

SOPHOS

Security made simple.

Sophos Mobile Control as a Service

Startup guide

Product version: 3.6

Document date: November 2013



Contents

1 About this guide.....	3
2 What are the key steps?.....	4
3 First login.....	5
4 Change your administrator user name.....	6
5 Activate Sophos Mobile Security license.....	7
6 Check your license.....	8
7 Configure general settings.....	9
8 Configure Self Service Portal settings.....	11
9 Create and upload an APNs certificate	12
10 Configure connections to standalone EAS Proxy Servers	14
11 Configure compliance rules.....	15
12 Create device groups.....	17
13 Configure iOS devices.....	18
14 Configure Android devices.....	21
15 Update Self Service Portal settings.....	23
16 Manage Self Service Portal users (end users).....	24
17 Technical support.....	29
18 Legal notices.....	30

1 About this guide

This guide tells you how to initially configure Sophos Mobile Control to manage your mobile devices.

Further information is available in the *Sophos Mobile Control administrator guide*.

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

1.1 Terminology

In this guide, the following terms are used:

Term	Explanation
Device	The mobile device to be managed (for example smartphone or tablet).
Sophos Mobile Control client	The Sophos Mobile Control client component that is installed on the device.
End user	The end user of the device.
Web console	The web interface of the server that is used to manage devices.
Provisioning	The process of equipping devices with the Sophos Mobile Control client.
Task bundle	A package you can create in the web console to bundle several tasks for mobile devices in one transaction. You can bundle all tasks necessary to have a device fully registered and running.
Self Service Portal (SSP)	The Sophos Mobile Control web interface that allows end users to register their own devices and carry out other tasks without having to contact the helpdesk.
Sophos Mobile Security	A security app for Android phones and tablets that can be managed from Sophos Mobile Control. The Sophos Mobile Security management functionality is an optional Sophos Mobile Control module. For managing the Sophos Mobile Security app from Sophos Mobile Control, a license needs to be available and activated in the Sophos Mobile Control web console.
SMSec	Abbreviation for Sophos Mobile Security used in the Sophos Mobile Control web console user interface.

2 What are the key steps?

To initially configure Sophos Mobile Control, you carry out the following steps:

1. Reset your password, log in to the Sophos Mobile Control web console and change your administrator user name.
2. Optional: Activate your Sophos Mobile Security license.

Note: Sophos Mobile Security management is an optional Sophos Mobile Control module. If you did not purchase a Sophos Mobile Security license, this step is not required.

3. Check your licenses.
4. Configure general settings (the platforms you want to use, password policies and technical contact information).
5. Configure settings for the use of the Self Service Portal by end users.
6. Create and upload Apple Push Notification service certificate.
7. Optional: Configure connections to standalone EAS Proxy Servers.
8. Configure compliance rules.
9. Create device groups.
10. Configure devices.
11. Update Self Service Portal settings, manage Self Service Portal users (that is end users) and test Self Service Portal provisioning.

Note: Sophos Mobile Control offers different methods for managing Self Service Portal users: internal and external user management. The configuration steps necessary depend on the user management method you choose. For further information, see [Manage Self Service Portal users \(end users\)](#) (section 16).

3 First login

For security reasons you have to reset your password on your first visit to the Sophos Mobile Control web console.

1. In the **Login** dialog of the web console, click **Forgot password?**

The **Reset password** dialog is displayed.

2. Enter your **Customer** and **User** information from the email you have received for the activation of your Sophos Mobile Control as a Service account and click **Reset**.

You receive an email with a link to reset your password.

3. Click the link.

The login dialog is displayed with a message that an email with a new password has been sent to you. This second email contains a randomly generated password.

4. Enter the password to log in.

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

5. Enter a new password. The new password must consist of 10 characters. There are no rules concerning special characters or digits.

Note: This is the default setting. You can modify the password policies in the Sophos Mobile Control web console and change your password according to the new policies. For further information, see [Configure password policies](#) (section 7.2).

4 Change your administrator user name

For security reasons we recommend that you change your administrator user name after first login.

1. In the Sophos Mobile Control web console menu bar, click **Administrators**.

The **Show administrators** view is displayed.

2. Click the **Edit** pencil icon next to the user **admin**.

The **Edit administrator** view is displayed.

3. In the **Login name** field, change your user name.

4. Enter your **Last name** and **First name**.

5. Enter your **Email** address.

6. Click the **Save** button.

Your user name is changed. Use the new name for the next login.

5 Activate Sophos Mobile Security license

Note: Sophos Mobile Security management is an optional Sophos Mobile Control module. If you did not purchase a Sophos Mobile Security license, this step is not required.

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

For managing the Sophos Mobile Security app from Sophos Mobile Control, a license needs to be available and activated in the Sophos Mobile Control web console.

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

The **System setup** view is displayed.

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

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

6 Check your license

Note: For Sophos Mobile Control and Sophos Mobile Security, a user-based license scheme applies. All devices assigned to one user count as one license. Devices without any user assignment are counted as one user.

In the web console menu bar, click **About** and check the license information shown in the **About** view:

■ SMC:

■ Number of user licenses:

Shows how many users you can manage with Sophos Mobile Control.

■ Licenses used:

Shows the number of licenses in use.

■ License valid until

Shows the license expiry date.

■ SMSec:

Note: Sophos Mobile Security management is an optional Sophos Mobile Control module. If you did not purchase and activate a Sophos Mobile Security license, the Sophos Mobile Security license information is not displayed.

■ Number of user licenses:

Shows the number of end users for which the Sophos Mobile Security app can be managed from the web console.

■ Licenses used:

Shows the number of licenses in use.

■ License valid until

Shows the license expiry date.

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

7 Configure general settings

The following settings need to be configured:

- The platforms you want to use
- Password policies
- Technical contact information to support users in case of questions or problems.

You configure these settings by using the **Settings** function.

7.1 Configure platforms

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 currently logged on user. You cannot deactivate any functions here.

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

The **General Settings** view is displayed.

2. In the **Personal** tab under **Activated platforms**, select the platforms you want to use with Sophos Mobile Control:

- Android
- iOS
- Windows Phone 8
- Windows Mobile

Note: This guide focuses on iOS and Android as the most common mobile platforms. For further information on all available platforms, see the *Sophos Mobile Control administrator guide*.

The menu is customized according to your settings. Unnecessary items are hidden.

3. Click the **Save** button.

7.2 Configure password policies

To enforce password security, configure password policies for users of the Sophos Mobile Control web console and the Self Service Portal. The password policies you define apply to new and changed passwords. There is a default policy that requires that passwords must contain 10 characters.

Note: The password policies only apply to Self Service Portal users managed by internal user management and administrator web console users. They do not apply to Self Service Portal users

managed by external user management. For further information about Self Service Portal user management methods, see [Manage Self Service Portal users \(end users\)](#) (section 16).

1. In the **General settings** view, go to the **Password Policies** tab.
2. Under **Password policies for SMC web console and SSP user - Rules**, define the required minimum values for the password.
3. Under **Password policies for SMC web console user and SSP user - Settings**, define the following settings:
 - **Password change interval (days)**: You can enter a value from **0** (no password change required) to **730** days.
 - **Number of previous passwords which must not be reused**: You can select a value between **1** and **10**.
 - **Maximum number of failed login attempts**: You can select a value between **2** and **10**.
4. Under **Reset password settings**, configure the emails to be sent to users after they have requested a password reset.
 - a) In the **Originator** field, enter the email sender address.
 - b) Under **Email with reset link**, the email subject and content is predefined. You can edit this according to your requirements. For further information, see the *Sophos Mobile Control administrator guide*.

Note: Do not remove the placeholder `_RESET_TOKEN_LINK_` from the email content.
 - c) Under **Email with new password**, the email subject and content is predefined. You can edit this according to your requirements. For further information, see the *Sophos Mobile Control administrator guide*.

Note: Do not remove the placeholder `_NEW_PASSWORD_` from the email content.
5. Click the **Save** button.

7.3 Configure technical contact

1. In the **General settings** view, go to the **Technical contact** tab.
2. Enter the required information for the technical contact. Under **Additional information**, you can enter any additional information for supporting users in case of questions or problems.
3. Click the **Save** button.

8 Configure Self Service Portal settings

You need to configure settings for the use of the Self Service Portal by end users.

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

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

2. In the **Configuration** tab, configure the Self Service Portal settings as required. For further information on all available settings, see the *Sophos Mobile Control administrator guide*. If you are not sure which settings to apply at this stage, you can also leave all options at their default settings.

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

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

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

- b) Under **Post install text**, you can enter a text to be displayed after the automatic installation steps in the Self Service Portal to give the user guidance for the next required steps, for example configuring the server in the iOS app or configuring the Android mail client.

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

4. Go to the **Welcome email** tab. In this tab, you configure the welcome email to be sent to Self Service Portal users to inform them about their logon credentials. This email is required to enable users to log in to the Self Service Portal.

Note: This email is only sent to Self Service Portal users managed by internal user management. For further information about Self Service Portal user management methods, see [Manage Self Service Portal users \(end users\)](#) (section 16).

5. In the **Originator** field, enter the email sender address. In the **Subject** field, an email subject is predefined. You can edit this according to your requirements.
6. In the text field, the email content is predefined. You can edit this according to your requirements. For further information, see the *Sophos Mobile Control administrator guide*.

Note: Do not remove the placeholders `_CUSTOMERNAME_`, `_LOGINNAME_` and `_RESET_TOKEN_LINK_` from the email content.

7. Click the **Save** button.

9 Create and upload an APNs certificate

To use the built-in Mobile Device Management (MDM) protocol of devices running Apple iOS 4 (or higher), Sophos Mobile Control must use Apple's Push Notification service (APNs) to trigger the iOS devices.

Prerequisites:

- You have configured the iOS platform, see [Configure platforms](#) (section 7.1).
- To create an APNs certificate, you use the APNs Certificate Wizard. The wizard is available for download in the web console. In the web console menu bar, go to **Settings**, click **System Setup** and go to the **iOS APNs** tab. To download the wizard, click the available download link.

1. Start the APNs Certificate Wizard by doubleclicking the file APNs Certificate Wizard.exe.

The APNs Certificate Wizard welcome dialog is shown.

2. Click **Next**.

The **License Agreement** dialog is displayed.

3. Click **I agree**.

The **Create Certificate Signing Request** dialog is shown.

4. Enter your **Company Name** and your **Country** code (for example US or UK). These fields are mandatory.

Note: Below these fields, the dialog shows where all data of the process is stored. Make a note of this information.

5. Click **Next**.

The **Upload PLIST** dialog is displayed.

6. In this step, you upload the Certificate Signing Request to Apple. Follow the instructions in the dialog:

- a) Open the Apple site indicated in the dialog in your browser.

Note: Do not use Internet Explorer to open the Apple site as this may cause problems. Use Firefox, Chrome or Safari instead. We recommend that you use the latest browser versions.

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

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

- d) Accept the terms and conditions.

- e) Browse for your Certificate Signing Request (*.plist) and click **Upload**.

You find the file name and the path in the **Upload PLIST** dialog of the Sophos APNs Certificate Wizard.

Your Apple push certificate is created.

- f) Download and save the certificate file (*.pem) in the directory indicated in the **Upload PLIST** dialog.

7. Click **Next**.

The **Create P12** dialog is displayed.

8. In this step, you 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.

Note: The **Create P12** dialog shows the directory the certificate will be stored in. Make a note of this information. We recommend that you create a backup of the folder that contains the certificate files.

9. Click **Next**.

The **Sophos Mobile Control APNs Certificate Wizard finished** dialog is displayed.

10. Click **Finish**.

11. In the web console menu bar, go to **Settings**, click **System Setup** and go to the **iOS settings** tab.

12. Browse for the .p12 certificate file you have created and enter your password. Optionally you can enter your Apple ID for future reference. Click **Upload**.

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

13. Click **Save**.

10 Configure connections to standalone EAS Proxy Servers

With Sophos Mobile Control you can set up an external EAS Proxy Server with several instances. Sophos Mobile Control offers a separate EAS Proxy installer for this purpose. For information on features and usage scenarios, see the *Sophos Mobile Control installation guide*. The EAS Proxy setup is available for download in the web console under **Settings > System Setup** in the **EAS Proxy** tab.

To configure connections to a standalone EAS Proxy Server, run the EAS proxy installer. For further information on the individual steps, see the *Sophos Mobile Control installation guide*. To complete the configuration, you need to upload the certificate generated during setup in the web console.

10.1 Upload EAS Proxy certificate

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

The **System setup** view is displayed.

2. Go to the **EAS Proxy** tab, browse for the certificate and click **Upload**.

The certificate is uploaded and shown in the **EAS Proxy** tab.

3. Click the **Save** button.

Note: The certificate needs to be uploaded before the EAS Proxy Server is started. Otherwise Sophos Mobile Control rejects the server and the service will not be started.

11 Configure compliance rules

In the web console, you can:

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

For further information, see the *Sophos Mobile Control administrator guide*.

1. In the web console menu bar, click **Compliance rules**.

The **Compliance rules** list view is displayed.

2. Click the **Add** button.

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

3. Enter a **Name** and a **Description** for the new compliance rule.

4. Go to the required device type tab.

5. Make sure that the **Enable platform** field is selected.

Note: If this field is not selected, devices of the relevant platform cannot be checked for compliance.

6. Under **Rule**, configure the compliance requirements for the selected device type. For a description of all settings available for each device type, see the *Sophos Mobile Control administrator guide*.

7. Under **Disallow Active Sync**, you can specify that email access will be denied automatically, if devices are not compliant. Select the required checkboxes next to the corresponding rules.

Note: This column is only available if you have configured an external EAS Proxy Server (optional). For further information, see [Configure connections to standalone EAS Proxy Servers](#) (section 10).

8. To notify administrators if particular rules are not met, select the checkbox **Notify admin** next to the corresponding rules.

9. Under **Transfer task bundle**, you can select task bundles to be transferred for the required **Rule** settings. Leave the fields unchanged at this stage. When used improperly, task bundles may misconfigure or even wipe devices. To assign the proper task bundles to compliance rules, a deeper knowledge of the system is required.

10. After you have defined all settings in all required device type tabs, click the **Save** button.

11. The new compliance set is displayed in the **Compliance rules** list view.

12. If you have specified that administrators receive email notifications when devices are not compliant, specify the relevant recipients under **Compliance mail recipients** and a notification schedule under **Compliance mail timetable**. Use ; to separate several administrators in the **Compliance mail recipients** field. Click the **Save** button.

To add further compliance rules, repeat the described steps. You can assign the created compliance rule(s) when you create a device group in the next step. If you plan to manage corporate and private devices, we recommend that you define separate settings for at least these two device types.

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

The **Device groups** view is displayed.

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

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

3. Enter a **Name** and a **Description** for the new device group.
4. Under **Compliance rules** in the fields **Company devices** and **Employee devices**, select the compliance sets you want to apply.
5. Click the **Save** button.

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

Note: If you delete a device group, the group's members are moved to another group that needs to be specified. If there is no other group left to move the devices to, the group cannot be deleted. Before a group is deleted a warning message is displayed.

13 Configure iOS devices

13.1 Create profiles for Apple iOS devices

In this step, you create a profile for initial configuration of iOS devices. A recommended initial configuration should include your password policies and the restrictions you want to apply to devices. We recommend that you include Exchange, VPN or WiFi settings in separate profiles.

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

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

This section describes how to create profiles directly in the web console. For further information on how to import profiles created with the Apple iPhone Configuration Utility, see the *Sophos Mobile Control administrator guide*.

1. In the web console menu bar, go to **Profiles** and click **Apple iOS**.

The **Profiles** view is displayed.

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

The **Edit profile** view is displayed.

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

We recommend that you use the name "iOS SSP profile" for profiles that are applied during the enrollment process through the Self Service Portal.

4. In the **ID** field, enter a unique ID for the profile, for example "com.mycompany.smc.baseprofile".

Note: Special characters like umlauts or spaces are not supported in iOS profile IDs.

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

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

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

- **Always**
- **With authentication**
- **Never**

Note: We recommend that you select the option **Never**.

8. In the **Automatically remove on** field, you can enter a date for the automatic removal of the profile from end user devices.
Note: We recommend that you do not configure a date for the automatic removal of the profile.
Note: This function is supported as of iOS 6.
 9. Under **Operating systems**, select the operating system the profile should apply to. Select all iOS versions for this profile.
 10. Click the **Add** button to add configurations with iPhone configuration settings to the profile.
The **Available configurations** view is displayed.
 11. Select **Password policies** and click **Next**.
The **Password policies** view is displayed.
 12. Specify the password policies settings for this profile. For a detailed description of all settings available, refer to the *Sophos Mobile Control administrator guide*.
 13. Click the **Apply** button.
The **Password policies** configuration is displayed in the **Edit profile** view under **Configurations**.
 14. To add a **Restrictions** settings profile, click the **Add** button again.
Note: Supported settings may depend on the iOS version in use on individual devices. Depending on the end user device, some settings may not have any effect. For further information, see the feature matrix in the *Sophos Mobile Control technical guide*.
 15. In the **Available configurations** view, select **Restrictions** and click **Next**.
The **Restrictions** view is displayed.
 16. Specify the restrictions settings for this profile. For a detailed description of all settings available, refer to the *Sophos Mobile Control administrator guide*.
 17. Click the **Apply** button.
The **Restrictions** configuration is displayed in the **Edit profile** view under **Configurations**.
 18. Click the **Save** button.
- The profile is available for transfer. It is displayed in the **Profiles** view. To configure profiles with Exchange, VPN and WiFi settings, repeat the steps described.

13.2 Create task bundles for iOS devices

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

2. Click the **Create new task bundle** button.

The **Edit task bundle** view is displayed.

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

We recommend that you use the name "iOS SSP task bundle" for task bundles that are applied during the enrollment process through the Self Service Portal.

4. Under **Operating systems**, select the operating systems the new task bundle applies to. Select all iOS settings for this task bundle.

5. Under **Tasks**, click the **Create new task** button.

- a) As a first task, select the task type **Bootstrap the iOS MDM client** and click **Next**. Give the task a meaningful name, for example "MDM bootstrap" and click **Next**.

- b) Add a second task of the type **Install an iOS profile** and click **Next**. Select the profile you have created ("iOS SSP profile", if you have used the suggested name) and click **Next**. Give the task a meaningful name, for example "Install provisioning profile", and click **Next**. If you have configured profiles with Exchange, VPN and WiFi settings, repeat this step for each profile.

- c) Add a third task of the type **Install a software package**. Select the Sophos Mobile Control Client package and click **Next**. Give the task a meaningful name, for example "Install SMC app", and click **Next**.

- d) Repeat this procedure to add further tasks. You can set the order for installation for selected tasks by using the sort arrows on the right-hand side of the **Tasks** list.

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

The task bundle is available for transfer. It is displayed in the **Task bundles** view.

14 Configure Android devices

14.1 Create profiles for Android devices

In this step, you create a configuration profile for initial configuration of Android devices. A recommended initial configuration should include your password policies and the restrictions you want to apply to devices. We recommend that you include Exchange, VPN or WiFi settings (if your Android devices support these settings) in separate profiles. We also recommend to upload root and client certificates in separate profiles.

1. In the web console, go to **Profiles** and click **Android**.
The **Profiles** view is displayed.
2. Click the **Create new profile** button.
The **Edit profile** view is displayed.
3. Enter a **Name** and a **Version** for the new profile.
We recommend that you use the name "Android SSP profile" for profiles that are applied during the enrollment process through the Self Service Portal.
4. In the **ID** field, enter a unique ID for the profile, for example "com.mycompany.smc.baseprofile".
5. In the **Description** field, enter a description for the profile, for example "base profile".
6. Under **Operating systems**, select the operating system the profile should apply to. Select all Android versions for this profile.
7. Click the **Add** button to add configurations with Android configuration settings to the profile.
The **Available configurations** view is displayed.
8. Select **Password policies** and click **Next**.
The **Password policies** view is displayed.
9. In the **Password type** field, select the type of password you want to define (for example **Complex**) and click **Next**.
10. Specify the password policies settings for this profile. For a detailed description of all settings available, refer to the *Sophos Mobile Control administrator guide*.
11. Click the **Apply** button.
The **Password policies** configuration is displayed in the **Edit profile** view under **Configurations**.
12. To add a **Restrictions** settings profile, click the **Add** button again.
13. In the **Available configurations** view, select **Restrictions** and click **Next**.
The **Restrictions** view is displayed.

14. Specify the restrictions settings for this profile. For a detailed description of all settings available, refer to the *Sophos Mobile Control administrator guide*.
15. Click the **Apply** button.

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

16. Click the **Save** button.

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

14.2 Create task bundles for Android devices

1. In the web console menu bar, click **Task bundles**.

The **Task bundles** view is displayed.

2. Click the **Create new task bundle** button.

The **Edit task bundle** view is displayed.

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

We recommend that you use the name "Android SSP task bundle" for task bundles that are applied during the enrollment process through the Self Service Portal.

4. Under **Operating systems**, select the compatible operating systems for the new task bundle. Select all Android settings for this task bundle.
5. Under **Tasks**, click the **Create new task** button.

- a) As a first task, select the task type **Install the MDM agent** and click **Next**. Select the Sophos Mobile Control Android client and click **Next**. Give the task a meaningful name and click **Next**.

Note: The name you define here is shown in Self Service Portal while tasks are processed.

- b) Add a second task of the type **Install an Android profile** and click **Next**. Select the profile you have created ("Android SSP profile", if you have used the suggested name) and click **Next**. Give the task a meaningful name and click **Next**. If you have configured further profiles, repeat this step for each profile.
- c) Repeat this procedure to add further tasks. You can set the order for installation for selected tasks by using the sort arrows on the right-hand side of the **Tasks** list.

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

The task bundle is available for transfer. It is displayed in the **Task bundles** view. To create further task bundles, repeat the steps described.

15 Update Self Service Portal settings

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

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

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

2. Go to the **Group settings** tab.
3. Under **Group settings**, click the **Edit** pencil icon next to the **Default** Self Service Portal group.
4. Under **Platform**, select the device types that should be available in the Self Service Portal:

- **Android**
- **iOS**
- **Windows Phone 8**
- **Windows Mobile**

Note: This guide focuses on iOS and Android as the most common mobile platforms. For further information on all available platforms, refer to the *Sophos Mobile Control administrator guide*.

5. In the **Add to device group** field, select the group that devices registered through the Self Service Portal should be added to.
6. In the **Enrollment package** field, select the task bundles you have created for iOS and Android devices and click **Apply**.
7. In the **Self Service Portal** tab, click the **Save** button.

16 Manage Self Service Portal users (end users)

Sophos Mobile Control offers different methods for managing end users:

- Internal user management

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

- External user management

With external user management you can connect to an existing LDAP directory and do not have to manage the users separately. Thus you can assign devices to groups and profiles based on directory membership.

In this step, you have to decide which user management method you want to use, configure the method in the web console and perform the configuration steps necessary for the selected method.

Note: You cannot change the user management method after devices have been linked to users.

16.1 Configure Self Service Portal user management method

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

The **System setup** view is displayed.

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

- Select **Internal directory** to use internal user management for users of the Sophos Mobile Control Self Service Portal.
- Select **External directory** to use external user management for users of the Sophos Mobile Control Self Service Portal. For further information, see [Using external user management](#) (section 16.3).

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.

3. Click the **Save** button.

The next steps depend on the user management method you have selected:

- Internal user management:

- Create a Self Service Portal user.
- Test provisioning with this user.
- Import your user list.

For further information, see [Using internal user management](#) (section 16.2).

- External user management:
 - Configure an external directory connection.
 - Test provisioning.

For further information, see [Using external user management](#) (section 16.3).

16.2 Using internal user management

16.2.1 Create a Self Service Portal user with internal user management

To test provisioning through the Self Service Portal, create a Self Service Portal user account for yourself. With this user account you can log in to the Self Service Portal.

1. In the web console menu bar, click **Users**.
The **Show users** view is displayed.
2. Click the **Create new user** button.
The **Edit user** view is displayed.
3. Enter the following information for the new Self Service Portal user:
 - a) Make sure that the **Send welcome mail** field is selected. This field is available, if you have configured a welcome mail in the **SSP welcome mail** tab in **Settings**. If the field is not displayed, configure a welcome mail first. The welcome mail has to include all required login credential information.
 - b) **User name**
 - c) **Last name**
 - d) **First name**
 - e) **Email**
 - f) **Phone number** (optional)

The new Self Service Portal user is displayed in the **Show users** view. An email with the Self Service Portal URL and the user credentials is sent to the email address specified.

16.2.2 Test provisioning through the Self Service Portal

We recommend that you test provisioning through the Self Service Portal with one user before you roll out Self Service Portal use to further users.

Log in to the Self Service Portal with the Self Service Portal user account you have created for yourself and register and provision devices. We recommend that you run a test for all platforms that you want to use with Sophos Mobile Control.

For further information on how to use the Self Service Portal, refer to the *Sophos Mobile Control user guides for Android, Apple iOS, Windows Phone 8 and Windows Mobile*.

Note: This guide focuses on iOS and Android as the most common mobile platforms. For further information on all available platforms, see the *Sophos Mobile Control administrator guide*.

16.2.3 Upload your user list to Sophos Mobile Control

After you have successfully tested provisioning through the Self Service Portal, import your user list to Sophos Mobile Control.

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

The **Show users** view is displayed.

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

The **Import users** view is displayed.

If you do not have a .csv file with users yet, you can download a sample file now and use it for creating your import file.

3. Make sure that the **Send welcome mails** field is selected. This field is available, if you have configured a welcome mail in the **Welcome email** tab in **Settings** under **Self Service Portal**. If the field is not displayed, configure a welcome mail first. The welcome mail has to include all required login credential information.

4. Select the .csv file you want to import and click **Upload file**.

The entries in the.csv file are checked for errors and displayed on the import page.

Note: If there are any errors in the .csv file, it cannot be imported. An error message is displayed next to the relevant entries. Edit the .csv file accordingly and try again.

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

The users are imported and displayed in the **Show users** view. They can use the Self Service Portal for registering and provisioning their devices.

16.3 Using external user management

16.3.1 Configure external directory connection for Active Directory

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

The **System setup** view is displayed.

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

The **Directory server details** view is displayed.

4. In this view, enter the following:
 - a) In the **Primary URL** field, enter the URL of the server. You can enter the server IP or the server name. Select **SSL** to use SSL for the server connection.
 - b) In the **Backup URL** field, enter the URL of the backup server. You can enter the server IP or the server name. Select **SSL** to use SSL for the server connection.
 - c) In the **User** field, enter a user who has reading rights for the server. You need to enter the user with the relevant domain. Supported formats are: <domain>\<user name> or <user name>@<domain>.<domain code>.
 - d) In the **Password** field, enter the password for the user.

Click **Next**.

The **Searchbase** view is displayed.

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

The **Search Fields** view is displayed.

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

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

Click **Next**.

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

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

The **System setup** view is displayed again.

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

16.3.2 Test provisioning through the Self Service Portal

We recommend that you test provisioning through the Self Service Portal with one user before you roll out Self Service Portal use to further users.

Log in to the Self Service Portal with your Active Directory credentials and register and provision devices. We recommend that you run a test for all platforms that you want to use with Sophos Mobile Control.

For further information on how to use the Self Service Portal, refer to the *Sophos Mobile Control user guides for Android, Apple iOS, Windows Phone 8 and Windows Mobile*.

Note: This guide focuses on iOS and Android as the most common mobile platforms. For further information on all available platforms, see the *Sophos Mobile Control administrator guide*.

17 Technical support

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

- Visit the SophosTalk community at <http://community.sophos.com/> and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at <http://www.sophos.com/en-us/support.aspx>.
- Download the product documentation at <http://www.sophos.com/support/documentation/mobile-control.aspx>.
- Send an email to support@sophos.com, including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

18 Legal notices

Copyright © 2011 - 2013 Sophos Ltd. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos is a registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.