SOPHOS

Cybersecurity
made
simple.

Sophos Mobile

migration guide

product version: 9

Contents

1 About this document

This document explains how to migrate your Sophos Mobile account from Sophos Mobile as a Service to Sophos Central.

2 What’s different in Sophos Central?

The following differences apply between Sophos Mobile as a Service and the Sophos Mobile product in Sophos Central:

Devices

The project-based device platforms “Android Things” and “Windows IoT” are not available.

User accounts

While in Sophos Mobile as a Service you manage users and administrators in separate lists, Sophos Central has a single **People** list. Users and administrators are distinguished by their role:

- Administrator roles (allowed to sign in to Sophos Central Admin): **Super Admin**, **Admin**, **Help Desk**, **Read-only**
- User role (allowed to sign in to the Self Service Portal): **User**

External user management

You can’t dynamically link an external LDAP user directory to Sophos Central. However, there’s a synchronization tool available that lets you create a static copy of your Active Directory users.

Sophos Central only supports Active Directory as an LDAP server.

Sophos SafeGuard Enterprise

Corporate keyring synchronization between the Sophos Secure Workspace app and Sophos SafeGuard Enterprise is not available.

Duo Security

Integration with the Duo Security authentication software is not available.

Password policies

Sophos Central uses common password policies for all users. You can’t configure these.

IT contact

The IT contact you configure in the Sophos Mobile settings is available on the users’ devices but not in the Self Service Portal.

Network Access Control

Integration with third-party Network Access Control (NAC) systems is not available. However, you can use Sophos Wireless integration. When you've registered your Sophos APX Series access points in Sophos Central, you can restrict network access for your managed devices based upon their Sophos Mobile compliance status.

3 Migration overview

To transfer objects and settings to Sophos Central, you can use the Sophos Mobile export/import feature:

1. In Sophos Mobile as a Service, you export your objects and settings to an exchange file.
2. In Sophos Central, you import that exchange file.

Depending on the features you’re using, you must perform additional migration tasks:

- Some features require pre-export tasks in Sophos Mobile as a Service.
- Some features require post-import tasks in Sophos Central.
- Some features require you to transfer items individually.

For details, see Additional migration tasks (page 5).

4 Additional migration tasks

You transfer most objects and settings Sophos Central with the Sophos Mobile export/import feature. Some items can't be transferred this way, or require additional pre-export and post-import tasks.

User accounts

For internal user management, you can transfer users and administrators through a CSV file.

For external user management, you can set up synchronization with your Active Directory server in Sophos Central.

User groups

To migrate user groups for the Self Service Portal, create them in Sophos Central and assign user accounts to them.

Self Service Portal configurations

Because user groups are not transferred, you must manually create them in Sophos Central and assign them to your Self Service Portal configurations.

Devices

To transfer devices, individually unenroll them in Sophos Mobile as a Service and enroll them in Sophos Central.

Tip
Create the **Devices** and the **Device inventory** reports in Sophos Mobile as a Service and refer to that information when enrolling devices in Sophos Central.

Device groups

Device groups configured for iOS auto-enrollment are not exported because they are bound to your Sophos Mobile as a Service server. To export these groups, turn off iOS auto-enrollment in the device group settings. You can turn it on again after you've imported the device groups into Sophos Central.

Because devices are not transferred, imported device groups are empty.

Profiles and policies

To transfer iOS profiles you've added to Sophos Mobile as a Service by import, individually download them from Sophos Mobile as a Service and upload them to Sophos Central.

Imported profiles are:

- Device profiles created in Apple Configurator
- Provisioning profiles for self-developed apps

Apps

To transfer app packages, individually download them from Sophos Mobile as a Service and upload them to Sophos Central.

Documents

To transfer documents, individually download them from Sophos Mobile as a Service and upload them to Sophos Central.

Alert emails

To transfer alert email settings, manually configure them on the **Global Settings** page of Sophos Central Admin.

Settings

To transfer the following settings, you must perform additional pre-export and post-import tasks:

- Apple Device Enrollment Program (DEP)
- Apple Volume Purchase Program (VPP)
- Android enterprise
- Android zero-touch enrollment
- Samsung Knox Mobile Enrollment
- Third-party EMM integration
- Microsoft Intune app protection

Standalone EAS proxy server

To migrate the standalone EAS proxy, adjust the Sophos Mobile server URL in the proxy server configuration and upload the proxy certificate to Sophos Central.

5 Migrate to Sophos Central

Prerequisite: You’ve set up your account in Sophos Central Admin, that is:

- You’ve activated your Sophos Mobile license.
- You’ve configured the settings on the Global Setting pages.
- You have the **Super Admin** role in Sophos Central.

Important
Perform the migration in the order specified below. Otherwise, your migrated data might be incomplete or inconsistent.

Skip steps related to features you’re not using.

1. Set up user and administrator accounts:
    - For internal user management: Transfer users and administrators (page 8).
    - For external (LDAD) user management: Set up synchronization with your Active Directory server. See Sophos Central Admin help - Set up synchronization with Active Directory.
2. Unenroll all devices from Sophos Mobile as a Service.
3. Prepare the export:
    - Prepare Apple Device Enrollment Program (DEP) migration (page 9)
    - Prepare Apple Volume Purchase Program (VPP) migration (page 9)
    - Prepare Android enterprise migration (page 10)
4. Transfer objects and settings with the export/import feature.
5. Transfer additional items manually:
    - Transfer app package files (page 13)
    - Transfer documents (page 13)
    - Transfer imported iOS profiles (page 14)
6. Configure features in Sophos Central:
    - Configure Self Service Portal (page 15)
    - Configure Apple Device Enrollment Program (DEP) (page 15)
    - Configure Apple Volume Purchase Program (VPP) (page 16)
    - Configure Android enterprise enrollment (page 17)
    - Configure Android zero-touch enrollment (page 17)
    - Configure Samsung Knox Mobile Enrollment (page 18)
    - Configure third-party EMM integration (page 18)
    - Configure Microsoft Intune app protection (page 19)
7. Migrate the standalone EAS proxy (page 21).
8. Enroll your devices with Sophos Central.

6 Transfer users and administrators

You transfer Sophos Mobile user and administrator accounts through a CSV file.

Prerequisite:

- You have the **Super Admin** role in Sophos Central.

The following information applies to internal user management. If your Sophos Mobile users and administrators are managed in Active Directory, see the Sophos Central Admin help for details on how to set up synchronization with your Active Directory server.

1. Go to the **People** page in Sophos Mobile as a Service.
2. Underneath the table, click **Export** and then click the TXT icon next to **All pages**.

   A CSV file with the user account details is saved to your computer.
3. Go to **Setup > Administrators** and repeat the previous step to create a CSV file for your administrator accounts.

Perform the remaining steps in Sophos Central Admin:

4. Go to the **People** page.
5. Click **Add > Import users from CSV**.
6. Click the **Template with example data** link.
7. Using the column structure shown in the template CSV file, create a new CSV file from the content of the two files you’ve exported from Sophos Mobile as a Service.
8. Import the new CSV file to Sophos Central.

7 Preparing to export

Some features require additional preparation before the export.

7.1 Prepare Apple Device Enrollment Program (DEP) migration

Before you export your data from Sophos Mobile as a Service, add a new MDM server in the Apple portal and move your DEP devices to it.

> **Note**
> Apple has recently introduced Apple Business Manager to replace their Device Enrollment Program (DEP). If you’ve not upgraded your Apple DEP account to Apple Business Manager yet, replace “Apple Business Manager” by “Apple DEP web portal” in the following description.

1. Set up a virtual MDM server for your Sophos Mobile account in Sophos Central.

   See the Sophos Mobile administrator help for details.
2. In Apple Business Manager, assign all your DEP devices from the MDM server you’ve created for Sophos Mobile as a Service to the new MDM server.
3. Unenroll your DEP devices from Sophos Mobile as a Service.
4. Reset Apple DEP: Go to **Setup > Apple setup > Apple DEP**, and then click **Reset DEP**.
5. In Apple Business Manager, delete the old MDM server.

Related information

Sophos Mobile administrator help - Set up Apple DEP

7.2 Prepare Apple Volume Purchase Program (VPP) migration

Before you export your data from Sophos Mobile as a Service, remove VPP license assignments.

1. Unassign VPP licenses from users:

   a) Go to **Apps > iOS**.

   b) Click a VPP app, click **Show** next to the **VPP licenses** field, and then deselect all users.

   c) Repeat this for all remaining iOS VPP apps, then for all macOS VPP apps.

   You don’t need to unassign VPP licenses from devices. License assignments are automatically removed when you unenroll the devices from Sophos Mobile as a Service.
2. Remove your VPP service token (sToken) from Sophos Mobile as a Service:

   a) Go to **Setup > Apple setup > Apple VPP**.

   b) Click **Remove VPP service token (sToken)**.

7.3 Prepare Android enterprise migration

Before you export your data from Sophos Mobile as a Service, disconnect your Android enterprise account from the Sophos Mobile as a Service server.

1. Go to **Setup > Android setup > Android enterprise**.
2. Click **Unbind**.

8 Transferring items to Sophos Central

To transfer Sophos Mobile objects and settings, you export the data from your Sophos Mobile server to an exchange file and then import that file into Sophos Central.

The following items are transferred:

- Device groups
- Device profiles and policies
- Compliance policies
- Task bundles
- App settings (without app package files)
- App groups
- Self Service Portal configurations (without user group assignments)
- Most system settings

Some settings are bound to a specific Sophos Mobile server and can’t be transferred.

8.1 Export items

To transfer objects and settings from your Sophos Mobile server to Sophos Central, you can export them to an exchange file.

1. On the menu sidebar, under **SETTINGS**, click **Setup > Sophos setup > Export**.

   Under **Export preview**, the items to be exported are displayed.
2. Click **Export**.
3. Set a password for the exchange file.
4. Click **Download**.

The exchange file `sophosmobile.export` is downloaded to your computer. You can import the file into Sophos Central.

8.2 Import items

When you’ve created an exchange file with objects and settings from a Sophos Mobile server, you can import it to Sophos Central.

1. In Sophos Central Admin, go to **Mobile**.
2. Click **Setup > Sophos setup > Import**.
3. Click **Upload exchange file**.
4. Select the exchange file and enter the password you’ve set when exporting the data.
5. Click **Upload**.
6. Under **Import preview**, the items to be imported are listed. Check if there are any warnings.

Important

If there are existing items with the same name as items to be imported, they are overwritten.

7. Click **Import** to import the data into Sophos Central.

9 Transferring items manually

Some Sophos Mobile items can’t be transferred by the export/import feature. You must transfer these individually.

9.1 Transfer app package files

To transfer apps for which you’ve uploaded the package file to Sophos Mobile as a Service, export the package file and upload it again in Sophos Central.

Prerequisite: You’ve transferred your app configurations to Sophos Central.

1. In Sophos Mobile as a Service, go to **Apps**, and then click the platform for which you want to export app packages.
2. In the app table, use the **Source** column to identify the apps that have a package file attached.
3. Click the blue triangle next to an app name and then click **Show**.
4. Click the **Download** icon next to the file name.

   The package file is saved to your computer.
5. Repeat this for all remaining apps and platforms.

Perform the remaining steps in Sophos Central Admin:

6. Go to **Mobile**.
7. Click **Apps**, and then click the platform for which you want upload app packages.
8. Click an app.
9. Click **Upload a file**, upload the package file, and then click **Save**.
10. Repeat this for all remaining apps and platforms.

9.2 Transfer documents

To transfer documents you’ve uploaded to Sophos Mobile as a Service, export them individually and then upload them again to Sophos Central.

1. In Sophos Mobile as a Service, go to **Reports**.
2. Download the **Uploaded documents** report.
3. Go to **Documents**.
4. For each document, click the blue triangle next to the name, click **Show**, and then click the **Download** icon next to the file name.

   The document file is saved to your computer.

Perform the remaining steps in Sophos Central Admin:

5. Go to **Mobile**.
6. Click **Documents > Add document**.
7. Upload the document file and enter the document properties, using the information from the report you’ve created before.
8. Repeat this for all remaining documents.

9.3 Transfer imported iOS profiles

To transfer iOS device profiles you’ve imported from Apple Configurator or provisioning profiles for your self-developed iOS apps, download them individually and then import them again in Sophos Central.

1. In Sophos Mobile as a Service, go to **Profiles, policies > iOS**.
2. For each profile with type **Imported profile**, click the blue triangle next to the name and then click **Download**.

   The profile file is saved to your computer.

Perform the remaining steps in Sophos Central Admin:

3. Go to **Mobile**.
4. Click **Profiles, policies > iOS > Create > Import profile**.
5. Upload the profile file.
6. Repeat this for all remaining profiles.

10 Configuration tasks

Some features require additional configuration after the import.

10.1 Configure Self Service Portal

Your Self Service Portal configurations are included in the data exchange file you export from Sophos Mobile as a Service and then import into Sophos Central. But because user groups are not included, you must manually assign Sophos Central user groups.

Prerequisites:

- You’ve created users and user groups in Sophos Central.
- You’ve imported your data to Sophos Central.

To assign user groups to your Self Service Portal configurations:

1. In Sophos Mobile as a Service, go to **Setup > Self Service Portal**.
2. Underneath the table, click **Export** and then click the TXT icon next to **All pages**.

   A CSV file with the configuration details is saved to your computer.
3. In Sophos Central Admin, go to **Mobile**.
4. Click **Setup > Self Service Portal**.
5. Click a configuration.
6. Click **Add** next to **User groups**.
7. Select the required user group(s), using the information from the report you’ve created before.
8. Save the configuration.
9. Repeat this for all remaining configurations.

   You don’t have to edit the **Default** configuration. This configuration always has the special user group ***** assigned.

Related information

Sophos Mobile administrator help - Configure Self Service Portal settings

10.2 Configure Apple Device Enrollment Program (DEP)

To complete the migration of Apple DEP, create DEP profiles in Sophos Central and assign them to your DEP devices.

Prerequisites:

- You’ve created users and user groups in Sophos Central.
- You’ve imported your data to Sophos Central.

Note
Apple has recently introduced Apple Business Manager to replace their Device Enrollment Program (DEP). If you've not upgraded your Apple DEP account to Apple Business Manager yet, replace "Apple Business Manager" by "Apple DEP web portal" in the following description.

To reconfigure Apple DEP:

1. Duplicate all DEP profiles from Sophos Mobile as a Service to Sophos Mobile in Sophos Central:
   a) In Sophos Mobile as a Service, go to **Setup > Apple setup > Apple DEP profiles**.
      Keep this page open while you're duplicating the DEP profiles.
   b) In Sophos Central Admin, go to **Mobile**.
   c) Click **Setup > Apple setup > Apple DEP profiles**.
   d) Create DEP profiles with the same settings you used in Sophos Mobile as a Service.
      See the Sophos Mobile administrator help for details.
2. Assign the DEP profiles to your devices:

   Note
   You may skip this step if you've configured a default DEP profile.

   a) Go to **Devices > Apple DEP**.
   b) Select the required devices and click **Actions > Assign profile**.
   c) Select the DEP profile you want to assign and click **Ok**.
3. Reset your DEP devices to their factory settings.

When the devices are turned on again, they enroll with your Sophos Mobile account in Sophos Central.

Related information

Sophos Mobile administrator help - Set up Apple DEP
Sophos Mobile administrator help - Create DEP profile

10.3 Configure Apple Volume Purchase Program (VPP)

To complete the migration of Apple VPP, upload your VPP service token (sToken) to Sophos Central.

Prerequisites:

- You've created users and user groups in Sophos Central.
- You've imported your data to Sophos Central.

To reconfigure Apple VPP:

1. In Sophos Central Admin, go to **Mobile**.
2. Click **Setup > Apple setup > Apple VPP**.
3. Upload your VPP sToken file.

You assign VPP apps to devices the same way you did in Sophos Mobile as a Service.

To assign VPP apps to users, you must first assign the user to a device. To do this:

1. You add a device to Sophos Mobile.
2. You assign the user to the device.
3. You invite the user to Apple VPP.
4. You assign a VPP license to the user.
5. The user installs the app through the App Store app on the device.

Related information

Sophos Mobile administrator help - Manage Apple VPP apps

10.4 Configure Android enterprise enrollment

To complete the migration of Apple enterprise enrollment, set up Android enterprise in Sophos Central.

Prerequisites:

- You've created users and user groups in Sophos Central.
- You've imported your data to Sophos Central.

To reconfigure Android enterprise:

- Set up Android enterprise in Sophos Central.

  Use the same Google account (for the Managed Google Account scenario) or domain (for the Managed Google Domain scenario) you used for Android enterprise in Sophos Mobile as a Service.

  For the Managed Google Domain scenario, you can skip these configuration steps:

  — Register your domain with Google.

  — Configure a Google service account.

Note

You don't need to reconfigure your managed Google Play apps (including app configurations) or your managed Google Play layout.

Related information

Sophos Mobile administrator help - Android enterprise

10.5 Configure Android zero-touch enrollment

The zero-touch configuration for Sophos Mobile you've created in the Google zero-touch enrollment portal contains a link to the Sophos Mobile as a Service server. To enroll zero-touch enabled Android devices ("zero-touch devices") with your Sophos Mobile account in Sophos Central, you must create a new configuration.

Prerequisites:

- You've created users and user groups in Sophos Central.
- You've imported your data to Sophos Central.

To reconfigure Android zero-touch enrollment:

1. In Sophos Central Admin, go to **Mobile**.
2. Click **Setup > Android setup > Zero-touch**.
3. Set up zero-touch enrollment the same way you did in Sophos Mobile as a Service.

   Use your settings in Sophos Mobile as a Service and your existing zero-touch configuration in the Google zero-touch enrollment portal for reference.
4. In Sophos Mobile as a Service, click **Setup > Android setup > Zero-touch**.
5. Revoke the zero-touch configuration.
6. In the Google zero-touch enrollment portal, delete the configuration for Sophos Mobile as a Service.
7. Reset your existing zero-touch devices to their factory settings.

When the devices are turned on again, they enroll with Sophos Mobile in Sophos Central.

Related information

Sophos Mobile administrator help - Zero-touch enrollment

10.6 Configure Samsung Knox Mobile Enrollment

The MDM profile for Sophos Mobile you’ve created in the Samsung Knox Mobile Enrollment console contains a link to the Sophos Mobile as a Service server. To enroll Knox Mobile Enrollment enabled devices (“KME devices”) with your Sophos Mobile account in Sophos Central, you must create a new MDM profile.

Prerequisites:

- You’ve created users and user groups in Sophos Central.
- You’ve imported your data to Sophos Central.

To reconfigure Samsung Knox Mobile Enrollment:

1. In Sophos Central Admin, go to **Mobile**.
2. Click **Setup > Android setup > Samsung KME**.
3. Set up Knox Mobile Enrollment the same way you did in Sophos Mobile as a Service.

   Use your settings in Sophos Mobile as a Service and your existing MDM profile in the Samsung Knox Mobile Enrollment console for reference.
4. In Sophos Mobile as a Service, click **Setup > Android setup > Samsung KME**
5. Revoke the KME configuration.
6. In the Samsung Knox Mobile Enrollment console, delete the MDM profile for Sophos Mobile as a Service.
7. Reset your existing KME devices to their factory settings.

When the devices are turned on again, they enroll with Sophos Mobile in Sophos Central.

Related information

Sophos Mobile administrator help - Knox Mobile Enrollment

10.7 Configure third-party EMM integration

The app configuration for Sophos Mobile Security you’ve created in your third-party EMM software contains a link to the Sophos Mobile as a Service server. To connect the Sophos Mobile Security app with your Sophos Mobile account in Sophos Central, you must update the app configuration in your third-party EMM software.

Prerequisites:

- You’ve created users and user groups in Sophos Central.
- You’ve imported your data to Sophos Central.

To reconfigure integration with a third-party EMM software:

1. In Sophos Central Admin, go to **Mobile**.
2. Click **Setup > Android setup > Third-party EMM**.
3. Set up the third-party EMM integration the same way you did in Sophos Mobile as a Service.

   Use your settings in Sophos Mobile as a Service for reference.
4. In your third-party EMM software, update the custom app configuration for Sophos Mobile Security.

   You only have to update the `smcData` parameter with the value displayed in Sophos Central.
5. In Sophos Mobile as a Service, click **Setup > Android setup > Third-party EMM**.
6. Revoke the connection code.
7. Delete the Sophos Mobile Security app on your devices and then re-install it through the third-party EMM software.

On the first start after installation, the Sophos Mobile Security app enrolls with Sophos Mobile in Sophos Central.

Related information

Sophos Mobile administrator help - Third-party EMM integration

10.8 Configure Microsoft Intune app protection

The Sophos Mobile application you’ve set up in the Microsoft Azure portal contains a link to the Sophos Mobile as a Service server. You must replace that link by a link to Sophos Central.

Prerequisites:

- You’ve created users and user groups in Sophos Central.
- You’ve imported your data to Sophos Central.

To update the server information in your Azure enterprise application:

1. In Sophos Central Admin, go to **Mobile**.
2. Click **Setup > Microsoft setup > Microsoft Azure**.
3. Copy the value displayed in **Sign-on URL**.
4. Open the Microsoft Azure portal in a web browser and go to the **App registrations** blade.
5. Open your application for Sophos Mobile.
6. Under **Settings > Properties**, paste the URL you’ve copied from Sophos Central Admin into the **Home page URL** field.
7. Under **Settings > Reply URLs**, make the following changes:

   a) Add the URL of the Sophos Central Admin server, that is, the value you’ve entered in **Home page URL**.

   b) Delete the URL of the Sophos Mobile as a Service server, that is, the previous value of the **Home page URL** field.

You can now manage your Intune app protection policies in Sophos Central.

Related information

Microsoft Azure portal - App registrations (external link)

11 Migrate the standalone EAS proxy

When you move from Sophos Mobile as a Service to Sophos Central, you can continue to use your standalone EAS proxy. You only have to adjust the Sophos Mobile server URL in the proxy server configuration and upload the proxy certificate to Sophos Central.

> **Important**
> After you've performed this procedure, the standalone EAS proxy will reject any devices still managed by your Sophos Mobile as a Service account.

1. In Sophos Central Admin, go to **Mobile**.
2. Click **Setup > Sophos setup > EAS proxy**.

   Keep this page open. You need to interact with it in the next steps.
3. On the computer on which you've installed the standalone EAS proxy, select **Sophos Mobile EAS Proxy > EAS Proxy Configuration Wizard** from the Windows Start menu to start the configuration wizard.
4. On the **Sophos Mobile server configuration** wizard page, enter the server URL displayed on the Sophos Central Admin page under **External**.
5. On the **EAS Proxy instance setup** wizard page, click the **Export config and upload to Sophos Mobile server** link.

   This opens the folder that contains the proxy certificate.
6. Upload the certificate to Sophos Central:

   On the Sophos Central Admin page, click **Upload a file**, then navigate to the certificate file and click **Open**.
7. If you've configured more than one EAS proxy instance, repeat the previous steps to upload the certificates of the remaining instances.
8. In Windows, open the **Services** dialog and restart the **EASProxy** service.

12 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 knowledge base 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.

13 Legal notices