Contents

1  About Sophos Mobile Control.................................................................................................................4
2  About the Sophos Mobile Control web console......................................................................................7
3  Key steps for managing devices with the web console..........................................................................10
4  Login to the Sophos Mobile Control web console................................................................................11
5  The web console user interface...............................................................................................................13
6  The Dashboard........................................................................................................................................16
7  Create new administrators......................................................................................................................18
8  Configure technical contact....................................................................................................................19
9  Configure personal settings....................................................................................................................20
10 Configure password policies..................................................................................................................21
11 Configure platform-specific settings....................................................................................................23
12 Configure compliance rules..................................................................................................................28
13 Configure provisioning by email............................................................................................................34
14 Add devices to Sophos Mobile Control...............................................................................................36
15 Provision devices through the Sophos Mobile Control web console.................................................41
16 Work with applications.........................................................................................................................45
17 Work with profiles.................................................................................................................................59
18 Work with task bundles.........................................................................................................................100
19 Work with command bundles..............................................................................................................103
20 Configure Self Service Portal use for end users.................................................................................106
21 Administer devices in the Inventory..................................................................................................117
22 Monitor tasks in the web console.......................................................................................................130
23 Reports.................................................................................................................................................134
24 Back up devices...................................................................................................................................137
25 Send messages to devices....................................................................................................................140
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 Phone 8
- 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, Windows Phone 8 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, Windows Phone 8 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>Term</td>
<td>Explanation</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</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>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, for example personal settings or platform-specific settings.
- Configure compliance rules and define actions to be taken if devices no longer comply with the rules specified, see Configure compliance rules (section 12).
- Register devices with Sophos Mobile Control, see Add devices to Sophos Mobile Control (section 14).
- Provision new devices, see Provision devices through the Sophos Mobile Control web console (section 15).
- Install application packages on registered devices, see Work with applications (section 16).
- Define profiles and security policies for devices, see Work with profiles (section 17).
- Create task bundles to bundle several tasks for mobile devices and transfer them in one transaction, Work with task bundles (section 18).
- Define custom Sophos Mobile Control client command bundles to be transferred to devices in a single task, Work with command bundles (section 19).
  Note: This function may not be available for you, depending on your personal settings. For further information, see Configure personal settings (section 9).
- Configure settings for the Self Service Portal, see Configure Self Service Portal use for end users (section 20).
- Carry out administrative tasks on devices, for example reset the password of devices, lock or wipe devices if they are lost or stolen, decommission devices, see Carry out administrative tasks (section 21.4).
- Configure data backups for Android and Windows Mobile devices, Back up devices (section 24).
  Note: Backups are not supported for Sophos Mobile Control as a Service.
  Note: This function may not be available for you, depending on your personal settings. For further information, see Configure personal settings (section 9).
Create and view reports and monitor the data traffic of devices, see *Reports* (section 23).

### 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 Web console user roles

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

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

You can assign the following roles:

<table>
<thead>
<tr>
<th>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 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, see Configure platform-specific settings (section 11).
- Configure compliance rules for devices in the web console, Configure compliance rules (section 12).
- Configure provisioning by email for devices that do not support text messages, for example iPads, see Configure provisioning by email (section 13).
- Create device groups, see Create device groups (section 14.1).

Device groups are used to categorize devices. We recommend that you put devices into groups. This helps you to manage them efficiently as you can carry out tasks on a group rather than on individual devices.

- Register and provision devices, see Add devices to Sophos Mobile Control (section 14) and Provision devices through the Sophos Mobile Control web console (section 15).

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 profiles and security settings for devices in the web console, see Work with profiles (section 17).
- Create task bundles for Self Service Portal configuration, see Work with task bundles (section 18).
- Configure Self Service Portal use for end users, see Configure Self Service Portal use for end users (section 20).
- Apply new or updated profiles 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 administrators* (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 Change your password

You can change your password any time after you have logged in to the web console:

1. In the web console menu bar, go to Settings and click General.
   The General settings view is displayed.

2. Go to the Change password tab.

3. Enter your old password, a new one and confirm it.

4. Click the Save button.

4.4 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.

4.5 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>
| ![Filter icon] | Filter | 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).  
  **Note:** This button is only shown, if a view can be filtered. |
| ![Reset icon] | Reset | This button is displayed after you have set a filter. It resets an active filter. |
| ![Home icon] | Home | Opens the homepage with the **Dashboard** view. |
| ![Help icon] | Help | Opens a link to the Sophos Mobile Control documentation web page. On this page, all manuals for Sophos Mobile Control are available. |
| ![Logout icon] | 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.

- **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 *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 Web console 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>📌</td>
<td>Show details of this item.</td>
</tr>
<tr>
<td>✎</td>
<td>Edit this item.</td>
</tr>
<tr>
<td>✕</td>
<td>Delete this item.</td>
</tr>
<tr>
<td>🔄</td>
<td>This icon is shown for software packages. Click it to download the software package from the web console, see Download uploaded application packages (section 16.1.1).</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).
- User filter, see Use the user filter (section 20.3.4)

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 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.

To return to the Dashboard view from other views, click the Home button or the pink Sophos Mobile Control logo in the web console header.

6.1 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 timezone of the server.

Below this information two pie charts are displayed showing the number of compliant/non compliant and managed/not managed devices. Click the links Not Compliant, Compliant, Managed and Not Managed below the pie charts to display the relevant device lists. 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>
</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. |
<p>| <strong>Self Service Portal configuration completed</strong> | 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). |
| <strong>Self Service Portal configuration pending</strong> | Shows the number of devices for which the configuration through the Self Service Portal is pending. |
| <strong>Self Service Portal configuration failed</strong> | Shows the number of devices for which the configuration through the Self Service Portal has failed. |</p>
<table>
<thead>
<tr>
<th>Line</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company devices</td>
<td>Shows the number of company devices registered.</td>
</tr>
<tr>
<td>Employee devices</td>
<td>Shows the number of employee devices registered.</td>
</tr>
</tbody>
</table>

- **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.
7 Create new administrators

1. In the web console menu bar, click **Administrators**.
   The **Show administrators** view is displayed.

2. Click the **Create new administrator** button.
   The **Edit administrator** 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 *Web console 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 administrators** 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 web console menu bar, go to **Settings** and click **General**.
   
   The **General settings** view is displayed.

2. Go to the **Technical contact** tab.

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.

For end users the technical contact information is shown in the Sophos Mobile Control app on iOS, Android and Windows Phone 8 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 web console menu bar, go to Settings and click General.

   The General settings view is displayed.

2. In the Personal tab, configure the following settings:

   a) In the Lines per page in tables field, select the maximum number of table lines you want to display per page in the web console. You can choose between 20 and 100 lines.

   b) Under Activated platforms, select the platforms you want to use in the web console: Android, Blackberry, iOS, Windows Phone 8 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.

   c) Select Enable command bundles (expert mode), to enable the Command bundles function. For further information, see Work with command bundles (section 19).

   d) Select Enable backup functionality to enable the Backup function. For further information, see Back up devices (section 24).

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.

**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 web console menu bar, go to **Settings** and click **General**.

   The **General settings** view is displayed.

2. Go to the **Password Policies** tab.

3. Under **Password policies for SMC web console user and SSP user - Rules** (if you use internal user management) or **Password policies for SMC web console user - Rules** (if you use external user management), 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** (if you use internal user management) or **Password policies for SMC web console user - Settings** (if you use external user management), 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 4.4).

   a) In the **Originator** field, enter the email sender address.

   b) Under **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_, _FIRSTNAME_ and _LASTNAME_ will be replaced by the corresponding values in the email.

c) Under 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, predefined the email content. Use the placeholder _NEW_PASSWORD_ to include the new password for the user. 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.

11.1 Configure iOS-specific settings

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.

11.1.1 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 web console menu bar, go to Settings and click System setup.
   The System setup view is displayed.
2. Go to the iOS settings 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.
4. In the Password for the keystore field, enter the required password.
5. In the Apple ID field, you can enter your Apple ID for future reference.
6. Click Upload.
   After the file has been uploaded successfully, a confirmation message is displayed.
7. Click Save.
11.1.2 Configure Locate function for iOS 6 devices

Note: The settings described in this section apply to iOS 6 devices only.

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 web console menu bar, go to Settings and click General.

   The General settings view is displayed.

2. Go to the iOS client tab.

3. Make sure that the Enable device location 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: Higher accuracy will decrease battery life. The lowest value in this field (100) means the highest accuracy.

5. Click the Save button.

11.1.3 Configure destinations for AirPlay mirroring

With Sophos Mobile Control you can remotely trigger AirPlay mirroring between an iOS device and predefined AirPlay destinations (for example AppleTV).

Note: AirPlay only works for devices within the same network.

You can define destinations for AirPlay mirroring in the web console.

1. In the web console menu bar, go to Settings and click System setup.

   The System setup view is displayed.
2. In the **iOS settings** tab, under **AirPlay destinations**, click the **Create new AirPlay destination** button.

   The **AirPlay destination** view is displayed.

3. Enter the **Device name** (obligatory) and the **MAC address** (optional). If necessary, enter the **Password** for the AirPlay destination device.

4. Click the **Apply** button.

   The device is shown under **AirPlay destinations** in the **iOS settings** tab of the **System setup** view.

5. In the **iOS settings** tab, click the **Save** button.

You can trigger AirPlay mirroring between an iOS device and the destination defined by using the **Request AirPlay mirroring** button in the **Show device** or **Edit device** view for the relevant device. For a description of this button and all other function buttons available in the **Show device** and **Edit device** views, see **Carry out administrative tasks** (section 21.4).

### 11.2 Configure Windows Phone 8 specific settings

For Windows Phone 8 you can configure the MDM synchronization interval.

**Note:** Synchronization is only performed in this interval. Synchronization through the server cannot be triggered.

In addition, you can configure the locate function for Windows Phone 8 devices, if this is allowed for the customer you are logged in to. The super administrator can activate or deactivate the locate function in customer management. For further information on customer management, see the *Sophos Mobile Control super administrator guide*.

In addition, you can configure an email to be sent to users for app activation on their devices.

#### 11.2.1 Configure synchronization interval

1. In the web console menu bar, go to **Settings** and click **General**.

   The **General settings** view is displayed.

2. Go to the **Windows Phone client** tab.

3. In the **MDM sync interval** field, select the time interval for synchronization with the server.

4. Click the **Save** button.

#### 11.2.2 Configure Locate function for Windows Phone 8 devices

If the **Locate** function is enabled, the Sophos Mobile Control app installed on Windows Phone 8 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 Windows Phone 8*).

**Note:** You can only configure the locate function for Windows Phone 8 devices, if this is allowed for the customer you are logged in to. The super administrator can activate or deactivate the Windows Phone 8 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 web console menu bar, go to **Settings** and click **General**.
   The **General settings** view is displayed.

2. Go to the **Windows Phone client** tab.
3. Make sure that the **Enable device location** 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:** Higher accuracy will decrease battery life. The lowest value in this field (100) means the highest accuracy.

5. Click the **Save** button.

### 11.2.3 Configure app activation email

1. In the web console menu bar, go to **Settings** and click **General**.
   The **General settings** view is displayed.

2. Go to the **Windows Phone client** tab.
3. Under **App activation email**, do the following:
   a) In the **Originator** field, enter the email sender address.
   b) In the **Subject** field, enter an email subject, for example "Activate the Sophos Mobile Control email on your device".
   c) In the text field under **Content**, predefine the email content. The following placeholders are available and will be replaced by the corresponding values in the email:
     - _ACTIVATIONTOKEN_
     - _CONFIG_LINK_
4. 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 web console menu bar, go to **Settings** and click **System setup**.
   
   The **System setup** 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 rules

In the web console, you can:

- Configure compliance rules for all available device types (platforms).
- Define actions to be taken if devices no longer comply with the rules specified.
- Define multiple compliance 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 web console menu bar, click Compliance rules.
   The Compliance rules list view is displayed.

2. Click the Add button.

3. The Compliance rules view with tabs for all available device types is shown.

4. Enter a Name and a Description for the new compliance rule.

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.

9. Under Disallow network access, you can specify that network access will be denied automatically, if devices are not compliant. Select the required checkboxes next to the corresponding rules.
   This column is only available, if network access control is configured for this customer. For further information, see the Sophos Mobile Control super administrator guide.

10. 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.

11. 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 Work with task bundles (section 18).
12. 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 rules** list view.

13. If you have specified that administrators receive email notifications when devices are not compliant, specify the relevant recipients under **Compliance mail recipients**. Use semicolons (;) to separate several administrators in the **Compliance mail recipients** field. Define a notification schedule under **Compliance mail timetable**.

14. Click the **Save** button.

The new compliance rule can be assigned to device groups. In device groups, you can select different compliance rules 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 rules** tabs.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Android</th>
<th>iOS</th>
<th>Windows Phone 8</th>
<th>Windows Mobile</th>
<th>BlackBerry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min. client version</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>
<td>✔️</td>
</tr>
<tr>
<td>Allow root rights</td>
<td>Select whether devices with root rights are allowed.</td>
<td>✔️</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✔️</td>
</tr>
<tr>
<td>Allow jailbreak</td>
<td>Select whether jailbroken devices are allowed.</td>
<td>✗</td>
<td>✔️</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Password required</td>
<td>Select whether a passcode is required for devices.</td>
<td>✗</td>
<td>✔️</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Allow non-market apps</td>
<td>Select whether non-market apps are allowed on devices.</td>
<td>✔️</td>
<td>✗</td>
<td>✔️</td>
<td>✗</td>
<td>✔️</td>
</tr>
<tr>
<td>Allow debug bridge (ADB)</td>
<td>Select whether ADB (Android Debug Bridge) is allowed on devices.</td>
<td>✔️</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 Phone 8</td>
<td>Windows Mobile</td>
<td>BlackBerry</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
<td>-----</td>
<td>-----------------</td>
<td>----------------</td>
<td>------------</td>
</tr>
<tr>
<td>Min. OS version</td>
<td>Select the earliest operating system version required on devices.</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Max. OS version</td>
<td>Select the latest operating system version allowed on devices.</td>
<td>✔️</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.</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✗</td>
</tr>
</tbody>
</table>
| Max. SMC app Synchronization gap | 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.  
**Note:** This setting only applies to devices with an iOS version below iOS 7. It has no effect on iOS 7 devices. | ✗      | ✔️  | ✔️              | ✗              | ✗          |
<p>| Max. SMSec scan interval     | 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. | ✔️      | ✗  | ✗              | ✗              | ✗          |</p>
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Android</th>
<th>iOS</th>
<th>Windows Phone 8</th>
<th>Windows Mobile</th>
<th>BlackBerry</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>scans performed by the Sophos Mobile Security app on the device.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malware apps allowed</td>
<td>This field is only displayed, if Sophos 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>
<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>
<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>
<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>
<td>✗</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
<td>Android</td>
<td>iOS</td>
<td>Windows Phone 8</td>
<td>Windows Mobile</td>
<td>BlackBerry</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</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 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 6 devices</em> (section 11.1.2).</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Blacklisted apps/Whitelisted apps</td>
<td>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.</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Mandatory apps</td>
<td>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.</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
12.2 Assign compliance rules 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 rules** in the fields **Company devices** and **Employee 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 **Policy for company devices** and **Policy for employee 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 web console menu bar, click **Compliance rules**.  
   The **Compliance rules** view is displayed.

2. Click the **Check now** button.

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

Android, Apple iOS and Windows Phone 8 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 web console menu bar, go to Settings and click General.
   
   The General 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, predefine 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, Content for iOS devices and/or Content for Windows Phone devices predefine the email content. The following placeholders are available:

- _DOWNLOAD_LINK_ (Android and iOS)
- _CONFIG_LINK_ (Android)
- _DEVICENAME_ (Android, iOS and Windows Phone 8)
- _DEVICEDESCRIPTION_ (Android, iOS and Windows Phone 8)
- _EMAIL_ (Windows Phone 8)
- _DOMAIN_ (Windows Phone 8)
- _USERNAME_ (Windows Phone 8)
- _PASSWORD_ (Windows Phone 8)
- _SERVERURL_ (Windows Phone 8)

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 *Work 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, Windows Phone 8 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. We recommend that you put devices into groups. This helps you to manage them efficiently as you can carry out tasks on a group rather than on individual 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 rules** in the fields **Company devices** and **Employee 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 **Group 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) 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".

   d) 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).

   e) 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).

f) Under Owner, select Company device or Employee device.

5. To add an LDAP link to the device, click the Assign user to device button. For further information, see Assign a user 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 Group members in the device group you have selected. You can now provision and manage the device.

### 14.3 Duplicate a device

You can create new devices in Sophos Mobile Control by duplicating existing devices.

Note: You can only duplicate devices that are not being edited. The duplicate is named "Copy of" plus the name of the original. You can rename the devices according to your requirements.

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

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

3. Click the Duplicate this device button.
   
   A message prompting you to confirm the duplication is displayed.

4. Click the Yes button.

The device is duplicated and shown in the Devices view. You can now edit the duplicated device as required. To edit the device, click the Edit pencil icon next to it.

### 14.4 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.
1. In the web console menu bar, go to **Inventory** and click **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.

### 14.5 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 click **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.
- Windows Phone 8 devices are provisioned by adding a company account to the device.

The web console offers the following options for provisioning devices:

- You can provision individual, unmanaged Android, Windows Phone 8 and Windows Mobile devices by installing the SMC client using the **Devices** function. For further information, see *Provision individual Android, and Windows Phone 8 devices* (section 15.2).

- You can provision individual, unmanaged Apple iOS devices by iOS MDM client bootstrap using the **Devices** function. For further information, see *Provision individual iOS devices* (section 15.3).

To provision and configure multiple devices efficiently, the following methods are recommended:

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

- You can have devices registered and provisioned by end users through the Self Service Portal. To do so, include 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, Windows Phone 8 and Windows Mobile*.

**Note:** For Android, iOS and Windows Phone 8 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, Apple iOS and Windows Phone 8*. 

Administrator guide
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 Settings and click 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, Android and Windows Phone 8 client packages, see Create links to packages (section 16.1.2).
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 individual Android, and Windows Phone 8 devices

Note: For Windows Phone 8 devices, an activation email is necessary for setting up Sophos Mobile Control, see Configure app activation email (section 11.2.3).

1. In the web console menu bar, go to Inventory and click Devices.
   The Devices view is displayed.
2. Click the Show or Edit icon next to the device you want to provision.
   The Show device/Edit device view is displayed.
3. Click the Install SMC Client button.
   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 \textbf{Scheduled date}, select \textbf{Now} or specify a \textbf{Date} and \textbf{Time} for the execution of this task.
7. Click the \textbf{Finish} button.

The device is provisioned at the specified date and time. After successful completion and synchronization with the server the device status is shown as \textbf{Managed}.

\section*{15.3 Provision individual iOS devices}

1. In the web console menu bar, go to \textbf{Inventory} and click \textbf{Devices}.
   
The \textbf{Devices} view is displayed.
2. Click the \textbf{Show} or \textbf{Edit} icon next to the device you want to provision.
   
The \textbf{Show device/Edit device} view is displayed.
3. Click the \textbf{Bootstrap this device} button.
   
   A confirmation message is displayed.
4. Click \textbf{Yes}.

A bootstrap task is created for the selected device and the \textbf{Task view} is displayed. The bootstrap task is carried out. To complete provisioning, you must install the Sophos Mobile Control app on the device, see \textit{Install application packages} (section 16.4).

\section*{15.4 Provision individual Windows Mobile devices}

1. In the web console menu bar, go to \textbf{Settings} and click \textbf{Client packages}.
   
The \textbf{Sophos Mobile Control client packages} view is displayed.
2. Click the \textbf{Transfer} button.
   
The \textbf{Select device(s)} view is displayed.
3. In this view, you can:
   
   \begin{itemize}
   \item Select individual devices you want to install the client package on.
   \item Click the \textbf{Group selection} button, to open the \textbf{Select device group(s)} view and select one or several device groups for installing the client package.
   \end{itemize}
4. After you have made your selection, click \textbf{Next}.
   
The \textbf{Select software} view is displayed.
5. Select the client package that you want to install and click \textbf{Next}.
   
The \textbf{Set execution date} view is displayed.
6. Under **Scheduled date**, select **Now** or specify a **Date** and **Time** for the execution of this task.
7. Select **Enforce** to force installation for the selected devices.
8. Click the **Finish** button.

The device is provisioned at the specified date and time. After successful completion and synchronization with the server the device status is shown as **Managed**.
16 Work with applications

In the web console under Applications, you can create application packages to be installed on devices.

When you create 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.

Note: Windows Phone 8 apps can only be installed by a link through the Enterprise App Store.

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

Note: For iOS devices in supervised mode silent installation of managed apps is supported, if the relevant device allows that.

16.1 Create application packages

1. In the web console menu bar, click Applications.
   The Applications 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 package. These two fields are mandatory. In the field App identifier, you can enter the identifier for the app.
   Note: If you do not know the exact identifier, leave this field empty. For iOS apps the identifier is usually entered automatically.

4. For iOS, Android and Windows Phone 8 devices you can provide the application through the Enterprise App Store and define it as recommended or required. To do so, select Recommended or Required in the Recommendation status field. If you select Recommended (managed installation) or Required (managed installation), the app is pushed as a managed application to the end user device as soon as the user selects to install it.

5. In the Description text field, you can enter a description for the new application package.

6. Under Operating systems, select the operating system the new package applies to.

7. Select how the 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**. If you have not created the required link yet, you can obtain it by clicking the platform-specific links provided under the **Link** field. For further information, see *Create links to iOS packages* (section 16.1.2.1) and *Create links to Android and Windows Phone 8 packages* (section 16.1.2.2). Enter the link obtained in the **Link** field.

8. Click the **Save** button.

The application package is available for installation. It is displayed in the **Applications** 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, Apple iOS and Windows Phone 8*.

### 16.1.1 Download uploaded application packages

Once you have uploaded an application 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, click **Applications**.

   The **Applications** view is displayed.

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

   The **Edit package** view is displayed.

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

   A file download dialog is displayed.

4. Save the file at the required location.

### 16.1.2 Create links to packages

If you want to provide links to packages, you can create them when you create the application packages in the web console or separately. The following sections describe how to create links to Apple iOS, Android and Windows Phone 8 packages.

#### 16.1.2.1 Create links to iOS packages

1. The first step depends on whether you create a link during the creation of application packages in the web console or separately:

   - If you are in the process of creating an application package, select **Link to package** in the **Edit package** view and click the **iOS** link beneath the **Link** field.
   - If you want to create a link before you create an application package, open your internet browser and go to **https://linkmaker.itunes.apple.com/us/**.
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**.

### 16.1.2.2 Create links to Android and Windows Phone 8 packages

1. The first step depends on whether you create a link during the creation of application packages in the web console or separately:
   - If you are in the process of creating an application package, select **Link to package** in the **Edit package** view and click the **Android** or **Windows Phone 8** link beneath the **Link** field.
   - If you want to create a link before you create an application package, open your internet browser and go to
     - **https://play.google.com/store/apps** for Android packages, or to

2. Search for the required app and open it.
3. Copy the link shown in the web address bar of your browser.

### 16.2 Configure per app VPN and settings for iOS apps

**Note:** Per app VPN and settings are supported as of iOS 7.

For iOS apps, you can select a per app VPN to support the iOS feature "Per app VPN". With this feature, apps can be configured to automatically connect to VPN when they are launched. You can also configure settings for the app that will be deployed on the end user device during app installation.

**Prerequisites:**
- To be able to select a per app VPN, you need to define a **Per app VPN** configuration in an iOS configuration profile in the web console, see *Create iOS profiles in the web console* (section 17.1.1) and *Available iOS configurations* (section 17.1.2).
To define settings, you need to know the required parameter and the parameter type.

1. In the web console menu bar, click **Applications**.
   The **Applications** 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 **Settings and VPN** field.
   The **Settings & VPN** view is displayed.

4. Select the required configuration from the **Per app VPN** dropdown list to define the VPN the app is supposed to connect to.

5. To add managed settings, click the **Create new parameter** icon.
   The **Configuration parameter** view is displayed.

6. In this view, configure the following:
   a) In the **Parameter** field, enter the required parameter, for example SMC_URL.
   b) In the **Value** field, enter the parameter value, for example smc.sophos.com.
   c) In the **Type** field, select the parameter type: **String**, **Bool**, **Integer** or **Real**.
   d) Click the **Apply** button.
      The set of managed settings is displayed in the **Settings and VPN** view.

7. In the **Settings and VPN** view, click the **Apply** button.
   The **Show** button in the **Edit package** view shows the number of sets of managed settings configured.

8. Click the **Save** button.
   The selected per app VPN will be used when the app connects to VPN. The settings will be provided to end user devices during app installation.

### 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/).

The procedures for managing apps purchased with the Apple VPP vary according to the licensing scheme used. With iOS 7 Apple has introduced a new VPP licensing scheme. The scheme has been changed from licensing based on redemption codes to licensing based on service tokens. The following sections describe the two different procedures.
16.3.1 Manage Apple VPP apps based on redemption codes

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.

16.3.1.1 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/.

- 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 16.1.2.1) and Create application packages (section 16.1).

1. In the web console menu bar, click Applications.

   The Applications 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 redemption codes (file) 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.
16.3.2 Manage Apple VPP apps based on service tokens

After an order placed with the Apple Volume Purchase Program has been completed, you can download a service token (sToken) that contains the licenses for the apps purchased.

To manage apps purchased with Apple Volume Purchase Program with Sophos Mobile Control, you can set up the service token in the Sophos Mobile Control web console. This service token is used for authentication at the Apple web service. You can provide the licenses the service token comprises to users by inviting them to become authorized Apple VPP users. For this purpose you can set up an invitation email in the web console. After users have accepted their invitations, they become authorized VPP users.

The process for inviting users to become authorized VPP users differs depending on whether you use Sophos Mobile Control's 'internal' or 'external' user management. The instructions in this section cover both.

Note: For information on internal and external user management, see the Sophos Mobile Control super administrator guide. Or, if you are using Sophos Mobile Control as a Service, see Configure Self Service Portal user management for Sophos Mobile Control as a Service (section 20.3.1).

The key steps for managing apps purchased with the Apple VPP based on service tokens are:

1. Set up the VPP service token in Sophos Mobile Control.
2. For external user management: Add VPP users manually or by import.
3. Set up an email inviting users to become authorized Apple VPP users.
4. Invite users.
5. Assign VPP licenses.

16.3.2.1 Set up VPP service token (sToken)

To provide licenses for apps purchased by the Apple Volume Purchase Program in Sophos Mobile Control, you need to set up a VPP service token (sToken) in the web console.

1. In the Sophos Mobile Control web console, go to Settings and click System setup.
   The System setup view is displayed.

2. In the iOS Volume Purchase Program tab under VPP service token (sToken), click the link to the Apple iTunes VPP Portal.
   The Apple Volume Purchase Program website is displayed.

3. Select Business.
   The Business Store Sign In page is displayed.

4. Enter your Apple ID and your Password to sign in.

5. On the next page, select your account.
   Your Purchase History page is displayed.
6. To generate a VPP service token and download it in a text file, click the **Download** button at the bottom of the page.

   An sToken is generated and sent to you in a .txt file.

7. Open the file and copy its content.

8. In the Sophos Mobile Control web console under **System setup** in the **iOS Volume Purchase Program** tab, paste the service token file content into the text field under **sToken**.

9. Click the **Save** button.

   **Note:** After you have saved your changes, the service token text is no longer displayed in the text field for security reasons. But the field shows that a service token is in place.

### 16.3.2.2 Set up VPP invitation email

To enable end users to use the licenses from the VPP service token, they need to become authorized VPP users. In the web console, you can invite users to become VPP users. You can set up an VPP invitation email that will be sent to all users you are inviting.

1. In the Sophos Mobile Control web console, go to **Settings** and click **System setup**.

   The **System setup** view is displayed.

2. Go to the **iOS Volume Purchase Program** tab.

3. Under **VPP invitation email**, configure the following:

   a) In the **Originator** field, enter the email sender address. In the **Subject** field, enter an email subject, for example "VPP invitation".

   b) In the text field under **Content**, predefine the email content. The following placeholders are available and will be replaced by the corresponding values in the email:

   - _FIRSTNAME_
   - _LASTNAME_
   - _VPP_INVITATION_URL_

4. Click the **Save** button.

### 16.3.2.3 Add VPP users with external user management

The process for inviting users to become authorized VPP users differs depending on whether you use Sophos Mobile Control’s 'internal' or 'external' user management. If you use external user management, you can add specific VPP users in the web console manually or by import.

#### 16.3.2.3.1 Create VPP users manually

1. In the web console menu bar, click **VPP users**.

   The **Show VPP users** view is displayed.
2. Click the **Create new VPP user** button.
   The **Edit VPP user** view is displayed.
3. Enter the **Last name**, the **First name** and the **Email** address for the new VPP user.
4. Click the **Save** button.

### 16.3.2.3.2 Import VPP users

1. In the web console menu bar, click **VPP users**.
   The **Show VPP users** view is displayed.
2. Click the **Import users** button.
   The **Import VPP 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.
   **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.
3. Select the .csv file you want to import and click **Upload file**.
   The entries in the .csv file are checked for errors and displayed on the import page.
   **Note:** If there are any errors in the .csv file, it cannot be imported. An error message is displayed next to the relevant entries. Edit the .csv file accordingly and try again.
4. If all entries are correct, click the **Finish** button.

### 16.3.2.4 Invite users managed with external user management

**Prerequisites:**
- You have added VPP users. For further information, see **Add VPP users with external user management** (section 16.3.2.3).
- You have configured an VPP invitation email. For further information, see **Set up VPP invitation email** (section 16.3.2.2).

1. In the web console menu bar, click **VPP Users**.
   The **Show VPP users** view is displayed.
2. You can invite multiple users or individual users.
   - To invite multiple users, click the **Invite multiple users to VPP** button and confirm the message displayed. All users not yet invited are invited to become VPP users.
   - To invite an individual user, click the **Edit** icon next to the user in the **Show VPP users** view. In the **Edit VPP user** view, click the **Invite to VPP** button and click the **Save** button.
The invitation emails are sent to the users invited. The users need to accept the invitation by clicking the VPP invitation URL included in the email and follow the relevant instructions to become authorized VPP users.

### 16.3.2.5 Invite users managed with internal user management

**Prerequisites:**
- Users have been added to the web console through internal user management. For further information, see *Manage Self Service Portal users* (section 20.3).
- You have configured a VPP invitation email. For further information, see *Set up VPP invitation email* (section 16.3.2.2).

1. In the web console menu bar, click **Users**.
   The **Show users** view is displayed.
2. You can invite multiple users or individual users.
   - To invite multiple users, click the **Invite multiple users to VPP** button and confirm the message displayed. All users not yet invited are invited to become VPP users.
   - To invite an individual user, click the **Edit** icon next to the user in the **Show users** view. In the **Edit user** view, click the **Invite to VPP** button and click the **Save** button.

The invitation emails are sent to the users invited. The users need to accept the invitation by clicking the VPP invitation URL included in the email and follow the relevant instructions to become authorized VPP users.

### 16.3.2.6 Assign VPP licenses

If you use the new licensing scheme you can assign VPP licenses in two ways:
- You can assign VPP licenses to users directly in user management.
- You can assign the VPP licenses of individual apps to users by using the **Applications** function.

#### 16.3.2.6.1 Assign VPP licenses to users in user management

After users have become authorized Apple Volume Purchase Program users, you can assign the licenses available within the VPP service token to them.

1. The first step varies depending on whether you are using internal or external user management:
   - Internal user management: In the web console menu bar, select **Users**.
   - External user management: In the web console menu bar, select **VPP users**.
   The **Show users** or **Show VPP users** view is displayed.
2. Click the **Edit** icon next to the required user.
   The **Edit user** or **Edit VPP user** view is displayed.
3. Click the **Show VPP licenses** button.
   The available and used licenses for this user are displayed.

4. Select the license you want to assign and click the **Apply** button.
5. In the **Edit user** or **Edit VPP user** view, click the **Save** button.

### 16.3.2.6.2 Assign VPP licenses to users through Applications

1. In the web console menu bar, click **Applications**.
   The **Applications** view is displayed.

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

3. Click the **Show** button next to **VPP licenses**.
   The **VPP licenses** view is displayed. It shows the licenses available and the licenses used.

4. Select the license you want to assign and click the **Apply** button.
5. In the **Edit package** view, click the **Save** button.

### 16.4 Install application packages

**Prerequisite:** The required application package has been created under **Applications**.

1. In the web console menu bar, click **Applications**.
   The **Applications** view is displayed.

2. Click the **Install** button.
   The **Select device(s)** view is displayed.

3. 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.

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

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

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

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

16.5 Uninstall application 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, click Applications.

   The Applications view is displayed.

2. Click the Uninstall button.

   The Select device(s) view is displayed.

3. 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.

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

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

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

   The Set execution date view is displayed.

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

7. Select Enforce to force the uninstallation for the selected devices.

8. 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 application 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, click Applications.

   The Applications 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 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 application 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, click **Applications**.
   The **Applications** view is displayed.

2. Click the **Enable/disable** button.
   The **Select device(s)** view is displayed.

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

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

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

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

7. In the **Description** field, modify the description displayed, if necessary.

8. 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, click **Applications**.
   The **Applications** view is displayed.

2. Click the **Enable/disable** button.
   The **Select device(s)** view is displayed.

3. 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.

4. After you have made your selection, click **Next**.
   The **Set device as data source** view is displayed.
5. Select the device you want to use as a data source for application 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.

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

7. Click Next.

The Select execution date and description view is displayed.

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

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

10. Click the Finish button.

The selected processes are enabled/disabled on the selected devices at the specified date and time.
17 Work with profiles

In the web console under Profiles, you can create and transfer settings profiles for Apple iOS, Android, Windows Phone 8 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 menu bar, go to Profiles and click 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 systems 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. The web console indicates if any setting is supported only since a particular iOS version or only in supervised mode. In the following descriptions, the relevant information is included at the beginning of the section or in a minimum requirements column, if applicable.
Password policies

In this configuration, you can define password rules for devices. You can only add one **Password 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 password, for example &quot;1111&quot; or &quot;abcde&quot;.</td>
</tr>
<tr>
<td>Require alphanumeric value</td>
<td>If you select this option, passwords must contain at least one letter or number.</td>
</tr>
<tr>
<td>Minimum password length</td>
<td>Specifies the minimum number of characters a password 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 password must contain.</td>
</tr>
<tr>
<td>Maximum password age (1 - 730 days or none)</td>
<td>Requires users to change their password 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>Password history (1 to 50 or 0)</td>
<td>In this field, you can specify how many old passwords are remembered and compared with new ones. When the user defines a new password, it will not be accepted, if it matches a previously used password. Value range: 1 to 50 or 0 (no password 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 password prompt. This setting specifies the maximum value the user is allowed to configure on the device. If you select <strong>None</strong>, the user can select any of the intervals available. If you select <strong>Immediately</strong>, users must enter a password every time they unlock their devices.</td>
</tr>
</tbody>
</table>
### Setting/field

<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of failed attempts until device wipe</td>
<td>In this field, you can specify the maximum number of failed attempts to enter the correct password before the device is wiped. After six failed attempts, a time delay is imposed before a password 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.</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 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>Setting/field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</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>Allow Siri while device is locked</td>
<td>If you deactivate this option, users must unlock their devices by entering their password before they use Siri.</td>
</tr>
<tr>
<td>Allow Siri querying content from the web</td>
<td>If you deactivate this option, Siri will not query content from the web.</td>
</tr>
<tr>
<td>Force Siri profanity filter</td>
<td>If you deactivate this option, the Siri profanity filter is not forced on the device.</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 Game Center</td>
<td>If you deactivate this option, Game Center cannot be used on the device.</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>Allow find my friends modification</td>
<td>If you deactivate this option, modifications to the Find my Friends app are disabled.</td>
</tr>
<tr>
<td>Allow host pairing</td>
<td>If you deactivate this option, host pairing is disabled with the exception of the supervision host. If no supervision host certificate has been configured, all pairing is disabled.</td>
</tr>
<tr>
<td>Setting/field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allow AirDrop</td>
<td>If you deactivate this option, content sharing with AirDrop is not allowed on the device.</td>
</tr>
<tr>
<td>Allow Control Center on lock screen</td>
<td>If you deactivate this option, settings cannot be managed with Control Center when the device screen is locked.</td>
</tr>
<tr>
<td>Allow Notification Center on lock screen</td>
<td>If you deactivate this option the Notification Center is not available when the device screen is locked.</td>
</tr>
<tr>
<td>Allow Today view on lock screen</td>
<td>If you deactivate this option the Today view is not available when the device screen is locked.</td>
</tr>
<tr>
<td>Allow over-the-air PKI updates</td>
<td>If you deactivate this option, over-the-air PKI updates are not possible.</td>
</tr>
<tr>
<td>Allow iBooks store</td>
<td>If you deactivate this option, users cannot purchase books in iBooks.</td>
</tr>
<tr>
<td>Allow explicit sexual content in iBooks store</td>
<td>If you deactivate this option, explicit sexual content is not available through iBooks store.</td>
</tr>
<tr>
<td>Allow users to install configuration profiles</td>
<td>If you deactivate this option, users cannot install configuration profiles.</td>
</tr>
<tr>
<td>Allow iMessage</td>
<td>If you deactivate this option, users cannot use iMessage for texting.</td>
</tr>
<tr>
<td>Allow app removal</td>
<td>If you deactivate this option, users cannot remove apps from the device.</td>
</tr>
<tr>
<td>Company data</td>
<td></td>
</tr>
<tr>
<td>Allow documents to be shared only within managed apps/accounts</td>
<td>With this setting you can define a restriction on opening documents with apps/accounts (for example a company email account) managed by Sophos Mobile Control. For example: If this option is selected, and users have an email account managed by Sophos Mobile Control and apps managed by Sophos Mobile Control on their devices, attachments from the managed email account can only be opened with managed apps. Thereby you can</td>
</tr>
<tr>
<td>Setting/field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Allow documents to be shared only within unmanaged apps/accounts</strong></td>
<td>With this setting you can define a restriction on opening documents with apps/accounts (for example a private email account) not managed by Sophos Mobile Control. For example: If this option is selected, and users have an email account and apps not managed by Sophos Mobile Control on their devices, attachments from the unmanaged email account can only be opened with unmanaged apps. Thereby you can prevent personal documents from being opened in managed apps.</td>
</tr>
<tr>
<td><strong>Applications</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Allow use of YouTube</strong></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></td>
<td><strong>Note:</strong> This setting only applies to iOS versions older than version 6.</td>
</tr>
<tr>
<td><strong>Allow use of iTunes Store</strong></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><strong>Allow use of Safari</strong></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><strong>Enable autofill</strong></td>
<td>If you deactivate this option, Safari does not autofill web forms with previously entered information.</td>
</tr>
<tr>
<td><strong>Force fraud warning</strong></td>
<td>If you select this option, Safari attempts to prevent users from visiting websites identified as fraudulent or compromised.</td>
</tr>
<tr>
<td>Setting/field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Enable JavaScript</td>
<td>If you deactivate this option, Safari ignores JavaScript on websites.</td>
</tr>
<tr>
<td>Block pop-ups</td>
<td>If you select this option, Safari blocks popups.</td>
</tr>
</tbody>
</table>
| Accept cookies | In this field, you can specify if cookies should be accepted:  
  ■ Always  
  ■ Never  
  ■ From visited sites | 5.0+ |
| Allow modification of cellular data usage per app | If you deactivate this option, users cannot change the cellular data usage per app. | 7.0+ supervised |
| **iCloud** | | |
| Allow backup | If you select this option, users can back up their devices to iCloud. | 5.0+ |
| Allow document sync | If you select this option, users can store documents in iCloud. | 5.0+ |
| Allow Photo Stream | If you select this option, users can enable Photo Stream.  
  **Note:** 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. | 5.0+ |
| Allow shared photo streams | If you select this option, users can invite others to view their photo streams and can view photo streams shared by others. | 6.0+ |
| Allow keychain sync | If you deactivate this option, the iCloud feature Keychain for synchronizing passwords across different iOS and OS X devices is not allowed on the device. | 7.0+ |

Security and privacy
<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
<th>Minimum requirements</th>
</tr>
</thead>
<tbody>
<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>
<td>5.0+</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 cannot be verified. This setting applies to Safari and to Mail Contacts and Calendar accounts.</td>
<td>5.0+</td>
</tr>
<tr>
<td>Allow account modification</td>
<td>If you deactivate this option, account modification is disabled. The Accounts menu is not available on the device.</td>
<td>7.0+ supervised</td>
</tr>
<tr>
<td>Allow Touch ID to unlock a device</td>
<td>If you deactivate this option, the device cannot be unlocked by Touch ID.</td>
<td>7.0+</td>
</tr>
<tr>
<td>Force limit ad-tracking</td>
<td>If you select this option, anonymous user data apps use for targeting ads are no longer provided.</td>
<td>7.0+ supervised</td>
</tr>
<tr>
<td>Force encrypted backups</td>
<td>If you select this option, users must encrypt backups in iTunes.</td>
<td>7.0+ supervised</td>
</tr>
<tr>
<td>Content ratings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow explicit music and podcasts</td>
<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>
<td></td>
</tr>
</tbody>
</table>

**Roaming/Hotspot settings**

Minimum requirement: iOS version 7.0+

In this configuration, you can define settings for roaming and personal hotspots.

**Note:** Users can change these settings on their devices anytime.

<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable voice roaming</td>
<td>If you deactivate this setting, voice roaming is disabled on the device.</td>
</tr>
</tbody>
</table>
Enable data roaming

If you deactivate this setting, data roaming is disabled on the device.

Enable personal hotspot

If you deactivate this setting, the device cannot be configured to serve as a personal hotspot.

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>
<th>Minimum requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account name</td>
<td>In this field, enter the account name for the Exchange ActiveSync account.</td>
<td></td>
</tr>
<tr>
<td>Exchange ActiveSync Host</td>
<td>In this field, enter the Microsoft Exchange Server.</td>
<td></td>
</tr>
<tr>
<td>Allow move</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>
<td>5.0+</td>
</tr>
<tr>
<td>Allow recent address syncing</td>
<td>If you deactivate this option, recently used addresses are not synchronized with other devices using iCloud.</td>
<td>6.0+</td>
</tr>
<tr>
<td>Use only in mail</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>
<td>5.0+</td>
</tr>
<tr>
<td>SSL</td>
<td>Make sure that this option is selected, to send all communication through SSL (Secure Socket Layer).</td>
<td></td>
</tr>
<tr>
<td>Setting/field</td>
<td>Description</td>
<td>Minimum requirements</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Domain</td>
<td>In this field, enter the domain of your environment. You can also leave this field empty.</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>In this field, enter the user for this account. You can use the variable %USERNAME_% and the server will replace it with the actual user name, if the device the profile is sent to has an LDAP link established.</td>
<td></td>
</tr>
<tr>
<td>Email address</td>
<td>In this field, enter the email address of the account. You can use the variable %EMAILADDRESS_% and the server will replace it with the actual email address, if the device the profile is sent to has an LDAP link established.</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>In this field, enter the password for this account.</td>
<td></td>
</tr>
<tr>
<td>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>
<td></td>
</tr>
<tr>
<td></td>
<td>Unlimited</td>
<td></td>
</tr>
<tr>
<td></td>
<td>One day</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Three days</td>
<td></td>
</tr>
<tr>
<td></td>
<td>One week</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Two weeks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>One month</td>
<td></td>
</tr>
</tbody>
</table>
### 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>
<th>Minimum requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
<td>In this field, enter the ID of the wireless network.</td>
<td>5.0+</td>
</tr>
<tr>
<td>Connect automatically</td>
<td>Select this option, to automatically connect to the target network.</td>
<td></td>
</tr>
<tr>
<td>Hidden network</td>
<td>Select this option, if the target network is not open or visible.</td>
<td></td>
</tr>
<tr>
<td>Security type</td>
<td>In this field, you select the security type of the WiFi network:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ None</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ WEP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ WPA/WPA2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Any (personal)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Corporate WEP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Corporate WPA/WPA2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Any (company)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you select the personal settings WEP, WPA/WPA2 or Any (personal), a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Password field is displayed. Enter the relevant password.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you select the corporate settings Corporate WEP, Corporate WPA/WPA2</td>
<td></td>
</tr>
<tr>
<td>Setting/field</td>
<td>Description</td>
<td>Minimum requirements</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Protocols</td>
<td>In the Protocols tab configure the following:</td>
<td></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>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Under EAP-FAST, configure the EAP-FAST Protected Access credential settings.</td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td>In the Authentication tab, you specify authentication settings:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ In the User field, enter the user name for the connection to the wireless network.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Select Use Per-Connection Password, if the password is to be queried for each connection and transferred with the authentication.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ In the Password field, enter the relevant password.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ In the Identity certificate field, select the certificate for the connection to the wireless network.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ In the External identity field, enter the externally visible ID (for TTLS, PEAP and EAP-FAST).</td>
<td></td>
</tr>
<tr>
<td>Proxy</td>
<td>In this field, select the proxy settings for the WiFi connection:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ None</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Manually</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Automatic</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you select Manually, the fields Server and port, Authentication and Password</td>
<td></td>
</tr>
</tbody>
</table>
Minimum requirements

<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>are displayed. Enter the required proxy information. If you select Automatic, the field <strong>Proxy server URL</strong> is displayed. Enter the URL of the proxy server.</td>
<td></td>
</tr>
</tbody>
</table>

**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>■ Cisco AnyConnect</td>
<td></td>
</tr>
<tr>
<td>■ IPSec (Cisco)</td>
<td></td>
</tr>
<tr>
<td>Different entry fields are shown in the <strong>VPN</strong> view depending on the connection type you select here.</td>
<td></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 <strong>Cisco AnyConnect</strong>)</td>
<td>In this field, enter the group that may be required for the authentication of the connection.</td>
</tr>
<tr>
<td><strong>User authentication</strong> (connection type <strong>Cisco AnyConnect</strong>)</td>
<td>In this field select the type of user authentication for the connection:</td>
</tr>
<tr>
<td>■ <strong>Password</strong></td>
<td></td>
</tr>
<tr>
<td>If you select this option, the <strong>Password</strong> field is shown below the <strong>User Authentication</strong> field. Enter the password for authentication.</td>
<td></td>
</tr>
<tr>
<td>■ <strong>Certificate</strong></td>
<td></td>
</tr>
<tr>
<td>Setting/field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>If you select this option, the Certificate field is shown below the User Authentication field. Select a certificate.</td>
<td></td>
</tr>
</tbody>
</table>
| **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. |
**Per app VPN**

Minimum requirement: iOS version 7.0+

In this configuration, you can define VPN settings to support the iOS feature "Per app VPN". With this feature, apps can be configured to automatically connect to VPN when they are launched. So you can for example ensure that data transmitted by managed apps travels through VPN.

After you have set up per app VPN configurations, you can select a configuration in the **Edit package** view of an application, see *Configure per app VPN and settings for iOS apps* (section 16.2).

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

**Single sign-on**
Minimum requirement: iOS version 7.0+
In this configuration, you can define settings for a single sign-on for third-party apps.
In the **URLs** tab, you can optionally set up a list of URL prefixes that must be matched to use this account for Kerberos authentication through HTTP. If you do not specify prefixes here, the account matches all http:// and https:// URLs.

In the **App identifiers** tab, you can optionally set up a list of app identifiers that are allowed to use this login. If you do not specify app identifiers here, the login matches all identifiers.

### Single app mode

**Minimum requirements: iOS version 6.0+ supervised**

In this configuration, you can define settings for the single mode that locks end user devices into a single app and prevents users from changing to other apps.

<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
<th>Minimum requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select source</strong></td>
<td>In this field, you can select the source for the single app:</td>
<td><strong>7.0+</strong></td>
</tr>
<tr>
<td></td>
<td>■ If you select <strong>App list</strong>, the <strong>Apps</strong> dropdown list is displayed with a list of all available iOS apps for this customer. Select the app from the list and click <strong>Apply</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ If you select <strong>Custom</strong>, the field <strong>App identifier</strong> is displayed. Enter the app identifier and click <strong>Apply</strong>.</td>
<td></td>
</tr>
<tr>
<td><strong>Options</strong></td>
<td>Select this option to disable touch for single app mode.</td>
<td><strong>7.0+</strong></td>
</tr>
<tr>
<td><strong>Disable touch</strong></td>
<td>Select this option to disable rotation for single app mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Disable rotation</strong></td>
<td>Select this option to disable rotation for single app mode.</td>
<td></td>
</tr>
<tr>
<td>Setting/field</td>
<td>Description</td>
<td>Minimum requirements</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Disable volume buttons</td>
<td>Select this option to disable volume buttons for single app mode.</td>
<td></td>
</tr>
<tr>
<td>Disable ringer switch</td>
<td>Select this option to disable ringer switch for single app mode.</td>
<td></td>
</tr>
<tr>
<td>Disable sleep wake button</td>
<td>Select this option to disable the wake button for single app mode.</td>
<td></td>
</tr>
<tr>
<td>Disable auto lock</td>
<td>Select this option to disable auto lock for single app mode.</td>
<td></td>
</tr>
<tr>
<td>Enable voice over</td>
<td>Select this option to enable voice over for single app mode.</td>
<td></td>
</tr>
<tr>
<td>Enable zoom</td>
<td>Select this option to enable zoom for single app mode.</td>
<td></td>
</tr>
<tr>
<td>Enable invert colors</td>
<td>Select this option to enable the inversion of colors for single app mode.</td>
<td></td>
</tr>
<tr>
<td>Enable AssistiveTouch</td>
<td>Select this option to enable AssistiveTouch for single app mode.</td>
<td></td>
</tr>
<tr>
<td>Enable speak selection</td>
<td>Select this option to enable speak selection for single app mode.</td>
<td></td>
</tr>
<tr>
<td>Enable mono audio</td>
<td>Select this option to enable mono audio for single app mode.</td>
<td></td>
</tr>
<tr>
<td>User enabled options</td>
<td></td>
<td>7.0+</td>
</tr>
<tr>
<td>Voice over</td>
<td>Select this option to allow Voice Over adjustment.</td>
<td></td>
</tr>
<tr>
<td>Zoom</td>
<td>Select this option to allow Zoom adjustment.</td>
<td></td>
</tr>
<tr>
<td>Invert colors</td>
<td>Select this option to allow Invert Colors adjustment.</td>
<td></td>
</tr>
<tr>
<td>AssistiveTouch</td>
<td>Select this option to allow AssistiveTouch adjustment.</td>
<td></td>
</tr>
</tbody>
</table>
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>Description</td>
<td>In this field, enter a description for the web clip.</td>
</tr>
<tr>
<td>URL</td>
<td>In this field, enter the URL for the web clip.</td>
</tr>
<tr>
<td>Can be removed</td>
<td>If you deactivate this option, the user cannot remove the web clip.</td>
</tr>
<tr>
<td></td>
<td>It cannot be deleted from the device unless the user removes the profile that installed it.</td>
</tr>
<tr>
<td>Full screen</td>
<td>If you select this option, the web clip is opened full screen on the device.</td>
</tr>
<tr>
<td></td>
<td>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>Access point name (APN)</td>
<td>In this field, enter the name of the access point of the carrier (GPRS).</td>
</tr>
<tr>
<td>User name for access point</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>Password for access point</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>
</tbody>
</table>
### Web content filter

Minimum requirements: iOS version **7.0+ supervised**

In this configuration, you can define URL blacklists and whitelisted bookmarks.

<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Blacklist**               | Select this field to define a blacklist of URLs that may not be accessed on end user devices. Click **Next** to display the **Web Content Filter** view. In this view, you can add individual URLs or import blacklisted URLs from a .csv file.  
**Note:** If you do not have a .csv file with blacklisted URLs yet, you can download a sample file from the **Import blacklist** view in the web console and use it for creating your import file.  
In the **Web Content Filter** view, the **Export blacklist** button is available for exporting the blacklist configured in the web console to a .csv file. |
| **Whitelist with bookmarks**| Select this field, to define a whitelist with bookmarks to be added to the Safari browser on end user devices. All other sites are blocked. Click **Next** to display the **Web Content Filter** view. In this view, you can add individual URLs as bookmarks.                                                                          |

### Global HTTP proxy

Minimum requirement: **supervised**

**Note:** This configuration is only effective for supervised devices.

With this configuration, you can configure a single corporate proxy server. You can only add one **Global HTTP proxy** configuration within a profile.
<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global proxy</td>
<td>In this field, select the proxy settings for the connection:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Manually</strong></td>
</tr>
<tr>
<td></td>
<td>If you select this option, the fields <strong>Server and port</strong>, <strong>Authentication</strong> and <strong>Password</strong> are displayed. In the <strong>Server and port</strong> field, enter the valid address and the port of the proxy server. In the <strong>Authentication</strong> field, enter the user name for the connection to the proxy server. In the <strong>Password</strong> field, enter the password for the connection to the proxy server.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Automatically</strong></td>
</tr>
<tr>
<td></td>
<td>If you select this option, the <strong>Proxy server URL</strong> field is displayed. Enter the URL of the server with the proxy setting in this field.</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: [ [ &quot;C&quot;, &quot;US&quot; ] ], [ &quot;O&quot;,&quot;Apple Inc.&quot; ] ], ..., [ &quot;1.2.5.3&quot;,&quot;bar&quot; ] ]</td>
</tr>
<tr>
<td>Type of subject alternative name</td>
<td>In this field, select the type of an alternative name for the SCEP server:</td>
</tr>
<tr>
<td></td>
<td>■ None</td>
</tr>
<tr>
<td></td>
<td>■ RFC 822 name (email address)</td>
</tr>
<tr>
<td></td>
<td>■ DNS name</td>
</tr>
<tr>
<td></td>
<td>■ Uniform Resource Identifier</td>
</tr>
<tr>
<td></td>
<td>If you select any other option than None, the fields <strong>Value of subject alternative name</strong> and <strong>NT user login name</strong> are displayed below the field <strong>Type of subject alternative name</strong>. Enter the required name values.</td>
</tr>
<tr>
<td>Challenge</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></td>
<td><strong>Note:</strong> If the SCEP module of the Sophos Mobile Control server is used, this field is prefilled with %<em>CACHALLENGE</em>%. Do not change this value.</td>
</tr>
<tr>
<td>Retries</td>
<td>In this field, enter the number of retries if the server sends a &quot;pending&quot; response.</td>
</tr>
<tr>
<td>Retry delay</td>
<td>In this field, enter the number of seconds between retries.</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](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 **Profiles** and click **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 and Windows Phone 8 devices

1. In the web console, go to Profiles and click Android or Windows Phone 8.
   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. For Android profiles: In the ID field, enter a unique ID for the profile.
   Note: This step does not apply for Windows Phone 8 profiles, where the ID field is not available.

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/Windows Phone 8 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) or Available Windows Phone 8 configurations (section 17.2.2).

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 for Android or Windows Phone 8.

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 and on the on the Android version in use on individual devices. Depending on the end user device, some settings may not have any effect. In the individual configuration, the web console shows labels to indicate if any setting is supported as of a particular Android version or only for devices with the Samsung Safe plugin (for example SAFEv2+) or with an active TouchDown email client (TouchDown). In the following
settings descriptions the relevant information is included at the beginning of the section or in a minimum requirements column, if applicable.

**Password policies**

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

When you select the **Password policies** configuration, the **Password type** field is displayed. In this field, select the type of password you want to define:

- **Any**
  
  If you select this setting, users have to set a password on their devices. But there are no requirements or restrictions concerning the password. If you have selected this option, no further settings are required for the **Password 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 password length</td>
<td>Specifies the minimum number of characters a password must contain.</td>
</tr>
<tr>
<td>Idle time in seconds before password 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 password.</td>
</tr>
<tr>
<td>Maximum password age (in days)</td>
<td>Requires users to change their password in the specified interval (in days).</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 password before the device is wiped.</td>
</tr>
<tr>
<td>Minimum history length</td>
<td>In this field, you can specify how many old passwords are remembered and compared with new ones. When the user defines a new password, it will not be accepted, if it matches a previously used password. 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 password types:

<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum number of letters</td>
<td>Specifies the minimum number of letters a password must contain.</td>
</tr>
<tr>
<td>Minimum number of lowercase letters</td>
<td>Specifies the minimum number of lowercase letters a password must contain.</td>
</tr>
<tr>
<td>Minimum number of uppercase letters</td>
<td>Specifies the minimum number of uppercase letters a password must contain.</td>
</tr>
<tr>
<td>Minimum number of non-alphabetic characters</td>
<td>Specifies the minimum number of non-alphabetic characters (for example &amp; or !) a password must contain.</td>
</tr>
<tr>
<td>Minimum number of numbers</td>
<td>Specifies the minimum number of numbers a password must contain.</td>
</tr>
<tr>
<td>Minimum number of special characters</td>
<td>Specifies the minimum number of special characters (for example !&quot;#$%&amp;/()=+-;@&lt;&gt; ) a password 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>
<th>Minimum requirements</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>
<td>SAFEv2+</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>
<td>SAFEv2+</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>
<td>SAFEv2+</td>
</tr>
<tr>
<td>Setting/field</td>
<td>Description</td>
<td>Minimum requirements</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Allow native browser</td>
<td>If you deactivate this option, native browsers are disabled on the device.</td>
<td>SAFEv2+</td>
</tr>
<tr>
<td>Allow camera</td>
<td>If you deactivate this option, cameras are completely disabled on the device.</td>
<td>SAFEv2+ 4.0+</td>
</tr>
<tr>
<td>Allow camera on lock screen</td>
<td>If you deactivate this option, cameras are disabled on the device when the screen is locked.</td>
<td>4.2+</td>
</tr>
<tr>
<td>Allow widgets on lock screen</td>
<td>If you deactivate this option, widgets are disabled on the device when the screen is locked.</td>
<td>4.2+</td>
</tr>
<tr>
<td>Allow clipboard</td>
<td><strong>Note:</strong> This setting applies to devices as of Android 4.2.2. If you deactivate this option, users cannot copy any contents to the clipboard.</td>
<td>SAFEv2+</td>
</tr>
<tr>
<td>Allow Play Store</td>
<td><strong>Note:</strong> This setting applies to devices as of Android 4.2.2. If you deactivate this option, Play Store is disabled on the device.</td>
<td>SAFEv2+</td>
</tr>
<tr>
<td>Allow non-market apps</td>
<td>If you deactivate this option, non-market apps are disabled on the device.</td>
<td>SAFEv2+</td>
</tr>
<tr>
<td>Allow Bluetooth</td>
<td>If you deactivate this option, Bluetooth is disabled on the device.</td>
<td>SAFEv2+</td>
</tr>
<tr>
<td>Allow NFC</td>
<td>If you deactivate this option, NFC (near field communication) is disabled on the device.</td>
<td>SAFEv2+</td>
</tr>
<tr>
<td>Allow screen capture</td>
<td>If you deactivate this option, users cannot take a screenshot of the display.</td>
<td>SAFEv2+</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>
<td>SAFEv2+</td>
</tr>
<tr>
<td>Allow USB debugging</td>
<td>If you deactivate this option, USB debugging is disabled on the device.</td>
<td>SAFEv2+</td>
</tr>
</tbody>
</table>
### Setting/field

<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
<th>Minimum requirements</th>
</tr>
</thead>
<tbody>
<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>
<td>SAFEv2+</td>
</tr>
<tr>
<td>Allow WiFi tethering</td>
<td>If you deactivate this option, WiFi tethering is disabled on the device.</td>
<td>SAFEv2+</td>
</tr>
<tr>
<td>Allow USB tethering</td>
<td>If you deactivate this option, USB tethering is disabled on the device.</td>
<td>SAFEv2+</td>
</tr>
<tr>
<td>Allow Bluetooth tethering</td>
<td>If you deactivate this option, Bluetooth tethering is disabled on the device.</td>
<td>SAFEv2+</td>
</tr>
<tr>
<td>Allow sync while roaming</td>
<td>If you deactivate this option, synchronisation while roaming is disabled.</td>
<td>SAFEv3+</td>
</tr>
<tr>
<td>Allow mobile data connection while roaming</td>
<td>If you deactivate this option, mobile data connections while roaming are disabled.</td>
<td>SAFEv2+</td>
</tr>
<tr>
<td>Allow voice calls while roaming</td>
<td>If you deactivate this option, voice calls while roaming are disabled.</td>
<td>SAFEv3+</td>
</tr>
<tr>
<td>Allow application crash reports</td>
<td>If you deactivate this option, application crash reports are disabled.</td>
<td>SAFEv4+</td>
</tr>
</tbody>
</table>

### App protection

In this configuration, you can define settings for protecting apps on end user devices with passwords. With app protection in use, users have to define a password when they start a protected app for the first time. In the **App protection** configuration, you define password requirements and the apps to be protected. After a failed login attempt a login delay is imposed.

If app protection is active on an end user device, a button is available in the **Edit device** view to reset the password defined by the user. For a description of this button and all other function buttons available the **Edit device** view, see *Carry out administrative tasks* (section 21.4). The user can also reset the app protection password in the Self Service Portal. For further information, see the *Sophos Mobile Control user guide for Android*.

You can add only one **App protection** configuration within a profile.
In this field define the minimum complexity requirements for the password to be defined by users, for example 6 char password.

Grace period in minutes

In this field, select a grace period. After the grace period has expired protected apps can only be unlocked by entering a password.

Click the Add icon to add apps to be password-protected. In the Edit identifier view, the following fields are available for configuring apps to be protected:

Select source

Select the source for the apps to be added to the list of protected apps. Depending on your choice, different fields for defining the apps to be protected are displayed:

- If you select App list, the Apps dropdown list is displayed with a list of all available Android apps for this customer. Select the app from the list and click Apply.
- If you select Custom, the fields App name and Identifier are displayed. Enter the app information and click Apply.

**Exchange ActiveSync**

Minimum requirements: SAFEv2+ TouchDown

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

**Note:** Some of the settings in this configuration only apply to devices with an active TouchDown email client. These settings are indicated by the label TouchDown in the web console.

If a TouchDown client is active on a user device, this client will be used as the primary email client in Sophos Mobile Control 3.6 and later.
<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
<th>Minimum requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>In this field, enter an account name.</td>
<td></td>
</tr>
<tr>
<td>Server address</td>
<td>In this field, enter the address of the Microsoft Exchange Server.</td>
<td></td>
</tr>
<tr>
<td>Domain</td>
<td>In this field, enter the domain for this account.</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>In this field, enter the user for this account. You can use the variable %USERNAME_% and the server will replace it with the actual user name, if the device the profile is sent to has an LDAP link established.</td>
<td></td>
</tr>
<tr>
<td>Email address</td>
<td>In this field, enter the email address of the account. You can use the variable %EMAILADDRESS_% and the server will replace it with the actual email address, if the device the profile is sent to has an LDAP link established.</td>
<td></td>
</tr>
<tr>
<td>Sender</td>
<td>In this field, enter a sender name for this account. You can use the variable %EMAILADDRESS_% and the server will replace it with the actual email address, if the device the profile is sent to has an LDAP link established.</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>In this field, enter the password for this account.</td>
<td></td>
</tr>
<tr>
<td>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>
<td></td>
</tr>
<tr>
<td></td>
<td>■ One day</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Three days</td>
<td></td>
</tr>
<tr>
<td>Setting/field</td>
<td>Description</td>
<td>Minimum requirements</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------</td>
</tr>
</tbody>
</table>
|                               | ■ One week  
■ Two weeks  
■ One month                                                                                                                           |                      |
| Synchronization interval      | In this field, select the interval between email synchronization processes:  
■ Never  
■ 5 minutes  
■ 10 minutes  
■ 15 minutes  
■ 30 minutes  
■ 1 hour                                                                                                                                |                      |
| Require manual sync when roaming | If you select this option, manual synchronization is required while roaming on a device with an active TouchDown email client. | TouchDown            |
| 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.                                                                 |                      |
| Disable copy/paste            | Select this option to disable copy/paste on devices with an active TouchDown email client.                                                     | TouchDown            |
| Disable copy to phonebook     | Select this option to prevent users from copying details to their phonebooks on devices with an active TouchDown email client.               | TouchDown            |
**Minimum requirements**

<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
<th>Minimum requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>TouchDown</td>
<td>Select this option to disable printing on devices with active TouchDown email clients.</td>
<td>TouchDown</td>
</tr>
</tbody>
</table>

**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>
</tbody>
</table>
| 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  
  - 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 |
VPN
Minimum requirement: SAFEv2+
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>
<tr>
<td>Connection type</td>
<td>In this field, select the connection type:</td>
</tr>
<tr>
<td></td>
<td>■ IPsec (PSK)</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>■ IPsec (Certificate)</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

Root certificate
Minimum requirement: SAFEv2+
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
Minimum requirement: SAFEv2+
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.

### 17.2.2 Available Windows Phone 8 configurations

The following configurations are available for Windows Phone 8 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.

**Password policies**

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

<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password type</strong></td>
<td>In this field, select the type of password you want to define:</td>
</tr>
<tr>
<td></td>
<td>■ Alphanumeric</td>
</tr>
<tr>
<td></td>
<td>■ Alphanumeric or numeric</td>
</tr>
<tr>
<td><strong>Allow simple password</strong></td>
<td>If you select this option, users are allowed to use sequential or repeated</td>
</tr>
<tr>
<td></td>
<td>characters in their password, for example &quot;1111&quot; or &quot;abcde&quot;.</td>
</tr>
<tr>
<td><strong>Minimum password length</strong></td>
<td>Specifies the minimum number of characters a password must contain.</td>
</tr>
<tr>
<td><strong>Maximum number of failed attempts (1 - 999 or 0)</strong></td>
<td>In this field, you can specify the maximum number of failed attempts to enter the correct password before the device is wiped.</td>
</tr>
<tr>
<td><strong>Time in minutes until the device is locked (1 - 999 or 0)</strong></td>
<td>In this field, you can specify when (minutes) the device should be locked after it has not been used. The device can be unlocked by entering the password.</td>
</tr>
<tr>
<td><strong>Password history (1 - 50 or 0)</strong></td>
<td>In this field, you can specify how many old passwords are remembered and compared with new ones. When the user defines a new password, it will not be accepted, if it matches a previously used password.</td>
</tr>
</tbody>
</table>
### Setting/field | Description
--- | ---
| | password. Value range: 1 to 50 or 0 (no password history).
| Maximum password age (1 - 730 days or 0) | Requires users to change their password in the specified interval. Value range: 0 (no password change required) to 730 days.
| Minimum number of different character groups | Specifies the minimum number of non-alphanumeric characters (for example & or !) a password must contain.

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

### Setting/field | Description
--- | ---
| Allow SD card | If you deactivate this option, SD cards cannot be used in devices.
| Allow unencrypted device | If you deactivate this option, devices must be encrypted.

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

### Setting/field | Description
--- | ---
| Name | In this field, enter an account name.
| Server address | In this field, enter the address of the Microsoft Exchange Server.
| SSL | Make sure that this option is selected, to send all communication through SSL (Secure Socket Layer).
| Domain | In this field, enter the domain for this account.
| User | In this field, enter the user for this account. You can use the variable %USERNAME% and the server
<table>
<thead>
<tr>
<th>Setting/field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email address</td>
<td>In this field, enter the email address of the account. You can use the variable <code>%_EMAILADDRESS_%</code> and the server will replace it with the actual email address, if the device the profile is sent to has an LDAP link established.</td>
</tr>
<tr>
<td>Password</td>
<td>In this field, enter the password for this account.</td>
</tr>
</tbody>
</table>
| Synchronization interval | In this field, select the interval between synchronization processes:  
- Sync on receipt  
- Manually  
- 10 minutes  
- 15 minutes  
- 30 minutes  
- One hour |
| Synchronization period | In this field, select the time period for synchronization. This is the number of days items are synchronized for. If you specify a time period here, not all items are synchronized to the inbox on the mobile device, but only the items from within the specified period. You can select the following synchronization periods:  
- Unlimited  
- Three days  
- One week  
- Two weeks  
- One month |
| Synchronize content types | In this field you select the type of items that are synchronized:  
- Email  
- Contact |
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.

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 Profiles 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 Mobile devices

1. In the web console, go to Profiles, and click 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 iOS, Android or Windows Mobile profiles

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

   The **Profiles** view for the mobile device type selected is displayed.

2. Click the **Transfer** button.

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

3. 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.

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

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

6. Under **Scheduled date**, select **Now** or specify a **Date** and **Time** for the execution of this task.
7. 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 Transfer Windows Phone 8 profiles

1. In the web console menu bar, go to **Profiles** and click **Windows Phone 8**.
   The **Profiles** view for Windows Phone 8 is displayed.

2. Click the **Transfer** button.
   The **Select device(s)** view is displayed.

3. 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.

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

5. Select the profile you want to transfer and click **Next**.
   The **Confirm** view is displayed.

6. Click the **Finish** button.
   The profile is transferred to the selected device(s) during the next synchronization process.

### 17.8 Download iOS, Android and Windows Phone 8 profiles from the web console

You can download iOS, Android and Windows Phone 8 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 **Profiles** and click the required mobile device type: **Apple iOS**, **Android** or **Windows Phone 8**.
   The **Profiles** view for the mobile device type selected is displayed.
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 .mobileconfig files (Plist), Android profiles as .smcprofile files (xml format) and Windows Phone 8 profiles as .windowsphoneconfig files.
18 Work 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 rules (section 12).

18.1 Create task bundles

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

2. Click the **Transfer** button.
   
   The **Select device(s)** view is displayed.

3. In this view, you can:
   
   - Select individual devices you want to transfer the task bundle to.
   - Click the **Group selection** button, to open the **Group selection** view and select one or several device groups for transferring the task bundle.

4. After you have made your selection, click **Next**.
   
   The **Select task bundle** view is displayed.

5. Select the task bundle to be transferred and click **Next**.
   
   The **Set execution date** view is displayed.

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

7. 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 Work with command bundles

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

**Note:** This function may not be available for you, depending on your personal settings. For further information, see *Configure personal settings* (section 9).

**Note:** Improperly used commands may lock or even damage devices. Therefore only expert 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

**Prerequisite:** The Command bundle function is enabled in your personal settings.

1. In the web console menu bar, click Command 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 WM6 (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>Windows Mobile</th>
<th>Android</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>ImsiChangeNotifyDelay</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 that are not being edited. Copies are named “Copy of” plus the name of the original. You can rename the bundles according to your requirements.

**Prerequisite:** The Command bundles function is enabled in your personal settings.

1. In the web console menu bar, click Command 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

Prerequisite: The Command bundle function is enabled in your personal settings.

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

2. Click the Transfer button.
   The Select device(s) view is displayed.

3. 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.

4. After you have made your selection, click Next.
   The Select command bundle view is displayed.

5. Select the command bundle to be transferred and click Next.
   The Set execution date view is displayed.

6. Under Scheduled date, select Now or specify a Date and Time for the execution of this task.
7. 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
- Windows Phone 8

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, Windows Phone 8 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. For information on how to define the user management methods for Sophos Mobile Control as a Service, see *Configure Self Service Portal user management for Sophos Mobile Control as a Service* (section 20.3.1).

To create a Self Service Portal group:

1. In the web console menu bar, click **Users**.
   
   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 web console menu bar, go to **Settings** and click **Self Service Portal**.

   The **Self Service Portal** view is displayed.

2. In the **Configuration** tab, configure the following settings:

   a) 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.

   b) Under **Available functionality**, 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 iOS, Android or Windows Phone 8 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.
- **Reset password**
  With this function users can reset their unlock screen password. For Android devices, a new password is set. The device can only be unlocked with the new password. For iOS, the password is completely deleted. The user has to set a new password within 60 minutes.

- **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 and Windows Phone 8 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 and Windows Phone 8 devices. To ensure that activation works, the app has to be opened once before on the device. The activation process is different for iOS and Windows Phone 8 devices. For iOS, a push message with credentials is sent. The Sophos Mobile Control app can process this push message. For Windows Phone 8, an email with credentials and a configuration link is sent. Select this function to enable users of iOS and Windows Phone 8 devices to register and provision their devices through the Self Service Portal.

3. Go to the **Agreement** tab and configure the following:

   a) **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.

   b) **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.

4. Go to the **Group settings** tab. In this tab, 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 external user management, you can assign phones to groups and profiles based on external directory group membership.

**Note:** External user management has to be configured for the relevant customer in customer management. For information on how to configure external 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. For information on how to define the user management methods for Sophos Mobile Control as a Service, see *Configure Self Service Portal user management for Sophos Mobile Control as a Service* (section 20.3.1).

a) Under **Group** settings, click the **Add** button.

The **Edit group settings** view is displayed.

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

c) In the **Directory group** field, enter the Self Service Portal Group you have defined in the internal user management or the external user management 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 **Enrollment package**, 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 *Work 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.
5. Go to the **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 Self Service Portal users managed by internal user management, see *Manage Self Service Portal users* (section 20.3).

6. 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".

7. 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_
   - _CUSTOMERNAME_

   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.

8. 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:

- **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.

- **External user management**
  
  With external user management you can assign devices to groups and profiles based on external directory membership.

   **Note:** The method used is customer-specific and is defined when the customer is created. For further information on how to define the method and on external user management, 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. For information on how to define the user management methods for Sophos Mobile Control as a Service, see *Configure Self Service Portal user management for Sophos Mobile Control as a Service* (section 20.3.1).
20.3.1 Configure Self Service Portal user management for Sophos Mobile Control as a Service

Note: This section only applies to Sophos Mobile Control as a Service. If you use Sophos Mobile Control as an on-premise installation, the user management for Self Service Portal users is configured by the super administrator for each customer. For further information, see the Sophos Mobile Control super administrator guide.

1. In the web console menu bar, go to Settings and click System setup.
   
   The System setup view is displayed.

2. Go to the User setup tab. In this tab, select the data source for the Self Service Portal (SSP) users to be managed by Sophos Mobile Control:

   - None. No SSP and user-specific profiles available.
   - Select Internal directory to use internal user management for users of the Sophos Mobile Control Self Service Portal. For further information, see the Sophos Mobile Control administrator guide.
   - Select External directory to use external user management for users of the Sophos Mobile Control Self Service Portal.

   Click Configure external directory to specify the server details, see Configure external directory connection for Active Directory for Sophos Mobile Control as a Service (section 20.3.1.1) or Configure external directory connection for Novell eDirectory for Sophos Mobile Control as a Service (section 20.3.1.2).

3. Click the Save button.

   If you have selected Internal directory or External directory, the selected option and the option None. No SSP and user-specific profiles available are displayed in the User setup tab. If you want to change your selection afterwards, select None. No SSP and user-specific profiles available first to make all options available.

   Note: The user management configuration cannot be changed as long as there are any devices linked to the directory. If you try to change the configuration while devices are still connected, an error message is displayed.

20.3.1.1 Configure external directory connection for Active Directory for Sophos Mobile Control as a Service

Note: This section only applies to Sophos Mobile Control as a Service. If you use Sophos Mobile Control as an on-premise installation, the user management for Self Service Portal users is
configured by the super administrator per customer. For further information, see the *Sophos Mobile Control super administrator guide*.

1. In the web console menu bar, go to **Settings** and click **System setup**.
   
The **System setup** view is displayed.

2. In the **User setup** tab, select **External directory** to use external user management for users of the Sophos Mobile Control Self Service Portal.

3. Click **Configure external directory** to specify the directory server details.
   
The **Directory server details** view is displayed.

4. In this view, enter the following:
   
a) In the **Primary URL** field, enter the URL of the server. You can enter the server IP or the server name. Select **SSL** to use SSL for the server connection.

b) In the **Backup URL** field, enter the URL of the backup server. You can enter the server IP or the server name. Select **SSL** to use SSL for the server connection.

c) In the **User** field, enter a user who has reading rights for the server. You need to enter the user with the relevant domain. Supported formats are: `<domain><user name>` or `<user name>@<domain>.<domain code>`.

d) In the **Password** field, enter the password for the user.

   Click **Next**.

   The **Searchbase** view is displayed.

5. Select the searchbase. The searchbase defines where to search for the user/group that tries to log in to the Self Service Portal. Click **Next**.

   The **Search Fields** view is displayed.

6. In this step, you define which fields are to be used for resolving the placeholders `%_USERNAME_%` and `%_EMAILADDRESS_%` in profiles. Select the required fields from the **User name** and **Email** dropdown lists.

   **Note:** The fields listed are the LDAP fields defined for the user you have specified. For example: If no email address is defined for this user, the mail field is not listed. You can enter field names manually.

   Click **Next**.

   The **LDAP SSP Configuration** view is displayed.

7. In the **SSP group** field, enter the name of the group that is to be allowed to log on at the Self Service Portal. This group has to be defined on the LDAP server. After you have entered the group, click the **Resolve group** button to resolve the group name into a complete Distinguished Name (DN).
8. Click the Finish button.
   The System setup view is displayed again.

9. Click the Save button to save your changes.

20.3.1.2 Configure external directory connection for Novell eDirectory for Sophos Mobile Control as a Service

Note: This section only applies to Sophos Mobile Control as a Service. If you use Sophos Mobile Control as an on-premise installation, the user management for Self Service Portal users is configured by the super administrator per customer. For further information, see the Sophos Mobile Control super administrator guide.

1. In the web console menu bar, go to Settings and click System setup.
   The System setup view is displayed.

2. In the User setup tab, select External directory to use external user management for users of the Sophos Mobile Control Self Service Portal.

3. Click Configure external directory to specify the server details.
   The Directory server details view is displayed.

4. In this view, enter the following:
   a) In the Primary URL field, enter the URL of the server. You can enter the server IP or the server name. Select SSL for the server connection.
   b) In the Backup URL field, enter the URL of the backup server. You can enter the server IP or the server name. Select SSL to use SSL for the server connection.
   c) In the User field, enter a user who has reading rights for the server. You need to enter the user with the relevant domain.
   d) In the Password field, enter the password for the user.
   Click Next.
   The Searchbase view is displayed.

5. Leave the Searchbase view empty and click Next.
   The Search Fields view is displayed.

6. In this step, you define which LDAP fields are to be used for resolving the placeholders %_USERNAME_% and %_EMAILADDRESS_% in profiles. Select the required fields from the User name and Email dropdown lists.
   Usually "uid" and "mail" are used.
   Click Next.
   The LDAP SSP Configuration view is displayed.
7. In the **SSP group** field, enter the name of the group that is to be allowed to log on at the Self Service Portal. This group has to be defined on the server. After you have entered the group, click the **Resolve group** button to resolve the group name into a complete Distinguished Name (DN).

8. Click the **Finish** button.

   The User Setup view is displayed again.

9. Click the **Save** button to save your changes.

### 20.3.2 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. Super administrators are not supported in Sophos Mobile Control as a Service. For information on how to define the user management methods for Sophos Mobile Control as a Service, see *Configure Self Service Portal user management for Sophos Mobile Control as a Service* (section 20.3.1).

1. In the web console menu bar, click **Users**.

   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 **Welcome email** tab in **Settings** under **Self Service Portal**, 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** (optional)

4. Click the **Save** button.

   The new Self Service Portal user is displayed in the Show users view. A welcome email is sent to the new user.
20.3.3 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. For information on how to define the user management methods for Sophos Mobile Control as a Service, see *Configure Self Service Portal user management for Sophos Mobile Control as a Service* (section 20.3.1).

1. In the web console menu bar, click **Users**.
   
   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 **Welcome email** tab in **Settings** under **Self Service Portal**, 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.
20.3.4 Use the user filter

By using filters you can restrict the number of items shown in lists according to defined criteria. With the user filter, you can filter the user list in the internal user management.

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

1. In the web console menu bar, click Users.
   The Show users view is displayed.

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

3. In the User 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 user name.</td>
</tr>
<tr>
<td>Email address</td>
<td>Filter according to email address.</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 user filter in the User filter dialog changes to Filter is active.
21 Administer 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.
- Lock or unlock devices remotely.
- Reset the passcodes/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, you can see the most important device information at a glance:

- Status (Managed or Not Managed)
- Compliant (Yes or No)
- Operating system
- Email access (Yes or No)
- Last synchronization

- For iOS and Windows Phone 8 devices, the Last app synchronization is shown.
Owner (Company device or Employee device)

Name

Description

User

If the device has an LDAP connection to an external user directory, the corresponding user name is shown here.

Email address

Device group

Device ID

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).

Installed profiles (iOS, Android and Windows Phone 8)

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.

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 (iOS, Android and Windows Mobile)**
  
  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.

- **System software (Android)**
  
  Shows Android system software on the device.
  
  **Note:** System software cannot be removed from the device.

- **Certificates (iOS and Windows Phone 8)**
  
  Shows the certificates in use on the 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 click 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>
</tbody>
</table>
| Exchange Active Sync| Select **Allowed**, to show all devices for which email access is allowed. Select **Not allowed**, to show all devices for which email access is not allowed.  
                      | **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 **Exchange Active Sync** field is not available. |
| Package             | Filter according to software package. In the fields **Name**, **Identifier** and **Version**, enter the details for the relevant software package. In the dropdown list, select **installed** to show all devices with the package installed. Select **not installed** to show all devices on which the package is not installed. |
| Device group        | Filter according to device group devices are assigned to.                                                                                  |
| Operating System    | Filter according to operating system. Here you can deselect devices equipped with a specific operating system.                           |
| Device property     | Filter according to a specific device property. Enter the **Name** and the **Value** of the device property.                                |

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 click 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 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 Assign a user to a device

You can assign users managed with internal user management to devices. If you use external user management, you can assign a user from an external directory to a device.

**Note:** The user management 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. Super administrators are not supported in Sophos Mobile Control as a Service. For information on how to define the user management methods for Sophos Mobile Control as a Service, see *Configure Self Service Portal user management for Sophos Mobile Control as a Service* (section 20.3.1).

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** icon.
   
   The **Edit device** view is displayed for the selected device.

3. Click the **Assign user to device** button.
   
   The **Enter user search parameters** view is displayed.

4. In the fields **Common Name (CN)** and/or **Email address**, enter a search parameter, for example the user name or part of it.
   
   The **Select data set** view is displayed.

5. Select the required user and click **Next**.
   
   The **Select detail fields to use** view is displayed.

6. Select the required **Email address** and the **User name** and click the **Apply** button.
   
   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 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;100839,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>![Image](125x626 to 155x653)</td>
<td>Click this button to set the name and the IMEI of the specific device in the device filter, see <em>Use the device filter</em> (section 21.2.1).</td>
</tr>
<tr>
<td>![Image](125x582 to 155x611)</td>
<td>Click this button to view all tasks for this device.</td>
</tr>
</tbody>
</table>
| ![Image](125x539 to 153x567) | 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. |
| ![Image](125x453 to 156x480) | Click this button to install the Sophos Mobile Control client on the device, see *Provision individual Android, and Windows Phone 8 devices* (section 15.2), or bootstrap an iOS device, see *Provision individual iOS devices* (section 15.3). |
| ![Image](125x401 to 161x431) | Click this button to assign a user to the device by a link to an external directory. |
| ![Image](125x358 to 155x386) | Click this button to unassign a user from the device. |
| ![Image](125x312 to 156x343) | Click this button to refresh device data. |
| ![Image](125x270 to 153x297) | Click this button to open the traffic counter details for the device, see *View data traffic* (section 23.4). |
| ![Image](196x670) | 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. |
<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
</table>
| Email | Indicates that email access is allowed.  
An additional icon on the button indicates whether email access was allowed  
■ manually 🔄  
■ automatically 🔄 .  
Click this button, to deny 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. |
| Warning | 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 | Click this button to lock the device remotely. If you click this button, a dialog is displayed where you can optionally enter a message of up to 300 characters that is to be displayed on the device to be locked. You can also enter a phone number that is to be shown on the device to provide the user with a contact number to call. |
| Reset | 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>| Delete | Click this button to delete all synchronization data of the device. The Sophos Mobile Control client needs to be reinstalled. |
| Wipe | 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. |</p>
<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Message" /></td>
<td>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. For Windows Phone 8 MPNS is used as a push service. If platforms are not managed yet, a text message can be sent, if a phone number has been specified.</td>
</tr>
<tr>
<td><img src="image" alt="Location" /></td>
<td>Click this button to locate an iOS, Android or Windows Phone 8 device.</td>
</tr>
</tbody>
</table>
| ![Backup](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. |
| ![Duplicate](image) | Click this button to duplicate the device. |
| ![Delete](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](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.  
**Note:** This procedure is only necessary for devices with an iOS version below iOS 7. For iOS 7 devices, the Sophos Mobile Control app is activated automatically. |
| ![Decommission](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, Apple iOS and Windows Phone 8 devices. |
| ![Security Scan](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. |
## 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.

**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.
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. We recommend that you put devices into groups. This helps you to manage them efficiently as you can carry out tasks on a group rather than on individual 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.
Monitor 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 details** 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 details** 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 details** view.

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 details** 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 view**.

   The **Task view** is displayed.
2. Click the **Task archive** button.

   The **Task archive** view is displayed. It shows all finished and failed tasks in the system.

3. 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 **Task view** or the **Task archive** click the Filter button (magnifier icon) in the web console header.

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

2. 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>

3. 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>🔄 ›</td>
<td>Installation</td>
</tr>
<tr>
<td>🔽 🔽</td>
<td>Uninstallation</td>
</tr>
<tr>
<td>🔄 🔄</td>
<td>Process activation/deactivation</td>
</tr>
<tr>
<td>🔄 🔄</td>
<td>Explicit refresh of device data.</td>
</tr>
<tr>
<td>📩</td>
<td>Text message to device.</td>
</tr>
<tr>
<td>📄</td>
<td>Windows Mobile profile transfer</td>
</tr>
<tr>
<td>📄</td>
<td>iOS profile transfer</td>
</tr>
<tr>
<td>🔊 🔊</td>
<td>Command bundle transfer</td>
</tr>
<tr>
<td>📊 📊</td>
<td>Task bundle transfer</td>
</tr>
<tr>
<td>🔄 🔄</td>
<td>Bootstrap</td>
</tr>
<tr>
<td>🔄 🔄</td>
<td>Command transfer</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>
<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>

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

**Note:** The Sophos Mobile Control client has been installed successfully. The device is provisioned now.
23 Reports

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

- Chart reports providing an overview on registered devices. You can display the chart reports in the web console by using the Reports function.
- A number of device reports, app reports and compliance reports. You can create these reports as .xlsx files by using the Reports function.
- Reports with detailed information on devices. You can create these reports from the Devices view in the Inventory by exporting device information.
- 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 chart reports 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 menu bar, click Reports.
   The report selection view is displayed.
2. Under Device reports, click Chart reports.
   The Chart reports view is displayed. This view shows the following information in pie charts:
   - Compliant/non-compliant devices
   - Managed/non-managed devices
   - Company/employee devices
   - Devices by operating system type
   - Devices by operating system version per operating system type.

23.2 Create device, app and compliance reports

1. In the web console menu bar, click Reports.
   The report selection view is displayed.
2. Under Device reports, App reports or Compliance reports, select the required report.
   A file download dialog is displayed.
3. Select a file location and click Save.

The report is saved in a .xlsx file at the selected location.

### 23.3 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 **Create 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 14.4).

### 23.4 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, go to **Inventory** and click **Devices**.

   The **Devices** view is displayed.

2. Click the **Traffic counter** button.

   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.
3. 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.

4. 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: This function may not be available for you, depending on your personal settings. For further information, see Configure personal settings (section 9).

Note: Backups are platform-specific.

24.1 Configure backup profiles

Prerequisite: The Backup function is enabled in your personal settings.

1. In the web console menu bar, click Backup.
   The Backup profiles view is displayed.

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

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

4. Under Operating systems, select the operating system the backup profile 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 profile view.
7. Click the Save button.

The new backup profile is displayed under **Backup profiles**. You can now transfer it to devices or device groups.

### 24.2 Transfer backup profiles

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

**Prerequisite:** The Backup function is enabled in your personal settings.

1. In the web console menu bar, click **Backup**.
   
The **Backup profiles** view is displayed.
2. Click the **Transfer** button.
3. 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 profile** view is displayed.
4. Select the backup profile you want to transfer and click **Next**.
   
The **Set execution date** view is displayed.
5. Specify a **Scheduled date** for the transfer of the backup profile.
6. Click the **Finish** button.

   The backup profile is transferred to the selected device(s) or device group(s) at the scheduled date and time.

### 24.3 Restore data from backups

**Prerequisite:** The Backup function is enabled in your personal settings.

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.

You can send messages to individual devices or device groups.

25.1 Send messages to individual devices

1. In the web console menu bar, go to Inventory and click Devices.
   The Devices view is displayed.
2. Click the Show or Edit icon next to the required device.
   The Show device or Edit device view is displayed.
3. Click the Send message button.
   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.
5. Click the Finish button.
6. A message prompting you to confirm that you want to send the message is displayed.
7. Click the Yes button.

25.2 Send messages to device groups

1. In the web console menu bar, go to Inventory and click Device groups.
   The Device groups view is displayed.
2. The next step depends on whether you want to send the message to all or only selected device groups:
   ■ To send a message to all device groups, click the Send Message button in the Device groups view.
   ■ To send a message to a specific device group, click the Show icon next to the required group and click the Send Message button in the Show device group view.
   The Enter message view is displayed.
3. 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.

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

5. Click the Finish button.

The message is sent at the specified date and time.
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 licenses for Software as a Service installations

1. In the web console menu bar, go to Settings and click System setup.
   The System setup view is displayed.
2. In the **SMSec License** tab, enter the license key you have received from Sophos in the **License key** field and click **Activate**.

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

### 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.

**Note:** Default settings are preconfigured. While you are changing settings you can reset them to the default values any time by clicking the **Restore default settings** button.

1. In the web console menu bar, go to **Settings** and click **General**.

   The **General 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 **Enable user to allow apps** to enable users to allow 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 **Webfilter 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 **Standard**, 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 compliance rule or open an existing set for editing. For further information, see Configure compliance rules (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 Sophos Mobile Security 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 Sophos Mobile Security 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" /></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 <a href="#">Select device group(s) view</a>. 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 <a href="#">Select device(s) view</a>. In this view, you can select one or several devices for a process.</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="lightning_bolt.png" alt="Lightning bolt" /></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="edit.png" alt="Edit icon" /></td>
<td>Edit</td>
<td>Opens an edit view where you can change settings or information.</td>
</tr>
<tr>
<td><img src="save.png" alt="Save icon" /></td>
<td>Save</td>
<td>Saves changed settings.</td>
</tr>
<tr>
<td><img src="reload.png" alt="Reload icon" /></td>
<td>Reload</td>
<td>Reloads the contents of a table.</td>
</tr>
<tr>
<td><img src="create.png" alt="Create new icon" /></td>
<td>Create new &lt;item&gt;</td>
<td>Adds an entry, for example a device.</td>
</tr>
<tr>
<td><img src="delete.png" alt="Delete icon" /></td>
<td>Delete</td>
<td>Deletes a selected entry</td>
</tr>
<tr>
<td><img src="import.png" alt="Import icon" /></td>
<td>Import &lt;items&gt;</td>
<td>Imports entries, for example devices from a CSV list, to Sophos Mobile Control.</td>
</tr>
<tr>
<td><img src="export.png" alt="Export icon" /></td>
<td>Creates a device report (CSV file).</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.