

SOPHOS

Security made simple.

Sophos Mobile Control startup guide

Product version: 6.1

Document date: September 2016



Contents

1	About this guide.....	4
2	About Sophos Mobile Control.....	5
3	Sophos Mobile Control licenses.....	7
3.1	Trial licenses.....	7
3.2	Upgrade trial licenses to full licenses.....	7
3.3	Update licenses.....	7
4	What are the key steps?.....	8
5	Log in as super administrator.....	9
6	Run the configuration wizard.....	10
7	Check your licenses.....	13
7.1	Activate SMC Advanced licenses.....	13
8	Create a customer.....	14
9	Switch to the customer.....	17
10	Create an administrator for the customer.....	18
11	Configure settings.....	19
11.1	Configure personal settings.....	19
11.2	Configure password policies.....	20
11.3	Configure technical support contact details.....	21
11.4	Configure Self Service Portal settings.....	21
12	Apple Push Notification service certificates.....	22
12.1	Requirements.....	22
12.2	Create and upload an APNs certificate.....	22
13	Compliance rules.....	24
13.1	Create compliance rules.....	24
14	Create device groups.....	27
15	Configure iOS devices.....	28
15.1	Create profiles for iOS devices.....	28
15.2	Create task bundles for iOS devices.....	29
16	Configure Android devices.....	31
16.1	Create profiles for Android devices.....	31
16.2	Create task bundles for Android devices.....	32
17	Update Self Service Portal settings.....	34

18	Create a Self Service Portal test user.....	35
19	Test device enrollment through the Self Service Portal.....	36
20	Import users into Sophos Mobile Control.....	37
21	Use the device enrollment wizard to assign and enroll new devices.....	38
22	Glossary.....	40
23	Technical support.....	42
24	Legal notices.....	43

1 About this guide

This guide explains how to initially configure Sophos Mobile Control step by step to manage your devices.

Further information is available in the [Sophos Mobile Control administrator help](#).

This guide focuses on Android and iOS as the most common mobile platforms. The settings apply to the other supported operating systems in a similar way.

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 on 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 Sophos Mobile Control licenses

Sophos Mobile Control offers two types of licenses:

- SMC Standard license
- SMC Advanced license

An SMC Advanced license adds functionality by enabling you to manage the Sophos Mobile Security, Sophos Secure Workspace and Sophos Secure Email apps.

For further information on managing Sophos Mobile Security, Sophos Secure Workspace and Sophos Secure Email through the Sophos Mobile Control web console, see the [Sophos Mobile Control administrator help](#).

As a super administrator, you can activate your purchased licenses in the super administrator customer and assign the required number of licensed users to individual customers.

3.1 Trial licenses

Sophos offers a free trial for Sophos Mobile Control. You can register for the trial on the Sophos website: <http://www.sophos.com/en-us/products/free-trials/mobile-control.aspx>.

A trial license allows you to manage up to five users and is valid for 30 days.

All you will need when you set up Sophos Mobile Control for evaluation is the email address you used to register when downloading the installer.

3.2 Upgrade trial licenses to full licenses

To upgrade trial licenses to full licenses you only have to enter your full license key in the Sophos Mobile Control web console. For further information, see the [Sophos Mobile Control administrator help](#).

3.3 Update licenses

To update your licenses you only have to enter the new license key in the Sophos Mobile Control web console. For further information, see the *Sophos Mobile Control super administrator guide*.

4 What are the key steps?

To start using Sophos Mobile Control:

1. Log in to the Sophos Mobile Control web console as a super administrator.
2. Start the configuration wizard to carry out initial configuration of the Sophos Mobile Control server.

Note: The configuration wizard includes an option to request a trial license.

3. Check your licenses.
4. Create a new customer for managing your devices.
5. Switch to the new customer.
6. Create an administrator for the new customer and log in to the web console as that administrator.
7. Configure personal settings, password policies for web console users, technical support contact details, and settings for the Self Service Portal.
8. Upload an Apple Push Notification service certificate.
9. Create compliance rules.
10. Create device groups.
11. Configure devices.
12. Update Self Service Portal settings and add a Self Service Portal test user.
13. If you use internal user management: Add users either by creating them or by uploading your user list.
14. If you use external user management: Configure the connection to your LDAP directory.
This is described in the *Sophos Mobile Control super administrator guide*.
15. Test device enrollment through the Self Service Portal.

5 Log in as super administrator

You must log in to the Sophos Mobile Control web console using the super administrator account that was configured during the installation of Sophos Mobile Control to perform some initial configuration steps.

1. Open the web console URL, that you configured during installation of Sophos Mobile Control, in your web browser.
2. In the login dialog, enter the super administrator customer name and the credentials of the super administrator, then click **Login**.

You are logged in as super administrator.

Note:

When you log in as a super administrator, you get a special version of the Sophos Mobile Control web console that is adapted to super administrator tasks.

For a detailed description of how to use the Sophos Mobile Control web console as a super administrator, see the *Sophos Mobile Control super administrator guide*.

6 Run the configuration wizard

When you log in to the Sophos Mobile Control web console for the first time after installation, a configuration wizard is started to configure certain server settings.

You need to provide:

- An SMC Standard license key, optionally an additional SMC Advanced license key
- SSL certificate(s)
- SMTP credentials
- HTTP proxy credentials (optional)

Note:

As a super administrator you can adjust these settings afterward on the **System setup** page of the Sophos Mobile Control web console. To open the **System setup** page from the menu sidebar, click **SETTINGS > Setup > System setup**.

To run the configuration wizard:

1. After you have logged in to the Sophos Mobile Control web console for the first time as super administrator, the **Welcome** view is displayed. Click **Next**.
2. If you use an HTTP proxy, configure the relevant server details in the **HTTP proxy** view:
 - a) Select **Proxy enabled**.
 - b) Enter the **Proxy host**.
 - c) Enter the **Proxy port**.
 - d) Click **Next**.

3. In the **License** view, enter your SMC Standard license key or request a trial license:

- **SMC Standard license key:**

When you enter the SMC Standard license key and click **Activate**, you are given the option to additionally enter an SMC Advanced license key. If you have purchased Advanced licenses, enter the key in **Advanced license key**.

- **Request a trial license:**

To request a trial license click **Request trial** and enter the email address you used when you registered to download the Sophos Mobile Control installer from www.sophos.com. Then click **Request trial** again.

Note: You can change the license settings at any time in the Sophos Mobile Control web console. If you do not enter an SMC Advanced license key here, you can do it in the web console later on.

Click **Next**.

4. In the **SSL** view, configure the certificates to be used for securing the SSL connection between the Sophos Mobile Control server and the clients.

You can configure up to four certificates because, depending on your network architecture, different certificates for clients connecting from the Internet or from your local intranet may be in use. The Sophos Mobile Control server will communicate the list of certificates to the clients. On establishing an SSL connection, the clients will only trust the server if the presented certificate is included in the list (*certificate pinning*).

a) Click **Auto-discover certificate(s)**.

In most cases the auto-discover function is sufficient to discover the certificates currently in use.

b) If the certificates cannot be discovered automatically, you can upload them manually by clicking **Upload a file** and selecting the relevant CER or DER file.

The certificates are displayed in the **SSL** view.

Important: Update the list when you have changed or renewed SSL certificates. At any given time, at least one valid certificate must be available. Otherwise the clients will not trust the server and will not connect to it.

5. In the **SMTP** view, configure the SMTP server information and logon credentials. SMTP must be configured to enable emails to be sent to new users, providing them with logon credentials. It also needs to be configured to enable enrollment through email.

Option	Description
SMTP Host	The SMTP server address.
Connection Type	Select SSL , TLS or plain .
SMTP user	If required by the SMTP server, enter the name of a user that is allowed to connect.
SMTP password	The password of the SMTP user.
Email originator	The email address that will appear in the <i>From</i> field of emails from Sophos Mobile Control.
Originator name	The author name that will appear in the <i>From</i> field. If required, you can configure a different originator name (but not email address) for each customer later on. See the Sophos Mobile Control administrator help .
Send error emails	Sophos Mobile Control will send error emails, for example when an APNs certificate expires.
Email recipients	Enter email addresses of the recipients that will receive error emails.

Note: Sophos Mobile Control does not support the OAUTH mechanism for SMTP authentication. Email providers that prefer OAUTH (like for example Google Gmail) might classify sign-in attempts from Sophos Mobile Control as insecure.

Sophos Mobile Control

6. After you have configured the relevant information, click **Send test email** to verify the email configuration.
7. Click **Save**.

7 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 end users (and unassigned devices) that can be managed from the web console.

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.
- **Licensed URL:** The URL of the Sophos Mobile Control server for which the license is issued.

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.

7.1 Activate SMC Advanced licenses

With SMC Advanced licenses you can use Sophos Mobile Control to manage the Sophos Mobile Security, Sophos Secure Workspace and Sophos Secure Email apps.

If SMC Advanced licenses have not been activated during the initial configuration of Sophos Mobile Control, the super administrator can activate them later from the Sophos Mobile Control web console:

1. On the menu sidebar, under **SETTINGS**, click **Setup > System setup**.
2. On the **License** tab, enter your license key in **Advanced license key** and click **Activate**.

When the key is activated, the license details are displayed.

8 Create a customer

You must be logged in to the Sophos Mobile Control web console as a super administrator to perform this task.

1. On the menu sidebar, under **INFORM**, click **Dashboard**.
2. Click **Create customer**.

3. On the **Edit customer** page, configure the following settings. All settings except the **Name** are optional.

Option	Description
Name	The customer's name.
Description	Text to describe the purpose of the customer account.
Maximum number of licenses	The number of end users and devices without an end user that can be managed for the customer.
Advanced licenses	If selected, the customer can use Sophos Mobile Control to manage the Sophos Mobile Security, Sophos Secure Workspace and Sophos Secure Email apps.
Valid until	The expiry date for the licenses that are assigned to the customer. After that date, you cannot create new tasks for devices that are managed for the customer.
Deactivate account	If selected, logging in to that customer is disabled. As super administrator, you can still switch to the customer's view, using the customer list on the system information bar. A deactivated account can be activated again by deselecting the Deactivate account check box.
Activated platforms	Select the platforms for which devices can be enrolled.
Locate devices	Select Allowed for users to enable users to locate their devices if they are lost or stolen. Select Allowed for administrators to enable administrators to locate devices.
Clone settings	Select the Settings and packages check box if you want all profiles, bundles, and packages created in the super administrator account to be available in the customer's account.
User directory	Select the data source for the Self Service Portal (SSP) users to be managed by Sophos Mobile Control. Choose from: <ul style="list-style-type: none"> • None. No SSP, user-specific profiles, or LDAP administrators available: This disables the creation of user accounts, and the lookup of web console accounts from an LDAP directory. • Internal directory: Use internal user management for SSP and web console accounts. For further information, see the Sophos Mobile Control administrator help. • External LDAP directory: In addition to internal user management, you can lookup SSP and web console accounts from an LDAP directory. Click Configure external LDAP to specify the server details.

4. Click **Save**.

The customer is created and displayed on the **Dashboard**.

9 Switch to the customer

To complete the initial configuration of the customer that you created in the previous section, you need to switch from the super administrator customer to that customer. This will change the web console view from the special view of the super administrator to the regular view.

To switch to the view of the new customer:

1. On the system information bar of the super administrator view, click the current customer name to open the list of available customers.
In that list, the super administrator customer is marked by an asterisk and shown at the top.
2. Select the customer you created in the previous section.

The Sophos Mobile Control web console view changes to the view of that customer, that is the view that you get when you log in with an administrator account for that customer.

10 Create an administrator for the customer

1. On the menu sidebar, under **SETTINGS**, click **Setup > Administrators**.
2. On the **Show administrators** page, click **Create administrator**.
3. On the **Edit administrator** page, configure the account details for the administrator.
 - When **External LDAP directory** is selected as the user directory for the customer, you can click **Lookup user via LDAP** to select an existing LDAP account.
 - When **Internal directory** or **None** is selected as user directory for the customer, 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. At first login, the administrator will be prompted to change it.
4. In the **Role** list, select the user role **Administrator**.
5. Click **Save** to create the administrator account.

To proceed with the configuration of the customer, log out from the web console and log in again, using the credentials of the administrator that you just created (customer name, login name, one-time password).

11 Configure settings

The following settings need to be configured:

- Personal settings, for example the platforms you want to manage
- Password policies
- Technical Support contact details
- Settings for the use of the Self Service Portal by end users

11.1 Configure personal settings

To use the Sophos Mobile Control web 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.

Prerequisite: You have logged in to the web console as the administrator you have created for the new customer.

1. On the menu sidebar, under **SETTINGS**, click **Setup > General**, and then click the **Personal** tab.

2. Configure the following settings:

Option	Description
Language	Select the language for the Sophos Mobile Control web console.
Timezone	Select the timezone in which dates are shown.
Unit of length	Select if you want to use metric or imperial units for length values.
Lines per page in tables	Select the maximum number of table lines you want to display per page in the web console.
Show extended device details	Select this check box to show all available information about the device. The Custom properties and Internal properties tabs will be added to the Show device page.
Activated platforms	<p>Select the platforms you want to manage for the customer:</p> <ul style="list-style-type: none"> • Android • iOS • Windows Mobile (includes Windows Phone 8.x and Windows 10 Mobile operating systems) • Windows Desktop <p>Based on your platform selection, the user interface of the web console will be adjusted. Only views and features that are relevant for the selected platforms are shown.</p> <p>Note: The list of available platforms depends on your platform settings from the super administrator configuration. For further information, see the <i>Sophos Mobile Control super administrator guide</i>.</p>

3. Click **Save**.

11.2 Configure password policies

To enforce password security, configure password policies for users of the Sophos Mobile Control web 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**.

11.3 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 will be 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**.

11.4 Configure Self Service Portal settings

1. On the menu sidebar, under **SETTINGS**, click **Setup > Self Service Portal**.
The **Self Service Portal** page opens.
2. On the **Configuration** tab, configure the Self Service Portal settings as required.
When you are not sure which settings to apply at this stage, we recommend that you use the default settings.
For a detailed description of the settings, click **Help** on the system information bar.
3. On the **Terms of use** tab, click **Edit** to enter a mobile policy, disclaimer or agreement text.
This text is displayed at the beginning of the device registration. Users have to accept the text before they can perform the registration.
Tip: You can use the editor toolbar to apply basic HTML formatting to the text. This also applies to the post-install text described in the next step.
4. Optional: On the **Post-install text** tab, click **Edit** to enter text that is displayed at the end of the device registration.
You can use this text to explain any steps the user has to perform after the registration.
5. Click **Save**.

12 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.

Sophos Mobile Control manages APNs certificates per customer. You must create and upload the certificates for each customer that you use.

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.

To facilitate the renewal of APNs certificates, the super administrator can in one step renew the certificates of all customers that use the same certificate. See the [Sophos Mobile Control administrator help](#).

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.

12.1 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)

12.2 Create and upload an APNs certificate

Use the APNs Certificate Wizard to create an Apple Push Notification service (APNs) certificate and to upload it to the Sophos Mobile Control server.

The wizard is available from [this Sophos support page](#). Alternatively, you can download the wizard from the Sophos Mobile Control web console. In the web console menu sidebar, under **SETTINGS**, go to the **Setup > System setup > iOS APNs** tab, then click the download link.

To create and upload an APNs certificate using the APNs Certificate Wizard:

1. Double-click the file `Sophos Mobile Control APNs Certificate Wizard.exe` to start the **APNs Certificate Wizard**.
2. On the **License Agreement** page, click **I Agree** to accept the license terms.

3. On the **Create Certificate Signing Request** page, enter your **Company Name** and your **Country** code (for example `US` or `UK`).

The certificate request is saved to a file with extension `.plist`. The file location is shown on the **Create Certificate Signing Request** page. Make a note of this information, then click **Next**.

4. On the **Upload PLIST** page, you will upload the certificate request file to Apple. Follow the instructions in the dialog:

- a) Click the displayed link <https://identity.apple.com/pushcert/> to open the Apple Push Certificates Portal in your web browser.

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.

- b) Log in with your Apple ID, or create an ID if you do not have one yet.

We recommend you create a corporate Apple ID and not a personal one.

- c) On the first page of the **Apple Push Certificates Portal**, click **Create a Certificate**.

- d) Accept the terms and conditions.

- e) Navigate to your `.plist` certificate request file and click **Upload**.

On the **Upload PLIST** page, you can click the `Upload to Apple` link to open the directory in which the `.plist` file has been created.

- f) Your APNs certificate is created as a file with extension `.pem`. Download the certificate file and save it in the `PEM from Apple` directory.

5. Click **Next**.

6. On the **Create P12** page, you will create your APNs certificate for Sophos Mobile Control. Enter a password for the APNs certificate. You need this password later, when you upload the `.p12` certificate file to Sophos Mobile Control.

The directory in which the certificate will be stored is shown on the **Create P12** page. Make a note of this information, then click **Next**.

Note: We recommend that you create a backup copy of that directory.

7. On the **Sophos Mobile Control APNs Certificate Wizard finished** page, click **Finish**.

8. On the **iOS APNs** tab of the Sophos Mobile Control web console, click **Upload a file**. Navigate to the `.p12` certificate file you have created and enter your password. Optionally you can also enter your Apple ID for future reference.

After the file has been uploaded successfully, a confirmation message is displayed and the **Topic**, **Type** and **Expiry date** information of your APNs certificate is shown.

9. Click **Save** to complete the procedure.

13 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.

13.1 Create compliance rules

To create a set of 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 will not be checked for compliance.
5. Under **Rule**, configure the compliance criteria 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.

For a description of the available rules for each device type, click **Help** on the system information bar.

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

Option	Description
Deny email	Forbid email access. This action can only be taken when you use the Sophos Mobile Control EAS Proxy server. See the <i>Sophos Mobile Control super administrator guide</i> .
Lock container	Disable the Sophos Secure Workspace and Secure Email apps. This affects document, email and web access that is managed by these apps. This action can only be taken when you have activated an SMC Advanced license. This option is only relevant for Android and iOS devices.
Deny network	Forbid network access. This action can only be taken if the super administrator has activated Network Access Control. See the <i>Sophos Mobile Control super administrator guide</i> .
Notify admin	Send compliance emails to selected recipients. 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.
Transfer task bundle	Transfer a specific task bundle to the device. We recommend that you set this to None at this stage. For further information, see the Sophos Mobile Control administrator help . Important: 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.

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.

To make use of a set of compliance rules, you assign it to a device group. This is described in the next section.

14 Create device groups

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

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

To create a new 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 auto-enrollment** option. This option allows you to enroll iOS devices with the Apple Configurator. For further information, see the [Sophos Mobile Control administrator help](#).

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

15 Configure iOS devices

15.1 Create profiles for iOS devices

In this step, you create a profile for initial configuration of Apple iOS devices.

We recommend that you set up separate profiles for:

- Password policies and restrictions
- Exchange ActiveSync settings (if required)
- VPN settings (if required)
- Wi-Fi settings (if required)
- Root and client certificates (if required)

Note:

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

- Create profiles directly in the web console.
- Import profiles created with Apple Configurator.

This section describes how to create profiles in the web console. For information on how to import profiles created with Apple Configurator, see the [Sophos Mobile Control administrator help](#).

To create an Apple iOS device profile for password policies and restrictions:

1. On the menu sidebar, under **CONFIGURE**, click **Profiles, policies > Apple iOS**.
2. On the **Profiles and policies** page, click **Create > Device profile**.
3. On the **Edit profile** page, configure the following settings:
 - a) **Name:** Enter a name for the profile. We recommend that you use the name `ios ssp profile` for profiles that are applied during enrollment through the Self Service Portal.
 - b) **Organisation:** Enter the name of the organization for the profile, for example a company name.
 - c) **Version:** Optionally, enter a version number for the profile.
 - d) **Description:** Enter a description for the profile, for example `base profile`.
 - e) **User can remove profile:** Select whether users are allowed to remove the profile from their device. Possible values are:
 - **Always**
 - **With authentication**
 - **Never**

We recommend that you select **Never**.

- f) **Automatically remove on**: Optionally, select a date for the automatic removal of the profile from the mobile devices.

We recommend that you do not set a date.

4. Click **Show** next to **Operating systems** and select the version of the operating system the profile applies to. Select all relevant iOS versions for this profile.

The list includes the iOS versions of already enrolled devices, and a generic version **iOS** that covers all supported iOS versions.

5. To add password policies to the profile, click **Add configuration**, select **Password policies** and click **Next**.
6. On the **Password policies** page, configure the required password settings.
For a detailed description of the settings, click **Help** on the system information bar.
7. Click **Apply** to save your settings.

The **Password policies** configuration is displayed on the **Edit profile** page under **Configurations**.

8. To add restrictions to the profile, click **Add configuration** again, select **Restrictions** and click **Next**.
9. On the **Restrictions** page, select the required restrictions.

Some restrictions require a certain device type or iOS version. These requirements are shown to the right of each restriction.

For a detailed description of the settings, click **Help** on the system information bar.

10. Click **Apply** to save your settings.

The **Restrictions** configuration is displayed on the **Edit profile** page under **Configurations**.

11. On the **Edit profile** page, click **Save** to save the profile.

The profile is displayed on the **Profiles and policies** page and is available for transfer onto Apple iOS devices.

If required, create additional profiles for Exchange ActiveSync settings, VPN settings, Wi-Fi settings and for the installation of root and client certificates.

15.2 Create task bundles for iOS devices

1. On the menu sidebar, under **CONFIGURE**, click **Task bundles > Apple iOS** to open the **Task bundles** page, and then click **Create task bundle**.

2. On the **Edit task bundle** page, configure the following settings:
 - a) **Name:** Enter a name for the task bundle. We recommend that you use the name `ios ssp task bundle` for task bundles that are applied during enrollment through the Self Service Portal.
 - b) **Version:** Optionally, enter a version number for the task bundle.
 - c) **Description:** Enter a description for the task bundle, for example `base ssp task bundle`.
 - d) **Selectable for compliance actions:** When you select this option, the task bundle can be loaded onto a device when the device breaks a compliance rule.
3. Click **Show** next to **Operating systems** and select the version of the operating system the task bundle applies to. Select all relevant iOS versions for this task bundle.

The list includes the iOS versions of already enrolled devices, and a generic version **iOS** that covers all supported iOS versions.
4. Click **Create task**, select **Enroll** and enter a name for the task. Click **Apply** to create the task. The name that you enter here will be displayed on the Self Service Portal while the task is processed.
5. Click **Create task** again and select **Install profile or assign policy**. Give the task a meaningful name, for example `Install password policies profile`, and select the profile you have created (`ios ssp profile`, if you have used the suggested name). Click **Apply** to create the task.
6. If you have configured profiles for Exchange ActiveSync, VPN or Wi-Fi settings, repeat the previous step for each profile.
7. If required, 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.
8. After you have added all required tasks to the task bundle, click the **Save** button on the **Edit task bundle** page.

The task bundle is displayed on the **Task bundles** page and is available for transfer onto Apple iOS devices.

16 Configure Android devices

16.1 Create profiles for Android devices

In this step, you create a profile for initial configuration of Android devices.

We recommend that you set up separate profiles for:

- Password policies and restrictions
- Exchange ActiveSync settings (if required)
- VPN settings (if required)
- Wi-Fi settings (if required)
- Root and client certificates (if required)

To create an Android device profile for password policies and restrictions:

1. On the menu sidebar, under **CONFIGURE**, click **Profiles, policies > Android**.
2. On the **Profiles and policies** page, click **Create > Device profile**.
3. On the **Edit profile** page, configure the following settings:
 - a) **Name:** Enter a name for the profile. We recommend that you use the name **Android SSP profile** for profiles that are applied during enrollment through the Self Service Portal.
 - b) **Version:** Optionally, enter a version number for the profile.
 - c) **Description:** Optionally, enter a description for the profile, for example **base profile**.
4. Click **Show** next to **Operating systems** and select the version of the operating system the profile applies to. Select all relevant Android versions for this profile.
The list includes the Android versions of already enrolled devices, and a generic version **Android** that covers all supported Android versions.
5. To add password policies to the profile, click **Add configuration**, select **Password policies** and click **Next**.
The **Password policies** page opens.
6. In **Password type**, select the type of password you want to define, for example **Complex**.
7. Configure the required password settings.
The available settings depend on the password type that you selected. For a detailed description of all settings, click **Help** on the system information bar.
8. Click **Apply** to save your settings.
The **Password policies** configuration is displayed on the **Edit profile** page under **Configurations**.
9. To add restrictions to the profile, click **Add configuration** again, select **Restrictions** and click **Next**.

10. On the **Restrictions** page, select the required restrictions.

Some restrictions require a certain device type or Android version. These requirements are shown to the right of each restriction.

For a detailed description of the settings, click **Help** on the system information bar.

11. Click **Apply** to save your settings.

The **Restrictions** configuration is displayed on the **Edit profile** page under **Configurations**.

12. On the **Edit profile** page, click **Save** to save the profile.

The profile is displayed on the **Profiles and policies** page and is available for transfer onto Android devices.

If required, create additional profiles for Exchange ActiveSync settings, VPN settings, Wi-Fi settings and for the installation of root and client certificates.

16.2 Create task bundles for Android devices

1. On the menu sidebar, under **CONFIGURE**, click **Task bundles > Android** to open the **Task bundles** page, and then click **Create task bundle**.
2. On the **Edit task bundle** page, configure the following settings:
 - a) **Name:** Enter a name for the task bundle. We recommend that you use the name **Android SSP task bundle** for task bundles that are applied during enrollment through the Self Service Portal.
 - b) **Version:** Optionally, enter a version number for the task bundle.
 - c) **Description:** Enter a description for the task bundle, for example **base SSP task bundle**.
 - d) **Selectable for compliance actions:** When you select this option, the task bundle can be loaded onto a device when the device breaks a compliance rule.
3. Click **Show** next to **Operating systems** and select the version of the operating system the task bundle applies to. Select all relevant Android versions for this task bundle.

The list includes the Android versions of already enrolled devices, and a generic version **Android** that covers all supported Android versions.
4. Click **Create task**, select **Enroll** and enter a name for the task. Click **Apply** to create the task.

The name that you enter here will be displayed on the Self Service Portal while the task is processed.
5. Click **Create task** again and select **Install profile or assign policy**. Give the task a meaningful name, for example **Install password policies profile**, and select the profile you have created (**Android SSP profile**, if you have used the suggested name). Click **Apply** to create the task.
6. If you have configured profiles for Exchange ActiveSync, VPN or Wi-Fi settings, repeat the previous step for each profile.
7. If required, 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.

8. After you have added all required tasks to the task bundle, click the **Save** button on the **Edit task bundle** page.

The task bundle is displayed on the **Task bundles** page and is available for transfer onto Android devices.

17 Update Self Service Portal settings

After you have created the task bundles to be transferred when users enroll their devices through the Self Service Portal, you need to update the Self Service Portal settings with the required group settings:

1. On the menu sidebar, under **SETTINGS**, click **Setup > Self Service Portal**, and then click the **Group settings** tab.
2. Click the **Default** group setting.

The **Edit group settings** dialog opens.

3. In the **Initial package - corporate devices** and **Initial package - personal devices** lists, select the task bundles you have created for Android and iOS devices.
4. Select the **Active** check box for the platforms that should be available on the Self Service Portal:
5. In the **Add to device group** list, select the group that devices will be added to when they are enrolled through the Self Service Portal.
6. Click **Apply**.
7. On the **Group settings** tab, click **Save**.

18 Create a Self Service Portal test user

To test provisioning through the Self Service Portal, create a Self Service Portal user account for yourself. You will use this account to log in to the Self Service Portal and test device enrollment.

Note: This procedure assumes that the customer was created with internal user management, see [Create a customer](#) (page 14). For information on external user management, see the *Sophos Mobile Control super administrator guide*.

To create a test user account for the Self Service Portal:

1. On the menu sidebar, under **MANAGE**, click **Users**, and then click **Create user**.
2. Configure the required account details.
Make sure that **Send welcome email** is selected.
3. Click **Save**.

The user is added to the list of Self Service Portal users and a welcome email is sent to the email address that you specified in the account details.

19 Test device enrollment through the Self Service Portal

We recommend that you test device enrollment through the Self Service Portal before you roll out Self Service Portal use to your users.

Log in to the Self Service Portal with the test user account you created for yourself in [Create a Self Service Portal test user](#) (page 35) and perform test enrollments for all platforms that you want to manage with Sophos Mobile Control.

For detailed information on how to use the Self Service Portal, see the [Sophos Mobile Control user help](#).

20 Import users into Sophos Mobile Control

After you have tested device enrollment through the Self Service Portal, you can import your user list into Sophos Mobile Control.

The import of users is only relevant for internal user management. For external user management, all users that are assigned to a certain LDAP group can log in to the system.

For information on external user management, see the *Sophos Mobile Control super administrator guide*.

You add new Self Service Portal users by importing a UTF-8 encoded comma-separated values (CSV) file with up to 300 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.

21 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.
- Assign the device to a user (optional).
- Enroll the device.
- Transfer an enrollment task bundle to the device (optional).

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
Platform	The device platform. You can only select a platform that is enabled for the customer that you logged in to.
Name	A unique name under which the device will be managed by Sophos Mobile Control.
Description	An optional description of the device.
Phone number	An optional phone number. Enter the number in international format, for example +491701234567 .
Email address	The email address to which the enrollment instructions will be sent.
Owner	Select the device owner: either Company or Employee .
Device group	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 Default , 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**. This will add the device to Sophos Mobile Control.

6. On the **Enrollment** wizard page, follow the instructions to install the Sophos Mobile Control app on 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.

22 Glossary

customer	The tenant that manages devices.
device	The device to be managed (for example smartphone, tablet or Windows 10 device).
end user	The end user of the device.
enrollment	The registration of a device with Sophos Mobile Control.
Enterprise App Store	An app repository that is hosted on the Sophos Mobile Control server. The administrator can use the web console to add apps to the Enterprise App Store. Users can then use the Sophos Mobile Control app to install these apps on their devices.
managed app	<p>An app installed by the Sophos Mobile Control server through any of the following methods:</p> <ul style="list-style-type: none">• Installation through a task bundle.• Manual installation from the web console.• Only for iOS devices, user-initiated installation from the Enterprise App Store, if the administrator has selected the SMC managed installation option.
provisioning	The process of installing the Sophos Mobile Control client on a device.
Self Service Portal (SSP)	The Sophos Mobile Control web interface that allows end users to enroll their own devices and carry out other tasks without having to contact the helpdesk.
SMC Advanced license	An SMC Advanced license adds functionality to a standard license by enabling you to manage the Sophos Mobile Security, Sophos Secure Workspace and Sophos Secure Email apps through Sophos Mobile Control.
SMSec	Abbreviation for Sophos Mobile Security used in the Sophos Mobile Control web console user interface.
Sophos Mobile Control client	The Sophos Mobile Control app that is installed on the managed device.

Sophos Mobile Security	A security app for Android devices. You can manage this app from Sophos Mobile Control, provided that an SMC Advanced license is available and activated in the Sophos Mobile Control web console.
Sophos Secure Email	An app for Android and iOS devices that provides a secure container for managing your email, calendar and contacts. You can manage this app from Sophos Mobile Control, provided that an SMC Advanced license is available and activated in the Sophos Mobile Control web console.
Sophos Secure Workspace	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 from Sophos Mobile Control, provided that an SMC Advanced license is available and activated in the Sophos Mobile Control web console.
task bundle	A package you can create in the web console to bundle several tasks into one transaction. You can bundle all tasks necessary to have a device fully enrolled and running.
web console	The web interface of the server that is used to manage devices.

23 Technical support

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

- Visit the Sophos Community at 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.
- Download the product documentation at 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>.

24 Legal notices

Copyright © 2011 - 2016 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.