graphical overview report on devices (section 23.1).

### 6.2 Information shown on the Dashboard

The Dashboard shows the following information:

- The customer the user has logged in to
- The currently logged in user with the user role (for example Administrator)
- The number of registered devices
- The number of licensed devices
- The license expiry date
- If a Sophos Mobile Security license is available for the relevant customer, a second line with license information for Sophos Mobile Security is shown. Sophos Mobile Security management is an optional module of Sophos Mobile Control. For further information, see Managing Sophos Mobile Security from Sophos Mobile Control (section 26).

In addition, information about the registered devices is shown in three areas:

- **Device status**
  Shows the status of registered devices:

<table>
<thead>
<tr>
<th>Line</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant</td>
<td>Shows the number of devices that comply with the current compliance settings.</td>
</tr>
<tr>
<td>Not compliant</td>
<td>Shows the number of devices that do not comply with the current compliance settings.</td>
</tr>
<tr>
<td>Managed</td>
<td>Shows the number of devices currently managed by Sophos Mobile Control.</td>
</tr>
<tr>
<td>Not managed</td>
<td>Shows the number of devices that are currently registered with, but not managed by Sophos Mobile Control.</td>
</tr>
<tr>
<td>Line</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Checked out** (iOS devices only)       | Shows the number of iOS devices where users have manually removed the Mobile Device Management profile. In this case the iOS device tries to notify the server.  
**Note:** The iOS feature "Checkout" is supported as of iOS 5. |
| **SSP configuration completed**          | Shows the number of devices for which configuration through the Self Service Portal has been completed. With the Self Service Portal end users can register their devices themselves. For further information on how to configure settings for Self Service Portal use, see *Configure Self Service Portal settings* (section 20.2). |
| **SSP configuration pending**            | Shows the number of devices for which the configuration through the Self Service Portal is pending. |
| **SSP configuration failed**              | Shows the number of devices for which the configuration through the Self Service Portal has failed. |
| **Corporate devices**                    | Shows the number of corporate devices registered. |
| **Private devices**                      | Shows the number of private devices registered. |

- **Platforms**
  
  Shows the number of devices for each operating system.

- **Device groups**
  
  Shows the available device groups with the number of devices they contain.

In the three device areas, you can click on a table row to open the device list filtered to the relevant item. So you can access registered devices in the different categories directly from the **Dashboard**.

**Note:** Remember to reset the filter manually when it is no longer needed. Otherwise lists or reports may not include the results you expect.

You can click the link **Privacy Policy and Terms & Conditions** below the three device areas to display legal information.
7 Create new web console users

1. In the Dashboard, click the User management button.
   The Show users view is displayed.

2. Click the Create new user button.
   The Edit user view is displayed.

3. Enter a Login name for the new user.
4. In the Role field, select the user role:
   - Administrator
   - User
   - Helpdesk
   For further information, see User roles (section 2.2).

5. Enter the Last name and the First name of the new user.
6. Enter the Email address of the new user.
7. Enter a onetime Password for the first login at the web console and confirm it.
8. Click the Save button.

The new user is created and shown in the Show users view. Forward the user credentials (user, customer and one-time password) to the new user. The new user can log in at the web console and is prompted to change the password.
8 Configure technical contact

In the web console, you can configure technical contact information to support users in case of questions or problems.

**Prerequisite:** To edit the technical contact information, you must have the user role *Administrator*.

1. In the **Dashboard** view, click the **Technical contact** button.

   The **Technical contact** view is displayed.

2. Click the **Edit** button.

   The fields in the **Technical contact** view become available for editing.

3. Enter the required information for the technical contact. Under **Additional information**, you can enter any additional information for supporting users in case of questions or problems.

4. Click the **Save** button.

The technical contact information is displayed when users click the **Technical contact** button in the **Dashboard**. For end users the technical contact information is shown in the Sophos Mobile Control app on iOS and Android devices. It is also shown when end users click the **Help** button in the Self Service Portal.
9 Configure personal settings

You can configure personal settings for the use of the Sophos Mobile Control web console.

**Note:** These settings are user-specific. They must be defined separately for each user account.

1. In the **Dashboard** view, click the **Settings** button.
   
The **Settings** view is displayed.

2. In the **Personal** tab, configure the following settings:
   
   a) In the **Data sets per table page** field, select the maximum number of data sets you want to display per page in the web console. You can choose between **20** and **100** data sets.

   b) Under **Activated platforms**, select the platforms you want to use in the web console: **Android**, **Blackberry**, **iOS** and/or **Windows Mobile**. If you select specific platforms, you can only use the selected platforms with Sophos Mobile Control. All other platforms are hidden. In addition, all modules and functions that are not required for a specific platform are hidden.

3. Click the **Save** button.

4. As some changes in the personal settings are only applied after the next login, log out from the web console and log in again.

The new personal settings are applied to your user account.
10 Configure password policies

To enforce password security, you can define customer-specific password policies for users of the Sophos Mobile Control web console and the Self Service Portal. The password policies you define apply to new and changed passwords.

Note: The password policies only apply to Self Service Portal users managed by internal user management. If you use external user management, the password policies defined in external user management apply to Self Service Portal users. In this case, the password policies defined in the Sophos Mobile Control web console only apply to web console users.

1. In the Dashboard, click the Settings button.
   The Settings view is displayed.

2. Go to the Password Policies tab.

3. Under Password policies for SMC web console user and SSP user - Quality of password, define the following minimum values for the password:
   - **Minimum password length**: You can select a value from 4 to 10.
   - **Minimum number of lower-case letters**: You can select a value from 1 to 10.
   - **Minimum number of upper-case letters**: You can select a value from 1 to 10.
   - **Minimum number of digits**: You can select a value from 1 to 10.
   - **Minimum number of special characters**: You can select a value from 1 to 10.

4. Under Password policies for SMC web console user and SSP user - Settings of password, define the following settings:
   - **Password change interval (days)**: You can enter a value from 0 (no password change required) to 730 days.
   - **Number of previous passwords which must not be reused**: You can select a value between 1 and 10.
   - **Maximum number of failed login attempts**: You can select a value between 2 and 10.

5. Under Reset password settings, configure the emails to be sent to users after they have requested a password reset. When users request a password reset, they receive an email with a link for generating a new password. After clicking the link, a second email with a one-time password is sent to the users. For further information, see Password recovery (section 4.3).
   a) In the Originator field, enter the email sender address.
   b) Under Reset password settings - Email with reset link, enter a Subject for the first email to be sent to users, for example "Generate a new password for Sophos Mobile Control". In the text field, predefine the email content. Use the placeholder _RESET_TOKEN_LINK_ to include a link for generating a password for the user. This link is required for providing the user with a new password. The placeholders _RESET_TOKEN_LINK_, _LOGINNAME_,
c) Under **Reset password settings - Email with new password**, enter a **Subject** for the second email to be sent to users, for example "New password for Sophos Mobile Control". In the text field, predefine the email content. Use the placeholder _NEW_PASSWORD_ to include the new password for the user. This link is required for providing the user with a new password. The placeholders _NEW_PASSWORD_, _LOGINNAME_, _FIRSTNAME_ and _LASTNAME_ will be replaced by the corresponding values in the email.

6. Click the **Save** button.

The password policies defined apply to web console and Self Service Portal users for this customer.
11 Configure platform-specific settings

You have to configure specific settings for different platforms to support management of these device types in Sophos Mobile Control:

■ Apple iOS

For iOS devices you must enable the use of Apple Push Notification service by uploading the APNs keystore to the web console. For further information on how to obtain your APNs certificate for Sophos Mobile Control, refer to the Sophos Mobile Control startup guide or the Sophos Mobile Control as a Service startup guide.

In addition, you can configure the locate function for iOS devices, if this is allowed for the customer you are logged in to. The super administrator can activate or deactivate the iOS locate function in customer management. For further information on customer management, see the Sophos Mobile Control super administrator guide.

Note: Super administrators are not supported for Sophos Mobile Control as a Service. For Sophos Mobile Control as a Service, customers are predefined.

■ BlackBerry

To support BlackBerry devices, you must specify the BlackBerry Enterprise Server in the web console.

11.1 Upload Apple Push Notification keystore

To use the built-in Mobile Device Management (MDM) protocol of devices running Apple iOS 4 (or higher), Sophos Mobile Control must use Apple Push Notification service (APNs) to trigger iOS devices. To enable the Apple Push Notification service, you must upload the Apple Push Notification keystore in the web console. For information on how to obtain your APNs certificate for Sophos Mobile Control, refer to the Sophos Mobile Control startup guide or the Sophos Mobile Control as a Service startup guide.

Prerequisite: You have obtained your APNs certificate for Sophos Mobile Control.

1. In the Dashboard view, click the Settings button.

   The Settings view is displayed.

2. Go to the iOS APNS tab.

3. Browse for the APNs certificate file. If you have not changed the suggested name during the creation process, this file should be called mdm_apns_certificate.pkcs12. Enter the required password and click Upload.

   After the file has been uploaded successfully, a confirmation message is displayed.

4. Click Save.
11.2 Configure Locate function for iOS devices

If the **Locate** function is enabled, the Sophos Mobile Control app installed on iOS devices determines the device location and sends it to the Sophos Mobile Control Server. You can configure a compliance setting that relates to the **Locate** function to make sure that the user allows the Sophos Mobile Control app to retrieve location data, see *Available compliance settings* (section 12.1). The **Locate** function is available to administrators in the **Show device** and **Edit device** views (see *Carry out administrative tasks* (section 21.4)) and to end users in the Sophos Mobile Control Self Service Portal (see the *Sophos Mobile Control user guide for Apple iOS*).

**Note:** You can only configure the locate function for iOS devices, if this is allowed for the customer you are logged in to. The super administrator can activate or deactivate the iOS locate function in customer management. For further information on customer management, see the *Sophos Mobile Control super administrator guide*. Super administrators are not supported in Sophos Mobile Control as a Service. In this case customers are predefined.

1. In the **Dashboard** view, click the **Settings** button.

   The **Settings** view is displayed.

2. Go to the **iOS client** tab.

3. Make sure that the **Enable location change monitor** field is selected.

4. In the **Desired accuracy (in meters)** field, select the radius for position changes detected by the **Locate** function:
   - 100
   - 1000
   - 3000

   **Note:** If you select a small radius in this field, the battery life of the end user device may be affected due to a high number of position queries. If you select a big radius, server load may be affected due to position notifications sent.

5. Click the **Save** button.

11.3 Configure BlackBerry Enterprise Server

BlackBerry devices are supported in Sophos Mobile Control through BlackBerry Enterprise Server. In the web console, you must specify the BlackBerry Enterprise Server URL and the account configured to be used for Sophos Mobile Control.

**Note:** BlackBerry devices are not supported for Sophos Mobile Control as a Service.

1. In the **Dashboard** view, click the **Settings** button.

   The **Settings** view is displayed.

2. Go to the **RIM BES** tab.
3. In the **BlackBerry BES URL** field, enter the URL of the BlackBerry Enterprise Server.
4. Enter the **User name** and the **Password** of the account to be used for Sophos Mobile Control.
5. Click the **Save** button.
12 Configure compliance settings

In the web console, you can:

- Configure compliance settings and rules for all available device types (platforms).
- Define actions to be taken if devices no longer comply with the rules specified.
- Define multiple sets of compliance settings and rules and assign them to device groups. In device groups, you can select different compliance sets for corporate or private devices. This allows you to apply different levels of security for different device groups.

1. In the Dashboard view, click the Device compliance criteria button.
   The Compliance settings list view is displayed.
2. Click the Add button.
3. The Compliance settings view with tabs for all available device types is shown.
4. Enter a Name and a Description for the new compliance set.
5. Go to the required tab.
6. Make sure that the Enable platform field is selected.
   **Note:** If this field is not selected, devices of the relevant platform cannot be checked for compliance.
7. Under Rule, configure the compliance requirements for the selected device type. For a list of all settings available per device type, see Available compliance settings (section 12.1).
8. Under Disallow Active Sync, you can specify that email access will be denied automatically, if devices are not compliant. Select the required checkboxes next to the corresponding rules.
   **Note:** Managing access to corporate email is not supported in Sophos Mobile Control as a Service. If you use Sophos Mobile Control as a Service, the Disallow Active Sync settings column is not available.
9. Under Notify admin, you can define that administrators are notified by email, if devices are not compliant. Select the required checkboxes next to the corresponding rules.
10. Under Transfer task bundle, you can select task bundles to be transferred for the required Rule settings. If devices do not comply with the rules, the task bundles selected are transferred automatically.
    **Note:** You must create the task bundle in the web console first. If you have not created a task bundle yet, update the compliance settings afterwards. For information on how to create a task bundle, see Working with task bundles (section 18).
11. After you have defined all settings in all required device type tabs, click the Save button.
   The new compliance set is displayed in the Compliance settings list view.
12. If you have specified that administrators receive email notifications when devices are not compliant, specify the relevant recipients under **Admin mail recipients**. Use ; to separate several administrators in the **Admin mail recipients** field. Define a notification schedule under **Admin mail timetable**.

13. Click the **Save** button.

The new compliance set can be assigned to device groups. In device groups, you can select different compliance sets for corporate or private devices.

### 12.1 Available compliance settings

The following table shows the compliance settings you can select for the individual platforms under **Rule** in the relevant **Compliance Settings** tabs.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Android</th>
<th>iOS</th>
<th>Windows Mobile</th>
<th>BlackBerry</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Min. client version</strong></td>
<td>Enter the minimum Sophos Mobile Control client version that has to be installed on the device.</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td><strong>Allow root rights</strong></td>
<td>Select whether devices with root rights are allowed.</td>
<td>✔️</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td><strong>Allow jailbreak</strong></td>
<td>Select whether jailbroken devices are allowed.</td>
<td>✗</td>
<td>✔️</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td><strong>Passcode required</strong></td>
<td>Select whether a passcode is required for devices.</td>
<td>✗</td>
<td>✔️</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td><strong>Allow non-market apps</strong></td>
<td>Select whether non-market apps are allowed on devices.</td>
<td>✔️</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td><strong>Allow debug bridge (ADB)</strong></td>
<td>Select whether ADB (Android Debug Bridge) is allowed on devices.</td>
<td>✔️</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
<td>Android</td>
<td>iOS</td>
<td>Windows Mobile</td>
<td>BlackBerry</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
<td>-----</td>
<td>----------------</td>
<td>------------</td>
</tr>
<tr>
<td>Min. OS version</td>
<td>Select the minimum operating system version required on devices.</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Max. Synchronization gap</td>
<td>Specify the maximum interval between synchronisation processes for devices. For further information, refer to the Sophos Mobile Control user guide for Apple iOS.</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✗</td>
</tr>
<tr>
<td>Max. iOS app Synchronization gap</td>
<td>Specify the maximum interval between iOS app synchronisation processes for devices. For further information, refer to the Sophos Mobile Control user guide for Apple iOS.</td>
<td>ℹ️</td>
<td>✔</td>
<td>ℹ️</td>
<td>ℹ️</td>
</tr>
<tr>
<td>Max. SMSec scan interval</td>
<td>This field is only displayed, if Sophos Mobile Security is available for this customer. For further information, see Managing Sophos Mobile Security from Sophos Mobile Control (section 26). In this field, you can specify the maximum scan interval for malware scans performed by the Sophos Mobile Security app on the device.</td>
<td>✔</td>
<td>✗</td>
<td>ℹ️</td>
<td>ℹ️</td>
</tr>
<tr>
<td>Malware apps allowed</td>
<td>This field is only displayed, if Sophos</td>
<td>ℹ️</td>
<td>ℹ️</td>
<td>ℹ️</td>
<td>ℹ️</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
<td>Android</td>
<td>iOS</td>
<td>Windows Mobile</td>
<td>BlackBerry</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
<td>-----</td>
<td>----------------</td>
<td>------------</td>
</tr>
<tr>
<td>Mobile Security is available for this customer. Select whether detected malware apps are allowed on devices.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Suspicious apps allowed</td>
<td>This field is only displayed, if Sophos Mobile Security is available for this customer. Select whether detected suspicious apps are allowed on devices.</td>
<td>✔️</td>
<td>⊗️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PUA allowed</td>
<td>This field is only displayed, if Sophos Mobile Security is available for this customer. Select whether detected PUAs (Potentially Unwanted Apps) are allowed on devices.</td>
<td>✔️</td>
<td>⊗️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption required</td>
<td>Select whether encryption is required for devices.</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data roaming allowed</td>
<td>Select whether data roaming is allowed for devices.</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>App must be able to locate</td>
<td>This setting refers to the Locate function for iOS devices. Select whether the</td>
<td>⊗️</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
<td>Android</td>
<td>iOS</td>
<td>Windows Mobile</td>
<td>BlackBerry</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
<td>-----</td>
<td>----------------</td>
<td>------------</td>
</tr>
<tr>
<td></td>
<td>user has to allow the Sophos Mobile Control app to retrieve location data for compliance. For further information, see <em>Configure Locate function for iOS devices</em> (section 11.2).</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Blacklisted apps/Whitelisted apps | Allow or disallow apps on devices. Select Blacklisted apps or Whitelisted apps from the dropdown list and click Edit. In the Whitelisted/Blacklisted apps view, add the app(s) you want to allow/disallow and click Apply.  
Note: If you use whitelisted apps, only the ones on the list can be installed on the device. | ✓       | ✓   | ✓              | ✓          |
| Mandatory apps                  | Specify apps that have to be installed on devices. Click Edit. In the Mandatory apps view, add the app(s) you want to define as mandatory and click Apply.                                                   | ✓       | ✓   | ✓              | ✓          |
12.2 Assign compliance sets to device groups

1. In the web console menu bar, go to Inventory and click Device groups. The Device groups view is displayed.

2. Click the Edit icon next to the device group you want to assign compliance sets to. In the web console, a Default device group is available. For information on how to create your own device groups, see Create device groups (section 14.1).

3. Under Compliance settings in the fields For corporate devices and For private devices, select the compliance sets you want to apply.

4. Click the Save button.

The selected compliance sets are shown in the Device groups view for the relevant device group under Policies for corporate devices and Policies for private devices.

12.3 Check devices for compliance

After you have configured compliance settings, you can check if registered devices comply with the rules defined.

1. In the Dashboard, click the Device compliance criteria button. The Compliance settings view is displayed.

2. Click the Check now button.

All registered devices are checked for compliance according to the rules defined in Compliance settings. The specified actions are carried out. The Device status overview in the Dashboard is updated accordingly.
13 Configure provisioning by email

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

Prerequisites:

- A mail server needs to be configured during Sophos Mobile Control installation. For further information, see the Sophos Mobile Control installation guide.

  Note: For Sophos Mobile Control as a Service, the mail server is preconfigured. The installation procedure described in the Sophos Mobile Control installation guide is not relevant.

- 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.

- The device phone number must be specified as 0 when the devices are added to Sophos Mobile Control manually or by import. The specified email address is only used for provisioning, if there is no telephone number available.

To configure the email to be sent:

1. In the Dashboard view, click the Settings button.
   The Settings view is displayed.

2. Go to the Provisioning via email tab.

3. In the Originator field, enter the email sender address.

4. In the Subject field, redefine an email subject. The following placeholders are available:
   - _DEVICENAME_
   - _DEVICEDESCRIPTION_
   The placeholders are replaced by the relevant values in the email sent to devices.

5. In the text fields Content for Android devices and/or Content for iOS devices, redefine the email content. The following placeholders are available:
   - _DOWNLOADLINK_
   - _CONFIG_LINK_
   - _DEVICENAME_
   - _DEVICEDESCRIPTION_
   The link placeholders are obligatory. They are replaced by the actual link in the email sent to devices.
6. Click the **Save** button.

The email you have configured will be sent to the device email accounts for provisioning.
14 Add devices to Sophos Mobile Control

Devices can be added to Sophos Mobile Control administration in the following ways:

- Add devices manually in the web console.
- Import devices in a .csv file in the web console.
- Enable end users to register their own devices through the Self Service Portal, see Configure Self Service Portal use for end users (section 20). 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. The devices are provisioned by executing defined task bundles, see Working with task bundles (section 18).

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

You can group devices for easier administration. You can assign devices to existing device groups when you add them to Sophos Mobile Control administration. In the web console, a Default device group is available. If you have not defined your own device groups yet, you can add devices to this group.

14.1 Create device groups

Device groups are used to categorize devices. You assign devices to device groups when you add them to Sophos Mobile Control device management manually or by import. For devices that end users register through the Self Service Portal, you can define the group they should be added to in the Self Service Portal settings, see Configure Self Service Portal settings (section 20.2).

A device belongs to exactly one device group. Device groups make administration easier as in most device management functions, you can select a complete group or single devices.

**Note:** We recommend that you only group devices with the same operating system. This makes it easier to use groups for installations and other operating system specific tasks.

In the web console, a Default device group is available. If you have not defined your own device groups yet, you can add devices to this group.

To create device groups:

1. In the web console menu bar, go to Inventory and click Device groups.

   The Device groups view is displayed.

2. Click the Create new device group button.

   The Edit device group view is displayed.
3. Enter a **Name** and a **Description** for the new device group.

4. Under **Compliance settings** in the fields **For corporate devices** and **For private devices**, you can select the compliance sets you want to apply.

5. Click the **Save** button.

The new device group is created and shown in the **Device groups** view. You can now add devices to the new group.

**Note:** After you have added devices to the group, you can display the details of device group members by clicking on the device in the **Members** table in the **Show device group** or **Edit device group** view.

**Note:** If you delete a device group, the group members are moved to another group that needs 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.

### 14.2 Create a new device

1. In the web console menu bar, go to **Inventory** and select **Devices**.

   The **Devices** view is displayed.

2. Click the **Create new device** button.

   The **Select device template** view is displayed.

3. Under **Template**, select the device template for the mobile device type (for example Android) and click **Next**.

   The **Edit device** view is displayed.

4. In the **Edit device** view, specify the following device details:

   a) In the **Name** field, enter a unique name for the new device.
   
   b) In the **Description** field, enter a description for the new device.
   
   c) Under **Device group**, select the device group the device is to be assigned to.

   **Note:** A **Default** device group is available. If you have not defined your own device groups yet, you can add devices to this group. For information on how to create your own device groups, see **Create device groups** (section 14.1).

   d) In the **Phone number** field, enter the phone number of the new device. This field is mandatory. If you add a device that does not have a phone number (for example a tablet...
device), enter 0 here. Enter the phone number in international format, for example "+491701234567".

e) If you want to provision the device by email, for example a tablet device that does not have a phone number, enter an email address in the Email address field. For further information, see Configure provisioning by email (section 13).

f) Under Owner, select Corporate device or Private device.

5. To add an LDAP link to the device, click the Add LDAP link button. For further information, see Add LDAP link to a device (section 21.3.1).

6. To add custom properties to the device, go to the Custom properties tab and click the Create new property button. For further information, see Define custom properties for devices (section 21.3.2).

7. After you have specified all relevant device details, click the Save button.

The new device is added to Sophos Mobile Control administration and displayed in the Devices view under Inventory. The device is also displayed under Members in the device group you have selected. You can now provision and manage the device.

14.3 Import 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 devices view.

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 web console menu bar, go to Inventory and select Devices

   The Devices view is displayed.

2. Click the Import devices button.

   A message for selecting the data source is displayed.

3. Select CSV file from the dropdown list and click the Yes button.

   The Import devices view 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.

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 Finish button.
The devices listed in the .csv file are imported and displayed in the Devices view. The devices are also displayed under Members in the device groups specified in the .csv file. You can now provision and manage the devices.

14.4 Import 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.

Note: BlackBerry devices are not supported for Sophos Mobile Control as a Service.

1. In the web console menu bar, go to Inventory and select Devices.

   The Devices view is displayed.

2. Click the Import devices button.

   A message for selecting the data source is displayed.

3. Select BlackBerry Enterprise Server from the dropdown list and click the Yes button.

   The Import devices view is displayed.

4. 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.

5. Select the devices to import and click the Finish button.

   A message is displayed.

6. In the message, select if all or only selected devices should be imported and specify the template and device group to be used.

7. Confirm your selection by clicking the Yes 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.
15 Provision devices through the Sophos Mobile Control web console

After you have added new devices in the web console, they need to be provisioned with the Sophos Mobile Control client component. The tasks necessary depend on the mobile device type:

- Android and Windows Mobile devices are provisioned by SMC client installation.
- Apple iOS devices are provisioned by iOS MDM client bootstrap.

Provisioning is usually done only once per device.

Note: For Android and iOS devices without phone numbers, for example tablets, the provisioning by email method can be used. You can configure this provisioning method in the web console, see Configure provisioning by email (section 13). Such devices can also be set up by the end user in the Self Service Portal. For further information, see the Sophos Mobile Control user guides for Android and Apple iOS.

Note: You can bundle all tasks necessary to have a device fully registered and running by creating task bundles to provision the device, apply required policies and install required applications (for example managed apps for Apple iOS devices). For further information, see Working with task bundles (section 18).

Note: Devices that are registered by end users through the Self Service Portal can be provisioned by including a task bundle for provisioning when configuring the settings for Self Service Portal use. For further information on how to create the task bundles required for provisioning, see the Sophos Mobile Control startup guide or the Sophos Mobile Control as a Service startup guide. For further information on how to select the task bundle in the Self Service Portal settings, see Configure Self Service Portal settings (section 20.2). For further information on the Self Service Portal and how to use it, refer to the Sophos Mobile Control user guides for Android, Apple iOS and Windows Mobile.

15.1 Add Sophos Mobile Control client packages

For provisioning devices, the current Sophos Mobile Control client packages must be available in the web console. New packages can be added by updates supplied by Sophos. You can also add new packages in the web console as follows:

1. In the web console menu bar, go to Provisioning and click SMC client packages.

   The Sophos Mobile Control client packages view is displayed.

2. Click the Create new package button.

   The Edit package view is displayed.

3. Enter a Name and a Version for the new client package.
4. Under Operating systems, select the compatible operating systems for the new client package.

5. Select how the client package is provided:
   - Select Upload package to directly upload the package to the web console. Select the required package and click Upload.
   - To provide a link to the client package, select Link to package. Under Link, enter the relevant link. The Link field is mandatory. For further information on how to create links to iOS and Android client packages, see Create links to packages (section 16.1).

6. Click the Save button.

The Sophos Mobile Control client package is available for provisioning. It is displayed in the Sophos Mobile Control client packages view.

### 15.2 Provision Android and Windows Mobile devices

1. In the web console menu bar, go to Provisioning and select SMC client installation.
   
   The Select device(s) view is displayed.

2. In this view, you can:
   - Select individual devices you want to provision.
   - Click the Group selection button, to open the Select device group(s) view and select one or several device groups for provisioning.

3. After you have made your selection, click Next.
   
   The Select software view is displayed.

4. Select the Sophos Mobile Control client package that you want to install and click Next.
   
   The Set execution date view is displayed.

5. Under Scheduled date, select Now or specify a Date and Time for the execution of this task.

6. Select Enforce, to force client installation for the selected devices.

7. Click the Finish button.

The selected devices are provisioned at the specified date and time. After successful completion and synchronization with the server their device status is shown as Managed.

### 15.3 Provision iOS devices

1. In the web console menu bar, go to Provisioning and select iOS MDM client bootstrap.
   
   The Select device(s) view is displayed.
2. In this view, you can:
   - Select individual devices you want to provision.
   - Click the Group selection button, to open the Select device group(s) view and select one or several device groups for provisioning.

3. After you have made your selection, click Next.
   The Set execution date view is displayed.

4. Under Scheduled date, select Now or specify a Date and Time for the execution of this task.
5. Select Enforce, to force iOS MDM client bootstrap for the selected devices.

The selected devices are bootstrapped at the specified date and time. To complete provisioning, you must install the Sophos Mobile Control app on the device, see Install software packages (section 16.4).
16 Working with software packages and applications

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

When you create software packages, you can provide the packages to be installed on the devices as follows:

- You can upload the package to the web console.
- You can provide a link to the package for download.

In addition to installing and uninstalling software packages on devices, you can enable and disable processes on Windows Mobile devices.

16.1 Create links to packages

If you want to provide links to packages, you need to create them before you create the software packages in the web console. The following sections describe how to create links to Apple iOS and Android packages.

16.1.1 Create links to iOS packages

1. In your browser, go to http://itunes.apple.com/linkmaker.
2. In the Link Maker fields, specify the following for the relevant app:
   - In the Search field, enter a search term, for example the app provider or part of the app name.
   - Country
   - Media Type
   - Genre/Category
3. Click Search.
   The apps found are shown below the search fields.
4. Go to the required app and click iPhone App Link or iPad App link.
   The Linking to App: window is displayed. It shows the generated link.
5. Copy the link shown under Direct Link.
   You can add the generated link when you create a software package.
16.1.2 Create links to Android packages

1. In your browser, go to https://play.google.com/store.
2. Search for the required app and open it.
3. Copy the link shown in the web address bar of your browser.

You can add the link when you create a software package.

16.2 Create software packages

1. In the web console, go to Applications and click Software packages.
   The Software Packages view is displayed.
2. Click the Create new package button.
   The Edit package view is displayed.
3. Enter a Name and a Version for the new software package. These two fields are mandatory.
4. For Android and Apple iOS devices you can provide the software through the Enterprise App Store and define it as recommended or required. To do so, select Recommended or Required in the Recommendation status field.
5. Under Operating systems, select the operating system the new software package applies to.
6. Select how the software package is provided:
   - Select Upload package to directly upload the package to the web console. Select the required package and click Upload.
   - To provide a link to the package, select Link to package. Under Link, enter the relevant link. The Link field is mandatory.
7. Click the Save button.

The software package is available for installation. It is displayed in the Software Packages view. If you have configured the software as Recommended or Required, it is displayed in the Enterprise App Store of the Sophos Mobile Control client on the end user device for download. Users can select it for installation. The installation process runs unattended or with very little user interaction. For further information on installing required and recommended apps on devices, refer to the Sophos Mobile Control user guides for Android and Apple iOS.
16.2.1 Download uploaded software packages

Once you have uploaded a software package to the system, you can download it again any time to check it, so you do not need to manage files separately.

1. In the web console menu bar, go to **Applications** and click **Software Packages**.

   The **Software Packages** view is displayed.

2. Go to the required software package and click the **Edit** pencil icon.

   The **Edit package** view is displayed.

3. Click the **Download** icon next to the software package.

   A file download dialog is displayed.

4. Save the file at the required location.

16.3 Manage apps purchased with the Apple Volume Purchase Program

With the Apple Volume Purchase Program (VPP), you can buy iOS apps in volume for distribution within your company. For detailed information on how to enroll and use the Apple Volume Purchase Program, see [http://www.apple.com/business/vpp/](http://www.apple.com/business/vpp/).

After an order placed with the Apple Volume Purchase Program has been completed, you can download an Excel spreadsheet with redemption codes for the apps you purchased. To manage apps purchased with Apple Volume Purchase Program with Sophos Mobile Control, you can upload the code spreadsheet and assign the individual VPP codes to the relevant software packages in the Sophos Mobile Control web console.

16.3.1 Upload and assign VPP codes

**Prerequisites:**

- You have downloaded the .xls spreadsheet with the redemption codes for purchased apps from Apple. For further information on how to use the Apple Volume Purchase Program, see [http://www.apple.com/business/vpp/](http://www.apple.com/business/vpp/).

- You have created software packages with links to the purchased iOS apps in the web console. For further information, see [Create links to iOS packages](section 16.1.1) and [Create software packages](section 16.2).

1. In the web console, go to **Applications** and click **Software packages**.

   The **Software Packages** view is displayed.
2. Click the **Edit** pencil icon next to the required iOS app.
   The **Edit package** view is displayed.

3. Click the **Show** button next to the **VPP codes** field.
   The **VPP codes** view is displayed.

4. Browse for the .xls file you have downloaded and click **Upload**.
   The **VPP codes** view is updated with the code information from the .xls file:
   - The **Available codes** field shows the number of available codes.
   - The **Reserved codes** field shows the number of codes reserved for specific devices.
   - The **Used codes** field shows the number of codes used.
   - The **Invalid codes** field shows the number of invalid codes.
   In the table below these fields, the individual codes are shown with their status. If codes have been reserved for particular devices, the device UDIDs are shown.

5. Select the code you want to assign to the iOS app and click the **Apply** button.
   The **Edit package** view is displayed again.

6. Click the **Save** button.

### 16.4 Install software packages

Prerequisite: The required software package has been created under **Applications - Software packages**.

1. In the web console menu bar, go to **Applications** and click **Install**.
   The **Select device(s)** view is displayed.

2. In this view, you can:
   - Select individual devices you want to install the software package on.
   - Click the **Group selection** button, to open the **Select device group(s) view** and select one or several device groups for installing the software.

3. After you have made your selection, click **Next**.
   The **Select software** view is displayed.

4. Select the software package that you want to install and click **Next**.
   The **Set execution date** view is displayed.

5. Under **Scheduled date**, select **Now** or specify a **Date** and **Time** for the execution of this task.

6. Select **Enforce** to force installation for the selected devices.
7. Select **Activate application** to activate the application on the device.
8. Select **Silent installation (if supported)** to install the software package silently without any user interaction.

   **Note:** Silent installation may not be supported for all devices.

9. Click the **Finish** button.

The software package is installed on the selected device(s) at the specified time.

### 16.5 Uninstall software packages

**Note:** Silent uninstallation works on iOS devices for managed apps distributed by Sophos Mobile Control and for Windows Mobile devices. It does not work for Android devices.

1. In the web console menu bar, go to **Applications** and click **Uninstall**.

   The **Select device(s)** view is displayed.

2. In this view, you can:

   - Select individual devices for uninstalling the software.
   - Click the **Group selection** button, to open the **Select device group(s)** view and select one or several device groups for uninstalling the software.

3. After you have made your selection, click **Next**.

   The **Select software** view is displayed with all applications installed on the selected device(s).

4. Select the application(s) you want to uninstall and click **Next**.

   The **Set execution date** view is displayed.

5. Under **Scheduled date**, select **Now** or specify a **Date** and **Time** for the execution of this task.
6. Select **Enforce** to force the uninstallation for the selected devices.
7. Click the **Finish** button.

The selected applications are uninstalled from the selected device(s) at the specified date and time.

### 16.6 Use the software filter

By using filters you can restrict the number of items shown in lists according to defined criteria. With the software filter, you can restrict the results in lists of software packages.

**Note:** The filter is not only valid for the function currently displayed, but for all functions where items of this type are listed.
To use the software filter:

1. In the web console menu bar, go to **Applications** and click **Software packages**.

   The **Software Packages** view is displayed.

2. Click the **Filter** button (magnifier icon) in the web console header.

   The **Software filter** dialog is displayed with the status **Filter is not active**.

3. In the **Software filter** dialog, you can select the following filter options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Filter according to package name.</td>
</tr>
<tr>
<td>Version</td>
<td>Filter according to package version.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Filter according to operating systems for which</td>
</tr>
<tr>
<td></td>
<td>the packages are applicable.</td>
</tr>
</tbody>
</table>

4. After you have selected the required criteria, click **Filter**.

   The filter is activated and the list of devices is reloaded. The **Filter** button in the web console header changes its color from blue to pink to indicate that the filter is active. A **Reset** button is available in the header for resetting the filter. The status of the software filter in the **Software filter** dialog changes to **Filter is active**.

**Note:** Remember to reset filters manually when they are no longer needed. Otherwise lists or reports may not include the results you expect.

### 16.7 Enable/disable processes on Windows Mobile devices

In the web console under **Applications**, you can enable or disable processes on Windows Mobile devices. Disabled processes are not allowed to run. The Sophos Mobile Control client monitors all processes running on a device and immediately kills disabled processes. So you as an administrator can disable certain applications. Enabled processes are unaffected and can be started.

**Note:** If software packages are installed on the device manually (not through Sophos Mobile Control), the included processes are disabled by default. If the package has been installed with 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 enabled or disabled for single or multiple devices.
Note: For Windows Mobile devices the enabling and disabling of processes is deactivated by default. You can activate this functionality with the setConfig command (ProcessSecurityOn).

16.7.1 Enable/disable processes on single devices

1. In the web console menu bar, go to Applications and click Enable/disable.
   The Select device(s) view is displayed.

2. Select the required device and click Next.
   The Activate/Deactivate processes view is displayed.

3. In the two tables displayed, select the required software packages and the system processes and activate or deactivate them by clicking the relevant icons.

4. Click Next.
   The Select execution date and description view is displayed.

5. Under Scheduled date, select Now or specify a Date and Time for the execution of this task.

6. In the Description field, modify the description displayed, if necessary.

7. Click the Finish button.
   The selected processes are enabled/disabled on the selected device at the specified date and time.

16.7.2 Enable/disable processes on multiple devices

1. In the web console menu bar, go to Applications and click Enable/disable.
   The Select device(s) view is displayed.

2. In this view, you can:
   - Select several individual devices.
   - Click the Group selection button, to open the Select device group(s) view and select device groups.

3. After you have made your selection, click Next.
   The Set device as data source view is displayed.

4. Select the device you want to use as a data source for software packages and system processes by clicking the arrow icon next to the device. The device selected serves as the process information basis. Only the processes for this device are available for activation/deactivation. But all devices selected in the Select device(s) or Select device group(s) view are affected by the activation/deactivation process, if they provide the same system processes.
   The Activate/Deactivate processes view is displayed.
5. In the two tables displayed, select the required software packages and the system processes and activate or deactivate them by clicking the relevant icons.

6. Click Next.

   The Select execution date and description view is displayed.

7. Under Scheduled date, select Now or specify a Date and Time for the execution of this task.

8. In the Description field, modify the description displayed, if necessary.

9. Click the Finish button.

   The selected processes are enabled/disabled on the selected devices at the specified date and time.
17 **Working with configurations (profiles)**

In the web console under **Configurations**, you can create and transfer settings profiles for Apple iOS, Android and Windows Mobile devices.

For iOS devices, you can also upload profiles created with the iPhone Configuration Utility and transfer them to devices.

For Windows Mobile devices, you can manage templates for settings profiles. They define the setting options available for web console users. Templates are supplied by Sophos.

**Note:** For Android devices, supported settings may depend on vendor specific APIs. Depending on the end user device, some settings may not have any effect. For further information, refer to the feature matrix in the *Sophos Mobile Control technical guide*.

### 17.1 Create profiles for Apple iOS devices

Sophos Mobile Control offers two methods for creating profiles for iOS devices:

- You can create iOS profiles directly in the web console.
- You can import profiles created with the Apple iPhone Configuration Utility into the web console.

#### 17.1.1 Create iOS profiles in the web console

1. In the web console, go to **Configurations** and click **Profiles** under **Apple iOS**.
   
   The **Profiles** view is displayed.

2. Click the **Create new profile** button.
   
   The **Edit profile** view is displayed.

3. Enter a **Name** and a **Version** for the new profile.

4. In the **ID** field, enter a unique ID for the profile.

   **Note:** Special characters like ä or ö or spaces are not supported in iOS profile IDs.

5. In the **Organization** field, enter the name of the organization for the profile, for example a company name.

6. In the **Description** field, enter a description for the profile.

7. In the **User can remove profile** field, you can select whether users may remove the profile from their device:

   - **Always**
With authentication

If you select this option, the Authentication password field is displayed below the User can remove profile field. Enter the password required for removing the profile. To enable users to remove the profile, provide them with the password.

Never

8. In the Automatically remove on field, you can enter a date for the automatic removal of the profile from end user devices. The profile will be removed on the set date at 11 pm.

9. Under Operating systems, select the operating system the profile should apply to.

   Note: The Operating system field shows all iOS versions that are currently available in the system. Not all configuration settings may be supported for individual iOS versions. If you select all versions under Operating systems, some settings may not have any effect depending on the iOS version on the end user device.

10. Click the Add button to add configurations with iPhone configuration settings to the profile.

    The Available configurations view is displayed.

11. Select the configuration you want to add and click Next.

    The settings view of the configuration is displayed.

12. Specify the required settings. For a detailed list of all configurations and settings available, see Available iOS configurations (section 17.1.2).

13. Click the Apply button to save your changes.

    The configuration is displayed in the Edit profile view under Configurations.

14. Add further configurations as required.

15. After you have added all required configurations, click the Save button.

    The profile is available for transfer. It is displayed in the Profiles view.

17.1.2 Available iOS configurations

The following configurations are available for iOS profiles in the Available configurations view when you create or edit a profile. Some configurations can be added only once within a profile, others several times.

Note: Supported settings may depend on the iOS version in use on individual devices. Depending on the end user device, some settings may not have any effect. For further information, refer to the feature matrix in the Sophos Mobile Control technical guide.

Passcode policies

In this configuration, you can define passcode rules for devices. You can only add one Passcode policies configuration within a profile.
<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow simple value</td>
<td>If you select this option, users are allowed to use sequential or repeated characters in their passcode, for example &quot;1111&quot; or &quot;abcde&quot;.</td>
</tr>
<tr>
<td>Require alphanumeric value</td>
<td>If you select this option, passcodes must contain at least one letter or number.</td>
</tr>
<tr>
<td>Minimum passcode length</td>
<td>Specifies the minimum number of characters a passcode must contain.</td>
</tr>
<tr>
<td>Minimum number of complex characters</td>
<td>Specifies the minimum number of non-alphanumeric characters (for example &amp; or !) a passcode must contain.</td>
</tr>
<tr>
<td>Maximum passcode age (1 - 730 days or none)</td>
<td>Requires users to change their passcode in the specified interval. Value range: 0 (no password change required) to 730 days.</td>
</tr>
<tr>
<td>Maximum Auto-Lock (in minutes)</td>
<td>In this field, you can specify when (in minutes) the device should be locked after it has not been used. This setting specifies the maximum value the user is allowed to configure on the device.</td>
</tr>
<tr>
<td>Passcode history (1 to 50 or 0)</td>
<td>In this field, you can specify how many old passcodes are remembered and compared with new ones. When the user defines a new passcode, it will not be accepted, if it matches a previously used passcode. Value range: 1 to 50 or 0 (no passcode history).</td>
</tr>
<tr>
<td>Maximum grace period for device lock</td>
<td>In this field, you can specify how long the device can be unlocked after a lock without a passcode prompt. This setting specifies the maximum value the user is allowed to configure on the device. If you select None, the user can select any of the intervals available. If you select Immediately, users must enter a passcode every time they unlock their devices.</td>
</tr>
<tr>
<td>Maximum number of failed attempts</td>
<td>In this field, you can specify the maximum number of failed attempts to enter the correct passcode before the device is wiped. After six failed attempts, a time delay is imposed before</td>
</tr>
</tbody>
</table>
a passcode can be entered again. The delay increases with each failed attempt. After the final failed attempt, all data and settings are securely removed from the device. The time delay starts after the sixth attempt. So if you set this value to 6 or lower, no delay is imposed and the device is wiped when the attempt limit is exceeded.

### Restrictions

In this configuration, you can define restrictions for devices. You can only add one **Restrictions** configuration within a profile.

<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device functionality</strong></td>
<td></td>
</tr>
<tr>
<td>Allow installing apps</td>
<td>If you deactivate this option, the App Store is disabled and its icon is removed from the Home screen. Users cannot install or update apps through the App Store or iTunes.</td>
</tr>
<tr>
<td>Allow use of camera</td>
<td>If you deactivate this option, cameras are completely disabled on the device and the Camera icon is removed from the Home screen. Users cannot take pictures, record videos, or use FaceTime.</td>
</tr>
<tr>
<td>Allow FaceTime</td>
<td>If you deactivate this option, users cannot place or receive FaceTime video calls.</td>
</tr>
<tr>
<td>Allow screen capture</td>
<td>If you deactivate this option, users cannot take a screenshot of the display.</td>
</tr>
<tr>
<td>Allow automatic sync while roaming</td>
<td>If you deactivate this option, devices that are roaming will only sync when the user accesses an account.</td>
</tr>
<tr>
<td>Allow Siri</td>
<td>If you deactivate this option, users cannot use Siri, voice commands, or dictations.</td>
</tr>
<tr>
<td>Setting/field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allow Siri while device is locked</td>
<td>If you deactivate this option, users must unlock their devices by entering their passcode before they use Siri.</td>
</tr>
<tr>
<td>Allow voice dialing</td>
<td>If you deactivate this option, users cannot dial by using voice commands.</td>
</tr>
<tr>
<td>Allow Passbook while device is locked</td>
<td>If you deactivate this option, a device does not show Passbook notifications while locked.</td>
</tr>
<tr>
<td>Allow In-App purchase</td>
<td>If you deactivate this option, users cannot make in-app purchases.</td>
</tr>
<tr>
<td>Force user to enter store password for all purchases</td>
<td>If you select this option, users have to enter their Apple ID password to make any purchase. Usually, there is a brief grace period after a purchase before users have to authenticate for subsequent purchases.</td>
</tr>
<tr>
<td>Allow multiplayer gaming</td>
<td>If you deactivate this option, users cannot play multiplayer games in Game Center.</td>
</tr>
<tr>
<td>Allow adding Game Center friends</td>
<td>If you deactivate this option, users cannot add friends in Game Center.</td>
</tr>
<tr>
<td>Applications</td>
<td></td>
</tr>
<tr>
<td>Allow use of YouTube</td>
<td>If you deactivate this option, the YouTube app is disabled and its icon is removed from the Home screen.</td>
</tr>
<tr>
<td>Allow use of iTunes Store</td>
<td>If you deactivate this option, the iTunes Store is disabled and its icon is removed from the Home screen. Users cannot preview, purchase or download content.</td>
</tr>
<tr>
<td>Allow use of Safari</td>
<td>If you deactivate this option, the Safari web browser is disabled and its icon is removed from the Home screen. This also prevents users from opening web clips.</td>
</tr>
<tr>
<td>Enable autofill</td>
<td>If you deactivate this option, Safari does not autofill web forms with previously entered information.</td>
</tr>
<tr>
<td>Setting/field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Force fraud warning</td>
<td>If you select this option, Safari attempts to prevent users from visiting websites identified as fraudulent or compromised.</td>
</tr>
<tr>
<td>Enable JavaScript</td>
<td>If you deactivate this option, Safari ignores JavaScript on websites.</td>
</tr>
<tr>
<td>Block popups</td>
<td>If you select this option, Safari blocks popups.</td>
</tr>
<tr>
<td>Accept cookies</td>
<td>In this field, you can specify if cookies should be accepted:</td>
</tr>
<tr>
<td></td>
<td>■ Always</td>
</tr>
<tr>
<td></td>
<td>■ Never</td>
</tr>
<tr>
<td></td>
<td>■ From visited sites</td>
</tr>
<tr>
<td>iCloud</td>
<td></td>
</tr>
<tr>
<td>Allow backup</td>
<td>If you select this option, users can back up their devices to iCloud.</td>
</tr>
<tr>
<td>Allow document sync</td>
<td>If you select this option, users can store documents in iCloud.</td>
</tr>
<tr>
<td>Allow Photo Stream</td>
<td>If you select this option, users can enable Photo Stream.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you install a configuration profile that restricts the use of Photo Stream, Photo Stream photos will be removed from the user’s device. Photos will not be sent from the Camera Roll to Photo Stream. If there are no further copies of these photos, they may be lost.</td>
</tr>
<tr>
<td>Allow shared photo streams</td>
<td>If you select this option, users can invite others to view their photo streams and can view photo streams shared by others.</td>
</tr>
<tr>
<td>Security and privacy</td>
<td></td>
</tr>
<tr>
<td>Allow diagnostic data to be sent to Apple</td>
<td>If you deactivate this option, iOS diagnostic information is not sent to Apple.</td>
</tr>
<tr>
<td>Allow user to accept untrusted TLS certificates</td>
<td>If you deactivate this option, users are not asked if they want to trust certificates that</td>
</tr>
</tbody>
</table>
### Setting/field
<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cannot be verified. This setting applies to Safari and to Mail Contacts and Calendar accounts.</td>
</tr>
<tr>
<td><strong>Force encrypted backups</strong></td>
</tr>
<tr>
<td>If you select this option, encryption of backups is required and enforced by iTunes for any encrypted profiles.</td>
</tr>
<tr>
<td><strong>Content ratings</strong></td>
</tr>
<tr>
<td>If you deactivate this option, explicit music or video content is hidden in the iTunes Store. Explicit content is flagged by content providers, for example record labels, when listed on the iTunes Store.</td>
</tr>
<tr>
<td><strong>Allow explicit music and podcasts</strong></td>
</tr>
<tr>
<td>If you deactivate this option, explicit music or video content is hidden in the iTunes Store. Explicit content is flagged by content providers, for example record labels, when listed on the iTunes Store.</td>
</tr>
</tbody>
</table>

### Exchange ActiveSync
In this configuration, you can define user settings for your Microsoft Exchange Server. You can add multiple Exchange ActiveSync configurations.

<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Account name</strong></td>
<td>In this field, enter the account name for the Exchange ActiveSync account.</td>
</tr>
<tr>
<td><strong>Exchange ActiveSync Host</strong></td>
<td>In this field, enter the Microsoft Exchange Server.</td>
</tr>
<tr>
<td><strong>Allow move</strong></td>
<td>If you deactivate this option, users cannot move messages sent or received by this account to a different mail account. This also prevents using a different account to reply or forward a message from this account.</td>
</tr>
<tr>
<td><strong>Allow recent address syncing</strong></td>
<td>If you deactivate this option, recently used addresses are not synchronized with other devices using iCloud.</td>
</tr>
<tr>
<td><strong>Use only in mail</strong></td>
<td>If you select this option, this account can only be used to send messages from Mail. It cannot be selected as a sending account for messages created with other apps, for example Photos or Safari.</td>
</tr>
<tr>
<td>Setting/field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SSL</td>
<td>Make sure that this option is selected, to send all communication through SSL (Secure Socket Layer).</td>
</tr>
<tr>
<td>Domain</td>
<td>In this field, enter the domain for this account. To show a prompt for the user on the device, leave this field and the User field empty.</td>
</tr>
<tr>
<td>User</td>
<td>In this field, enter the user for this account. To show a prompt for the user on the device, leave this field and the Domain field empty.</td>
</tr>
<tr>
<td>Email address</td>
<td>In this field, enter the email address of the account.</td>
</tr>
<tr>
<td>Password</td>
<td>In this field, enter the password for this account.</td>
</tr>
<tr>
<td>Email synchronization period</td>
<td>In this field, select the time period for email synchronization. This is the number of days, emails are synchronized for. If you specify a time period here, not all emails are synchronized to the inbox on the mobile device, but only the emails from within the specified period. You can select the following synchronization periods:</td>
</tr>
</tbody>
</table>
|                            | - Unlimited  
|                            | - One day  
|                            | - Three days  
|                            | - One week  
|                            | - Two weeks  
|                            | - One month |
| Identity certificate       | In this field, select the identity certificate for the connection to ActiveSync. If no certificate is available for selection, a message is displayed. |

**WiFi**

In this configuration, you specify settings for connecting to WiFi networks. You can add multiple WiFi configurations.
<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
<td>In this field, enter the ID of the wireless network.</td>
</tr>
<tr>
<td>Connect automatically</td>
<td>Select this option, to automatically connect to the target network.</td>
</tr>
<tr>
<td>Hidden network</td>
<td>Select this option, if the target network is not open or visible.</td>
</tr>
<tr>
<td>Security type</td>
<td>In this field, you select the security type of the Wifi network:</td>
</tr>
<tr>
<td></td>
<td>■ None</td>
</tr>
<tr>
<td></td>
<td>■ WEP</td>
</tr>
<tr>
<td></td>
<td>■ WPA/WPA2</td>
</tr>
<tr>
<td></td>
<td>■ Any (personal)</td>
</tr>
<tr>
<td></td>
<td>■ Corporate WEP</td>
</tr>
<tr>
<td></td>
<td>■ Corporate WPA/WPA2</td>
</tr>
<tr>
<td></td>
<td>■ Any (company)</td>
</tr>
<tr>
<td></td>
<td>If you select the personal settings WEP, WPA/WPA2 or Any (personal), a Password field is displayed. Enter the relevant password.</td>
</tr>
<tr>
<td></td>
<td>If you select the corporate settings Corporate WEP, Corporate WPA/WPA2 or Any (company), the two tabs Protocols and Authentication are displayed.</td>
</tr>
<tr>
<td></td>
<td>In the Protocols tab configure the following:</td>
</tr>
<tr>
<td></td>
<td>■ Under Accepted EAP types, specify the EAP methods to be used for authentication. Depending on the types selected here, the values in the Internal identity field in this tab become available for selection.</td>
</tr>
<tr>
<td></td>
<td>■ Under EAP-FAST, configure the EAP-FAST Protected Access credential settings.</td>
</tr>
<tr>
<td></td>
<td>In the Authentication tab, you specify authentication settings:</td>
</tr>
<tr>
<td></td>
<td>■ In the User field, enter the user name for the connection to the wireless network.</td>
</tr>
</tbody>
</table>
### Setting/field

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ Select <strong>Use Per-Connection Password</strong>, if the password is to be queried for each connection and transferred with the authentication.</td>
</tr>
<tr>
<td>■ In the <strong>Password</strong> field, enter the relevant password.</td>
</tr>
<tr>
<td>■ In the <strong>Identity certificate</strong> field, select the certificate for the connection to the wireless network.</td>
</tr>
<tr>
<td>■ In the <strong>External identity</strong> field, enter the externally visible ID (for TTLS, PEAP and EAP-FAST).</td>
</tr>
</tbody>
</table>

### Proxy

In this field, select the proxy settings for the WiFi connection:

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ None</td>
</tr>
<tr>
<td>■ Manually</td>
</tr>
<tr>
<td>■ Automatic</td>
</tr>
</tbody>
</table>

If you select **Manually**, the fields **Server and port**, **Authentication** and **Password** are displayed. Enter the required proxy information. If you select **Automatic**, the field **Proxy server URL** is displayed. Enter the URL of the proxy server.

### VPN

In this configuration, you can define VPN settings for network connections. You can add multiple **VPN** configurations.

<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connection name</strong></td>
<td>In this field, enter the name of the connection shown on the device.</td>
</tr>
<tr>
<td><strong>Connection type</strong></td>
<td>In this field, select the connection type:</td>
</tr>
<tr>
<td>■ <strong>Cisco AnyConnect</strong></td>
<td></td>
</tr>
<tr>
<td>Setting/field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>IPSec (Cisco)</strong></td>
<td>Different entry fields are shown in the VPN view depending on the connection type you select here.</td>
</tr>
<tr>
<td><strong>Server</strong> (both connection types)</td>
<td>In this field, enter the host name or the IP address of the server.</td>
</tr>
<tr>
<td><strong>Account</strong> (both connection types)</td>
<td>In this field, enter the user account for the authentication of the connection.</td>
</tr>
<tr>
<td><strong>Group</strong> (connection type Cisco AnyConnect)</td>
<td>In this field, enter the group that may be required for the authentication of the connection.</td>
</tr>
</tbody>
</table>
| **User Authentication** (connection type Cisco AnyConnect) | In this field select the type of user authentication for the connection:  
  - **Password**  
    If you select this option, the Password field is shown below the User Authentication field. Enter the password for authentication.  
  - **Certificate**  
    If you select this option, the Certificate field is shown below the User Authentication field. Select a certificate. |
| **Device authentication** (connection type IPSec (Cisco)) | In this field, select the type of device authentication:  
  - **Keys (Shared Secret)/Group name**  
    If you select this option, the fields Group name, Keys (Shared Secret), Use hybrid authentication and Request password are displayed below the Device authentication field. Enter the required authentication information in the Group name and Keys (Shared Secret) fields. Select Use hybrid authentication and Request password as required.  
  - **Certificate** |
If you select this option, the fields **Certificate** and **Including user PIN** are displayed below the **Device authentication** field. In the **Certificate** field, select the required certificate. Select **Including user PIN** to include the user PIN in device authentication.

**Proxy (both connection types)**

In this field, select the proxy settings for the connection:

- **None**
- **Manually**

If you select this option, the fields **Server and port**, **Authentication** and **Password** are displayed. In the **Server and port** field, enter the valid address and the port of the proxy server. In the **Authentication** field, enter the user name for the connection to the proxy server. In the **Password** field, enter the password for the connection to the proxy server.

- **Automatic**

If you select this option, the **Proxy server URL** field is displayed. Enter the URL of the server with the proxy setting in this field.

**Web clip**

In this configuration, you can define web clips to be added to the Home screen of user devices. Web clips provide fast access to favorite web pages. But you can also add a web clip with a support phone number for example, to provide a quick way to dial the helpdesk. You can add multiple **Web clip** configurations.

<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>In this field, enter a description for the web clip.</td>
</tr>
</tbody>
</table>
### Setting/field

<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>URL</strong></td>
<td>In this field, enter the URL for the web clip.</td>
</tr>
<tr>
<td><strong>Can be removed</strong></td>
<td>If you deactivate this option, the user cannot remove the web clip. It cannot be deleted from the device unless the user removes the profile that installed it.</td>
</tr>
<tr>
<td><strong>Full screen</strong></td>
<td>If you select this option, the web clip is opened full screen on the device. A full screen web clip opens the URL as a web app.</td>
</tr>
</tbody>
</table>

### APN

With this configuration, you can change the device’s Access Point Name (APN) and cell network proxy settings. These settings define how devices connect to the carrier’s network. You can only add one APN configuration within a profile.

**Note:** If these settings are not correct, the device cannot access data using the cellular network. To undo settings changes, the profile must be removed from the device.

<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access point name (APN)</strong></td>
<td>In this field, enter the name of the access point of the carrier (GPRS).</td>
</tr>
<tr>
<td><strong>User name for access point</strong></td>
<td>In this field, enter the user name for the access point.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> iOS supports APN user names of up to 64 characters.</td>
</tr>
<tr>
<td><strong>Password for access point</strong></td>
<td>In this field, enter the password for the access point.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> iOS supports APN passwords of up to 64 characters.</td>
</tr>
<tr>
<td><strong>Proxy server and port</strong></td>
<td>In this field, you can enter the valid address and the port of the proxy server.</td>
</tr>
</tbody>
</table>
**Root certificate**

In this configuration, you can upload a root certificate for devices. You can add multiple Root certificate configurations. In the **File** field, browse for the relevant certificate and click **Upload**. The name of the certificate is shown in the **Certificate name** field.

**Note:** The certificate you upload here is only available for this profile. If you require certificates in other profiles, you have to upload them again.

**Client certificate**

In this configuration, you can upload a client certificate for devices. You can add multiple Client certificate configurations. In the **File** field, browse for the relevant certificate and click **Upload**. The name of the certificate is shown in the **Certificate name** field. Enter the **Password** for the selected certificate.

**Note:** The certificate you upload here is only available for this profile. If you require certificates in other profiles, you have to upload them again.

**SCEP**

In this configuration, you can define settings that allow the devices to obtain certificates from a Certificate Authority by using Simple Certificate Enrollment Protocol (SCEP). You can only add one SCEP configuration within a profile.

**Note:** This configuration is only available, if SCEP has been configured during Sophos Mobile Control setup. SCEP needs to be enabled during Sophos Mobile Control installation, see the Sophos Mobile Control installation guide. A super administrator can then configure the required SCEP settings in the web console, see the Sophos Mobile Control super administrator guide. The settings defined are transferred to iOS profiles.

**Note:** Super administrators are not supported for Sophos Mobile Control as a Service.

<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>In this field, enter the URL of the SCEP server.</td>
</tr>
<tr>
<td>Name</td>
<td>In this field, enter a name that is understood by the Certificate Authority. The name can for example be used to distinguish between instances.</td>
</tr>
<tr>
<td>Subject</td>
<td>In this field, enter the representation of an X.500 name as an array of OID and value. For example: /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar. This translates to: [ [“C”,“US”], [“O”,“Apple Inc.”], ..., [“1.2.5.3”,“bar”] ]</td>
</tr>
<tr>
<td>Setting/field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Type of subject alternative name</strong></td>
<td>In this field, select the type of an alternative name for the SCEP server:</td>
</tr>
<tr>
<td>■ None</td>
<td></td>
</tr>
<tr>
<td>■ RFC 822 name (email address)</td>
<td></td>
</tr>
<tr>
<td>■ DNS name</td>
<td></td>
</tr>
<tr>
<td>■ Uniform Resource Identifier</td>
<td>If you select any other option than <strong>None</strong>, the fields <strong>Value of subject alternative name</strong> and <strong>NT user login name</strong> are displayed below the <strong>Type of subject alternative name</strong>. Enter the required name values.</td>
</tr>
<tr>
<td><strong>Challenge</strong></td>
<td>In this field, enter a pre-shared secret the SCEP server can use to identify the request or user.</td>
</tr>
<tr>
<td><strong>Retries</strong></td>
<td>In this field, enter the number of retries if the server sends a &quot;pending&quot; response.</td>
</tr>
<tr>
<td><strong>Retry delay</strong></td>
<td>In this field, enter the number of seconds between retries.</td>
</tr>
<tr>
<td><strong>Key size</strong></td>
<td>In this field, select the key size:</td>
</tr>
<tr>
<td>■ 1024</td>
<td></td>
</tr>
<tr>
<td>■ 2048</td>
<td></td>
</tr>
<tr>
<td><strong>Use as digital signature</strong></td>
<td>Select this option to define the use as a digital signature as acceptable for the key.</td>
</tr>
<tr>
<td><strong>Use for encryption</strong></td>
<td>Select this option to define the use for encryption as acceptable for the key.</td>
</tr>
<tr>
<td><strong>Signature</strong></td>
<td>In this field, enter a hexadecimal character string as a signature.</td>
</tr>
</tbody>
</table>

### 17.1.3 Import iOS profiles created with the Apple iPhone Configuration Utility

You can import profiles created with the Apple iPhone Configuration Utility into the web console.  
**Note:** The Apple iPhone Configuration Utility is available for installation here:  
For Mac OS X: http://support.apple.com/kb/DL1465

1. After you have created a profile in the Apple iPhone Configuration Utility, export it (unencrypted and unsigned) and save it on your computer.
2. In the web console, go to Configurations and click Profiles under Apple iOS.
   The Profiles view is displayed.
3. Click the Import profile button.
   The Edit profile view is displayed.
4. Enter a Name and a Version for the new profile.
5. Under Operating systems, select the operating system the profile should apply to.
6. Browse for the profile you have saved on your computer and click Upload.
   The profile is displayed in the Edit profile view.
7. Click the Save button.
   The profile is available for transfer. It is displayed in the Profiles view.

### 17.2 Create profiles for Android devices

1. In the web console, go to Configurations and click Profiles under Android.
   The Profiles view is displayed.
2. Click the Create new profile button.
   The Edit profile view is displayed.
3. Enter a Name and a Version for the new profile.
4. In the ID field, enter a unique ID for the profile.
5. In the Description field, enter a description for the profile.
6. Under Operating systems, select the operating system the profile should apply to.
7. Click the Add button to add configurations with Android configuration settings to the profile.
   The Available configurations view is displayed.
8. Select the configuration you want to add and click Next.
   The settings view of the configuration is displayed.
9. Specify the required settings. For a detailed list of all configurations and settings available, see Available Android configurations (section 17.2.1).
10. Click the Apply button to save your changes.
    The configuration is displayed in the Edit profile view under Configurations.
11. After you have added all required configurations, click the **Save** button. The profile is available for transfer. It is displayed in the **Profiles** view.

### 17.2.1 Available Android configurations

The following configurations are available for Android profiles in the **Available configurations** view when you create or edit a profile. Some configurations can be added only once within a profile, others several times.

**Note:** Supported settings may depend on vendor specific APIs. Depending on the end user device, some settings may not have any effect. For further information, refer to the feature matrix in the *Sophos Mobile Control technical guide*.

#### Passcode policies

In this configuration, you can define passcode rules for devices. You can only add one **Passcode policies** configuration within a profile.

When you select the **Passcode policies** configuration, the **Passcode type** field is displayed. In this field, select the type of passcode you want define:

- **Any**

  If you select this setting, users have to set a passcode on their devices. But there are no requirements or restrictions concerning the password. If you have select this option, no further settings are required for the **Passcode policies** configuration.

- **Alphabetic**

- **PIN**

- **Alphanumeric**

- **Complex**

If you select **Alphabetic**, **PIN** or **Alphanumeric**, the following fields are displayed:

<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum passcode length</td>
<td>Specifies the minimum number of characters a passcode must contain.</td>
</tr>
<tr>
<td>Idle time in seconds before passcode prompt</td>
<td>In this field, you can specify when (in seconds) the device should be locked after it has not been used. The device can be unlocked by entering the passcode.</td>
</tr>
<tr>
<td>Maximum passcode age (in days)</td>
<td>Requires users to change their passcode in the specified interval (in days).</td>
</tr>
</tbody>
</table>
### Setting/field

<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Maximum number of failed attempts</strong></td>
<td>In this field, you can specify the maximum number of failed attempts to enter the correct passcode before the device is wiped.</td>
</tr>
<tr>
<td><strong>Minimum history length</strong></td>
<td>In this field, you can specify how many old passcodes are remembered and compared with new ones. When the user defines a new passcode, it will not be accepted, if it matches a previously used passcode. Value range: 1 to 5 or none.</td>
</tr>
</tbody>
</table>

If you select **Complex**, the following fields are displayed in addition to the fields shown for the other passcode types:

<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Minimum number of letters</strong></td>
<td>Specifies the minimum number of letters a passcode must contain.</td>
</tr>
<tr>
<td><strong>Minimum number of lowercase letters</strong></td>
<td>Specifies the minimum number of lowercase letters a passcode must contain.</td>
</tr>
<tr>
<td><strong>Minimum number of non-alphabetic characters</strong></td>
<td>Specifies the minimum number of non-alphabetic characters (for example &amp; or !) a passcode must contain.</td>
</tr>
<tr>
<td><strong>Minimum number of uppercase letters</strong></td>
<td>Specifies the minimum number of uppercase letters a passcode must contain.</td>
</tr>
<tr>
<td><strong>Minimum number of numbers</strong></td>
<td>Specifies the minimum number of numbers a passcode must contain.</td>
</tr>
<tr>
<td><strong>Minimum number of special characters</strong></td>
<td>Specifies the minimum number of special characters (for example !&quot;$%&amp;/()=.;_;@&lt;&gt;) a passcode must contain.</td>
</tr>
</tbody>
</table>

### Restrictions

In this configuration, you can define restrictions for devices. You can only add one **Restrictions** configuration within a profile.
<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow factory reset</td>
<td>If you deactivate this option, users cannot reset their devices to factory state.</td>
</tr>
<tr>
<td>Allow settings changes</td>
<td>If you deactivate this option, users cannot change settings on the device. Depending on individual devices the settings icon is removed.</td>
</tr>
<tr>
<td>Allow backup</td>
<td>If you deactivate this option, users cannot create system backups. Google backup is deactivated. Other backup methods (for example Sophos Mobile Control backups) remain active.</td>
</tr>
<tr>
<td>Allow Bluetooth</td>
<td>If you deactivate this option, Bluetooth is disabled on the device.</td>
</tr>
<tr>
<td>Allow camera</td>
<td>If you deactivate this option, cameras are completely disabled on the device.</td>
</tr>
<tr>
<td>Allow clipboard</td>
<td>If you deactivate this option, users cannot copy any contents to the clipboard.</td>
</tr>
<tr>
<td>Allow NFC</td>
<td>If you deactivate this option, NFC (near field communication) is disabled on the device.</td>
</tr>
<tr>
<td>Allow screen capture</td>
<td>If you deactivate this option, users cannot take a screenshot of the display.</td>
</tr>
<tr>
<td>Allow SD card</td>
<td>If you deactivate this option, SD cards cannot be used in devices. SD cards are deactivated.</td>
</tr>
<tr>
<td>Allow USB debugging</td>
<td>If you deactivate this option, USB debugging is disabled on the device.</td>
</tr>
<tr>
<td>Allow USB</td>
<td>If you deactivate this option, the USB mass storage mode and the USB media player are disabled on the device.</td>
</tr>
<tr>
<td>Allow WiFi tethering</td>
<td>If you deactivate this option, WiFi tethering is disabled on the device.</td>
</tr>
<tr>
<td>Allow USB tethering</td>
<td>If you deactivate this option, USB tethering is disabled on the device.</td>
</tr>
<tr>
<td>Allow Bluetooth tethering</td>
<td>If you deactivate this option, Bluetooth tethering is disabled on the device.</td>
</tr>
</tbody>
</table>
Exchange ActiveSync

In this configuration, you can define user settings for your Microsoft Exchange Server. You can add multiple Exchange ActiveSync configurations.

<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>In this field, enter an account name.</td>
</tr>
<tr>
<td>Server address</td>
<td>In this field, enter the address of the Microsoft Exchange Server.</td>
</tr>
<tr>
<td>Domain</td>
<td>In this field, enter the domain for this account.</td>
</tr>
<tr>
<td>User</td>
<td>In this field, enter the user for this account.</td>
</tr>
<tr>
<td>Email address</td>
<td>In this field, enter the email address of the account.</td>
</tr>
<tr>
<td>Password</td>
<td>In this field, enter the password for this account.</td>
</tr>
<tr>
<td>Synchronization period in days</td>
<td>In this field, select the time period for email synchronization. This is the number of days emails are synchronized for. If you specify a time period here, not all emails are synchronized to the inbox on the mobile device, but only the emails from within the specified period. You can select the following synchronization periods:</td>
</tr>
<tr>
<td></td>
<td>■ One day</td>
</tr>
<tr>
<td></td>
<td>■ Three days</td>
</tr>
<tr>
<td></td>
<td>■ One week</td>
</tr>
<tr>
<td></td>
<td>■ Two weeks</td>
</tr>
<tr>
<td></td>
<td>■ One month</td>
</tr>
<tr>
<td>Synchronization interval</td>
<td>In this field, select the interval between email synchronization processes:</td>
</tr>
<tr>
<td></td>
<td>■ Never</td>
</tr>
<tr>
<td></td>
<td>■ 5 minutes</td>
</tr>
<tr>
<td></td>
<td>■ 10 minutes</td>
</tr>
<tr>
<td></td>
<td>■ 15 minutes</td>
</tr>
</tbody>
</table>
Setting/field | Description
--- | ---
30 minutes | 
1 hour | 
Sender | In this field, enter a sender name for this account. All emails sent with this account use this sender name.
SSL | Make sure that this option is selected, to send all communication through SSL (Secure Socket Layer).
Default account | Select this option to define the account as the default email account.
Allow all certificates | Select this option to allow all certificates in transfer processes from the email server.
Client certificate | In this field, select the client certificate for the connection to ActiveSync.

WiFi
In this configuration, you specify settings for connecting to WiFi networks. You can add multiple WiFi configurations.

Setting/field | Description
--- | ---
SSID | In this field, enter the ID of the wireless network.
Security type | In this field, you select the security type of the WiFi network:
None | 
WEP | 
WPA | 
EAP/PEAP | 
EAP/LEAP | 
EAP/TLS | 
EAP/TTLS |
### Setting/field

<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
</tr>
</thead>
</table>
| EAP/FAST      | If you select the personal settings WEP or WPA, a **Password** field is displayed. Enter the relevant password. If you select the EAP settings, the fields **Identity**, **Anonymous Identity** and **Password** are displayed. Enter the required EAP information. If you select the EAP setting EAP TTLS, the field **Phase 2 Authorization** is displayed in addition. Select the type of authorization:  
  ■ PAP  
  ■ CHAP  
  ■ MSCHAP  
  ■ MSCHAPv2 |

### VPN

In this configuration, you can define VPN settings for network connections. You can add multiple VPN configurations.

<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection name</td>
<td>In this field, enter the name of the connection shown on the device.</td>
</tr>
<tr>
<td>Server</td>
<td>In this field, enter the host name or the IP address of the server.</td>
</tr>
</tbody>
</table>
| Connection type | In this field, select the connection type:  
  ■ IPsec (PSK)  
    If you select this type, the fields **User**, **Password** and **IPsec (PSK)** are displayed. Enter the user and password. In the **IPsec (PSK)** field, enter the pre-shared key for authentication.  
  ■ IPsec (Certificate)  
    If you select this type, the fields **Client certificate**, **Root certificate**, **User** and **Password** are displayed. In the fields **Client certificate** and **Root certificate**, select the relevant certificates. In addition, enter the **User** and the relevant **Password**. |
**Root certificate**

In this configuration, you can upload a root certificate for devices. You can add multiple **Root certificate** configurations. In the **File** field, browse for the relevant certificate and click **Upload**. The name of the certificate is shown in the **Certificate name** field.

**Note:** The certificate you upload here is only available for this profile. If you require certificates in other profiles, you have to upload them again.

**Client certificate**

In this configuration, you can upload a client certificate to devices. You can add multiple **Client certificate** configurations. In the **File** field, browse for the relevant certificate and click **Upload**. The name of the certificate is shown in the **Certificate name** field. Enter the **Password** for the selected certificate.

**Note:** The certificate you upload here is only available for this profile. If you require certificates in other profiles, you have to upload them again.

### 17.3 Upload templates for Windows Mobile profiles

You can use templates to create Windows Mobile profiles. To do so, you need to upload the templates provided by Sophos to the web console.

1. In the web console, go to **Configurations** and click **Profile templates** under **Windows Mobile**. The **Profile template** view is displayed.
2. Click the **Create new template** button. The **Edit template** view is displayed.
3. Under **Operating systems**, select the operating system the template should apply to.
4. Browse for the template supplied by Sophos and click **Upload**.
5. Click the **Save** button.

The template is available for creating profiles for Windows Mobile devices. It is displayed in the **Profile template** view.

### 17.4 Create profiles for Windows devices

1. In the web console, go to **Configurations**, and click **Profiles** under **Windows Mobile**. The **Profiles** view is displayed.
2. Click the **Create new profile** button.
   The **Select profile template** view is displayed.
3. Select the template to be used for the profile and click **Next**.

The **Edit profile** view is displayed.

4. Enter a **Name** and a **Version** for the new profile.

5. Under **Operating systems**, select the operating system the profile should apply to.

6. In the profile settings displayed, click on the individual settings and enter any required information. Under **Send settings**, select **true** or **false** and click **Apply**.

   **Note:** Make sure that you click **Apply** for each setting. Otherwise your settings will be lost.

7. After you have made your changes, click the **Save** button.

The profile is available for transfer. It is displayed in the **Profiles** view.

### 17.5 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_%`

**Device property placeholder:**

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

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

### 17.6 Transfer profiles

1. In the web console menu bar, go to **Configurations** and click **Transfer** under the required mobile device type: **Apple iOS**, **Android** or **Windows Mobile**.

   The **Select device(s)** view is displayed.

2. In this view, you can:

   - Select individual devices you want to transfer the profile to.
   - Click the **Group selection** button, to open the **Select device group(s) view** and select one or several device groups for transferring the profile.

3. After you have made your selection, click **Next**.

   The **Select profile** view is displayed.
4. Select the profile you want to transfer and click **Next**.
   The *Set execution date* view is displayed.

5. Under *Scheduled date*, select **Now** or specify a **Date** and **Time** for the execution of this task.
6. Click the **Finish** button.
   The *Task view* is shown.

The profile is transferred to the selected device(s) at the specified date and time.

### 17.7 Download iOS and Android profiles from the web console

You can download iOS and Android profiles that you have configured in the web console. This is for example useful if you need to pass the defined settings on to Sophos Support.

1. In the web console menu bar go to **Configurations** and click **Profiles** under **Apple iOS** or **Android**.
2. Click the **Show** magnifier icon next to the required profile.
   The *Show profile* view is displayed.

3. Click the **Download** button.
   A download dialog is displayed.

4. Download the profile to a location of your choice.
   iOS profiles are saved as .config files and Android profiles as .xml files.
18 Working with task bundles

By using task bundles 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 Apple iOS devices).

You can also include wipe commands in task bundles to automatically wipe non-compliant (for example jailbroken or rooted) devices. For further information, see Configure compliance settings (section 12).

18.1 Create task bundles

1. In the web console menu bar, go to Task bundles and click Bundles.  
   
   The Task bundles view is displayed.

2. Click the Create new task bundle button.  
   
   The Edit task bundle view is displayed.

3. Enter a Name and a Version for the new task bundle.

4. Under Operating systems, select the operating systems the new task bundle applies to.

5. Under Tasks, click the Create new task button.  
   
   The Select type view is displayed.

6. Select the task type and click Next.  
   
   The next view depends on the task type you have selected. For example, if you have selected the type Install a software package, the Select package view is displayed.

7. Follow the wizard steps to add the required task.

8. Repeat this procedure to add further tasks. When adding new tasks you can specify your own meaningful task names. These task names are shown during installation in the Self Service Portal. You can set the order for installation for selected tasks by using the sort arrows on the right-hand side of the Tasks list.

9. After you have added all required tasks to the task bundle, click the Save button in the Edit task bundle view.  
   
   The task bundle is available for transfer. It is displayed in the Task bundles view.
18.2 Duplicate task bundles

Since creating a task bundle can be time-consuming, you can duplicate finished task bundles. This function is helpful, if several extensive task bundles with similar tasks are required. Then only a few tasks need to be deleted or added.

**Note:** You can only duplicate task bundles, if they are not edited at the same time. Copies are named “Copy of” plus the name of the original. You can rename the bundles according to your requirements.

1. In the web console menu bar, go to Task bundles and click Bundles.
   The Task bundles view is displayed.
2. Go to the task bundle you want to duplicate and click the Show magnifier icon.
   The Show task bundle view is displayed.
3. Click the Duplicate this task bundle button.
   The task bundle is duplicated and shown in the Task bundles view. You can now edit the duplicated task bundle as required. To edit the task bundle, click the Edit pencil icon next to it.

18.3 Transfer task bundles

1. In the web console menu bar, go to Task bundles and click Transfer.
   The Select device(s) view is displayed.
2. In this view, you can:
   - Select individual devices you want to transfer the task bundle to.
   - Click the Group selection button, to open the Select device group(s) view and select one or several device groups for transferring the task bundle.
3. After you have made your selection, click Next.
   The Select task bundle view is displayed.
4. Select the task bundle to be transferred and click Next.
   The Set execution date view is displayed.
5. Under Scheduled date, select Now or specify a Date and Time for the execution of this task.
6. Click the Finish button.
   The Task view is shown.

The task bundle is transferred to the selected device(s) at the specified date and time.
19 Working with command bundles

Note: Command bundles are only available for Android and Windows Mobile devices.

By using command bundles, you can bundle various commands to configure many different functions with only one transfer. This is especially helpful, if many devices are to be configured the same way.

Note: Improperly used commands may lock or even damage 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.

19.1 Create command bundles

1. In the web console menu bar, go to Command bundles and click Bundles.
   The Command bundles view is displayed.

2. Click the Create new bundle button.
   The Edit command bundle view is displayed.

3. Enter a Name and a Version for the new command bundle. These two fields are mandatory.
4. Under Operating systems, select the compatible operating systems for the new command bundle.
5. Under Commands, click the Create new command button.
   The Select command view is displayed.

   Note: Standard commands are supported on all available platforms. Other commands are only supported on specific platforms. The columns AND (Android) and WIN (Windows Mobile) next to the commands indicate for which platform(s) the commands are available. If you select various platforms and add a platform-specific command, devices that do not support the specific function refuse the command.

6. Select the command you want to add and click Next.
   The Edit command view is displayed.

7. Enter the required parameters for the command and click the Apply button.
   The Edit command bundle view is displayed. The new command is shown under Commands.

8. Add further commands as required. You can set the order for installation for selected commands by using the sort arrows on the right-hand side of the Commands list

9. After you have added all required commands click the Save button.
   The command bundle is available for transfer. It is displayed in the Command bundles view.
19.1.1 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 NotifyDelay</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>

19.2 Duplicate command bundles

Since creating a command bundle can be time-consuming, you can duplicate finished command bundles. This function is helpful, if several extensive command bundles with similar commands are required. Then only few commands need to be deleted or added.

**Note:** You can only duplicate command bundles, if they are not edited at the same time. Copies are named “Copy of” plus the name of the original. You can rename the bundles according to your requirements.

1. In the web console menu bar, go to **Command bundles** and click **Bundles**.
   
   The **Command bundles** view is displayed.

2. Go to the command bundle you want to duplicate and click the **Show** magnifier icon.
   
   The **Show command bundle** view is displayed.

3. Click the **Duplicate this bundle** button.
The command bundle is duplicated and shown in the Command bundles view. You can now edit the duplicated command bundle as required. To edit the command bundle, click the Edit pencil icon displayed next to it.

19.3 Transfer command bundles

1. In the web console menu bar, go to Command bundles and click Transfer.

   The Select device(s) view is displayed.

2. In this view, you can:
   - Select individual devices you want to transfer the command bundle to.
   - Click the Group selection button, to open the Select device group(s) view and select one or several device groups for transferring the command bundle.

3. After you have made your selection, click Next.

   The Select command bundle view is displayed.

4. Select the command bundle to be transferred and click Next.

   The Set execution date view is displayed.

5. Under Scheduled date, select Now or specify a Date and Time for the execution of this task.

6. Click the Finish button.

   The Task view is shown

The command bundle is transferred to the selected device(s) at the specified date and time.
20 Configure Self Service Portal use for end users

With the Self Service Portal you can reduce IT efforts by allowing end users to register their own devices and carry out other tasks without having to contact the helpdesk. The use of the Self Service Portal is supported for the following platforms:

- Android
- Apple iOS
- Windows Mobile

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

In the web console, you can configure settings for the use of the Self Service Portal, for example for which platforms registration through the Self Service Portal should be active or which functions should be available in the Self Service Portal. You can also manage the users of the Self Service Portal.

20.1 Create Self Service Portal groups with internal user management

Self Service Portal configurations are applied to groups of Self Service Portal users. With internal user management, you can create Self Service Portal groups and assign users to them. For further information on user management, see Manage Self Service Portal users (section 20.3).

Note: Internal user management is only available for a customer, if it has been activated by the super administrator. For further information, see the Sophos Mobile Control super administrator guide. This does not apply to Sophos Mobile Control as a Service. Super administrators are not supported in Sophos Mobile Control as a Service. In this case customers are predefined and internal user management is used.

To create a Self Service Portal group:

1. In the Dashboard view, click the Internal user management button.
   
   The Show users view is displayed.

2. Click the Show groups button.
   
   The Show groups view is displayed.

3. Click the Create new user group button.
   
   The Edit group view is displayed.

4. In the Name field, enter a name for the new Self Service Portal user group.

5. Click the Save button.
The new Self Service Portal user group is displayed in the **Show groups** view. When you create new users, you can assign them to the group. When you define Self Service Portal settings, you can select the group to assign the settings to it.

### 20.2 Configure Self Service Portal settings

1. In the **Dashboard** view, click the **Settings** button.
   
   The **Settings** view is displayed.

2. Go to the **Self Service Portal** tab.

3. First you configure the group settings, for example the device groups that SSP-registered devices will be added to and the task bundle that will be deployed on the devices.

   If you use LDAP user management, you can assign phones to groups and profiles based on group membership.

   **Note:** LDAP user management has to be configured for the relevant customer in customer management. For information on how to configure LDAP user management for a customer, refer to the *Sophos Mobile Control super administrator guide*. This does not apply to Sophos Mobile Control as a Service. In this case customers are predefined and internal user management is used. Super administrators are not supported in Sophos Mobile Control as a Service.

   a) Under **Group** settings, click the **Add** button.
   
   The **Edit SSP configuration** view is displayed.

   b) Enter a **Name** for the Self Service Portal configuration group.

   c) In the **LDAP group** field, enter the Self Service Portal Group you have defined in the internal user management or the Active Directory group with the full LDAP path or with wildcards. You can use an asterisk (*) as the first, the last or the only sign in this field to specify several groups. For example: Enter Dev* to specify all group names that start with "Dev". Enter * to specify all available groups.

   d) Under **Platform** select the platforms that should be available in the Self Service Portal.

   e) Under **Add to device group**, select the group the device should be added to.

   **Note:** In the web console, a **Default** device group is available. If you have not defined your own device groups yet, you can add devices to this group. For further information, see *Create device groups* (section 14.1).

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

   **Note:** You must create the task bundle in the web console first. If you have not created a task bundle yet, update the Self Service Portal settings afterwards. For further information on how to create a task bundle, see *Working with task bundles* (section 18). For further information on the requirements for a task bundle that is to be used for provisioning through
the Self Service Portal, see the Sophos Mobile Control startup guide or the Sophos Mobile Control as a Service startup guide.

g) Click the **Apply** button.

4. Under **Agreement text**, you can configure a mobile policy, disclaimer or agreement text that is displayed as a first step when end users register their devices. Users have to confirm that they have read this text to be able to continue.

Simple HTML formatting tags are supported for the text. The text will be displayed in the relevant browser accordingly.

5. Under **Post install text**, you can configure a 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.

Simple HTML formatting tags are supported for the text. The text will be displayed in the relevant browser accordingly.

6. In the **Maximum number of devices** field, select 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.

7. Under **Available SSP functions**, select the functions that 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 may require additional actions with helpdesk assistance. The functions supported vary according to mobile device type (platform). For a matrix of the features supported for individual device types, refer to the Sophos Mobile Control technical guide. You can select the following functions:

- **Locate device**
  
  With this function users can locate Android or iOS devices if they are lost or stolen.

- **Lock device**
  
  With this function users can lock their devices if they are lost or stolen.

- **Reconfigure device**
  
  With this function users can reconfigure their devices, if Sophos Mobile Control has been removed from the device, but the device is still registered.

- **Show compliance violations**
  
  With this function users can view the compliance violations for all devices registered for them in the Self Service Portal.

- **Refresh data**
  
  With this function users can manually synchronize their devices with the Sophos Mobile Control Server. This is useful, for example if the device has been switched off for a longer period of time and therefore has not been synchronized with the server. In this case, the device may be non-compliant (depending on the compliance settings configured) and needs to be synchronized with the server to make it compliant again.
- **Wipe device**
  With this function users can reset their registered devices to their factory settings if devices are lost or stolen. All data on the device is deleted.

- **Decommission device**
  With this function users can decommission devices that they no longer use. This is useful, for example if the number of devices users can register through the Self Service Portal is limited.

- **Delete unmanaged device**
  With this function users can delete decommissioned devices. This is for example useful to free up licenses.

- **Activate Sophos Mobile Control app**
  With this function users of Apple iOS devices can activate the Sophos Mobile Control app on their devices after installation.

  **Note:** This is a necessary step for setting up Sophos Mobile Control on Apple iOS devices. To ensure that activation works, the app has to be opened once before on the device. Select this function to enable users of Apple iOS devices to register and provision their devices through the Self Service Portal.

8. After you have configured all necessary settings in the **Self Service Portal** tab, click the **Save** button.

9. Go to the **SSP welcome email** tab. In this tab, you configure the welcome email to be sent to Self Service Portal users to inform them about their logon credentials.

  **Note:** This mail is only sent for internal Self Service Portal users managed by internal user management, see **Manage Self Service Portal users** (section 20.3).

10. In the **Originator** field, enter the email sender address. In the **Subject** field, enter an email subject, for example "Welcome to the Sophos Mobile Control Self Service Portal".

11. In the text field, predefine the email content. The following placeholders are available and will be replaced by the corresponding values in the email:

  - `_RESET_TOKEN_LINK_`
  - `_LOGINNAME_`
  - `_FIRSTNAME_`
  - `_LASTNAME_`

  Use the placeholder `_RESET_TOKEN_LINK_` to include a link for generating a password for the user. This link is required for providing the user with a password.

12. After you have configured the welcome email, click the **Save** button.

  **Note:** As a super administrator, you can also define the default customer for the login of end users at the Self Service Portal. For further information, refer to the **Sophos Mobile Control super administrator guide**. Note that this does not apply to Sophos Mobile Control as a Service. Super administrators are not supported in Sophos Mobile Control as a Service.
20.3 Manage Self Service Portal users

Sophos Mobile Control offers different methods for managing Self Service Portal users.

**Note:** The method used is customer-specific and is defined when the customer is created. For further information, see the *Sophos Mobile Control super administrator guide*. This does not apply to Sophos Mobile Control as a Service. In this case customers are predefined. Super administrators are not supported in Sophos Mobile Control as a Service.

- **Internal user management**
  
  With internal user management you can create users by adding them manually in the web console or by importing them in a .csv file.

- **LDAP user management**
  
  With LDAP user management you can assign devices to groups and profiles based on Active Directory/LDAP membership. For further information, see the *Sophos Mobile Control super administrator guide*.

20.3.1 Create Self Service Portal users with internal user management

**Prerequisite:** Internal user management has been enabled for the customer you are logged in to. For on-premise installations this is done in customer management by the super administrator. For further information, see the *Sophos Mobile Control super administrator guide*. This does not apply to Sophos Mobile Control as a Service. In this case customers are predefined. Super administrators are not supported in Sophos Mobile Control as a Service.

1. In the **Dashboard** view, click the **Internal user management** button.
   
   The **Show users** view is displayed.

2. Click the **Create new user** button.
   
   The **Edit user** view is displayed.

3. In the **Edit user** view, specify the following settings:
   
   a) Make sure that the **Send welcome mail** field is selected. This field is shown, if you have configured a welcome mail in the ** SSP welcome mail** tab in **Settings**, see *Configure Self
**Service Portal settings** (section 20.2). If the field is not shown, configure a welcome mail first. The welcome mail has to include all required login credential information.

b) **User name**

c) **Last name**

d) **First name**

e) **Email**

f) **Phone number** (optional)

g) **Groups**

4. Click the **Save** button.

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.

From the **Show users** view, you can view the user details, edit them and delete users.

## 20.3.2 Import Self Service Portal users with internal user management

With internal user management, you can add new Self Service Portal 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.

**Prerequisite:** Internal user management has been enabled for the customer you are logged in to. For further information, see the *Sophos Mobile Control super administrator guide*. This does not apply to Sophos Mobile Control as a Service. Super administrators are not supported in Sophos Mobile Control as a Service. In this case customers are predefined and internal user management is used.

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

   The **Show users** view is displayed.

2. Click the **Import users** button.

   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 shown, if you have configured a welcome mail in the **SSP welcome mail** tab in **Settings**, see *Configure Self Service Portal settings* (section 20.2). If the field is not shown, 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 **Finish** button.

   The users are imported and displayed in the **Show users** view.

   From the **Show users view**, you can view the user details, edit them and delete users.
21 Administering devices in the Inventory

The Inventory is the central module for administering devices. With the Inventory, you can keep track of all registered devices and device groups and carry out a number of administrative tasks. After adding devices to Sophos Mobile Control you can for example:

- View and edit device details.
- Allow or disallow email access for devices.
  
  **Note:** This function is not available for Sophos Mobile Control as a Service.
- Lock or unlock devices remotely.
- Reset the passcode/passwords of devices.
- Wipe the device remotely in case of loss or theft.
- Decommission devices (Android and iOS).
- Delete devices.

For an overview of all available functions with the corresponding function buttons, see *Carry out administrative tasks* (section 21.4).

21.1 View devices

1. In the web console menu bar, go to Inventory and click Devices.

   The Devices view is displayed with all devices registered with Sophos Mobile Control for this customer.

2. Go to the required device and click the magnifier icon.

   The Show device view is displayed for the selected device.

21.1.1 The Show device view

In the Show 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 Private 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.

In addition, the Show device view shows detailed device information in the following tabs. The tabs and information shown depend on the mobile device type (platform).

- 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 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. When you edit a device, 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 device. Click the **Show** (magnifier) icon next to a compliance violation to view the violation **History**.

  You can update the compliance information shown for the device from the **Compliance violations** tab. 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 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. In addition any additional space that may be required is shown. This additional space may be required for downloads, configurations, settings and so on.

  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 iOS devices by clicking the **Delete** icon next to the relevant app.

- **Installed profiles (iOS and Android)**
  Shows the profiles installed on devices.
**Note:** For Android devices, profiles are displayed as of Sophos Mobile Control client version 3.0.

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

This tab also lists provisioning profiles.

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

  **Note:** System software cannot be removed from the device.

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

- **SMSec results (Android)**
  
  This tab is only available, if the Sophos Mobile Security functionality is available for the customer you are logged in to. It shows the results of the last Sophos Mobile Security scan performed on the device. Sophos Mobile Security is a security app for Android phones and tablets that protects devices from malicious apps and assists end users in detecting apps permissions that could be a security risk. The app can be managed from the Sophos Mobile Control web console. For further information, see *Managing Sophos Mobile Security from Sophos Mobile Control* (section 26).

From the **Show device** view, you can directly switch to the **Edit device** view. To edit the device you are viewing, click the **Edit** button.

### 21.2 Use filters in the Inventory

By using filters you can restrict the number of items shown in lists according to defined criteria. To apply a filter, click the **Filter** button (magnifier icon) in the web console header. The filter is opened and you can specify the filter criteria you want to apply.

In the **Inventory**, you can use the following filters:

- Device filters
- Device group filters

#### 21.2.1 Use the device filter

With the device filter, you can filter device lists.

**Note:** The filter is not only valid for the function currently displayed, but for all functions where items of this type are listed.
To use the device filter:

1. In the web console menu bar, go to **Inventory** and select **Devices**.
   
   The **Devices** view is displayed.

2. Click the **Filter** button (magnifier icon) in the web console header.

   The **Device filter** dialog is displayed with the status **Filter is not active**.
3. In the **Device filter** dialog, you can select the following filter options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Filter according to device name. You can enter a device name or part of a device name.</td>
</tr>
<tr>
<td>IMEI</td>
<td>Filter according to IMEI.</td>
</tr>
<tr>
<td>Phone number</td>
<td>Filter according to phone number.</td>
</tr>
<tr>
<td>Managed</td>
<td>Select <strong>Yes</strong>, to only show provisioned devices. Select <strong>No</strong>, to only show devices that have not been provisioned.</td>
</tr>
<tr>
<td>Compliant</td>
<td>Select <strong>Yes</strong>, to only show compliant devices. Select <strong>No</strong>, to only show non-compliant devices.</td>
</tr>
<tr>
<td>Owner</td>
<td>Filter according to ownership. Select <strong>Corporate device</strong> or <strong>Private device</strong>.</td>
</tr>
<tr>
<td>Device wiped</td>
<td>Select <strong>Wiped</strong>, to show all wiped devices. Select <strong>Not wiped</strong>, to show all non-wiped devices.</td>
</tr>
<tr>
<td>Exchange Active Sync</td>
<td>Select <strong>Allowed</strong>, to show all devices for which email access is allowed. Select <strong>Not allowed</strong>, to show all devices for which email access is not allowed.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Managing access to corporate email is not supported in Sophos Mobile Control as a Service. If you use Sophos Mobile Control as a Service, the <strong>Exchange Active Sync</strong> field is not available.</td>
</tr>
<tr>
<td>Package</td>
<td>Filter according to software package. In the fields <strong>Name</strong>, <strong>Identifier</strong> and <strong>Version</strong>, enter the details for the relevant software package. In the dropdown list, select <strong>installed</strong> to show all devices with the package installed. Select <strong>not installed</strong> to show all devices on which the package is not installed.</td>
</tr>
<tr>
<td>Device group</td>
<td>Filter according to device group devices are assigned to.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Filter according to operating system. Here you can deselect devices equipped with a specific operating system.</td>
</tr>
<tr>
<td>Device property</td>
<td>Filter according to a specific device property. Enter the <strong>Name</strong> and the <strong>Value</strong> of the device property.</td>
</tr>
</tbody>
</table>

4. After you have selected the required criteria, click **Filter**.
The filter is activated and the list of devices is reloaded. The Filter button in the web console header changes its color from blue to pink to indicate that the filter is active. A Reset button is available in the header for resetting the filter. The status of the device filter in the Device filter dialog changes to Filter is active.

Note: Remember to reset filters manually when they are no longer needed. Otherwise lists or reports may not include the results you expect.

21.2.2 Use the device group filter

With the device group filter, you can restrict the items displayed in the device group lists.

Note: The filter is not only valid for the function currently displayed, but for all functions where items of this type are listed.

To use the device group filter:

1. In the web console menu bar, go to Inventory and select Device groups.
   The Device groups view is displayed.

2. Click the Filter button (magnifier icon) in the web console header.
   The Group filter dialog is displayed with the status Filter is not active.

3. Enter the Name of the device group and click Filter.
   The filter is activated and the list of device groups is reloaded. The Filter button in the web console header changes its color from blue to pink to indicate that the filter is active. A Reset button is available in the header for resetting the filter. The status of the device group filter in the Group filter dialog changes to Filter is active.

Note: Remember to reset filters manually when they are no longer needed. Otherwise lists or reports may not include the results you expect.

21.3 Edit devices

1. In the web console menu bar, go to Inventory and click Devices.
   The Devices view is displayed with all devices registered with Sophos Mobile Control for this customer.

2. Go to the required device and click the Edit pencil icon.
   The Edit device view is displayed for the selected device.

3. Make the necessary changes (for example install or remove software in the Installed software tab) and click the Save button.
   Your changes are applied to the edited device.
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.

### 21.3.1 Add LDAP link to a device

You can add an LDAP link to individual devices when you create a device from a template or by editing a device.

1. In the web console menu bar, go to Inventory and click Devices.
   The Devices view is displayed with all devices registered with Sophos Mobile Control for this customer.
2. Go to the required device and click the Edit pencil icon.
   The Edit device view is displayed for the selected device.
3. Click the Add LDAP link button.
   The Enter LDAP search parameters view is displayed.
4. In the fields Directory server, Root node, Common name (CN) and Email address, enter the relevant search criteria and click Next.
   The Select data set view is displayed.
5. Select the required data set and click Next.
   The Select detail fields to use view is displayed.
6. Select the required Email address and the User name and click Apply.
   The Edit device view is displayed again.
7. Click the Save button.

Note: The device is shown in the Self Service Portal for the relevant user.

### 21.3.2 Define custom properties for devices

You can define custom properties, for example system processes, for individual devices when you create a device from a template or edit a device.

1. In the web console menu bar, go to Inventory and click Devices.
   The Devices view is displayed with all devices registered with Sophos Mobile Control for this customer.
2. Go to the required device and click the Edit pencil icon.
   The Edit device view is displayed for the selected device.
3. Go to the **Custom properties** tab and click the **Create new property** button. The **Edit property** view is displayed.

4. Enter a **Name** and a **Value** for the new custom property.
   - For example, for system processes:
     - Name: SystemProcess2
     - Value: Internet;10008d39,BrowserNG.exe
   - For system processes the **Name** is always "SystemProcess" followed by an index starting at "0". Spaces are not allowed. When you create another process, use the subsequent index, for example "SystemProcess1", "SystemProcess2".
   - The syntax for **Value** is: <display name>;<UID of the process>,<name of the process>.
   - You can also combine multiple processes, for example: <display name>;<UID of the process>,<name of the process>;<UID of the process>,<name of the process>.

5. Click the **Apply** button.
   - The new property is displayed in the **Edit device** view in the **Custom properties** tab.

6. Click the **Save** button.

### 21.4 Carry out administrative tasks

The web console offers a number of function buttons in the **Show device** and the **Edit device** view to carry out administrative tasks.

To carry out tasks on an individual device, open the **Show device** or **Edit device** view for the required device (see **View devices** (section 21.1) and **Edit devices** (section 21.3)) and click on the function button for the required task.

**Note:** The function buttons available depend on mobile device type (platform), configuration and device view (**Show device** or **Edit device**).

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🌐</td>
<td>Click this button to set the name and the IMEI of the specific device in the device filter, see <strong>Use the device filter</strong> (section 21.2.1).</td>
</tr>
<tr>
<td>📊</td>
<td>Click this button to view all tasks for this device.</td>
</tr>
<tr>
<td>Button</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| ![Red Checkmark] | This button is available for devices where the registration through the Self Service Portal has failed. Click this button to 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. |
| ![Green Plus] | Click this button to add an Active Directory link to the device |
| ![Red X] | Click this button to remove an Active Directory link to the device. |
| ![Refresh] | Click this button to refresh device data. |
| ![Traffic Counters] | Click this button to open the traffic counter details for the device, see *View data traffic* (section 23.3). |
| ![Email Denied] | Indicates that email access is denied.  
An additional icon on the button indicates whether email access was denied  
- manually 🗣️ or  
- automatically 🤖.  
Click this button, to allow email access or set it to automatic mode.  

**Note:** Managing access to corporate email is not supported in Sophos Mobile Control as a Service. If you use Sophos Mobile Control as a Service, this button is not available. |
| ![Email Allowed] | Indicates that email access is allowed.  
An additional icon on the button indicates whether email access was allowed  
- manually 🗣️ or  
- automatically 🤖.  
Click this button, to deny email access or set it to automatic mode. |
<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
</table>
| ![Info Icon] | Note: Managing access to corporate email is not supported in Sophos Mobile Control as a Service. If you use Sophos Mobile Control as a Service, this button is not available. 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.  
Note: Managing access to corporate email is not supported in Sophos Mobile Control as a Service. If you use Sophos Mobile Control as a Service, this button is not available. |
| ![Lock Icon] | Click this button to lock the device remotely. |
| ![Unlock Icon] | Click this button to reset the passcode/password of a device.  
- For Apple iOS devices, the passcode/password is reset on the device and the user is prompted to define a new one.  
- For Android devices, you can replace the passcode/password with a new one. It must comply with the passcode/password rules. |
<p>| ![Trash Icon] | Click this button to delete all synchronization data of the device. The Sophos Mobile Control client needs to be reinstalled. |
| ![Trash Icon] | Click this button to wipe the device remotely if it is lost or stolen. The device is reset to its factory settings, all data are deleted. |
| ![Chat Icon] | Click this button to send a user-defined message to a specific device. If an iOS device has been bootstrapped and the Sophos Mobile Control app is installed, APNs messages are sent. If an Android device has been set up, GCM push messages are sent. |</p>
<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Locate Device" /></td>
<td>Click this button to locate an iOS or Android device.</td>
</tr>
</tbody>
</table>
| ![Restore Device](image) | Click this button to restore device data from backup. For further information on backups, see Back up devices (section 24).  
**Note:** This function is only available for Android and Windows Mobile devices. Backups are not supported for Sophos Mobile Control as a Service. |
| ![Delete Device](image) | Click this button to delete the device.  
**Note:** 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 you need to uninstall the client, you have to remove the Sophos Mobile Control client manually. |
| ![Activate Device](image) | Click this button, to activate the Sophos Mobile Control app on an iOS device after installation. This is a necessary step for setting up Sophos Mobile Control on Apple iOS devices. To ensure that activation works, the app has to be opened once before on the device. |
| ![Decommission Device](image) | Click this button to decommission an iOS or Android device, see Decommission devices (section 21.5).  
**Note:** This function is only available for Android and Apple iOS devices. |
| ![Scan Device](image) | This button is available when you have a license for managing the Sophos Mobile Security app from the Sophos Mobile Control web console. For further information, see Managing Sophos Mobile Security from Sophos Mobile Control (section 26).  
Click this button to start a Sophos Mobile Security scan on a specific device. |

**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.
21.5 Decommission devices

You can decommission managed Android and Apple iOS devices that will no longer be used, for example if a user gets a new device. This is useful, for example if you have limited the number of devices a user can register through the Self Service Portal.

1. In the web console menu bar, go to Inventory and click Devices.
   The Devices view is displayed with all devices registered with Sophos Mobile Control for this customer.

2. Go to the required device and click the Edit pencil icon.
   The Edit device view is displayed for the selected device.

3. Click the Device decommissioning button.
   A message is displayed prompting you to confirm that you want to decommission the device.

4. Click Yes.

   The device is decommissioned. 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 are removed.

   **Apple 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 received through Mobile Device Management are removed.

21.6 Device groups

Device groups are used to categorize devices. You assign devices to device groups when you add them to Sophos Mobile Control device management manually or by import. You can change the device group for a device by editing it. A device always belongs to exactly one device group. Device groups make administration easier as in most device management functions you can select a complete group or single devices.

**Note:** We recommend that you only group devices with the same operating system. This makes it easier to use groups for installations and other operating system specific tasks.

For information on how to create device groups, see *Create device groups* (section 14.1).
**Note:** If you delete a device group, the group's members are moved to another group that needs 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.
22 Viewing tasks in the web console

You can monitor all existing tasks for devices in the web console:

- The Task view shows all unfinished and failed tasks as well as the finished tasks of the last few days. The Task view is refreshed automatically, so you can watch the states of the tasks evolve.
- The Task history shows general information on a task from the Task view or the Task archive.
- The Task archive shows all tasks.

22.1 View unfinished, failed and latest finished tasks

1. In the web console menu bar, click Task view.

   The Task view is displayed. The State column shows the task status, for example Completely failed.

2. In the Refresh interval (in sec.) field, you can select how often the Task view is to be refreshed.

3. To view further details about a task, click the Show magnifier icon next to the required task.

   The Task history view is displayed. Besides general information on the task (for example Device, Package name and Creation date) 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 is available in the Task history.

4. If available, click the Details button to view the command to be executed by the device.

   The Commands view is displayed with the relevant commands. 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.

5. To return to the Task history view, click the Back button.

6. To manually retry failed tasks, click the Execute now button.

   Note: This button is only available for failed tasks. You can only retry tasks that have not failed completely.

22.2 View task archive

1. In the web console menu bar, click Task archive.

   The Task archive view is displayed. It shows all finished and failed tasks in the system.
2. In this view you can:
   ■ Click the **Reload** button to refresh the **Task archive** view.
   ■ Select tasks and click the **Delete selected** button to delete them from the archive.

22.3 **Use the task filter**

By using filters you can restrict the number of items shown in lists according to defined criteria. With the task filter, you can filter tasks displayed in both the task view and the task archive.

**Note:** The filter is not only valid for the function currently displayed, but for all functions where items of this type are listed.

To use the task filter:

1. In the web console menu bar, click **Task view** or **Task archive**.
   
   The **Task view/Task archive** view is displayed.

2. Click the **Filter** button (magnifier icon) in the web console header.
   
   The **Task filter** dialog is displayed with the status **Filter is not active**.

3. In the **Task filter** dialog, you can select the following filter options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Filter according to device name.</td>
</tr>
<tr>
<td>Package</td>
<td>Filter according to package name</td>
</tr>
<tr>
<td>Created by</td>
<td>Filter according to the name of the user who has created the tasks.</td>
</tr>
<tr>
<td>State</td>
<td>Filter according to task state. You can select:</td>
</tr>
<tr>
<td></td>
<td>■ Scheduled</td>
</tr>
<tr>
<td></td>
<td>■ In progress</td>
</tr>
<tr>
<td></td>
<td>■ Successful</td>
</tr>
<tr>
<td></td>
<td>■ Failed</td>
</tr>
<tr>
<td>Group</td>
<td>Filter according to device group.</td>
</tr>
</tbody>
</table>

4. After you have selected the required criteria, click **Filter**.
The filter is activated and the list of devices is reloaded. The Filter button in the web console header changes its color from blue to pink to indicate that the filter is active. A Reset button is available in the header for resetting the filter. The status of the task filter in the Task filter dialog changes to Filter is active. In the dialog, a Reset button is available for resetting the filter.

Note: Remember to reset filters manually when they are no longer needed. Otherwise lists or reports may not include the results you expect.

22.4 Task icons

In the Task view and the Task archive, icons are used to categorize the tasks shown. These icons have the following meaning:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![installation_icon]</td>
<td>Installation</td>
</tr>
<tr>
<td>![uninstallation_icon]</td>
<td>Uninstallation</td>
</tr>
<tr>
<td>![activation_deactivation_icon]</td>
<td>Process activation/deactivation</td>
</tr>
<tr>
<td>![refresh_icon]</td>
<td>Explicit refresh of device data.</td>
</tr>
<tr>
<td>![message_icon]</td>
<td>Text message to device.</td>
</tr>
<tr>
<td>![profile_transfer_icon]</td>
<td>Windows Mobile profile transfer</td>
</tr>
<tr>
<td>![profile_transfer_icon]</td>
<td>iOS profile transfer</td>
</tr>
<tr>
<td>![command_bundle_icon]</td>
<td>Command bundle transfer</td>
</tr>
<tr>
<td>![task_bundle_icon]</td>
<td>Task bundle transfer</td>
</tr>
<tr>
<td>![bootstrap_icon]</td>
<td>Bootstrap</td>
</tr>
<tr>
<td>![command_icon]</td>
<td>Command transfer</td>
</tr>
<tr>
<td>![security_icon]</td>
<td>Windows Mobile security settings</td>
</tr>
</tbody>
</table>
## 22.5 Task states

The following table provides an overview on the task states indicated in the Task view and the Task archive.

<table>
<thead>
<tr>
<th>Color icon</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Accepted</td>
<td>The task has been created.</td>
</tr>
<tr>
<td></td>
<td>Retry</td>
<td>The task will be retried later.</td>
</tr>
<tr>
<td></td>
<td>Started</td>
<td>The task has been started.</td>
</tr>
<tr>
<td></td>
<td>In progress</td>
<td>The execution of the task is being prepared.</td>
</tr>
<tr>
<td></td>
<td>Sending notification</td>
<td>The client is being notified.</td>
</tr>
<tr>
<td></td>
<td>Waiting for delivery</td>
<td>The server is waiting for a confirmation of the notification by the client.</td>
</tr>
<tr>
<td></td>
<td>Notified</td>
<td>The client has received the notification.</td>
</tr>
<tr>
<td></td>
<td>Exported</td>
<td>The client has received the package and/or the commands.</td>
</tr>
<tr>
<td></td>
<td>Result evaluation started</td>
<td>The client has answered and the evaluation of the result has been started.</td>
</tr>
<tr>
<td></td>
<td>Result incomplete</td>
<td>The result evaluation showed that not all commands’ results have been received by now.</td>
</tr>
<tr>
<td></td>
<td>Successful</td>
<td>The package has been installed or the commands have been successfully executed.</td>
</tr>
<tr>
<td></td>
<td>Installed</td>
<td>The Sophos Mobile Control client has been installed successfully. The device is provisioned now.</td>
</tr>
<tr>
<td></td>
<td>Result evaluation failed</td>
<td>The result evaluation could not be executed.</td>
</tr>
<tr>
<td></td>
<td>Task partly failed</td>
<td>Not all commands of the task could be executed successfully.</td>
</tr>
<tr>
<td></td>
<td>Delayed</td>
<td>The task will be restarted later.</td>
</tr>
</tbody>
</table>

**Note:** For the initial provisioning of the Sophos Mobile Control client the task must finish with the state “installed”.

---

**Sophos Mobile Control**

102
<table>
<thead>
<tr>
<th>Color icon</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Failed (retry queued)</td>
<td>The task has failed and will be retried later.</td>
</tr>
<tr>
<td></td>
<td>Task failed</td>
<td>The task has failed and no further retries are queued.</td>
</tr>
<tr>
<td></td>
<td>Completely failed</td>
<td>The task has failed.</td>
</tr>
</tbody>
</table>
23 Reports

The Sophos Mobile Control web console offers different types of reports:

- A graphical report providing an overview of registered devices. This report is shown in the Reports view in the web console.
- A report containing detailed information on devices. This report is exported to a .csv file.
- A Traffic counter that shows the data traffic used for the current and the previous month in the web console.

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

23.1 Create graphical overview report on devices

You can create a graphical report on devices that shows statistical information on the registered devices for the relevant customer in pie charts.

1. In the web console Dashboard view, click the Reports button.

The Reports view is displayed. This view shows the following information in pie charts:

- Compliant/non-compliant devices
- Managed/non-managed devices
- Corporate/private devices
- Devices by operating system type
- Devices by operating system version per operating system type.

23.2 Export device information to a device report

1. In the web console menu bar, go to Inventory and click Devices.

The Devices view is displayed.

2. Click the Creates a device report (CSV file) button.

A file download dialog is displayed.

3. Select a file location and click Save.

The report is saved in a .csv file at the selected 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. For further information, see Import devices (section 14.3).

23.3 View data traffic

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

In the Traffic counter, the data traffic for the current and previous month is shown. It gives a rough overview of all devices. When a device reaches the configured limit, the server sends a text message or a message box including a warning message.

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

1. In the web console menu bar, click Traffic counter.

   The Traffic counter view is displayed. It shows an overview of the data traffic of all registered devices for the current and previous month.

   Note: In the Traffic counter view, several values are marked in red if traffic occurs. This provides a better overview on wanted and unwanted traffic. Therefore, WiFi 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 occurs.

2. To view the traffic counter details for a specific device, click on the device in the Traffic counter view.

   The Show traffic counter details view is displayed. It shows device information and an annual survey for the selected device.

3. In this view, you can:

   ■ Select between different traffic types, to restrict the display accordingly:
     ■ Show WiFi
     ■ Show GSM
     ■ Show GSM-Roaming

     Click Update to refresh the display accordingly.

   ■ Under Annual survey, click on a month to display the data for the selected month.
24 Back up devices

Note: Backup configuration is only available for Android and Windows Mobile devices. Backup configuration is not supported in Sophos Mobile Control as a Service.

You can configure backups for devices to back up text messages, bookmarks and user defined directory paths.

Note: Backups are platform-specific.

24.1 Configure device backups

1. In the web console menu bar, go to Backup and click Profiles.

The Backup configurations view is displayed.

2. Click the Create new package button.

The Edit backup configuration view is displayed.

3. Enter a Name and a Version for the new backup configuration.

4. Under Operating systems, select the operating system the backup configuration applies to.

5. Under Schedule, select the weekdays and time for backup creation.

6. Select the components that should be included in the backup:

a) Select SMS to include text messages.

b) Select Bookmarks of system browser to include bookmarks.

c) Under Paths to backup, click the Add Path button.

The Path view is displayed.

d) In the Path view, enter a path to be included in the backup, for example /files/. If required, select Recursive.

e) Under Files to backup (wildcards * possible), enter the files to be included in the backup and click Add.

The files are added in the text field below.

f) Click the Save button.

The path specified is shown under Paths to backup in the Edit backup configuration view.

7. Click the Save button.

The new backup configuration is displayed under Backup configurations. You can now transfer it to devices or device groups.
24.2 Transfer backup configurations

To make sure that devices are backed up, you need to transfer the backup configurations created to devices or device groups.

1. In the web console menu bar, go to Backup and click Transfer.
   The Select device(s) view is displayed.

2. The next step depends on whether you want to transfer the configuration to individual devices or device groups:
   ■ If you want to transfer the configuration to individual devices, select the required ones in the Select device(s) view and click Next.
   ■ If you want to transfer the configuration to device groups, click the Group selection button, select the required device group(s) in the Group selection view and click Next.
   The Choose backup configuration view is displayed.

3. Select the backup configuration you want to transfer and click Next.
   The Set execution date view is displayed.

4. Specify a Scheduled date for the transfer of the backup configuration.

5. Click the Finish button.
   The backup configuration is transferred to the selected device(s) or device group(s) at the scheduled date and time.

24.3 Restore data from backups

1. In the web console, go to Inventory and click Devices.

2. The Devices view is displayed.

3. Click the Show or Edit icon next to the device for which you want to restore data from backup.
   The Show device/Edit device view is displayed.

4. Click the Restore data from backup button.
   The Set execution date view is displayed.

5. Under Scheduled date, select Now or specify a Date and Time for the execution of this task.

6. Click the Finish button.
   The backed up data is restored on the selected device at the specified time.
25 Send messages to devices

From the web console, you can send user-defined messages to managed devices. After an iOS device has been bootstrapped and the Sophos Mobile Control app is installed, APNs messages are sent. After an Android device has been set up, GCM push messages are sent.

1. In the web console menu bar, click **Send Messages**.
   The **Select device(s)** view is displayed.

2. In this view, you can:
   - Select individual devices you want to send the message to.
   - Click the **Group selection** button, to open the **Select device group(s)** view and select one or several device groups to send the message to.

3. After you have made your selection, click **Next**.
   The **Enter message** view is displayed.

4. In the text field, enter the message you want to send. A character counter below the field counts from the number of available characters to 0. After 0 has been reached, you cannot enter any further characters. After you have entered the message, click **Next**.
   The **Set execution date** view is displayed.

5. Under **Scheduled date**, select **Now** or specify a **Date** and **Time** for the execution of this task.

6. Click the **Finish** button.

The message is sent to the selected device(s) at the specified date and time.

**Note:** You can also send messages to devices from the **Inventory**. For further information, see *Carry out administrative tasks* (section 21.4).
26 Managing Sophos Mobile Security from Sophos Mobile Control

Sophos Mobile Security is a security app for Android phones and tablets that protects devices from malicious apps and assists end users in detecting apps permissions that could be a security risk.

The Sophos Mobile Security management functionality is an optional Sophos Mobile Control module. In order to manage the Sophos Mobile Security app from Sophos Mobile Control, a license needs to be available and activated in the Sophos Mobile Control web console.

You can manage the Sophos Mobile Security app on managed devices from the Sophos Mobile Control web console as follows:

- You can configure settings for the Sophos Mobile Security app on all managed end user devices remotely and centrally in the web console.
- You can make sure that the Sophos Mobile Security app is installed on end user devices and runs scans at defined intervals. You can define this as a compliance criterion.
- You can trigger scans for specific devices.
- You can view scan results for devices in the web console.

For further information on Sophos Mobile Security, see the Sophos Mobile Security help.

26.1 Licenses for managing Sophos Mobile Security

In order to manage the Sophos Mobile Security app from Sophos Mobile Control, valid licenses are required. After purchase you receive the license key for activating your Sophos Mobile Security license. How you activate the license in the web console depends on the Sophos Mobile Control variant in use (on-premise installation or Software as a Service).

26.1.1 Activate licenses for on-premise installations

For on-premise Sophos Mobile Control installations, Sophos Mobile Security licenses are managed by the super administrator in customer management. For further information, refer to the Sophos Mobile Control super administrator guide.

26.1.2 Activate license for Software as a Service installations

1. In the Dashboard view, click the Settings button.
   The Settings view is displayed.

2. Go to the SMSec tab.
3. In the License key field, enter the license key you have received from Sophos and click Activate.

The Sophos Mobile Security license is activated. The Active license key field shows the activated license key. The Number of clients field shows the number of available clients. The Valid until field shows the license expiry date.

In the Dashboard, the relevant license information is shown in the SMSec line in the fields Managed devices, Licensed devices and License valid until.

26.2 Configure settings for Sophos Mobile Security

Prerequisite: A license for managing Sophos Mobile Security from the Sophos Mobile Control web console is available.

1. In the Dashboard view, click the Settings button.
   The Settings view is displayed.

2. Go to the SMSec tab.

3. Under General, you can specify the following:

   a) In the Cloud scan mode field, define when Sophos Mobile Security should scan for the latest malware information. Select one of the following options to define when the app should use a cloud lookup:
      
      ■ Always
      ■ Not while roaming
      ■ Wi-Fi only

      With this setting you can control the data traffic of the app. If you set Cloud scan mode to Wi-Fi only, the cloud lookup will only be performed when the device has a Wi-Fi connection. If you set Cloud scan mode to Not while roaming, a cloud lookup will never be performed while the device is roaming in a foreign network.

   b) In the Scheduled scan interval field, select how often scans are carried out.

   c) Select Allow user to trust apps to allow users to trust apps although they have been identified as malware. The user can mark them as ignored. In subsequent scans, these apps will not be shown as threats.

4. Under Targets, you can select the following:

   a) Select Scan system apps to include system apps in scans.
System apps are not scanned by default as they are protected by the Android OS and cannot be removed by the user. But you can activate the scanning of system apps here.

b) Select **Scan SD Card, USB, ...** to scan all files on SD cards, USB and other external storage devices in addition to per default scanning of all installed apps on the device.

c) Select **Detect PUAs** to scan for Potentially Unwanted Applications.

Potentially Unwanted Applications (PUAs) are apps that, while not malicious, are generally considered unsuitable for business networks. The major PUA classifications are Adware, Dialer, System monitor, Remote administration tools and Hacking tools. But certain apps that can fall into the PUA category might be considered useful by some users.

If you select this option, Sophos Mobile Security will detect PUAs during scans and notify the end user accordingly.

5. Under **Live Protection**, you can select the following:

a) Sophos Mobile Security scans apps during installation on the Android device by default. To deactivate this behavior, deselect **On install scan**.

b) Make sure that **Scan notification** is selected to receive scan notifications.

c) Select **Monitor SD Card** to monitor the SD card for any changes. If new files are stored on the card, they are scanned.

a) In the **Web filter mode** field, define the settings for filtering web pages with inappropriate or offensive content:

- If you select **Never**, users can view any website on their devices, regardless of content.

- If you select **Minimal**, a warning message is displayed as soon as a user opens a website with inappropriate content. The user can choose to ignore this message and continue to the website.

- If you select **Maximal**, websites with inappropriate content are blocked.

Websites are categorized based on contents by SophosLabs. Data is updated constantly.

6. Click the **Save** button.

The settings are valid for all Android devices with the Sophos Mobile Security app installed in the customer you are logged on to. The settings defined in the Sophos Mobile Control web console cannot be changed on the end user device. They are greyed out.

### 26.3 Define Sophos Mobile Security compliance settings

**Prerequisite:** A license for managing Sophos Mobile Security from the Sophos Mobile Control web console is available.
You can configure compliance settings that relate to Sophos Mobile Security in the web console.

1. Add a new set of compliance settings or open an existing set for editing. For further information, see Configure compliance settings (section 12).
2. Go to the Android tab.
3. In the Max. SMSec scan interval field, you can specify the maximum scan interval for malware scans performed by the Sophos Mobile Security app on the device.
4. In the Malware apps allowed field, select whether detected malware apps are allowed on devices.
5. In the Suspicious apps allowed field, select whether detected suspicious apps are allowed on devices.
6. In the PUA allowed field, select whether detected PUAs (Potentially Unwanted Apps) are allowed on devices.
7. After you have configured all required settings, click the Save button.

### 26.4 Trigger a scan for a specific device

**Prerequisite:** A license for managing Sophos Mobile Security from the Sophos Mobile Control web console is available.

1. In the web console menu bar, go to Inventory and click Devices.
   
   The Devices view is displayed with all devices registered with Sophos Mobile Control for this customer.

2. Click the Show icon or the Edit icon next to the required device.
   
   The Show device or the Edit device view is displayed.

3. Click the Start SMSec scan button.

The device is scanned according to the Sophos Mobile Security settings configured in the web console.

### 26.5 Trigger a scan through a task bundle

You can define a scan task in a task bundle, for example to trigger a scan on multiple devices and to combine the scan with further tasks.

1. Create a new task bundle or open an existing one for editing. For further information, see Create task bundles (section 18.1).
2. Click the Create new task button.
3. In the Select type view, select Start SMSec scan and click Next.
   
   The Edit task properties view is displayed.
4. In the **Task name** field, specify a meaningful name for the task and click **Next**. The task is displayed under **Tasks** in the **Edit task bundle** view.

5. After you have added all required tasks to the task bundle, click the **Save** button in the **Edit task bundle** view.

### 26.6 View Sophos Mobile Security scan results

**Prerequisite:** A license for managing Sophos Mobile Security from the Sophos Mobile Control web console is available.

1. In the web console menu bar, go to **Inventory** and click **Devices**.
   
The **Devices** view is displayed with all devices registered with Sophos Mobile Control for this customer.

2. Click the **Show** icon or the **Edit** icon next to the required device.
   
The **Show device** or the **Edit device** view is displayed.

3. Go to the **Scan results** tab.
   
The tab shows the SMSec scan results. The non-clean packages, for example potentially unwanted apps, are shown in a table below. Under **Threat name**, you can click on the shown links to display further information on the relevant threat from SophosLabs.

4. Go to the **Compliance violations** tab to view the compliance violations related to the scan results. The violations shown depend on the Sophos Mobile Security compliance settings defined.
### Appendix: Common web console buttons

This appendix provides an illustrated overview of all common buttons throughout the web console and their functions.

<table>
<thead>
<tr>
<th>Button</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Next" /></td>
<td>Next</td>
<td>Navigates to the next view, for example after a process step has been completed.</td>
</tr>
<tr>
<td><img src="image" alt="Back" /></td>
<td>Back</td>
<td>Navigates to the last view.</td>
</tr>
<tr>
<td><img src="image" alt="Information" /></td>
<td>Information</td>
<td>Provides further information on a specific topic.</td>
</tr>
<tr>
<td><img src="image" alt="Duplicate this bundle" /></td>
<td>Duplicate this bundle</td>
<td>Duplicates a profile/command bundle/task bundle.</td>
</tr>
<tr>
<td><img src="image" alt="Yes" /></td>
<td>Yes</td>
<td>Confirms an action.</td>
</tr>
<tr>
<td><img src="image" alt="No" /></td>
<td>No</td>
<td>Cancels an action.</td>
</tr>
<tr>
<td><img src="image" alt="Group selection" /></td>
<td>Group selection</td>
<td>Switches to the <strong>Select device group(s) view</strong>. In this view, you can select one or several device groups for a process.</td>
</tr>
<tr>
<td><img src="image" alt="Select device(s)" /></td>
<td>Select device(s)</td>
<td>Switches to the <strong>Select device(s) view</strong>. In this view, you can select one or several devices for a process.</td>
</tr>
<tr>
<td><img src="image" alt="Finish" /></td>
<td>Finish</td>
<td>After you have completed the required steps for a specific process, this button executes the relevant action.</td>
</tr>
<tr>
<td><img src="image" alt="Edit" /></td>
<td>Edit</td>
<td>Opens an edit view where you can change settings or information.</td>
</tr>
<tr>
<td><img src="image" alt="Save" /></td>
<td>Save</td>
<td>Saves changed settings.</td>
</tr>
<tr>
<td>Button</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td><img src="reload.png" alt="Reload" /></td>
<td><strong>Reload</strong></td>
<td>Reloads the contents of a table.</td>
</tr>
<tr>
<td><img src="create.png" alt="Create new" /></td>
<td><strong>Create new &lt;item&gt;</strong></td>
<td>Adds an entry, for example a device.</td>
</tr>
<tr>
<td><img src="delete.png" alt="Delete" /></td>
<td><strong>Delete</strong></td>
<td>Deletes a selected entry</td>
</tr>
<tr>
<td><img src="import.png" alt="Import" /></td>
<td><strong>Import &lt;items&gt;</strong></td>
<td>Imports entries, for example devices from a CSV list, to Sophos Mobile Control.</td>
</tr>
<tr>
<td><img src="create.png" alt="Create" /></td>
<td><strong>Create a device report (CSV file).</strong></td>
<td>Exports device information to a CSV file.</td>
</tr>
</tbody>
</table>
28 Technical support

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

- Visit the SophosTalk community at http://community.sophos.com/ and search for other users who are experiencing the same problem.
- 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.
29 Legal notices

Copyright © 2011 - 2013 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.