SOPHOS

Security made simple.

Sophos Mobile Control

Super administrator guide

Product version: 5.1

Document date: July 2015

Contents

1 About Sophos Mobile Control

Sophos Mobile Control is a device management solution for mobile devices like smartphones and tablets. Sophos Mobile Control helps to keep corporate data safe by managing apps and security settings. It allows configuration and software distribution as well as security settings and many other device management operations on mobile devices.

The Sophos Mobile Control system consists of a server and a client component which communicate through data connections.

The Sophos Mobile Control client is easily installed and managed with over-the air setup and configuration through the Sophos Mobile Control web console.

With the Sophos Mobile Control Self Service Portal for your users, you can reduce IT efforts by allowing users to register their own devices and carry out other tasks without having to contact the helpdesk.

Sophos Mobile Control supports the following mobile device platforms:

- Android
- Apple iOS
- Windows Phone 8

Due to the nature of the different platforms supported features vary. For a matrix of the features supported for the different platforms, refer to the *Sophos Mobile Control technical guide*.

1.1 About this guide

This guide describes how to carry out super administrator specific tasks in the Sophos Mobile Control web console for on-premise Sophos Mobile Control installations.

For a description of the Sophos Mobile Control web console for regular administrators, see the *Sophos Mobile Control administrator guide*. Besides the description of the web console for regular administrators, you also find general information (for example prerequisites) and task descriptions in the *Sophos Mobile Control administrator guide*.

General information and user interface descriptions in the administrator guide also apply to the super administrator, unless stated otherwise in this super administrator guide.

Note: Super administrators are not supported for Sophos Mobile Control as a Service. For further information on Sophos Mobile Control as a Service and the differences compared to an on-premise installation, see the *Sophos Mobile Control administrator guide*.

1.2 Sophos Mobile Control licenses

Sophos Mobile Control offers two types of license:

- Standard license
- SMC Advanced license

An SMC Advanced license adds functionality by enabling you to manage **Sophos Mobile Security** and **Sophos Secure Workspace**.

- Sophos Mobile Security is a security app for Android phones and tablets. The app protects your Android device and your privacy without impacting performance or battery life. Using up-to-the-minute intelligence from SophosLabs, your apps will be automatically scanned as you install them. This anti-virus functionality protects you from malicious software which can lead to data loss and unexpected costs. Moreover, if your device is lost or stolen, a remote lock or wipe will shield your personal information from prying eyes.
- Sophos Secure Workspace is an app for iOS and Android phones that provides a secure workspace for your important documents: Browse, manage, edit, share, encrypt and decrypt documents from various storage providers or distributed by your company. It is designed to prevent any data loss even when your device gets stolen or you send a document to an unintended source.

  Files can be decrypted and viewed in a seamless way. Encrypted files can be handed over by other apps and uploaded to one of the supported cloud storage providers. Alternatively the documents can be stored locally within the app.

  With Sophos Secure Workspace you can read files encrypted by SafeGuard Cloud Storage or SafeGuard Data Exchange. Both are modules of SafeGuard Enterprise or one of its different editions. They allow you to encrypt files using a local key. These local keys are derived from a passphrase that is entered by a user. You can only decrypt a file when you know the passphrase that was used to encrypt the file.

  For details of the SafeGuard Cloud Storage and SafeGuard Data Exchange modules please refer to the SafeGuard Enterprise 7.0 documentation on www.sophos.com.

Note: You can activate your licenses in the Sophos Mobile Control configuration wizard. The wizard is launched automatically when you log in to the Sophos Mobile Control web console for the first time after installation.

2 Super administrator rights and tasks

After Sophos Mobile Control installation, the system needs to be set up and customers need to be configured. In Sophos Mobile Control, customers are the tenants that manage the devices of their users. The super administrator is primarily used to set up and manage customers for device management.

As a super administrator, you can:

- Carry out the initial configuration of the Sophos Mobile Control server.

  Note: The configuration wizard is launched automatically when you log in to the Sophos Mobile Control web console for the first time after installation. You need to provide:

  - HTTP proxy credentials (optional)
  - A Standard license key and/or an Advanced license key
  - A certificate to be used for the SSL connection (certificate pinning)
  - SMTP credentials

- Configure technical contact information.
- Enable Sophos Mobile Security and Sophos Secure Workspace management by activating and assigning the SMC Advanced license.

  Note: Sophos Mobile Security and Sophos Secure Workspace management is an optional Sophos Mobile Control module. For further information, see Enable Sophos Mobile Security and Sophos Secure Workspace management (page 11).

- Create and manage customers.
- Define configuration items (for example settings and packages) and clone them to new customers (optional).
- Define configuration items (for example packages, profiles for Android, iOS, Windows Phone 8) and push them to existing customers.
- Configure connections to EAS Proxy servers.
- Configure connections to third-party Network Access Control systems to enable network access management for Android, iOS and Windows Phone 8 devices.
- Configure access whitelist for Sophos Mobile Control web console and Self Service Portal..
- Create different reports for all customers.
- Download all log files from the server as a .zip file.
- Log all actions of administrators of the different customers (**Audit logging**).
- Create other super administrator accounts.

3 Super administrator account

A super administrator has specific rights and tasks in Sophos Mobile Control administration. The first super administrator account is created during Sophos Mobile Control installation. With a super administrator account you log in to the super administrator customer. This customer is also created during Sophos Mobile Control installation. When you log in to the Sophos Mobile Control web console for the first time, a configuration wizard is launched automatically. You need to provide:

- HTTP proxy credentials (optional)
- A Standard license key and/or an Advanced license key
- SSL certificate(s)
- SMTP credentials

Note: As a super administrator you can change these settings in the Sophos Mobile Control web console at any time after initial configuration.

The Sophos Mobile Control web console shows a specific view for the super administrator customer. As a super administrator you can switch from the super administrator customer to other customers any time after login. You can also create new super administrators in the super administrator customer.

3.1 Log in to the super administrator customer

Prerequisites:

- A super administrator account has been created during Sophos Mobile Control setup and you have the credentials (customer, user name and password) for the account.

1. Enter the Sophos Mobile Control web console URL in your preferred web browser, for example https://smc.yourcompany.com/admin.

   The Sophos Mobile Control login page is displayed.

2. In the **Customer** field, enter the super administrator customer.
3. In the **User** and **Password** fields, enter your super administrator user name and password.
4. Click **Login**.

You are logged in to the super administrator customer and the configuration wizard is launched automatically.

After you completed the wizard the super administrator costumer **Dashboard** is displayed. The current customer is displayed in the upper-right corner of the Sophos Mobile Control web console. The super administrator customer is marked by an asterisk and shown at the top of the drop-down list.

3.2 Configuration wizard

Note: As a super administrator you can change these settings in the Sophos Mobile Control web console at any time after initial configuration under **SYSTEM** > **Setup** > **System Setup**.

1. After you have logged in to the Sophos Mobile Control web console the **Welcome** view is displayed. Click **Next**.
2. If you use a HTTP proxy, enter the relevant server details in the **HTTP proxy** view:
   a) Select **Proxy enabled**.
   b) Enter the **Proxy host**.
   c) Enter the **Proxy port**.
   d) Click **Next**.
3. In the **License** view, enter your Sophos Mobile Control Standard license key or request a trial license:
   - **Sophos Mobile Control Standard license key:**

     When you enter the Sophos Mobile Control Standard license key and click **Activate**, you are given the option to enter a Sophos Mobile Control Advanced license key. If you have purchased Advanced licenses, enter the key in the **Advanced license key** field.

   - **Request a trial license:**

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

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

   Click **Next**.
4. In the **SSL** view, enter the certificates to be used for securing the SSL connection between server and clients. The certificates guarantee the authenticity of the server. The clients will only trust the certificates specified here (certificate pinning).
   a) Click the **Auto-discover certificate(s)** button.

      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 by clicking **Upload a file**, selecting the desired file (.CER or .DER) and clicking **Open**.

   The certificates are displayed in the **SSL** view. Sophos Mobile Control supports up to four certificates. If a certificate is no longer valid the client will use any other valid certificate from the list to establish the SSL connection to the server.

   Note: You have to update the list after changing or renewing SSL certificates. It is important to ensure that at least one valid certificate is always available. Otherwise the clients will not trust the server and will no longer connect to it, until the list has been updated.

5. SMTP has to 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 via email. In the **SMTP** view, enter SMTP information and logon credentials:
   - **SMTP host**
   - **Connection Type** (SSL, TSL or plain)
   - **SMTP user**
   - **SMTP password**
   - **Email originator**
   - **Send error emails**: Select this option if you want error mails to be sent, for example in case of an expired APNs certificate.
   - **Email recipient**: Enter the recipients for error mails here.

   Note: To check sending of emails, click the **Send test email** button.
6. Click **Finish**

3.3 Switch to other customers

After you have logged in to the super administrator customer, you can easily switch to other existing customers. Do one of the following:

- In the super administrator customer **Dashboard**, the current customer is displayed in the upper-right corner. The super administrator customer is marked by an asterisk and shown at the top of the drop-down list. Select the customer you have created from the drop-down list.
- On the **Dashboard**, click the blue triangle next to the customer and then click **Choose**.

The Sophos Mobile Control web console **Dashboard** for the selected customer is displayed. For further information, see the *Sophos Mobile Control administrator guide*.

4 The super administrator customer

The super administrator customer is created during Sophos Mobile Control installation together with the first super administrator account. For further information, see the *Sophos Mobile Control installation guide*. The super administrator customer offers a specific view of the Sophos Mobile Control web console. This view is customized for super administrator tasks. The main differences between the super administrator customer web console view and the view for other customers and administrators are:

- **Devices**, **Users** and **Documents** are not available in the menu.

  Note: As devices are not available, the **Dashboard** does not show a view of all managed devices and no new devices can be added to the super administrator customer. Devices can only be added in the customers created by the super administrator. For adding devices you have to switch from the super administrator customer to a regular customer, see Switch to other customers (page 9).

- In the **Compliance rules** view, the button **Check now** is not available. To check devices for compliance according to the criteria defined, you need to switch to the relevant customer.
- In the **About** view, the **Download log files (ZIP file)** for downloading all log files in a .zip file is available, see Download log files (page 29).
- In the **Dashboard**, you can create new customers. For further information, see Create customers (page 15).
- In the **Reports** view you can create and export:
  - **Device reports**
  - **App reports**
  - **Compliance reports**
- Under **SYSTEM** > **System setup** as a super administrator you can configure:
  - **License** (initially done by means of the configuration wizard)
  - **SSL** (initially done by means of the configuration wizard)
  - **iOS APNS** (see the *Sophos Mobile Control Administrator help*)
  - **EAS proxy**
  - **Network Access Control**
  - **SMTP** (initially done by means of the configuration wizard)
  - **HTTP proxy** (initially done by means of the configuration wizard)
  - **Access whitelist**
  - **Audit logging**

For a description of the web console interface for regular customers and administrators, refer to the *Sophos Mobile Control administrator guide*.

5 Enable Sophos Mobile Security and Sophos Secure Workspace management

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

Sophos Secure Workspace is an encryption app for iOS and Android phones and tablets that can be managed from Sophos Mobile Control.

Sophos Mobile Security and Sophos Secure Workspace management is an optional Sophos Mobile Control module. In order to manage these apps from Sophos Mobile Control, an SMC Advanced license needs to be available and activated in the Sophos Mobile Control web console.

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

For further information on managing Sophos Mobile Security and Sophos Secure Workspace from the Sophos Mobile Control web console, see the *Sophos Mobile Control administrator guide*.

5.1 Activate Sophos Mobile Security and Sophos Secure Workspace licenses

1. In the web console, under **SYSTEM**, click **Setup** and then **System setup**.

   The **System setup** view is displayed.

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

The Sophos Mobile Security and Sophos Secure Workspace licenses are activated. The **Active license key** field shows the activated license key. The **Number of licenses** field shows the number of available end users. The **Valid until** field shows the license expiry date.

In the **About** view, the relevant license information is shown in the fields **Number of user licenses**, **Licenses used** and **License valid until**. You can assign the required number of end user licenses to individual customers when you create or edit customers.

5.2 Assign licenses to customers

1. Create a customer or open an existing one for editing, see Create customers (page 15) or Edit customers (page 18).

   The **Edit customer** view is displayed.

2. Activate the **Advanced licenses** option.

   The customer may now manage Sophos Mobile Security and Sophos Mobile Encryption.

3. Click the **Save** button.

6 Configure technical contact

To support users who have questions or problems, you can configure technical contact information. The information you enter here will be displayed in the Sophos Mobile Control app and in the Self Service Portal.

1. In the web console, under **SYSTEM**, click **Setup** and then **General**.

   The **General settings** view is displayed.

2. Go to the **Technical contact** tab.
3. Enter the required information for the technical contact. Under **Additional information**, you can enter information for supporting users who have questions or problems.
4. Click the **Save** button.

For end users the technical contact information is shown in the Sophos Mobile Control app on iOS, Android and Windows Phone 8 devices. When you create a new customer and select **Clone settings - Settings and packages**, the technical contact information is automatically copied to the new customer.

7 Manage customers

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

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

7.1 Customer overview on the Dashboard

On the super administrator customer **Dashboard**, an overview of all existing regular customers is shown. The table shows the following information:

Column	Description
Name	Shows the name of the customer.
Activated state	Indicates if the customer is activated.
Valid until	Shows the expiry date of the customer, if specified. Otherwise this column shows **unlimited**. When the expiry date for a customer has passed, the date in the **Valid until** column is shown in red.
Licenses	Shows the maximum number of Sophos Mobile Control licenses that can be used for the customer, if specified. Otherwise this column shows **unlimited**.
Advanced	Shows if the customer has an SMC Advanced license to manage Sophos Mobile Security and Sophos Secure Workspace. For further information, see Enable Sophos Mobile Security and Sophos Secure Workspace management (page 11).
Devices	Shows the number of devices registered for this customer.
AND	Shows the number of Android devices registered for this customer.
iOS	Shows the number of iOS devices registered for this customer.

Column	Description
WP8	Shows the number of Windows Phone 8 devices registered for this customer.
Directory	Indicates the type of user management used for the customer: internal directory, external directory or none.

7.2 Create customers

1. In the super administrator customer **Dashboard**, click the **Create customer** button.
2. The **Edit customer** view is displayed.
3. Enter a **Name** and a **Description** for the new customer.
4. In the **Maximum number of licenses** field, define how many users can be managed for this customer.
5. If you have activated an SMC Advanced license, the **Advanced licenses** checkbox is displayed. Select **Advanced licenses**, if you want the customer to be capable of managing Sophos Mobile Security and Sophos Secure Workspace. For further information, see the *Sophos Mobile Control administrator guide*.
6. In the **Valid until** field, specify the expiry date for the customer. If you do not specify an expiry date here, **unlimited** is shown in the **Valid until** column in the customer overview.
7. Under **Activated platforms**, select the platforms for which devices may be registered for the customer.
8. Under **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.
9. Under **Clone Settings**, select the **Settings and packages** checkbox if you want all profiles, bundles, and packages created in the super administrator account to be available in the customer's account, see Clone configuration items to new customers (page 20).
10. Under **User directory**, select the data source for the Self Service Portal (SSP) users to be managed by Sophos Mobile Control:
    - **None. No SSP and user-specific profiles available.**
    - Select **Internal directory** to use internal user management for users of the Sophos Mobile Control Self Service Portal. For further information, see the *Sophos Mobile Control administrator guide*.
    - Select **External LDAP directory** to use external user management for users of the Sophos Mobile Control Self Service Portal. Click **Configure external LDAP** to specify the server details, see Configure external directory connection for Self Service Portal user management (page 16).
11. Click the **Save** button.

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

7.3 Create an administrator for the new customer

1. Switch to the new customer: In the super administrator customer **Dashboard**, the current customer is displayed in the upper-right corner. The super administrator customer is marked by an asterisk and shown at the top of the drop-down list. Select the customer you have created from the drop-down list.

   The Sophos Mobile Control web console changes from the specific super administrator view to the regular view. You can now carry out further required steps for initial configuration.

2. In the web console, under **SYSTEM**, click **Setup** and then click **Administrators**.

   The **Show administrators** view is displayed.

3. Click the **Create administrator** button.

   The **Edit administrator** view is displayed.

4. Enter a **Login name** for the new user.
5. In the **Role** field, select the user role **Administrator**.
6. Enter the **First name** and the **Last name** of the new user.
7. Enter the **Email address** of the new user.
8. Enter a one-time **Password** for the first login at the web console and confirm it.
9. Click the **Save** button.

The new administrator is created. You can hand over these adminstrator credentials to a person, who then can manage this customer. At first login the administrator will be prompted to change the password.

7.4 Configure external directory connection for Self Service Portal user management

For the Sophos Mobile Control Self Service Portal, external user management can be used. With external user management, you can assign phones to groups and profiles based on external directory membership.

The Self Service Portal allows end users to register their own devices and carry out other tasks without having to contact the helpdesk. For further information on how to configure settings for the Self Service Portal, see the *Sophos Mobile Control administrator guide*.

As a super administrator, you can configure an external directory connection for a costumer to use external user management for Self Service Portal users.

7.4.1 Configure external directory connection

1. Create a new customer or open an existing one for editing, see Create customers (page 15) or Edit customers (page 18).

   The **Edit customer** view is displayed.

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

   The **Server details** view is displayed.

4. In this view, enter the following:

   a) Select the **LDAP type**. Sophos Mobile Control supports:

   - **Active Directory**
   - **Domino**
   - **eDirectory**
   - **Zimbra**

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

   c) 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.

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

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

   Click **Next**.

   The **Search base** view is displayed.

5. Select the external directory search base. The search base defines where to search for the user/the 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 directory fields are to be used for resolving the placeholders %_USERNAME_% and %_EMAILADDRESS_% in profiles. Select the required fields from the **User name** and **Email** drop-down lists.
7. Click **Next**.

   The **SSP configuration** view is displayed.

8. 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 directory server. All members of this group can access the Self Service Portal. If you do not want to restrict access to one group, enter * to allow all authenticated directory users access to the Self Service Portal. After you have entered the group, click the **Resolve group** button to resolve the group name into a complete Distinguished Name (DN).

   Note: The group you specify here is not identical to the Self Service Portal configuration group you define as an administrator for each customer under **Settings** in the **Group settings** tab of the **Self Service Portal** view. There you can define task bundles, Sophos Mobile Control group membership and the mobile platforms for each directory group. For further information, see the *Sophos Mobile Control administrator help*.

9. Click **Apply**.

   The **Edit customer** view is displayed again.

10. Click **Save**.

7.5 Edit customers

1. On the super administrator customer **Dashboard**, locate the customer you want to edit, click the blue triangle next to the customer and then click **Edit**.
2. The **Edit customer** view is displayed.
3. Make the required changes.

   Note: You cannot deselect customers under **Assigned customers** which use a task bundle as compliance action or **Enrollment package**. These customers are greyed out. For further information, see the *Sophos Mobile Control administrator guide*.

4. Click the **Save** button.

7.6 Deactivate customers

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

1. On the super administrator customer **Dashboard**, locate the customer you want to edit, click the blue triangle next to the customer and then click **Edit**.
2. The **Edit customer** view is displayed.
3. Select the **Deactivate account** option.

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

7.7 Delete customers

You can delete customers that have no devices registered with Sophos Mobile Control.

1. On the super administrator customer **Dashboard**, locate the customer you want to edit, click the blue triangle next to the customer. and then click **Edit**.
2. Click **Delete**.

   Note: This icon is only available, if no devices are registered for the customer.

3. In the message displayed, confirm that you want to delete the customer.

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

Note: You cannot deleted a customer, which has devices assigned.

7.8 Create customer reports

In the web console, under **Reports** the following reports are available for super administrators:

- Device reports
  - Devices
  - Devices per user
  - Number of devices by OS version
  - Devices enrolled in last 7 days
  - Devices not synchronized in last 7 days
  - Devices checked out in last 7 days
  - Devices wiped in last 7 days
- App reports
  - Apps on all platforms
  - Number of apps on all platforms
  - Apps on Android
  - Apps on iOS
- Compliance reports
  - Compliance violations
  - Number of compliance violations

Click on a report to export the information to a Microsoft Excel file.

7.8.1 Export customer list

You can export a customer list from the **Dashboard** in Microsoft Excel or text format (.csv):

1. Click the **Export** button at the end of customer list. Select to export the displayed page only (**This page**) or **All pages** and the format (Microsoft Excel or text).

   A dialog to open or to save the file is displayed.

2. Open or save the file.

Note: The customer list takes any filters currently set into consideration. If the list does not contain the expected results, check if the customer filter is set.

8 Manage configuration items

As a super administrator you can define device groups, profiles, task bundles, apps, settings and compliance rules in the super administrator customer and apply them to other customers:

- When you create customers, you can define that **Settings and packages** that you have defined in the super administrator customer are cloned to new customers.
- You can create profiles and packages in the super administrator customer and push them to existing customers.

Note: Configuration items pushed to existing customers cannot be edited or deleted in these customers. For example: An inherited app cannot be edited or deleted. If administrators have the required rights, they can copy the package and edit it. Inherited software packages that have been added to task bundles can no longer be deleted by the super administrator in the super administrator customer.

- When you create customers, all existing device groups are copied to new customers.

For information on how to define the required configuration items, see the *Sophos Mobile Control administrator guide*.

8.1 Clone configuration items to new customers

As a super administrator you can define the following configuration items and clone them to new customers:

- Device groups
- Profiles for Apple iOS, Android, Windows Phone 8
- Task bundles for Apple iOS and Android
- Apps for Apple iOS, Android and Windows Phone 8
- Settings:
  - **General** settings
    - **Password policies** settings
    - **iOS client**
    - **Windows Phone client** settings
    - **Email configuration** settings
    - **Technical Contact** settings
  - **Self Service Portal** settings
    - **Configuration** settings
    - **Agreement** settings

- **Group settings**
- **Post-install text** settings

- Compliance rules

Note: For information on how to define configuration items, see the *Sophos Mobile Control administrator guide*.

To clone configuration items to new customers:

1. Create a new customer (see Create customers (page 15)).
2. Under **Clone settings**, select **Settings and packages**.
3. Click the blue **Save** icon.

The settings and packages are transferred to the new customer. They can be edited in the new customer.

8.2 Push configuration items to existing customers

As a super administrator you can define the following configuration items in the super administrator customer and push them to existing customers:

- Profiles for Android, Apple iOS and Windows Phone 8
- Task bundles Apple iOS and Android
- Apps for Apple iOS, Android and Windows Phone 8
- Profiles for Apple iOS, Android and Windows Phone 8

Note: For information on how to create one of the configuration items listed, see the *Sophos Mobile Control administrator guide*.

To push configuration items to existing customers:

1. In the super administrator customer, create the configuration item that you want to push.
2. From the Sophos Mobile Control menu bar, select the relevant configuration item, for example a task bundle under **Task bundles**.

   The overview table for the selected configuration item is displayed.

3. Click the blue triangle next to the configuration item and then click **Edit**.

   The **Edit** view for the selected configuration item is displayed.

4. Click the **Show** button next to the **Assigned customers** option.
5. Select the customer(s) the configuration item is to be pushed to.

   Note: You cannot deselect customers which use a task bundle as compliance action or **Enrollment package**. These customers are greyed out. For further information, see the *Sophos Mobile Control administrator guide*.

6. Click the blue **Save** button.

The configuration item is applied to the customer(s) selected.

Note: Configuration items pushed to existing customers cannot be edited or deleted in these customers. For example: An inherited software package cannot be edited or deleted. If administrators have the required rights, they can copy the package and edit it. Inherited software packages that have been added to task bundles can no longer be deleted by the super administrator in the super administrator customer.

9 Define customer preselection settings for login to the Self Service Portal

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

In the web console, you can configure settings for the use of the Self Service Portal, for example for which platforms registration through the Self Service Portal should be active or which functions should be available in the Self Service Portal. You can also manage the users of the Self Service Portal. For further information, see the *Sophos Mobile Control administrator guide*.

As a super administrator you can preselect the default customer for end users for their login at the Self Service Portal.

1. In the web console under **SYSTEM**, click **Setup** and then click **Self Service Portal**.

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

2. In the **Configuration** tab under **Login customer preselection**, select **Default customer** and select the required costumer from the drop-down list.
3. If you want end users to be able to see the customer and change it when logging on, make sure that the **visible and editable** checkbox is selected.
4. Click the **Save** button.

10 Configure connections to EAS proxy servers

With Sophos Mobile Control you can set up connections to internal and external EAS Proxy servers with several instances.

10.1 Configure internal EAS proxy server

1. In the web console, under **SYSTEM**, click **Setup** and then **System setup**.
2. Go to the **EAS proxy** tab.
3. In the **Internal** section enter the Exchange or groupware server URL in the **Exchange/groupware server URL** text field.
4. Select **Use SSL** to use a secure connection.
5. To test the connection click **Check connection**.

   A message will be displayed if the server can be reached.

6. Click **Save**.

10.2 Configure external EAS proxy server

For setting up an external EAS proxy server Sophos Mobile Control offers a separate EAS Proxy installer. 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 **SYSTEM** > **Setup** > **System Setup** on the **EAS Proxy** tab.

To configure connections to 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.

10.2.1 Upload EAS Proxy certificate

1. In the web console under **SYSTEM**, click **Setup** and then click **System setup** and go to the **EAS proxy** tab.
2. On the **EAS Proxy** tab, in the **External** section, click **Upload a file** and browse for the certificate. Click **Open**.

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

3. Click **Save**.

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

11 Configure Network Access Control

Sophos Mobile Control offers an interface to third-party Network Access Control (NAC) systems. By configuring connections to NAC systems you can allow them to obtain a list of devices and their compliance states. In compliance rules, you can define that network access should be denied if compliance rules are not met, if you have configured Network Access Control as described in this section. For further information on how to define compliance rules, see the *Sophos Mobile Control administrator guide*.

1. In the web console, under **SYSTEM**, click **Setup** and then click **System setup**.

   The **System setup** view is displayed.

2. Go to the **Network Access Control** tab.
3. You can select the following integrations:

   - **Sophos UTM**

     This setting enables Sophos UTM integration (version 9.2 and higher). The integration requires you to set the SMC server URL and admin user credentials in the UTM WebAdmin under Management - Sophos Mobile Control, as described in the UTM online help.

   - **Cisco ISE**

     This setting enables Cisco ISE integration. The integration requires setting the SMC server URL and the following credentials on the ISE:

     User name: The string displayed here is the user name that has to be specified in Cisco ISE. It is used by Cisco ISE to log in to Sophos Mobile Control

     Password: In this field specify the password for logging in to Sophos Mobile Control

     Password confirmation: Confirm the password.

     Redirect page for disallowed devices: Devices that are not allowed to access the network are redirected to the web page entered her.

     Usually this is the URL of the Self Service Portal or of an information page with a link to the Self Service Portal.

   - **Check Point**

     This setting enables Check Point integration. The integration requires some specific settings on the security gateway (version R77.10 and higher). Click the link on the Network Access Control tab to see details.

     User name: The string displayed here is the user name that has to be specified in Check Point. It is used by Check Point to log in to Sophos Mobile Control.

     Password: In this field specify the password for logging in to Sophos Mobile Control

     Password confirmation: Confirm the password.

- **Custom**

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

12 Configure access whitelists

In the Sophos Mobile we console you can configure IP range access whitelists for accessing the Sophos Mobile web console (**Admin portal**) and the **Self Service Portal** and timeouts for these portals.

Note:

Enter only valid IP addresses or subnets. Otherwise, you cannot access the web portals. To enable access from any IP address or network, leave the fields empty.

1. In the web console, under **SYSTEM**, click **Setup** and then click **System setup**.

   The **System setup** view is displayed.

2. Go to the **Access whitelist** tab.
3. Select the timeouts for the **Admin portal** and the **Self Service Portal** from the drop-down lists.

   The sessions will be closed automatically after the preset time period without user interaction.

4. Enter the IP ranges in the text fields under **Admin portal** and **Self Service portal** and click **Add**. Example: 10.1.0.0/8 or 192.168.100.0/24.

   The IP addresses are displayed in the **IP address** list.

5. Click **Save**.

13 Configure audit logging

Sophos Mobile Control's Audit logging functionality allows to log all actions of administrators of the different customers to the database. Sophos Mobile Control logs the following:

- The **Date** of the action
- The **Action**
- The **User** who performed the action
- The Customer the administrator belongs to
- A description of the action performed (**Log data**)

In order to use the **Audit logging** functionality you have to enable it first:

1. In the web console, under **SYSTEM**, click **Setup** and then click **System setup**.

   The **System setup** view is displayed.

2. Go to the **Audit logging** tab.
3. On the **Audit logging** tab click **Enable Audit logging**.

The **Audit logging** functionality is activated. **Audit logging** is displayed in the web console under **INFORM**.

Note: The SMC service needs to be restarted for the changes to take effect.

13.1 View audit log

To display the audit log:

1. In the web console, under **INFORM**, click **Audit logging**.

   The **Audit logging** view is displayed.

2. Enter a **From** and a **To** date.
   Clicking in the date edit fields displays a calendar to select date and time.
3. Click **Show log**.

All log entries for the specified time are displayed in a table. Click **Export** in the lower right-hand corner to export the audit log to an XLS or .TXT file.

14 Download log files

As a super administrator, you can download all log files from the server in a .zip file. The .zip file contains all log files of the past five days.

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

   The **About** view is displayed.

2. Click the **Download log files (ZIP file)** button.

   A file download dialog is displayed.

3. Click **Save** to save the .zip file to the required location.

15 Create new super administrators

1. In the web console, under **System** click Setup and then click **Administrators**.

   The **Show administrators** view is displayed.

2. Click the **Create administrator** button.

   The **Edit administrator** view is displayed.

3. Enter a **Login name** for the new user.
4. In the **Role** field, select **Administrator**.
5. Enter the **First name** and the **Last name** of the new user.
6. Enter the **Email** address of the new user.
7. Enter a one-time **Password** for the first login at the web console and confirm it.
8. Click the **Save** button.

The new administrator is created and shown in the **Show administrator** view. Forward the credentials (user, customer and one-time password) to the new administrator. The new administrator can log in at the web console with them and is prompted to change the password.

16 Technical support

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

- Visit the SophosTalk 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.

17 Legal notices