SOPHOS

Security made simple.

Sophos Mobile in Central startup guide

Product version: 7.1

Contents

1 About this guide

This guide explains how to set up Sophos Mobile when it is managed through Sophos Central.

Further information is available in the Sophos Mobile administrator help.

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

2 What are the key steps?

To start using Sophos Mobile:

1. Optional: Activate your SMC Advanced licenses for managing the Sophos Mobile Security, Sophos Secure Workspace and Sophos Secure Email apps.
2. Configure personal settings, technical support contact details, and settings for the Self Service Portal.
3. Upload an Apple Push Notification service certificate to manage iOS devices.
4. Optional: Set up a standalone EAS proxy to filter email traffic from the managed devices to an email server.
5. Create compliance policies.
6. Create device groups.
7. Configure devices.
8. Update Self Service Portal settings.
9. Test device enrollment in the Self Service Portal.

3 Activate SMC Advanced licenses

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

You activate SMC Advanced licenses from Sophos Central Admin:

1. In Sophos Central Admin, click your account name (upper right of the user interface), select **Licensing** and then enter your license key in the **Apply Activation Code** field.

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

4 Configure settings

Configure the following settings:

- Personal settings, for example the platforms you want to manage
- Technical support contact details
- Self Service Portal settings

4.1 Configure personal settings

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

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

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

2. Configure the following settings:

Option	Description
Timezone	Select the timezone in which dates are shown.
Unit system	Select the unit system for length values (**Metric** or **Imperial**).
Lines per page in tables	Select the maximum number of table lines you want to display per page.
Show extended device details	Select this check box to show all available information about the device. The **Custom properties** and **Internal properties** tabs will be added to the **Show device** page.
Activated platforms	Select the platforms you want to manage: ▪ **Android** ▪ **Android Things** ▪ **iOS** ▪ **Windows Mobile** (includes Windows Phone 8.1 and Windows 10 Mobile operating systems) ▪ **Windows Desktop** ▪ **Windows IoT** Based on your platform selection, the user interface of the Sophos Mobile console is adjusted. Only views and features that are relevant for the selected platforms are shown.

3. Click **Save**.

4.2 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.

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**.

4.3 Configure Self Service Portal settings

1. On the menu sidebar, under **SETTINGS**, click **Setup** > **Self Service Portal**.

   The **Self Service Portal** page opens.

2. On the **Configuration** tab, configure the Self Service Portal settings as required.

   If you are not sure which settings to apply at this stage, we recommend that you use the default settings.

   For a detailed description of the settings, click **Help** in the page header.

3. On the **Terms of use** tab, click **Edit** to enter a mobile policy, disclaimer or agreement text.

   This text is displayed at the beginning of the device registration. Users have to accept the text before they can perform the registration.

   Tip: You can use the editor toolbar to apply basic HTML formatting to the text. This also applies to the post-install text described in the next step.

4. Optional: On the **Post-install text** tab, click **Edit** to enter text that is displayed at the end of the device registration.

   You can use this text to explain any steps the user has to perform after the registration.

5. Click **Save**.

5 Apple Push Notification service certificates

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

APNs certificates have a validity period of one year.

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

5.1 Requirements

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

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

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

5.2 Create an APNs certificate

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

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

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

   This saves the certificate signing request file `apple.csr` to your local computer.

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

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

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

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

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

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

   This opens the Apple Push Certificates Portal.

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

7. Download the `.pem` APNs certificate file and save it to your computer.
8. In the **Upload APNs certificate** step, click **Upload certificate** and then browse for the `.pem` file that you received from the Apple Push Certificates Portal.
9. Click **Save** to add the APNs certificate to Sophos Mobile.

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

6 Standalone EAS proxy

You can set up an EAS proxy to control the access of your managed devices to an email server. Email traffic of your managed devices is routed through that proxy. You can block email access for devices, for example a device that violates a compliance rule.

The devices must be configured to use the EAS proxy as email server for incoming and outgoing emails. The EAS proxy will only forward traffic to the actual email server if the device is known in Sophos Mobile and matches the required policies. This guarantees higher security as the email server does not need to be accessible from the Internet and only devices that are authorized (correctly configured, for example with passcode guidelines) can access it. Also, you can configure the EAS proxy to block access from specific devices.

The standalone EAS proxy is downloaded and installed separately from Sophos Mobile. It communicates with the Sophos Mobile server through an HTTPS web interface.

Features

- Support for multiple Microsoft Exchange or IBM Notes Traveler email servers. You can set up one EAS proxy instance per email server.

- Load balancer support. You can set up standalone EAS proxy instances on several computers and then use a load balancer to distribute the client requests among them.

- Support for certificate-based client authentication. You can select a certificate from a certification authority (CA), from which the client certificates must be derived.

- Support for email access control through PowerShell. In this scenario, the EAS proxy service communicates with the email server through PowerShell to control the email access of your managed devices. Email traffic happens directly from the devices to the email server and is not routed through a proxy. See Set up email access control through PowerShell (page 14).

Note: For non-iOS devices, filtering abilities of the standalone EAS proxy are limited due to the specifics of the IBM Notes Traveler protocol. Traveler clients on non-iOS devices do not send the device ID with every request. Requests without a device ID are still forwarded to the Traveler server, even though the EAS proxy is not able to verify that the device is authorized.

6.1 Download the EAS proxy installer

1. Log in to Sophos Central Admin.
2. On the menu sidebar, under **My Products**, click **Mobile**.
3. On the menu sidebar of the **Mobile** view, under **SETTINGS**, click **Setup** > **System setup** and then click the **EAS proxy** tab.
4. Under **External**, click the link to download the EAS proxy installer.

The installer file is saved to your local computer.

6.2 Install the standalone EAS proxy

Prerequisite:

- All required email servers are accessible. The EAS proxy installer will not configure connections to servers that are not available.

- You are an administrator on the computer where you install the EAS proxy.

Note: The Sophos Mobile server deployment guide contains schematic diagrams for the integration of the standalone EAS proxy into your company's infrastructure. We recommend that you read the information before performing the installation and deployment of the standalone EAS proxy.

1. Run `Sophos Mobile Control EAS Proxy Setup.exe` to start the **Sophos Mobile Control EAS Proxy - Setup Wizard**.

2. On the **Choose Install Location** page, choose the destination folder and click **Install** to start installation.

   After the installation has been completed, the **Sophos Mobile Control EAS Proxy - Configuration Wizard** is started automatically and guides you through the configuration steps.

3. In the **SMC Server configuration** dialog, enter the URL of the SMC server that the EAS proxy will connect with.

   You should also select **Use SSL for incoming connections (Clients to EAS Proxy)** to secure the communication between clients and the EAS proxy.

   Optionally, select **Use client certificates for authentication** if you want the clients to use a certificate in addition to the EAS proxy credentials for authentication. This adds an additional layer of security to the connection.

   Select **Allow all certificates** if your Sophos Mobile server presents varying certificates to the EAS proxy, for example because there are several server instances behind a load balancer, and each instance uses a different certificate. When this option is selected, the EAS proxy will accept any certificate from the Sophos Mobile server.

   Important: Because the **Allow all certificates** option reduces the security level of the server communication, we strongly recommend that you select it only if required by your network environment.

4. If you selected **Use SSL for incoming connections (Clients to EAS Proxy)** before, the **Configure server certificate** page is displayed. On this page you create or import a certificate for the secure (HTTPS) access to the EAS proxy.

   Note: You can download an SSL Certificate Wizard from MySophos to request your SSL certificate for the Sophos Mobile EAS proxy.

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

   - If you do not have a trusted certificate yet, select **Create self-signed certificate**.

   - If you have a trusted certificate, click **Import a certificate from a trusted issuer** and select one of the following options from the list:

     - **PKCS12 with certificate, private key and certificate chain (intermediate and CA)**

     - **Separate files for certificate, private key, intermediate and CA certificate**

5. On the next page, enter the relevant certificate information, depending on the type of certificate that you selected.

   Note: For a self-signed certificate, you need to specify a server that is accessible from the client devices.

6. If you selected **Use client certificates for authentication** before, the **SMC client authentication configuration** page is displayed. On this page, you select a certificate from a certification authority (CA), from which the client certificates must be derived.

   When a client tries to connect, the EAS proxy will check if the client certificate is derived from the CA that you specify here.

7. On the **EAS Proxy instance setup** page, configure one or more EAS proxy instances.

   - **Instance type**: Select **EAS proxy**.
   - **Instance name**: A name to identify the instance.
   - **Server port**: The port of the EAS proxy for incoming email traffic. If you set up more than one proxy instance, each of these must use a different port.
   - **Require client certificate authentication**: Email clients must authenticate themselves when connecting to the EAS proxy.
   - **ActiveSync server**: The name or IP address of the server with which the proxy instance will connect.
   - **SSL**: Communication between the proxy instance and the ActiveSync server is secured by SSL.
   - **Allow EWS subscription requests from Secure Email**: Select this 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.

     Note: 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.

   - **Enable Traveler client access**: Only select this check box if you need to allow access by IBM Notes Traveler clients on non-iOS devices.

8. After entering the instance information, click **Add** to add the instance to the **Instances** list.

   For every proxy instance, the installer creates a certificate that you need to upload to the Sophos Mobile server. After you have clicked **Add**, a message window opens, explaining how to upload the certificate.

9. In the message window, click **OK**.

   This will open a dialog, showing the folder in which the certificate has been created.

   Note: You can also open the dialog by selecting the relevant instance and clicking the **Export config and upload to SMC** link on the **EAS Proxy instance setup** page.

10. Make a note of the certificate folder. You need this information when you upload the certificate to Sophos Mobile.

11. Optional: Click **Add** again to configure additional EAS proxy instances.

12. When you have configured all required EAS proxy instances, click **Next**.

    The server ports that you entered are tested and inbound rules for the Windows Firewall are configured.

13. On the **Allowed mail user agents** page, you can specify mail user agents (i.e. email client applications) that are allowed to connect to the EAS proxy. When a client connects to the EAS proxy using an email application that is not specified, the request will be rejected.

   - Select **Allow all mail user agents** to configure no restriction.
   - Select **Only allow the specified mail user agents** and then select a mail user agent from the list. Click **Add** to add the entry to the list of allowed agents. Repeat this for all mail user agents that are allowed to connect to the EAS proxy.

14. On the **Sophos Mobile Control EAS Proxy - Configuration Wizard finished** page, click **Finish** to close the Configuration Wizard and return to the Setup Wizard.

15. In the Setup Wizard, make sure that the **Start Sophos Mobile Control EAS Proxy server now** check box is selected, then click **Finish** to complete the configuration and to start the Sophos Mobile EAS proxy for the first time.

To complete the EAS proxy configuration, upload the certificates that were created for every proxy instance to Sophos Mobile:

16. Log in to Sophos Central Admin.

17. On the menu sidebar, under **My Products**, click **Mobile**.

18. On the menu sidebar of the **Mobile** view, under **SETTINGS**, click **Setup** > **System setup** and then click the **EAS proxy** tab.

19. Under **External**, click **Upload a file**. Upload the certificate that the setup wizard created for the PowerShell connection.

   If you have set up more than one instance, repeat this for all instance certificates.

20. Click **Save**.

21. In Windows, open the **Services** dialog and restart the **EASProxy** service.

This completes the initial setup of the standalone EAS proxy.

Note: Every day, the EAS proxy log entries are moved to a new file, using the naming pattern `EASProxy.log.yyyy-mm-dd`. These daily log files are not deleted automatically and thus may cause disk space issues over time. We recommend that you set up a process to move the log files to a backup location.

6.3 Set up email access control through PowerShell

You can set up a PowerShell connection to an Exchange or an Office 365 server. This means that the EAS proxy service communicates with the email server through PowerShell to control the email access for your managed devices. Email traffic is routed directly from the devices to the email server. It is not routed through a proxy.

The PowerShell scenario has these advantages:

- Devices communicate directly with the Exchange server.

- You do not need to open a port on your server for incoming email traffic from your managed devices.

Supported email servers are:

- Exchange Server 2010

- Exchange Server 2013

- Exchange Server 2016
- Office 365 with an Exchange Online plan

To set up PowerShell:

1. Configure PowerShell.
2. Create a service account on the Exchange server or in Office 365. This account is used by Sophos Mobile to execute PowerShell commands.
3. Set up one or more PowerShell connection instances to Exchange or Office 365.
4. Upload the instance certificates to Sophos Mobile.

Configure PowerShell

1. On the computer on which you are going to install the EAS proxy, open Windows PowerShell, as an administrator, and enter:

```
PS C:\Windows\system32> Set-ExecutionPolicy RemoteSigned
```

Note: If PowerShell is not available, install it as described in the Microsoft article Installing Windows PowerShell (external link).

2. If you want to connect to a local Exchange server, open Windows PowerShell as administrator on that computer and enter the same command as before:

```
PS C:\Windows\system32> Set-ExecutionPolicy RemoteSigned
```

Note: This step is not required for Office 365.

Create a service account

3. Log in to the relevant admin console:

   - For Exchange Server 2010: **Exchange Management Console**
   - For Exchange Server 2013/2016: **Exchange Admin Center**
   - For Office 365: **Office 365 Admin Center**

4. Create a user account. This account is used as a service account by Sophos Mobile to execute PowerShell commands.

   - Use a user name like `smc_powershell` that identifies the account purpose.

   - Turn off the setting to make the user change their password the next time they log in.

   - Remove any Office 365 license that was automatically assigned to the new account. Service accounts don't require a license.

5. Create a new role group and assign it the required permissions.

   - Use a role group name like `smc_powershell`.

   - Add the **Mail Recipients** and **Organization Client Access** roles.

   - Add the service account as a member.

Set up PowerShell connections

6. Use the setup wizard as if you would set up a standalone EAS Proxy. In wizard step **EAS Proxy instance setup**, configure the following settings:

   - **Instance type**: Select **PowerShell Exchange/Office 365**.
   - **Instance name**: A name to identify the instance.
   - **Exchange server**: The name or IP address of the Exchange server (for a local Exchange server installation) or `outlook.office365.com` (for Office 365). Don't include a prefix `https://` or a suffix `/powershell`. These are added automatically.
   - **Allow all certificates**: The certificate that the Exchange server presents is not verified. Use this for example if you have a self-signed certificate installed on your Exchange server. Because the **Allow all certificates** option reduces the security level of the server communication, we strongly recommend that you select it only if required by your network environment.
   - **Allow EWS subscription requests from Secure Email**: Select this 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.

     Note: 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.

   - **Service account**: The name of the user account you created in the Exchange or Office 365 admin console.
   - **Password**: The password of the user account.

7. Click **Add** to add the instance to the **Instances** list.
8. **Optional:** Repeat the previous steps to set up PowerShell connections to other Exchange or Office 365 servers.
9. Complete the setup wizard as described in Install the standalone EAS proxy (page 12).

Upload certificates

10. Log in to Sophos Central Admin.
11. On the menu sidebar, under **My Products**, click **Mobile**.
12. On the menu sidebar of the **Mobile** view, under **SETTINGS**, click **Setup** > **System setup** and then click the **EAS proxy** tab.
13. Under **External**, click **Upload a file**. Upload the certificate that the setup wizard created for the PowerShell connection.

    If you have set up more than one instance, repeat this for all instance certificates.

14. Click **Save**.
15. In Windows, open the **Services** dialog and restart the **EASProxy** service.

This completes the initial setup of PowerShell connections. Email traffic between a managed device and the Exchange or Office 365 servers is blocked if the device violates a compliance rule. You can block an individual device by setting the email access mode for that device to **Deny**.

Note: Depending on the configuration of your Exchange server, devices receive a notification when their email access is blocked.

6.4 Configure a connection to the internal EAS proxy server

1. On the menu sidebar, under **SETTINGS**, click **Setup** > **System setup**.
2. On the **System setup** page, click the **EAS proxy** tab.
3. Under **Internal**, 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. 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**.

6.5 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 Standalone EAS proxy (page 11).

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. In the **External** section, 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.
3. Click **Save**.
4. In Windows, open the **Services** dialog and restart the **EASProxy** service.

7 Compliance policies

With compliance policies you can:

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

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

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

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

7.1 Create compliance policy

1. On the menu sidebar, under **CONFIGURE**, click **Compliance policies**.
2. On the **Compliance policies** page, click **Create compliance policy**.
3. Enter a name and, optionally, a description for the new set of compliance rules.

Repeat the following steps for all required platforms.

4. Make sure that the **Enable platform** check box on each tab is selected.

   If this check box is not selected, devices of that platform are not checked for compliance.

5. Under **Rule**, configure the compliance rules for the particular platform.

   For a description of the available rules for each device type, click **Help** in the page header.

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

   Note: For devices where Sophos Mobile manages the Sophos container instead of the whole device, only a subset of compliance rules is applicable. In **Highlight rules**, select a management type to highlight the rules that are relevant.

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

Option	Description
Deny email	Forbid email access. This action can only be taken if you have configured a connection to the standalone EAS proxy. See Configure a connection to the standalone EAS proxy server (page 17).
Lock container	Disable the Sophos Secure Workspace and Secure Email apps. This affects document, email and web access that is managed by these apps. This action can only be taken when you have activated a Mobile Advanced license. This option is only relevant for Android and iOS devices.
Create alert	Create an alert. The alerts are displayed on the **Alerts** page of Sophos Central Admin.
Transfer task bundle	Transfer a specific task bundle to the device. We recommend that you set this to **None** at this stage. For further information, see the Sophos Mobile administrator help. **Important:** When used incorrectly, task bundles may misconfigure or even wipe devices. To assign the correct task bundles to compliance rules, an in-depth knowledge of the system is required.

Note: These actions are only executed on the first reporting of a violation. If you turn an action on, this only affects future violations.

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

   The new compliance policy is displayed on the **Compliance policies** page.

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

8 Device groups

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

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

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

8.1 Create device group

1. On the menu sidebar, under **MANAGE**, click **Device groups**, and then click **Create device group**.
2. On the **Edit device group** page, enter a name and a description for the new device group.
3. Under **Compliance policies**, select the compliance policies that are applied to corporate and to personal devices.
4. Click **Save**.

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

9 Configure iOS devices

9.1 Create iOS device profile

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

We recommend that you set up separate profiles for:

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

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

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

This section describes how to create profiles in the Sophos Mobile console. For information on how to import profiles created with Apple Configurator, see the Sophos Mobile administrator help.

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

1. On the menu sidebar, under **CONFIGURE**, click **Profiles, policies** > **Apple iOS**.
2. On the **Profiles and policies** page, click **Create** > **Device profile**.
3. On the **Edit profile** page, configure the following settings:

   a) **Name**: Enter a name for the profile. We recommend that you use the name `iOS SSP profile` for profiles that are applied during enrollment in the Self Service Portal.

   b) **Organisation**: Enter the name of the organization for the profile, for example a company name.

   c) **Description**: Enter a description for the profile, for example `base profile`.

4. To add password policies to the profile, click **Add configuration** and then select **Password policies**.
5. On the **Password policies** page, configure the required password settings.

   For a detailed description of the settings, click **Help** in the page header.

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

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

7. To add restrictions to the profile, click **Add configuration** again and then select **Restrictions**.

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

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

    For a detailed description of the settings, click **Help** in the page header.

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

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

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

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

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

9.2 Create task bundle for iOS devices

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

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

3. Enter a name and, optionally, a description for the new task bundle in the relevant fields.

    The version is automatically incremented every time you save the task bundle.

4. Optional: Select **Selectable for compliance actions** to transfer the task bundle onto a device when it violates a compliance rule. See Compliance policies (page 18).

    Note: This option is disabled when you edit an existing task bundle and the task bundle is already used as a compliance action.

5. Optional: Select **Ignore app installation failures** to continue the task bundle processing even if an app installation fails.

6. Click **Create task**, select **Enroll** and enter a name for the task. Click **Apply** to create the task.

    The name that you enter here will be displayed in the Self Service Portal while the task is processed.

7. Click **Create task** again and select **Install profile or assign policy**. Give the task a meaningful name, for example `Install password policies profile`, and select the profile you have created. Click **Apply** to create the task.

8. If you have configured profiles for Exchange ActiveSync, VPN or Wi-Fi settings, repeat the previous step for each profile.

9. Optional: Add further tasks to the task bundle.

    Tip: You can change the installation order of the tasks by using the sort arrows on the right-hand side of the tasks list.

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

The task bundle is available for transfer. It is displayed on the **Task bundles** page.

10 Configure Android devices

10.1 Create Android device profile

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

We recommend that you set up separate profiles for:

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

1. On the menu sidebar, under **CONFIGURE**, click **Profiles, policies** > **Android**.
2. On the **Profiles and policies** page, click **Create** > **Device profile**.
3. On the **Edit profile** page, configure the following settings:

   a) **Name**: Enter a name for the profile. We recommend that you use the name `Android SSP` `profile` for profiles that are applied during enrollment in the Sophos Central Self Service portal.

   b) Optional: **Description**: Enter a description for the profile, for example `base profile`.

4. To add password policies to the profile, click **Add configuration** and then select **Password policies**.

   The **Password policies** page opens.

5. In the **Password type** field, select the type of password you want to define, for example **Complex**.
6. Configure the required password settings.

   The available settings depend on the password type that you selected. For a detailed description of all settings, click **Help** in the page header.

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

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

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

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

   For a detailed description of the settings, click **Help** in the page header.

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

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

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

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

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

10.2 Create task bundle for Android devices

1. On the menu sidebar, under **CONFIGURE**, click **Task bundles** > **Android**.
2. On the **Task bundles** page, click **Create task bundle**.

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

3. Enter a name and, optionally, a description for the new task bundle in the relevant fields.

   The version is automatically incremented every time you save the task bundle.

4. Optional: Select **Selectable for compliance actions** to transfer the task bundle onto a device when it violates a compliance rule. See Compliance policies (page 18).

   Note: This option is disabled when you edit an existing task bundle and the task bundle is already used as a compliance action.

5. Optional: Select **Ignore app installation failures** to continue the task bundle processing even if an app installation fails.
6. Click **Create task**, select **Enroll** and enter a name for the task. Click **Apply** to create the task.

   The name that you enter here will be displayed in the Self Service Portal while the task is processed.

7. Click **Create task** again and select **Install profile or assign policy**. Give the task a meaningful name, for example `Install password policies profile`, and select the profile you have created. Click **Apply** to create the task.
8. If you have configured profiles for Exchange ActiveSync, VPN or Wi-Fi settings, repeat the previous step for each profile.
9. Optional: Add further tasks to the task bundle.

   Tip: You can change the installation order of the tasks by using the sort arrows on the right-hand side of the tasks list.

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

The task bundle is available for transfer. It is displayed on the **Task bundles** page.

11 Update Self Service Portal settings

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

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

   The **Edit group settings** dialog box opens.

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

12 Test device enrollment through the Self Service Portal

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

Log in to the Self Service Portal with a test user account you created for yourself and perform test enrollments for all platforms that you want to manage with Sophos Mobile.

13 Use the device enrollment wizard to assign and enroll new devices

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

- Add a new device to Sophos Mobile.

- Assign a user to the device.

- Enroll the device.

- Optional: Transfer a task bundle to the device.

To start the device enrollment wizard:

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

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

2. On the **Enter user search parameters** wizard page, enter search criteria to look up a user the device will be assigned to.

3. The wizard displays a list of matching users. Select the required user.

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

Option	Description
Platform	The device platform.
Name	A unique name under which the device will be managed by Sophos Mobile.
Description	An optional description of the device.
Phone number	An optional phone number. Enter the number in international format, for example `+491701234567`.
Email address	The email address to which the enrollment instructions are sent. This is the email address of the user assigned to the device, as configured in Sophos Central user management.
Owner	Select the device owner type: either **Corporate** or **Personal**.
Device group	Select the device group the device will be assigned to. If you have not created a device group yet, you can select the device group **Default**, which is always available.

5. Select a task bundle that will be transferred to the device after it has been enrolled. Or select **Only enroll device** to enroll the device without transferring a task bundle.

   When you click **Next**, the device is added to Sophos Mobile.

6. On the **Enrollment** wizard page, follow the instructions to install the Sophos Mobile Control app onto the device and to complete the enrollment and provisioning.

7. When enrollment has been completed successfully, click **Finish** to close the device enrollment wizard.

Note:

- When you have made all the selections, you can close the wizard without having to wait for the **Finish** button to appear. An enrollment task is created and processed in the background.

14 Glossary

device	The device to be managed (for example smartphone, tablet or Windows 10 device).
enrollment	The registration of a device with Sophos Mobile.
Enterprise App Store	An app repository that is hosted on the Sophos Mobile server. The administrator can use the Sophos Mobile console to add apps to the Enterprise App Store. Users can then use the Sophos Mobile Control app to install these apps onto their devices.
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 through Sophos Mobile.
provisioning	The process of installing the Sophos Mobile Control app on a device.
SMSec	Abbreviation for Sophos Mobile Security.
Sophos Central Admin	The web interface that you use to manage devices.
Sophos Central Self Service portal	The web interface that allows users to enroll their own devices and carry out other tasks without having to contact the helpdesk.
Sophos Mobile client	The Sophos Mobile Control app that is installed onto devices managed by Sophos Mobile.
Sophos Mobile Security	A security app for Android devices. You can manage this app with Sophos Mobile, provided that a license of type Mobile Advanced is activated.
Sophos Secure Email	An app for Android and iOS devices that provides a secure container for managing your email, calendar and contacts. You can manage this app with Sophos Mobile, provided that a license of type Mobile Advanced is activated.
Sophos Secure Workspace	An app for Android and iOS devices that provides a secure workspace where you can browse, manage, edit, share, encrypt and decrypt documents from various storage providers or distributed by your company. You can manage this app with Sophos Mobile, provided that a license of type Mobile Advanced is activated.

task bundle	You create a package to bundle several tasks into one transaction. You can bundle all tasks necessary to have a device fully enrolled and running.

15 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.

16 Legal notices