

**SOPHOS**

Security made simple.

# Sophos Mobile Control administrator help (with IoT)

Product version: 7



# Contents

1	About this help.....	6
2	About Sophos Mobile Control.....	7
3	About the Sophos Mobile Control console.....	9
3.1	User interface.....	9
3.2	Table views.....	10
3.3	Prerequisites.....	10
3.4	User roles.....	10
3.5	Login to the Sophos Mobile Control console.....	11
3.6	Log out from the Sophos Mobile Control console.....	12
3.7	Change your password.....	12
3.8	Password recovery.....	12
4	Key steps for managing devices with Sophos Mobile Control.....	13
5	Dashboard.....	14
6	Reports.....	15
7	Tasks.....	16
7.1	Monitor tasks.....	16
8	General settings.....	19
8.1	Configure personal settings.....	19
8.2	Configure password policies.....	20
8.3	Configure SMC app settings.....	20
8.4	Enable Baidu Cloud Push service.....	21
8.5	Configure iOS settings.....	21
8.6	Configure polling interval for Windows devices.....	22
8.7	Configure Email.....	22
8.8	Configure technical support contact details.....	22
8.9	Define customer properties.....	22
9	Configure Self Service Portal.....	24
9.1	Create Self Service Portal groups with internal user management.....	24
9.2	Configure Self Service Portal settings.....	25
9.3	Available Self Service Portal settings.....	26
9.4	Manage Self Service Portal users.....	29
10	System setup.....	34

10.1	Check your licenses.....	34
10.2	Apple Push Notification service certificates.....	34
10.3	Configure iOS AirPlay destinations.....	38
10.4	Samsung Knox license.....	39
10.5	Configure SCEP.....	39
10.6	Configure user setup.....	40
11	Compliance rules.....	41
11.1	Create compliance rules.....	41
11.2	Available compliance rules.....	43
11.3	Assign compliance rules to device groups.....	48
11.4	Check devices for compliance.....	48
12	Devices.....	49
12.1	Add devices.....	49
12.2	Enroll devices.....	51
12.3	Unenroll devices.....	57
12.4	Manage devices.....	58
12.5	Apple DEP.....	63
13	Device groups.....	71
13.1	Create device group.....	71
13.2	Delete device groups.....	71
14	Profiles and policies.....	72
14.1	Create profile or policy.....	72
14.2	Import iOS device profiles created with Apple Configurator.....	73
14.3	Import provisioning profiles for iOS apps.....	74
14.4	Windows Desktop password complexity rules.....	74
14.5	Samsung Knox support.....	75
14.6	Placeholders in profiles and policies.....	75
14.7	Install a profile onto devices.....	76
14.8	Assign a policy to devices.....	76
14.9	Remove profile.....	77
14.10	Download profiles and policies.....	77
14.11	Configurations for Android device profiles.....	78
14.12	Configurations for Android for Work policies.....	95
14.13	Configurations for Sophos container policies for Android.....	104
14.14	Configurations for Mobile Security policies.....	114
14.15	Configurations for Knox container profiles.....	114

14.16	Configurations for Android Things policies.....	119
14.17	Configurations for iOS device profiles.....	119
14.18	Configurations for Sophos container policies for iOS.....	145
14.19	Configurations for Windows Mobile policies.....	155
14.20	Configurations for Windows Desktop policies.....	163
14.21	Configurations for Windows IoT policies.....	169
15	Task bundles.....	172
15.1	Create task bundle.....	172
15.2	Available Android task types.....	173
15.3	Available iOS task types.....	176
15.4	Duplicate task bundles.....	178
15.5	Transfer task bundles to individual devices or to device groups.....	179
16	Apps.....	180
16.1	Add app.....	180
16.2	Install app.....	182
16.3	Uninstall app.....	183
16.4	Managed apps for iOS.....	183
16.5	Manage apps purchased through Apple VPP.....	184
16.6	Configure per app VPN and settings for iOS apps.....	189
17	App groups.....	190
17.1	Create app group.....	190
17.2	Import app group.....	191
18	Corporate documents.....	192
18.1	Add corporate documents.....	192
19	Android for Work.....	194
19.1	Set up Android for Work.....	194
19.2	Configure Android for Work.....	198
19.3	Manage Android for Work users.....	199
19.4	Enroll devices with Android for Work.....	199
19.5	Lock work profile.....	200
19.6	Remove work profile from device.....	200
19.7	User-initiated work profile removal.....	201
19.8	Work apps.....	201
20	Create administrators.....	207
21	Send message to devices.....	208
22	Advanced license.....	209

23	Manage Sophos Mobile Security.....	210
23.1	Configure antivirus settings for Sophos Mobile Security.....	210
23.2	Configure web filtering settings for Sophos Mobile Security.....	212
23.3	Define Sophos Mobile Security compliance rules.....	213
23.4	View Sophos Mobile Security scan results.....	213
24	Manage Sophos container apps.....	215
24.1	Reset Sophos container password.....	216
24.2	Lock and unlock the Sophos container.....	216
24.3	Corporate keyring synchronization.....	217
25	Glossary.....	218
26	Technical support.....	220
27	Legal notices.....	221

# 1 About this help

This help describes how to use the Sophos Mobile Control console.

Further information is available in the following documents:

- For a description of Sophos Mobile Control installation, see the [Sophos Mobile Control installation guide](#). This guide is not relevant for Sophos Mobile Control as a Service.
- For information on how to use the Sophos Mobile Control console as a super administrator for customer management, see the [Sophos Mobile Control super administrator guide](#). This guide is not relevant for Sophos Mobile Control as a Service.
- For a description of the key steps for initial configuration, see the [Sophos Mobile Control startup guide](#) and the [Sophos Mobile Control as a Service startup guide](#).
- For information on the Sophos Mobile Control Self Service Portal, see the [Sophos Mobile Control user help](#).

## Document conventions

The following conventions are used in this help:

- Unless otherwise noted, *Windows Mobile* refers to Windows 10 *Mobile* and *Mobile Enterprise* editions and to Windows Phone 8.1.
- Unless otherwise noted, *Windows Desktop* or *Windows 10 Desktop* refers to Windows 10 *Pro*, *Enterprise*, *Education*, and *Home* editions.
- Unless otherwise noted, *Windows IoT* refers to the Windows 10 *IoT Core* edition.
- Unless otherwise noted, all procedures assume that you are logged in to the Sophos Mobile Control console using an administrator account.

## 2 About Sophos Mobile Control

### Sophos Mobile Control

Sophos Mobile Control is a management tool for mobile devices like smartphones and tablets, and also for Windows 10 desktop devices. It helps to keep corporate data safe by managing apps and security.

The Sophos Mobile Control system consists of a server and a client component.

The server is the core component of the Sophos Mobile Control product. It provides a web interface to administer Sophos Mobile Control and to manage the enrolled devices.

The client is an app to be installed onto the devices. It supports over-the-air setup and configuration through the web interface of the Sophos Mobile Control server.

With the Sophos Mobile Control Self Service Portal for your users, you can reduce IT effort by allowing users to enroll devices on their own and to carry out other tasks without contacting the helpdesk.

Sophos Mobile Control can also be used to manage the Sophos Mobile Security, Sophos Secure Workspace and Sophos Secure Email mobile apps. This requires an SMC Advanced license.

### Sophos Mobile Security

Sophos Mobile Security is a security app for Android devices. Using up-to-the-minute intelligence from SophosLabs, your apps will be automatically scanned as you install them. This antivirus functionality protects you from malicious software which can lead to data loss and unexpected costs.

### Sophos Secure Workspace

Sophos Secure Workspace is an app for Android and iOS devices that provides a secure workspace where you can browse, manage, edit, share, encrypt and decrypt documents from various storage providers or distributed by your company. It is designed to prevent any data loss even when your device is lost or stolen or when you send a document to an unintended destination.

Files can be decrypted and viewed in a seamless way. Files that are handed over by other apps can be encrypted and either uploaded to one of the supported cloud storage providers or stored locally within Sophos Secure Workspace.

With Sophos Secure Workspace you can read files encrypted by SafeGuard Cloud Storage or SafeGuard Data Exchange. Both are modules of SafeGuard Enterprise or one of its different editions.

Sophos Secure Workspace also includes Corporate Browser, a web browser that lets you securely access corporate intranet pages and other allowed pages, as defined by a Sophos Mobile Control policy.

## Sophos Secure Email

Sophos Secure Email is an app for Android and iOS devices that provides a secure container for managing your email, calendar and contacts. All data is encrypted and is protected from third-party access.



## 3 About the Sophos Mobile Control console

The Sophos Mobile Control 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 portal you can implement a corporate policy for the use of devices and apply it to the devices that are enrolled with Sophos Mobile Control.

In the Sophos Mobile Control 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 [Compliance rules](#) (page 41).
- Enroll devices with Sophos Mobile Control. See [Add devices](#) (page 49).
- Provision new devices. See [Enroll devices](#) (page 51).
- Install application packages on enrolled devices. See [Apps](#) (page 180).
- Define profiles and security policies for devices. See [Profiles and policies](#) (page 72).
- Create task bundles to bundle several tasks and transfer them to the devices in one transaction. See [Task bundles](#) (page 172).
- Configure settings for the Self Service Portal. See [Configure Self Service Portal](#) (page 24).
- Carry out administrative tasks on devices, for example reset the password of devices, lock or wipe devices if they are lost or stolen, unenroll devices. See [Manage devices](#) (page 58).
- Create and view reports. See [Reports](#) (page 15).

### 3.1 User interface

The user interface of the Sophos Mobile Control console is divided into a header, a main menu, and the main frame. The main frame displays the different pages of the Sophos Mobile Control console, based on the selected menu.

- **Header**

The page header has these links on the right side:

- Your account name and the customer name.
- The **Help** button that opens online help in a separate browser window.
- The **Logout** button that logs you off from the Sophos Mobile Control console.

- **Main menu**

The main menu on the left lets you access the main functions of Sophos Mobile Control.

**Note:** Your assigned administrator role affects what you can do. See [User roles](#) (page 10).

## 3.2 Table views

Many pages of the Sophos Mobile Control console display information in a tabular form.

These tables have common controls that you can interact with.

Above the table:

- Use the **Show or hide columns** icon to configure which table columns are visible.
- Enter text in the **Search all fields** field to only display data rows that contain that text in any column. Note that date columns are searched by their internal format `yyyy-mm-dd`.

In the table:

- Click a column header to sort the table rows by that property. Click again to revert the sort order.
- Click the blue triangle next to an entry name to perform actions on that entry, like **Show**, **Edit**, **Delete**.

Below the table:

- Use the navigation buttons to display a specific table page.
- Use the **Export** icon to export either the whole table or the current page to a Microsoft Excel file or a comma-separated values (CSV) file. If you have configured a row filter, only the currently visible rows are exported.

## 3.3 Prerequisites

Before using the Sophos Mobile Control console:

- You need a computer connected to the internet and equipped with a web browser. For information on supported browsers and the relevant versions, see the *Sophos Mobile Control release notes*.
- The super administrator must have created a customer (a tenant whose devices are managed in Sophos Mobile Control). 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 Sophos Mobile Control console. The credentials consist of customer, user and password. For further information, see [Login to the Sophos Mobile Control console](#) (page 11).

## 3.4 User roles

Users of Sophos Mobile Control have different roles. You assign these roles when you create new administrators. See [Create administrators](#) (page 207).

The available modules and functions in the Sophos Mobile Control console depend on the role.

You can assign the following roles:

Role	Description
Administrator	This role has the rights to perform all available actions.
Limited Administrator	This role is allowed to perform all actions required for enrolling and managing a device, but cannot specify essential settings and cannot manage other administrators.
Reporting	This role can view the list of devices and is able to create reports. For example, an auditor or an employee who needs to document the settings in Sophos Mobile Control.
Content admin	This role is intended for employees responsible for uploading, updating or removing documents distributed via the <b>Documents</b> feature. Usually this role is assigned to a person outside the IT department. The permissions are set to limit visibility and access only the content in the <b>Documents</b> menu.
Helpdesk	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, such as defining settings and creating, deleting or editing devices/device groups, packages and profiles.
App Group Administrator	This role can manage app groups. A typical user is an administrator that accesses the Sophos Mobile Control web service interface to create, update or read app groups.

If you require further roles, please contact the Sophos support team.

## 3.5 Login to the Sophos Mobile Control console

1. Open the web address of the Sophos Mobile Control console in your web browser.
2. In the login dialog, enter your customer name and your user credentials (name and password), then click **Login**.

The customer's **Dashboard** is displayed.

**Note:** When you log in to the Sophos Mobile Control console for the first time, you are prompted to change your password.

**Note:** The administrator can display messages in the login dialog, for example regarding upcoming upgrades or outage times. Click the message to display its entire content.

## 3.6 Log out from the Sophos Mobile Control console

To log out from the Sophos Mobile Control console, click **Logout** in the page header.

## 3.7 Change your password

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

1. On the menu sidebar, under **SETTINGS**, click **Setup > General**, and then click the **Change password** tab.
2. Enter your old password, a new one and confirm it.
3. Click **Save**.

## 3.8 Password recovery

If you have forgotten your password for the Sophos Mobile Control console, you can reset it.

1. In the **Login** dialog box of the Sophos Mobile Control console, click **Forgot password?**

The **Reset password** dialog box is displayed.

2. Enter your **Customer** and **User** information and click **Reset password**.

You receive an email with a link for resetting your password.

3. Click the link.

The **Change password** dialog box is displayed.

4. Enter a new password, confirm it and click **Change password**.

Your password has been changed and you are logged in to the Sophos Mobile Control console.

## 4 Key steps for managing devices with Sophos Mobile Control

Sophos Mobile Control offers a wide range of Mobile Device Management functions depending on device types, corporate security policies and specific requirements in your company.

The key steps for managing devices with Sophos Mobile Control are:

- Configure compliance rules for devices. See [Compliance rules](#) (page 41).
- Create device groups. See [Create device group](#) (page 71).

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.

- Enroll and provision devices. See [Add devices](#) (page 49) and [Enroll devices](#) (page 51).

Devices can either be enrolled and provisioned by administrators through the Sophos Mobile Control console or by device users through the Self Service Portal.

- Set up profiles and security settings for devices. See [Profiles and policies](#) (page 72).
- Create task bundles. See [Task bundles](#) (page 172).
- Configure the available features of the Self Service Portal. See [Configure Self Service Portal](#) (page 24).
- Apply new or updated profiles and security settings to enrolled devices.

## 5 Dashboard

**Note:** This section applies to the **Dashboard** of regular administrators. For the super administrator, the **Dashboard** is used to manage customers. See the [Sophos Mobile Control super administrator guide](#).

The customizable **Dashboard** is the regular start page of Sophos Mobile Control and provides access to the most important information at a quick glance. It consists of several widgets providing information about:

- Devices, all or per group
- Compliance status by platform or for all devices
- Managed status by platform or for all devices
- The SSP registration status
- The platform versions in use

There also is a special widget **Add device** to start the device enrollment wizard. See [Use the device enrollment wizard to assign and enroll new devices](#) (page 52).

The following options are available to customize the **Dashboard**:


- To add a widget to the page, click **Add widget**.
- To remove a widget from the page, click the **Close** button in its header.
- To reset the page to its default layout, click **Restore default layout**.
- To rearrange the widgets on the page, drag a widget header.

## 6 Reports

With Sophos Mobile Control you can create various reports from the following areas:

- Devices
- Apps and documents
- Compliance violations
- Malware

To create a report:

1. On the menu sidebar, under **INFORM**, click **Reports**, and then click the name of the required report.
2. In the **Choose format** dialog, click one of the available icons to select the output format:
  - Click  to export the report to a Microsoft Excel file.
  - Click  to export the report to a comma-separated values (CSV) file.

The report file is saved to your local computer, using the download settings of your web browser.

# 7 Tasks

The **Task view** page gives you an overview of all tasks you created and started and displays their current state.

You can monitor all your tasks and intervene in case of problems. For example, you can delete a task that obviously cannot be completed but blocks the device.

To delete a task, click the **Delete** icon next to it.

You can filter tasks according to **Type** and **State** and sort them by device name, package name, creator and scheduled date.

## 7.1 Monitor tasks

In the Sophos Mobile Control console, you can monitor all existing tasks for devices.

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

### 7.1.1 View unfinished, failed and latest finished tasks

1. On the menu sidebar, under **INFORM**, click **Tasks**.
2. On the **Task view** page, the **State** column shows the task status, for example, **Completely failed**.
3. In the **Refresh interval (in sec.)** field, you can select how often the **Task view** page is to be refreshed.
4. To view further details about a task, click the **Show** magnifier icon next to the required task.

The **Task details** page is displayed. Besides general information on the task (for example, device name, package name and creator) 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 on the **Task details** page.

5. If available, click **Details** to view the commands to be executed by the device.

The commands sent to the device are part of the task. They are executed by the SMC app or by the MDM 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.

6. To return to the **Task details** page, click **Back**.



## 7.1.2 View task archive

1. On the menu sidebar, under **INFORM**, click **Tasks**.
2. On the **Task view** page, click **Task archive**.

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











3. On this page, you can:
  - Click **Reload** to refresh the **Task archive** page.
  - Delete a task from the archive by clicking the **Delete** icon next to the relevant task.
  - Select several tasks and click **Delete selected** to delete them from the archive.

To go back to the **Task view** page, click **Tasks** on the menu sidebar.

## 7.1.3 Task states

The following table provides an overview of the task states shown on the **Task view** and on the **Task archive** pages.

Every state is associated with a color code that indicates the state category.

Color code	State	Description
	Accepted	Task has been created.
	Will be retried	Task will be retried later.
	Started	Task has been started.
	In progress	Execution of the task is being prepared.
	Task bundle in progress	Execution of the task bundle is being prepared.
	Notified	SMC app was notified.
	Commands sent	SMC app has received the package and/or the commands.
	Result evaluation started	SMC app has answered and the evaluation of the result has been started.
	Result incomplete	Result evaluation showed that not all commands' results have been received by now.
	Waiting for user interaction	There is a pending user action on the device.

Color code	State	Description
●	Device is locked	Task waits for the device to become unlocked (iOS only).
●	Successful	Package has been installed or the commands have been successfully executed. <b>Note:</b> For the initial provisioning of the Sophos Mobile Control app the task must finish with the state <i>Installed</i> .
●	Installed	The Sophos Mobile Control app has been installed successfully. The device is provisioned now.
●	Result evaluation failed	Result evaluation could not be executed.
●	Task partly failed	Not all commands of the task could be executed successfully.
●	Delayed	Task will be restarted later.
●	Failed (retry queued)	Task has failed and will be retried later.
●	Task failed	Task has failed and no further retries are queued.
●	Completely failed	Task has failed, and it is not possible to retry it.
●	Not started	Task is part of a task bundle and was not processed yet.
●	Session requested	An AirPlay session was requested (iOS only).
●	Unknown	The server has no information about the task status.

Color code	Category
●	Open
●	In progress
●	Success
●	Failure
●	Other

## 8 General settings

On the **General settings** page you can configure some basic settings of Sophos Mobile Control.

### 8.1 Configure personal settings

To use the Sophos Mobile Control console more efficiently, you can customize the user interface to show only the platforms you work with.

**Note:** By configuring the platforms you only change the view of the user who is currently logged in. You cannot deactivate any functions here.

1. On the menu sidebar, under **SETTINGS**, click **Setup > General**, and then click the **Personal** tab.
2. Configure the following settings:

Option	Description
<b>Language</b>	Select the language for the Sophos Mobile Control console.
<b>Timezone</b>	Select the timezone in which dates are shown.
<b>Unit system</b>	Select the unit system for length values ( <b>Metric</b> or <b>Imperial</b> ).
<b>Lines per page in tables</b>	Select the maximum number of table lines you want to display per page.
<b>Show extended device details</b>	Select this check box to show all available information about the device. The <b>Custom properties</b> and <b>Internal properties</b> tabs will be added to the <b>Show device</b> page.
<b>Activated platforms</b>	<p>Select the platforms you want to manage for the customer:</p> <ul style="list-style-type: none"> <li>▪ <b>Android</b></li> <li>▪ <b>iOS</b></li> <li>▪ <b>Windows Mobile</b> (includes Windows Phone 8.1 and Windows 10 Mobile operating systems)</li> <li>▪ <b>Windows Desktop</b></li> </ul> <p>Based on your platform selection, the user interface of the Sophos Mobile Control console is adjusted. Only views and features that are relevant for the selected platforms are shown.</p> <p><b>Note:</b> The list of available platforms depends on your platform settings from the super administrator configuration. For further information, see the <a href="#">Sophos Mobile Control super administrator guide</a>.</p>

3. Click **Save**.

## 8.2 Configure password policies

To enforce password security, configure password policies for users of the Sophos Mobile Control console and the Self Service Portal.

**Note:** The password policies do not apply to users from an external LDAP directory. For information on external user management, see the [Sophos Mobile Control super administrator guide](#).

1. On the menu sidebar, under **SETTINGS**, click **Setup > General**, and then click the **Password policies** tab.
2. Under **Rules**, you can define password requirements, like a minimum number of lower-case, upper-case or numerical characters that a password must contain to be valid.
3. Under **Settings**, configure the following settings:
  - a) **Password change interval (days):** Enter the number of days until a password expires (between 1 and 730), or leave the field empty to disable password expiration.
  - b) **Number of previous passwords which must not be reused:** Select a value between 1 and 10, or select --- to disable this restriction.
  - c) **Maximum number of failed login attempts:** Select the number of failed login attempts until the account gets locked (between 1 and 10), or select --- to allow an unlimited number of failed login attempts.
4. Click **Save**.

## 8.3 Configure SMC app settings

On the **SMC app** tab of the **General settings** page, you configure settings for the Sophos Mobile Control app on Android, iOS and Windows Mobile devices.

1. On the menu sidebar, under **SETTINGS**, click **Setup > General**, and then click the **SMC app** tab.
2. Configure the following settings:

Option	Description
<b>Disable unenrollment through app</b>	Remove the <b>Unenroll</b> button from the Sophos Mobile Control app to prevent users from unenrolling their device through the app.  <b>Note:</b> To completely prevent user-initiated unenrollment, also disable the <b>Unenroll device</b> option in the Self Service Portal settings. See <a href="#">Configure Self Service Portal settings</a> (page 25).

3. Click **Save**.

## 8.4 Enable Baidu Cloud Push service

Sophos Mobile Control uses the Google Cloud Messaging (GCM) service to send push notifications to Android devices, to trigger them to contact the Sophos Mobile Control server. In China, GCM will likely not work. Therefore, Sophos Mobile Control can also use Baidu Cloud Push, which is a Chinese push notification service.

If you manage Android devices that are located in China, enable the Baidu Cloud Push service as follows:

1. On the menu sidebar, under **SETTINGS**, click **Setup > General**, and then click the **Android** tab.
2. In the **Baidu Cloud Push service** section, select **Enable Baidu Cloud Push service**.
3. Click **Save**.

When Baidu Cloud Push is enabled, Sophos Mobile Control sends all push notifications through GCM and through Baidu Cloud Push.

## 8.5 Configure iOS settings

On the **iOS** tab of the **General settings** page, you configure settings that are specific to iOS devices.

1. On the menu sidebar, under **SETTINGS**, click **Setup > General**, and then click the **iOS** tab.
2. Configure the following settings:

Option	Description
<b>Activation Lock bypass</b>	<p>Select <b>Enable</b> to be able to clear the Activation Lock on supervised devices.</p> <p>When this option is selected, Sophos Mobile Control retrieves a bypass code when syncing with a supervised device that has Activation Lock enabled. If required, you can perform the <b>Activation Lock bypass</b> action from the device's <b>Show device</b> page to clear Activation Lock when the device needs to be erased and re-deployed.</p> <p>Activation Lock is an iOS security feature to prevent the reactivation of lost or stolen devices. Normally, you need the correct Apple ID and password to clear Activation Lock. With the Activation Lock bypass feature, you can clear Activation Lock by providing the bypass code only.</p>
<b>Synchronize device name</b>	<p>Select <b>Enable</b> to manage iOS devices under the name that is configured on the device.</p> <p>When this option is selected, the device name that Sophos Mobile Control uses is set every time the device synchronizes with Sophos Mobile Control.</p> <p>When this option is deselected, you set the device name during device enrollment.</p>

3. Click **Save**.

## 8.6 Configure polling interval for Windows devices

For Windows devices, you can configure the polling interval at which the Windows MDM client contacts the Sophos Mobile Control server. Usually, the server contacts the client using push notifications. Polling is used as a safety measure when the push notification service is not available.

**Note:** The default values are sufficient in most cases. Using shorter intervals impacts battery life and data consumption and causes higher server load.

1. On the menu sidebar, under **SETTINGS**, click **Setup > General**, and then click the **Windows** tab.
2. Select polling intervals for the different Windows operating systems. You can configure individual settings for:
  - Windows 10 Mobile and Windows Phone 8.1 devices
  - Windows 10 Desktop devices
3. Click **Save**.

## 8.7 Configure Email

On the **Email configuration** tab, you can configure settings for emails that are sent by Sophos Mobile Control to the users.

1. On the menu sidebar, under **SETTINGS**, click **Setup > General**, and then click the **Email configuration** tab.
2. In the **Language** list, select the email language.
3. In the **Originator name** field, enter the name that will appear as email originator.
4. Click **Save**.

## 8.8 Configure technical support contact details

To support users who have questions or problems, you can provide them with details of how to contact technical support. The information that you enter here is displayed in the Sophos Mobile Control app and on the Self Service Portal.

1. On the menu sidebar, under **SETTINGS**, click **Setup > General**, and then click the **Technical contact** tab.
2. Enter the required information for the technical contact.
3. Click **Save**.

## 8.9 Define customer properties

You can define customer-level properties.

When you define a property with name `my property`, you can refer to the value of the property in profiles and policies by using the placeholder `$_CUSTPROP(my property)_%`. For example, you can use this to refer to a domain that is specific to the customer.

For details on profile and policy placeholders, see [Placeholders in profiles and policies](#) (page 75).

To define a customer property:

1. On the menu sidebar, under **SETTINGS**, click **Setup > General**, and then click the **Customer properties** tab.
2. Click **Add customer property**.
3. Enter a **Name** and a **Value** for the new property.
4. Click **Apply** to add the property.
5. Click **Save** to save the changes to the customer settings.

## 9 Configure Self Service Portal

With the Self Service Portal you can reduce IT efforts by allowing users to enroll devices on their own and carry out other tasks without having to contact the helpdesk.

On the menu sidebar, you can configure settings for the use of the Self Service Portal, for example:

- The platforms for which devices can be enrolled.
- The available functions.
- The users that are allowed to access the Self Service Portal.

The Self Service Portal is available for the following platforms:

- Android
- Apple iOS
- Windows Mobile
- Windows Desktop

### 9.1 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](#) (page 29).

**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](#) (page 29).

To create a Self Service Portal group:

1. On the menu sidebar, under **MANAGE**, click **Users**.  
The **Show users** page is displayed.
2. Click **Show user groups**.  
The **Show user groups** page is displayed.
3. Click **Create group**.  
The **Edit group** page is displayed.
4. In the **Name** field, enter a name for the new Self Service Portal user group.
5. Click **Save**.



The new Self Service Portal user group is displayed on the **Show user groups** page. 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.

## 9.2 Configure Self Service Portal settings

1. On the menu sidebar, under **SETTINGS**, click **Setup**, and then click **Self Service Portal**.  
The **Self Service Portal** page is displayed.
2. On the **Configuration** tab, configure the following settings:
  - a) In the **Maximum number of devices** list, select the maximum number of devices a user can enroll through the Self Service Portal. This ensures that the number of available licenses is not exceeded.
  - b) In the **Device owner preselection** list, select if new devices are classified as corporate or personal devices, and if the users are able to change this classification when they enroll their devices through the Self Service Portal. You can select one of the following settings:
    - **no preselection:** The owner field in the Self Service Portal is left blank. Users can select the device type.
    - **corporate preselected:** On the Self Service Portal, **Corporate device** is preselected. Users can change the setting to **Personal device**.
    - **corporate fixed:** Device type cannot be selected. **Company** is listed as owner.
    - **personal preselected:** On the Self Service Portal, **Personal device** is preselected. Users can change the setting to **Corporate device**.
    - **personal fixed:** Device type cannot be selected. **Employee** is listed as owner.
  - c) Under **Available functionality**, select the functions that should be available for users of the Self Service Portal. The functions supported vary according to the device platform. See [Available Self Service Portal settings](#) (page 26).
3. On the **Terms of use** tab, you configure a mobile policy, disclaimer or agreement text that is displayed as a first step when users enroll their devices. Users must accept the text to be able to continue.  
HTML formatting tags are supported for the text. The text will be displayed in the relevant browser accordingly.
4. On the **Post-install text** tab, you configure text to be displayed on the Self Service Portal after automatic installation. This text can tell the user what must be done next, for example configuring the server in the iOS app or configuring the Android mail client.  
HTML formatting tags are supported for the text. The text will be displayed in your chosen browser accordingly.
5. On the **Group settings** tab, you configure the group settings, for example, the device groups enrolled devices will be added to and the task bundle that will be transferred to the devices.

**Important:** Because of the complexity of the group settings configuration, we recommend that you test device enrollment for different user groups before you roll out the settings to your actual users.

- a) Click **Add**.

The **Edit group settings** page 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 character in this field to specify several groups. For example: Enter **Dev\*** to specify all group names that start with the string **Dev**. Enter **\*** to specify all available groups.
- d) Select if the texts that are configured in the **Terms of use** and **Post-install text** tabs will be displayed.
- e) In columns **Initial package - corporate device** and **Initial package - personal device**, select the task bundle (for Android and iOS) or policy (for Windows Mobile and Windows Desktop) to be executed on corporate and personal devices.
- f) In column **Active**, select the platforms that should be available on the Self Service Portal. You must select an initial package before you can select a platform.
- g) In column **Add to device group**, select the group the device should be added to.

**Note:** On the menu sidebar, 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 [Device groups](#) (page 71).





- h) Click **Apply**.

6. The **Self Service Portal** page is displayed. Click **Save**.

**Note:** As a super administrator, you can also define the default customer for the login of users at the Self Service Portal. For further information, see 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.

### 9.3 Available Self Service Portal settings

The following table shows the functions of the Self Service Portal that you can enable or disable as described in [Configure Self Service Portal settings](#) (page 25), and the device platforms for which a function is supported.

Setting	Description	Android	iOS	Windows Mobile	Windows Desktop
<b>Locate device</b>	With this function users can locate devices if they are lost or stolen.				

Setting	Description	Android	iOS	Windows Mobile	Windows Desktop
<b>Lock device</b>	With this function users can lock their devices if they are lost or stolen.				
<b>Reconfigure device</b>	With this function users can reconfigure their devices if Sophos Mobile Control has been removed from the device, but the device is still enrolled.				
<b>Show compliance violations</b>	With this function users can view the compliance violations for their devices.				
<b>Refresh data</b>	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 long 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 rules configured) and needs to be synchronized with the server to make it compliant again.				
<b>Reset password</b>	With this function users can reset their unlock screen password. For Android and iOS devices, a temporary password is displayed on the Self Service portal. The device can only be unlocked with this password. After unlocking their devices, users can set a new password. For iOS, the password is completely deleted. The user has to set a new password within 60 minutes.				

Setting	Description	Android	iOS	Windows Mobile	Windows Desktop
<b>Wipe</b>	<p>With this function users can reset their enrolled devices to their factory settings if devices are lost or stolen. All data on the device is deleted.</p> <p>For devices that are enrolled with Android for Work, only the work profile is removed. The device itself is not reset.</p>				
<b>Unenroll device</b>	<p>With this function users can decommission devices that they no longer use. This is useful, for example, if the number of devices users can enroll through the Self Service Portal is limited or users get new devices.</p>				
<b>Delete unmanaged device</b>	<p>With this function users can delete decommissioned devices.</p>				
<b>Reset App Protection password</b>	<p>With this function users can reset their App Protection password on Android devices. The App Protection password protects defined apps and has to be entered each time users start these apps. The password will be deleted and they have to set a new one.</p>				
<b>Reset Sophos container password</b>	<p>With this function users can reset their Sophos container password. The Sophos container password has to be entered each time users start one of the container apps. The password will be deleted and they have to set a new one.</p>				
<b>Reconfigure the SMC app</b>	<p>With this function users can reconfigure an already installed Sophos Mobile Control app.</p>				

## 9.4 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 to Sophos Mobile Control or by importing them from a comma-separated values (CSV) file.
- **External user management:** With external user management you can assign devices to groups and profiles based on external directory membership.

The user management method is customer-specific. For on-premise installations of Sophos Mobile Control, it is defined by the super administrator when a customer is created. For Sophos Mobile Control as a Service, you must define it before adding users. See [Configure Self Service Portal user management](#) (page 29).

### 9.4.1 Configure Self Service Portal user management

**Note:** For on-premise installations of Sophos Mobile Control, user management for the Self Service Portal is configured by the super administrator when a customer is created. See the *Sophos Mobile Control super administrator guide*.

1. On the menu sidebar, under **SETTINGS**, click **Setup**, and then click **System setup**.

The **System setup** page 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, user-specific profiles, or LDAP administrators available.**
- Select **Internal directory** to use internal user management for users of the Sophos Mobile Control Self Service Portal.
- Select **External LDAP directory** to use external user management for users of the Sophos Mobile Control Self Service Portal.

Click **Configure external LDAP** to specify the server details. See [Configure external directory connection](#) (page 30).

3. Click **Save**.

If you have selected **Internal directory** or **External LDAP directory**, the selected option and the option **None. No SSP, user-specific profiles, or LDAP administrators available.** are displayed on the **User setup** tab. If you want to change your selection afterward, select **None. No SSP, user-specific profiles, or LDAP administrators 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.

### 9.4.1.1 Configure external directory connection

When you use an external LDAP directory for managing user accounts for the Sophos Mobile Control console and the Self Service Portal, you must configure the directory connection so that Sophos Mobile Control can retrieve the user data from the LDAP server. For on-premise installations of Sophos Mobile Control, this is done by the super administrator when the customer is created.

**Note:** There is no synchronization between the LDAP directory and Sophos Mobile Control. Sophos Mobile Control only accesses the LDAP directory to look up user information. Changes to an LDAP user account are not implemented on the Sophos Mobile Control database, and vice versa.

1. On the menu sidebar, under **SETTINGS**, click **Setup > System setup**, and then click the **User setup** tab.
  2. Select **External LDAP directory**.
  3. Click **Configure external LDAP** to specify the server details.
  4. On the **Server details** page, configure the following settings:
    - a) Select the **LDAP type**. Sophos Mobile Control supports:
      - **Active Directory**
      - **IBM Domino**
      - **NetIQ eDirectory**
      - **Red Hat Directory Server**
      - **Zimbra**
    - b) In the **Primary URL** field, enter the URL of the primary directory server. You can enter the server IP or the server name. Select **SSL** to use SSL for the server connection. For Sophos Mobile Control as a Service, **SSL** cannot be deselected.
    - c) Optional: In the **Secondary URL** field, enter the URL of a directory server that is used as fallback in case the primary server cannot be reached. You can enter the server IP or the server name. Select **SSL** to use SSL for the server connection. For Sophos Mobile Control as a Service, **SSL** cannot be deselected.
    - d) In the **User** field, enter an account for lookup operations on the directory server. Sophos Mobile Control uses the account credentials when it connects to the directory server.  
For Active Directory, you also need to enter the relevant domain. Supported formats are:
      - `<domain>\<user name>`
      - `<user name>@<domain>.<domain code>`

**Note:** For security reasons, we recommend you specify a user that only has read permissions for the directory server and not write permissions.
    - e) In the **Password** field, enter the password for the user.
- Click **Next**.

5. On the **Search base** page, enter the Distinguished Name (DN) of the search base object. The search base object defines the location in the external directory from which the search for a user or user group begins.

6. On the **Search fields** page, define which directory fields are to be used for resolving the `%_USERNAME_` and `%_EMAILADDRESS_` placeholders in profiles and policies. Type the required field names or select them from the **User name** and **Email** lists.

**Note:** The lists only contain fields that are configured for the user that is currently connected to the LDAP directory, specified in step 4.d earlier in this description. If, for example, an email field was not configured for that user, you need to manually enter the required value in the **Email** field.

In the case of Active Directory, these field mappings apply:

- **User name:** `sAMAccountName`
- **First name:** `givenName`
- **Last name:** `sn`
- **Email:** `mail`

7. On the **SSP configuration** page, specify the users that are allowed to log in to the Self Service Portal. Enter the relevant information in the **SSP group** field, using one of the following options:

- If you enter an asterisk `*`, all authenticated directory users are allowed to log in to the Self Service Portal.
- If you enter the name of a group that is defined on the directory server, all members of that group are allowed to log in to the Self Service Portal. After you have entered the group name, click **Resolve group** to resolve the group name into a Distinguished Name (DN).
- If you leave the field empty, no users from the directory server are allowed to log in to the Self Service Portal. Use this option if you want to enable external user management for the Sophos Mobile Control console but not for the Self Service Portal.

**Note:**

The group you specify here is not related to the directory group you define on the **Group settings** tab of the **Self Service Portal** page. With those settings, you define task bundles, Sophos Mobile Control group membership and available device platforms for each directory group.

8. Click **Apply**.

9. On the **User setup** tab, click **Save**.

## 9.4.2 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](#) (page 29).

1. On the menu sidebar, under **MANAGE**, click **Users**.

The **Show users** page is displayed.

2. Click **Create user**.

The **Edit user** page is displayed.

3. Select the **Send welcome email** check box.

4. Enter the following information:

- a) **User name**
- b) **First name**
- c) **Last name**
- d) **Email address**
- e) **Groups** (optional)

Click **Show**, to display all available user groups and select one.

5. Click **Save**.

The new Self Service Portal user is displayed on the **Show users** page. A welcome email is sent to the new user.

If you click the blue triangle next to the required user, you can view the user details (**Show**), **Edit** or **Delete** the user.

**Note:** If you click a user name, the **Show user** page is displayed. This page contains the **Resend welcome email** button, which you can use to send the email again if the user did not receive or lost the initial email.

### 9.4.3 Import 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 of Sophos Mobile Control, see the [Sophos Mobile Control super administrator guide](#).
- For Sophos Mobile Control as a Service, see [Configure Self Service Portal user management](#) (page 29).

With internal user management, you can add new Self Service Portal users by importing a UTF-8 encoded comma-separated values (CSV) file with up to 500 users.

**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 extension `.csv`.

**Tip:** A sample file with the correct column names and column order is available for download from the **Import users** page.

To import users from a CSV file:

1. On the menu sidebar, under **MANAGE**, click **Users**, and then click **Import users**.



2. On the **Import users** page, select **Send welcome emails**.
3. Click **Upload a file** and then navigate to the CSV file that you have prepared.

The entries are read in from the file and are displayed.

4. If the data is not formatted correctly or is inconsistent, the file as a whole cannot be imported. In this case, follow the error messages that are displayed next to the relevant entries, correct the content of the CSV file accordingly and upload it again.
5. Click **Finish** to create the user accounts.

The users are imported and displayed on the **Show users** page. They will receive emails with their login credentials for the Self Service Portal.

# 10 System setup

## 10.1 Check your licenses

Sophos Mobile Control uses a user-based license scheme. One user license is valid for all devices assigned to that user. Devices that are not assigned to a user require one license each.

To check your available licenses:

1. On the menu sidebar, under **SETTINGS**, click **Setup > System setup**.
2. On the **System setup** page, click the **License** tab.

The following information is displayed:

- **Maximum number of licenses:** Maximum number of device users (and unassigned devices) that can be managed.  
  
If the super administrator did not set a quota for the customer, the number of licenses is limited by the overall number for the Sophos Mobile Control server.
- **Used licenses:** Number of licenses in use.
- **Valid until:** The license expiry date.

If you have any questions or concerns regarding the displayed license information, contact your Sophos sales representative.

**Note:** To notify when the license is about to expire, Sophos Mobile Control sends several email reminders to all administrators, starting 30 days prior to the expiry date.

## 10.2 Apple Push Notification service certificates

To use the built-in Mobile Device Management (MDM) protocol of iOS devices, Sophos Mobile Control must use the Apple Push Notification service (APNs) to trigger the devices.

APNs certificates have a validity period of one year. To notify when the certificate is about to expire, Sophos Mobile Control sends several email reminders to the administrators, starting 30 days prior to the expiry date.

The following sections describe the requirements that must be fulfilled and the steps you must take to get access to the APNs servers with your own client certificate.

### 10.2.1 Requirements

For communication with the Apple Push Notification Service (APNs), TCP traffic to and from the following ports must be allowed:

- The Sophos Mobile Control server needs to connect to `gateway.push.apple.com:2195`  
TCP (17.0.0.0/8)

- Each iOS device with Wi-Fi only access needs to connect to `*.push.apple.com:5223`  
TCP (17.0.0.0/8)

## 10.2.2 Create an APNs certificate

This procedure assumes that you have not uploaded a certificate for the Apple Push Notification service (APNs) to Sophos Mobile Control yet.

To renew an existing certificate, see [Renew an APNs certificate](#) (page 35).

**Tip:** You can use the same certificate for several customers. See [Copy an APNs certificate to another customer](#) (page 37).

1. On the menu sidebar, under **SETTINGS**, click **Setup > System setup** and then click the **iOS APNs** tab.

The description on that tab guides you through the steps you have to perform to request a certificate from Apple and to upload it to Sophos Mobile Control.

2. In the **Download certificate signing request** step, click **Download certificate signing request**.

This saves the certificate signing request file `apple.csr` to your local computer. The signing request file is specific to the current customer.

3. You need an Apple ID. Even if you already have an ID, we recommend that you create a new one for use with Sophos Mobile Control. In the **Create Apple ID** step, click **Create a new Apple ID**.

This opens an Apple web page where you can create an Apple ID for your company.

**Note:** Store the credentials in a safe place where your colleagues can access them. Your company will need these credentials to renew the certificate each year.

4. For your reference, enter your new Apple ID in the **Apple ID** field on the top of the **iOS APNs** tab.

When you renew the certificate each year, you must always use that same Apple ID.

5. In the **Create or renew APNs certificate** step, click **Apple Push Certificates Portal**.

This opens the Apple Push Certificates Portal.

6. Log in with your Apple ID and upload the certificate signing request file `apple.csr`.

7. Download the `.pem` APNs certificate file and save it to your computer.

8. In the **Upload APNs certificate** step, click **Upload certificate** and then browse for the `.pem` file that you received from the Apple Push Certificates Portal.

9. Click **Save** to add the APNs certificate to Sophos Mobile Control.

Sophos Mobile Controls reads the certificate and displays the certificate details on the **iOS APNs** tab.

## 10.2.3 Renew an APNs certificate

This procedure assumes that you already have uploaded a certificate for the Apple Push Notification service (APNs) to Sophos Mobile Control that is about to be expire and needs to be renewed.

To create and upload a new certificate, see [Create an APNs certificate](#) (page 35).

**Important:** On the Apple portal, it is important that you select the correct APNs certificate for renewal. If you renew the wrong certificate, you might need to re-enroll all iOS devices.

1. On the menu sidebar, under **SETTINGS**, click **Setup > System setup** and then click the **iOS APNs** tab.
2. In the **Download certificate signing request** step, click **Download certificate signing request**.  
This saves the certificate signing request file `apple.csr` to your local computer.
3. Skip the step **Create Apple ID**. This step is only required if you are creating an APNs certificate for Sophos Mobile Control for the first time.
4. In the **Create or renew APNs certificate** step, click **Apple Push Certificates Portal**.  
This opens the Apple Push Certificates Portal.
5. Log in with your Apple ID. This must be the same ID that you used for the creation of the initial APNs certificate.
6. On the Apple Push Certificates Portal, click **Renew** next to your Sophos Mobile Control APNs certificate.
7. Upload the certificate signing request file `apple.csr` you prepared before.
8. Download the `.pem` APNs certificate file and save it to your computer.
9. In the **Upload APNs certificate** step, click **Upload certificate** and then browse for the `.pem` file that you received from the Apple Push Certificates Portal.
10. Click **Save**.
11. When you are logged in as super administrator, there is an additional dialog that lists all customers that currently use the same APNs certificate as the super administrator customer, that is a certificate with the same **Topic** attribute.
  - Click **Save for all customers concerned** to renew the APNs certificate for all of these customers.
  - Click **Save only for super administrator customer** to renew the APNs certificate only for the super administrator customer.

**Important:**

If the following message is shown, you are not renewing the correct certificate:

```
"The topic of the new certificate does not correspond to the old one.
If devices have been
    set up with the previous certificate, they have to be set up
again. Do you really want to save
    your changes?"
```

This message indicates that you are about to create a new APNs certificate with a different identifier. If you confirm the message, all existing iOS devices are not manageable any more and you have to re-enroll them.

For information how to select the correct certificate, see [Identify the correct APNs certificate for renewal](#) (page 37).

## 10.2.4 Copy an APNs certificate to another customer

You can copy a certificate for the Apple Push Notification service (APNs) to another customer within the same or a different installation of Sophos Mobile Control.

**Important:** If there already exists an APNs certificate at the target location, it is important that the *Topic* property of the certificate that you want to copy is identical to the *Topic* of the existing certificate. If you copy the wrong certificate, you might need to re-enroll all iOS devices of the customer.

Download the certificate from the source location:

1. Log in to the Sophos Mobile Control console as an administrator of the customer whose APNs certificate you want to copy.
2. On the menu sidebar, under **SETTINGS**, click **Setup > System setup** and then click the **iOS APNs** tab.
3. Make a note of the **Topic** value that is displayed in the certificate details.
4. Click **Download certificate as PKCS #12 file**.
5. In the confirmation dialog, the password for the certificate file is displayed. Make a note of that password and then click **Download**.

This saves the certificate file `apns_cert.p12` to your local computer.

Upload the certificate to the target location:

6. Log in to the Sophos Mobile Control console as an administrator of the customer to whom you want to upload the certificate.
7. On the menu sidebar, under **SETTINGS**, click **Setup > System setup** and then click the **iOS APNs** tab.
8. If there already exists an APNs certificate, verify that the **Topic** value is identical to the value of the certificate you are about to copy.
9. In the **Upload APNs certificate** step, click **Upload certificate** and then browse for the `apns_cert.p12` file that you downloaded before.
10. Enter the password and then click **Apply**.
11. Click **Save**.

## 10.2.5 Identify the correct APNs certificate for renewal

When you renew your Apple Push Notification service (APNs) certificate for the Sophos Mobile Control server as described in [Renew an APNs certificate](#) (page 35), it is important that on the Apple portal you select the correct APNs certificate for renewal.


This section describes how to identify the APNs certificate that is currently uploaded to the Sophos Mobile Control server.

Retrieve the certificate identifier:

1. Log in to the Sophos Mobile Control console with an administrator account for the customer whose APNs certificate needs to be renewed.
2. On the menu sidebar, under **SETTINGS**, click **Setup > System setup** and then click the **iOS APNs** tab.

3. In section **Content of the Apple Push Notification keystore**, the properties of the uploaded APNs certificate are displayed.
4. Make a note of the value that is displayed for **Topic**.  
This is the identifier of your APNs certificate.

Identify the certificate:

5. Use your web browser to open the URL of the Apple Push Certificates Portal, <https://identity.apple.com/pushcert/>.  
If you are experiencing issues with certain features of the Apple portal when using Microsoft Internet Explorer, we recommend that you use the latest version of the Firefox, Opera, Chrome or Safari browser instead.
6. Log in with the Apple ID that you used for the creation of the initial APNs certificate.
7. In the list of APNs certificates, click the **Certificate Info** icon  next to a certificate entry.  
This displays the certificate details.
8. In field **Subject DN**, locate the value that follows the string `UID=`. If this matches the identifier that you determined in the Sophos Mobile Control console, you have identified the correct certificate.

## 10.2.6 Check APNs connectivity of devices

Users of the Sophos Mobile Control app for iOS can check if their devices are able to connect to the Apple Push Notification service (APNs) server.

1. In the Sophos Mobile Control app, tap the **Information** icon to open the **About** screen.
2. Tap **Check APNs**.

The app tries to connect to the Apple APNs server. The expected server response time is 5 seconds or less.

If the app notifies you that the APNs server could be reached, the device is able to receive commands from Sophos Mobile Control server through APNs.

If the app notifies you that the APNs server could not be reached, your network does not allow APNs communication and thus Sophos Mobile Control is not able to manage iOS devices. To correct this, make sure that the requirements described in [Requirements](#) (page 34) are met.

## 10.3 Configure iOS AirPlay destinations

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.

1. On the menu sidebar, under **SETTINGS**, click **Setup** and then **System setup**, and go to the **iOS AirPlay** tab.
2. In the **AirPlay destinations** section, click **Create AirPlay destination**.

The **AirPlay destination** page is displayed.

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

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

5. Click **Save**.

You can trigger AirPlay mirroring between an iOS device and this destination by clicking **Request AirPlay mirroring** from the **Actions** menu on the **Show device** page for the relevant device.

## 10.4 Samsung Knox license

If your company has purchased a Samsung Knox Premium license, you have to enter your license key, the number of licenses and the expiry date on the **Samsung Knox license** tab in order to manage the Knox container on your Samsung Knox devices with Sophos Mobile Control.

## 10.5 Configure SCEP

You can configure Simple Certificate Enrollment Protocol (SCEP) to provide certificates. This allows devices to obtain certificates from a Certificate Authority by using SCEP.

You can configure all the settings required to access a Certificate Authority server with SCEP in the Sophos Mobile Control console.

You can define the settings required for devices in an SCEP **Device profile** for Android and iOS or a policy for Windows Mobile.

### 10.5.1 Prerequisites

In order to use the Simple Certificate Enrollment Protocol, the following prerequisites must be fulfilled:

- An SCEP-enabled Windows CA exists in the environment.
- Login credentials for a user who can create a challenge code are available.
- The Sophos Mobile Control server has http or https access to the following sites:
  - `https://YOUR-SCEP-SERVER/CertSrv/MSCEP_ADMIN`
  - `https://YOUR-SCEP-SERVER/CertSrv/MSCEP`

### 10.5.2 Configure SCEP

1. On the menu sidebar, under **SETTINGS**, click **Setup** and then **System setup**, and go to the **SCEP** tab.

2. Specify the following:

a) In the **SCEP server URL** field, enter `https://YOUR-SCEP-SERVER/CertSrv/MSCEP`.

b) In the **Challenge URL** field, enter `https://YOUR-SCEP-SERVER/CertSrv/MSCEP_ADMIN`.

**Note:** If you use a Windows 2003 server as the SCEP server, enter `https://YOUR-SCEP-SERVER/CertSrv/MSCEP`.

c) In the **User** and **Password** fields, enter the user credentials of the user who can create a challenge code.

**Note:** In the **User** field, enter a user who has the necessary rights to enroll certificates. Use the logon format: `username@domain`

d) In the **Challenge characters** field, select the character types that are used for the challenge password.

e) In the **Challenge length** field, accept the default length.

f) Optional: Clear the **Use HTTP proxy** option if you want Sophos Mobile Control to bypass the HTTP proxy when connecting to the SCEP server. This option is only available if the HTTP proxy is enabled.

For on-premise installation, the super administrator can configure an HTTP proxy that Sophos Mobile Control uses for outbound HTTP and SSL connections. See the [Sophos Mobile Control super administrator guide](#).

For Sophos Mobile Control as a Service, the HTTP proxy is always enabled.

3. Click **Save**.

Sophos Mobile Control tests the connection to your SCEP server.

To deploy a profile using SCEP, you must add a **SCEP** configuration to an Android or iOS device profile or to a Windows Mobile policy.

## 10.6 Configure user setup

On the **User setup** tab you can change the user management settings. For further information, see [Manage Self Service Portal users](#) (page 29) and the Sophos Mobile Control super administrator guide.



# 11 Compliance rules

With compliance rules you can:

- Allow, forbid or enforce certain features of a device.
- Define actions that are executed when a compliance rule is violated.

You can create various sets of compliance rules and assign them to device groups. This allows you to apply different levels of security to your managed devices.

**Tip:** If you are planning to manage both corporate and private devices, we recommend that you define separate sets of compliance rules for at least these two device types.

**Note:** There are two predefined compliance rules available. These are based on the HIPAA and the PCI DSS security standards.

## 11.1 Create compliance rules

To create compliance rules:

1. On the menu sidebar, under **CONFIGURE**, click **Compliance rules**.
2. On the **Compliance rules** page, click **Create compliance rules**.
3. Enter a **Name** and an optional **Description** for the new set of compliance rules.

The **Compliance rules** page contains individual tabs for the device platforms that are activated for the customer. Repeat the following steps for all required platforms.

4. Make sure that the **Enable platform** check box on each tab is selected.  
If this check box is not selected, devices of that platform are not checked for compliance.
5. Under **Rule**, configure the compliance rules for the particular platform.

Each compliance rule has a fixed severity level (high, medium, low) that is depicted by a blue icon. The severity helps you to assess the importance of each rule and the actions you should implement when it is violated.

If you have defined app groups, you can assign these to the compliance rules **Allowed apps**, **Forbidden apps** and **Mandatory apps**.

6. Under **If rule is violated**, define the actions that will be taken when a rule is violated:

Option	Description
<b>Deny email</b>	<p>Forbid email access.</p> <p>This action can only be taken if the super administrator has configured a connection to the internal or to the standalone EAS Proxy. See the <a href="#">Sophos Mobile Control super administrator guide</a>.</p>
<b>Lock container</b>	<p>Disable the Sophos Secure Workspace and Secure Email apps. This affects document, email and web access that is managed by these apps.</p> <p>This action can only be taken when you have activated an SMC Advanced license.</p> <p>This option is only relevant for Android and iOS devices.</p>
<b>Deny network</b>	<p>Forbid network access.</p> <p>This action can only be taken if the super administrator has configured Network Access Control. See the <a href="#">Sophos Mobile Control super administrator guide</a>.</p>
<b>Notify admin</b>	<p>Send compliance emails to selected recipients.</p> <p>The list of recipients and the time schedule is specified collectively for all sets of compliance rules that you create. See the instructions later in this section.</p>
<b>Transfer task bundle</b>	<p>Transfer a specific task bundle to the device.</p> <p>Select a task bundle from the list, or select <b>None</b> to transfer no task bundle when the compliance rule is violated.</p> <p><b>Important:</b> When used incorrectly, task bundles may misconfigure or even wipe devices. To assign the correct task bundles to compliance rules, an in-depth knowledge of the system is required.</p>

7. When you have made the settings for all required platforms, click **Save** to save the set of compliance rules under the name that you specified.

The new set is displayed on the **Compliance rules** page.

8. If you have selected the **Notify admin** action for one of the compliance rules, click **Compliance email settings** to specify the recipients that will receive compliance emails and the times when compliance emails are sent.

You can specify the recipients either by entering the name of an administrator or by entering a valid email address.

**Note:** These are common settings that apply to all compliance rules that have a **Notify admin** action.

9. Click **Save** to save the compliance email settings.

## 11.2 Available compliance rules

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



Setting	Description	Android	Android Things	iOS	Windows Mobile	Windows Desktop	Windows IoT
<b>Managed required</b>	Define the action that will be executed when a device is no longer managed.						
<b>Minimum SMC app version</b>	Enter the minimum Sophos Mobile Control app version that has to be installed onto the device.						
<b>Root rights allowed</b>	Select whether devices with root rights are allowed.  <b>Note:</b> For Sony devices with Enterprise API version 4 or above and for Samsung devices with Knox version 5.5 or below, this includes all devices that are classified <i>insecure</i> by the MDM API, for example because the bootloader is unlocked.						
<b>Apps from unknown sources allowed</b>	Select whether apps from unknown sources are allowed.						
<b>Android Debug Bridge (ADB) allowed</b>	Select whether ADB (Android Debug Bridge) is allowed.						
<b>Allow jailbreak</b>	Select whether jailbroken devices are allowed.						

Setting	Description	Android	Android Things	iOS	Windows Mobile	Windows Desktop	Windows IoT
<b>Password required</b>	Select whether a device password or other screen lock mechanism (like pattern or PIN) is required.  For Android, this includes the display lock types <i>Pattern</i> , <i>PIN</i> and <i>Password</i> , but not <i>Swipe</i> .						
<b>Min. OS version</b>	Select the earliest operating system version required.						
<b>Max. OS version</b>	Select the latest operating system version allowed.						
<b>Max. synchronization gap</b>	Specify the maximum interval between synchronization processes for devices.						
<b>Maximum SMC app synchronization interval</b>	Specify the maximum interval between iOS app synchronization processes for devices.						
<b>Max. SMSec scan interval</b>	This field is only displayed if Sophos Mobile Security is available for this customer. For further information, see <a href="#">Manage Sophos Mobile Security</a> (page 210). In this field, you can specify the maximum scan interval for malware scans performed by the Sophos Mobile Security app on the device.						
<b>Denial of SMSec permissions allowed</b>	Sophos Mobile Security needs permissions on the device to work properly. The user has						

Setting	Description	Android	Android Things	iOS	Windows Mobile	Windows Desktop	Windows IoT
	to grant these permissions when the app is installed. Select whether a denial of the required permissions results in a compliance violation.						
<b>Malware apps allowed</b>	This field is only displayed if Sophos Mobile Security is available for this customer. Select whether detected malware apps are allowed.						
<b>Suspicious apps allowed</b>	This field is only displayed if Sophos Mobile Security is available for this customer. Select whether detected suspicious apps are allowed.						
<b>PUAs allowed</b>	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.						
<b>Encryption required</b>	Select whether encryption is required for devices. On devices with Android 5 or higher, users must additionally enable the <b>Require PIN to start device</b> or <b>Require Password to start device</b> setting when they set a screen lock.						

Setting	Description	Android	Android Things	iOS	Windows Mobile	Windows Desktop	Windows IoT
	See <a href="#">Sophos knowledgebase article 123947</a> .						
<b>Data roaming allowed</b>	Select whether data roaming is allowed for devices.						
<b>Locate permission required</b>	This setting refers to the <b>Locate</b> function. Select whether the user has to allow the Sophos Mobile Control app at installation time to retrieve location data in order to be compliant.						
<b>Denial of SMC permissions allowed</b>	The Sophos Mobile Control app needs permissions on the device to work properly. The user has to grant these permissions when the app is installed.  Select whether a denial of the required permissions results in a compliance violation.						
<b>App is able to locate</b>	Location services must be turned on and the Sophos Mobile Control app must be allowed to use them.  For Windows Mobile, this rule only affects Windows Phone 8.1 devices.						
<b>Process control permission required</b>	Sophos Mobile Security needs usage access to ensure that blocked apps cannot be opened and protected apps will ask for a password.  Select whether a denial of usage access results						

Setting	Description	Android	Android Things	iOS	Windows Mobile	Windows Desktop	Windows IoT
	in a compliance violation.						
<b>Allowed apps / Forbidden apps</b>	<p>You can specify either <b>Allowed apps</b> or <b>Forbidden apps</b>. Select the desired option from the first list and then select the app group containing the apps that should be allowed or forbidden from the second list. For information on creating app groups, see <a href="#">App groups</a> (page 190).</p> <p>If you specify <b>Allowed apps</b>, only the listed apps are allowed. If other apps are detected the device will no longer be compliant.</p> <p><b>Note:</b> Android system apps are automatically allowed.</p> <p>If you specify <b>Forbidden apps</b>, the device will no longer be compliant if these apps are detected.</p>						
<b>Mandatory apps</b>	Specify apps that must be installed. Select the app group containing the mandatory apps from the list. For information on creating app groups, see <a href="#">App groups</a> (page 190).						
<b>Windows Defender must be turned on</b>	The Windows Defender setting <b>real-time protection</b> must be turned on.						
<b>Clean status from Windows Defender required</b>	Device is not compliant when Windows Defender shows alerts.						

Setting	Description	Android	Android Things	iOS	Windows Mobile	Windows Desktop	Windows IoT
<b>Up-to-date Windows Defender definitions required</b>	Windows Defender must use the latest spyware definitions.						

## 11.3 Assign compliance rules to device groups

1. On the menu sidebar, under **MANAGE**, click **Device groups**.

The **Device groups** page is displayed.

2. Click the blue triangle next to the device group you want to assign a set of compliance rules to and then click **Edit**.

There is always a **Default** device group available. For information on how to create your own device groups, see [Create device group](#) (page 71).

3. Under **Compliance rules** in the fields **Corporate devices** and **Personal devices**, select the compliance rules you want to apply.
4. Click **Save**.

The selected compliance rules are shown on the **Device groups** page for the relevant device group under **Compliance rules (corporate)** and **Compliance rules (personal)**.

## 11.4 Check devices for compliance

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

1. On the menu sidebar, under **CONFIGURE**, click **Compliance rules**.

The **Compliance rules** page is displayed.

2. Click **Check now**.

All enrolled devices are checked for compliance according to the rules defined in **Compliance rules**. The specified actions are carried out. The pie chart on the **Dashboard** is updated accordingly.



# 12 Devices

## 12.1 Add devices

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

- Add devices manually. See [Add device](#) (page 49).
- Import devices from a comma-separated values (CSV) file. See [Import devices](#) (page 50).
- Use the device enrollment wizard to add a device to Sophos Mobile Control, assign it to a user, enroll it, and transfer an enrollment task bundle. See [Use the device enrollment wizard to assign and enroll new devices](#) (page 52).
- Enable users to enroll devices on their own through the Self Service Portal. See [Configure Self Service Portal](#) (page 24). This portal reduces IT effort by allowing users to carry out tasks without contacting the helpdesk. The devices are provisioned by executing defined task bundles. See [Task bundles](#) (page 172).

We recommend that you use device groups to group devices for easier administration. See [Device groups](#) (page 71).


### 12.1.1 Add device

We recommend that you create one or more device groups before adding your first device to Sophos Mobile Control. You can then assign each device to a device group, to simplify device management. See [Create device group](#) (page 71).

To add a new device to Sophos Mobile Control:

1. On the menu sidebar, under **MANAGE**, click **Devices**.  
The **Devices** page is displayed.
2. Click **Add** and then select the platform from the **Add device manually** menu section.  
The **Edit device** page is displayed.
3. On the **Edit device** page, specify the following device details:
  - a) In the **Name** field, enter a unique name for the new device.
  - b) In the **Description** field, enter a description for the new device.
  - c) Under **Owner**, select **Company** or **Employee**.
  - d) In the **Email address** field enter an email address.
  - e) In the **Phone number** field, enter the phone number of the new device. Enter the phone number in international format, for example **+491701234567**.
  - f) 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 group](#) (page 71).

4. To assign a user to the device, click the **Edit user assignment** icon  next to the **User** field and then click **Assign user to device**. For further information, see [Assign a user to a device](#) (page 61).
5. To add custom properties to the device, go to the **Custom properties** tab and click **Add custom property**. For further information, see [Define custom properties for devices](#) (page 61).
6. After you have specified all relevant device details, click **Save**.

The new device is added to Sophos Mobile Control and displayed on the **Devices** page under **MANAGE**. You can now provision and manage the device.

**Note:** For iOS devices, when you have configured Sophos Mobile Control to synchronize the device name with the device as described in [Configure iOS settings](#) (page 21), the name you entered in the **Name** field is replaced by the name set during synchronization.

### 12.1.2 Duplicate a device

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

**Note:** This section doesn't apply to Android Things and Windows IoT 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. On the menu sidebar, under **MANAGE**, click **Devices**.

The **Devices** page is displayed.

2. Click the device you want to duplicate.

The **Show device** page is displayed.

3. Click **Actions** and then click **Duplicate this device**.

The device is duplicated and shown on the **Devices** page. You can now edit the duplicated device as required. To edit the device, click the blue triangle next to it and click **Edit**.

### 12.1.3 Import devices

You can add new devices by importing a UTF-8 encoded comma-separated values (CSV) file with up to 500 devices.

**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 extension `.csv`.

**Note:** The users that are specified in your CSV file must already be available in Sophos Mobile Control.

**Tip:** A sample file with the correct column names and column order is available for download from the **Import devices** page.

To import devices from a CSV file:

1. On the menu sidebar, under **MANAGE**, click **Devices**.
2. On the **Devices** page, click **Add > Import devices**.
3. On the **Import devices** page, click **Upload a file** and then navigate to the CSV file that you have prepared.

The entries are read in from the file and are displayed.

4. If the data is not formatted correctly or is inconsistent, the file as a whole cannot be imported. In this case, follow the error messages that are displayed next to the relevant entries, correct the content of the CSV file accordingly and upload it again.
5. Click **Finish** to create the devices.

The devices listed in the CSV file are imported and displayed on the **Devices** page. You can now enroll and configure the devices.

## 12.2 Enroll devices

After you have added new devices in the Sophos Mobile Control console, they must be enrolled with Sophos Mobile Control. You have the following options:

- You can enroll individual, unmanaged devices using the **Devices** function. For further information, see [Enroll individual devices](#) (page 51).
- You can use the device enrollment wizard to add a device to Sophos Mobile Control, assign it to a user, enroll it, and transfer an enrollment task bundle. See [Use the device enrollment wizard to assign and enroll new devices](#) (page 52).

**Note:** If required, you can use the device enrollment wizard or the auto-enrollment method to enroll iOS devices without Apple ID. This can be useful, for example to preconfigure the device before handing it over to a user. See [Enroll iOS devices without Apple ID](#) (page 54).

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

- You can bundle the tasks that are necessary to enroll devices, apply required policies and install required applications (for example, managed apps for iOS devices). For further information, see [Task bundles](#) (page 172).
- You can enable users to enroll devices through the Self Service Portal. To do so, include a task bundle for enrollment when configuring the settings for Self Service Portal use. For further information on how to create the task bundles required for enrollment, 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](#) (page 25).

### 12.2.1 Enroll individual devices

1. On the menu sidebar, under **MANAGE**, click **Devices**.

The **Devices** page is displayed.

2. Select the desired device, click **Actions** and then click **Enroll**.

**Note:** It is possible to select several devices for enrollment.

3. Click **Yes**, when you are asked if you want to enroll the selected devices.

The enrollment task is started and displayed on the **Task view** page. An email with enrollment instructions is sent to the user.

## 12.2.2 Use the device enrollment wizard to assign and enroll new devices

You can easily enroll new devices with the device enrollment wizard. It provides a workflow that combines the following tasks:

- Add a new device to Sophos Mobile Control.
- Optional: Assign a user to the device.
- Enroll the device.
- Optional: Transfer a task bundle to the device.

To start the device enrollment wizard:

1. On the menu sidebar, under **MANAGE**, click **Devices**, and then click **Add > Enrollment wizard**.

**Tip:** Alternatively, you can start the wizard from the **Dashboard** page by clicking the **Add device** widget.

2. On the **Enter user search parameters** wizard page, you can either enter search criteria to look up a user the device will be assigned to, or select **Skip user assignment** to enroll a device that will not be assigned to a user yet.

Click **Next** to continue.

3. When you have entered search criteria, the wizard displays a list of matching users. Select the required user and click **Next**.

4. On the **Device details** wizard page, configure the following settings:

Option	Description
<b>Platform</b>	The device platform. You can only select a platform that is enabled for the customer that you logged in to.
<b>Name</b>	A unique name under which the device will be managed by Sophos Mobile Control.
<b>Description</b>	An optional description of the device.
<b>Phone number</b>	An optional phone number. Enter the number in international format, for example <b>+491701234567</b> .
<b>Email address</b>	The email address to which the enrollment instructions will be sent.
<b>Owner</b>	Select the device owner: either <b>Company</b> or <b>Employee</b> .
<b>Device group</b>	Select the device group the device will be assigned to. If you have not created a device group yet, you can select the device group <b>Default</b> , which is always available.

When you are ready, click **Next**.

5. On the **Bundle selection** wizard page, select a task bundle that will be transferred to the device after it has been enrolled, or select **Only enroll device** to enroll the device without transferring a task bundle.

**Note:** Only task bundles that contain an *Enroll* task are displayed.

When you are ready, click **Next**. The device is added to Sophos Mobile Control.

6. On the **Enrollment** wizard page, follow the instructions to install the Sophos Mobile Control app onto the device and to complete the enrollment and provisioning.
7. When enrollment has been completed successfully, click **Finish** to close the device enrollment wizard.

**Note:**

- When you have made all the selections, you can close the wizard without having to wait for the **Finish** button to appear. An enrollment task is created and processed in the background.
- If you have selected a task bundle to be transferred to the device after enrollment, you can monitor the task status on the **Task view** page. See [View unfinished, failed and latest finished tasks](#) (page 16).
- For iOS devices, when you have configured Sophos Mobile Control to synchronize the device name with the device as described in [Configure iOS settings](#) (page 21), the name you entered in the **Name** field is ignored and the name that is configured on the device is used instead.

### 12.2.3 Auto-enroll iOS devices

You can configure iOS devices to auto-enroll with Sophos Mobile Control during device activation. To do so, you use Apple Configurator 2 to assign devices to the Sophos Mobile Control MDM server. When the users switch on their devices for the first time, the iOS setup assistant starts. During setup, the devices are automatically enrolled with Sophos Mobile Control.

**Note:** For a detailed description of Apple Configurator 2, see the [Apple Configurator 2 online help](#).

To configure auto-enrollment of iOS devices with Sophos Mobile Control:

1. As a one-time step to prepare auto-enrollment, create a device group that will be assigned to devices during auto-enrollment with Sophos Mobile Control. In the device group properties, select the **Enable iOS auto-enrollment** option. See [Create device group](#) (page 71).
2. Make a note of the URL that is displayed in the **Auto-enrollment URL** field of the device group.  
You need this URL when you configure devices with Apple Configurator 2.
3. Connect the iOS device you want to auto-enroll to an USB port of a Mac with Apple Configurator 2 installed.
4. In Apple Configurator 2, use the Prepare Assistant to set up the device configuration.
5. Select **Manual Enrollment** and then enter the auto-enrollment URL of the device group.
6. Follow the further steps of the Prepare Assistant. You can optionally configure the following aspects of the device activation:
  - Enable device supervision mode.
  - Configure host computers to which the device is allowed to connect with, using USB ports.
  - For supervised devices, generate or choose a "supervision identity".
  - Disable configuration steps of the iOS setup assistant.

After you have completed the configuration, hand over the device to the user. When the user switches on the device for the first time, the iOS setup and the enrollment with Sophos Mobile Control are performed as configured.

**Tip:** By default, Sophos Mobile Control manages auto-enrolled devices under a name that is composed from the device ID and the device type. Alternatively, Sophos Mobile Control can use the name that is configured on the device. See the **Synchronize device name** option in [Configure iOS settings](#) (page 21).

### 12.2.4 Enroll iOS devices without Apple ID

You can enroll an iOS device with Sophos Mobile Control without having to associate the device with an Apple ID first. This can be useful for example to preconfigure the device before handing it over to a user.

The standard enrollment method includes the installation of the Sophos Mobile Control app onto the device. Because the app is installed from the App Store and an Apple ID is required to access the App Store, you need to associate the device with the ID before starting the enrollment.

Alternatively, you can enroll an iOS device without installing the Sophos Mobile Control app, so there is no need to associate the device with an Apple ID. This is provided by:

- The auto-enrollment method. See [Auto-enroll iOS devices](#) (page 54).
- The device enrollment wizard. See [Use the device enrollment wizard to assign and enroll new devices](#) (page 52).

In the Device enrollment wizard, do as follows:

1. On the **Enrollment** page, select the **Enrollment without Apple ID** tab.
2. Use the device's web browser to open the enrollment URL. This opens a Sophos Mobile Control enrollment form.
3. In that form, enter the token and then click **Enroll**.
4. Follow the instructions on the device to install the enrollment task bundle.

## 12.2.5 Enroll Android Things device

This section describes how to enroll an Android Things device, using the device enrollment wizard.

### Prerequisites:

- You have set up a computer (hereafter referred to as *host computer*) that is connected to your local IP network and that has the Android Debug Bridge command-line tool (*adb*) installed. *adb* is part of the *Android SDK Platform-Tools* package. This package can either be installed as part of the Android SDK or as a standalone package. For details, see the Android developer documentation.
- You have flashed an Android Things image file onto the device that you want to enroll.
- You have connected the device to your local IP network through Ethernet or Wi-Fi.

To enroll the Android Things device with Sophos Mobile Control:

1. On the menu sidebar, under **MANAGE**, click **Devices**, and then click **Add > Enrollment wizard**.
2. Use the device enrollment wizard as described in [Use the device enrollment wizard to assign and enroll new devices](#) (page 52) to initiate the enrollment procedure. For an Android Things device, do as follows:
  - a) In the **Device details** wizard step, in the **Platform** field, select **Android Things**.
  - b) In the **Enrollment** wizard step, click **Open Sophos Mobile Control download area**, and then download the latest **SMC Android Client** version from there.
3. Copy the APK file that you downloaded to the host computer.
 

**Tip:** You can use the same APK file for all Android Things devices that you enroll.
4. On the host computer, use the *adb* command-line tool to connect to the Android Things device, where *<ip-address>* is the IP address of the device:

```
adb connect <ip-address>
connected to <ip-address>:5555
```

5. Install the Sophos Mobile Control app onto the Android Things device, using the following *adb* command:

```
adb install <path-to-apk-file>
```

6. Reboot the device, for example by using the following *adb* command:

```
adb reboot
```

**Note:** A reboot is required to grant the required permissions to the Sophos Mobile Control app.

7. After reboot, connect to the device again:

```
adb connect <ip-address>
```

8. Configure the Sophos Mobile Control app, using the *adb* command that is displayed in the device enrollment wizard or in the instructions email:

```
adb shell am start -d "<configuration-parameters>"
```

**Note:** You might receive a system message `Warning: Activity not started, its current task has been brought to the front.` This can be ignored.

The Sophos Mobile Control app on the Android Things device connects to your Sophos Mobile Control server. After the enrollment process has completed, the device is shown with status **Managed** in Sophos Mobile Control.

## 12.2.6 Enroll Windows IoT device

This section describes how to enroll a Windows IoT device, using the device enrollment wizard.

**Prerequisites:**

- You have flashed Windows 10 IoT Core onto the device that you want to enroll.
- You have connected the device to your local IP network through Ethernet or Wi-Fi.

To enroll the Windows IoT device with Sophos Mobile Control:

1. On the menu sidebar, under **MANAGE**, click **Devices**, and then click **Add > Enrollment wizard**.
2. Use the device enrollment wizard as described in [Use the device enrollment wizard to assign and enroll new devices](#) (page 52) to initiate the enrollment procedure. For a Windows IoT device, do as follows:
  - a) In the **Device details** wizard step, in the **Platform** field, select **Windows IoT**.
  - b) In the **Enrollment** wizard step, click **Download provisioning package** to download a PPKG file with the provisioning package for Sophos Mobile Control. This link is also available from the instructions email.



3. On a Windows computer that is connected to the same local network as the Windows IoT device, use the Windows File Explorer to connect to the device.

In the File Explorer address bar, enter the following address, where *<ip-address>* is the IP address of the device:

```
\\<ip-address>\c$
```

Enter your administrator username and password for the device if prompted.

4. Copy the PPKG file that you downloaded from the enrollment wizard to the `C:\Windows\Provisioning\Packages` folder on the device.

**Note:** There must only be a single PPKG file in that folder.

5. Reboot the device.

After reboot, the Windows IoT device executes the provisioning package and connects to your Sophos Mobile Control server. After the enrollment process has completed, the device is shown with status **Managed** in Sophos Mobile Control.

**Important:** On the **Show device** page, don't perform the device actions **Set to "Not managed"** or **Delete** before you have unenrolled the device. If you do so, you have to wipe the device—i.e. re-flash a Windows 10 IoT Core image onto the device—before you can enroll it again.

## 12.3 Unenroll devices

You can unenroll 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 enroll through the Self Service Portal.

1. On the menu sidebar, under **MANAGE**, click **Devices**.

The **Devices** page is displayed with all devices enrolled with Sophos Mobile Control for this customer.

2. Select the desired device, click **Actions** and then click **Unenroll**.

A message is displayed prompting you to confirm that you want to unenroll the device.

**Note:** It is possible to select several devices for unenrollment.

3. Click **Yes**.

The device is unenrolled. 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.
- The container apps (Sophos Secure Workspace and Sophos Secure Email) and the Sophos Mobile Security app are reset.

### **iOS devices:**

- All profiles are removed.

- All managed apps are removed.
- All certificates received through Mobile Device Management are removed.
- The container apps (Sophos Secure Workspace and Sophos Secure Email) are reset.

## 12.4 Manage devices

On the menu sidebar, under **MANAGE > Devices** and **Device groups**, you can keep track of 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 forbid email access for devices.
- Lock or unlock devices remotely.
- Reset device passwords.
- Wipe the device remotely in case of loss or theft.
- Decommission devices (Android and iOS).
- Delete devices.

### 12.4.1 View devices

1. On the menu sidebar, under **MANAGE**, click **Devices**.

The **Devices** page is displayed, showing all devices enrolled with Sophos Mobile Control for this customer.

2. Go to the required device and click its name.

The **Show device** page is displayed for the selected device.

**Tip:**

On the **Devices** page you can display additional information by pointing to certain elements:

- Point to the "Not managed" icon of a device to display the actual status like **Unenrolled** or **Checked out**.
- Point to the "Not compliant" icon of a device to display the severity level (high, medium, low).

#### 12.4.1.1 The Show device page

On the **Show device** page, all relevant information for an individual device is displayed.

In the upper part of the page, you can see the most important device information at a glance.

In the lower part of the page, detailed device information is displayed on several tabs. The tabs and information shown depend on the device platform.

- **Profiles** (Android, iOS)

Shows the profiles (including provisioning profiles) installed on the device.

The tab also contains commands to install profiles onto the device or to remove them.

- **Policies**

Shows the policies assigned to the device.

On this tab, the **Assign policy** button is available to assign a policy to the device.

- **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 custom device properties. These are the properties that you can create yourself. Custom device 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 and the actions taken because of the violation.

These actions are defined during the compliance rule configuration. See [Create compliance rules](#) (page 41).

- **Installed apps** (Android, iOS)

Shows the software installed onto the device.

For iOS devices, the **Managed** column on the **Installed apps** tab indicates managed apps. With Sophos Mobile Control you can push such apps to iOS devices and also silently remove them.

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

The **Size** column shows the disk space usage of an app itself. The **Data** column shows the additional disk space that an app uses for user data, configurations, and so on.

With the **Install app** button, you can install software onto the device. You can also remove managed apps from iOS devices by clicking the **Delete** icon next to the relevant app.

- **System apps** (Android)

Shows Android system apps on the device.

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

- **Knox apps** (Android)

This tab shows the apps that the user has installed in the Samsung Knox container.

- **Knox system apps** (Android)

This tab shows the system apps that are installed in the Samsung Knox container.

- **Scan 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 devices that protects devices from malicious apps and assists users in detecting app permissions that could be a security risk. The app can be managed by Sophos Mobile Control. For further information, see [Manage Sophos Mobile Security](#) (page 210).

- **Certificates**

Shows the certificates in use on the device.

- **Tasks**

This tab shows all unfinished and failed tasks for the device as well as the finished tasks of the last few days. You can also view these tasks, together with the tasks for all other devices, on the **Task view** page. See [Monitor tasks](#) (page 16).

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

### 12.4.1.2 Use the extended device filter

With the extended device filter, you can filter the device lists according to your needs.

To use the device filter:

1. On the **Devices** page, click the **Extended filter** button (magnifier icon) in the header bar.  
The **Device filter: Filter is not active.** dialog box is displayed.
2. Define your filter criteria.
3. After you have selected the required criteria, click **Filter**.

The filter is activated and the list of devices is reloaded. The magnifier icon in the header bar changes its color from blue to green to indicate that the filter is active. To reset the filter, click **Extended filter** again and click **Reset** in the filter dialog.

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

### 12.4.2 Edit devices

1. On the menu sidebar, under **MANAGE**, click **Devices**.

The **Devices** page is displayed with all devices enrolled with Sophos Mobile Control for this customer.

2. Click the blue triangle next to the required device and then click **Edit**.


The **Edit device** page is displayed for the selected device.

3. Make the necessary changes (for example, install or remove software on the **Installed apps** tab) and click **Save**.


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.

#### 12.4.2.1 Assign a user to a device

1. On the menu sidebar, under **MANAGE**, click **Devices**.
2. On the **Devices** page, click the blue triangle next to the required device and then click **Edit**.
3. On the **Edit device** page, click the **Edit user assignment** icon  next to the **User** field and then click the relevant entry from the selection list:
  - To assign a user to a device that has no user assigned to it yet, click **Assign user to device**.
  - To assign a different user to a device that already has a user assigned to it, click **Reassign user to device**.
4. In the **Enter user search parameters** step of the assignment dialog, enter search parameter in one or more fields to filter the user list that will be displayed in the next step. For example, enter the user name or part of it.
5. In the **Select user** step, select the required user and then click **Apply**.
6. On the **Edit device** page, click **Save**.

#### 12.4.2.2 Deassign a user from a device

1. On the menu sidebar, under **MANAGE**, click **Devices**.
2. On the **Devices** page, click the blue triangle next to the required device and then click **Edit**.
3. On the **Edit device** page, click the **Edit user assignment** icon  next to the **User** field and then click **Deassign user from device**.
4. In the confirmation dialog, click **Yes**.
5. Click **Save**.

#### 12.4.2.3 Define custom properties for devices

You can define custom properties for individual devices.

When you define a property with name `my property`, you can refer to the value of the property in profiles and policies by using the placeholder `_%_DEVPROP(my property)_%`. For example, you can use this to refer to the user that is assigned to a device.

For details on profile and policy placeholders, see [Placeholders in profiles and policies](#) (page 75).

**Note:**

- You cannot create a custom device property with the same name as a standard device property.
- When you duplicate a device as described in [Duplicate a device](#) (page 50), the new device receives the custom properties of the source device.

- As well as the device-level custom properties described here, you can also define customer-level custom properties. See [Define customer properties](#) (page 22).

To define a custom device property:

1. On the menu sidebar, under **SETTINGS**, click **Setup > General**. On the **Personal** tab, make sure that the **Show extended device details** option is selected.
2. On the menu sidebar, under **MANAGE**, click **Devices**.

The **Devices** page is displayed with all devices enrolled with Sophos Mobile Control for this customer.

3. Click the blue triangle next to the required device and then click **Edit**.
4. On the **Edit device** page, go to the **Custom properties** tab and click **Add custom property**.
5. Enter a **Name** and a **Value** for the new custom device property.
6. Click **Apply** to add the property.
7. Click **Save** to save the changes to the device.

#### 12.4.2.4 Configure network access

Before you can configure network access for a device, Network Access Control (NAC) must be enabled in Sophos Mobile Control.

For on-premise installation, NAC is enabled by the super administrator. See the [Sophos Mobile Control super administrator guide](#).

For Sophos Mobile Control as a Service, NAC is always enabled.

There are two options to configure network access for a device:

1. Allow or deny network access unconditionally.
2. Disable network access when the device violates a compliance rule, enable network access otherwise.

**Note:** Sophos Mobile Control does not control the network access by itself. Instead, it provides a *Deny network* status that can be used by external NAC software like Sophos UTM to block network communication.

To configure network access for a device:

1. On the menu sidebar, under **MANAGE**, click **Devices**.
2. On the **Devices** page, select the devices for which you want to set the network access mode.
3. Click **Actions**, and then click **Set network access**.
4. Select the network access mode:
  - **Allow:** Network access for the selected devices is allowed.
  - **Deny:** Network access for the selected devices is denied.
  - **Auto mode:** Network access for the selected devices is based on the compliance status of the devices.
5. Click **Yes** to save the changes.

For information on how to configure network access in compliance rules, see [Create compliance rules](#) (page 41).

### 12.4.3 Lock device

You can lock a device that is managed by Sophos Mobile Control. This activates the screen lock.

1. On the menu sidebar, under **MANAGE**, click **Devices**.
2. On the **Devices** page, click the blue triangle next to the device that you want to lock or unlock and then click **Show**.
3. On the **Show device** page, click **Actions > Lock**.

A task to activate the lock screen is created and transferred to the device. Users must enter their device password (or their PIN or pattern, if configured) to unlock the device.

You can display the task status on the **Task view** page.

## 12.5 Apple DEP

With the Apple Device Enrollment Program (DEP), you can purchase iOS (and OS X) devices in volume for distribution within your company. DEP simplifies the deployment of mobile devices by providing the following features:

- Configurable activation process.
- Wireless enabling of supervision mode.
- Over-the-air configuration.
- Automatic enrollment of iOS devices with Sophos Mobile Control during device activation.

**Tip:** For detailed information on DEP, visit the Apple DEP website at <http://www.apple.com/business/dep/>.

### Preparation steps

To prepare the management of DEP devices with Sophos Mobile Control, perform the following one-time steps:

1. On the Apple DEP web portal, create a virtual MDM server and link it to Sophos Mobile Control. See [Set up a virtual MDM server](#) (page 64).
2. In Sophos Mobile Control, create one or more DEP profiles that control various device attributes specific to DEP. With the DEP profile, you can also customize the iOS setup assistant that starts when a device is switched on for the first time. See [Create DEP profile](#) (page 65).

### Deployment steps

When you purchase DEP devices, the typical deployment process includes the following steps:

1. Purchase the devices from Apple or an approved DEP vendor.
2. On the Apple DEP web portal, assign the devices to the Sophos Mobile Control MDM server. For this and the next step, see [Deploy DEP devices](#) (page 68).
3. In the Sophos Mobile Control console, assign a DEP profile to the devices.
4. Distribute the devices to your users.

5. When the users switch on their devices for the first time, the customized iOS setup assistant starts. During setup, the devices are enrolled with Sophos Mobile Control and the user is assigned to the device.
6. If required, you can transfer additional task bundles to the devices to complete the provisioning.

## 12.5.1 Set up a virtual MDM server

**Prerequisite:** This procedure assumes that you have already enrolled in the Apple Device Enrollment Program (DEP) and set up an administrator account for the Apple DEP web portal.

**Note:** For detailed information on enrolling in DEP, visit the Apple DEP website at <http://www.apple.com/business/dep/> or see the [Apple Deployment Programs online help](#).

**Tip:** If you have already enrolled in the Apple Volume Purchase Program (VPP), you can use the same Apple ID for DEP.

To use Apple DEP with Sophos Mobile Control, you need to create a virtual MDM server on the Apple DEP web portal and link it to the Sophos Mobile Control server. This includes a verification process to establish a secure connection between Sophos Mobile Control and the Apple DEP web service.

To set up a virtual MDM server for Sophos Mobile Control:

1. Log in to the Sophos Mobile Control console with an administrator account for the customer for which you want to manage the DEP devices.
2. On the menu sidebar, under **SETTINGS**, click **Setup > System setup**, and then click the **Apple DEP** tab.
3. Click **Download public key** to download the Sophos Mobile Control public key file for Apple DEP.  
The file is saved to your local computer, using the download settings of your web browser.
4. Open the Apple DEP web portal at <https://deploy.apple.com> in a new browser window. You can do this by clicking the **Apple DEP web portal** link in Sophos Mobile Control.
5. Log in to the Apple DEP web portal with your company Apple ID.
6. On the portal, go to **Device Enrollment Program > Manage Servers**, and then click **Add MDM Server**.
7. Enter a name for MDM server, for example **sophos Mobile Control**.
8. In the next step, upload the public key file that you downloaded from Sophos Mobile Control.
9. In the next step, download the server token.  
At this point, you may log out from the Apple DEP web portal.
10. On the **Apple DEP** tab of Sophos Mobile Control, click **Upload a file** and select the server token that you downloaded from the Apple DEP web portal.  
The details of your virtual MDM server are displayed.
11. Click **Save** to save your changes.

The DEP server token is valid for one year. To notify when the token is about to expire, Sophos Mobile Control sends several email reminders to all administrators of the relevant customer, starting 30 days prior to the expiry date.

**Important:** When you create a new server token on the Apple DEP web portal, you must use the same Apple ID that you used for the creation of the initial token.



## 12.5.2 Create DEP profile

You need to set up the Apple Device Enrollment Program (DEP) before you can create DEP profiles. See [Set up a virtual MDM server](#) (page 64).

A DEP profile is assigned to a DEP device and provides information to the Apple server when the device is activated. This information includes:

- The MDM server (that is Sophos Mobile Control) assigned to manage the device.
- Configuration options for the enrollment with Sophos Mobile Control.
- A list of hosts that the device is allowed to pair with.
- Customization options for the iOS setup assistant that starts when the device is switched on for the first time.

If required, you can create several DEP profiles to use different setup and enrollment settings for your DEP devices.

To create a DEP profile:

1. On the menu sidebar, under **SETTINGS**, click **Setup > System setup**, and then click the **Apple DEP profiles** tab.
2. Click **Add**.
3. In the **Edit DEP profile** dialog, enter a name and optionally a description for the DEP profile.
4. Optional: In the **Device group** list, select a device group that will be assigned to devices when they are enrolled with Sophos Mobile Control.

For information on device groups, see [Device groups](#) (page 71).

**Note:** To simplify device management, we recommend that you use a separate device group for DEP devices.

5. Optional: In the **Task bundle** list, select a task bundle that will be transferred onto the devices when they are enrolled with Sophos Mobile Control.

The list includes all iOS task bundles that contain no enrollment task.

For information on task bundles, see [Task bundles](#) (page 172).

6. On the **Enrollment** tab, you can configure the following settings:

Option	Description
<b>Supervise device</b>	Supervision mode is enabled.
<b>User can remove MDM profile</b>	<p>The user is able to remove the Sophos Mobile Control enrollment profile through the iOS user interface.</p> <p>This option can only be deselected for supervised devices.</p>
<b>Install SMC app</b>	<p>Install the Sophos Mobile Control app onto the device.</p> <p>If you enable this option, you must also disable the <b>Skip Apple ID</b> option on the <b>iOS setup</b> tab to make sure that Sophos Mobile Control can install the app from the App Store.</p> <p><b>Note:</b> Alternatively, if you are enrolled in the Apple Volume Purchase Program (VPP), the Sophos Mobile Control app can be installed as a VPP app, even if the device is not associated with an Apple ID. Devices must be in status <i>managed</i> and must use iOS 9 or higher. See <a href="#">Automatically assign VPP apps</a> (page 187).</p>
<b>User can skip MDM profile assignment</b>	The user is able to skip the setup step that applies the Sophos Mobile Control enrollment profile.
<b>Assign user to device</b>	<p>During the enrollment process with Sophos Mobile Control, users are asked for their Self Service Portal credentials and then assigned to the device.</p> <p>Use this option to auto-assign a user to the device.</p>

- On the **iOS setup** tab, you can disable configuration steps of the iOS setup assistant that starts when the device is switched on for the first time.

**Note:** These settings only affect the iOS setup. If you disable a configuration step, the user is still able to enable the relevant option later. To completely disable a feature, use a **Restrictions** configuration. See [Restrictions configuration \(iOS device profile\)](#) (page 121).

Option	Description
<b>Skip Apps &amp; Data</b>	The page <b>Apps &amp; Data</b> is not displayed. The user cannot restore data from an iCloud or iTunes backup, or transfer data from an Android device.
<b>Disable "Move Data from Android"</b>	On the <b>Apps &amp; Data</b> page, the option <b>Move Data from Android</b> is not available. The user cannot transfer data from an Android device. This can only be enabled when <b>Skip Apps &amp; Data</b> is also enabled.
<b>Skip Diagnostics</b>	The page <b>Diagnostics</b> is not displayed. Sending diagnostic and usage data to Apple is disabled.
<b>Skip Location Services</b>	The page <b>Location Services</b> is not displayed. The user cannot enable location services.
<b>Skip Siri</b>	The page <b>Siri</b> is not displayed. The user cannot set up Siri.
<b>Skip Display Zoom</b>	The page <b>Display Zoom</b> is not displayed. The user cannot change the display view.
<b>Skip Apple ID</b>	The page <b>Apple ID</b> is not displayed. The user cannot log in with their Apple ID to access Apple services.
<b>Skip Apple Pay</b>	The page <b>Apple Pay</b> is not displayed. The user cannot add credit or debit card information for paying in stores or within apps using Apple Pay.
<b>Skip Touch ID</b>	The page <b>Touch ID</b> is not displayed. The user cannot set up a fingerprint in place of a passcode.
<b>Skip Passcode</b>	The page <b>Create a Passcode</b> is not displayed. The user cannot set up a passcode to unlock the device.
<b>Skip Terms and Conditions</b>	The page <b>Terms and Conditions</b> is not displayed.

8. On the **Support information** tab, you can configure the following settings:

Option	Description
<b>Department</b>	The department or location name associated with the profile. This name is included in the information that the user can access by clicking <b>About Configuration</b> during device setup.
<b>Phone number</b>	The support phone number for your company. This field is pre-populated with the phone number from the technical support contact details. See <a href="#">Configure technical support contact details</a> (page 22). <b>Note:</b> The phone number is stored internally in the DEP profile but is not available to the device user.
<b>Email</b>	The support email address for your company. This field is pre-populated with the email address from the technical support contact details. See <a href="#">Configure technical support contact details</a> (page 22). <b>Note:</b> The email address is stored internally in the DEP profile but is not available to the device user.

9. On the **USB pairing** tab, you configure host computers to which the device is allowed to connect with, using USB ports.

This can be used to sync the device with iTunes or to manage it with Apple Configurator.

- To allow USB connection with all hosts, select **Allow USB pairing with all hosts**.
- To forbid USB connection or to restrict it to certain hosts, deselect **Allow USB pairing with all hosts** and then upload a certificate file for each host to which the device is allowed to connect with.

10. When you have configured all tabs of the **Edit DEP profile** dialog, click **Apply** to save the DEP profile.

11. To assign the profile to all new DEP devices to which no profile has been manually assigned to, select it in the **Default DEP profile assigned to new devices** list.

When you select **None**, you have to manually assign a DEP profile to new DEP devices as described in [Deploy DEP devices](#) (page 68). Otherwise, DEP devices will not be enrolled with Sophos Mobile Control when they are activated.

12. Click **Save** to save your changes.

### 12.5.3 Deploy DEP devices

Perform this procedure to connect your devices to Apple DEP and to enroll them with Sophos Mobile Control.

You can manage devices that you have purchased from Apple or from an approved DEP vendor. Before you can connect devices to Apple DEP, you need to configure the device vendor on the Apple DEP portal.

**Note:** In a typical DEP workflow, you perform this procedure before handing over the devices to your users for activation and usage.

**Note:** For a detailed description of the Apple DEP portal, see the [Apple Deployment Programs online help](#).

To assign your devices to Sophos Mobile Control and to assign a DEP profile to them:

1. Open the web portal for the Apple deployment programs at <https://deploy.apple.com> in your web browser and then log in with your company Apple ID.
2. On the portal, go to **Device Enrollment Program > Manage Devices**.
3. Under **Choose Devices By**, select your new devices by serial number, by order number, or upload a CSV file containing the serial numbers of your devices.

**Note:** If you have purchased your devices from a reseller, they are available on the DEP portal within 24 hours after the reseller posts your order to Apple.

4. Under **Choose Action**, select **Assign to Server** and then select the virtual MDM server that you have set up for Sophos Mobile Control as described in [Set up a virtual MDM server](#) (page 64).
5. Click **OK** to perform the assignment.

At this point, you may log out from the Apple DEP web portal.

You may skip the remaining steps if you have configured a default DEP profile as described in [Create DEP profile](#) (page 65).

6. Log in to the Sophos Mobile Control console with an administrator account for the customer for which you want to manage the DEP devices.
7. On the menu sidebar, under **MANAGE**, click **Devices** and then click **Apple DEP**.  
The **Apple DEP devices** page lists all devices that you have assigned to Sophos Mobile Control on the Apple DEP web portal.
8. If the devices that you just assigned to Sophos Mobile Control do not appear in the list, click **Synchronize with Apple DEP portal**.

**Note:** To limit the load on the Apple DEP server, repeated synchronization is possible only after a short queue time.

9. Select the new devices and then click **Actions > Assign profile**.
10. In the confirmation dialog, select the DEP profile you want to assign to the devices and then click **OK**.

When the purchased devices arrive at your company, you can hand them over to your users. No further configuration is required. When the users switch on their devices for the first time, the iOS setup and the enrollment with Sophos Mobile Control are performed as configured in the assigned DEP profile.

When you have selected the **Assign user to device** profile option as described in [Create DEP profile](#) (page 65), the users are automatically assigned to their device.

## 12.5.4 Manage DEP devices

DEP devices are managed in Sophos Mobile Control just as non-DEP devices are. See [Manage devices](#) (page 58).

Specifically to DEP, you can assign a DEP profile to a device. The DEP profile provides information to the Apple server when the device is activated. See [Create DEP profile](#) (page 65).

**Note:** Because a DEP profile is only used for device activation, changing the assigned DEP profile has no effect on the device until it is reset and then activated again.

To change the DEP profile of a device:

1. On the menu sidebar, under **MANAGE**, click **Devices** and then click **Apple DEP**.

The **Apple DEP devices** page lists all devices that you have assigned to Sophos Mobile Control on the Apple DEP web portal.

2. Click **Synchronize with Apple DEP portal** to update the DEP information.

**Note:** To limit the load on the Apple DEP server, the **Synchronize with Apple DEP portal** option is disabled after a synchronization and becomes available again after a few minutes.

3. Select the devices to which you want to assign a different DEP profile.
4. Click **Actions > Assign profile**.
5. In the confirmation dialog, select the DEP profile you want to assign to the devices and then click **OK**.

# 13 Device groups

Device groups are used to categorize devices. They help you to manage devices efficiently as you can carry out tasks on a group rather than on individual devices.

A device always belongs to exactly one device group. You assign a device to a device group when you add it to Sophos Mobile Control.

**Tip:** Only group devices with the same operating system. This makes it easier to use groups for installations and other operating system specific tasks.

## 13.1 Create device group

1. On the menu sidebar, under **MANAGE**, click **Device groups**, and then click **Create device group**.
2. On the **Edit device group** page, enter a **Name** and a **Description** for the new device group.
3. In the **Compliance rules** section, use the **Corporate devices** and **Personal devices** lists to select the compliance rules you want to apply.
4. Click **Save**.

**Note:** The device group settings contain the **Enable iOS auto-enrollment** option. This option allows you to enroll iOS devices with the Apple Configurator. See [Auto-enroll iOS devices](#) (page 54)

The new device group is created and shown on the **Device groups** page.

## 13.2 Delete device groups

1. On the menu sidebar, under **MANAGE**, click **Device groups**.
2. On the **Device groups** page, click the blue triangle next to the device group that you want to delete, and then click **Delete**.
3. In the confirmation dialog, select one of the remaining device groups to which devices from the current device group will be re-assigned.  
This selection is not available when there are no devices assigned to the current device group.
4. Click **Yes** to delete the device group.

**Note:** When there is only one device group left and there are devices assigned to it, you cannot delete this device group.

# 14 Profiles and policies

## Profiles

Profiles are settings that you define and then install onto a device or device group.

To install a profile on one or more devices, Sophos Mobile Control creates a task and executes it at the specified time. When you update a profile, you must install it again for the changed configurations to take effect on the device.

The following profile types are available:

- [Configurations for Android device profiles](#) (page 78)
- [Configurations for Android for Work policies](#) (page 95)
- [Configurations for Knox container profiles](#) (page 114)
- [Configurations for iOS device profiles](#) (page 119)

## Policies

Policies are settings that you define and then assign to a device or device group. You can only assign one policy of each type to one device.

If you assign a policy to a device, a sync is triggered and the settings take effect immediately. Assigned policies are updated on the device each time a device connects to the Sophos Mobile Control server. So when you update a policy, you do not have to explicitly re-apply it to the device.

The following policy types are available:

- [Configurations for Sophos container policies for Android](#) (page 104)
- [Configurations for Mobile Security policies](#) (page 114)
- [Configurations for Android Things policies](#) (page 119)
- [Configurations for Sophos container policies for iOS](#) (page 145)
- [Configurations for Windows Mobile policies](#) (page 155)
- [Configurations for Windows Desktop policies](#) (page 163)
- [Configurations for Windows IoT policies](#) (page 169)

## 14.1 Create profile or policy

Profiles and policies are made up of one or more configurations. By adding configurations, you define the scope of the profile or policy, that is, the areas that are managed on the devices.

1. On the menu sidebar, under **CONFIGURE**, click **Profiles, policies** and then click the platform for which you want to create the profile or policy.
2. On the **Profiles and policies** page, click **Create**. If there is more than one profile or policy type available for a platform, **Create** opens a menu from which you can select the required type.

For a list of available profile and policy types, see [Profiles and policies](#) (page 72).



3. Enter a name, a version and a description.  
Required fields are marked with a red asterisk.
4. For Sophos container policies, a **General** configuration is mandatory and is automatically added to the policy. On the **Edit policy** page, click **General** to open the configuration and make the required changes.
5. For Android for Work policies, a **Restrictions** configuration is mandatory and is automatically added to the policy. On the **Edit policy** page, click **Restrictions** to open the configuration and make the required changes.
6. To add more configurations to the profile or policy, click **Add configuration** and then select the configuration you want to add.  
  
**Note:** The configurations supported may depend on the version of the operating system or on other device features. The requirements are indicated by a blue label.
7. In the settings page of the configuration, specify the required settings.
8. Optional: Repeat the previous steps to add more configurations.
9. After you have added all required configurations, click **Save**.

The profile or policy is created. For information on how to apply it to devices, see [Install a profile onto devices](#) (page 76) or [Assign a policy to devices](#) (page 76).

## 14.2 Import iOS device profiles created with Apple Configurator

You can import profiles created with Apple Configurator into Sophos Mobile Control.

Apple Configurator can be downloaded from the App Store.

**Note:** You import device profiles with the same procedure as provisioning profiles for your self-developed iOS apps. When you upload a profile file, Sophos Mobile Control analyzes its content in order to distinguish between the two profile types.

1. After you have created a profile in Apple Configurator, export it (unencrypted and unsigned) and save it on your computer.
2. On the menu sidebar, under **CONFIGURE**, click **Profiles, policies > Apple iOS**.
3. On the **Profiles and policies** page, click **Create > Import profile**.

The **Edit profile** page is displayed.

4. Enter a name, a description and, optionally, a version for the new profile in the relevant fields.
5. Click **Upload a file** and navigate to the file you have saved on your computer, select it and click **Open**.
6. Click **Save**.

The profile is created. It can be installed onto devices. See [Install a profile onto devices](#) (page 76).

## 14.3 Import provisioning profiles for iOS apps

When you develop your own iOS apps, you create provisioning profiles so that your apps can be installed from an IPA file instead of the App Store. You can upload these provisioning profiles to the Sophos Mobile Control server to subsequently distribute them to your devices.

For details on provisioning profiles, see the *iOS Developer Library*.

**Note:** You import provisioning profiles with the same procedure as device profiles created with Apple Configurator. When you upload a profile file, Sophos Mobile Control analyzes its content in order to distinguish between the two profile types.

1. After you have generated a provisioning profile in your iOS development environment, save it on your computer.
2. On the menu sidebar, under **CONFIGURE**, click **Profiles, policies > Apple iOS**.
3. On the **Profiles and policies** page, click **Create > Import profile**.

The **Edit profile** page is displayed.

4. Enter a name, a description and, optionally, a version for the new profile in the relevant fields.
5. Click **Upload a file** and navigate to the file you have saved on your computer, select it and click **Open**.
6. Click **Save**.

The profile is created. It can be installed onto devices. See [Install a profile onto devices](#) (page 76).

## 14.4 Windows Desktop password complexity rules

Password complexity rules (for example length, number of uppercase and lowercase letters) for Windows Desktop devices are fixed and cannot be set by a Sophos Mobile Control policy. Different rules apply for local and for Microsoft accounts.

### Local accounts

- Password must not contain the user's account name or more than two consecutive characters from the user's full name.
- Password must be six or more characters long.
- Password must contain characters from three of the following four categories:
  - Uppercase characters A-Z (Latin alphabet)
  - Lowercase characters a-z (Latin alphabet)
  - Digits 0-9
  - Special characters (!, \$, #, %, etc.)

## Microsoft accounts

- Password must be eight or more characters long.
- Password must contain characters from two of the following four categories:
  - Uppercase characters A-Z (Latin alphabet)
  - Lowercase characters a-z (Latin alphabet)
  - Digits 0-9
  - Special characters (!, \$, #, %, etc.)

## 14.5 Samsung Knox support

You can manage your Samsung Knox devices with Sophos Mobile Control.

**Note:** In order to manage Samsung Knox devices, a Samsung **Knox Premium license key** needs to have been entered in the Sophos Mobile Control **System setup**.

To configure the Knox container of Samsung devices, see [Configurations for Knox container profiles](#) (page 114).

To install apps in a Samsung Knox container, see [Add app](#) (page 180).

To manage your Samsung Knox devices you can create task bundles for the following actions:

- **Knox container: lock**
- **Knox container: unlock**
- **Knox container: reset password**
- **Knox container: remove** (removes the container and all related configuration from the device)

To create a task bundle for a Samsung Knox device, see [Create task bundle](#) (page 172).

## 14.6 Placeholders in profiles and policies

Profiles and policies may contain placeholders which are replaced by actual data at the time of task execution. The following placeholders can be used in profiles:

- Placeholders for user data:
  - `_%EMAILADDRESS_%`
  - `_%USERNAME_%`
- Placeholders for device properties:
  - `_%DEVPROP(property name)_%`  
*property name* can be either a standard property or a custom property of the device. See [Define custom properties for devices](#) (page 61).

- Placeholders for customer properties:
  - `%_CUSTPROP(property name)_%`  
See [Define customer properties](#) (page 22).

## 14.7 Install a profile onto devices

1. On the menu sidebar, under **CONFIGURE**, click **Profiles, policies** and then click one of the device platforms that support profiles:
  - **Android**
  - **Apple iOS**The **Profiles and policies** page for the selected platform is displayed.
2. Click the blue triangle next to the profile to be installed and then click **Install**.  
The **Select devices** page is displayed.
3. On this page, you can:
  - Select individual devices onto which you want to install the profile.
  - Click **Select device groups** and select one or several device groups.
4. After you have made your selection, click **Next**.  
The **Set execution date** page is displayed.
5. Under **Scheduled date**, select **Now** or specify a **Date** and **Time** for the execution of the task.
6. Click **Finish**.  
The **Task view** is shown.

The profile is installed onto the selected devices at the specified date and time.

**Note:** You can also install a profile by using one of the following options:

- Create a task bundle with an **Install profile or assign policy** task and transfer it to the required devices or device groups.
- On the device's **Show device** page, select the **Profiles** tab and click **Install profile**.

## 14.8 Assign a policy to devices

1. On the menu sidebar, under **CONFIGURE**, click **Profiles, policies** and then click one of the device platforms that support policies:
  - **Android**
  - **Android Things**
  - **Apple iOS**
  - **Windows Mobile**
  - **Windows Desktop**
  - **Windows IoT**

The **Policies** page for the selected platform is displayed.

2. Click the blue triangle next to the policy to be assigned and then click **Assign**.

The **Select devices** page is displayed.

3. On this page, you can:

- Select individual devices you want to assign the policy to.
- Click **Select device groups** and select one or several device groups for assigning the policy.

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

The policy is assigned to the selected devices and a synchronization process for the selected devices is triggered.

**Note:** You can also assign a policy by using one of the following options:

- Create a task bundle with an **Install profile or assign policy** task and transfer it to the required devices or device groups.
- On a device's **Show device** page, select the **Policies** tab and click **Assign policy**.

**Note:** Policies cannot be removed from a device. To disable a policy, you must assign a different policy to that device.

## 14.9 Remove profile

Use one of the following procedures to remove a profile from devices:

- On a device's **Show device** page select the **Profiles** tab. Click the blue triangle next to profile you want to remove and then click **Remove**.
- Create a task bundle with a **Remove profile** task and transfer it to the required devices or device groups.

## 14.10 Download profiles and policies

You can download profiles and policies that you have configured in the Sophos Mobile Control console. This is useful, for example, if you need to pass the defined settings on to Sophos Support.

1. On the menu sidebar, go to **Profiles, policies** and click a device platform.

The **Profiles and policies** page for the selected platform is displayed.

2. Click the name of the required profile or policy.

The **Show profile** or **Show policy** page is displayed.

3. Click **Download**.

The profile or policy is saved to your local computer.

## 14.11 Configurations for Android device profiles

With an Android device profile you configure various aspects of Android devices, like password policies, restrictions or Wi-Fi settings.

For information on how to create a device profile, see [Create profile or policy](#) (page 72).

### 14.11.1 Password policies configuration (Android device profile)

With the **Password policies** configuration you define password rules for devices.

**Note:** The settings supported may depend on the version of the operating system or on other device features. The scope is indicated by a blue label in Sophos Mobile Control.

#### Password type

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

Setting/Field	Description
<b>Any</b>	Users must set a screen lock. They can choose a type <b>Pattern</b> , <b>PIN</b> or <b>Password</b> screen lock. No additional restrictions are imposed.
<b>Alphabetic</b>	Users must set a <b>Password</b> screen lock. Digits are allowed, but the password must contain at least one letter. You can define a minimum length. See the following table.
<b>PIN</b>	Users must set a <b>PIN</b> or <b>Password</b> screen lock. You can define a minimum length. See the following table.
<b>Alphanumeric</b>	Users must set a <b>Password</b> screen lock. The password must contain both letters and digits. You can define a minimum length. See the following table.
<b>Complex</b>	Users must set a <b>Password</b> screen lock. The password must contain both letters and digits. You can define a minimum length and a minimum number of digits, lowercase and uppercase letters and special characters. See the following two tables.

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

Setting/Field	Description
<b>Minimum password length</b>	The minimum number of characters a password must contain.
<b>Idle time before password prompt</b>	The time (in seconds) after the device will be locked if it has not been used. The device can be unlocked by entering the password.
<b>Maximum password age in days</b>	Requires users to change their password in the specified interval. Value range: 0 (no password change required) to 730 days.
<b>Maximum number of failed attempts until device wipe</b>	The maximum number of failed attempts to enter the correct password before the device is wiped.
<b>Minimum history length</b>	The number of old passwords that are remembered and compared with new ones. When the user defines a new password, it is not accepted if it matches a previously used password. Value range: 1 to 5 or none.

If you select **Complex**, the following additional fields are displayed:

Setting/Field	Description
<b>Minimum number of letters</b>	The minimum number of letters a password must contain.
<b>Minimum number of lowercase letters</b>	The minimum number of lowercase letters a password must contain.
<b>Minimum number of uppercase letters</b>	The minimum number of uppercase letters a password must contain.
<b>Minimum number of non-alphabetic characters</b>	The minimum number of non-alphabetic characters (for example & or !) a password must contain.
<b>Minimum number of numerals</b>	The minimum number of numerals a password must contain.
<b>Minimum number of special characters</b>	The minimum number of special characters (for example !"\$\$%&/()=,.-:;_@<>) a password must contain.

## 14.11.2 Restrictions configuration (Android device profile)

With the **Restrictions** configuration you define restrictions for devices.

### Security

Setting/Field	Description
<b>Force encryption</b>	Users must encrypt their devices.
<b>Force SD card encryption</b>	When the profile is installed onto a device, the user must encrypt the SD card. <b>Note:</b> For some device types, users can choose to cancel the encryption. They will be reminded again on the next SD card mount.
<b>Allow fast encryption</b>	If the check box is cleared, the fast encryption options in the device settings are unavailable.
<b>Allow factory reset</b>	If the check box is cleared, users cannot reset their devices to factory state.
<b>Allow developer options</b>	If the check box is cleared, users cannot change the developer options.
<b>Allow safe mode</b>	If the check box is cleared, users cannot boot the device in safe mode.
<b>Allow USB debugging</b>	If the check box is cleared, USB debugging is turned off. <b>Note:</b> For Sony devices with Enterprise API version 9 or above, clearing the <b>Allow USB debugging</b> checkbox makes all developer options unavailable.
<b>Allow firmware recovery</b>	If the check box is cleared, all types of firmware updates (like over-the-air, download etc.) are turned off.
<b>Allow backup</b>	If the check box is cleared, users cannot create system backups. Google backup is turned off. Other backup methods (for example Sophos Mobile Control backups) remain available.



Setting/Field	Description
<b>Allow settings changes</b>	If the check box is cleared, users cannot change device settings. Depending on individual devices the settings icon is removed.
<b>Allow clipboard</b>	If the check box is cleared, users cannot copy any contents to the clipboard. <b>Note:</b> This setting applies to devices with Android 4.2.2 or higher.
<b>Enable shared clipboard</b>	Allows users to copy clipboard content between apps. If the check box is cleared, each app has an individual clipboard. This setting is only available if you select <b>Allow clipboard</b> .
<b>Allow screen capture</b>	If the check box is cleared, users cannot take a screenshot of the display.
<b>Allow mock GPS locations</b>	If the check box is cleared, users cannot select a mock location app in the Android developer options.
<b>Allow over-the-air firmware updates</b>	If the check box is cleared, over-the-air firmware updates are turned off.
<b>Allow audio recording</b>	If the check box is cleared, users cannot perform audio recording.
<b>Allow video recording</b>	If the check box is cleared, users cannot record videos. They can take pictures and stream videos.
<b>Allow Activation Lock</b>	If the check box is cleared, the Activation Lock options in the device settings are unavailable.
<b>Allow S Beam</b>	If the check box is cleared, the Samsung S Beam app is unavailable.
<b>Allow S Voice</b>	If the check box is cleared, the Samsung S Voice app is unavailable.
<b>Allow “Share via”</b>	If the check box is cleared, the <b>Share via</b> feature is turned off.

## Accounts

Setting/Field	Description
<b>Allow multiple user accounts</b>	If the check box is cleared, multi-user support is turned off. Users or other apps cannot create additional user accounts.
<b>Allow addition of new email accounts</b>	If the check box is cleared, users cannot add email accounts. This does not affect the account creation through a device profile.
<b>Allow removal of the Google account</b>	If the check box is cleared, users cannot remove the Google account from the device.
<b>Allow auto-sync for Google accounts</b>	If the check box is cleared, Google accounts are not synchronized automatically. Users are still able to perform a manual sync from inside some apps like Gmail.

## Network and communication

Setting/Field	Description
<b>Allow airplane mode</b>	If the check box is cleared, users cannot enable airplane mode.
<b>Allow sync while roaming</b>	If the check box is cleared, synchronization while roaming is turned off.
<b>Allow emergency calls only</b>	Only emergency calls are allowed. All other calls will be blocked.
<b>Force manual sync during roaming</b>	Automatic data synchronization is turned off when the device is roaming. This affects all configured accounts, such as Google or Exchange.
<b>Force mobile data connection</b>	Users cannot turn off cellular data.
<b>Allow SMS</b>	If the check box is cleared, users cannot send text messages.

Setting/Field	Description
<b>Allow mobile data connection while roaming</b>	If the check box is cleared, mobile data connections while roaming are turned off.
<b>Allow voice calls while roaming</b>	If the check box is cleared, voice calls while roaming are turned off.
<b>Allow user mobile data limit</b>	If the check box is cleared, users cannot set a mobile data limit.
<b>Allow VPN</b>	If the check box is cleared, users cannot use VPN connections.
<b>Allow Wi-Fi Direct</b>	If the check box is cleared, data transfer through Wi-Fi Direct is turned off.
<b>Allow Android Beam</b>	If the check box is cleared, data transfer through Android Beam is turned off. This includes the Samsung S Beam app.
<b>Allow Miracast policy</b>	If the check box is cleared, data transfer through Miracast is turned off.
<b>Allow Bluetooth</b>	If the check box is cleared, Bluetooth is turned off.
<b>Allow NFC</b>	If the check box is cleared, NFC (near field communication) is turned off.
<b>Allow Wi-Fi</b>	If the check box is cleared, Wi-Fi is turned off.

## Tethering

Setting/Field	Description
<b>Allow tethering</b>	If the check box is cleared, all tethering is turned off. This includes tethering over Wi-Fi, USB and Bluetooth.  <b>Note:</b> If the check box is cleared, the settings <b>Allow Wi-Fi tethering</b> , <b>Allow USB tethering</b> and <b>Allow Bluetooth tethering</b> have no effect.
<b>Allow Wi-Fi tethering</b>	If the check box is cleared, Wi-Fi tethering ( <i>Wi-Fi hotspot</i> ) is turned off.

Setting/Field	Description
<b>Allow USB tethering</b>	If the check box is cleared, USB tethering is turned off.
<b>Allow Bluetooth tethering</b>	If the check box is cleared, Bluetooth tethering is turned off.
<b>Allow configuring Wi-Fi tethering</b>	The user can configure the settings of the Wi-Fi hotspot.

## Hardware

Setting/Field	Description
<b>Allow camera</b>	If the check box is cleared, the camera is unavailable.
<b>Force GPS for location queries</b>	GPS information is used for device location.
<b>Allow SD card</b>	If the check box is cleared, SD cards cannot be used in devices.
<b>Allow moving apps to the SD card</b>	If the check box is cleared, users cannot move apps from the internal storage to the SD card.
<b>Allow writing to the SD card</b>	If the check box is cleared, it is not possible to write to unencrypted SD cards.
<b>Allow microphone</b>	If the check box is cleared, the microphone is unavailable.
<b>Allow USB</b>	The USB mass storage mode and the USB media player are available on the device.
<b>Allow USB media player</b>	If the check box is cleared, the Media Transfer Protocol (MTP) is unavailable. Because Android uses MTP for USB file transfer, any file transfer over USB is blocked.

## Applications

Setting/Field	Description
<b>Allow app install</b>	If the check box is cleared, users cannot install apps.

Setting/Field	Description
<b>Allow app uninstall</b>	If the check box is cleared, users cannot uninstall apps.
<b>Allow unsigned app install</b>	If the check box is cleared, users can only install signed APK files.
<b>Allow Play Store</b>	If the check box is cleared, the Google Play Store app is unavailable. <b>Note:</b> This setting applies to devices with Android 4.2.2 or higher.
<b>Allow apps from unknown sources</b>	If the check box is cleared, users can only install apps through the Google Play Store app.
<b>Allow native browser</b>	If the check box is cleared, the native browser is unavailable. Third-party browser apps are not affected.
<b>Allow app crash reports</b>	If the check box is cleared, apps cannot send crash reports.
<b>Allow wallpaper change</b>	If the check box is cleared, users cannot change the wallpaper.
<b>Allow camera on lock screen</b>	If the check box is cleared, the camera is unavailable when the screen is locked.
<b>Allow widgets on lock screen</b>	If the check box is cleared, widgets are unavailable when the screen is locked.
<b>Allow Knox contact info for personal calls</b>	By default, a Samsung Knox device displays contact information when the user receives a call from a Knox contact while in personal mode.  If the check box is cleared, Knox contact information is not displayed in personal mode.
<b>Allow autofill in browser</b>	The user can enable autofill in the settings of the native Android browser. If enabled, web pages can provide suggestions when the user is filling in form data.  If the check box is cleared, autofill is turned off and the browser setting is unavailable.

Setting/Field	Description
<b>Allow cookies in browser</b>	The user can enable cookies in the settings of the native Android browser. If enabled, web pages can store cookies on the device.  If the check box is cleared, cookies are turned off and the browser setting is unavailable.
<b>Allow JavaScript in browser</b>	The user can enable JavaScript in the settings of the native Android browser. If enabled, web pages can execute JavaScript code on the device.  If the check box is cleared, JavaScript is turned off and the browser setting is unavailable.
<b>Allow pop-ups in browser</b>	The user can enable pop-ups in the settings of the native Android browser. If enabled, web pages can open new browser windows.  If the check box is cleared, pop-ups are turned off and the browser setting is unavailable.
<b>Allow changing date and time settings</b>	The user can change the date and time settings.
<b>Allowed apps / Forbidden apps</b>	You can configure either <b>Allowed apps</b> or <b>Forbidden apps</b> . Select the desired option from the first list and then select the app group containing the apps that should be allowed or forbidden from the second list.  App installations initiated by the Sophos Mobile Control server are not restricted by this setting.  For information on creating app groups, see <a href="#">App groups</a> (page 190).

### 14.11.3 Knox Premium restrictions configuration (Android device profile)

With the **Knox Premium restrictions** configuration you define restrictions for Samsung Knox devices. These restrictions apply to the device, not to the Knox container.

Option	Description
<b>Allow firmware auto update options</b>	The device automatically checks for firmware updates. Users cannot change this in the device settings.

Option	Description
<b>Enable ODE Trusted Boot verification</b>	<p>The device decrypts the data partition on boot only if the binary and the kernel are official, i.e. if the device is not rooted.</p> <p>If the check box is cleared, the device always decrypts the data partition on boot.</p>
<b>Prevent installation of another administrator app</b>	<p>The installation of apps that require device administrator privileges is prevented. This does not affect apps that are installed by Sophos Mobile Control.</p>
<b>Prevent activation of another administration app</b>	<p>The activation of device administrator privileges for apps is prevented.</p>
<b>Allow Common Criteria mode</b>	<p>The Common Criteria mode (CC mode) of the device is turned on, ensuring that the device meets the security requirements stated by the Mobile Device Fundamentals Protection Profile (MDFPP).</p> <p><b>Note:</b> CC mode is only used if the following requirements are met:</p> <ul style="list-style-type: none"> <li>▪ Device encryption is turned on.</li> <li>▪ Fast encryption is turned off.</li> <li>▪ External storage encryption is turned on.</li> <li>▪ A maximum number of failed login attempts until device wipe is set.</li> <li>▪ Certificate revocation is turned on.</li> <li>▪ Password history is turned off.</li> </ul>

#### 14.11.4 App Protection configuration (Android device profile)

With the **App Protection** configuration you define password requirements for protecting apps.

With App Protection in use, users must define a password when they start a protected app for the first time. After a failed login attempt a login delay is imposed.

If App Protection is active on a device, the command **Reset App Protection password** is available in the **Actions** menu of the **Show device** page. The user can also reset the App Protection password in the Self Service Portal.

Setting/Field	Description
<b>Password complexity</b>	The minimum complexity requirements for the password to be defined by users, for example <b>6 char password</b> .
<b>Grace period in minutes</b>	After the grace period has expired, protected apps can only be unlocked by entering a password.
<b>App group</b>	Select the app group containing the apps that are password protected. For creating app groups, see <a href="#">App groups</a> (page 190).

### 14.11.5 App Control configuration (Android device profile)

With the **App Control** configuration you define apps that users are not allowed to start. For example, you can use this to block apps that have been pre-installed by the device manufacturer and cannot be uninstalled.

Setting/Field	Description
<b>App group</b>	Select the app group containing the blocked apps. For information on creating app groups, see <a href="#">App groups</a> (page 190).

### 14.11.6 Exchange ActiveSync configuration (Android device profile)

With the **Exchange ActiveSync** configuration you define user settings for your Microsoft Exchange Server.

Setting/Field	Description
<b>Account name</b>	The account name.
<b>Exchange ActiveSync host</b>	The address of the Microsoft Exchange Server. <b>Note:</b> If you use the SMC EAS proxy, enter the URL of the SMC proxy server.
<b>Domain</b>	The domain for this account.



Setting/Field	Description
<b>User</b>	The user for this account. If you enter the variable %_USERNAME_%, the server replaces it with the actual user name.
<b>Email address</b>	The email address of the account. If you enter the variable %_EMAILADDRESS_%, the server replaces it with the actual email address.
<b>Sender</b>	A sender name for this account. If you enter the variable %_EMAILADDRESS_%, the server replaces it with the actual email address.
<b>Password</b>	The password for this account. If you leave this field empty, users must enter the password on their devices.
<b>Synchronization period</b>	The time period emails are synchronized for. If you select a time period, only the emails from within the specified period are synchronized to the inbox on the managed device.
<b>Synchronization interval</b>	The interval between email synchronization processes.
<b>SSL</b>	All communication is sent through SSL (Secure Socket Layer). We recommend that you select this check box.
<b>Default account</b>	The account is used as the default email account.
<b>Allow all certificates</b>	Allow all certificates in transfer processes from the email server.
<b>Client certificate</b>	The client certificate for the connection to ActiveSync.
<b>Allow forwarding emails</b>	Allow forwarding of emails.
<b>Allow use of HTML format</b>	Allow the use of HTML format in emails.
<b>Maximum attachment size in MB</b>	The maximum size of a single email message (1, 3, 5, 10, Unlimited).
<b>Synchronize content types</b>	The content types to be synchronized.

**Note:**

For Sony devices with Enterprise API version 6.x or below, it is important that the Exchange ActiveSync account information matches the user that is assigned to the device.

On these devices, the SMC client is not able to send the ActiveSync ID to the SMC server. When a device contacts the SMC EAS proxy for the first time, the ActiveSync ID that the email client sends is not known to Sophos Mobile Control. To verify the account details, the SMC EAS proxy searches for a device with an unknown ActiveSync ID and an assigned user that matches the user information supplied by the email client. If such a device is found, the ActiveSync ID is assigned to that device and the email request is passed on to the Exchange server. Otherwise, the request is rejected.

For details, see [Sophos knowledgebase article 121360](#).

### 14.11.7 Wi-Fi configuration (Android device profile)

With the **Wi-Fi** configuration you specify settings for connecting to Wi-Fi networks.

Setting/Field	Description
<b>SSID</b>	The ID of the Wi-Fi network.
<b>Security type</b>	<p>The security type of the Wi-Fi network:</p> <ul style="list-style-type: none"> <li>▪ <b>None</b></li> <li>▪ <b>WEP</b></li> <li>▪ <b>WPA/WPA2</b></li> <li>▪ <b>EAP/PEAP</b></li> <li>▪ <b>EAP/TLS</b></li> <li>▪ <b>EAP/TTLS</b></li> </ul> <p>If you select <b>WEP</b> or <b>WPA/WPA2</b>, a <b>Password</b> field is displayed. Enter the relevant password.</p> <p>If you select one of the EAP settings, the fields <b>Identity</b>, <b>Anonymous Identity</b> and <b>Password</b> are displayed. Enter the required EAP information.</p> <p>If you select <b>EAP/PEAP</b> or <b>EAP/TTLS</b>, the field <b>Phase 2 authorization</b> is displayed in addition. Select the type of authorization:</p> <ul style="list-style-type: none"> <li>▪ <b>PAP</b></li> <li>▪ <b>CHAP</b></li> <li>▪ <b>MSCHAP</b></li> <li>▪ <b>MSCHAPv2</b></li> </ul>

### 14.11.8 VPN configuration (Android device profile)

With the **VPN** configuration you define VPN settings for network connections.

Setting/Field	Description
<b>Connection name</b>	The name of the connection shown on the device.
<b>Server</b>	The host name or the IP address of the server.
<b>Connection type</b>	<p>The type of the VPN connection:</p> <ul style="list-style-type: none"> <li>▪ <b>L2TP/IPsec (PSK)</b> If you select this type, the fields <b>User</b>, <b>Password</b> and <b>L2TP/IPsec (PSK)</b> are displayed. Enter the user and password. In the <b>L2TP/IPsec (PSK)</b> field, enter the pre-shared key for authentication.</li> <li>▪ <b>L2TP/IPsec (Certificate)</b> If you select this type, the fields <b>Client certificate</b>, <b>Root certificate</b>, <b>User</b> and <b>Password</b> are displayed. In the fields <b>Client certificate</b> and <b>Root certificate</b>, select the relevant certificates. In addition, enter the <b>User</b> and the relevant <b>Password</b>.</li> </ul>

### 14.11.9 Root certificate configuration (Android device profile)

With the **Root certificate** configuration you upload a root certificate to devices.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. 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.

### 14.11.10 Client certificate configuration (Android device profile)

With the **Client certificate** configuration you install a client certificate onto Android devices.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. 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.

### 14.11.11 SCEP configuration (Android device profile)

With the **SCEP** configuration you enable devices to request certificates from a Certificate Authority using the Simple Certificate Enrollment Protocol (SCEP).

**Note:** You must first add a **Root certificate** configuration to upload the CA certificate of the SCEP server before you can add a **SCEP** configuration.

Setting/Field	Description
<b>URL</b>	The web address of the Certificate Authority server. Use the variable <code>_%_SCEPPROXYURL_%</code> to refer to the server URL that is configured on the <b>SCEP</b> tab of the <b>System setup</b> page.
<b>Alias name</b>	The name under which the certificate will appear in selection dialogs. This should be a memorable name to identify the certificate. For example, use the same value as in the <b>Subject</b> field, but without the <b>CN=</b> prefix.
<b>Subject</b>	The name of the entity (for example person or device) that will receive the certificate. You can use placeholders for user data or device properties. The value that you enter (with placeholders replaced by the actual data) must be a valid X.500 name. For example: <ul style="list-style-type: none"> <li>▪ Enter <code>CN=_%_USERNAME_%</code> to specify a user.</li> <li>▪ Enter <code>CN=_%_DEVPROP(serial_number)_%</code> to specify a device.</li> </ul> For information on available placeholders, see <a href="#">Placeholders in profiles and policies</a> (page 75).
<b>Type of Subject Alternative Name</b>	Optionally, configure a Subject Alternative Name (SAN). Select one of the available SAN types.
<b>Value of Subject Alternative Name</b>	If you have selected a SAN type, enter the SAN value.
<b>NT user login name</b>	

Setting/Field	Description
<b>Challenge</b>	The web address to obtain a challenge password from the SCEP server.  Use the variable <code>%_CACHALLENGE_</code> to refer to the challenge URL that is configured on the <b>SCEP</b> tab of the <b>System setup</b> page.
<b>Root certificate</b>	The CA certificate.  Select the certificate from the list. The list contains all certificates that you have uploaded in <b>Root certificate</b> configurations of the current profile.
<b>Key size</b>	The size of the public key in the issued certificate.  Make sure that the value matches the size configured on the SCEP server.
<b>Use as digital signature</b>	If you select this check box, the public key can be used as a digital signature.
<b>Use for encryption</b>	If you select this check box, the public key can be used for data encryption.

### 14.11.12 Access Point Name configuration (Android device profile)

With the **Access Point Name** configuration you specify an Access Point Name (APN) configuration for mobile devices. APN configurations define how devices connect to a mobile network.

**Important:** We recommend that you ask your carrier for the required settings. If you select **Use as default APN** and the settings are not correct, the device cannot access data through cellular networks.

**Note:** With the exception of the **APN** field, all settings are optional and should only be specified if required by your mobile network carrier.

Setting/Field	Description
<b>APN</b>	The APN that the device quotes when it opens a connection with the carrier.  This must match an APN that the carrier accepts. Otherwise, the connection cannot be established.
<b>User-friendly name</b>	An optional name that is displayed on the device in addition to the APN.

Setting/Field	Description
<b>Proxy server and port</b>	The address and port of the HTTP server that is used for web traffic.
<b>User name, User password</b>	A user name and password for connecting to the APN.
<b>Server</b>	The WAP Gateway Server.
<b>MMSC</b>	The Multimedia Messaging Service Center (MMSC).
<b>MMS proxy server and port</b>	The address and port of a HTTP server that is used for communication with the MMSC.
<b>Mobile Country Code (MCC), Mobile Network Code (MNC)</b>	MCC and MNC for specifying the carrier. The APN is only used for this carrier.
<b>Authentication type</b>	The authentication method for PPP connections.
<b>APN type</b>	The types of data connection that this APN is used for.  To use the APN for all data types, enter * or leave the field empty.
<b>Bearer</b>	The Radio Access Technology (RAT) that the carrier uses.
<b>Protocol</b>	The network protocol that is supported by the carrier.
<b>Roaming protocol</b>	The network protocol that is supported by the carrier when in roaming mode.
<b>Use as default APN</b>	If selected, devices will use this APN as default.  An error is raised when you try to select this option in more than one <b>Access Point Name</b> configuration.

### 14.11.13 Kiosk mode configuration (Android device profile)

With the **Kiosk mode** configuration you define restrictions for devices to put them into a kiosk mode.

Click **Select source** and then do one of the following to specify an app that is started when the profile is transferred to a device:

- Select **Custom** and enter an app identifier.

- Select **App list** and then select an app from the **App identifier** list. The list contains all apps that you have configured on the **Apps** page. See [Add app](#) (page 180).
- Select **None** to configure kiosk mode without specifying an app. The kiosk mode restrictions are applied to the device, but no app is started.

Under **Options**, deselect hardware and software features you want to disable in kiosk mode.

When the profile is transferred to a device, the app that you specified is started. However, if you have not turn off any of the available hardware or software features, the user will be able to leave the app and use the device as normal. To set the device into a true kiosk mode, you must clear at least the **Allow Home button** and **Allow task manager** checkboxes.

**Note:**

- The app that you specify must be installed on the device. If it is not, the transfer tasks will remain in state *Incomplete* until the app is installed. To install the app, create a task bundle with an **Install app** task, for example, and transfer it to your devices.
- If you want to specify an app for Samsung Knox devices, make sure it is a launcher app. This type of app provides an alternative desktop for Android.
- For Sony devices with Enterprise API version 9 or above, if you clear any of the **Allow volume up**, **Allow volume down** or **Allow volume mute** checkboxes, all volume buttons of the device are disabled.

## 14.12 Configurations for Android for Work policies

With an Android for Work policy you configure settings that are related to the work profile of a device.

For information on how to create an Android for Work policy, see [Create profile or policy](#) (page 72).

### 14.12.1 Password policies configuration (Android for Work policy)

With the **Password policies** configuration you define password rules for the work profile.

**Note:** The settings supported may depend on the version of the operating system or on other device features. The scope is indicated by a blue label in Sophos Mobile Control.

#### Password type

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

Setting/Field	Description
<b>Any</b>	Users must set a screen lock. They can choose a type <b>Pattern</b> , <b>PIN</b> or <b>Password</b> screen lock. No additional restrictions are imposed.

Setting/Field	Description
<b>Alphabetic</b>	Users must set a <b>Password</b> screen lock. Digits are allowed, but the password must contain at least one letter. You can define a minimum length. See the following table.
<b>PIN</b>	Users must set a <b>PIN</b> or <b>Password</b> screen lock. You can define a minimum length. See the following table.
<b>Alphanumeric</b>	Users must set a <b>Password</b> screen lock. The password must contain both letters and digits. You can define a minimum length. See the following table.
<b>Complex</b>	Users must set a <b>Password</b> screen lock. The password must contain both letters and digits. You can define a minimum length and a minimum number of digits, lowercase and uppercase letters and special characters. See the following two tables.

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

Setting/Field	Description
<b>Minimum password length</b>	The minimum number of characters a password must contain.
<b>Idle time before password prompt</b>	The time (in seconds) after the device will be locked if it has not been used. The device can be unlocked by entering the password.
<b>Maximum password age in days</b>	Requires users to change their password in the specified interval. Value range: 0 (no password change required) to 730 days.
<b>Maximum number of failed attempts until device wipe</b>	The maximum number of failed attempts to enter the correct password before the device is wiped.
<b>Minimum history length</b>	The number of old passwords that are remembered and compared with new ones. When the user defines a new password, it is not accepted if it matches a previously used password. Value range: 1 to 5 or none.

If you select **Complex**, the following additional fields are displayed:



Setting/Field	Description
<b>Minimum number of letters</b>	The minimum number of letters a password must contain.
<b>Minimum number of lowercase letters</b>	The minimum number of lowercase letters a password must contain.
<b>Minimum number of uppercase letters</b>	The minimum number of uppercase letters a password must contain.
<b>Minimum number of non-alphabetic characters</b>	The minimum number of non-alphabetic characters (for example & or !) a password must contain.
<b>Minimum number of numerals</b>	The minimum number of numerals a password must contain.
<b>Minimum number of special characters</b>	The minimum number of special characters (for example !"\$\$%&/()=,.-;:_@<>) a password must contain.

### 14.12.2 Restrictions configuration (Android for Work policy)

With the **Restrictions** configuration you configure restrictions and related settings for Android for Work.

#### Security

Setting/Field	Description
<b>Allow screen capture</b>	Users can capture the screen content of work apps.
<b>Allow user to configure credentials</b>	Users can install or remove certificates in the work profile.
<b>Allow work clipboard in personal apps</b>	Users can copy text from a work app and paste it into a personal app. Pasting clipboard text from a personal app into a work app is always possible.
<b>Allow Smart Lock</b>	Users can turn on the Android Smart Lock feature that automatically unlocks the device in certain situations.

Setting/Field	Description
<b>Allow location sharing</b>	Work apps can access the device's location features. If the check box is cleared, work apps cannot access the device's location features, even if the user has turned location sharing on.
<b>Allow opening web links in personal apps</b>	Web links that the user taps in a work app can be opened by a personal browser app.
<b>Allow debugging</b>	Users can turn on the debugging features in the Android developer options.
<b>Allow unlocking device by fingerprint</b>	Users can use the fingerprint sensor to unlock the device.

## Accounts

Setting/Field	Description
<b>Allow managing accounts</b>	Users can add or remove accounts from the work profile, for example app accounts. Users cannot remove the Google account from the work profile.

## Network and communication

Setting/Field	Description
<b>Allow Android Beam</b>	Users can send data from work apps through Android Beam (data transfer through NFC).
<b>Allow VPN</b>	Users can use VPN connections for work apps.

## Hardware

Setting/Field	Description
<b>Allow camera</b>	Work apps can access the camera.

## Applications

Setting/Field	Description
<b>Allow app uninstall</b>	Users can uninstall work apps.
<b>Allow installing apps from unknown sources</b>	If the check box is cleared, users can only install work apps from the Google Play Store, not from unknown sources or through Android Debug Bridge (ADB).
<b>Allow managing apps</b>	If the check box is cleared, users cannot perform the following tasks for work apps: <ul style="list-style-type: none"> <li>▪ Uninstall apps</li> <li>▪ Disable apps</li> <li>▪ Stop apps</li> <li>▪ Clear app cache</li> <li>▪ Clear app data</li> <li>▪ Clear setting <b>Open by default</b></li> </ul>
<b>Short message</b>	A company-specific support message that is displayed to the user when functionality has been turned off. <b>Note:</b> If you enter more than 200 characters, the message may be truncated.
<b>Long message</b>	Additional text to complement the short message. The text is displayed when the user taps <b>More details</b> in screens that display the short message. <b>Note:</b> This text is also displayed on the Android <b>Device administrator</b> screen for the Sophos Mobile Control app.

### 14.12.3 App Protection configuration (Android for Work policy)

With the **App Protection** configuration you define password requirements for protecting work apps, i.e. the apps that are installed in the work profile.

With App Protection in use, users must define a password when they start a protected app for the first time. After a failed login attempt a login delay is imposed.

If App Protection is active on a device, the command **Reset App Protection password** is available in the **Actions** menu of the **Show device** page. The user can also reset the App Protection password in the Self Service Portal.

Setting/Field	Description
<b>Password complexity</b>	The minimum complexity requirements for the password to be defined by users, for example <b>6 char password</b> .
<b>Grace period in minutes</b>	After the grace period has expired, protected apps can only be unlocked by entering a password.
<b>App group</b>	Select the app group containing the apps that are password protected. For creating app groups, see <a href="#">App groups</a> (page 190).

### 14.12.4 App Control configuration (Android for Work policy)

With the **App Control** configuration you define work apps that users are not allowed to start.

Setting/Field	Description
<b>App group</b>	Select the app group containing the blocked apps. For information on creating app groups, see <a href="#">App groups</a> (page 190).

### 14.12.5 App permissions configuration (Android for Work policy)

With the **App permissions** configuration you configure what happens when a work app requests a permission at runtime.

Setting/Field	Description
<b>Default permission handling</b>	<p>The default response for future runtime permission requests of work apps:</p> <ul style="list-style-type: none"> <li>▪ <b>Prompt:</b> Apps prompt the user to grant a permission.</li> <li>▪ <b>Auto-accept:</b> All runtime permission requests are automatically granted.</li> <li>▪ <b>Auto-deny:</b> All runtime permission requests are automatically denied.</li> </ul> <p>The user cannot change the permissions later.</p>
<b>App-specific runtime permissions</b>	<p>You can grant or deny certain runtime permissions for individual apps. Click <b>Add</b> and then configure the settings for an app:</p> <p>In the <b>App identifier</b> field, enter the internal identifier of the app.</p> <p>For each runtime permission, select the desired grant state:</p> <ul style="list-style-type: none"> <li>▪ <b>Selectable:</b> The user can grant or deny the permission.</li> <li>▪ <b>Granted:</b> Permission is granted and cannot be denied by the user.</li> <li>▪ <b>Denied:</b> Permission is denied and cannot be granted by the user.</li> </ul>

### 14.12.6 Exchange ActiveSync configuration (Android for Work policy)

With the **Exchange ActiveSync** configuration you define user settings for your Microsoft Exchange Server. These settings are applied to the Gmail app in the work profile.

Setting/Field	Description
<b>Account name</b>	The account name.
<b>Exchange ActiveSync host</b>	<p>The address of the Microsoft Exchange Server.</p> <p><b>Note:</b> If you use the SMC EAS proxy, enter the URL of the SMC proxy server.</p>

Setting/Field	Description
<b>Domain</b>	The domain for this account.
<b>User</b>	The user for this account. If you enter the variable %_USERNAME_%, the server replaces it with the actual user name.
<b>Email address</b>	The email address of the account. If you enter the variable %_EMAILADDRESS_%, the server replaces it with the actual email address.
<b>Sender</b>	A sender name for this account. If you enter the variable %_EMAILADDRESS_%, the server replaces it with the actual email address.
<b>Password</b>	The password for this account. If you leave this field empty, users must enter the password on their devices.
<b>Synchronization period</b>	The time period emails are synchronized for. If you select a time period, only the emails from within the specified period are synchronized to the inbox on the managed device.
<b>SSL</b>	All communication is sent through SSL (Secure Socket Layer). We recommend that you select this check box.
<b>Allow all certificates</b>	Allow all certificates in transfer processes from the email server.
<b>Client certificate</b>	The client certificate for the connection to ActiveSync.

### 14.12.7 Root certificate configuration (Android for Work policy)

With the **Root certificate** configuration you install a root certificate onto devices. This certificate will be available to work apps, i.e. to apps that are installed in the work profile.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. 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.

### 14.12.8 Client certificate configuration (Android for Work policy)

With the **Client certificate** configuration you install a client certificate onto Android devices. This certificate will be available to work apps, i.e. to apps that are installed in the work profile.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. 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.

### 14.12.9 SCEP configuration (Android for Work policy)

With the **SCEP** configuration you enable devices to request certificates from a Certificate Authority using the Simple Certificate Enrollment Protocol (SCEP). These certificates will be available to work apps, i.e. to apps that are installed in the work profile.

**Note:** You must first add a **Root certificate** configuration to upload the CA certificate of the SCEP server before you can add a **SCEP** configuration.

Setting/Field	Description
<b>URL</b>	The web address of the Certificate Authority server. Use the variable <code>%_SCEPPROXYURL_%</code> to refer to the server URL that is configured on the <b>SCEP</b> tab of the <b>System setup</b> page.
<b>Alias name</b>	The name under which the certificate will appear in selection dialogs.  This should be a memorable name to identify the certificate. For example, use the same value as in the <b>Subject</b> field, but without the <b>CN=</b> prefix.
<b>Subject</b>	The name of the entity (for example person or device) that will receive the certificate.  You can use placeholders for user data or device properties.  The value that you enter (with placeholders replaced by the actual data) must be a valid X.500 name. For example: <ul style="list-style-type: none"> <li>▪ Enter <code>CN=%_USERNAME_%</code> to specify a user.</li> <li>▪ Enter <code>CN=%_DEVPROP(serial_number)_%</code> to specify a device.</li> </ul> For information on available placeholders, see <a href="#">Placeholders in profiles and policies</a> (page 75).

Setting/Field	Description
<b>Type of Subject Alternative Name</b>	Optionally, configure a Subject Alternative Name (SAN). Select one of the available SAN types.
<b>Value of Subject Alternative Name</b>	If you have selected a SAN type, enter the SAN value.
<b>NT user login name</b>	
<b>Challenge</b>	The web address to obtain a challenge password from the SCEP server. Use the variable %_CACHALLENGE_% to refer to the challenge URL that is configured on the <b>SCEP</b> tab of the <b>System setup</b> page.
<b>Root certificate</b>	The CA certificate. Select the certificate from the list. The list contains all certificates that you have uploaded in <b>Root certificate</b> configurations of the current profile.
<b>Key size</b>	The size of the public key in the issued certificate. Make sure that the value matches the size configured on the SCEP server.
<b>Use as digital signature</b>	If you select this check box, the public key can be used as a digital signature.
<b>Use for encryption</b>	If you select this check box, the public key can be used for data encryption.

## 14.13 Configurations for Sophos container policies for Android

With a Sophos container policy you configure settings that are related to the Sophos container apps Sophos Secure Email and Sophos Secure Workspace.

For information on how to create a Sophos container policy, see [Create profile or policy](#) (page 72).



### 14.13.1 General configuration (Android Sophos container policy)

With the **General** configuration you define settings that apply to all Sophos container apps, if applicable.

Setting/Field	Description
<b>Enable Sophos container password</b>	Users must enter an additional password to be able to start a Sophos container app. The password has to be defined when the first container app is started after the configuration has been applied. This password applies to all container apps.
<b>Password complexity</b>	<p>The required minimum complexity of the Sophos container password. More secure passwords are always allowed. Passwords (a mix of numeric and alphanumeric characters) are always seen as more secure than PINs (numeric characters only).</p> <ul style="list-style-type: none"> <li>▪ <b>Any:</b> Sophos container passwords do not have restrictions.</li> <li>▪ <b>4 digit PIN</b></li> <li>▪ <b>6 digit PIN</b></li> <li>▪ <b>4 char password</b></li> <li>▪ <b>6 char password</b></li> <li>▪ <b>8 char password</b></li> <li>▪ <b>10 char password</b></li> </ul>
<b>Password age in days</b>	The number of days that a password can be used before users are prompted to change it.
<b>Failed logins until lock</b>	The number of failed login attempts that are tolerated before the container apps are locked. Once they are locked an administrator needs to unlock the apps or, if allowed, users can use the Self Service Portal to do so.
<b>Allow fingerprint</b>	Users can use their fingerprint to unlock the app.
<b>Grace period in minutes</b>	<p>The period of time within which no Sophos container password must be entered when a container app comes to the foreground again.</p> <p>The grace period applies to all container apps. You can switch between the apps during the grace period without entering a password.</p> <p>You can select <b>1, 2, 5, 10, 15</b> minutes.</p>

Setting/Field	Description
<p><b>Lock on device lock</b></p>	<p>When the device is locked, the Sophos container is locked as well.</p> <p>If the check box is cleared, the container is locked only after the grace period has expired.</p>
<p><b>Last server connect</b></p>	<p>The period of time within users can use a Sophos container app without a connection to the Sophos Mobile Control server.</p> <p>When a Sophos container app becomes active and does not have contact with the server within the defined period of time, a lock screen will be displayed. Users can only unlock the app by tapping <b>Retry</b> on the lock screen. The app will then try to connect to the server. If the connection can be established, the app will be unlocked. If not, access will be denied.</p> <ul style="list-style-type: none"> <li>▪ <b>On access:</b> Server connection is always required and the app is locked when the server cannot be reached.</li> <li>▪ <b>1 hour:</b> Server connection is required when the app becomes active one hour or more after the last successful server connection.</li> <li>▪ <b>3 hours</b></li> <li>▪ <b>6 hours</b></li> <li>▪ <b>12 hours</b></li> <li>▪ <b>1 day</b></li> <li>▪ <b>3 days</b></li> <li>▪ <b>1 week</b></li> <li>▪ <b>none:</b> No regular contact is required.</li> </ul>
<p><b>Offline starts without server connection</b></p>	<p>In this field you define how often users can start one of the Sophos container apps without a server connection.</p> <p><b>Note:</b> This setting requires the Sophos container password feature to be turned on.</p> <p>A counter is incremented whenever users enter the Sophos container password. If the counter exceeds the defined number, the same lock screen as for the <b>Last server connect</b> setting will be displayed. The counter will be reset if a connection to the Sophos Mobile Control server is established.</p> <ul style="list-style-type: none"> <li>▪ <b>Unlimited:</b> No server connection is required.</li> <li>▪ <b>0:</b> Starting the app without a server connection is not possible.</li> </ul>

Setting/Field	Description
	<ul style="list-style-type: none"> <li>▪ <b>1</b>: After one start of the app, a successful server connection is necessary.</li> <li>▪ <b>3</b></li> <li>▪ <b>5</b></li> <li>▪ <b>10</b></li> <li>▪ <b>20</b></li> </ul>
<b>Root allowed</b>	Container apps are allowed to run on rooted devices.
<p><b>App usage constraints</b> Here you can define constraints on using the Sophos container apps. Click <b>Add</b> to enter constraints.</p>	
<b>Geo-fencing</b>	Lets you add latitude and longitude and a radius within which the Sophos container apps can be used.
<b>Time-fencing</b>	Lets you specify a start and end time within which the Sophos container apps can be used. Days of the week on which the apps can be used can be specified as well.
<b>Wi-Fi fencing</b>	<p>Lets you specify Wi-Fi networks to which the device must be connected in order to use the Sophos container apps.</p> <p>The device must actually be connected to one of the listed networks. Being able to see a particular network in the list of available networks is not enough.</p> <p><b>Important:</b> We recommend that you do not rely on Wi-Fi fencing as the only security mechanism because Wi-Fi names can be spoofed very easily.</p>

### 14.13.2 Corporate Email configuration (Android Sophos container policy)

With the **Corporate Email** configuration you define user settings for your Microsoft Exchange Server. These settings are applied to the Sophos Secure Email app if it is installed in the Sophos container.

Setting/Field	Description
<b>Exchange ActiveSync host</b>	The address of the Microsoft Exchange Server. <b>Note:</b> If you use the SMC EAS proxy, enter the URL of the SMC proxy server.
<b>User</b>	The user for this account. If you enter the variable %_USERNAME_%, the server replaces it with the actual user name.
<b>Email address</b>	The email address of the account. If you enter the variable %_EMAILADDRESS_%, the server replaces it with the actual email address.
<b>Domain</b>	The domain for this account.
<b>Support contact email</b>	The email address that will be used as the "Contact Support" email address.
<b>Export contacts to device</b>	Users are allowed to export the exchange contacts with a phone number to the local device contacts. Sophos Secure Email will keep them synchronized. Only name and telephone number will be exported to enable the user to identify company contacts in an incoming call. Note that even after a remote reset of the Sophos Secure Email app, the information will still be available in the local storage of the device.
<b>Show notification settings</b>	This setting controls the display of email notifications and event reminders in Sophos Secure Email. When you select the check box: <ul style="list-style-type: none"> <li>▪ The user can turn email notifications on or off.</li> <li>▪ Event reminders are turned on.</li> </ul> When you clear the check box: <ul style="list-style-type: none"> <li>▪ Email notifications and event reminders are turned off.</li> </ul>

Setting/Field	Description
	<b>Note:</b> If you think notifications displayed on a lost or stolen device is a security risk, you may want to clear this check box.
<b>Open attachments</b>	If you select the check box, <b>Save</b> and <b>View</b> buttons are displayed below the attachment. <b>Save</b> passes the attachment on to Sophos Secure Workspace, <b>View</b> opens the file in Sophos Secure Email. If Sophos Secure Email cannot open the file, users can select where to pass the file on to.  If you clear the check box, attachment cannot be opened or passed on to other apps.
<b>Add</b>	Click <b>Add</b> to configure settings that a future version of the Sophos Secure Email app might require.  <b>Important:</b> Only configure these settings if instructed by the Sophos support team.

### 14.13.3 Corporate Documents configuration (Android Sophos container policy)

With the **Corporate Documents** configuration you define settings for the Corporate Documents feature of the Sophos Secure Workspace app.

#### Configure storage providers

For each storage provider you can define the following settings separately:

Setting/Field	Description
<b>Enable</b>	The storage provider is available in the app.
<b>Offline</b>	Users are allowed to add files from the storage provider to the app's <b>Favorites</b> list for offline use.
<b>Open in (encrypted)</b>	Users can share encrypted files with other apps via <b>Open In</b> .
<b>Open in (unencrypted)</b>	Users can share unencrypted files with other apps via <b>Open In</b> .
<b>Clipboard</b>	Users can copy parts of a document and paste them into other apps.

## Enterprise provider settings

For **WebDAV** provider, also referred to as *enterprise provider*, you can centrally define server settings and login credentials. These cannot be changed by users.

Credential settings that you do not define centrally can be chosen by the users in the app's provider credential screens.

For example you can centrally define the server and user account to be used but you can leave the password field undefined. Users then would have to know the password when accessing the storage provider.

Setting/Field	Description
<b>Name</b>	The name of the provider that is displayed in the Sophos Secure Workspace app.
<b>Server</b>	<p>In this field, enter:</p> <ul style="list-style-type: none"> <li>▪ The URL of the root folder on the <b>Corporate Documents</b> WebDAV server.</li> <li>▪ The URL of the root folder on the <b>WebDAV</b> server.</li> </ul> <p>Use the following format:  <code>https://server.company.com</code>            Only the <code>https</code> protocol is supported.</p>
<b>User name</b>	The user name for the relevant server. You can also use the <code>%_USERNAME_</code> variable.
<b>Password</b>	The password for the relevant account.
<b>Upload folder</b>	The upload folder for the relevant account.

## Other settings

Setting/Field	Description
<b>Enable Documents</b>	This turns on the <b>Documents</b> feature to securely distribute company documents.

Setting/Field	Description
<b>Passphrase complexity</b>	<p>The required minimum complexity of passphrases for encryption keys. More secure passphrases are always allowed.</p> <p>You can select the following settings:</p> <ul style="list-style-type: none"> <li>▪ <b>4 char password</b></li> <li>▪ <b>6 char password</b></li> <li>▪ <b>8 char password</b></li> <li>▪ <b>10 char password</b></li> </ul>

#### 14.13.4 Corporate Browser configuration (Android Sophos container policy)

With the **Corporate Browser** configuration you define settings for the Corporate Browser feature of the Sophos Secure Workspace app.

The Corporate Browser allows you to securely access corporate intranet pages and other allowed pages. You can define domains and bookmarks within a domain.

Every bookmarks belongs to a certain domain. When you use **Add bookmark** to define a bookmark, the domain entry is created automatically if it does not exist.

#### Domain settings

Setting/Field	Description
<b>URL</b>	The domain that you want to allow.
<b>Allow copy/paste</b>	Users can copy and paste text from the Corporate Browser to other apps.
<b>Allow open with</b>	Users can download attachments or pass them on to other apps.
<b>Allow save password</b>	Users can save their passwords in the Corporate Browser.

## Bookmark settings

Setting/Field	Description
<b>Name</b>	The name for the bookmark.
<b>URL</b>	The web address for the bookmark.

### 14.13.5 Client certificate configuration (Android Sophos container policy)

With the **Client certificate** configuration you install a client certificate onto devices. This certificate will be available to the Sophos Secure Email and Sophos Secure Workspace apps if they are installed in the Sophos container.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. 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.

### 14.13.6 Root certificate configuration (Android Sophos container policy)

With the **Root certificate** configuration you upload a root certificate to devices. This certificate will be available to the Sophos Secure Email and Sophos Secure Workspace apps if they are installed in the Sophos container.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. 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.

### 14.13.7 SCEP configuration (Android Sophos container policy)

With the **SCEP** configuration you enable devices to request certificates from a Certificate Authority using the Simple Certificate Enrollment Protocol (SCEP). These certificates are available to the Sophos Secure Workspace app if it is installed in the Sophos container.

**Note:** You must first add a **Root certificate** configuration to upload the CA certificate of the SCEP server before you can add a **SCEP** configuration.



Setting/Field	Description
<b>URL</b>	<p>The web address of the Certificate Authority server.</p> <p>Use the variable <code>_%_SCEPPROXYURL_%</code> to refer to the server URL that is configured on the <b>SCEP</b> tab of the <b>System setup</b> page.</p>
<b>Alias name</b>	<p>The name under which the certificate will appear in selection dialogs.</p> <p>This should be a memorable name to identify the certificate. For example, use the same value as in the <b>Subject</b> field, but without the <b>CN=</b> prefix.</p>
<b>Subject</b>	<p>The name of the entity (for example person or device) that will receive the certificate.</p> <p>You can use placeholders for user data or device properties.</p> <p>The value that you enter (with placeholders replaced by the actual data) must be a valid X.500 name.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>▪ Enter <code>CN=_%_USERNAME_%</code> to specify a user.</li> <li>▪ Enter <code>CN=_%_DEVPROP(serial_number)_%</code> to specify a device.</li> </ul> <p>For information on available placeholders, see <a href="#">Placeholders in profiles and policies</a> (page 75).</p>
<b>Type of Subject Alternative Name</b>	<p>Optionally, configure a Subject Alternative Name (SAN). Select one of the available SAN types.</p>
<b>Value of Subject Alternative Name</b>	<p>If you have selected a SAN type, enter the SAN value.</p>
<b>NT user login name</b>	
<b>Challenge</b>	<p>The web address to obtain a challenge password from the SCEP server.</p> <p>Use the variable <code>_%_CACHALLENGE_%</code> to refer to the challenge URL that is configured on the <b>SCEP</b> tab of the <b>System setup</b> page.</p>
<b>Root certificate</b>	<p>The CA certificate.</p> <p>Select the certificate from the list. The list contains all certificates that you have uploaded in <b>Root certificate</b> configurations of the current profile.</p>

Setting/Field	Description
<b>Key size</b>	The size of the public key in the issued certificate. Make sure that the value matches the size configured on the SCEP server.
<b>Use as digital signature</b>	If you select this check box, the public key can be used as a digital signature.
<b>Use for encryption</b>	If you select this check box, the public key can be used for data encryption.

## 14.14 Configurations for Mobile Security policies

With a Mobile Security policy you configure settings that are related to the Sophos Mobile Security app.

For detailed information on Mobile Security policies, see these sections:

[Configure antivirus settings for Sophos Mobile Security](#) (page 210)

[Configure web filtering settings for Sophos Mobile Security](#) (page 212)

## 14.15 Configurations for Knox container profiles

With a Knox container profile you configure settings that are related to the Knox container of Samsung devices.

For information on how to create a Knox container profile, see [Create profile or policy](#) (page 72).

### 14.15.1 Password policies configuration (Knox container profile)

#### Password type

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

Setting/Field	Description
<b>Any</b>	Users must set a screen lock. They can choose a type <b>Pattern</b> , <b>PIN</b> or <b>Password</b> screen lock. No additional restrictions are imposed.

Setting/Field	Description
<b>Alphabetic</b>	Users must set a <b>Password</b> screen lock. Digits are allowed, but the password must contain at least one letter. You can define a minimum length. See the following table.
<b>PIN</b>	Users must set a <b>PIN</b> or <b>Password</b> screen lock. You can define a minimum length. See the following table.
<b>Alphanumeric</b>	Users must set a <b>Password</b> screen lock. The password must contain both letters and digits. You can define a minimum length. See the following table.
<b>Complex</b>	Users must set a <b>Password</b> screen lock. The password must contain both letters and digits. You can define a minimum length and a minimum number of digits, lowercase and uppercase letters and special characters. See the following two tables.

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

Setting/Field	Description
<b>Minimum password length</b>	The minimum number of characters a password must contain.
<b>Idle time before password prompt</b>	The time (in seconds) after the device will be locked if it has not been used. The device can be unlocked by entering the password.
<b>Maximum password age in days</b>	Requires users to change their password in the specified interval. Value range: 0 (no password change required) to 730 days.
<b>Maximum number of failed attempts until device wipe</b>	The maximum number of failed attempts to enter the correct password before the device is wiped.
<b>Minimum history length</b>	The number of old passwords that are remembered and compared with new ones. When the user defines a new password, it is not accepted if it matches a previously used password. Value range: 1 to 5 or none.

If you select **Complex**, the following additional fields are displayed:

Setting/Field	Description
<b>Minimum number of letters</b>	The minimum number of letters a password must contain.
<b>Minimum number of lowercase letters</b>	The minimum number of lowercase letters a password must contain.
<b>Minimum number of uppercase letters</b>	The minimum number of uppercase letters a password must contain.
<b>Minimum number of non-alphabetic characters</b>	The minimum number of non-alphabetic characters (for example & or !) a password must contain.
<b>Minimum number of numerals</b>	The minimum number of numerals a password must contain.
<b>Minimum number of special characters</b>	The minimum number of special characters (for example !"\$\$%&/()=,.-;:_@<>) a password must contain.

## Biometric authentication

Setting/Field	Description
<b>Allow fingerprint authentication</b>	If supported by the device, the user can use fingerprint authentication to unlock the Knox container.
<b>Allow iris authentication</b>	If supported by the device, the user can use iris authentication to unlock the Knox container.

### 14.15.2 Restrictions configuration (Knox container profile)

Setting/Field	Description
<b>Allow screen capture</b>	Users can capture the screen content of apps inside the Samsung Knox container.
<b>Allow camera</b>	Apps inside the Samsung Knox container can access the camera.

Setting/Field	Description
<b>Allow clipboard</b>	Users can copy any contents to the clipboard.
<b>Allow "Share via"</b>	The <b>Share via</b> feature that certain apps use is turned on.
<b>Allow microphone</b>	Apps inside the Samsung Knox container can access the microphone.
<b>Enforce the use of the secure keypad</b>	Users must use the secure keypad.
<b>Allow addition of new email accounts</b>	Users can add email accounts beyond the accounts that are configured by a Sophos Mobile Control profile.
<b>Allow data export</b>	Private apps can access data from within the Samsung Knox container.
<b>Allow copying files into the container</b>	Private files can be copied or moved into the Samsung Knox container.
<b>Allowed apps / Forbidden apps</b>	<p>You can configure either <b>Allowed apps</b> or <b>Forbidden apps</b>. Select the desired option from the first list and then select the app group containing the apps that should be allowed or forbidden from the second list.</p> <p>App installations initiated by the Sophos Mobile Control server are not restricted by this setting.</p> <p>For information on creating app groups, see <a href="#">App groups</a> (page 190).</p>

### 14.15.3 Exchange ActiveSync configuration (Knox container profile)

Setting/Field	Description
<b>Account name</b>	The account name.
<b>Exchange ActiveSync host</b>	<p>The address of the Microsoft Exchange Server.</p> <p><b>Note:</b> If you use the SMC EAS proxy, enter the URL of the SMC proxy server.</p>
<b>Domain</b>	The domain for this account.

Setting/Field	Description
<b>User</b>	The user for this account. If you enter the variable %_USERNAME_%, the server replaces it with the actual user name.
<b>Email address</b>	The email address of the account. If you enter the variable %_EMAILADDRESS_%, the server replaces it with the actual email address.
<b>Sender</b>	A sender name for this account. If you enter the variable %_EMAILADDRESS_%, the server replaces it with the actual email address.
<b>Password</b>	The password for this account. If you leave this field empty, users must enter the password on their devices.
<b>Synchronization period</b>	The time period emails are synchronized for. If you select a time period, only the emails from within the specified period are synchronized to the inbox on the managed device.
<b>Synchronization interval</b>	The interval between email synchronization processes.
<b>SSL</b>	All communication is sent through SSL (Secure Socket Layer). We recommend that you select this check box.
<b>Default account</b>	The account is used as the default email account.
<b>Allow all certificates</b>	Allow all certificates in transfer processes from the email server.
<b>Allow forwarding emails</b>	Allow forwarding of emails.
<b>Allow use of HTML format</b>	Allow the use of HTML format in emails.
<b>Maximum attachment size in MB</b>	The maximum size of a single email message (1, 3, 5, 10, Unlimited).
<b>Synchronize content types</b>	The content types to be synchronized.

## 14.16 Configurations for Android Things policies

With an Android Things policy you configure various aspects of Android Things devices, like password policies, restrictions or Wi-Fi settings.

For information on how to create an Android Things policy, see [Create profile or policy](#) (page 72).

### 14.16.1 Wi-Fi configuration (Android Things policy)

With the **Wi-Fi** configuration you specify settings for connecting to Wi-Fi networks.

Setting/Field	Description
<b>SSID</b>	The ID of the Wi-Fi network.
<b>Security type</b>	<p>The security type of the Wi-Fi network:</p> <ul style="list-style-type: none"> <li>▪ <b>None</b></li> <li>▪ <b>WEP</b></li> <li>▪ <b>WPA/WPA2</b></li> </ul> <p>If you select <b>WEP</b> or <b>WPA/WPA2</b>, a <b>Password</b> field is displayed. Enter the relevant password.</p>

## 14.17 Configurations for iOS device profiles

With an iOS device profile you configure various aspects of iOS devices, like password policies, restrictions or Wi-Fi settings.

For information on how to create a device profile, see [Create profile or policy](#) (page 72).

### 14.17.1 Password policies configuration (iOS device profile)

With the **Password policies** configuration you define password rules for devices.

Setting/Field	Description
<b>Allow simple value</b>	Users are allowed to use sequential or repeated characters in their password, for example <b>1111</b> or <b>abcde</b> .
<b>Require alphanumeric value</b>	Passwords must contain at least one letter or number.

Setting/Field	Description
<b>Minimum password length</b>	Specifies the minimum number of characters a password must contain.
<b>Minimum number of complex characters</b>	Specifies the minimum number of non-alphanumeric characters (for example & or !) a password must contain.
<b>Maximum password age in days</b>	Requires users to change their password in the specified interval. Value range: 0 (no password change required) to 730 days.
<b>Maximum Auto-Lock (in minutes)</b>	In this field, you can specify the maximum value the user is allowed to configure on the device. Auto-Lock specifies how soon (in minutes) the device will be locked if it has not been used.
<b>Password history</b>	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 is not accepted if it matches a previously used password. Value range: 1 to 50 or 0 (no password history).
<b>Maximum grace period for device lock</b>	In this field, you can specify the maximum value the user is allowed to configure on the device. The grace period for device lock specifies for how long the device can be unlocked after a lock without a password prompt. If you select <b>None</b> , the user can select any of the intervals available. If you select <b>Immediately</b> , users must enter a password every time they unlock their devices.
<b>Maximum number of failed attempts until device wipe</b>	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 <b>6</b> or lower, no delay is imposed and the device is wiped when the attempt limit is exceeded.



## 14.17.2 Restrictions configuration (iOS device profile)

With the **Restrictions** configuration you define restrictions for devices.

### Device

Setting/Field	Description
<b>Allow app installation</b>	If the check box is cleared, the App Store is unavailable and its icon is removed from the Home screen. Users cannot install or update apps from the App Store, iTunes or Apple Configurator.
<b>Allow app installation from device UI</b>	If the check box is cleared, the App Store is unavailable and its icon is removed from the Home screen. Users can still install or update apps from iTunes or Apple Configurator.
<b>Allow use of camera</b>	If the check box is cleared, the camera is unavailable and the Camera icon is removed from the Home screen. Users cannot take pictures, record videos, or use FaceTime.
<b>Allow FaceTime</b>	Users can place or receive FaceTime video calls.
<b>Allow screen capture</b>	Users can take a screenshot of the display.
<b>Allow automatic sync while roaming</b>	If the check box is cleared, devices that are roaming will only sync when the user accesses an account.
<b>Allow Siri</b>	If the check box is cleared, users cannot use Siri, voice commands, or dictation.
<b>Allow Siri while device is locked</b>	If the check box is cleared, users must unlock their devices by entering their password before they use Siri.
<b>Allow Siri querying content from the web</b>	If the check box is cleared, Siri does not query content from the web.
<b>Force Siri explicit language filter</b>	If the check box is cleared, the Siri filter for explicit language is not enforced on the device.
<b>Allow voice dialing while device is locked</b>	If the check box is cleared, users cannot dial by using voice commands when the device is locked by a password. <b>Note:</b> If the user has not configured a device password, voice dialing is always allowed.

Setting/Field	Description
<b>Allow Passbook while device is locked</b>	Passbook notifications are displayed when the device is locked.
<b>Allow in-app purchase</b>	Users can make in-app purchases.
<b>Force user to enter store password for all purchases</b>	Users must enter their Apple ID password to make any purchase.  If the check box is cleared, there is a brief grace period during which users can make subsequent purchases without having to enter their password again.
<b>Allow multiplayer gaming</b>	Users can play multi-player games in Game Center.
<b>Allow Game Center</b>	If the check box is cleared, Game Center is unavailable.
<b>Allow adding Game Center friends</b>	Users can add friends in Game Center.
<b>Allow find my friends modification</b>	If the check box is cleared, modifications to the Find my Friends app are unavailable.
<b>Allow host pairing</b>	If the check box is cleared, host pairing is turned off with the exception of the supervision host. If no supervision host certificate is configured, all pairing is turned off.
<b>Allow pairing with Apple Watch</b>	If the check box is cleared, users cannot pair the device with an Apple Watch. Any currently paired Apple Watch is unpaired.
<b>Allow AirDrop</b>	Content sharing with AirDrop is turned on.
<b>Allow Control Center on lock screen</b>	If the check box is cleared, the Control Center is unavailable when the device screen is locked.
<b>Allow Notification Center on lock screen</b>	If the check box is cleared, the Notification Center is unavailable when the device screen is locked.
<b>Allow Today view on lock screen</b>	If the check box is cleared, the Today view is unavailable when the device screen is locked.
<b>Allow News</b>	The News app is available.
<b>Allow over-the-air PKI updates</b>	Over-the-air PKI updates are possible.
<b>Allow iBooks Store</b>	Users can purchase books in iBooks.

Setting/Field	Description
<b>Allow explicit sexual content in iBooks Store</b>	If the check box is cleared, explicit sexual content through iBooks Store is blocked.
<b>Allow user to install configuration profiles</b>	Users can install configuration profiles.
<b>Allow iMessage</b>	Users can use iMessage to send or receive text messages.
<b>Allow app removal</b>	Users can remove apps from the device.
<b>Allow erase all contents and settings</b>	If the check box is cleared, the <b>Erase all Content And Settings</b> option in the Reset UI is unavailable.
<b>Allow internet search result for Spotlight</b>	If the check box is cleared, Spotlight does not return internet search results.
<b>Allow enabling of restrictions option</b>	If the check box is cleared, the <b>Enable Restrictions</b> option in the Reset UI is unavailable.
<b>Allow Handoff</b>	Users can use the Apple Continuity feature Handoff. With Handoff, users can start to work on a document, email or message on one device and continue from another device.
<b>Allow device name modification</b>	Users can change the device name.
<b>Allow wallpaper modification</b>	Users can change the wallpaper.
<b>Allow keyboard shortcuts</b>	Users can use keyboard shortcuts.
<b>Allow automatic app download</b>	If the check box is cleared, the automatic downloading of apps purchased on other devices is turned off. This does not affect updates to existing apps.
<b>Allow Apple Music</b>	Users can access the Apple Music library.
<b>Allow Apple Music Radio</b>	Users can access Apple Music Radio.
<b>Allow modification of Bluetooth settings</b>	Users can modify the Bluetooth settings.

## Company data

Setting/Field	Description
<b>Allow documents to be shared only within managed apps/accounts</b>	<p>With this setting you define a restriction on opening documents with apps or accounts (for example a company email account) managed by Sophos Mobile Control.</p> <p>If 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. In this way you can prevent corporate documents from being opened in unmanaged apps.</p>
<b>Allow documents to be shared only within unmanaged apps/accounts</b>	<p>With this setting you define a restriction on opening documents with apps/accounts (for example a private email account) not managed by Sophos Mobile Control.</p> <p>If 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. In this way you can prevent personal documents from being opened in managed apps.</p>
<b>Force AirDrop documents to be used as unmanaged documents</b>	AirDrop is considered an unmanaged drop target.
<b>Allow managed apps to sync with iCloud</b>	Managed apps can use iCloud synchronization.
<b>Allow backup for enterprise books</b>	Enterprise books are backed up.
<b>Allow enterprise books notes and highlights sync</b>	Enterprise books notes and highlights are synchronized.

## Applications

Setting/Field	Description
<b>Allow use of the iTunes Store</b>	If the check box is cleared, the iTunes Store is unavailable and its icon is removed from the Home screen. Users cannot preview, purchase or download content.

Setting/Field	Description
<b>Allow use of Safari</b>	If the check box is cleared, the Safari web browser is unavailable and its icon is removed from the Home screen. This also prevents users from opening web clips.
<b>Enable auto-fill</b>	If the check box is cleared, Safari does not auto-fill web forms with previously entered information.
<b>Block pop-ups</b>	The Safari pop-up blocker is turned on.
<b>Allow JavaScript in browser</b>	Web pages can execute JavaScript code on the device.
<b>Accept cookies</b>	In this field, you specify if cookies will be accepted: <ul style="list-style-type: none"> <li>▪ Always</li> <li>▪ Never</li> <li>▪ From visited sites</li> </ul>
<b>Allow modification of cellular data usage per app</b>	Users can change the cellular data usage per app.
<b>Allowed apps / Forbidden apps</b>	You can specify either <b>Allowed apps</b> or <b>Forbidden apps</b> . Select the desired option from the first list and then select the app group containing the apps that should be allowed or forbidden from the second list. For information on creating app groups, see <a href="#">App groups</a> (page 190).

## iCloud

Setting/Field	Description
<b>Allow backup</b>	Users can back up their devices to iCloud.
<b>Allow document sync</b>	Users can store documents in iCloud.
<b>Allow Photo Stream</b>	If the check box is cleared, users cannot turn on Photo Stream.  <b>Note:</b> If you install a configuration profile that restricts the use of Photo Stream, Photo Stream photos are removed from the device. Photos are not sent from the Camera Roll

Setting/Field	Description
	to Photo Stream. If there are no further copies of these photos, they are lost.
<b>Allow iCloud Photo Library</b>	Users can use the iCloud Photo Library.
<b>Allow shared photo streams</b>	Users can invite others to view their photo streams and can view photo streams shared by others.
<b>Allow keychain sync</b>	The Keychain feature of iCloud for synchronizing passwords across different iOS and OS X devices is available.

## Security and privacy

Setting/Field	Description
<b>Allow diagnostic data to be sent to Apple</b>	If the check box is cleared, iOS diagnostic information is not sent to Apple.
<b>Allow user to accept untrusted TLS certificates</b>	If the check box is cleared, 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.
<b>Trust enterprise apps</b>	Enterprise apps are trusted.
<b>Allow password modification</b>	Users can add, change or remove the device password.
<b>Allow account modification</b>	If the check box is cleared, users cannot modify accounts. The <b>Accounts</b> menu is unavailable.
<b>Allow Touch ID to unlock device</b>	If the check box is cleared, the device cannot be unlocked by Touch ID.
<b>Force limit ad-tracking</b>	Anonymous user data apps used for targeting ads are no longer provided.
<b>Force encrypted backups</b>	Users must encrypt backups in iTunes.

## Content ratings

Setting/Field	Description
<b>Allow explicit music and podcasts</b>	If the check box is cleared, 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.

### 14.17.3 Roaming/Hotspot settings configuration (iOS device profile)

With the **Roaming/Hotspot settings** configuration you define settings for roaming and personal hotspots.

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

Setting/Field	Description
<b>Enable voice roaming</b>	Voice roaming is available.
<b>Enable data roaming</b>	Data roaming is available.
<b>Enable personal hotspot</b>	The user can configure the device to serve as a personal hotspot.

### 14.17.4 Exchange ActiveSync configuration (iOS device profile)

With the **Exchange ActiveSync** configuration you define user settings for your Microsoft Exchange Server.

Setting/Field	Description
<b>Account name</b>	The account name.
<b>Exchange ActiveSync host</b>	The address of the Microsoft Exchange Server. <b>Note:</b> If you use the SMC EAS proxy, enter the URL of the SMC proxy server.
<b>Domain</b>	The domain for this account.

Setting/Field	Description
<b>User</b>	<p>The user for this account.</p> <p>If you enter the variable % <b>USERNAME</b> %, the server replaces it with the actual user name.</p>
<b>Email address</b>	<p>The email address of the account.</p> <p>If you enter the variable % <b>EMAILADDRESS</b> %, the server replaces it with the actual email address.</p>
<b>Password</b>	<p>The password for this account.</p> <p>If you leave this field empty, users must enter the password on their devices.</p>
<b>Synchronization period</b>	<p>The time period emails are synchronized for.</p> <p>If you select a time period, only the emails from within the specified period are synchronized to the inbox on the managed device.</p>
<b>SSL</b>	<p>All communication is sent through SSL (Secure Socket Layer).</p> <p>We recommend that you select this check box.</p>
<b>Allow move</b>	<p>The user can move emails from this account to another. This also allows users to use a different account when replying to or forwarding a message from this account.</p>
<b>Allow recent address syncing</b>	<p>The account is included in the syncing of recently used addresses with other devices using iCloud.</p>
<b>Use in Mail only</b>	<p>The account can only be used to send messages from the Mail app. It cannot be selected as a sending account for messages created with other apps, for example Photos or Safari.</p>
<b>Identity certificate</b>	<p>Select the identity certificate for the connection to ActiveSync.</p> <p>The list includes all certificates from <b>Client certificate</b> configurations of the current profile.</p>



### 14.17.5 Wi-Fi configuration (iOS device profile)

With the **Wi-Fi** configuration you specify settings for connecting to Wi-Fi networks.

Setting/Field	Description
<b>SSID</b>	The ID of the Wi-Fi network.
<b>Connect automatically</b>	Automatically connect to the target network.
<b>Hidden network</b>	The target network is not open or visible.
<b>Security type</b>	<p>The security type of the Wi-Fi network:</p> <ul style="list-style-type: none"> <li>▪ <b>None</b></li> <li>▪ <b>WEP</b></li> <li>▪ <b>WPA/WPA2</b></li> <li>▪ <b>Any (personal)</b></li> <li>▪ <b>Corporate WEP</b></li> <li>▪ <b>Corporate WPA/WPA2</b></li> <li>▪ <b>Any (company)</b></li> </ul> <p>If you select <b>WEP</b>, <b>WPA/WPA2</b> or <b>Any (personal)</b>, a <b>Password</b> field is displayed. Enter the relevant password.</p> <p>If you select <b>Corporate WEP</b>, <b>Corporate WPA/WPA2</b> or <b>Any (company)</b>, the tabs <b>Protocols</b>, <b>Authentication</b> and <b>Trust</b> are displayed.</p> <p>In the <b>Protocols</b> tab configure the following:</p> <ul style="list-style-type: none"> <li>▪ Under <b>Accepted EAP types</b>, specify the EAP methods to be used for authentication. Depending on the types selected here, the values in the <b>Internal identity</b> field in this tab become available for selection.</li> <li>▪ Under <b>EAP-FAST</b>, configure the EAP-FAST Protected Access credential settings.</li> </ul> <p>In the <b>Authentication</b> tab, configure client authentication settings:</p> <ul style="list-style-type: none"> <li>▪ In the <b>User</b> field, enter the user name for the connection to the Wi-Fi network.</li> <li>▪ Select <b>Require password on each connect</b>, if the password is to be queried for each connection and transferred with the authentication.</li> <li>▪ In the <b>Password</b> field, enter the relevant password.</li> <li>▪ In the <b>Identity certificate</b> list, select the certificate for the connection to the Wi-Fi network.</li> </ul>

Setting/Field	Description
	<p><b>Note:</b> The certificate to be used has to be specified in a <b>Client certificate</b> configuration.</p> <ul style="list-style-type: none"> <li>In the <b>External identity</b> field, enter the externally visible ID (for TTLS, PEAP and EAP-FAST).</li> </ul> <p>In the <b>Trust</b> tab, configure server authentication settings: Select the trusted certificates from the list.</p> <p><b>Note:</b> You must specify the certificates in a <b>Root certificate</b> configuration.</p>
<b>Proxy</b>	<p>In this list, select the proxy settings for the Wi-Fi connection:</p> <ul style="list-style-type: none"> <li><b>None</b></li> <li><b>Manually</b></li> <li><b>Automatic</b></li> </ul> <p>If you select <b>Manually</b>, the fields <b>Server and port</b>, <b>Authentication</b> and <b>Password</b> are displayed. Enter the required proxy information. If you select <b>Automatic</b>, the field <b>Proxy server URL</b> is displayed. Enter the URL of the proxy server.</p>

### 14.17.6 VPN configuration (iOS device profile)

With the **VPN** configuration you define VPN settings for network connections.

Setting/Field	Description
<b>Connection name</b>	The name of the connection shown on the device.
<b>Connection type</b>	<p>The type of the VPN connection:</p> <ul style="list-style-type: none"> <li><b>Cisco AnyConnect</b></li> <li><b>IPSec (Cisco)</b></li> <li><b>F5</b></li> <li><b>Check Point</b></li> <li><b>Custom SSL</b></li> </ul> <p>Different entry fields are shown on the <b>VPN</b> page depending on the connection type you select here.</p>

Setting/Field	Description
<b>Identifier (reverse DNS format)</b> (connection type <b>Custom SSL</b> )	The custom identifier in reverse DNS format.
<b>Server</b> (all connection types)	The host name or the IP address of the server.
<b>Account</b> (all connection types)	The user account for the authentication of the connection.
<b>Custom data</b> (connection type <b>Custom SSL</b> )	If your vendor has specified custom connection properties, you can enter them in this field. To enter a property, click <b>Add</b> and then enter <b>Key</b> and <b>Value</b> of the property in the dialog box.
<b>Send all traffic through VPN</b>	All traffic is sent through VPN.
<b>Group</b> (connection type <b>Cisco AnyConnect</b> )	The group that may be required for the authentication of the connection.
<b>User authentication</b> (connection types <b>Cisco AnyConnect, F5, Custom SSL</b> )	Select the type of user authentication for the connection: <ul style="list-style-type: none"> <li>▪ If you select <b>Password</b>, a <b>Password</b> field is shown below the <b>User Authentication</b> field. Enter the password for authentication.</li> <li>▪ If you select <b>Certificate</b>, a <b>Certificate</b> field is shown below the <b>User authentication</b> field. Select a certificate.</li> </ul>
<b>Device authentication</b> (connection type <b>IPSec (Cisco)</b> )	The type of device authentication: <ul style="list-style-type: none"> <li>▪ <b>Keys (Shared Secret)/Group name</b> If you select this option, the fields <b>Group name</b>, <b>Keys (Shared Secret)</b>, <b>Use hybrid authentication</b> and <b>Request password</b> are displayed below the <b>Device authentication</b> field. Enter the required authentication information in the <b>Group name</b> and <b>Keys (Shared Secret)</b> fields. Select <b>Use hybrid authentication</b> and <b>Request password</b> as required.</li> <li>▪ <b>Certificate</b> If you select this option, the fields <b>Certificate</b> and <b>Including user PIN</b> are displayed below the <b>Device authentication</b> field. In the <b>Certificate</b> list, select the required certificate. Select <b>Including user PIN</b> to include the user PIN in device authentication.</li> </ul>

Setting/Field	Description
<b>Proxy</b> (all connection types)	<p>The proxy settings for the connection:</p> <ul style="list-style-type: none"> <li>▪ <b>None</b></li> <li>▪ <b>Manually</b> <p>If you select this option, the fields <b>Server and port</b>, <b>Authentication</b> and <b>Password</b> are displayed. In the <b>Server and port</b> field, enter the valid address and the port of the proxy server. In the <b>Authentication</b> field, enter the user name for the connection to the proxy server. In the <b>Password</b> field, enter the password for the connection to the proxy server.</p> </li> <li>▪ <b>Automatic</b> <p>If you select this option, the <b>Proxy server URL</b> field is displayed. Enter the URL of the server with the proxy setting in this field.</p> </li> </ul>

### 14.17.7 Per app VPN configuration (iOS device profile)

With the **Per app VPN** configuration you define VPN settings to support the iOS feature **Per app VPN**.

You can configure apps to automatically connect to VPN when they are started. 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 on the **Edit package** page of an application. See [Configure per app VPN and settings for iOS apps](#) (page 189).

Setting/Field	Description
<b>Connection name</b>	The name of the connection shown on the device.
<b>Connection type</b>	<p>The type of the VPN connection:</p> <ul style="list-style-type: none"> <li>▪ <b>Cisco AnyConnect</b></li> <li>▪ <b>F5</b></li> <li>▪ <b>Check Point</b></li> <li>▪ <b>Custom SSL</b></li> </ul> <p>Different entry fields are shown on the <b>VPN</b> page depending on the connection type you select here.</p>

Setting/Field	Description
<b>Identifier (reverse DNS format)</b> (connection type <b>Custom SSL</b> )	The custom identifier in reverse DNS format.
<b>Server</b> (all connection types)	The host name or the IP address of the server.
<b>Account</b> (all connection types)	The user account for the authentication of the connection.
<b>Custom data</b> (connection type <b>Custom SSL</b> )	<p>If your vendor has specified custom connection properties, you can enter them in this field.</p> <p>To enter a property, click <b>Add</b> and then enter <b>Key</b> and <b>Value</b> of the property in the dialog box.</p>
<b>Group</b> (connection type <b>Cisco AnyConnect</b> )	In this field, enter the group that may be required for the authentication of the connection.
<b>Send all traffic through VPN</b>	All traffic is sent through VPN.
<b>User authentication</b> (connection type <b>Cisco AnyConnect, F5, Custom SSL</b> )	<p>In this list, select the type of user authentication for the connection:</p> <ul style="list-style-type: none"> <li>▪ <b>Password</b> If you select this option, the <b>Password</b> field is shown below the <b>User Authentication</b> field. Enter the password for authentication.</li> <li>▪ <b>Certificate</b> If you select this option, the <b>Certificate</b> field is shown below the <b>User Authentication</b> field. Select a certificate.</li> </ul>
<b>Device authentication</b> (connection type <b>IPSec (Cisco)</b> )	<p>In this list, select the type of device authentication:</p> <ul style="list-style-type: none"> <li>▪ <b>Keys (Shared Secret)/Group name</b> If you select this option, the fields <b>Group name</b>, <b>Keys (Shared Secret)</b>, <b>Use hybrid authentication</b> and <b>Request password</b> are displayed below the <b>Device authentication</b> field. Enter the required authentication information in the <b>Group name</b> and <b>Keys (Shared Secret)</b> fields. Select <b>Use hybrid authentication</b> and <b>Request password</b> as required.</li> <li>▪ <b>Certificate</b> If you select this option, the fields <b>Certificate</b> and <b>Including user PIN</b> are displayed below the <b>Device authentication</b> field. In the <b>Certificate</b></li> </ul>

Setting/Field	Description
	<p>list, select the required certificate. Select <b>Including user PIN</b> to include the user PIN in device authentication.</p>
<p><b>Proxy</b> (all connection types)</p>	<p>In this list, select the proxy settings for the connection:</p> <ul style="list-style-type: none"> <li>▪ <b>None</b></li> <li>▪ <b>Manually</b> <p>If you select this option, the fields <b>Server and port</b>, <b>Authentication</b> and <b>Password</b> are displayed. In the <b>Server and port</b> field, enter the valid address and the port of the proxy server. In the <b>Authentication</b> field, enter the user name for the connection to the proxy server. In the <b>Password</b> field, enter the password for the connection to the proxy server.</p> </li> <li>▪ <b>Automatic</b> <p>If you select this option, the <b>Proxy server URL</b> field is displayed. Enter the URL of the server with the proxy setting in this field.</p> </li> </ul>
<p><b>Safari domains</b></p>	<p>In this field, you can enter a list of domain strings.</p> <p>When a domain that matches one of the domain strings is opened in Safari or another browser app, the VPN connection is triggered.</p> <p>Use a new line for each domain string.</p> <p>The rule matching behavior is as follows:</p> <ul style="list-style-type: none"> <li>▪ Leading and trailing dots are ignored. For example, the string <code>.example.com</code> matches the same domains as the string <code>example.com</code>.</li> <li>▪ Each string component must match a whole domain component. For example, the string <code>example.com</code> matches the domain <code>www.example.com</code>, but not <code>www.myexample.com</code>.</li> <li>▪ Strings with a single component only match that specific domain. For example, the string <code>example</code> matches the domain <code>example</code>, but not <code>www.example.com</code>.</li> </ul>

### 14.17.8 Single sign-on configuration (iOS device profile)

With the **Single sign-on** configuration you define settings for a single sign-on for third-party apps.

Setting/Field	Description
<b>Name</b>	A human-readable name for the account.
<b>Kerberos principal name</b>	The Kerberos principal name. If you do not enter a value, the user must enter the name during profile installation.
<b>Realm</b>	The Kerberos realm name. You must enter the name in upper-case letters.

### 14.17.9 Single app mode configuration (iOS device profile)

With the **Single app mode** configuration you define settings for the single mode that locks devices into a single app and prevents users from changing to other apps.

Setting/Field	Description
<b>Select source</b>	Select how you want to specify the app for the single app mode: <ul style="list-style-type: none"> <li>▪ <b>App list:</b> Select the app from a list of all available iOS apps for the customer.</li> <li>▪ <b>Custom:</b> Manually enter the bundle ID of the app.</li> </ul>
<b>App identifier</b>	The app for the single app mode. Either select an app from the list or enter a bundle ID.
<b>Disable touchscreen</b>	Touch gestures are unavailable.
<b>Disable rotation</b>	The screen does not rotate.
<b>Disable volume buttons</b>	Volume buttons are unavailable.
<b>Disable ringer switch</b>	The ringer switch is unavailable.
<b>Disable sleep wake button</b>	The wake button is unavailable.

Setting/Field	Description
<b>Disable Auto-Lock</b>	The Auto-Lock feature that puts the device into sleep after an idle period is turned off.
<b>Enable VoiceOver</b>	VoiceOver is available.
<b>Enable Zoom</b>	The Zoom feature is available.
<b>Enable Invert Colors</b>	The Invert Colors feature is available.
<b>Enable AssistiveTouch</b>	AssistiveTouch is available.
<b>Enable Speak Selection</b>	The Speak Selection feature is available.
<b>Enable Mono Audio</b>	The Mono Audio feature is available.
<b>VoiceOver</b>	VoiceOver adjustments are available.
<b>Zoom</b>	Zoom adjustment are available.
<b>Invert Colors</b>	Invert Colors adjustment are available.
<b>AssistiveTouch</b>	AssistiveTouch adjustment are available.

#### 14.17.10 Web clip configuration (iOS device profile)

With the **Web clip** configuration you 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.

Setting/Field	Description
<b>Description</b>	A description for the web clip.
<b>URL</b>	The web address of the web clip.
<b>Can be removed</b>	If the check box is cleared, the user cannot remove the web clip. It cannot be deleted from the device unless the user removes the profile that installed it.
<b>Full screen</b>	The web clip is opened full screen on the device. A full screen web clip opens the URL as a web app.



### 14.17.11 Access Point Name configuration (iOS device profile)

With the **Access Point Name** configuration you specify an Access Point Name (APN) configuration for iOS devices. APN configurations define how devices connect to a mobile network.

**Note:** The **Access Point Name** configuration is deprecated in favor of the **Cellular** configuration. See [Cellular configuration \(iOS device profile\)](#) (page 140)

**Important:** 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.

Setting/Field	Description
<b>APN</b>	The APN that the device quotes when it opens a GPRS connection with the carrier.  This must match an APN that the carrier accepts. Otherwise, the connection cannot be established.
<b>User name for access point</b>	The user name for the access point.  <b>Note:</b> iOS supports APN user names of up to 64 characters.
<b>Password for access point</b>	The password for the access point.  <b>Note:</b> iOS supports APN passwords of up to 64 characters.
<b>Proxy server and port</b>	The address and the port of the proxy server.

### 14.17.12 Web content filter configuration (iOS device profile)

With the **Web content filter** configuration you define forbidden URLs and allowed URLs with bookmarks.

Setting/Field	Description
<b>Forbidden URLs</b>	If you select the check box, you can define a list of blocked URLs that may not be accessed on the devices.  Click <b>Next</b> to display the <b>Select web content filter type</b> page. On this page, you can add individual URLs.  Use a new line for each URL.

Setting/Field	Description
<b>Allowed URLs with bookmarks</b>	<p>If you select the check box, you can define allowed URLs with bookmarks to be added to the Safari browser on the devices. All other sites are blocked.</p> <p>Click <b>Next</b> to display the <b>Web content filter</b> page. Click <b>Add</b> to add individual URLs as bookmarks.</p>

### 14.17.13 Global HTTP proxy configuration (iOS device profile)

With the **Global HTTP proxy** configuration you define a corporate proxy server.

Setting/Field	Description
<b>Global HTTP proxy</b>	<p>Select the proxy settings for the connection:</p> <ul style="list-style-type: none"> <li>▪ <b>Manually</b> <p>If you select this option, the fields <b>Server and port</b>, <b>Authentication</b> and <b>Password</b> are displayed. In the <b>Server and port</b> field, enter the valid address and the port of the proxy server. In the <b>Authentication</b> field, enter the user name for the connection to the proxy server. In the <b>Password</b> field, enter the password for the connection to the proxy server.</p> </li> <li>▪ <b>Automatic</b> <p>If you select this option, the <b>Proxy server URL</b> field is displayed. Enter the URL of the server with the proxy setting in this field.</p> </li> </ul>

### 14.17.14 Root certificate configuration (iOS device profile)

With the **Root certificate** configuration you install a root certificate onto devices.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. 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.

### 14.17.15 Client Certificate configuration (iOS device profile)

With the **Client certificate** configuration you install a client certificate onto iOS devices.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. 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.

### 14.17.16 SCEP configuration (iOS device profile)

With the **SCEP** configuration you enable devices to request certificates from a Certificate Authority using the Simple Certificate Enrollment Protocol (SCEP).

Setting/Field	Description
<b>URL</b>	The web address of the Certificate Authority server. Use the variable <code>_%_SCEPPROXYURL_%</code> to refer to the server URL that is configured on the <b>SCEP</b> tab of the <b>System setup</b> page.
<b>CA name</b>	A name that is understood by the Certificate Authority. The name can, for example, be used to distinguish between instances.
<b>Subject</b>	The name of the entity (for example person or device) that will receive the certificate. You can use placeholders for user data or device properties. The value that you enter (with placeholders replaced by the actual data) must be a valid X.500 name. For example: <ul style="list-style-type: none"> <li>▪ Enter <code>CN=_%_USERNAME_%</code> to specify a user.</li> <li>▪ Enter <code>CN=_%_DEVPROP(serial_number)_%</code> to specify a device.</li> </ul> For information on available placeholders, see <a href="#">Placeholders in profiles and policies</a> (page 75).
<b>Type of Subject Alternative Name</b>	Optionally, configure a Subject Alternative Name (SAN). Select one of the available SAN types.
<b>Value of Subject Alternative Name</b>	If you have selected a SAN type, enter the SAN value.
<b>NT user login name</b>	

Setting/Field	Description
<b>Challenge</b>	The web address to obtain a challenge password from the SCEP server.  Use the variable %_CACHALLENGE_% to refer to the challenge URL that is configured on the <b>SCEP</b> tab of the <b>System setup</b> page.
<b>Retries</b>	The number of retries if the server sends a response of type <i>pending</i> .
<b>Retry delay</b>	The number of seconds between retries.
<b>Key size</b>	The size of the public key in the issued certificate.  Make sure that the value matches the size configured on the SCEP server.
<b>Use as digital signature</b>	If you select this check box, the public key can be used as a digital signature.
<b>Use for encryption</b>	If you select this check box, the public key can be used for data encryption.

### 14.17.17 Managed domains configuration (iOS device profile)

With the **Managed domains** configuration you define managed domains for iOS devices.

When domains are managed, files downloaded from specific websites in Safari can only be opened using apps that were pushed to the device using MDM.

You can enter managed Email domains and Web domains. Enter one domain per line.

**Note:** If a managed web domain entry contains a port number, only addresses that specify that port number will be considered managed. Otherwise, only the standard ports will be considered managed (port 80 for http and 443 for https).

### 14.17.18 Cellular configuration (iOS device profile)

With the **Cellular** configuration you define cellular network settings for iOS devices.

**Note:** A cellular configuration cannot be installed onto a device if an APN configuration is already installed.

Setting/Field	Description
<b>Authentication</b>	<b>PAP</b> <b>CHAP</b>
<b>APN</b>	The APN that the device quotes when it opens a GPRS connection with the carrier. This must match an APN that the carrier accepts. Otherwise, the connection cannot be established.
<b>User name for access point</b>	The user name for the access point. <b>Note:</b> iOS supports APN user names of up to 64 characters.
<b>Password for access point</b>	The password for the access point. <b>Note:</b> iOS supports APN passwords of up to 64 characters.
<b>Proxy server and port</b>	The address and the port of the proxy server.

### 14.17.19 CalDAV configuration (iOS device profile)

With the **CalDAV** configuration you configure the synchronization of calendar data with a CalDAV server. For example, this can be used to sync Google Calendar with an iOS device.

Setting/Field	Description
<b>Account name</b>	The display name of the CalDAV account on the device.
<b>Account host and port</b>	The host name or IP address and optionally the port number of the CalDAV server. For example, for Google Calendar enter: <code>calendar.google.com:443</code>
<b>Principal URL</b>	If required by the CalDAV server, enter the principal URL of the calendar resource. For example, to sync with a calendar other than the primary calendar in a Google account, enter: <code>https://apidata.googleusercontent.com/calDav/v2/calendar_id/user</code>

Setting/Field	Description
	where <i>calendar_id</i> is the ID of the calendar you want to sync with. In the Google Calendar web application, the calendar ID is displayed in the calendar settings. See the Google Calendar help for details.
<b>User name, Password</b>	The login credentials for the CalDAV account. For example, for Google Calendar enter the credentials of the Google account.

### 14.17.20 CardDAV configuration (iOS device profile)

With the **CardDAV** configuration you configure the synchronization of contact data with a CardDAV server. For example, this can be used to sync Google Contacts with an iOS device.

Setting/Field	Description
<b>Account name</b>	The display name of the CardDAV account on the device.
<b>Account host and port</b>	The host name or IP address and optionally the port number of the CardDAV server. For example, for Google Contacts enter: <code>google.com</code>
<b>Principal URL</b>	If required by the CardDAV server, enter the principal URL of the contacts resource. For example, the Google CardDAV API supports the following principal URL: <code>https://www.googleapis.com/calddav/v1/principals/account_name@gmail.com</code> where <i>account_name</i> is the Google account name.
<b>User name, Password</b>	The login credentials for the CardDAV account. For example, for Google Contacts enter the credentials of the Google account.

### 14.17.21 IMAP/POP configuration (iOS device profile)

With the **IMAP/POP** configuration you add an IMAP or POP email account to the iOS device.

Setting/Field	Description
<b>Account name</b>	The display name of the email account on the device.
<b>Account type</b>	The type of the email server for incoming email. Can be either <b>IMAP</b> or <b>POP</b> .
<b>User display name</b>	The display name of the user for outgoing email. You can use the variable <b>%_USERNAME_%</b> and the server will replace it with the actual user name.
<b>Email address</b>	The email address of the account. You can use the variable <b>%_EMAILADDRESS_%</b> and the server will replace it with the actual email address.
<b>Allow move</b>	The user can move emails from this account to another. This also allows users to use a different account when replying to or forwarding a message from this account.
<b>Allow recent address syncing</b>	The account is included in the syncing for the list of recent addresses.
<b>Use in Mail only</b>	The account can only be used to send messages from the Mail app. It cannot be selected as a sending account for messages created with other apps, for example Photos or Safari.
<b>Allow Mail Drop</b>	Allow Apple Mail Drop for this account.
<b>Enable S/MIME</b>	Support the S/MIME encryption standard.
<b>Signing certificate</b> <b>Encryption certificate</b>	The certificates that are used for email signing and encryption. To select a certificate, you must first upload it in a <b>Client certificate</b> configuration of the current profile.
<b>Allow user to send unencrypted emails</b>	For each outgoing email, the user can choose to encrypt it or not.
<b>Incoming email</b>	
<b>Email server and port</b>	The host name or IP address and the port number of the server for incoming email (inbound server).

Setting/Field	Description
<b>User name</b>	The user name for connecting to the inbound server.
<b>Authentication type</b>	The authentication method for connecting to the inbound server.
<b>Password</b>	The password for connecting to the inbound server (if required).
<b>SSL</b>	Use Secure Sockets Layer for incoming email transfer.
<b>Outgoing email</b>	
<b>Email server and port</b>	The host name or IP address and the port number of the server for outgoing email (outbound server).
<b>User name</b>	The user name for connecting to the outbound server.
<b>Authentication type</b>	The authentication method for connecting to the outbound server.
<b>Password</b>	The password for connecting to the outbound server (if required).
<b>Use same password as for incoming email</b>	Use the password that is specified for incoming email.
<b>SSL</b>	Use Secure Sockets Layer for outgoing email transfer.

### 14.17.22 Network usage rules configuration (iOS device profile)

With the **Network usage rules** configuration you specify how managed apps are allowed to use cellular data networks.

#### General rules

Under **Rules for all managed apps**, specify the settings for managed apps in general.

Setting/Field	Description
<b>Allow cellular data</b>	Managed apps are allowed to use data communication over cellular networks.
<b>Allow data roaming</b>	Managed apps are allowed to use data communication while the device is roaming on a foreign cellular network.



## Exceptions

Exceptions override the general rules. Use **Add exception** to define rules that are specific to an app group.

Setting/Field	Description
<b>App group</b>	Select an app group that contains the managed apps to which the exception applies.
<b>Allow cellular data</b>	Managed apps from the selected app group are allowed to use data communication over cellular networks.
<b>Allow data roaming</b>	Managed apps from the selected app group are allowed to use data communication while the device is roaming on a foreign cellular network.

**Note:** You cannot define multiple exceptions for the same app group.

## 14.18 Configurations for Sophos container policies for iOS

With a Sophos container policy you configure settings that are related to the Sophos container apps Sophos Secure Email and Sophos Secure Workspace.

For information on how to create a Sophos container policy, see [Create profile or policy](#) (page 72).

### 14.18.1 General configuration (iOS Sophos container policy)

With the **General** configuration you define settings that apply to all Sophos container apps, if applicable.

Setting/Field	Description
<b>Enable Sophos container password</b>	Users must enter an additional password to be able to start a Sophos container app. The password has to be defined when the first container app is started after the configuration has been applied. This password applies to all container apps.
<b>Password complexity</b>	The required minimum complexity of the Sophos container password. More secure passwords are always allowed. Passwords (a mix of numeric and

Setting/Field	Description
	<p>alphanumeric characters) are always seen as more secure than PINs (numeric characters only).</p> <ul style="list-style-type: none"> <li>▪ <b>Any</b>: Sophos container passwords do not have restrictions.</li> <li>▪ <b>4 digit PIN</b></li> <li>▪ <b>6 digit PIN</b></li> <li>▪ <b>4 char password</b></li> <li>▪ <b>6 char password</b></li> <li>▪ <b>8 char password</b></li> <li>▪ <b>10 char password</b></li> </ul>
<b>Password age in days</b>	The number of days that a password can be used before users are prompted to change it.
<b>Failed logins until lock</b>	The number of failed login attempts that are tolerated before the container apps are locked. Once they are locked an administrator needs to unlock the apps or, if allowed, users can use the Self Service Portal to do so.
<b>Allow fingerprint</b>	Users can use their fingerprint to unlock the app.
<b>Grace period in minutes</b>	<p>The period of time within which no Sophos container password must be entered when a container app comes to the foreground again.</p> <p>The grace period applies to all container apps. You can switch between the apps during the grace period without entering a password.</p> <p>You can select <b>1, 2, 5, 10, 15</b> minutes.</p>
<b>Lock on device lock</b>	<p>When the device is locked, the Sophos container is locked as well.</p> <p>If the check box is cleared, the container is locked only after the grace period has expired.</p>
<b>Last server connect</b>	<p>The period of time within users can use a Sophos container app without a connection to the Sophos Mobile Control server.</p> <p>When a Sophos container app becomes active and does not have contact with the server within the defined period of time, a lock screen will be displayed. Users can only unlock the app by tapping <b>Retry</b> on the lock screen. The app will then try to connect to the server. If the connection can be</p>

Setting/Field	Description
	<p>established, the app will be unlocked. If not, access will be denied.</p> <ul style="list-style-type: none"> <li>▪ <b>On access:</b> Server connection is always required and the app is locked when the server cannot be reached.</li> <li>▪ <b>1 hour:</b> Server connection is required when the app becomes active one hour or more after the last successful server connection.</li> <li>▪ <b>3 hours</b></li> <li>▪ <b>6 hours</b></li> <li>▪ <b>12 hours</b></li> <li>▪ <b>1 day</b></li> <li>▪ <b>3 days</b></li> <li>▪ <b>1 week</b></li> <li>▪ <b>none:</b> No regular contact is required.</li> </ul>
<p><b>Offline starts without server connection</b></p>	<p>In this field you define how often users can start one of the Sophos container apps without a server connection.</p> <p><b>Note:</b> This setting requires the Sophos container password feature to be turned on.</p> <p>A counter is incremented whenever users enter the Sophos container password. If the counter exceeds the defined number, the same lock screen as for the <b>Last server connect</b> setting will be displayed. The counter will be reset if a connection to the Sophos Mobile Control server is established.</p> <ul style="list-style-type: none"> <li>▪ <b>Unlimited:</b> No server connection is required.</li> <li>▪ <b>0:</b> Starting the app without a server connection is not possible.</li> <li>▪ <b>1:</b> After one start of the app, a successful server connection is necessary.</li> <li>▪ <b>3</b></li> <li>▪ <b>5</b></li> <li>▪ <b>10</b></li> <li>▪ <b>20</b></li> </ul>
<p><b>Jailbreak allowed</b></p>	<p>Container apps are allowed to run on jailbroken devices.</p>
<p><b>App usage constraints</b></p>	

Setting/Field	Description
Here you can define constraints on using the Sophos container apps. Click <b>Add</b> to enter constraints.	
<b>Geo-fencing</b>	Lets you add latitude and longitude and a radius within which the Sophos container apps can be used.
<b>Time-fencing</b>	Lets you specify a start and end time within which the Sophos container apps can be used. Days of the week on which the apps can be used can be specified as well.
<b>Wi-Fi fencing</b>	<p>Lets you specify Wi-Fi networks to which the device must be connected in order to use the Sophos container apps.</p> <p>The device must actually be connected to one of the listed networks. Being able to see a particular network in the list of available networks is not enough.</p> <p><b>Important:</b> We recommend that you do not rely on Wi-Fi fencing as the only security mechanism because Wi-Fi names can be spoofed very easily.</p>

### 14.18.2 Corporate Email configuration (iOS Sophos container policy)

With the **Corporate Email** configuration you define user settings for your Microsoft Exchange Server. These settings are applied to the Sophos Secure Email app if it is installed in the Sophos container.

Setting/Field	Description
<b>Exchange ActiveSync host</b>	<p>The address of the Microsoft Exchange Server.</p> <p><b>Note:</b> If you use the SMC EAS proxy, enter the URL of the SMC proxy server.</p>
<b>User</b>	<p>The user for this account.</p> <p>If you enter the variable % <b>USERNAME</b> %, the server replaces it with the actual user name.</p>
<b>Email address</b>	<p>The email address of the account.</p> <p>If you enter the variable % <b>EMAILADDRESS</b> %, the server replaces it with the actual email address.</p>

Setting/Field	Description
<b>Domain</b>	The domain for this account.
<b>Support contact email</b>	The email address that will be used as the "Contact Support" email address.
<b>Use secure text fields</b>	The content of input fields is secured. Auto-complete and auto-correction are disabled within the Sophos Secure Email app to prevent sensitive words to be saved in the memory of the device.
<b>Export contacts to device</b>	Users are allowed to export the exchange contacts with a phone number to the local device contacts. Sophos Secure Email will keep them synchronized. Only name and telephone number will be exported to enable the user to identify company contacts in an incoming call. Note that even after a remote reset of the Sophos Secure Email app, the information will still be available in the local storage of the device.
<b>Show notification details</b>	<p>This option controls the display of email notifications and event reminders in the Sophos Secure Email app.</p> <p>When you select the option:</p> <ul style="list-style-type: none"> <li>▪ Email notifications are displayed with sender and subject.</li> <li>▪ Event reminders are displayed with time, location and title.</li> </ul> <p>When you deselect the option:</p> <ul style="list-style-type: none"> <li>▪ Email notifications are disabled.</li> <li>▪ Event reminders are displayed with time only.</li> </ul> <p><b>Note:</b> If you think notifications displayed on a lost or stolen device is a security risk, you may want to disable notification details.</p>
<b>Deny copy to clipboard</b>	Users cannot copy or cut texts from the Sophos Secure Email app.
<b>Allow external viewers</b>	The user can save attachments or open them in other apps.
<b>Maximum email size</b>	If required, select the maximum email size for Sophos Secure Email app from the list.
<b>Open attachments</b>	If you select this option, <b>Save</b> and <b>View</b> buttons are displayed under the attachment. <b>Save</b> passes the attachment on to Sophos Secure Workspace, <b>View</b>

Setting/Field	Description
	<p>opens the file in Sophos Secure Email. If Sophos Secure Email cannot open the file, users can select where to pass the file on to.</p> <p>If you deselect this option, attachment cannot be opened or passed on to other apps.</p>
<b>Add</b>	<p>Click <b>Add</b> to configure settings that a future version of the Sophos Secure Email app might require.</p> <p><b>Important:</b> Only configure these settings if instructed by the Sophos support team.</p>

### 14.18.3 Corporate Documents configuration (iOS Sophos container policy)

#### Configure storage providers

For each storage provider you can define the following settings separately:

Setting/Field	Description
<b>Enable</b>	The storage provider is available in the app.
<b>Offline</b>	Users are allowed to add files from the storage provider to the app's <b>Favorites</b> list for offline use.
<b>Open in (encrypted)</b>	Users can share encrypted files with other apps via <b>Open In</b> .
<b>Open in (unencrypted)</b>	Users can share unencrypted files with other apps via <b>Open In</b> .
<b>Clipboard</b>	Users can copy parts of a document and paste them into other apps.

#### Enterprise provider settings

For **Egnyte** and **WebDAV** provider, also referred to as *enterprise provider*, you can centrally define server settings and login credentials. These cannot be changed by users.

Credential settings that you do not define centrally can be chosen by the users in the app's provider credential screens.

For example you can centrally define the server and user account to be used but you can leave the password field undefined. Users then would have to know the password when accessing the storage provider.

Setting/Field	Description
<b>Name</b>	The name of the provider that is displayed in the Sophos Secure Workspace app.
<b>Server</b>	In this field, enter: <ul style="list-style-type: none"> <li>▪ The URL of the root folder on the <b>Corporate Documents</b> WebDAV server.</li> <li>▪ The URL of the root folder on the <b>Egnyte</b> server.</li> <li>▪ The URL of the root folder on the <b>WebDAV</b> server.</li> </ul> Use the following format: <b>https://server.company.com</b>
<b>User name</b>	In this field, enter the user name for the relevant server.
<b>Password</b>	In this field, enter the password for the relevant account.
<b>Upload folder</b>	In this field, enter the upload folder for the relevant account.

## Other settings

Setting/Field	Description
<b>Enable Documents</b>	This turns on the <b>Documents</b> feature to securely distribute company documents.
<b>Passphrase complexity</b>	The required minimum complexity of passphrases for encryption keys. More secure passphrases are always allowed. You can select the following settings: <ul style="list-style-type: none"> <li>▪ <b>4 char password</b></li> <li>▪ <b>6 char password</b></li> <li>▪ <b>8 char password</b></li> </ul>

Setting/Field	Description
	<ul style="list-style-type: none"> <li>▪ <b>10 char password</b></li> </ul>

#### 14.18.4 Corporate Browser configuration (iOS Sophos container policy)

With the **Corporate Browser** configuration you define settings for the Corporate Browser feature of the Sophos Secure Workspace app.

The Corporate Browser allows you to securely access corporate intranet pages and other allowed pages. You can define domains and bookmarks within a domain.

Every bookmarks belongs to a certain domain. When you use **Add bookmark** to define a bookmark, the domain entry is created automatically if it does not exist.

##### Domain settings

Setting/Field	Description
<b>URL</b>	The domain that you want to allow.
<b>Allow copy/paste</b>	Users can copy and paste text from the Corporate Browser to other apps.
<b>Allow open with</b>	Users can download attachments or pass them on to other apps.
<b>Allow save password</b>	Users can save their passwords in the Corporate Browser.

##### Bookmark settings

Setting/Field	Description
<b>Name</b>	The name for the bookmark.
<b>URL</b>	The web address for the bookmark.



### 14.18.5 Client certificate configuration (iOS Sophos container policy)

With the **Client certificate** configuration you install a client certificate onto devices. This certificate will be available to the Sophos Secure Email and Sophos Secure Workspace apps if they are installed in the Sophos container.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. 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.

### 14.18.6 Root certificate configuration (iOS Sophos container policy)

With the **Root certificate** configuration you upload a root certificate to devices. This certificate will be available to the Sophos Secure Email and Sophos Secure Workspace apps if they are installed in the Sophos container.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. 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.

### 14.18.7 SCEP configuration (iOS Sophos container policy)

With the **SCEP** configuration you enable devices to request certificates from a Certificate Authority using the Simple Certificate Enrollment Protocol (SCEP). These certificates are available to the Sophos Secure Workspace app if it is installed in the Sophos container.

**Note:** You must first add a **Root certificate** configuration to upload the CA certificate of the SCEP server before you can add a **SCEP** configuration.

Setting/Field	Description
<b>URL</b>	The web address of the Certificate Authority server. Use the variable <code>_%SCEPPROXYURL_%</code> to refer to the server URL that is configured on the <b>SCEP</b> tab of the <b>System setup</b> page.
<b>Alias name</b>	The name under which the certificate will appear in selection dialogs. This should be a memorable name to identify the certificate. For example, use the same value as in the <b>Subject</b> field, but without the <b>CN=</b> prefix.

Setting/Field	Description
<b>Subject</b>	<p>The name of the entity (for example person or device) that will receive the certificate.</p> <p>You can use placeholders for user data or device properties.</p> <p>The value that you enter (with placeholders replaced by the actual data) must be a valid X.500 name.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>▪ Enter <code>CN=%_USERNAME_%</code> to specify a user.</li> <li>▪ Enter <code>CN=%_DEVPROP(serial_number)_%</code> to specify a device.</li> </ul> <p>For information on available placeholders, see <a href="#">Placeholders in profiles and policies</a> (page 75).</p>
<b>Type of Subject Alternative Name</b>	Optionally, configure a Subject Alternative Name (SAN). Select one of the available SAN types.
<b>Value of Subject Alternative Name</b>	If you have selected a SAN type, enter the SAN value.
<b>NT user login name</b>	
<b>Challenge</b>	<p>The web address to obtain a challenge password from the SCEP server.</p> <p>Use the variable <code>%_CACHALLENGE_%</code> to refer to the challenge URL that is configured on the <b>SCEP</b> tab of the <b>System setup</b> page.</p>
<b>Root certificate</b>	<p>The CA certificate.</p> <p>Select the certificate from the list. The list contains all certificates that you have uploaded in <b>Root certificate</b> configurations of the current profile.</p>
<b>Key size</b>	<p>The size of the public key in the issued certificate.</p> <p>Make sure that the value matches the size configured on the SCEP server.</p>
<b>Use as digital signature</b>	If you select this check box, the public key can be used as a digital signature.
<b>Use for encryption</b>	If you select this check box, the public key can be used for data encryption.

## 14.19 Configurations for Windows Mobile policies

With a Windows Mobile policy you configure various aspects of Windows Mobile devices, like password policies, restrictions or Wi-Fi settings.

For information on how to create a Windows Mobile policy, see [Create profile or policy](#) (page 72).

### 14.19.1 Password policies configuration (Windows Mobile policy)

With the **Password policies** configuration you define password rules for devices.

Setting/Field	Description
<b>Password type</b>	Select the type of password you want to define: <ul style="list-style-type: none"> <li>▪ <b>Alphanumeric</b></li> <li>▪ <b>Alphanumeric or numeric</b></li> </ul>
<b>Allow simple password</b>	Passwords can contain sequential or repeated characters, for example <b>abcde</b> or <b>1111</b> .
<b>Minimum password length</b>	The minimum number of characters a password must contain.
<b>Maximum number of failed attempts</b>	The maximum number of failed login attempts to enter the correct password before the device is wiped.  Enter a value between <b>1</b> and <b>999</b> , or <b>0</b> for no restriction.
<b>Time in minutes until the device is locked</b>	The time period (in minutes) after which the device is locked if it has not been used. The user can unlock the device.  Enter a value between <b>1</b> and <b>999</b> , or <b>0</b> for no restriction.
<b>Password history</b>	The number of old passwords that are remembered and compared with new ones. When the user defines a new password, it is not accepted if it matches a previously used password.  Enter a value between <b>1</b> and <b>999</b> , or <b>0</b> for no restriction.

Setting/Field	Description
<b>Maximum password age in days</b>	The number of days after which users must change their password.  Enter a value between 1 and 730, or 0 for no restriction.
<b>Minimum number of different character groups</b>	The minimum number of non-alphanumeric characters (for example & or !) a password must contain.
<b>Allow the password grace period to be set</b>	Users are allowed to set the password grace period.

## 14.19.2 Restrictions configuration (Windows Mobile policy)

With the **Restrictions** configuration you define restrictions for devices.

### Device

Setting/Field	Description
<b>Forbid SD card</b>	Users cannot access the storage card. This does not prevent apps from accessing the storage card.
<b>Forbid unencrypted device</b>	Internal storage encryption is turned on.  <b>Important:</b> After internal storage encryption has been turned on on a device, you cannot turn it off again through a policy.  <b>Note:</b> You must enable BitLocker on the device before applying the policy.
<b>Forbid action center notifications above lock screen</b>	No Action Center notifications are displayed above the device lock screen.
<b>Forbid manual addition of non-Microsoft email accounts</b>	Forbids adding all types of email accounts, as well as Exchange, Office 365 and Outlook.com accounts.
<b>Forbid Microsoft account connection</b>	The Microsoft account is the system account used for synchronization, backup and the Store.
<b>Forbid developer mode</b>	The Windows developer mode is turned off.

Setting/Field	Description
<b>Forbid Windows Store</b>	The app store is unavailable.
<b>Forbid native browser</b>	The Microsoft Edge browser is unavailable.
<b>Forbid camera</b>	The Privacy setting <b>Let apps use my camera</b> is turned off.
<b>Telemetry</b>	Select if the device can send diagnostic and usage telemetry data: <ul style="list-style-type: none"> <li>▪ <b>Allowed</b></li> <li>▪ <b>Allowed, except for secondary data requests</b></li> <li>▪ <b>Not allowed</b></li> </ul>

## Various

Setting/Field	Description
<b>Forbid copy and paste</b>	The clipboard is unavailable.
<b>Forbid Cortana</b>	Cortana is turned off.
<b>Forbid "Save as" for Office files</b>	Users cannot save a file on the device as an Office file.
<b>Forbid screen capture</b>	Screen captures are turned off.
<b>Forbid sharing of Office files</b>	Users cannot share Office files.
<b>Forbid "Sync my settings"</b>	Device settings cannot be synchronized to and from other Windows devices.
<b>Forbid voice recording</b>	Voice recording is turned off.

## Wi-Fi

Setting/Field	Description
<b>Forbid Wi-Fi</b>	Wi-Fi connections are turned off.
<b>Forbid internet sharing</b>	Internet Connection Sharing (ICS) is turned off.
<b>Forbid Wi-Fi Sense (hotspot auto-connect)</b>	The device does not automatically connect to Wi-Fi hotspots.
<b>Forbid hotspot reporting</b>	The device does not send information about Wi-Fi connections.
<b>Forbid manual configuration</b>	Users cannot configure Wi-Fi connections beyond the connections that are configured by Sophos Mobile Control.

## Connectivity

Setting/Field	Description
<b>Forbid NFC</b>	Near Field Communication (NFC) is turned off.
<b>Forbid Bluetooth</b>	Bluetooth is turned off.
<b>Forbid USB connection</b>	USB connection between the device and a computer to sync files or to use developer tools to deploy or debug applications is forbidden. This does not affect USB charging.

## Roaming and costs

Setting/Field	Description
<b>Forbid cellular data roaming</b>	Data connections over foreign cellular networks are turned off.

Setting/Field	Description
<b>Forbid VPN over cellular</b>	VPN connections over cellular networks are turned off.
<b>Forbid VPN roaming over cellular</b>	VPN connections over foreign cellular networks are turned off.

## Security and privacy

Setting/Field	Description
<b>Forbid Bing Vision to store images from Bing Vision search</b>	Bing Vision does not store the contents of the images captured when performing Bing Vision search.
<b>Forbid use of location when searching</b>	The search cannot utilize location information.
<b>Forbid manual installation of root certificates</b>	Users cannot manually install root and intermediate CA certificates.
<b>Forbid locating</b>	All location privacy settings on the device are turned off. No apps can use the location service. This also forbids Sophos Mobile Control to locate the device.
<b>SafeSearch permission</b>	The level of search result filtering that is enforced on the device: <ul style="list-style-type: none"> <li>▪ <b>Moderate:</b> Moderate filtering against adult content. Valid search results are not filtered.</li> <li>▪ <b>Strict:</b> Highest filtering against adult content.</li> </ul>

## Unenrollment

Setting/Field	Description
<b>Forbid user to reset the phone</b>	Users cannot factory reset the device through the control panel or hardware key combinations.
<b>Forbid manual MDM unenrollment</b>	Users cannot delete the workplace account.

### 14.19.3 Exchange ActiveSync configuration (Windows Mobile policy)

With the **Exchange ActiveSync** configuration you define user settings for your Microsoft Exchange Server.

Setting/Field	Description
<b>Account name</b>	The account name.
<b>Exchange ActiveSync host</b>	The address of the Microsoft Exchange Server. <b>Note:</b> If you use the SMC EAS proxy, enter the URL of the SMC proxy server.
<b>Domain</b>	The domain for this account.
<b>User</b>	The user for this account. If you enter the variable %_USERNAME_%, the server replaces it with the actual user name.
<b>Email address</b>	The email address of the account. If you enter the variable %_EMAILADDRESS_%, the server replaces it with the actual email address.
<b>Password</b>	The password for this account. If you leave this field empty, users must enter the password on their devices.
<b>Synchronization period</b>	The time period emails are synchronized for. If you select a time period, only the emails from within the specified period are synchronized to the inbox on the managed device.
<b>Synchronization interval</b>	The interval between email synchronization processes.
<b>SSL</b>	All communication is sent through SSL (Secure Socket Layer). We recommend that you select this check box.
<b>Synchronize content types</b>	The content types to be synchronized.



### 14.19.4 Wi-Fi configuration (Windows Mobile policy)

With the **Wi-Fi** configuration you specify settings for connecting to Wi-Fi networks.

Setting/Field	Description
<b>SSID</b>	In this field, enter the ID of the Wi-Fi network.
<b>Connect automatically</b>	The connection will be established automatically.
<b>Hidden network</b>	The target network is not open or visible.
<b>Security type</b>	Select the Security type from the list. If you select either <b>WPA-PSK</b> or <b>WPA2-PSK</b> you must specify the password.
<b>Proxy</b>	If you select <b>Manually</b> from the list, you must specify Server and port.

### 14.19.5 App restrictions configuration (Windows Mobile policy)

With the **App restrictions** configuration you specifically allow or block apps on the devices.

Setting/Field	Description
<b>Allowed apps</b>	<p>Contains a set of individual apps that users are allowed to install and use on the device. Users will be unable to install or use any apps that are not explicitly listed.</p> <p>Use <b>Allowed apps</b> when you know the list of apps that you want to allow and want to block all other apps.</p>
<b>Forbidden apps</b>	<p>Contains a set of individual apps that users are prevented from installing on the device. Users will be able to install any apps that are not explicitly listed.</p> <p>Use <b>Forbidden apps</b> when you know the list of apps that you want to block and want to allow all other apps.</p>
<b>App group</b>	<p>Select the <b>App group</b> that contains the list of apps you want to allow or block.</p> <p><b>Note:</b> The app group has to be created beforehand. See <a href="#">App groups</a> (page 190).</p>

## 14.19.6 Root certificate configuration (Windows Mobile policy)

With the **Root certificate** configuration you install a root certificate onto devices.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. 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.

## 14.19.7 SCEP configuration (Windows Mobile policy)

With the **SCEP** configuration you enable devices to request certificates from a Certificate Authority using the Simple Certificate Enrollment Protocol (SCEP).

Setting/Field	Description
<b>Description</b>	A description for the configuration.
<b>URL</b>	The web address of the Certificate Authority server. Use the variable <code>_%_SCEPPROXYURL_%</code> to refer to the server URL that is configured on the <b>SCEP</b> tab of the <b>System setup</b> page.
<b>Subject</b>	The name of the entity (for example person or device) that will receive the certificate. You can use placeholders for user data or device properties. The value that you enter (with placeholders replaced by the actual data) must be a valid X.500 name. For example: <ul style="list-style-type: none"> <li>Enter <code>CN=_%_USERNAME_%</code> to specify a user.</li> <li>Enter <code>CN=_%_DEVPROP(serial_number)_%</code> to specify a device.</li> </ul> For information on available placeholders, see <a href="#">Placeholders in profiles and policies</a> (page 75).
<b>Subject Alternative Name</b>	Optionally, configure one or more Subject Alternative Name (SAN) values. Click <b>Add</b> and then enter a SAN type and a SAN value.

Setting/Field	Description
<b>Challenge</b>	The web address to obtain a challenge password from the SCEP server.  Use the variable %_CACHALLENGE_% to refer to the challenge URL that is configured on the <b>SCEP</b> tab of the <b>System setup</b> page.
<b>Root certificate</b>	The CA certificate.  Select the certificate from the list. The list contains all certificates that you have uploaded in <b>Root certificate</b> configurations of the current profile.
<b>Retries</b>	The number of retries if the server sends a response of type <i>pending</i> .
<b>Retry delay</b>	The number of seconds between retries.
<b>Key size</b>	The size of the public key in the issued certificate.  Make sure that the value matches the size configured on the SCEP server.
<b>Use as digital signature</b>	If you select this check box, the public key can be used as a digital signature.
<b>Use for encryption</b>	If you select this check box, the public key can be used for data encryption.
<b>Hash algorithm</b>	Select one or more hash algorithms that are supported by the SCEP server.

## 14.20 Configurations for Windows Desktop policies

With a Windows Desktop policy you configure various aspects of Windows Desktop devices, like password policies, restrictions or Wi-Fi settings.

For information on how to create a Windows Desktop policy, see [Create profile or policy](#) (page 72).

### 14.20.1 Password policies configuration (Windows Desktop policy)

With the **Password policies** configuration you define password rules for devices.

**Note:** Password complexity rules (for example length, number of uppercase and lowercase letters) for Windows Desktop devices are fixed and cannot be set by a Sophos Mobile Control policy. For details see [Windows Desktop password complexity rules](#) (page 74).

**Note:** Password policies cannot be assigned to a Windows Desktop device, if there are other local users configured on the device (in addition to the user that is enrolled with Sophos Mobile Control), and at least one of them is not allowed to change their password.

Setting/Field	Description
<b>Maximum number of failed attempts</b>	The maximum number of failed login attempts to enter the correct password before the device is wiped. Enter a value between 1 and 999, or 0 for no restriction.
<b>Time in minutes until the device is locked</b>	The time period (in minutes) after which the device is locked if it has not been used. The user can unlock the device. Enter a value between 1 and 999, or 0 for no restriction.
<b>Password history</b>	The number of old passwords that are remembered and compared with new ones. When the user defines a new password, it is not accepted if it matches a previously used password. Enter a value between 1 and 999, or 0 for no restriction.
<b>Maximum password age in days</b>	The number of days after which users must change their password. Enter a value between 1 and 730, or 0 for no restriction.

## 14.20.2 Restrictions configuration (Windows Desktop policy)

With the **Restrictions** configuration you define restrictions for devices.

### Device

Setting/Field	Description
<b>Forbid SD card</b>	Users cannot access the storage card. This does not prevent apps from accessing the storage card.

Setting/Field	Description
<b>Forbid manual addition of non-Microsoft email accounts</b>	Forbids adding all types of email accounts, as well as Exchange, Office 365 and Outlook.com accounts.
<b>Forbid developer mode</b>	The Windows developer mode is turned off.
<b>Forbid camera</b>	The Privacy setting <b>Let apps use my camera</b> is turned off.
<b>Disable Edge autofill</b>	The <b>Save form entries</b> setting in the Edge web browser is turned off and cannot be turned on by the user.  If the check box is cleared, the setting is turned on and cannot be turned off by the user.
<b>Disable Edge F12 Developer Tools</b>	The F12 Developer Tools of the Edge web browser are unavailable.
<b>Disable Edge pop-up blocker</b>	The <b>Block pop-ups</b> setting in the Edge web browser is turned off and cannot be turned on by the user.  If the check box is cleared, the setting is turned on and cannot be turned off by the user.
<b>Disable AutoPlay settings</b>	The relevant sections of the Windows Control Panel are unavailable. The user cannot change any of these settings after the policy has been assigned to the device.  <b>Note: Disable AutoPlay settings</b> does not affect connected devices, like for example mobile phones.
<b>Disable Date &amp; Time settings</b>	
<b>Disable Language settings</b>	
<b>Disable Power &amp; Sleep settings</b>	
<b>Disable Region settings</b>	
<b>Disable Sign-in settings</b>	
<b>Disable VPN settings</b>	
<b>Disable Workplace settings</b>	
<b>Disable Account settings</b>	

Setting/Field	Description
<b>Telemetry</b>	Select if the device can send diagnostic and usage telemetry data: <ul style="list-style-type: none"> <li>▪ <b>Allowed</b></li> <li>▪ <b>Allowed, except for secondary data requests</b></li> <li>▪ <b>Not allowed</b></li> </ul>

## Various

Setting/Field	Description
<b>Forbid Cortana</b>	Cortana is turned off.
<b>Forbid "Sync my settings"</b>	Device settings cannot be synchronized to and from other Windows devices.
<b>Disable Windows tips</b>	The Windows notification setting <b>Show me tips about Windows</b> is cleared and unavailable.

## Wi-Fi

Setting/Field	Description
<b>Forbid internet sharing</b>	Internet Connection Sharing (ICS) is turned off.
<b>Forbid Wi-Fi Sense (hotspot auto-connect)</b>	The device does not automatically connect to Wi-Fi hotspots.

## Connectivity

Setting/Field	Description
<b>Forbid Bluetooth</b>	Bluetooth is turned off.

## Security and privacy

Setting/Field	Description
<b>Forbid use of location when searching</b>	The search cannot utilize location information.

## Unenrollment

Setting/Field	Description
<b>Forbid manual MDM unenrollment</b>	Users cannot delete the workplace account.

### 14.20.3 Exchange ActiveSync configuration (Windows Desktop policy)

With the **Exchange ActiveSync** configuration you define user settings for your Microsoft Exchange Server.

**Important:** If you use multiple configurations to set up Exchange ActiveSync accounts, the devices might only be able to retrieve mail for one account. This typically happens when the accounts are located on different Exchange ActiveSync servers and there are different mailbox policies defined on these servers. Because the Windows Desktop devices can only enforce a single mailbox policy, they will fail to connect to the accounts that use a different policy.

Setting/Field	Description
<b>Account name</b>	The account name.
<b>Exchange ActiveSync host</b>	The address of the Microsoft Exchange Server. <b>Note:</b> If you use the SMC EAS proxy, enter the URL of the SMC proxy server.
<b>Domain</b>	The domain for this account.
<b>User</b>	The user for this account. If you enter the variable <code>%_USERNAME_</code> , the server replaces it with the actual user name.

Setting/Field	Description
<b>Email address</b>	The email address of the account. If you enter the variable %_EMAILADDRESS_%, the server replaces it with the actual email address.
<b>Password</b>	The password for this account. If you leave this field empty, users must enter the password on their devices.
<b>Synchronization period</b>	The time period emails are synchronized for. If you select a time period, only the emails from within the specified period are synchronized to the inbox on the managed device.
<b>Synchronization interval</b>	The interval between email synchronization processes.
<b>SSL</b>	All communication is sent through SSL (Secure Socket Layer). We recommend that you select this check box.
<b>Synchronize content types</b>	The content types to be synchronized.

#### 14.20.4 Wi-Fi configuration (Windows Desktop policy)

Setting/Field	Description
<b>SSID</b>	In this field, enter the ID of the Wi-Fi network.
<b>Connect automatically</b>	The connection will be established automatically.
<b>Hidden network</b>	The target network is not open or visible.

#### 14.20.5 Root certificate configuration (Windows Desktop policy)

With the **Root certificate** configuration you install a root certificate onto devices.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. 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.



## 14.21 Configurations for Windows IoT policies

With a Windows IoT policy you configure various aspects of Windows IoT devices, like password policies, restrictions or Wi-Fi settings.

For information on how to create a Windows IoT policy, see [Create profile or policy](#) (page 72).

### 14.21.1 Restrictions configuration (Windows IoT policy)

With the **Restrictions** configuration you define restrictions for devices.

#### Device

Setting/Field	Description
<b>Forbid SD card</b>	Users cannot access the storage card. This does not prevent apps from accessing the storage card.
<b>Forbid developer mode</b>	The Windows developer mode is turned off.
<b>Forbid camera</b>	The Privacy setting <b>Let apps use my camera</b> is turned off.
<b>Disable Edge autofill</b>	The <b>Save form entries</b> setting in the Edge web browser is turned off and cannot be turned on by the user. If the check box is cleared, the setting is turned on and cannot be turned off by the user.
<b>Disable Edge pop-up blocker</b>	The <b>Block pop-ups</b> setting in the Edge web browser is turned off and cannot be turned on by the user. If the check box is cleared, the setting is turned on and cannot be turned off by the user.
<b>Telemetry</b>	The amount of Windows diagnostic and usage data that devices are allowed to send. <ul style="list-style-type: none"> <li>▪ <b>Full:</b> All data required to identify and analyze issues.</li> <li>▪ <b>Enhanced:</b> Data about how Windows and apps are used and how they perform.</li> <li>▪ <b>Basic:</b> A limited set of data that's critical for understanding the device and its configuration.</li> </ul>

Setting/Field	Description
	<ul style="list-style-type: none"> <li>▪ <b>Security:</b> Information that is required to keep the device protected with the latest security updates.</li> </ul> <p><b>Note:</b> Levels are cumulative from bottom to top, e.g. <b>Enhanced</b> includes all data from <b>Basic</b> and <b>Security</b>.</p> <p><b>Tip:</b> For detailed information on the telemetry levels, see the Microsoft article <a href="#">Configure Windows telemetry in your organization (external link)</a>.</p>

## Wi-Fi

Setting/Field	Description
<b>Forbid internet sharing</b>	Internet Connection Sharing (ICS) is turned off.
<b>Forbid Wi-Fi Sense (hotspot auto-connect)</b>	The device does not automatically connect to Wi-Fi hotspots.

## Connectivity

Setting/Field	Description
<b>Forbid Bluetooth</b>	Bluetooth is turned off.

### 14.21.2 Wi-Fi configuration (Windows IoT policy)

With the **Wi-Fi** configuration you specify settings for connecting to Wi-Fi networks.

Setting/Field	Description
<b>SSID</b>	In this field, enter the ID of the Wi-Fi network.
<b>Connect automatically</b>	The connection will be established automatically.

Setting/Field	Description
<b>Hidden network</b>	The target network is not open or visible.
<b>Security type</b>	Select the Security type from the list. If you select either <b>WPA-PSK</b> or <b>WPA2-PSK</b> you must specify the password.

### 14.21.3 Root certificate configuration (Windows IoT policy)

With the **Root certificate** configuration you install a root certificate onto devices.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. 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.

# 15 Task bundles

By using task bundles you can bundle several tasks in one transaction. So you can bundle all tasks necessary to have a device enrolled and configured:

- Enroll the device.
- Apply required policies.
- Install required applications (for example managed apps for iOS devices).
- Apply required profiles.

You can also include wipe commands in task bundles to automatically wipe non-compliant (for example jailbroken or rooted) devices. For further information, see [Compliance rules](#) (page 41).

Task bundles are available for the following platforms:

- Android
- Apple iOS

## 15.1 Create task bundle

1. On the menu sidebar, under **CONFIGURE**, click **Task bundles** and select **Android** or **Apple iOS**.

2. On the **Task bundles** page, click **Create task bundle**.

The **Edit task bundle** page is displayed.

3. Enter a name and, optionally, a version and a description for the new task bundle in the relevant fields.

4. When you select the **Selectable for compliance actions** option, the task bundle can be transferred onto a device when the device breaks a compliance rule. See [Compliance rules](#) (page 41).

**Note:** This option will be disabled when you edit an existing task bundle and the task bundle is already used as a compliance action.

5. On the menu sidebar, under **CONFIGURE**, click **Task bundles** and select **Android** or **Apple iOS**.

6. Click **Create task**.

7. Select the task type and click **Next**.

The next view depends on the task type you have selected. In each view you can specify your own meaningful task names. These task names are shown during installation on the Self Service Portal.

8. Follow the wizard steps to add the required task and click **Apply** to create the task.

For a description of the available task types, see [Available Android task types](#) (page 173) and [Available iOS task types](#) (page 176).

9. Optional: Add further tasks to the task bundle.

**Tip:** You can change the installation order of the tasks by using the sort arrows on the right-hand side of the tasks list.

10. After you have added all required tasks to the task bundle, click **Save** on the **Edit task bundle** page.

The task bundle is available for transfer. It is displayed on the **Task bundles** page.

**Note:** When you edit an existing task bundle which is used as **Initial package** in the Self Service Portal settings, the enrollment task cannot be deleted. See [Configure Self Service Portal settings](#) (page 25).

## 15.2 Available Android task types

The following task types are available for Android task bundles:

### Enroll

When the task is transferred to devices, an enrollment email is sent to the email address that is configured for each device. Users must perform the steps that are described in the email to enroll their device.

When the task is transferred to a device that is already enrolled, no enrollment email is sent.

### Install profile or assign policy

Select a profile or policy from the list of available profiles and policies. For information on how to add profiles or policies to this list, see [Profiles and policies](#) (page 72).

When the task is transferred to devices, the profile is silently installed or the policy is silently assigned.

You can add more than one task of this type to a task bundle.

### Remove profile

In **Select source**, select **Profiles** and then select a profile from the list.

In addition to the profiles that are available on the Sophos Mobile Control server, the list includes profiles that are in use on the managed devices.

You can also remove a profile that is not contained in the list. Select **Identifier** and then enter the identifier of the profile you want to remove from devices.

When the task is transferred to devices, the profile is silently removed.

You can add more than one task of this type to a task bundle.

**Note:** You cannot directly remove a Sophos container policy or a Mobile Security policy from devices. Instead, use the device action **Unenroll Sophos container** or **Unenroll SMSec**. This will also remove the related policies from the device.

## Install app

Select an app from the list of all available apps. For information on how to add apps to this list, see [Add app](#) (page 180).

When the task is transferred to devices, users receive a notification on their devices that Sophos Mobile Control wants to install the app. Users can tap **OK** to start the process, or **Not now** to be notified again after a short period of time.

If users tap **OK** but then tap **Cancel** in the subsequent Android dialog, the task fails.

If the app is already installed on a device that receives the task, it is updated.

You can add more than one task of this type to a task bundle.

## Install Android for Work app

This task type is available if you have configured Android for Work for the customer.

Select an app from list of all available work apps. For information how to add apps to this list, see [Edit work app](#) (page 202).

The installation task is sent to a Google service. Google then manages the installation of the app onto the device. On the **Task view** page, the state of the task is **successful** when it has been sent to Google.

You can add more than one task of this type to a task bundle.

Alternatively, you can install work apps from the **Android for Work apps** page. See [Install work app](#) (page 204).

For information how to uninstall a work app from devices, see [Uninstall work app](#) (page 205).

## Remove app

In **Select source**, select **Apps** to select an app for removal from the list of available apps.

In addition to the apps that are available on the Sophos Mobile Control server, the list includes apps that are in use on the managed devices - with the exception of Android system apps and apps that have been pre-installed by the device manufacturer.

You can also remove an app that is not contained in the list. Select **Identifier** and then enter the package name of the app you want to remove from devices. If you select **Knox container app**, the app will be removed from the Samsung Knox container.

When the task is transferred to devices, users receive a notification on their devices that Sophos Mobile Control wants to remove the app. Users can tap **OK** to start the process, or **Not now** to be notified again after a short period of time.

If users tap **OK** but then tap **Cancel** in the subsequent Android dialog, the task fails.

If the app is not installed on a device that receives the task, no notification is displayed.

You can add more than one task of this type to a task bundle.

## Send message

Enter a plain text to be displayed on the devices.

When the task is transferred to devices, the message text is displayed in a notification window. Users can display past messages on the **Messages** page of the Sophos Mobile Control app.

You can add more than one task of this type to a task bundle.

## Unenroll

When the task is transferred to devices, they are unenrolled from Sophos Mobile Control. See [Unenroll devices](#) (page 57). Device users do not need to confirm the operation.

You cannot add an **Unenroll** and a **Wipe** task to the same task bundle.

## Wipe

When the task is transferred to devices, they are reset to their factory settings. Device users do not need to confirm the operation.

**Important:** Use this task type with care. All data on the devices that receive the task is deleted without user confirmation.

**Note:** When a **Wipe** task is transferred to a device that is enrolled with Android for Work, only the work profile and all work apps are removed.

You cannot add an **Unenroll** and a **Wipe** task to the same task bundle.

## Knox container: lock

When the task is transferred to a Samsung device that supports Samsung Knox, the Knox container is locked.

If the task is transferred to a device that does not support Samsung Knox, the task fails.

## Knox container: unlock

When the task is transferred to a Samsung device that supports Samsung Knox, the Knox container is unlocked.

If the task is transferred to a device that does not support Samsung Knox, the task fails.

## Knox container: reset password

When the task is transferred to a Samsung device that supports Samsung Knox, the Knox container password is reset. Users must set a new password to unlock the Knox container.

If the task is transferred to a device that does not support Samsung Knox, the task fails.

### Knox container: remove

When the task is transferred to a Samsung device that supports Samsung Knox, the Knox container (including any container-related configuration) is removed.

If the task is transferred to a device that does not support Samsung Knox, the task fails.

### Trigger SMSec scan

When the task is transferred to devices, the Sophos Mobile Security app is silently triggered to perform a scan against malware and potentially unwanted apps (PUAs).

This task requires that Sophos Mobile Security is managed from Sophos Mobile Control, that is, a Mobile Security policy is assigned to the device. See [Manage Sophos Mobile Security](#) (page 210).

If Sophos Mobile Security is not managed by Sophos Mobile Control on a device that receives the task (that is, if a Mobile Security policy is not assigned to the device), the task remains in the state *Will be retried*.

## 15.3 Available iOS task types

The following task types are available for iOS task bundles:

### Enroll

When the task is transferred to devices, an enrollment email is sent to the email address that is configured for each device. Users must perform the steps that are described in the email to enroll their device.

When the task is transferred to a device that is already enrolled, no enrollment email is sent.

### Install profile or assign policy

Select a profile or policy from the list of available profiles and policies. For information on how to add profiles or policies to this list, see [Profiles and policies](#) (page 72).

When the task is transferred to devices, the profile is silently installed or the policy is silently assigned.

You can add more than one task of this type to a task bundle.

### Remove profile

In **Select source**, select **Profiles** and then select a profile from the list.

In addition to the profiles that are available on the Sophos Mobile Control server, the list includes profiles that are in use on the managed devices.



You can also remove a profile that is not contained in the list. Select **Identifier** and then enter the identifier of the profile you want to remove from devices.

When the task is transferred to devices, the profile is silently removed.

You can add more than one task of this type to a task bundle.

**Note:** You cannot directly remove a Sophos container policy from devices. Instead, use the device action **Unenroll Sophos container**. This will also remove the related policy from the device.

## Install provisioning profile

Select an app provisioning profile from the list of available profiles. For information on how to add profiles to this list, see [Import provisioning profiles for iOS apps](#) (page 74).

When the task is transferred to devices, the provisioning profile is silently installed.

## Remove provisioning profile

In **Select source**, select **Profiles** and then select a provisioning profile from the list.

In addition to the profiles that are available on the Sophos Mobile Control server, the list includes profiles that are in use on the managed devices.

You can also remove a provisioning profile that is not contained in the list. Select **Identifier** and then enter the identifier of the profile you want to remove from devices.

When the task is transferred to devices, the provisioning profile is silently removed.

## Install app

Select an app from the list of all available apps. For information on how to add apps to this list, see [Add app](#) (page 180).

When the task is transferred to devices, users receive a notification on their devices that Sophos Mobile Control wants to install the app. Users can tap **Install** to start the process, or **Cancel** to reject the installation.

If users reject the installation, the task fails.

If the app is already installed on a device that receives the task, it is updated.

You can add more than one task of this type to a task bundle.

## Remove app

In **Select source**, select **Apps** to select an app for removal from the list of available apps.

In addition to the apps that are available on the Sophos Mobile Control server, the list includes apps that are in use on the managed devices - with the exception of iOS system apps.

You can also remove an app that is not contained in the list. Select **Identifier** and then enter the bundle ID of the app you want to remove from devices.

When the task is transferred to devices, the app is removed silently.

You can add more than one task of this type to a task bundle.

## Send message

Enter a plain text to be displayed on the devices.

When the task is transferred to devices, the message text is displayed in a notification window. Users can display past messages on the **Messages** page of the Sophos Mobile Control app.

You can add more than one task of this type to a task bundle.

## Unenroll

When the task is transferred to devices, they are unenrolled from Sophos Mobile Control. See [Unenroll devices](#) (page 57). Device users do not need to confirm the operation.

You cannot add an **Unenroll** and a **Wipe** task to the same task bundle.

## Wipe

When the task is transferred to devices, they are reset to their factory settings. Device users do not need to confirm the operation.

**Important:** Use this task type with care. All data on the devices that receive the task is deleted without user confirmation.

You cannot add an **Unenroll** and a **Wipe** task to the same task bundle.

## 15.4 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. On the menu sidebar, under **CONFIGURE**, click **Task bundles** and select **Android** or **Apple iOS**.

The **Task bundles** page is displayed.

2. Click the blue triangle next to the task bundle you want to duplicate and then click **Duplicate**.

The task bundle is duplicated and shown on the **Task bundles** page. You can now edit the duplicated task bundle as required. To edit the task bundle, click the blue triangle next to it and then click **Edit**.

## 15.5 Transfer task bundles to individual devices or to device groups

1. On the menu sidebar, under **CONFIGURE**, click **Task bundles** and select **Android** or **Apple iOS**.

The **Task bundles** page is displayed.

2. Click the blue triangle next to the required task and then click **Transfer**.

The **Select devices** page is displayed.

3. On this page, you can:

- Select individual devices you want to transfer the task bundle to.
- Click **Select device groups**, to open the **Select device groups** page and select one or several device groups for transferring the task bundle.

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

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

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

6. Click **Finish**.

The **Task view** is shown.

The task bundle is transferred to the selected devices at the specified date and time.

# 16 Apps

You configure apps in Sophos Mobile Control to make them available for installation through the Sophos Mobile Control console (administrator-initiated) or through the Sophos Mobile Control app (user-initiated).

App management is available for the following platforms:

- Android
- Apple iOS
- Windows Mobile

To make an app available in Sophos Mobile Control, you can do one of the following:

- You upload the app package to the Sophos Mobile Control server. This option is not available for Windows Mobile apps.
- You provide a link to the app in the relevant app store.

For both options, see section [Add app](#) (page 180).

To install an app on a device, create a task bundle that contains an **Install app** task. For Android and iOS devices, you can create such task bundles directly from the **Apps** page. See [Install app](#) (page 182).

**Note:**

To be able to install app packages that are stored on the Sophos Mobile Control server (in contrast to the installation from the app store), the following conditions must be met:

- For Android, the Android security setting **Unknown sources** must be enabled on the devices. When you try to install an APK file when **Unknown sources** is disabled, the Sophos Mobile Control app will direct the users to the page where they can enable the setting. This restriction does not apply to devices with LG GATE, Samsung Knox or Sony Enterprise API.
- For iOS, the installation of apps from IPA files is only possible for self-developed apps. When the app is ready for distribution, you must create a provisioning profile for the app and make it available on the devices, either installed separately beforehand or included in the app's IPA file. You can use Sophos Mobile Control to distribute provisioning profiles to your iOS devices. See [Import provisioning profiles for iOS apps](#) (page 74). For details on provisioning profiles, see the *iOS Developer Library*.

## 16.1 Add app

You make an app available for installation either by uploading the app package or by linking to the app in the relevant app store.

1. On the menu sidebar, under **CONFIGURE**, click **Apps** and then select the platform for which you want to add the app.

2. On the **Apps** page, click **Add app** and then select:
  - **Android package** or **iOS package** to add the app by uploading the APK file (for Android apps) or IPA file (for iOS apps).
  - **Android link**, **iOS link** or **Windows Mobile link** to add the app by linking to it in the relevant app store.

On the next page, you configure the app details.

**Note:** For iOS links, you can click **Search in iTunes** to search for the app in the iTunes database. When you select an app in the search results list, the relevant fields on the **Edit iOS link** page will be populated from the corresponding iTunes values.

3. Enter a **Name** for the new app.
4. Optional: For app packages, enter a **Version** that is displayed in the Enterprise App Store. For app links, the version is displayed as *Google Play Store* or *App Store*. In the Enterprise App Store this is replaced by the actual version from the app store.
5. Optional: In the **App identifier** field, enter the internal identifier of the app. Leave this field empty if you do not know the exact identifier. In most cases, Sophos Mobile Control can read the value from the app itself and then fills in this field automatically.
6. Optional: In the **App category** field, enter a category name, for example **Recommended**. When you make the app available in the Enterprise App Store as described in the next step, the app will be listed in a section with that name.
7. You can make the app available in the Enterprise App Store so that its installation can be initiated by the user. Click **Show** next to **Available to device groups** and select one or more device groups for which the app will be listed in the Enterprise App Store.
8. For iOS devices, when you select **SMC managed installation**, the app will be installed as a managed app. Certain device profile settings are only available for managed apps.
 

**Note:** The **SMC managed installation** setting only affects apps that are installed by the user from the Enterprise App Store. Apps that you install from the Sophos Mobile Control console are always managed.

For information on managed apps, see [Managed apps for iOS](#) (page 183).
9. Optional: In the **Description** text field, enter a description that is displayed in the Enterprise App Store.
 

**Note:** You may use the placeholder `%_appstoretext_` anywhere in your description text. In the Enterprise App Store, this is replaced by the actual app description from Google Play or the App Store.
10. Click **Show** next to **Operating systems** and select the operating system versions the app applies to.
11. For Samsung Knox devices, when you select **Install in Knox container**, the app will be installed inside the Knox container. This option is only available when a Samsung Knox Premium license key is configured on the **System setup** page.

12. Configure the app source.

- For app links, enter the URL of the app in the relevant app store in the **Link** field.  
To determine the URL, click the link below the **Link** field to open the app store in a new browser tab and navigate to the app page. Then copy the URL from the tab's address bar and paste it into the **Link** field.
- For app packages, click **Upload a file** to upload the app to the Sophos Mobile Control server. Navigate to the APK file (for Android apps) or IPA file (for iOS apps) and click **Open**.

**Note:**

The package file size must not exceed a certain limit.

For on-premise installations, the limit is configured by your super administrator. For Sophos Mobile Control as a Service, it is set to 100 MB per package.

13. When you have configured the app details, click **Save** to save the app settings and to return to the **Apps** page.

The app is available for installation. It is displayed on the **Apps** page. If you have configured the **Available to device groups** field, the app is also displayed in the Enterprise App Store of the Sophos Mobile Control app from where users can install it. The installation process runs unattended or with very little user interaction.

## 16.2 Install app

**Note:** This section only applies to Android and iOS devices.

When you have added an app to Sophos Mobile Control as described in [Add app](#) (page 180), you can manually install it on selected devices or device groups.

1. On the menu sidebar, under **CONFIGURE**, click **Apps** and then click **Android** or **Apple iOS**.
2. On the **Apps** page, click the blue triangle next to the required app and then click **Install**.
3. Select the devices on which you want to install the app. Do one of the following:
  - Select individual devices.
  - Click **Select device groups** and then select one or more device groups.

When you are ready, click **Next**.

4. On the **Set execution date** page, specify the date when the app will be installed:
  - Select **Now** for an immediate execution.
  - Select **Date** and then enter a date and a time for a scheduled execution.

5. Click **Finish**.

The selected app is installed onto the selected devices at the specified date.

On supervised iOS devices and on Android devices with the Sophos Samsung Plugin app installed, apps are installed silently, that is without user interaction.

## 16.3 Uninstall app

**Note:** This section only applies to Android and iOS devices.

When you have added an app to Sophos Mobile Control as described in [Add app](#) (page 180), you can manually uninstall it from selected devices or device groups.

1. On the menu sidebar, under **CONFIGURE**, click **Apps** and then click **Android** or **Apple iOS**.
2. On the **Apps** page, click **Uninstall**.
3. Select the devices from which you want to uninstall an app. Do one of the following:
  - Select individual devices.
  - Click **Select device groups** and then select one or more device groups.

When you are ready, click **Next**.

4. On the **Select app** page, select the required app.
5. On the **Set execution date** page, specify the date when the app will be uninstalled:
  - Select **Now** for an immediate execution.
  - Select **Date** and then enter a date and a time for a scheduled execution.
6. Click **Finish**.

The selected app is uninstalled from the selected devices at the specified date.

Managed apps on supervised iOS devices are uninstalled silently, that is without user interaction.

**Tip:** Alternatively, you can use the following procedure to uninstall an app from a single device: Open the device's **Show device** page, go to the **Installed apps** tab and then click the trash can icon next to the app name.

## 16.4 Managed apps for iOS

For iOS apps that you add to Sophos Mobile Control, you can choose to have the app installed as *managed* or *unmanaged* on the users' devices.

Managed apps have the following characteristics:

- When users select a managed app in the Enterprise App Store, an installation task is created and processed in Sophos Mobile Control. In contrast, when users select an unmanaged app, they are redirected to the Apple App Store to install the app from there.
- You can uninstall managed apps through the Sophos Mobile Control console. This is not possible for unmanaged apps.
- On supervised iOS devices, managed apps are installed and uninstalled silently, that is without user interaction.
- Certain settings in iOS device profiles are only available for managed apps.
- When an iOS device is unenrolled from Sophos Mobile Control, all managed apps are automatically removed from the device. Unmanaged apps will remain on the device.

The following rules determine if an app is installed managed or unmanaged:

- Apps that you install from the Sophos Mobile Control console are always managed.

- Apps that the user installs from the App Store are always unmanaged.
- Apps that the user installs from the Enterprise App Store are managed if you have activated the **SMC managed installation** setting in the app properties, as described in [Add app](#) (page 180).

To check the app status on a device, open the **Show device** page for that device and go to the **Installed apps** tab. See [The Show device page](#) (page 58).

**Tip:** If a user has installed an unmanaged app you can convert it into a managed app. To do this, configure the app in Sophos Mobile Control as managed, and then create an installation task for it. Because the app is already installed, it is not installed again, but its status changes from *unmanaged* to *managed*.

## 16.5 Manage apps purchased through Apple VPP

With the Apple Volume Purchase Program (VPP), you can buy iOS apps in volume for distribution within your company.

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

In Sophos Mobile Control, you can provide the licenses included in the *sToken* to users by inviting them to become authorized Apple VPP users. After users have accepted their invitation, they become authorized VPP users and you can assign VPP apps to them. Users can install assigned VPP apps onto their devices using iTunes.

You can also assign VPP apps to devices with iOS 9 or higher. You do not need to invite devices to VPP. You install an assigned VPP app on a device through Sophos Mobile Control.

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 the subsequent sections cover both.

For information on internal and external user management, see the [Sophos Mobile Control super administrator guide](#).

For detailed information on how to enroll and use Apple VPP, see <http://www.apple.com/business/vpp/>.

For detailed information on how to assign VPP apps to users or devices, see [Automatically assign VPP apps](#) (page 187) and [Manually assign VPP apps](#) (page 187).

### 16.5.1 Set up a VPP sToken

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

1. On the menu sidebar, under **SETTINGS**, click **Setup > System setup**.
2. On the **System setup** page, click the **Apple VPP** tab.
3. Click the **Apple iTunes VPP Portal** link.

This opens the Apple VPP web portal in a new browser window.

4. On that page, select **Business**.



5. In the **Business Store Sign In** dialog, enter your Apple ID and your password.
6. Go to the **Account Summary** page and click **Download Token**.  
The sToken is generated and saved to your local computer in a text file with extension `.vpptoken`, using the download settings of your web browser.
7. Optional: Move the sToken file to a location that you can access from the Sophos Mobile Control console.
8. Go back to the **Apple VPP** tab of the Sophos Mobile Control console, click **Upload a file**, select the sToken file and then click **Open**.  
Sophos Mobile Control reads in the file and populates the **Organization** and **Expiry date** fields from the sToken details.
9. In the **Automatically assign VPP apps on installation** list, you can configure the automatic assignment of VPP apps. See [Automatically assign VPP apps](#) (page 187).
10. Optional: Fill in the remaining fields of the **Apple VPP** tab.  
In the **Country** field, enter your two-letter country code, for example `us` for the United States.
11. Click **Save**.

**Note:** To notify when the sToken is about to expire, Sophos Mobile Control sends several email reminders to all administrators of the relevant customer, starting 30 days prior to the expiry date.

## 16.5.2 Invite users to Apple VPP

You need to set up an sToken before you can invite users to the Apple Volume Purchase Program (VPP). See [Set up a VPP sToken](#) (page 184).

1. On the menu sidebar, under **MANAGE**, click **Users**.
2. On the **Show users** page, you can invite all users or individual users to Apple VPP:
  - To invite all users:
    1. Click **Invite users to Apple VPP** at the top of the **Show users** page.
    2. Click **Yes** in the confirmation dialog box.
  - To invite a single user:
    1. Click the required user name.
    2. On the **Show user** page, click **Invite user to VPP**.
    3. Click **Yes** in the confirmation dialog box.
  - To invite a single user, when using external user management and the user has no devices enrolled yet:
    1. Click **Search and invite a user to Apple VPP** at the top of the **Show users** page.
    2. In the **Search user** dialog, search for the user either by name or by email address.
    3. In the search result list, select the user that you want to invite to Apple VPP.
    4. Click **Apply**.

Sophos Mobile Control sends an invitation email to all relevant users.

Users must follow the link in their invitation email to connect their Apple iTunes account with Apple VPP. Afterward, they can install and use the apps that are licensed by your company.

**Note:**

When you are using external user management and invite all users to Apple VPP, users that do not have an email address assigned will be registered for Apple VPP, but do not receive the link to connect their Apple iTunes account with Apple VPP.

For information on how to complete the VPP registration process in this case, see [Invite users without email address to Apple VPP](#) (page 186).

### 16.5.3 Invite users without email address to Apple VPP

**Prerequisite:** This procedure requires a super administrator account, so it does not apply to Sophos Mobile Control as a Service.

When you invite users from an external user directory to Apple VPP as described in [Invite users to Apple VPP](#) (page 185), users that do not have an email address assigned will be registered for Apple VPP, but will not receive the link to connect their Apple iTunes account with Apple VPP.

If this happens, perform the following steps to complete the Apple VPP registration process.

1. As Sophos Mobile Control super administrator, download the server log files.  
See the [Sophos Mobile Control super administrator guide](#).
2. Identify the affected user accounts from the log files.
3. On the menu sidebar of the Sophos Mobile Control console, under **MANAGE**, click **Users**.
4. On the **Show users** page, click one of the affected user names.
5. On the **Show user** page, click **Show invitation link**.  
For external users without email address, this function does not send an invitation email, but instead shows the invitation link in a message box.
6. Copy the link from the message box and communicate it to the user.
7. Repeat this for all affected users.

The users need to follow the link to connect their Apple iTunes account with Apple VPP.

### 16.5.4 Manage Apple VPP users

When you have set up an Apple VPP sToken as described in [Set up a VPP sToken](#) (page 184), the **Show user** page of each user includes an **Apple Volume Purchase Program (VPP)** section.

In this section, you can perform the following tasks to view or edit the Apple VPP status of the user:

- View the Apple VPP user status. This can be:
  - **Not registered:** The user has not been invited to Apple VPP.
  - **Registered:** The user has been invited to Apple VPP, but has not connected their Apple iTunes account with Apple VPP.
  - **Associated:** The user has connected their Apple iTunes account with Apple VPP and can install VPP apps.
- View the Apple VPP apps that the user has installed.
- Invite the user to Apple VPP by clicking **Invite user to VPP**.

In most cases, an email with an invitation link is sent to the user. If the user account does not contain an email address, an invitation link will be displayed in a message box.

- Send another invitation email if the user did not receive or lost the initial email, by clicking **Re-send invitation email**.
- Deregister the user from Apple VPP by clicking **Delete VPP registration**.

## 16.5.5 Automatically assign VPP apps

By default, apps that you purchased through the Apple Volume Purchase Program (VPP) are automatically assigned to the device on which the app is installed. If the device does not support the assignment of VPP apps, the app is assigned to the user that is assigned to the device.

**Note:** To support the assignment of VPP apps, the device must have the status *managed* and use iOS 9 or higher.

You can invert the order of precedence and favor user assignment over device assignment, or you can disable automatic assignment and instead assign VPP apps manually, as described in [Manually assign VPP apps](#) (page 187).

The automatic assignment of VPP apps is configured per customer.

1. On the menu sidebar, under **SETTINGS**, click **Setup > System setup**.
2. On the **System setup** page, click the **Apple VPP** tab.
3. In the list **Automatically assign VPP apps on installation**, select the desired option:
  - **Preferably to device:** If the device supports it, the VPP app is assigned to the device. Otherwise, the VPP is assigned to the user that is assigned to the device. If there is no user assigned to the device, app assignment will fail.
  - **Preferably to user:** If a user is assigned to the device, the VPP app is assigned to that user. Otherwise, the app is assigned to the device. If the device does not support it, app assignment will fail.
  - **Disabled:** VPP apps are not assigned automatically. If you select this option, VPP apps must be assigned manually.

## 16.5.6 Manually assign VPP apps

This section describes the manual assignment of individual VPP apps. By default, apps that you purchased through the Apple Volume Purchase Program (VPP) are automatically assigned to the device on which the app is installed. See [Automatically assign VPP apps](#) (page 187).

You can assign apps that you purchased through the Apple Volume Purchase Program (VPP) to users or to devices. After you assign a VPP app to users that are associated with Apple VPP, they can install it on all iOS devices that are associated with their Apple ID. After you assign a VPP app to devices, you can push it to the devices through Sophos Mobile Control.

To assign a VPP app to users or devices:

1. On the menu sidebar, under **CONFIGURE**, click **Apps > Apple iOS**.  
This opens the **Apps** page that displays a list of all apps that you have added to Sophos Mobile Control.

2. To add apps you purchased through Apple VPP to the app list, click **Import VPP apps**.  
This retrieves the app information from the Apple VPP server and creates app entries in Sophos Mobile Control, if required.
3. Click the blue triangle next to the VPP app you want to assign to users or devices and then click **Edit**.
4. On the **Edit iOS link** page, click **Show** next to the **VPP licenses** option.  
This opens the **VPP licenses** dialog.
5. To assign the app to one or more users, click **VPP users** and then select the required users.  
The list contains all users that are registered for or associated with Apple VPP.
6. To assign the app to one or more devices, click **Devices** and then select the required devices.  
The list contains all devices with iOS 9 or higher and status *Managed*.
7. Click **Apply** to confirm the changes and to close the **VPP licenses** dialog.
8. Click **Save** to save the changes and to synchronize the app assignment with the Apple VPP server.

**Tip:** To discard assignment changes that you made in the **VPP licenses** dialog, click **Apply** to close the dialog box and then click **Back** to leave the **Edit iOS link** page without saving the changes to the database.

To install the assigned app on a device:

- After the app is assigned to users, it is listed in the **Purchased** view of the iTunes app on their devices. The users can install it from there.
- After the app is assigned to devices, you can install it through Sophos Mobile Control. See [Install app](#) (page 182).

To deassign an app:

- Open the **VPP licenses** dialog box as described before and then clear the selection of the required users or devices.

**Note:** Because the status of VPP apps is managed by the Apple VPP server, it may take some time until changes that you make in Sophos Mobile Control are visible on the devices.

## 16.5.7 Synchronize VPP license information

For performance reasons, Sophos Mobile Control keeps a local copy of VPP license information. You can trigger Sophos Mobile Control to synchronize its VPP data with the Apple VPP server.

**Note:** You only need to synchronize the VPP data if the displayed license information for an app is incorrect.

1. On the menu sidebar, under **SETTINGS**, click **Setup > System setup** and then click the **Apple VPP** tab.
2. Click **Clear VPP cache**.

Sophos Mobile Control discards its local VPP information for the customer and synchronizes the data with the Apple VPP server.

**Note:** For information how to display the license information for a VPP app, see [Manually assign VPP apps](#) (page 187).

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

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 started. You can also configure settings for the app that will be deployed on the device during the 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. See [Per app VPN configuration \(iOS device profile\)](#) (page 132).
  - To define settings, you need to know the required parameter and the parameter type.
1. On the menu sidebar, under **CONFIGURE**, click **Apps** and then click **Apple iOS**.
  2. On the **Apps** page, click the blue triangle next to the required app and then click **Edit**.
  3. On the **Edit iOS link** or **Edit iOS package** page, click **Show** next to the **Settings and VPN** field.
  4. On the **Edit settings and VPN** page, select the required configuration from the **Per app VPN** list to define the VPN the app is supposed to connect to.
  5. To add managed settings, click **Create parameter**.
  6. In the **Configuration parameter** dialog, 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** list, select the parameter type: **String**, **Bool**, **Integer** or **Real**.
    - d) Click **Apply**.
 

The set of managed settings is displayed on the **Edit Settings and VPN** page.
  7. On the **Edit settings and VPN** page, click **Apply**.
  8. Click **Save**.

The selected per app VPN will be used when the app connects to VPN. The settings will be provided to the devices during the app installation.

## 17 App groups

In Sophos Mobile Control you create app groups to define list of apps for profiles, policies and compliance rules.

App groups are used in the following settings:

- In the **App Protection** configuration of Android device profiles.
- In the **App Control** configuration of Android device profiles.
- In the **Restrictions** configuration of Android device profiles, iOS device profiles and Knox container profiles.
- In the **App restrictions** configuration of Windows Mobile policies.
- In compliance rules to specify lists of allowed, forbidden and mandatory apps.

### 17.1 Create app group

1. On the menu sidebar, under **SETTINGS**, click **App groups** and then select the platform for which you want to create the group.
2. On the **App group** page, click **Create app group**.
3. On the **Edit app group** page, enter a **Name** for the new app group and then click **Add app**.
4. In the **Edit app** dialog box you can either select an app from a list or enter custom app data.
  - To select an app from a list, click **App list** and then select an app from the list of all apps that are currently installed on the managed devices for the platform you selected.
  - To enter custom app data for an Android app, click **Custom** and then configure the following information:
    - **App name**: An arbitrary name that is used to identify the app.
    - **Identifier**: The package name of the app. The package name can be retrieved from the app's URL in Google Play. For example for the Sophos Mobile Control Android app, the Google Play URL is <https://play.google.com/store/apps/details?id=com.sophos.mobilecontrol.client.android> and the package name is **com.sophos.mobilecontrol.client.android**.
  - To enter custom app data for an iOS app, click **Custom** and then configure the following information:
    - **App name**: An arbitrary name that is used to identify the app.
    - **Identifier**: The bundle ID of the app.

- To enter custom app data for a Windows Mobile app, click **Custom** and then configure the following information:
    - **App name:** An arbitrary name that is used to identify the app.
    - **Link:** The URL of the app in the Windows Store. For example, the Windows Store URL of the Sophos Mobile Control Windows app is <https://www.microsoft.com/en-us/store/apps/mobile-control/9nblggh0g04v>.
    - **GUID:** If you know the GUID of the app, you can enter it instead of the link. Otherwise, leave this field empty.
- 5. After you have selected an app from the list or entered custom app data, click **Add** to add it to the app group.
- 6. Optional: Add more apps to the app group.
- 7. When you are ready, click **Save** to save the app group.

## 17.2 Import app group

You can create an app group by importing a UTF-8 encoded comma-separated values (CSV) file with up to 10,000 apps.

**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 extension `.csv`.

**Tip:** A sample file with the correct column names and column order is available for download from the **Import apps** page.

To import apps from a CSV file and add them to an app group:

1. On the menu sidebar, under **SETTINGS**, click **App groups** and then select the platform for which you want to create the group.
2. On the **App group** page, click **Create app group**.
3. On the **Edit app group** page, enter a **Name** for the new app group and then click **Import apps**.
4. On the **Import apps** page, click **Upload a file** and then navigate to the CSV file that you have prepared.

The entries are read in from the file and are displayed.

5. If the data is not formatted correctly or is inconsistent, the file as a whole cannot be imported. In this case, follow the error messages that are displayed next to the relevant entries, correct the content of the CSV file accordingly and upload it again.
6. Click **Finish** to add the apps to the app group.
7. On the **Edit app group** page, click **Save**.

# 18 Corporate documents

**Note:** This feature requires an SMC Advanced license.

In Sophos Mobile Control, you can upload files for distribution to the devices of your users.

- Documents managed in Sophos Mobile Control are automatically added to the **Corporate Documents** store of Sophos Secure Workspace.
- In the **Corporate Documents** store on the device, the **Category** that can be defined for each document is shown as folder.
- If Sophos Secure Workspace is not managed by Sophos Mobile Control, the **Corporate Documents** store is not visible.
- Documents in **Corporate Documents** are read only. They cannot be edited in Sophos Secure Workspace and then uploaded again.

To distribute corporate documents:

1. Install the Sophos Secure Workspace app onto the devices. See [Apps](#) (page 180).
2. Assign a Sophos container policy with a **Corporate Documents** configuration.
3. Upload documents to Sophos Mobile Control.

## 18.1 Add corporate documents

**Prerequisite:** You have activated an SMC Advanced license.

To distribute documents to devices:

1. On the menu sidebar, under **CONFIGURE**, click **Documents**.

The **Documents** page is displayed.

2. Click **Add document**.

The **Edit document** page is displayed.

3. Enter a category for the document.
  - The **Category** is the name of the folder in which the document is displayed in the **Corporate Documents** store on the device.
  - Multiple files can have the same **Category**.
  - If you leave this field blank, the file will be shown in the root folder of **Corporate Documents**.



4. Define settings for the document:

- Select **Copy to clipboard** to allow users to copy the document to the clipboard.
- Select **Share document** to allow users to share the document.
- Select **Use document offline** to allow users to create a **Favorite** for the document.

When a plain document from **Corporate Documents** is marked as **Favorite**, it will be stored encrypted in the Sophos Secure Workspace app. When sharing the document is allowed, the encrypted favorite file will be decrypted automatically before it is forwarded to other apps. If you clear the **Use document offline** check box and users already have offline copies, the file stored in Sophos Secure Workspace **Favorites** on the managed devices will be removed automatically as part of the next synchronization.

5. Click **Show** next to **Assigned groups** and select the group that should have access to the document.

6. Add a description for the document.

7. Click **Upload a file** and navigate to the document. Select it and click **Open**.

The document file size must not exceed a certain limit.

For on-premise installations, the limit is configured by your super administrator. For Sophos Mobile Control as a Service, it is set to 5 MB per document.

8. Repeat this step for each document you want to distribute.

The document is added to the documents list. It is distributed to the users, who can view it in the Sophos Secure Workspace app.

## 19 Android for Work

Android for Work is a Google program to separate personal and corporate data on an Android device.

If you have registered your company with Android for Work, you can set up Sophos Mobile Control as a third-party EMM (*Enterprise Mobility Management*) provider for your Android for Work domain.

Android for Work supports different deployment scenarios. Sophos Mobile Control uses the BYOD (*bring your own device*) scenario:

- Users have to create a *work profile* on their devices.
- The work profile will be attached to the primary device profile, that is the personal profile, so that its content is available to the personal profile.
- Sophos Mobile Control manages the content of the work profile. It registers itself as the *profile owner*.
- When a device is enrolled with Android for Work, all the apps in the work profile, including the Sophos Mobile Control app, are marked with a briefcase badge.
- Users use the badged version of the Google Play Store app to install work apps from Google Play for Work.
- You can configure the content and layout of Google Play for Work using Sophos Mobile Control.

### 19.1 Set up Android for Work

You must initially set up Android for Work for a customer to enable the Android for Work features.

1. Register an Android for Work domain with Google.
2. Create an enterprise service account and configure the APIs that are required to communicate with the Google services.
3. Bind Sophos Mobile Control to your Android for Work domain.

#### 19.1.1 Register domain with Google

In the first stage of the setup procedure for Android for Work, you register a domain with Google (*Managed Google Domain*), create a domain administrator (*Managed Google Account*) and verify your domain ownership.

**Note:** If you already have a Managed Google Domain, for example because you have signed up for G Suite (formerly Google Apps), you can skip this section. Instead, enable Android for Work for your domain from the Google Admin console.

1. Click the following link [https://www.google.com/a/signup/?enterprise\\_product=ANDROID\\_WORK](https://www.google.com/a/signup/?enterprise_product=ANDROID_WORK) to sign up for Android for Work.

2. Fill the web form with the required information.
  - Under **About your business**, enter the domain that will be used as the Managed Google Domain in **Business domain address**. For example, you could use the domain of your Sophos Mobile Control server.
 

**Note:** If you want to configure Android for Work for more than one customer in Sophos Mobile Control, you need a separate domain for each customer.
  - Under **Your Google admin account**, enter the credentials for a new domain administrator.
 

**Note:** Make a note of the credentials as you will need them later in the setup procedure.
3. Click the button to create the domain administrator account.
 

This opens the setup page for Android for Work in the Google Admin console.

**Tip:** You can also access the setup page manually: Open the following web address <https://admin.google.com> and log in with the credentials of the domain administrator you've created.
4. In the Google Admin console, start the procedure to verify your domain ownership.
 

Follow the instructions provided by Google to verify your domain.

After your domain ownership is verified, you receive a token to connect your Android for Work domain with your third-party EMM provider, that is, with Sophos Mobile Control.

Next, you must create a Google service account and configure the relevant APIs for Android for Work. See [Configure Google service account](#) (page 195).

## 19.1.2 Configure Google service account

In the second stage of the setup procedure for Android for Work, you create and configure a *Google service account*.

**Prerequisite:** You have a domain administrator account for your Android for Work domain.

A Google service account is a special type of Google account for an application. This account is used by Sophos Mobile Control to communicate with the Google Android for Work API.

Create a project:

1. Click the following link <https://console.developers.google.com/apis/library> to open the Google API console. Log in with the credentials of your domain administrator account.
2. In the header bar of the Google API console, click **Project > Create project**.
 

If you already have a project, the header bar shows the project name instead of the word *Project*.
3. In the **New project** dialog, enter a project name, for example **Android for work**, and then click **Create**.

Enable the required APIs:

4. On the menu sidebar, click **Library**, and then enter the string **admin sdk** in the search field.
5. In the search result list, click **Admin SDK**.
6. At the top of the **Admin SDK** page, click **Enable**.

7. Click **Library** again and repeat the previous three steps for the **Google Play EMM API**.  
This time, use `emm` as a search string.

Create a service account:

8. On the **Google Play EMM API** page, click **Go to Credentials**.
9. In step one of the **Add credentials to your project** page, click the **service account** link.
10. On the **Service Accounts** page, click **Create Service Account**.
11. In the **Create service account** dialog box, enter the following settings:
  - a) In **Name**, enter a name to identify the service account, for example **Android for Work**.
  - b) Select **Furnish a new private key** and then select **JSON**.
  - c) Select **Enable G Suite Domain-wide Delegation**.
  - d) In **Product name for the consent screen**, enter for example **Android for Work**.

When you click **Create**, the private key for your service account is generated and saved to your computer in a JSON file.

**Note:** Store the JSON file in a secure location. You need it to bind Sophos Mobile Control to your Android for Work domain.

Configure API access:

12. Click the following link <https://admin.google.com> to open the Google Admin console and log in with the credentials of your domain administrator account.
13. Click **Security** and then click **Advanced settings**.  
**Tip:** You may need to click **Show more** to display **Advanced settings**.
14. Click **Manage API client access**.
15. Open the JSON file in a text editor and copy the `client_id` value into the **Client Name** field.  
For example, if your JSON file contains a line

```
"client_id": "123456789",
```

then enter `123456789` in the **Client Name** field.

16. In the **One or more API Scopes** field, enter the following two URLs, separated by a comma:

```
https://www.googleapis.com/auth/admin.directory.user,  
https://www.googleapis.com/auth/androidenterprise
```

17. Click **Authorize**.

You can now bind Sophos Mobile Control to your Android for Work domain. See [Bind Sophos Mobile Control to your domain](#) (page 197).

### 19.1.3 Bind Sophos Mobile Control to your domain

In the third stage of the setup procedure for Android for Work, you bind Sophos Mobile Control to your Android for Work domain.

**Prerequisites:**

- You have a domain administrator account for your Android for Work domain.
  - You have verified your domain ownership.
  - You have enabled the Android for Work APIs.
  - You have created a service account for Android for Work.
1. Log in to the Sophos Mobile Control console. Use an administrator account for the customer for which you want to set up Android for Work.
  2. On the menu sidebar, under **SETTINGS**, click **Setup > General**, and then click the **Android** tab.
  3. Under **Android for Work**, click **Configure**.
  4. In the dialog box that opens, configure the following settings:

<b>Business domain</b>	Your Android for Work domain that has been verified by Google.
<b>Domain administrator</b>	The name of your domain administrator account. This is the administrator that you created when you registered your Android for Work domain with Google.
<b>EMM token</b>	The token that you received from Google after you verified your domain ownership.  You can view the token when you log in to the Google admin console ( <a href="https://admin.google.com">https://admin.google.com</a> ) with your domain administrator credentials and navigate to <b>Security &gt; Android for Work settings</b> .

5. Click **Upload a file** and then navigate to the JSON file that you downloaded from Google when creating the service account for Android for Work.
6. Click **Bind**.
7. On the **Android** tab, click **Save**.

Sophos Mobile Control contacts the Google web service to bind itself as an EMM provider to your Android for Work domain.

In the final stage of the setup procedure for Android for Work, you must configure the Google EMM settings. See [Configure EMM settings](#) (page 198).

## 19.1.4 Configure EMM settings

In the final stage of the setup procedure for Android for Work, you configure the Google EMM settings.

**Prerequisite:** You have bound Sophos Mobile Control to your Android for Work domain.

1. Click the following link <https://admin.google.com> to open the Google Admin console and log in with the credentials of your domain administrator account.
2. Click **Security** and then click **Manage EMM provider for Android**.

**Tip:** You may need to click **Show more** to display **Manage EMM provider for Android**.

3. Under **General Settings**, select **Enforce EMM policies on Android devices**.

This completes the setup procedure for Android for Work.

## 19.2 Configure Android for Work

To enable your users to enroll their devices with Android for Work, you must complete the following configuration tasks:

1. Create an Android for Work policy and configure at least one **Restrictions** configuration. See [Configurations for Android for Work policies](#) (page 95).
2. Create a task bundle that is transferred to a device when a user enrolls with Android for Work on the Self Service Portal. The task bundle must contain at least an **Enroll** task and an **Install profile or assign policy** task for an Android for Work policy. You may use different task bundles for corporate and private devices. See [Create task bundle](#) (page 172).
3. In the Self Service Portal setup, decide whether enrollment with Android for Work is optional or mandatory when users enroll a device with Sophos Mobile Control. See [Configure Android for Work device enrollment](#) (page 198).

### 19.2.1 Configure Android for Work device enrollment

Your users enroll their devices with Android for Work through the Self Service Portal. In Sophos Mobile Control, you configure whether enrollment with Android for Work is optional or mandatory, and which task bundles are transferred to the devices.

#### **Prerequisites**

- You have configured Android for Work for the customer.
- You have created a task bundle for the Android for Work device enrollment. The task bundle must contain at least an **Enroll** task and an **Install profile or assign policy** task for an Android for Work policy. You may use different task bundles for corporate and private devices.

1. On the menu sidebar, under **SETTINGS**, click **Setup > Self Service Portal**, and then click the **Group settings** tab.

2. Click the blue triangle next to the Self Service Portal group for which you want to configure the Android for Work device enrollment, and then click **Edit**. Or create a new group.  
The Self Service Portal group must be configured for the Android platform.  
For details on the Self Service Portal configuration, see [Configure Self Service Portal settings](#) (page 25).
3. In at least one of the columns **Initial package - corporate devices** and **Initial package - personal devices**, you must select a task bundle to be executed on corporate and personal devices.
4. Set whether enrollment is required or not in **Android for Work - corporate devices** and **Android for Work - personal devices**.
  - **Optional:** Users can choose to enroll with Android for Work when they enroll their devices with Sophos Mobile Control.
  - **Required:** Enrollment with Android for Work is mandatory.
5. Click **Apply**.
6. In the **Group settings** tab, click **Save**.

## 19.3 Manage Android for Work users

A user must have a *Managed Google Account* to enroll a device with Android for Work. This Android for Work account is connected to the domain that you registered with Google.

Android for Work account names are formed like an email addresses, for example `user@your_android_for_work_domain`.

When a user enrolls a device with Android for Work on the Self Service Portal, Sophos Mobile Control checks if an Android for Work account for the user already exists on the Google server. For this, the left part of the user's email address in Sophos Mobile Control is combined with your Android for Work domain. If an account with that name does not exist, Sophos Mobile Control creates it.

**Example:** If the user's email address in Sophos Mobile Control is `user@your_company.com` and your Android for Work domain is `your_android_for_work_domain`, Sophos Mobile Control checks the Google server for an account `user@your_android_for_work_domain`.

Other than creating an Android for Work account during enrollment, Sophos Mobile Control does not manage the account lifecycle. If you delete the user account in Sophos Mobile Control, the user's Android for Work account remains.

You can manage the Android for Work accounts for your domain from the Google Admin console. If required, you can create Android for Work accounts from your LDAP directory, using Google Apps Directory Sync (GADS).

## 19.4 Enroll devices with Android for Work

Your users enroll their devices with Android for Work during the enrollment with Sophos Mobile Control through the Self Service Portal. Enrollment with Android for Work through the Sophos Mobile Control console is not possible.

However, you can unenroll a user's device from Android for Work through the Sophos Mobile Control console, for example to delete corporate data from the device in case of lost or theft.

**Note:** Sophos Mobile Control supports the enrollment with Android for Work for devices with Android 6 or higher.

## 19.5 Lock work profile

For devices that are enrolled with Android for Work, you can lock or unlock the work profile. When the work profile is locked, all work apps are unavailable and no notifications are displayed for work apps.

**Tip:** Users can lock the work profile from the Quick Settings panel on their device, for example when they are on leave.

1. On the menu sidebar, under **MANAGE**, click **Devices**.
2. Click the blue triangle next to the device for which you want to lock or unlock the work profile and then click **Show**.
3. Click **Actions > Set container access**.
4. Select the access permissions.
  - **Deny:** The work profile is locked. Users can no longer access apps or data within the work profile.
  - **Allow:** The work profile is unlocked.
  - **Auto mode:** The work profile is locked if the device violates a compliance rule that contains a **Lock container** action. This is the default behavior if you have not set an access permission.
5. Click **Yes**.

The device is synchronized with the Sophos Mobile Control server. Once this is complete the setting is applied to the device.

## 19.6 Remove work profile from device

For devices that are enrolled with Android for Work, you can remove the work profile. For example to delete corporate data from the device in case of lost or theft.

When you remove the work from the device, all work apps, including the Sophos Mobile Control app, are also removed. In the Sophos Mobile Control console, the device is displayed with status *Unenrolled*.

1. On the menu sidebar, under **MANAGE**, click **Devices**.
2. Click the blue triangle next to the device from which you want to remove the work profile and then click **Show**.
3. Click **Actions > Wipe Android for Work**.

A task to remove the work profile is created and transferred to the device. You can display the task status on the **Task view** page.

**Note:** If the user has already removed the work profile manually, the task fails as the device cannot receive it anymore.



To re-enroll the device with Android for Work, the user must repeat the enrollment procedure on the Self Service Portal.

## 19.7 User-initiated work profile removal

Users can remove the work profile from their device, either accidentally or intentionally. Sophos Mobile Control is unable to detect this type of removal. It continues to display the device status as *Managed (Android for Work)*.

After the user has removed the work profile, the device cannot synchronize with the Sophos Mobile Control server.

**Tip:** You can use the **Devices not synchronized in last 7 days** report to identify potentially affected devices.

If the work profile was removed accidentally, you can re-enroll the device with Android for Work:

1. You delete the device from Sophos Mobile Control.
2. The user repeats the enrollment procedure through the Self Service Portal.

## 19.8 Work apps

Work apps are apps that are compatible with Android for Work.

You use Google Play for Work to select the work apps that are available to your Android for Work users. Your users install these apps through the Google Play Store app in their work profile.

You must perform the following tasks in Google Play for Work and in Sophos Mobile Control to make work apps available to your users:

1. In Google Play for Work, you select the apps for your Android for Work domain. To do this:
  - Approve the app.
  - Purchase app licenses.
  - Accept the app permissions.See [Approve work app](#) (page 201).
2. In Sophos Mobile Control, you configure the app. To do this:
  - Define the location of the app in the Google Play Store app on the users' devices.
  - For apps that support it, configure custom app settings.
  - For paid apps, assign users a license for the app.See [Edit work app](#) (page 202).

### 19.8.1 Approve work app

1. Open the Google Play for Work Store (<https://play.google.com/work>) and log in with your Google administrator account.
2. In the Google Play for Work Store, select the app you want to make available to your users.

3. Either click **Approve** (for free apps) or **Buy** (for paid apps).

**Note:** Paid apps for Android for Work are currently only available in the United States and in Canada.

4. If the app requires permissions, accept these on behalf of your company.  
When your users install that app, they are not asked to grant permissions.
5. For paid apps, enter the number of licenses and the payment method.

**Note:** If you receive an error when trying to buy an app, check in the Google Admin console that Google payment services are enabled for your domain or your account.

At this stage, the app is approved for your domain but users are not able to install it yet. You must complete the allocation process in Sophos Mobile Control. See [Edit work app](#) (page 202).

**Note:** If an update to your work app includes additional app permissions, you must accept these before your users can install the update. In the Google Play for Work menu, click **Update** to view and approve pending updates.

## 19.8.2 Edit work app

After you have approved an app in the Google Play for Work Store, you must configure the app in Sophos Mobile Control to make it available to your Android for Work users.

1. On the menu sidebar, under **CONFIGURE**, click **Apps** and then click **Android**.
2. On the **Apps** page, click **Android for Work apps**.  
This opens the **Android for Work apps** page that displays a list of all work apps that you have approved in the Google Play for Work Store.
3. Click **Retrieve app list from Google** to synchronize the changes you made in the Google Play for Work Store. After synchronization, users can install the apps through the Google Play Store app in their work profile.
4. Click the blue triangle next to the required app and then click **Edit**.
5. Use the **Page** and **App category** fields to define the location of the app in the Google Play Store app on the users' devices:
  - a) In the **Page** list, select the page in which the app will appear. The page items are pre-configured by Sophos Mobile Control and cannot be changed.
  - b) In the **App category** field, enter the name of a category in which the app will appear.  
When you start to type in the **App category** field, a list of matching categories is displayed. If you enter a category that is not available, it is created.
6. For paid apps, the **Edit Android for Work app** page contains a **Licenses** field. Click **Show** next to the **Licenses** field to view or edit the license information for the app.  
It may take a few seconds before Sophos Mobile Control retrieves the license information from Google.
  - a) In the **Licenses** dialog, you can see the number of used and remaining licenses for the app, and the Android for Work users that have a license assigned.
  - b) Select users to assign them a license for the app, or deselect users to remove their license. Click **Apply** to close the **Licenses** dialog.

7. If the app offers managed configuration, the **Edit Android for Work app** page contains an **App settings** button. Click that button to view or edit the available app settings.  
For information on the available settings, see the documentation that is provided by the app developer.
8. On the **Edit Android for Work app** page, click **Save** to save your changes.
9. On the **Android for Work apps** page, click **Send configuration to Google** to send the updated layout information and app configuration to Google.

**Note:** If you skip this last step, the app configuration is only stored locally in Sophos Mobile Control. It is not transferred to the Google server and is not available to your users.

After the data is synchronized to the Google server, the work app is available through the Google Play Store app in the work profile. Free apps are available to all of your users, while paid apps are only available to users that have a license assigned.

### 19.8.3 Work app settings

Setting/Field	Description
<b>Title</b>	The external app name as displayed in the Google Play for Work Store.
<b>Product ID</b>	The internal app name.
<b>Pricing</b>	The pricing type: <ul style="list-style-type: none"> <li>▪ <b>Free</b></li> <li>▪ <b>Free with in-app purchases</b></li> <li>▪ <b>Paid</b></li> </ul>
<b>Distribution type</b>	<ul style="list-style-type: none"> <li>▪ <b>Public (Google-hosted):</b> The app is available to the general public in Google Play for Work.</li> <li>▪ <b>Private (Google-hosted):</b> The app is developed by you and only available to users within your Android for Work domain. The APK file was uploaded to Google Play for Work.</li> <li>▪ <b>Private (self-hosted):</b> Like <b>Private (Google-hosted)</b>, but the APK file is installed from your local server. Google Play for Work is only used to manage the distribution.</li> </ul>
<b>Google Play for Work URL, Google Play URL</b>	The web address of the app in Google Play for Work and Google Play.  Click the link to open that page in a new browser window.

Setting/Field	Description
<b>Page</b>	The page on which the app will appear in the users' Google Play Store app. The values are pre-configured by Sophos Mobile Control and cannot be changed.
<b>App category</b>	The name of a category under which the app will appear in the users' Google Play Store app.
<b>Licenses</b>	Click <b>Show</b> next to <b>Licenses</b> to view or edit the license information for the app. This setting is only available for paid apps.
<b>App settings</b>	Click <b>App settings</b> to view or edit app-specific settings. For information on the available settings, see the documentation provided by the app developer. This setting is only available if the app offers managed configuration.

### 19.8.4 Install work app

After you have approved a work app in Google Play for Work and have assigned app licenses to your users, you can install the app to selected devices or device groups.

**Note:** Users can install approved apps through the Google Play Store app in their work profile.

1. On the menu sidebar, under **CONFIGURE**, click **Apps** and then click **Android**.
2. On the **Apps** page, click **Android for Work apps**.
3. Click the blue triangle next to the required app and then click **Install**.
4. Select the devices on which you want to install the app. Do one of the following:
  - Select individual devices.
  - Click **Select device groups** and then select one or more device groups.

When you are ready, click **Next**.

5. On the **Set execution date** page, specify the date when the app will be installed:
  - Select **Now** for an immediate execution.
  - Select **Date** and then enter a date and a time for a scheduled execution.
6. Click **Finish**.

The installation task is sent to a Google service. Google then manages the installation of the app onto the device. On the **Task view** page, the state of the task is **successful** when it has been sent to Google.

## 19.8.5 Uninstall work app

You can uninstall a work app from selected devices or device groups.

1. On the menu sidebar, under **CONFIGURE**, click **Apps** and then click **Android**.
2. On the **Apps** page, click **Android for Work apps**.
3. On the **Android for Work apps** page, click **Uninstall**.
4. Select the devices from which you want to uninstall an app. Do one of the following:
  - Select individual devices.
  - Click **Select device groups** and then select one or more device groups.

When you are ready, click **Next**.

5. On the **Select app** page, select the required app.
6. On the **Set execution date** page, specify the date when the app will be uninstalled:
  - Select **Now** for an immediate execution.
  - Select **Date** and then enter a date and a time for a scheduled execution.
7. Click **Finish**.

A task to uninstall the app is sent to a Google service. Google then manages the removal of the app from the device. On the **Task view** page, the state of the task is **successful** when it has been sent to Google.

**Tip:** Alternatively, you can use the following procedure to uninstall an app from a single device: Open the device's **Show device** page, go to the **Installed apps** tab and then click the trash can icon next to the app name.

## 19.8.6 Licenses for work apps

By assigning licenses for paid work apps to users, you define which apps are available to a user.

You only assign licenses for paid work apps to users. Free apps that you have approved in Google Play for Work are automatically available to all of your users after you synchronize the app list from Google to Sophos Mobile Control.

**Tip:** You do not need to assign a license for administrator-initiated app installations. When you install a work app as described in [Install work app](#) (page 204), a license from your pool of purchased licenses will automatically be assigned to the relevant users.

You configure the license assignment on the **Edit Android for Work app** page. See [Edit work app](#) (page 202).

## 19.8.7 Layout of Google Play for Work

You can define the location of each work app in the Google Play Store app on the users' devices.

The configurable layout elements are **Pages** and **Categories**.

- **Pages** are named, vertically scrollable views. Pages and their names are pre-defined by Sophos Mobile Control.

- **Categories** are named, horizontally scrollable subsections of a page that you define. In the Google documentation, categories are also called *clusters*.
- Each category is specific to a certain page, and each app appears within a certain category.
- Pages that do not contain any apps are not displayed.
- You can configure up to 30 categories per page and up to 100 apps per category.

For each app, you define the page and, optionally, the category in which the app is displayed in the Google Play Store app on the users' devices. By default, apps are placed on a page named **Other**.

You configure the store layout on the **Edit Android for Work app** page. See [Edit work app](#) (page 202).

### 19.8.8 Configurable work apps

A work app can offer a *managed configuration*. This feature is included by the app developer and allows you to configure custom settings for the app.

If an app supports managed configuration, a note **This app offers managed configuration** is displayed on the app's page in Google Play for Work.

You configure the app settings on the **Edit Android for Work app** page. See [Edit work app](#) (page 202).

### 19.8.9 Private and self-hosted work apps

All work apps that you want to make available to your users must be distributed through Google Play for Work.

- **Public work apps** are apps that are available to all users with an Google Play for Work account.
- **Private work apps** are apps developed by you that are only available to users inside your domain.
- **Self-hosted work apps** are private apps for which the application package (that is the APK file) is located on a server belonging to your organization instead of the Google server. However, the app store metadata for self-hosted apps must be uploaded to Google so that the app can be distributed through Google Play for Work.

For information on private work apps, see the [Android for Work Developer](#) web pages (external link).

## 20 Create administrators

1. On the menu sidebar, under **SETTINGS**, click **Setup > Administrators** to open the **Show administrators** page, and then click **Create administrator**.
2. On the **Edit administrator** page, configure the account details for the administrator.
  - When **External LDAP directory** is used as the user directory for the customer, you can click **Lookup user via LDAP** to select an existing LDAP account.
  - If you do not use an external user directory enter the relevant data for **Login name**, **First name**, **Last name**, **Email address** and **Password**.

The password that you specify is a one-time password. When the administrator logs in for the first time they are prompted to change it.

**Note:** The **Login name** only supports the following characters:

- Uppercase characters A-Z (Latin alphabet)
  - Lowercase characters a-z (Latin alphabet)
  - Digits 0-9
  - Special characters ! . \_ - #
3. In the **Role** list, select one of the available roles.

The role defines the type of access rights the new administrator will have to Sophos Mobile Control. See [User roles](#) (page 10).
  4. Click **Save** to create the administrator account.

The new administrator is created and shown on the **Show administrators** page. Forward the user credentials (user, customer and one-time password) to the new user. The new user can log in to the Sophos Mobile Control console and is prompted to change the password.

## 21 Send message to devices

You can send a custom message to managed devices.

**Note:** You can't send messages to Windows Desktop or Windows IoT devices.

1. On the menu sidebar, under **MANAGE**, click **Devices**.

The **Devices** page is displayed.

2. Select one or more devices, click **Actions** and then click **Send message**.

3. In the **Enter message** dialog, enter the message you want to send.

The message can contain up to 500 characters. Below the text field, the number of remaining characters is displayed.

4. Click **Finish**.



## 22 Advanced license

When you activate an SMC Advanced license, you can use these additional features:

- Manage the Sophos Secure Workspace and Sophos Secure Email apps. See [Manage Sophos container apps](#) (page 215).
- For Android devices, manage the Sophos Mobile Security app. See [Manage Sophos Mobile Security](#) (page 210).

After you have received your license key you need to activate the license.

### Activate an SMC Advanced license for on-premise installations

For on-premise installations of Sophos Mobile Control, licenses are managed by the super administrator in customer management. For further information, see the [Sophos Mobile Control super administrator guide](#).

### Activate an SMC Advanced license for Sophos Mobile Control as a Service

In the Sophos Mobile Control console, go to **SETTINGS > Setup > System setup > License** and enter your license key in the **Advanced license key** field.

## 23 Manage Sophos Mobile Security

**Note:** This feature requires an SMC Advanced license.

Sophos Mobile Security is a security app for Android devices that protects devices from malicious apps and assists users in detecting app permissions that could be a security risk. Its web filtering capability allows you to filter websites by category and lets you block inappropriate content.

You can manage the Sophos Mobile Security app on devices that are enrolled with Sophos Mobile Control as follows:

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

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

### 23.1 Configure antivirus settings for Sophos Mobile Security

**Prerequisite:** You have activated an SMC Advanced license.

1. On the menu sidebar, under **CONFIGURE**, click **Profiles, policies** and then click **Android**.

The **Profiles and policies** page is displayed.

2. Click **Create** and select **Mobile Security policy**.

The **Edit policy** page is displayed.

3. Enter a **Name** and a **Version** for the new profile.
4. In the **Description** field, enter a description for the profile.
5. Click **Add configuration**.

The **Available configurations** page is displayed.

6. Select **Antivirus** and click **Next**.

The settings view of the configuration is displayed.

7. Go to the **Antivirus** tab.

8. 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 on a foreign network.

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

9. 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 the default scanning of all installed apps.

10. Under **PUAs**, you can do as follows:

a) 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. PUAs include adware, dialers, system monitors, remote administration tools, and hacking tools. However, 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 device user accordingly.

b) Select **Enable user to allow PUAs** to enable users to allow apps although they have been identified as PUAs. The user can mark them as ignored. In subsequent scans, these apps will not be shown as PUAs.

11. Under **Apps with low reputation**, you can specify how to deal with these apps. Classification of apps is based on Sophos Live Protection data. Under **Mode**, you can do as follows:

a) Select **Allow** to turn off scanning for low reputation apps.

b) Select **Warn** to display a warning on the device when a low reputation app is detected. Users can then choose how to deal with the app. They can add it to a list of allowed apps so that no further warning is displayed if this app is detected.

c) Select **Block** in order to prevent low reputation apps from being started. A warning will be displayed but the user cannot start the app.

12. Under **Live protection**, you can do as follows:

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

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

13. If your scan results include apps that should be allowed to start, you can add them to the list of allowed apps. Apps on this list will always be allowed to start. The apps will not be reported.

To identify such an app, you can use the scan results of Sophos Mobile Security. See [View Sophos Mobile Security scan results](#) (page 213). Before you can allow these apps to start on the devices, you must add them to an **App group**, as described in [App groups](#) (page 190).

14. To add allowed apps, select the **App group** containing the allowed apps.
15. Click **Apply**.

## 23.2 Configure web filtering settings for Sophos Mobile Security

**Prerequisite:** You have activated an SMC Advanced license.

The Sophos Mobile Security app protects you from browsing sites with malicious, undesirable or illegal content.

**Note:** Web filtering only works with the Android web browser or with Google Chrome.

1. On the menu sidebar, under **CONFIGURE**, click **Profiles, policies** and then click **Android**.

The **Profiles and policies** page is displayed.

2. Click **Create** and select **Mobile Security policy**.

The **Edit policy** page is displayed.

3. Enter a **Name** and a **Version** for the new profile.
4. In the **Description** field, enter a description for the profile.
5. Click **Add configuration**.

The **Available configurations** page is displayed.

6. Select **Web filtering** and click **Next**.

The **Web filtering** page is displayed.

7. In the **Filter malicious websites** field, specify whether you want to **Allow** access to malicious websites, **Warn** the user against malicious websites, or **Block** these sites.
8. Under **Filter websites by category**, specify for each category whether you want to **Allow** access to websites of this category, **Warn** the user against potential malicious, undesirable or illegal content, or **Block** websites of this category.

Websites are categorized based on data from SophosLabs. The data is updated constantly.

9. Under **Website exceptions**, you can define:

- a) **Allowed domains:** add domains or IP addresses that are allowed, even though the category they belong to is blocked.
- b) **Blocked domains:** add domains or IP addresses that are blocked, even though the category they belong to is allowed.

You can insert domain names or IP addresses. Examples: www.company.com, \*.company.com, 10.2.0.1, 10.2.0.1/24

10. Click **Apply**.

Users cannot change the settings that you specified in the Sophos Mobile Control.

## 23.3 Define Sophos Mobile Security compliance rules

**Prerequisite:** You have activated an SMC Advanced license.

You can configure compliance rules that relate to Sophos Mobile Security.

1. Add a new compliance rule or open an existing set for editing. For further information, see [Compliance rules](#) (page 41).
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.
4. In the **Denial of SMSec permissions allowed** list, select whether a denial of the required permissions results in a compliance violation.
5. In the **Malware apps allowed** list, select whether detected malware apps are allowed.
6. In the **Suspicious apps allowed** list, select whether detected suspicious apps are allowed.
7. In the **PUAs allowed** list, select whether detected PUAs (Potentially Unwanted Apps) are allowed.
8. After you have configured all required settings, click **Save**.

## 23.4 View Sophos Mobile Security scan results

**Prerequisite:** You have activated an SMC Advanced license.

1. On the menu sidebar, under **MANAGE**, click **Devices**.

The **Devices** page is displayed with all devices enrolled with Sophos Mobile Control for this customer.

2. Click the blue triangle next to the required device and then click **Edit** or click its name.

The **Show device** or the **Edit device** page 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. Under **Threat name**, you can click the links to display further information from Sophos Labs about the relevant threat.

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 rules.

## 23.4.1 Create a list of allowed PUAs and apps with low reputation

You can use the scan results to create a list of allowed apps. This list will be valid for all Android devices with the Sophos Mobile Security app installed for the customer you are logged on to.

1. Go to the **Scan results** tab of one of your scanned devices.

The non-clean packages are shown in a table. The **Threat name** column indicates whether the displayed package is a low reputation app, a PUA or malware. You can click the links to display further information on the relevant threat from SophosLabs.

Detected low reputation apps and PUAs have a blue check mark icon to the left of the package name. Only these apps can be added to the allowed apps list.

2. Click the blue check mark icon to add the app to the allowed apps list.
3. In the dialog box, click **Yes** to confirm the operation.

The app is added to the allowed apps list.

4. Repeat this step for all apps you want to add.
5. To view the list, go to **Settings** and click **General**.
6. Click **Show allow list**.

All apps you added are displayed. Apps on this list will be allowed to start on all managed devices. The apps are not reported anymore.

When you click **Clear allow list**, all entries in the list are deleted.

## 24 Manage Sophos container apps

**Note:** This feature requires an SMC Advanced license.

For better data separation on the managed devices, Sophos Mobile Control provides the Sophos container apps Sophos Secure Email and Sophos Secure Workspace:

- Sophos Secure Email is an app for Android and iOS devices that provides a secure container for managing your email, calendar and contacts.
- Sophos Secure Workspace is an app for Android and iOS devices that allows users to access encrypted files stored in the cloud. Files can be decrypted and viewed in a seamless way. Encrypted files can be handed over by other apps and uploaded to one of the supported cloud storage providers. Alternatively, the documents can be stored locally within the app.

With Sophos Secure Workspace, you can read files encrypted by SafeGuard Cloud Storage or SafeGuard Data Exchange. Both are modules of SafeGuard Enterprise or one of its different editions. They allow you to encrypt files using a local key. These local keys are derived from a passphrase that is entered by a user. You can only decrypt a file when you know the passphrase that was used to encrypt the file.

The Sophos container provides:

- Centrally defined password rules
- Password rules for all container apps
- Single-Sign-On for all container apps
- Sophos Secure Workspace document settings
- Sophos Secure Workspace browser settings
- Sophos Secure Email settings

You can manage the Sophos apps with Sophos Mobile Control as follows:

- You can configure settings for the Sophos container apps on all managed devices remotely and centrally in Sophos Mobile Control. See [Configurations for Sophos container policies for Android](#) (page 104) and [Configurations for Sophos container policies for iOS](#) (page 145).
- You can make sure that the Sophos container apps are installed on the devices. You can define this as a compliance rule.
- You can enable secure distribution of documents using the *Corporate Documents* storage provider. See [Corporate documents](#) (page 192).
- You can enable corporate keyring synchronization between the Sophos Secure Workspace app and Sophos SafeGuard Enterprise. This makes the keys from a user's SafeGuard keyring available in the Sophos Secure Workspace keyring. See [Enable corporate keyring synchronization](#) (page 217).

**Note:** In order to manage the Sophos container apps, they must be distributed using Sophos Mobile Control. If users already have an unmanaged version of Sophos Secure Workspace installed on their devices, they must uninstall it first and then install the managed version.

For further information on Sophos Secure Workspace, see the *Sophos Secure Workspace help*.

## 24.1 Reset Sophos container password

**Prerequisite:** You have activated an SMC Advanced license.

**Note:** This section applies to devices that have an assigned Sophos container policy.

You can reset the Sophos container password. This is useful, for example, when users forget their password. If you reset a Sophos container password, users will be asked to define a new container password.

1. On the menu sidebar, under **MANAGE**, click **Devices**.

The **Devices** page is displayed.

2. Click the device for which you want to reset the Sophos container password.

The **Show device** page is displayed.

3. Click **Actions**.

The **Actions** menu is displayed.

4. Click **Reset Sophos container password**.

5. In the dialog box, click **Yes** to confirm the operation.

The Sophos container password is reset. The user has to enter a new Sophos container password.

## 24.2 Lock and unlock the Sophos container

**Prerequisite:** You have activated an SMC Advanced license.

**Note:** This section applies to devices that have an assigned Sophos container policy.

You can lock or unlock the Sophos container, that is, set the access permissions for the Sophos container apps and for data within the Sophos container.

1. On the menu sidebar, under **MANAGE**, click **Devices**.

2. On the **Devices** page, click the blue triangle next to the device for which you want to lock or unlock the Sophos container and then click **Show**.

3. On the **Show device** page, click **Actions > Set Sophos container access**.

4. In the dialog box for setting the access permissions, select one of the following:

- **Deny:** The Sophos container is locked. Users can no longer use it.
- **Allow:** The Sophos container is unlocked.
- **Auto mode:** The Sophos container is locked as long as the device violates a compliance rule for which **Lock container** is activated. This is the default behavior if you have not set an access permission.

5. Click **Yes**.

The device is triggered to synchronize with the Sophos Mobile Control server. On synchronization, the setting is applied to the device.



## 24.3 Corporate keyring synchronization

Corporate keyring synchronization adds the following features to the Sophos Secure Workspace app:

- The keys from a user's SafeGuard Enterprise keyring are available in the Sophos Secure Workspace keyring (SSW keyring).
- Users of the app can then use the keys to decrypt and view documents, or encrypt documents.
- Users can continue to use local keys that were available in their SSW keyring when you enabled keyring synchronization.
- Users cannot create new local keys.
- For security reasons, the keys from the SafeGuard keyring are removed from a device when the Sophos container is locked.

### 24.3.1 Enable corporate keyring synchronization

#### Prerequisites:

- You use Sophos SafeGuard Enterprise 8.0.
- You have configured external user management for the Self Service Portal, using the same Active Directory user database that is configured in SafeGuard Enterprise.
- Sophos Secure Workspace is managed by Sophos Mobile Control. This requires an SMC Advanced license.

To enable corporate keyring synchronization, you set up a connection between Sophos Mobile Control and Sophos SafeGuard Enterprise as follows:

1. On the menu sidebar, under **SETTINGS**, click **Setup > System setup**, and then click the **SGN** tab.
2. Click the **Certificate** link to download the certificate of the Sophos Mobile Control server.
3. Open SafeGuard Management Center and go to **Tools > Configuration Package Tool**.
4. On the **Servers** tab, click **Add**, browse for the certificate file and then click **OK**. Do not change the value of the **Server name** field.
5. Optional: Select **Recovery via mobile** to enable the synchronization of BitLocker and FileVault recovery keys with the Sophos Secure Workspace app.
6. On the **Managed client packages** tab, configure the following settings:
  - In the **Configuration Package Name** field, select **Managed Client (Default)**.
  - In the **Primary Server** field, select your SGN server.
  - In the **Transport Encryption** field, select **SSL**.
7. Click **Create Configuration Package**.
8. On the **SGN** tab of the Sophos Mobile Control console, click **Upload a file** to upload the configuration package that you created in the SafeGuard Management Center to Sophos Mobile Control.
9. Click **Save** to save the SafeGuard integration settings.

## 25 Glossary

<b>customer</b>	The tenant that manages devices.
<b>device</b>	The device to be managed (for example smartphone, tablet or Windows 10 device).
<b>enrollment</b>	The registration of a device with Sophos Mobile Control.
<b>Enterprise App Store</b>	An app repository that is hosted on the Sophos Mobile Control server. The administrator can use the Sophos Mobile Control console to add apps to the Enterprise App Store. Users can then use the Sophos Mobile Control app to install these apps onto their devices.
<b>provisioning</b>	The process of installing the Sophos Mobile Control app on a device.
<b>Self Service Portal</b>	The web interface that allows users to enroll their own devices and carry out other tasks without having to contact the helpdesk.
<b>SMC Advanced license</b>	With a license of type SMC Advanced you can manage the Sophos Mobile Security, Sophos Secure Workspace and Sophos Secure Email apps through Sophos Mobile Control.
<b>SMSec</b>	Abbreviation for Sophos Mobile Security.
<b>Sophos Mobile Control client</b>	The Sophos Mobile Control app that is installed onto the managed device.
<b>Sophos Mobile Security</b>	A security app for Android devices. You can manage this app with Sophos Mobile Control, provided that a license of type SMC Advanced is activated.
<b>Sophos Secure Email</b>	An app for Android and iOS devices that provides a secure container for managing your email, calendar and contacts. You can manage this app with Sophos Mobile Control, provided that a license of type SMC Advanced is activated.
<b>Sophos Secure Workspace</b>	An app for Android and iOS devices that provides a secure workspace where you can browse, manage, edit, share, encrypt and decrypt documents from various storage providers or distributed by your company. You can manage this app with Sophos Mobile Control, provided that a license of type SMC Advanced is activated.

**task bundle** You create a package to bundle several tasks into one transaction. You can bundle all tasks necessary to have a device fully enrolled and running.

**Sophos Mobile Control console** The web interface that you use to manage devices.

## 26 Technical support

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

- Visit the Sophos Community at [community.sophos.com/](https://community.sophos.com/) and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at [www.sophos.com/en-us/support.aspx](https://www.sophos.com/en-us/support.aspx).
- Download the product documentation at [www.sophos.com/en-us/support/documentation.aspx](https://www.sophos.com/en-us/support/documentation.aspx).
- Open a ticket with our support team at <https://secure2.sophos.com/support/contact-support/support-query.aspx>.

## 27 Legal notices

Copyright © 2011-2017 Sophos Limited. 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 Limited and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

Last update: 20170222