SOPHOS
Security made simple.

Sophos Mobile

super administrator guide

Product Version: 8

Contents

1 About this guide

This guide describes how to carry out super administrator tasks in Sophos Mobile Admin for Sophos Mobile on Premise.

For a description of Sophos Mobile Admin for regular administrators, see the Sophos Mobile administrator help. You can also find general information (for example prerequisites) and task descriptions in the Sophos Mobile administrator help.

The descriptions in the administrator help also apply to the super administrator, unless otherwise noted.

For Sophos Mobile in Central, see the Sophos Mobile in Central startup guide and the Sophos Mobile in Central administrator help.

For Sophos Mobile as a Service, see the Sophos Mobile as a Service startup guide and the Sophos Mobile administrator help.

1.1 Document conventions

The following conventions are used in this document.

- Unless otherwise noted, the term *Windows Mobile* refers to Windows Phone 8.1 and the Windows 10 operating system editions *Mobile* and *Mobile Enterprise*.
- Unless otherwise noted, the term *Windows* or *Windows 10* refers to the Windows 10 operating system editions *Pro*, *Enterprise*, *Education*, *Home* and *S*.
- Unless otherwise noted, all procedures assume that you are logged in to Sophos Mobile Admin using a super administrator account.

2 Super administrator

In Sophos Mobile, customers are the tenants that manage the devices of their users. For every customer, one or more administrator accounts exist.

Besides these regular customers and administrators, there is a super administrator customer and a related super administrator. The role of this super administrator is to set up Sophos Mobile after installation and to create and manage customers. The first super administrator account and the super administrator customer are created during Sophos Mobile installation. A super administrator can create additional super administrators later on.

For information on the initial creation of the super administrator and the super administrator customer during installation, see the Sophos Mobile installation guide.

2.1 Super administrator tasks

The following list provides an overview of the tasks that the super administrator can perform. For detailed information see the respective sections of this guide.

The super administrator can:

- Create other super administrator accounts.
- Manage Sophos Mobile licenses.
- Start the configuration wizard to perform initial configuration of the Sophos Mobile server.
- Configure technical contact information. Customer administrators can use this as a template for providing contact information for users of the Sophos Mobile Control app and the Self Service Portal.
- Create and manage customers.
- Create reports for all customers.
- Define configuration items like profiles, task bundles, apps or settings and then transfer them to customers.
- Renew APNs certificates for all customers in one step.
- Define a default customer for the Self Service Portal login.
- Configure connections to EAS proxy servers.
- Configure connections to third-party Network Access Control systems, to enable network access management for the managed devices.
- Configure access to Sophos Mobile Admin and the Self Service Portal.
- Add a custom logo to the login pages of Sophos Mobile Admin and the Self Service Portal.
- Configure file size limits for uploaded apps and documents.
- Configure the title that is shown in the Sophos Mobile Control app.
- Configure logging of actions by administrators when they are logged in to the web portal.
- Configure system messages that are displayed on the login pages of Sophos Mobile Admin and the Self Service Portal.
- Download server log files.

2.2 Super administrator customer

The super administrator customer offers a specific view of the Sophos Mobile web portal that is adapted to super administrator tasks. The differences are based on these two facts:

- The super administrator does not manage devices or users.
- The super administrator is allowed to configure Sophos Mobile system settings.

In detail, the view of the super administrator customer has these differences compared to the view of a regular customer:

- On the **Dashboard** page, a list of all available customers is displayed, and you can create new customers. See Create a customer (page 12).
- Below the menu section **SETTINGS**, an additional item, **Health**, is available to display server and database details.
- The menu items **Devices**, **Users** and **Documents** are not available.
- On the **Compliance policies** page, the **Check now** button is not available. To check devices for compliance, you need to switch to the relevant customer.
- On the **About** page, a **Download log files (ZIP file)** link for downloading all log files in a ZIP file is available. See Download server log files (page 36).
- The tabs on the **System setup** page differ.

  These tabs are only available for the super administrator customer:

  - **License**: For regular customers, a read-only version of this tab displays the details of the licenses assigned to that customer.
  - **SSL/TLS**
  - **EAS proxy**
  - **Network Access Control**
  - **SMTP**
  - **HTTP proxy**
  - **Web portals**
  - **File uploads**
  - **Audit logging**
  - **System messages**

  These tabs are only available for a regular customer:

  - **iOS AirPlay**
  - **Apple VPP**
  - **Apple DEP**
  - **Apple DEP profiles**
  - **Samsung Knox license**
  - **SCEP**
  - **SGN**: This tab is only available when LDAP is used.

  These tabs are available for both customer types and let you configure settings for that specific customer:

  - **APNs**
  - **User setup**

2.3 Log in as super administrator

1. Open the Sophos Mobile Admin web address that you configured during installation of Sophos Mobile.
2. In the login dialog, enter the super administrator customer name and the credentials of the super administrator, then click **Login**.

2.4 Switch to a different customer

As super administrator, you can switch from the super administrator customer to a regular customer.

The administrator currently logged in and the current customer are displayed in the page header.

To switch to a different customer:

1. In the page header, click the current customer name to open the list of available customers.
   The super administrator customer is the first item in the list and is marked by an asterisk.
2. Select the customer to whom you want to switch.

The **Dashboard** page for the selected customer is displayed.

> **Tip**
> As super administrator, you can switch to a different customer from the **Dashboard** page: Click the blue triangle next to the customer to whom you want to switch and then click **Choose**.

For a description of Sophos Mobile Admin for regular customers, see the Sophos Mobile administrator help.

2.5 Create additional super administrators

To create additional super administrators for the super administrator customer:

1. On the menu sidebar, under **SETTINGS**, click **Setup > Administrators**.
2. On the **Show administrators** page, click **Create administrator**.
3. Enter the account details for the new super administrator.
   - When **External LDAP directory** is selected as user directory for the super administrator, you can click **Lookup user via LDAP** to select an existing LDAP account.
   - When **Internal directory** or **None** is selected as user directory, enter the relevant data in the **Login name**, **First name**, **Last name**, and **Email address** fields.
4. In the **Role** list, select the **Administrator** user role.
5. Under **Authentication**, specify the password for the new super administrator.

   For a local account, enter a one-time password that the super administrator must change at first login.

   For an LDAP account, you can either use the LDAP password for authentication, or enter a one-time password.
6. Click **Save** to create the super administrator account.

The new super administrator is created and displayed on the **Show administrator** page.

Forward the credentials (login name, super administrator customer name and one-time password) to the relevant person.

3 Sophos Mobile licenses

Sophos Mobile offers two types of licenses:

- Mobile Standard license
- Mobile Advanced license

With a license of type Mobile Advanced you can 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 with Sophos Mobile, see the Sophos Mobile 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 Check your licenses

Sophos Mobile 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:

- **Number of licenses**: Maximum number of device users (and unassigned devices) of all customers that can be managed.

  This field is only present for the super administrator customer.
- **Maximum number of licenses**: Maximum number of device users (and unassigned devices) that can be managed.

  This information is only shown for regular customers.

  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 server.
- **Used licenses**: Number of licenses in use.
- **Valid until**: The license expiration date.
- **Licensed URL**: The URL of the Sophos Mobile server for which the license is issued.

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

3.2 Activate Mobile Advanced licenses

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

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

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.

3.3 Assign licenses to customers

1. On the menu sidebar, under **INFORM**, click **Dashboard**.
2. Click the blue triangle next to the customer you want to assign licenses to, then click **Edit**.
3. Configure the license settings:
   a) In the **Maximum number of licenses** field, enter the number of device users and unassigned devices that can be managed for the customer.
   b) Select **Advanced licenses** if you want to enable the management of the Sophos Mobile Security, Sophos Secure Workspace and Sophos Secure Email apps for the customer.
   c) In the **Valid until** field, specify the expiration date for the licenses that are assigned to the customer.

      After that date, no tasks can be created or processed for the customer.
4. Click **Save**.

4 Run the configuration wizard

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

You need to provide:

- A Mobile Standard license key, optionally an additional Mobile Advanced license key
- SSL/TLS certificate(s)
- SMTP credentials

Note
As a super administrator you can adjust these settings afterward on the **System setup** page of Sophos Mobile Admin. 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 Sophos Mobile Admin for the first time as super administrator, the **Welcome** view is displayed. Click **Next**.
2. In the **License** view, enter your Mobile Standard license key or request a trial license:
   - **Mobile Standard license key:**

     When you enter the Mobile Standard license key and click **Activate**, you are given the option to additionally enter a Mobile Advanced license key. If you have purchased Mobile 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 installer from www.sophos.com. Then click **Request trial** again.

   Note
   You can change the license settings at any time in Sophos Mobile Admin.

   Click **Next**.
3. In the **SSL/TLS** view, configure the certificates to be used for securing the SSL or TLS connection between the Sophos Mobile 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 server will communicate the list of certificates to the clients. On establishing an SSL or TLS 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/TLS** 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.

4. 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 port	The server port to connect to. **Note** The displayed connection types (TLS, SSL, and unencrypted) only show standard port usages. See the documentation of the SMTP server for guidelines on which port to use.
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 *From* field of emails from Sophos Mobile.
Originator name	The author name that will appear in the *From* field. If required, you can configure a different originator name (but not email address) for each customer later on. See the Sophos Mobile administrator help.
Send error emails	Sophos Mobile 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 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 as insecure.

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

5 Configure technical support contact details

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

6 Manage customers

After Sophos Mobile installation and setup, a key step required for using Sophos Mobile is to create at least one customer, this means a tenant whose devices are managed in Sophos Mobile.

As a super administrator you use the super administrator customer to create and manage customers for device management with Sophos Mobile.

6.1 Customer overview on the Dashboard

On the super administrator customer **Dashboard** page, an overview of all existing regular customers is displayed, including the information shown below:

Column	Description
Name	The name of the customer.
Activated state	Indicates if the customer is activated.
Valid until	The expiration date of the customer. The value **unlimited** is displayed if no expiration date is set. Dates that lie in the past are displayed in red.
Licenses	The maximum number of Sophos Mobile licenses that can be used for the customer. The value **unlimited** is displayed if no maximum number is set.
Advanced	Indicates if Mobile Advanced licenses are enabled for the customer.
Devices	The number of enrolled devices for this customer.
AND	The number of enrolled Android devices for this customer.
iOS	The number of enrolled iOS devices for this customer.
WM	The number of enrolled Windows Phone and Windows 10 Mobile devices for this customer.
Win	The number of enrolled Windows 10 computers for this customer.
AND T	The number of enrolled Android Things devices for this customer.
W IoT	The number of enrolled Windows 10 IoT devices for this customer.

Column	Description
Directory	The type of user management that is configured for the customer.

6.2 Create a customer

You must be logged in to Sophos Mobile Admin 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.

Option	Description
Name	The customer's name.
Description	Text to describe the purpose of the customer account.
Maximum number of licenses	The number of device users and unassigned devices that can be managed for the customer.
Advanced licenses	If selected, the customer can use Sophos Mobile to manage the Sophos Mobile Security, Sophos Secure Workspace and Sophos Secure Email apps.
Valid until	The expiration 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 in the page header. 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. Choose from: • **None. No SSP, user-specific profiles, or LDAP administrators available**: This disables the creation of user accounts for the Self Service Portal, and the lookup of accounts for Sophos Mobile Admin from an LDAP directory. • **Internal directory**: Use internal user management for Sophos Mobile Admin and the Self Service Portal. For

Option	Description
	further information, see the Sophos Mobile administrator help. • **External LDAP directory**: In addition to internal user management, you can lookup accounts for Sophos Mobile Admin and the Self Service Portal from an LDAP directory. Click **Configure external LDAP** to specify the server details.

4. Click **Save**.

The customer is created.

6.3 Create an administrator for the new customer

1. In the page header, click the current customer name to open the list of available customers, and then select the customer for whom you want to create an administrator account.
2. On the menu sidebar, under **SETTINGS**, click **Setup > Administrators**.
3. On the **Show administrators** page, click **Create administrator**.
4. On the **Edit administrator** page, enter the account details for the administrator.
   - When **External LDAP directory** is selected as 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, enter the relevant data in the **Login name**, **First name**, **Last name**, and **Email address** fields.
5. In the **Role** list, select the **Administrator** user role.
6. In section **Authentication**, specify the password for the new super administrator.

   For a local account, enter a one-time password that the super administrator must change at first login.

   For an LDAP account, you can either use the LDAP password for authentication, or enter a one-time password.
7. Click **Save** to create the administrator account.

The new administrator is created.

Forward the credentials (login name, customer name and one-time password) to the relevant person.

6.4 Edit customer

1. On the menu sidebar, under **INFORM**, click **Dashboard**.
2. On the **Dashboard** page, click the blue triangle next to the customer that you want to edit, and then click **Edit**.
3. On the **Edit customer** page, make the required changes.
4. Click **Save**.

6.5 Configure external directory connection

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

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

1. On the menu sidebar, under **INFORM**, click **Dashboard**.
2. On the **Dashboard**, click the blue triangle next to the customer for whom you want to configure an LDAP connection, and then click **Edit**.
3. On the **Edit customer** page, under **User directory**, select **External LDAP directory**.
4. Click **Configure external LDAP** to specify the server details.
5. On the **Server details** page, configure the following settings:
   a) In the **LDAP type** field, select the LDAP server type:
      - **Active Directory**
      - **IBM Domino**
      - **NetIQ eDirectory**
      - **Red Hat Directory Server**
      - **Zimbra**
   b) In the **Primary URL** field, enter the URL of the primary directory server. You can enter the server IP or the server name. Select **SSL/TLS** to secure the server connection by SSL or TLS (depending on what the server supports). For Sophos Mobile as a Service, **SSL/TLS** cannot be deselected.
   c) Optional: In the **Secondary URL** field, enter the URL of a directory server that is used as fallback in case the primary server cannot be reached. You can enter the server IP or the server name. Select **SSL/TLS** to secure the server connection by SSL or TLS (depending on what the server supports). For Sophos Mobile as a Service, **SSL/TLS** cannot be deselected.
   d) In the **User** field, enter an account for lookup operations on the directory server. Sophos Mobile uses the account credentials when it connects to the directory server.

      For Active Directory, you also need to enter the relevant domain. Supported formats are:

      - `<domain>\<user name>`
      - `<user name>@<domain>.<domain code>`

      Note
      For security reasons, we recommend you specify a user that only has read permissions for the directory server and not write permissions.

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

   Click **Next**.

6. On the **Search base** page, enter the Distinguished Name (DN) of the search base object.
   The search base object defines the location in the external directory from which the search for a user or user group begins.
7. On the **Search fields** page, define which directory fields are to be used for resolving the *%_USERNAME_%* and *%_EMAILADDRESS_%* placeholders in profiles and policies. Type the required field names or select them from the **User name** and **Email** lists.

   Note
   The lists only contain fields that are configured for the user that is currently connected to the LDAP directory, specified in step 5.d (page 14) earlier in this description. If, for example, an email field was not configured for that user, you need to manually enter the required value in the **Email** field.

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

   - **User name**: `sAMAccountName`
   - **First name**: `givenName`
   - **Last name**: `sn`
   - **Email**: `mail`
8. On the **SSP configuration** page, specify the users that are allowed to log in to the Self Service Portal. Enter the relevant information in the **LDAP directory group** field, using one of the following options:

   - If you enter an asterisk *, members of all LDAP directory groups are allowed to log in to the Self Service Portal.

     Note
     The value * represents *all groups*, not *all users*. Users that are not a member of any LDAP directory group are not included.

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

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

   For further information on the Self Service Portal group settings, see the Sophos Mobile administrator help.

9. Click **Apply**.
10. On the **Edit customer** page, click **Save**.

6.6 Deactivate customer

If a customer is no longer used for device management with Sophos Mobile, you can deactivate it.

1. On the menu sidebar, under **INFORM**, click **Dashboard**.
2. On the **Dashboard** page, click the blue triangle next to the customer you want to deactivate, and then click **Edit**.
3. On the **Edit customer** page, select **Deactivate account**.

The customer is deactivated. Users managed in this customer can no longer log in to Sophos Mobile Admin or the Self Service Portal. Devices managed in this customer can still synchronize with the Sophos Mobile server.

6.7 Delete customer

You cannot delete a customer as long as there are:

- Devices enrolled with Sophos Mobile.
- Users registered for the Apple Volume Purchase Program (VPP).

1. On the menu sidebar, under **INFORM**, click **Dashboard**.
2. On the **Dashboard** page, click the blue triangle next to the customer you want to delete, and then click **Delete**.

> **Note**
> The **Delete** option is only available when no devices are assigned to the customer.

The customer is deleted and removed from the **Dashboard** page.

6.8 Export a list of customers

You can export a list of customers in Microsoft Excel or CSV text format:

1. On the menu sidebar, under **INFORM**, click **Dashboard**.
2. Optional: Filter the list of customers by entering a text string in the search field at the top of the customer list.

   Only customers that match the search string are displayed. This filter will also be applied to the export.
3. On the **Dashboard** page, click **Export** at the bottom of the customer list.
4. Click one of the four icons to specify the scope and the format of the export. You can choose between these pair of options:
   - Export customers from the current list page or from all pages.
   - Export to Microsoft Excel or to CSV format.

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

7 Reports

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

- Devices
- Apps and documents
- Compliance
- Malware
- Certificates

When you are logged in to the super administrator customer, the reports include information for all customers. When you are logged in to a regular customer, the reports only include information for that customer.

To create a report:

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

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

8 Manage configuration items

As a super administrator you can define configuration items like profiles, task bundles or apps and then transfer them to customers.

There are two different transfer types:

- Clone configuration items for new customers (page 18): The items are transferred by copying and can be edited for the receiving customer.
- Assign customers to configuration items (page 19): The items are transferred by link and cannot be edited for the receiving customer.

8.1 Clone configuration items for new customers

When a new customer is created, the following configuration items from the super administrator customer can be cloned, that is, transferred by copying:

- Device groups
- Compliance policies
- The settings from these tabs of the **General settings** page:
  - **Password policies**
  - **Android**
  - **iOS**
  - **Windows**
  - **Email configuration**
  - **Technical contact**
- The settings from all tabs of the **Self Service Portal** page.
- The settings from the **APNs** tab of the **System setup** page.

The configuration items are always cloned as a whole. You can select if the items will be cloned or not, but you cannot clone individual items.

Note
For information on how to define configuration items, see the Sophos Mobile administrator help.

To clone the configuration items for a new customer:

- Create a new customer as described in Create a customer (page 12).
  Under **Clone settings**, select **Settings and packages**.

The configuration items are transferred to the new customer. They can be edited by the customer administrator.

Note

When **Settings and packages** is selected, the new customer will also be assigned to these items of the super administrator customer:

- Profiles and policies
- Task bundles
- Apps and app groups

See Assign customers to configuration items (page 19).

8.2 Assign customers to configuration items

A customer can be assigned to the following configuration items of the super administrator customer:

- Profiles and policies
- Task bundles
- Apps and app groups

When a customer is assigned to a configuration item, the item is transferred to that customer by link, that is, the super administrator customer's original and the assigned customer's version are actually the same item.

Because of this link, a few restrictions must be observed:

- The assigned customer's version cannot be edited or deleted. However, the administrator of that customer can duplicate a linked profile, policy or task bundles. That copy is not linked to the original item and can be edited.
- When a customer is assigned to an app, the super administrator cannot remove the assignment or delete the app as long as it is used in a task bundle of the customer.
- When a customer is assigned to a task bundle, the super administrator cannot remove the assignment or delete the task bundle as long as that customer uses the task bundle as a compliance action or enrollment package.

Note

For information on how to define configuration items, see the Sophos Mobile administrator help.

To push a configuration item to a customer:

1. From the menu sidebar, open the relevant configuration item for editing.

   For example, to assign the customer to an Android task bundle, click **Task bundles > Android**, then click the blue triangle next to the relevant task bundle, and then click **Edit**.
2. On the **Edit** page of the relevant item, click **Show** next to the **Assigned customers** option.
3. Select one or more customers which will be assigned to the configuration item.

   You can also deselect customers that have been assigned to the configuration item before. If a customer appears dimmed, the assignment cannot be removed because the configuration item is used by that customer.
4. On the **Edit** page, click **Save** to assign the selected customers to the configuration item.

8.3 Renew APNs certificate for all customers

Sophos Mobile manages APNs certificates per customer. Even when an APNs certificate is cloned from the super administrator customer to a regular customer when that customer is created, the customer's certificate must be renewed separately when it is about to expire.

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.

To renew the APNs certificate for all customers:

1. As super administrator, renew the APNs certificate for the super administrator customer as described in Sophos knowledgebase article 118926.
2. At the end of the procedure, when clicking **Save** to save the renewed certificate, there is an additional dialog that lists all customers that currently use the same APNs certificate as the super administrator, that is a certificate with the same **Topic** attribute.
   - Click **Save for all customers concerned** to renew the APNs certificate for all of these customers.
   - Click **Save only for super administrator customer** to renew the APNs certificate only for the super administrator customer.

9 General settings for Android device management

The super administrator can configure the following Android specific settings:

- Configure the source location of Sophos apps (page 21).
- Configure the synchronization interval of the Sophos Mobile Control app (page 22).

9.1 Configure the source location of Sophos apps

You can configure the location from which users install the Sophos Mobile Control app and the Sophos Mobile Security app during enrollment. This can be:

- The Google Play Store
- An internal web server

You might want to use an internal web server because:

- Device users do not need a Google account.
- You have control over the app versions that are installed on the devices.

Note
The option to configure the source location of the Sophos Mobile Security app is only available if you have activated a Mobile Advanced license.

Important
Note the following when you are hosting the Sophos Mobile Control app on an internal web server:

- On the Android devices, the **Unknown sources** option in the **Security** settings must be enabled. Because this introduces potential vulnerabilities to the devices, we recommend you not to use the internal web server option.
- You need to make sure that new app versions are installed on the mobile devices. You can achieve that by uploading the app to Sophos Mobile and then using a task bundle to install it onto the devices.

To configure the source location of the Sophos Mobile Control app:

1. When you are going to host the Sophos Mobile Control app on an internal web server, download the APK file from the Sophos Product Downloads and Updates web page and publish it on your web server.

   We suggest that you use the web server that is included in Sophos Mobile. To do so, copy the APK file to the `wildfly\tools-content` subdirectory of your Sophos Mobile installation directory.

   For general information about how to download Sophos software, see Sophos knowledgebase article 111195.

2. On the menu sidebar of Sophos Mobile Admin, under **SETTINGS**, click **Setup > General**, and then click the **Android** tab.
3. In **Select installation source**, select one of these options:
   - **Google Play Store**
   - **Hosted APK file**
4. If you selected **Hosted APK file**, enter the URL of the APK files for the Sophos Mobile Control app in the fields **URL of the SMC APK file** and **URL of the SMSec APK file**.

   For example, if you have copied the APK file to the `wildfly\tools-content` subdirectory of your Sophos Mobile installation directory as recommended before, enter this URL: `<self_service_portal_address>/tools/smc.apk`

   Note
   The devices must be able to access the URL.

5. Likewise, you can enter the URL of the APK file for the Sophos Mobile Security app in the field **URL of the SMSec APK file**.

   This requires a Mobile Advanced license.
6. Click **Save**.

The installation instructions that a user receives when enrolling a device will refer to the installation source that you configured.

9.2 Configure the synchronization interval of the Sophos Mobile Control app

The Sophos Mobile Control app synchronizes with the Sophos Mobile server at these times:

- Immediately, when it needs to communicate device-side changes.
- On request, when it is triggered by the server through the push notification services Google Cloud Messaging (GCM) and, optionally, Baidu Cloud Push.
- Time scheduled, every 24 hours by default.

If required, you can use a shorter interval for the time scheduled synchronization.

Important
The default value of 24 hours is sufficient in most cases. We recommend that you only use a shorter interval if the push notification services do not work in your environment. Using shorter intervals impacts battery life and data consumption and causes higher server load.

To configure the synchronization interval that the Sophos Mobile Control app on Android devices uses:

1. On the menu sidebar, under **SETTINGS**, click **Setup > General**, and then click the **Android** tab.
2. In the **SMC app sync interval** section, select the required interval length from the **Sync interval** list.

   You can select a value between 15 minutes and 24 hours.
3. Click **Save**.

10 General settings for iOS device management

The super administrator can configure the following iOS specific settings:

- Upload profile-signing certificate (page 23).

10.1 Upload profile-signing certificate

You can upload a certificate for signing the Sophos Mobile MDM profile on iOS devices. The certificate must be qualified as digital signature and should be issued by a globally trusted CA.

Note
If you don't upload a profile-signing certificate, the MDM profile is signed with the customer's SMC root certificate. In this case, the MDM profile is initially classified as *untrusted* because it is installed at an earlier stage in the enrollment process than the certificate.

To upload a signing certificate for the MDM profile:

1. Log in to the super administrator customer.
2. On the menu sidebar, under **SETTINGS**, click **Setup > General**, and then click the **iOS** tab.
3. Under **Profile-signing certificate**, click **Upload certificate (PKCS #12 keystore)** and then browse for the P12 keystore file that contains your certificate.
4. Enter the password for the keystore file and then click **Apply**.
5. Click **Save**.

Subject, fingerprint and expiration date of the uploaded certificate are displayed. You can use this information later to identify the certificate.

11 General settings for the Self Service Portal

In addition to the Self Service Portal configuration that an administrator can perform, a super administrator can configure settings that apply to all customers:

- Define a default customer that is used when a user logs in to the Self Service Portal.
- Hide the **Forgot password?** link in the login dialog of the Self Service Portal.

  Use this option if external user management is configured for all customers. With external user management, the **Forgot password?** link is without effect because passwords for LDAP directory accounts cannot be reset through Sophos Mobile.

For a full description of the Self Service Portal configuration, see the Sophos Mobile administrator help.

1. On the menu sidebar, under **SETTINGS**, click **Setup > Self Service Portal**, and then click the **Configuration** tab.
2. In the **Login customer preselection** section, select **Default customer** and then select the required costumer from the list.
3. Select **Visible and editable** to allow Self Service Portal users to change the customer when they log in.
4. Clear **Display password reset link on login page** to hide the **Forgot password?** link in the login dialog of the Self Service Portal.
5. Clear **Display link to admin console on login page** to hide the **Link to admin console** link in the login dialog of the Self Service Portal.
6. Click **Save**.

12 Configure connections to EAS proxy servers

With Sophos Mobile, you can set up an EAS proxy to filter email traffic from the managed devices to an email servers.

There are two types of EAS proxy:

- The internal EAS proxy that is automatically installed with Sophos Mobile. It supports incoming ActiveSync traffic as used by Microsoft Exchange or Lotus Traveler for iOS and Samsung Knox devices.
- A standalone EAS proxy that can be downloaded and installed separately. It communicates with the Sophos Mobile server through an HTTPS web interface.

Note

The EAS proxy ignores email traffic from your Android Things and Windows IoT devices. This allows you to assign the same user to an Internet of Things device and to a standard device.

Note

Because macOS doesn't support the ActiveSync protocol, you can't use the internal or the standalone EAS proxy to filter email traffic coming from Macs.

12.1 Configure a connection to the internal EAS proxy server

1. On the menu sidebar, under **SETTINGS**, click **Setup > System setup** and then click the **EAS proxy** tab.
2. Optional: Under **General**, select **Restrict to Sophos Secure Email** to restrict email access to the Sophos Secure Email app, available for Android and iOS.

   This prevents other email apps from connecting to your email server.
3. Under **Internal**, enter the Exchange or groupware server URL in the **Exchange/groupware server URL** text field.
4. Select **Use SSL/TLS** to use a secure connection.
5. Select **Allow EWS subscription requests from Secure Email** to allow the Sophos Secure Email app on iOS to subscribe to push notifications through Exchange Web Services (EWS). Push notifications inform the device when there are messages for Secure Email.

   By default, the EAS proxy blocks all requests to the Exchange server's EWS interface for security reasons. If you select this check box, subscription requests are allowed. Other requests remain blocked.
6. Click **Check connection** to test the connection.
   A message will be displayed if the server can be accessed.
7. Click **Save**.

12.2 Configure a connection to the standalone EAS proxy server

To configure the connection between Sophos Mobile and the standalone EAS proxy, you upload the certificate of the EAS proxy server to Sophos Mobile. The certificate was generated when you configured the EAS proxy instance.

For information on the installation and configuration of the standalone EAS proxy, see the Sophos Mobile installation guide.

Important

If the EAS proxy service is started before you have uploaded the certificate, Sophos Mobile rejects the connection to the server and the service fails to start.

To upload the certificate of the standalone EAS proxy:

1. On the menu sidebar, under **SETTINGS**, click **Setup > System setup** and then click the **EAS proxy** tab.
2. Optional: Under **General**, select **Restrict to Sophos Secure Email** to restrict email access to the Sophos Secure Email app, available for Android and iOS.

   This prevents other email apps from connecting to your email server.
3. Under **External**, click **Upload a file** and navigate to the certificate file.

   If you have set up more than one EAS proxy instance, repeat this for all instances.
4. Click **Save**.
5. In Windows, open the **Services** dialog and restart the **EASProxy** service.

13 Configure Network Access Control

Sophos Mobile includes an interface to third-party Network Access Control (NAC) systems. By configuring connections to NAC systems, you allow them to obtain a list of devices and their compliance states. Also, when you configure Network Access Control as described in this section, you can later define a compliance policy that denies network access when certain compliance rules are violated.

For information on how to define compliance policies, see the Sophos Mobile administrator help.

To configure Network Access Control:

1. On the menu sidebar, under **SETTINGS**, click **Setup > System setup**, and then click the **Network Access Control** tab.
2. Select one of the available NAC integrations from the list:

   - **Sophos UTM**

     This option enables Sophos UTM integration (for version 9.2 and higher). The integration requires you to set the SMC server URL and admin user credentials in the WebAdmin interface of Sophos UTM, under **Management > Sophos Mobile**. For details, see the *Sophos UTM administration guide*.

   - **Cisco ISE**

     This option enables Cisco ISE integration. Configure the following settings:

User name	The user name that has to be specified in Cisco ISE. It is used by Cisco ISE to log in to Sophos Mobile.
Password	Enter a password for logging in to Sophos Mobile.
Password confirmation	Repeat the password.
Redirection page for blocked devices	A URL to which devices are redirected if they are not allowed to access the network. We recommend that you use the URL of the Self Service Portal or of an information page with a link to the Self Service Portal.

     On Cisco ISE, you must configure the relevant settings so that it uses the URL of the Sophos Mobile server and the credentials that you entered here when connecting to the NAC interface.

   - **Check Point**

     This option enables Check Point integration (for version R77.10 and higher). Configure the following settings:

User name	The user name that has to be specified in Check Point. It is used by Check Point to log in to Sophos Mobile.
Password	Enter a password for logging in to Sophos Mobile.
Password confirmation	Repeat the password.

In the Check Point Mobile Access Gateway, you must configure some specific settings, as described in the Check Point Support Center article MDM cooperative enforcement for Mobile clients.

- **Web service**

  This option allows you to connect a third-party NAC system to the web service interface.

  Sophos Mobile offers a RESTful web service interface that delivers MAC addresses and network access status of the managed devices.

  A third-party NAC system can connect to that interface by using the login credentials of a Sophos Mobile administrator account.

  For implementation details of the web service interface see the Sophos Mobile Network Access Control interface guide.

- **Custom**

  This option allows you to configure certificate based access to the NAC interface.

  > **Note**
  > The legacy **Custom** option is deprecated and will be removed in a future release. Use the **Web service** option instead to connect a third-party NAC system to Sophos Mobile.

  Click **Upload a file** and navigate to the certificate of the third-party NAC system. The certificate is uploaded and displayed in a table.

  A third-party NAC system that presents the certificate to the Sophos Mobile server will gain access to the NAC interface.

3. On the **Network Access Control** tab, click **Save**.

14 Configure portal access

You can configure ranges of allowed IP addresses and session timeouts for Sophos Mobile Admin and for the Self Service Portal.

1. On the menu sidebar, under **SETTINGS**, click **Setup > System setup**, and then click the **Web portals** tab.
2. Under **Session timeouts**, select the desired time values from the **Admin console** and **Self Service Portal** lists. Sessions will be closed automatically when the user does not interact with the portal for the selected period of time.
3. Under **Allowed access list**, in the input fields of the **Admin console** and **Self Service Portal** sections, enter IP addresses or subnets that are allowed to access the relevant portal. To enable access from any IP address or network, leave the fields empty.

   Repeat these steps for all IP addresses or subnets that you want to configure.

   a) Either enter an IP address or a subnet range in CIDR notation.

      For example, enter `192.168.100.0/24` to specify the 192.168.100.0–192.168.100.255 address range.

   b) Click **Add** to add the IP address or subnet to the list.

   Important

   If you specify improper addresses, you may lock out yourself from Sophos Mobile Admin. However, you can always access the console from `localhost`, that is from the computer on which the Sophos Mobile server is installed.

4. Click **Save**.

It may take up to 60 seconds for the changes to take effect.

15 Add custom logo

As a super administrator, you can add a custom logo to the login pages of the web console and the Self Service Portal.

The following rules apply for the logo:

- File format must be Portable Network Graphics (PNG).
- Image width should be about 200 pixel to fit the layout of the login pages.
- Image background color should be white or transparent to blend in with the background of the login pages.

To add a custom logo to the login pages:

1. Prepare a PNG file with your custom logo that complies with the rules mentioned before.
2. Go to the `wildfly\resources\images` subdirectory of your Sophos Mobile installation directory.

   In this directory, there is a file `customer_logo.png`. By default, this file contains an empty placeholder image of size 1 pixel x 1 pixel.
3. Replace the existing file `customer_logo.png` with your custom version.

The custom logo will be displayed above the credential fields of the login pages.

You do not need to restart the Sophos Mobile service to apply the changes. However, users might need to clear the cache of their web browser in order to see the custom logo.

Note

To remove the custom logo and restore the default state of the login pages, replace the file `customer_logo.png` with `customer_logo.png.bak`, which contains a backup copy of the original 1 pixel x 1 pixel placeholder image.

16 Configure file upload limits

You can configure file size limits for uploaded apps and documents. When the administrator uploads app packages or documents to the Sophos Mobile server, files that exceed the configured limits are rejected.

Note

- The limits apply to all customers.
- The limits apply to a single app packages or document. There is no overall limit.
- The limits only apply to future uploads. Files that have been uploaded before the limits are configured are not restricted.

To configure the maximum size of uploaded files:

1. On the menu sidebar, under **SETTINGS**, click **Setup > System setup**, and then click the **File uploads** tab.
2. For each of the available categories, enter the maximum size in megabytes for a single file.
3. Click **Save**.

17 Configure app title

As a super administrator, you can configure the title that is shown in the title bar of the Sophos Mobile Control app. The default title is *Sophos Mobile*.

Note
This setting applies to all customers.

Note
This setting does not change the app name **Control** that is for example shown on the device desktop next to the app icon.

1. On the menu sidebar, under **SETTINGS**, click **Setup > General**, and then click the **SMC app** tab.
2. Under **App title**, select **Use custom app title** to disable the default title.
3. In the **Custom app title** field, enter the app title that you want to use.
4. Click **Save**.

The Sophos Mobile Control app uses the new title once the device synchronizes with the Sophos Mobile server.

18 Audit logging

You can log the actions of users while they are logged in to Sophos Mobile Admin. This includes the following information:

- Date
- Performed action
- User name
- Customer name
- Action details

Note
The audit log also includes all changes to Sophos Mobile database objects in general.

18.1 Enable audit logging

1. On the menu sidebar, under **SETTINGS**, click **Setup > System setup**, and then click the **Audit logging** tab.
2. Select **Enable audit logging**.
3. Click **Save**.
4. Restart the Sophos Mobile service from the menu of the **Sophos Mobile** system tray icon.

18.2 View audit log

1. On the menu sidebar, under **INFORM**, click **Audit logging**.
2. On the **Audit logging** page, use the **From** and **To** fields to specify a time period.
3. Click **Show log**.
   All log entries for the time within the specified time period are displayed on the **Audit logging** page.
4. To export the displayed list to a Microsoft Excel or CSV file, click **Export** at the bottom of the list and select the required format.

19 Create system messages

As a super administrator, you can create system messages that are displayed on the login pages of Sophos Mobile Admin and the Self Service Portal. You can use this for example to communicate outage times to users and administrators.

For every message you can configure:

- A start and an end date that define the validity period of the message.
- A severity level that defines how the message is displayed.

To create a system message:

1. On the menu sidebar, under **SETTINGS**, click **Setup > System setup**, and then click the **System messages** tab.
2. Click **Add system message**.
3. In the **Edit system message** dialog, configure the following settings:

Option	Description
Subject	The message subject. When the message is displayed on the login page, only the subject is visible by default.
Severity	Select the severity level (*critical*, *warning* or *note*). The severity is used to tag the message with an appropriate icon.
Start date	The date from which the message is displayed.
End date	The date until which the message is displayed.
Message	The message body. When the message is displayed on the login page, the message body is hidden by default and can be expanded by clicking the subject line. You can use the editor toolbar to apply basic formatting to the text.
Visible for users	If selected, the message is displayed on the login page of the Self Service Portal.
Visible for administrators	If selected, the message is displayed on the login page of the web portal.

4. Click **Apply** to create the message.
5. On the **System messages** tab, click **Save**.

20 Receive Sophos notifications

As a super administrator, you can receive news and notifications from Sophos related to Sophos Mobile. This includes information like:

- New release announcements
- New patch announcements
- App releases
- End-of-life announcements
- Security notifications

For Sophos Mobile on Premise, the notifications are pushed to the server once per day. All users that are registered for Sophos Mobile error emails will also receive these notifications.

To add a user to the list of email recipients:

1. On the menu sidebar, under **SETTINGS**, click **Setup > System setup**, and then click the **SMTP** tab.
2. Enter the user's email address in the **Email recipients** field.
3. Click **Save**.

Note
The super administrator can view all notifications on the **News** page.

21 Download server log files

As a super administrator, you can download the log files of the past five days from the server.

Note
If Sophos Mobile is set up as a cluster of server nodes, only the log files of the current node are available, that is the Sophos Mobile server instance to which the load balancer currently redirects the web portal requests. For information on clustering, see the *Sophos Mobile installation guide*.

To download the server log files:

1. On the menu sidebar, under **SETTINGS**, click **About**.
2. On the **About** page, click the **Download log files** link.
3. Click **Ok**.

A ZIP file containing the log files of the past five days is saved to your local computer, using the download settings of your web browser.

22 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.

23 Legal notices

Last update: 20180115