SOPHOS

Cybersecurity made simple.

Sophos Mobile

migration guide

product version: 9.6

Contents

Preface 1
Migration checklist 2
Migration overview 3
- Device migration 3
- User migration 4

Preparation 5
- Prepare for migration 5
- Prepare EAS proxy for migration 7

Migration 10
- Get your migration code 10
- Run the migration assistant 10
- Transfer app package files 13
- Transfer documents 14
- Cancel migration 15

Post-migration tasks 16
- Additional migration tasks 16
- Migrate Microsoft Intune app protection 17
- Migrate Android Enterprise QR code enrollment 17
- Migrate Android zero-touch enrollment 17
- Migrate Knox Mobile Enrollment 18
- Migrate Sophos Chrome Security auto-enrollment 18
- Migrate third-party EMM integration 19
- Migrate iOS auto-enrollment 19
- Migrate the EAS proxy 19
- Migrate Sophos Mobile Self Service Portal access 22

Migration issues 23
Support 27
Legal notices 28

1 Preface

This document explains how to migrate from an on-premise Sophos Mobile server or from Sophos Mobile as a Service to the Sophos Mobile product in Sophos Central.

We call this “Migration from Sophos Mobile to Sophos Central.”

We strongly recommend that you do as follows:

- Contact our Professional Services team to see how they can help you migrate successfully.
- Follow the steps in this migration guide.
- Resolve any issues found by the migration assistant.

You can’t undo migration after you’ve started, so it’s important to plan properly.

Before you begin

Before you start migration, you need to know the following restrictions:

- Your Sophos Mobile license in Sophos Central must match the license of the account that you want to migrate. For example, you can’t migrate from a Mobile Advanced license to a Mobile Standard license.
- You can’t migrate to a trial account.
- You can’t migrate if you already added devices to Sophos Mobile in Sophos Central.
- You can’t select the items to migrate. If you want to exclude some devices or policies, delete them before starting the migration.
- You can’t undo migration.
- You can’t resume migration after you canceled it.
- You can’t repeat migration. After you started migration, you can’t migrate the same account again or migrate another account to the same Sophos Central account.

Related information

Sophos Professional Services

2 Migration checklist

This checklist is a condensed version of the Prepare for migration, Migration, and Post-migration tasks sections. Use it to track your migration status.

1. Check that you're not using a feature that blocks migration:
   - Windows Mobile or Windows Phone devices
   - iPhones or iPads with iOS 9.2.1 or earlier
   - Corporate keyring synchronization with SafeGuard Enterprise
   - Sophos UTM integration
   - Integration with third-party Network Access Control (NAC) software
   - Duo Security integration for Android devices
   - LDAP user management, except for Active Directory
   - App Groups API integration with a third-party app reputation vendor
   - Other Sophos Mobile REST APIs
2. Set up your Sophos Central account.
3. Download a migration token from Sophos Central.
4. If applicable, turn off Sophos Mobile auto-enrollment:
   - Revoke the Android Enterprise QR code.
   - Revoke the Android zero-touch configuration.
   - Revoke the Samsung Knox Mobile Enrollment (KME) configuration.
   - Revoke the Google Workspace connection code for Sophos Chrome Security.
   - Revoke the third-party connection code for Sophos Intercept X for Mobile.
   - Turn off iOS auto-enrollment with Apple Configurator in the device group settings.
5. If applicable, turn off TeamViewer integration.
6. Update the Sophos Mobile apps.
7. If applicable, turn off mail filtering with the Sophos Mobile EAS proxy.
8. Request your migration code from `mobilemigration@sophos.com`.
9. Start the migration assistant.
10. Correct issues that the migration assistant reports.
11. Start migration from the final page of the migration assistant.

Wait until the migration assistant starts to migrate devices. Then continue as follows:

12. Check your migrated data in Sophos Central.
13. Set up user management in Sophos Central and invite users to the Sophos Mobile Self Service Portal.
14. Do the following if applicable:
    a) Configure Intune app protection in Sophos Central.
    b) Configure Sophos Mobile auto-enrollment in Sophos Central.
    c) Turn on mail filtering with the Sophos Mobile EAS proxy.

3 Migration overview

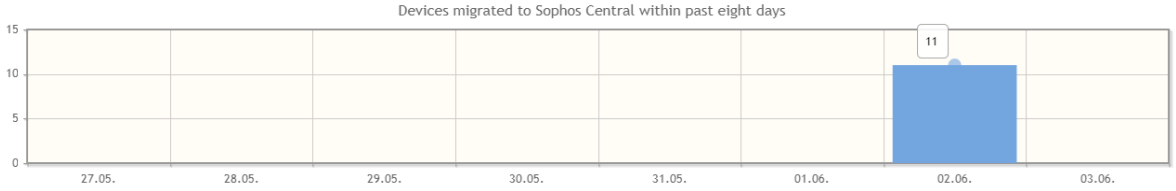
3.1 Device migration

The migration assistant moves your devices to Sophos Central.

Each device is migrated individually the next time it connects to the Sophos Mobile server. Because the default sync interval is 24 hours, you can expect most devices to be migrated after one day.

When a device is migrated, it's removed from the **Devices** page in Sophos Mobile and added to the corresponding page in Sophos Central. There's a short period of time where a device appears in both Sophos Mobile and Sophos Central.

To track the migration progress, the **Devices** page in Sophos Mobile displays the number of migrated devices per day (see below). There's also a **Sophos Central device migration** report.



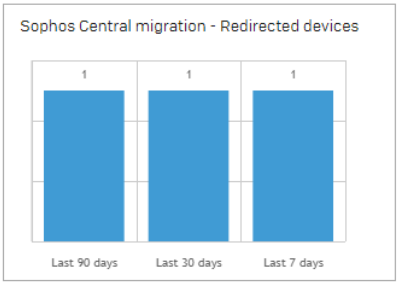
Android and Chrome devices

For Android and Chrome devices, the migration assistant registers the URL of the Sophos Central server in the Sophos Mobile client on the device. After migration, these devices are connected to your Sophos Central account as if they had been enrolled with it in the first place.

iPhones, iPads, Macs, and Windows computers

iPhones, iPads, Macs, and Windows computers remain connected to your old Sophos Mobile server. The Sophos Mobile server redirects them to Sophos Central every time they connect. Apart from the redirection, you manage these devices in Sophos Central the same way as other devices.

You can track the number of redirected devices in Sophos Mobile with the **Sophos Central migration - Redirected devices** dashboard widget (see below). The latest redirection date for each device is available in the **Sophos Central device migration** report.



Note
You must keep the Sophos Mobile server running as long as redirected devices remain enrolled with it. You're not required to update licenses or the Sophos Mobile software on that server. Because the server load is reduced when there are only redirected devices, you may consider scaling down server hardware.

3.2 User migration

The migration assistant copies your user accounts to Sophos Central.

If you're using internal user management, the migration assistant copies user groups as well.

If you're using external user management with Active Directory (AD), the migration assistant doesn't copy user groups. Nevertheless, it copies your Sophos Mobile Self Service Portal configurations, which contain user group information. Before starting migration, check that the user groups you use in your Sophos Mobile Self Service Portal configuration are available in Sophos Central. We recommend that you set up synchronization with your Active Directory server in Sophos Central before starting migration.

After migration, you must invite users to the Sophos Central Sophos Mobile Self Service Portal. See Migrate Sophos Mobile Self Service Portal access.

Also note the following:

- Administrators aren't copied. If required, create them in Sophos Central.
- A user isn't copied if there's already a user with the same email address in Sophos Central.
- For AD user management, you may import users to Sophos Central and invite them to the Sophos Mobile Self Service Portal before starting migration.

4 Preparation

4.1 Prepare for migration

You must complete a few tasks before you can start migration.

Note
You can't migrate several customer accounts to the same Sophos Central account.

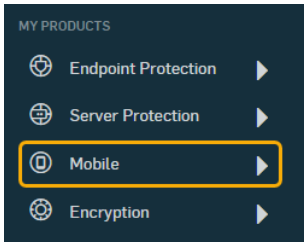
Do as follows:

1. Check that you're not using a feature that blocks migration:
   - Windows Mobile or Windows Phone devices
   - iPhones or iPads with iOS 9.2.1 or earlier
   - Corporate keyring synchronization with SafeGuard Enterprise
   - Sophos UTM integration
   - Integration with third-party Network Access Control (NAC) software
   - Duo Security integration for Android devices
   - LDAP user management, except for Active Directory
   - App Groups API integration with a third-party app reputation vendor
   - Other Sophos Mobile REST APIs
2. Set up your Sophos Central account.
   a) Create an administrator account that has the **Super admin** role.
   b) Activate your Sophos Mobile license.
   c) Configure global settings as required.

   For details on these and the following tasks, see the Sophos Central Admin help.
3. Optional: In Sophos Central, set up synchronization with your Active Directory server.

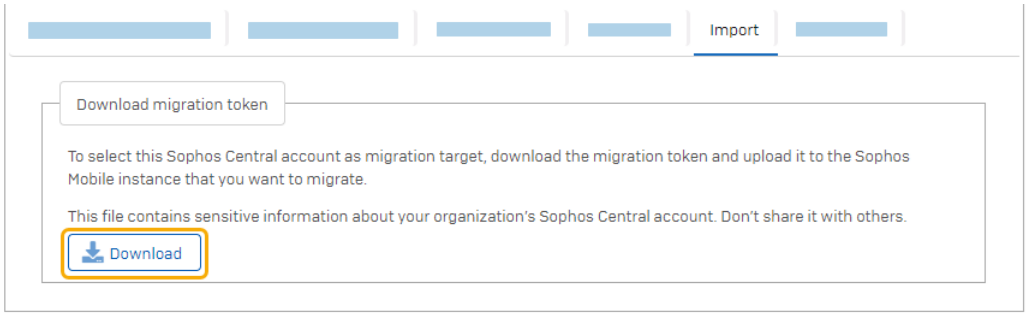
   Check that the user groups you use in your Sophos Mobile Self Service Portal configuration are available in Sophos Central.
4. Optional: If you've already added users to Sophos Central, invite them to the Sophos Mobile Self Service Portal.

   See Migrate Sophos Mobile Self Service Portal access.
5. If you're using federated authentication with Azure Active Directory, do as follows:
   a) In Sophos Mobile, turn off federated authentication and turn on a different user management mode, for example internal user management.
   b) In Sophos Central, configure federated authentication.
6. Download a migration token from Sophos Central.
   a) Sign in to Sophos Central Admin and go to **Mobile**.



b) On the menu sidebar, under **SETTINGS**, select **Setup > Sophos setup**, and then select the **Import** tab.

c) Click **Download**.



A `sophosmobile_migration.target` file containing the migration token is downloaded to your computer.

7. If applicable, turn off Sophos Mobile auto-enrollment:
   - Revoke the Android Enterprise QR code.
   - Revoke the Android zero-touch configuration.
   - Revoke the Samsung Knox Mobile Enrollment (KME) configuration.
   - Revoke the Google Workspace connection code for Sophos Chrome Security.
   - Revoke the third-party connection code for Sophos Intercept X for Mobile.
   - Turn off iOS auto-enrollment with Apple Configurator in the device group settings.

   Note
   We recommend that you record your settings before you turn off a configuration. This helps you to reproduce the settings in Sophos Central after migration.

8. If applicable, turn off TeamViewer integration.
9. In Sophos Mobile, unenroll and delete any Windows Phone and Windows Mobile devices.
10. Update the Sophos Mobile apps.

    On Android devices, iPhones, and iPads:
    - Sophos Mobile Control
    - Sophos Intercept X for Mobile
    - Sophos Secure Workspace
    - Sophos Secure Email

    On Chrome devices:
    - Sophos Chrome Security

If you're using the Sophos Mobile EAS proxy, you must prepare it before starting the migration.

If you're not using the Sophos Mobile EAS proxy, skip to section Migration.

Related information

Sophos Central Admin help

4.2 Prepare EAS proxy for migration

If you're using the Sophos Mobile EAS proxy, we recommend that you temporarily turn off mail filtering until you've configured the standalone EAS proxy for Sophos Central. Otherwise, devices that are already migrated would be blocked.

CAUTION
For an on-premise Sophos Mobile server, turning off mail filtering affects all customers, not only the customer that you migrate to Sophos Central.

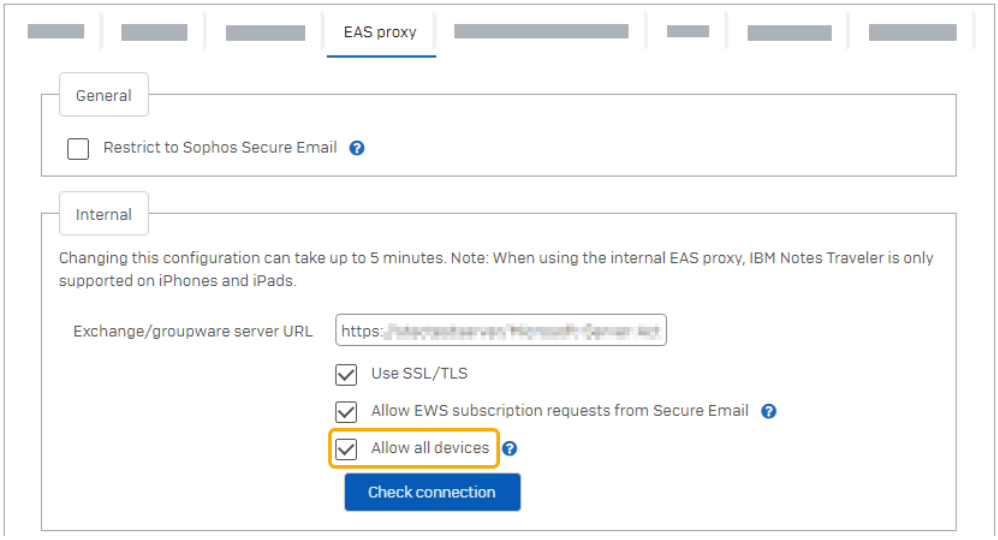
To turn off mail filtering, follow the steps for your EAS proxy type (internal, standalone, or standalone in PowerShell mode).

Turn off mail filtering for the internal EAS proxy

You must start the migration assistant described in Run the migration assistant before you can perform the following steps. The **Allow all devices** setting is only then available.

Do as follows:

1. Sign in to Sophos Mobile Admin as a super administrator.
2. On the menu sidebar, under **SETTINGS**, click **Setup > Sophos setup**, and then click the **EAS proxy** tab.
3. Under **Internal**, select **Allow all devices**.
4. Click **Save**.



Turn off mail filtering for the standalone EAS proxy in proxy mode

Do as follows:

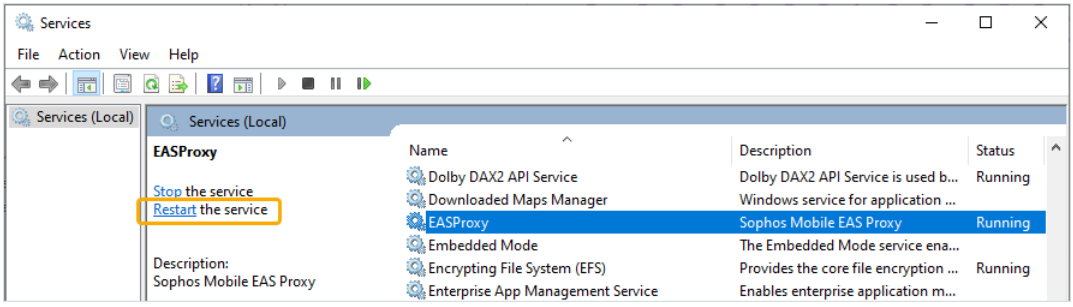
1. Open the EAS proxy's configuration file, `easproxy.conf.xml`, in a text editor.

   The file is located in the installation folder. By default, this is `C:\Program Files (x86)\Sophos\Sophos Mobile EAS Proxy\`.
2. Change all occurrences of the text `verificationEnabled="true"` to `verificationEnabled="false"`.

   There's one occurrence for each EAS proxy instance that you've set up.

```
    <instanceList>
        <instance id="1" name="test" bindPort="9999" destinationHost="example.com" destinationPort="80"
destinationSSLEnabled="0" travelerSupportEnabled="0" ewsEnabled="false" creationTimestamp="20200602161221"
remoteEasServletUrl="https://                                                                          "
remoteEasServletCertPath="C:\Program Files (x86)\Sophos\Sophos Mobile EAS Proxy\config\1\easproxy_cert.p12"
verificationEnabled="false" responseCodeInternalError="501" responseCodeAccessDenied="403" bindHost="0.0.0.0"
accessLogCommitInterval="10" accessLogFile="C:\Program Files (x86)\Sophos\Sophos Mobile EAS Proxy\logs
\accessLog_test.json" inboundAuthRequired="0" />
        <instance id="2" name="test1" bindPort="9998" destinationHost="example.com" destinationPort="80"
destinationSSLEnabled="0" travelerSupportEnabled="0" ewsEnabled="false" creationTimestamp="20200602161529"
remoteEasServletUrl="https://                                                                          "
remoteEasServletCertPath="C:\Program Files (x86)\Sophos\Sophos Mobile EAS Proxy\config\2\easproxy_cert.p12"
verificationEnabled="false" responseCodeInternalError="501" responseCodeAccessDenied="403" bindHost="0.0.0.0"
accessLogCommitInterval="10" accessLogFile="C:\Program Files (x86)\Sophos\Sophos Mobile EAS Proxy\logs
\accessLog_test1.json" inboundAuthRequired="0" />
    </instanceList>
```

3. Save the file.
4. In Windows, open **Services** and restart the **EASProxy** service.



Turn off mail filtering for the standalone EAS proxy in PowerShell mode

Do as follows:

1. Connect to Exchange Online PowerShell or, if you have an Exchange server, open the Exchange Management Shell.
2. Run the following command:

   ```
   Get-ActiveSyncOrganizationSettings
   ```

   Record the `DefaultAccessLevel` value. You need this value when you turn on mail filtering again.
3. Run the following command:

   ```
   Set-ActiveSyncOrganizationSettings -DefaultAccessLevel allow
   ```

Related information

Connect to Exchange Online PowerShell (Microsoft documentation)
Open the Exchange Management Shell (Microsoft documentation)

5 Migration

5.1 Get your migration code

You need a migration code from Sophos to start migration.

Contact us via `mobilemigration@sophos.com`. We'll check your data to ensure a smooth and successful migration process. When everything's ready, we'll send you your migration code.

5.2 Run the migration assistant

The migration assistant moves your data from Sophos Mobile to Sophos Central.

CAUTION
Ensure that no other administrator is signed in to the account that you want to migrate. For an on-premise Sophos Mobile server, this also applies to the super administrator account.

If data is changed after you start the migration assistant, migrated data might be inconsistent and, in the worst case, you must re-enroll all devices.

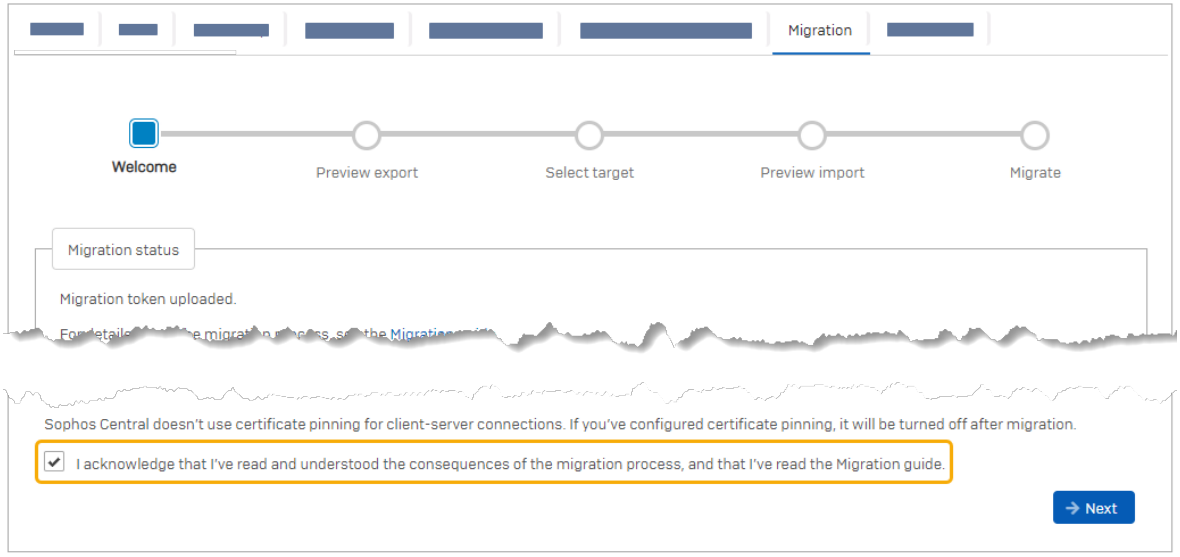
This restriction applies from the time you click **Next** on the **Preview export** page until the first device is migrated.

CAUTION
You can't undo migration after you click **Start migration** in the migration assistant.

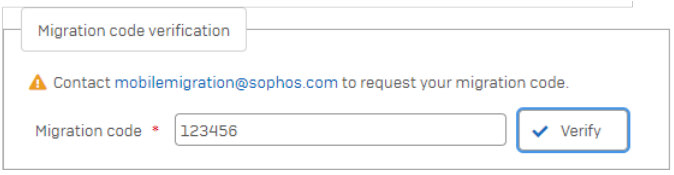
Do as follows:

1. Sign in to Sophos Mobile Admin.

   For an on-premise Sophos Mobile server, sign in as an administrator of the customer that you want to migrate.
2. On the menu sidebar, under **SETTINGS**, select **Setup > Sophos setup**, and then select the **Migration** tab.
3. Read and acknowledge the information that is displayed on the **Welcome** page.



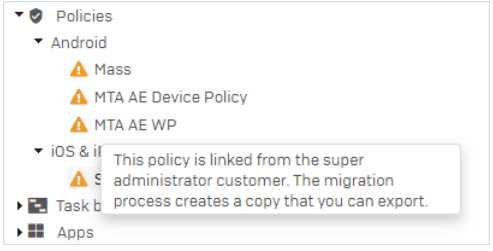
4. On the **Preview export** page, enter the migration code that you received from Sophos and click **Verify**.



5. Also on the **Preview export** page, check if there are any issues:

   - : A condition that blocks migration. You must resolve the issue before you can start migration.
   - : A condition where the migration assistant will modify your data. If you agree to the change, no action is required.

   Hover over an item to display details about the issue.



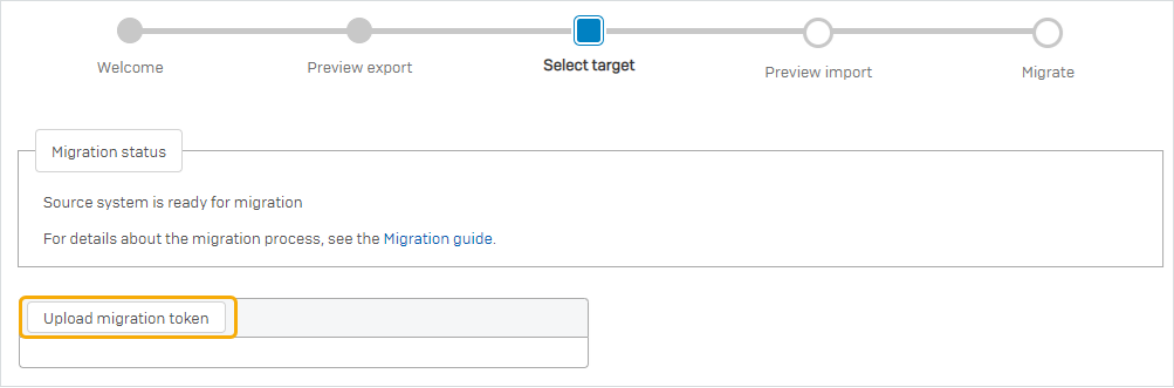
   For information on how to resolve issues, see Migration issues.

6. Click **Next**.

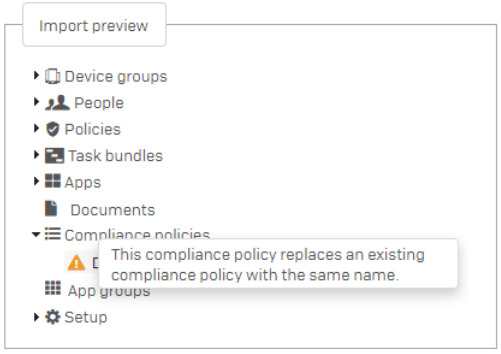
   If the migration assistant has to modify your data, this starts now and might take a few minutes.

   Review the changes on the **Preview export** page and click **Next** again.

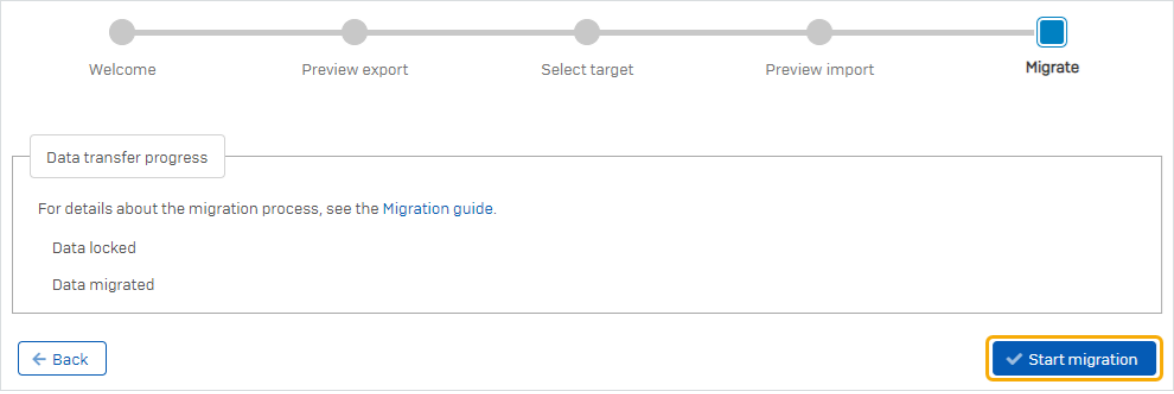
7. On the **Select target** page, upload the `sophosmobile_migration.target` file with the migration token that you downloaded from your Sophos Central account.



8. On the **Preview import** page, check if there are any issues.



9. On the **Migrate** page, click **Start migration**.

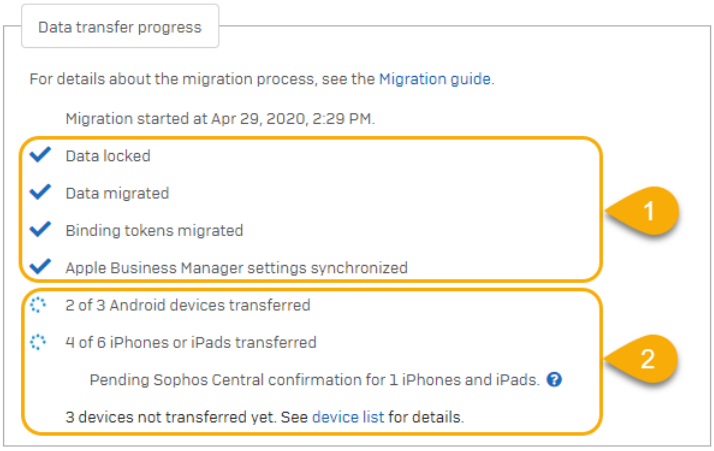


Migration runs in two phases:

1. In the data migration phase (labeled 1 in the subsequent image), the migration assistant copies your user accounts, policies, app packages, documents, and other settings. The history of tasks, alerts, and privacy-related events isn't migrated.

   With the exception of changes the migration assistant performs to make your data migratable, no data is changed in Sophos Mobile.

2. In the device migration phase (labeled 2 in the subsequent image), the migration assistant transfers your devices. For details, see Device migration.



During migration, you can't edit any data in Sophos Mobile. Only device actions **Lock**, **Unenroll**, **Wipe**, and **Delete** are available.

Depending on your configuration, you must perform a few manual tasks in Sophos Central to complete migration.

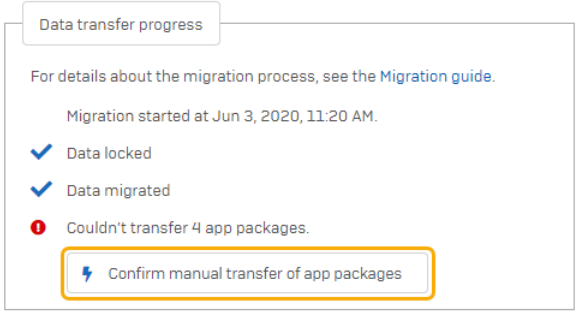
See Additional migration tasks.

5.3 Transfer app package files

The migration assistant might fail to migrate apps that have a very large package file. In this case, upload the package file manually to Sophos Central.

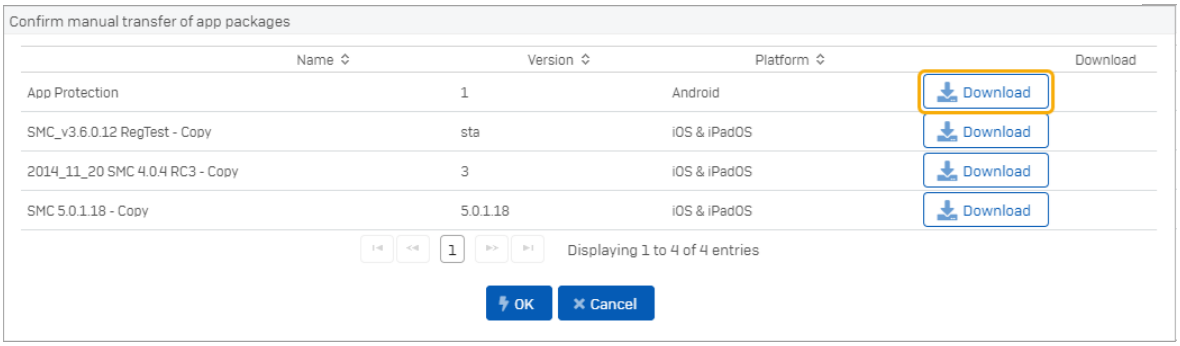
Do as follows:

1. On the **Migrate** page of the migration assistant, click **Confirm manual transfer of app packages**.



   A dialog is displayed with a list of affected app packages.

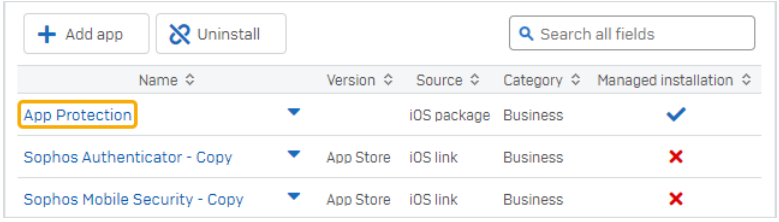
2. Click **Download** next to an app package.



   The file is downloaded to your computer.

3. Sign in to Sophos Central Admin and go to **Mobile**.
4. Click **Apps**, and then click the affected platform.

   The migration assistant has already added and configured an entry for the app. Only the app package file is missing.
5. Click on the app.



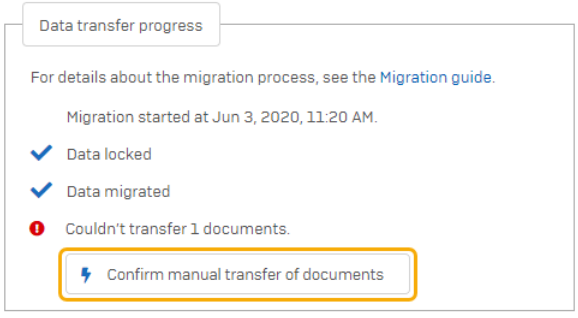
6. Click **Upload a file** and select the app package file.
7. Click **Save**.
8. Repeat the previous steps for the remaining apps.

5.4 Transfer documents

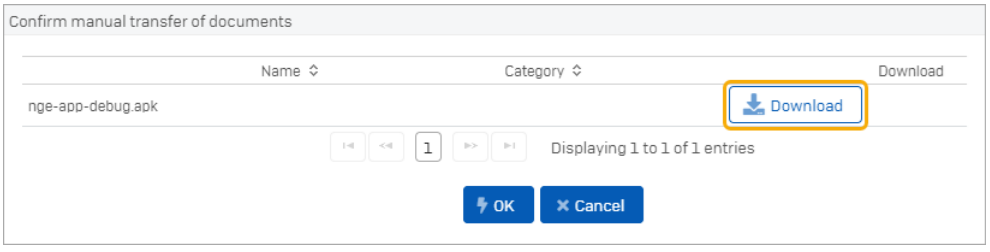
The migration assistant might fail to migrate very large documents. In this case, upload the document file manually to Sophos Central.

Do as follows:

1. On the **Migrate** page of the migration assistant, click **Confirm manual transfer of documents**.

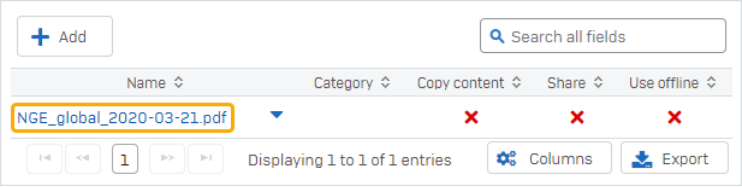


   A dialog is displayed with a list of affected documents.
2. Click **Download** next to a document.



   The file is downloaded to your computer.
3. Sign in to Sophos Central Admin and go to **Mobile**.
4. Click **Documents**.

   The migration assistant has already added and configured an entry for the document. Only the document file is missing.
5. Click on the document.



6. Click **Upload a file** and select the document file.
7. Click **Save**.
8. Repeat the previous steps for the remaining documents.

5.5 Cancel migration

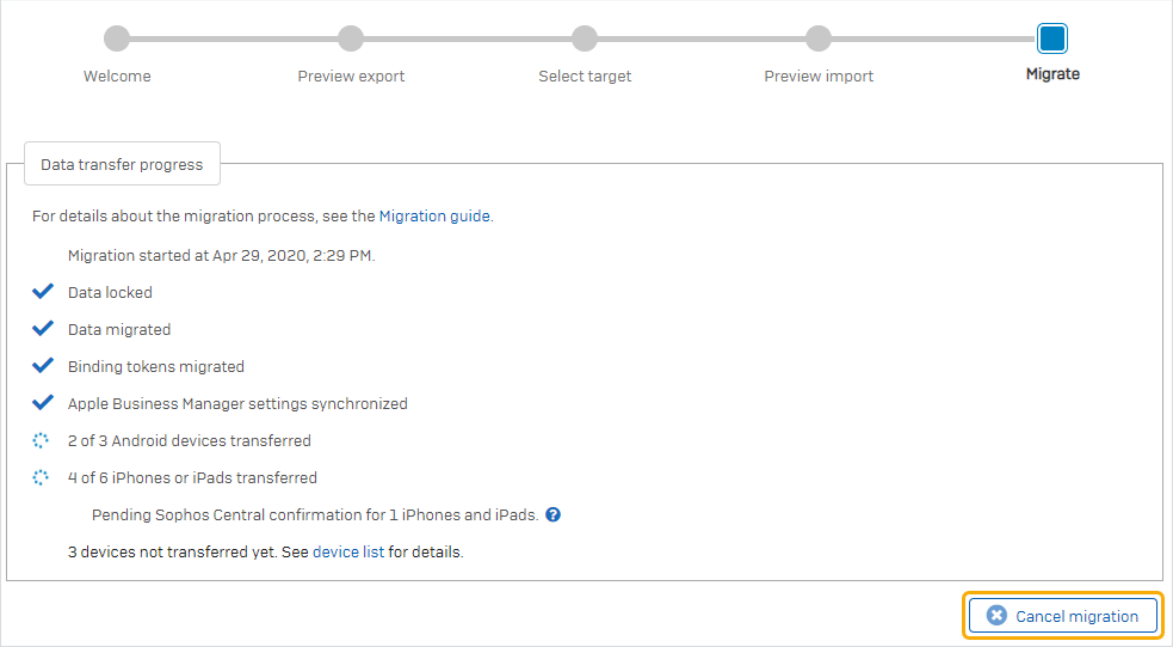
You can cancel migration before all devices have been transferred, for example if the remaining devices have been lost or can't synchronize with the Sophos Mobile server for other reasons.

CAUTION
When you cancel migration, you can't resume it later. To migrate remaining devices, you must enroll them individually with Sophos Central.

Instead of canceling migration, consider deleting the remaining devices.

To cancel migration, do as follows:

1. On the menu sidebar, under **SETTINGS**, select **Setup > Sophos setup**, and then select the **Migration** tab.
2. On the **Migrate** page of the migration assistant, click **Cancel migration**.



6 Post-migration tasks

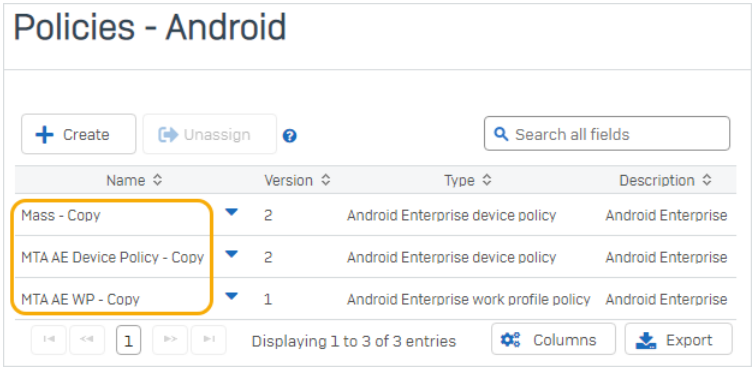
6.1 Additional migration tasks

Depending on your configuration, you must perform a few manual tasks in Sophos Central to complete migration.

You can carry out these steps as soon as device migration has started, that is, when there's an entry **<X> of <Y> Android devices transferred** (or equivalent for other platforms) under **Data transfer progress** in the migration assistant.

In Sophos Central Admin, do as follows:

1. Configure access to the Sophos Central Sophos Mobile Self Service Portal. See Migrate Sophos Mobile Self Service Portal access.
2. Remove the text "Copy" that the migration assistant might have added to the names of the following items:
   - Apps
   - App groups
   - Policies
   - Task bundles



3. If required, set up the following features:
   - Intune app protection
   - Android Enterprise QR code enrollment
   - Android zero-touch enrollment
   - Samsung Knox Mobile Enrollment
   - Sophos Chrome Security auto-enrollment
   - Third-party Enterprise Mobile Management (EMM) integration for Sophos Intercept X for Mobile
   - iOS auto-enrollment with Apple Configurator
   - TeamViewer integration
4. If you're using the EAS proxy, configure it for Sophos Central. See Migrate the EAS proxy
5. If your Sophos Central user accounts are coming from Active Directory (AD), configure an LDAP connection between Sophos Mobile and AD.

This allows users to use their AD credentials for Apple Business Manager, Google zero-touch enrollment, and Samsung Knox Mobile Enrollment.

See Configure LDAP connection in the Sophos Mobile administrator help.

Related information

Configure LDAP connection (Sophos Mobile administrator help)

6.2 Migrate Microsoft Intune app protection

If you're using Microsoft Intune app protection, you must set it up after migration.

The Sophos Mobile application that you created in the Microsoft Azure portal is associated with Sophos Mobile. After migration, delete this application and create a new one for Sophos Central.

Do as follows:

1. Set up Microsoft Intune integration.
2. Create an Intune app protection policy.
3. Assign apps and users to that policy.

Related information

Set up Microsoft Intune integration (Sophos Mobile administrator help)
Create Intune app protection policy (Sophos Mobile administrator help)
Assign apps to an Intune app protection policy (Sophos Mobile administrator help)
Assign users to an Intune app protection policy (Sophos Mobile administrator help)

6.3 Migrate Android Enterprise QR code enrollment

If you're using Android Enterprise QR code enrollment, you must create a new QR code for Sophos Central.

Related information

Set up QR code enrollment (Sophos Mobile administrator help)

6.4 Migrate Android zero-touch enrollment

If you're using Android zero-touch enrollment, you must set it up after migration.

The zero-touch configuration that you created in the Google zero-touch enrollment portal is associated with Sophos Mobile. To enroll zero-touch enabled Android devices (zero-touch devices) with Sophos Central, you must create a new configuration.

Do as follows:

1. In Sophos Central Admin, set up zero-touch enrollment.
2. In the Google zero-touch enrollment portal, update your configuration for Sophos Mobile with the new configuration code.
3. Reset your zero-touch devices to their factory settings.

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

Related information

Set up zero-touch enrollment (Sophos Mobile administrator help)

6.5 Migrate Knox Mobile Enrollment

If you're using Samsung Knox Mobile Enrollment (KME), you must set it up after the migration.

The Mobile Device Management (MDM) profile that you created in the Samsung Knox Mobile Enrollment console is associated with Sophos Mobile. To enroll Knox Mobile Enrollment enabled devices (KME devices) with Sophos Central, you must create a new MDM profile.

Do as follows:

1. In Sophos Central Admin, set up Knox Mobile Enrollment.
2. In the Samsung Knox Mobile Enrollment console, delete the MDM profile for Sophos Mobile and create a new profile for Sophos Central.
3. Reset your KME devices to their factory settings.

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

Related information

Set up Knox Mobile Enrollment (Sophos Mobile administrator help)

Create KME profile (Sophos Mobile administrator help)

6.6 Migrate Sophos Chrome Security auto-enrollment

If you're using Sophos Chrome Security auto-enrollment, you must set it up after migration.

The Sophos Chrome Security configuration in your Google Workspace (formerly G Suite) account is associated with Sophos Mobile. To use Sophos Chrome Security auto-enrollment with Sophos Central, you must update the configuration.

Do as follows:

1. In Sophos Central Admin, create a connection code for Sophos Chrome Security auto-enrollment.
2. In the Google Admin console, go to **Device Management > Chrome Management > App Management > Sophos Chrome Security** and upload the new connection code.
3. Unenroll Sophos Chrome Security on all managed Chrome devices.

The next time a Google Workspace user signs in to the Chrome device, Sophos Chrome Security automatically enrolls with Sophos Central.

Related information

Configure Sophos Chrome Security auto-enrollment (Sophos Mobile administrator help)

6.7 Migrate third-party EMM integration

If you're using third-party Enterprise Mobile Management (EMM) integration for Sophos Intercept X for Mobile, you must adjust your configuration after migration.

The configuration for Sophos Intercept X for Mobile that you created in your third-party EMM software is associated with Sophos Mobile. To connect the app with Sophos Central, you must update the configuration.

Do as follows:

1. In Sophos Central Admin, create a connection code for third-party EMM integration.
2. In your third-party EMM software, update the configuration for Sophos Intercept X for Mobile.
   You only have to update the `smcData` parameter with the value displayed in Sophos Central.
3. Uninstall Sophos Intercept X for Mobile on your devices and re-install it through the third-party EMM software.

The first time a device starts after installation, Sophos Intercept X for Mobile enrolls with Sophos Central.

Related information

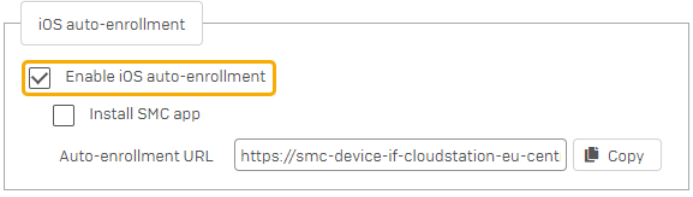
Use Sophos Intercept X for Mobile with third-party EMM software (Sophos Mobile administrator help)

6.8 Migrate iOS auto-enrollment

If you're using iOS auto-enrollment with Apple Configurator, you must turn it on after migration.

Do as follows:

1. In Sophos Central Admin, go to the device group that you want to use for iOS auto-enrollment.
2. Turn on **Enable iOS auto-enrollment**.



When configuring devices in Apple Configurator, use the value that is displayed for **Auto-enrollment URL**.

Related information

Auto-enroll iPhones and iPads (Sophos Mobile administrator help)

6.9 Migrate the EAS proxy

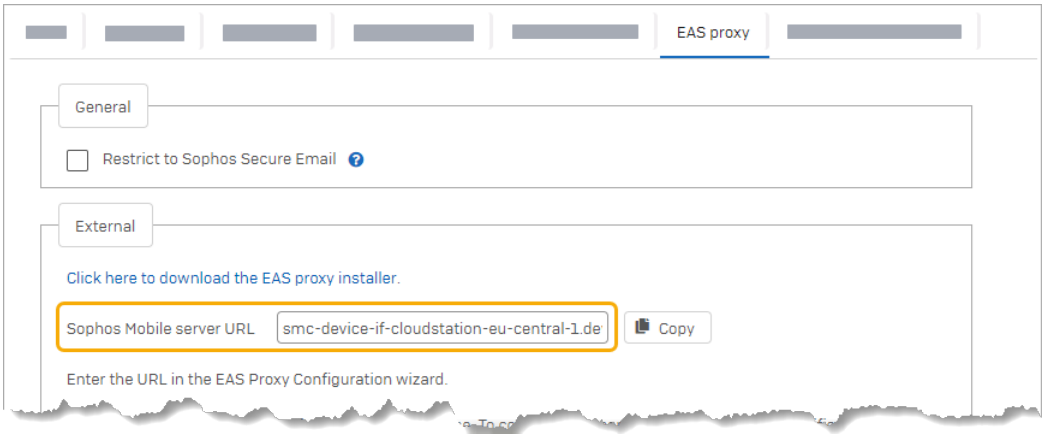
If you're using the EAS proxy for Sophos Mobile, you must configure it for Sophos Central.

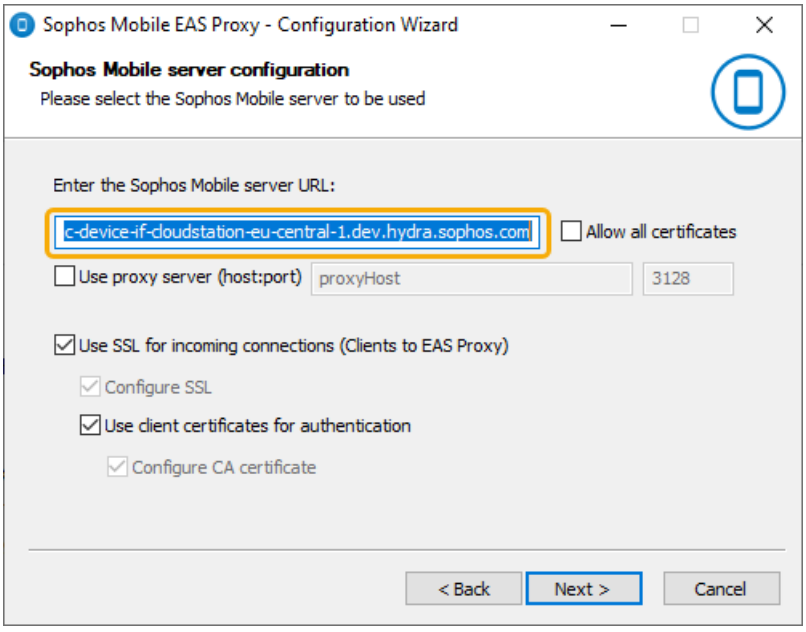
If you're using the internal EAS proxy for Sophos Mobile, you must set up the standalone EAS proxy instead. The internal EAS proxy isn't available for Sophos Central. See Standalone EAS proxy in the Sophos Mobile administrator help.

If you're already using the standalone EAS proxy, you must update its configuration. Do as follows:

1. Sign in to Sophos Central Admin and 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 assistant.
4. On the **Sophos Mobile server configuration** page, enter the server URL that is displayed on the Sophos Central Admin page under **External**.

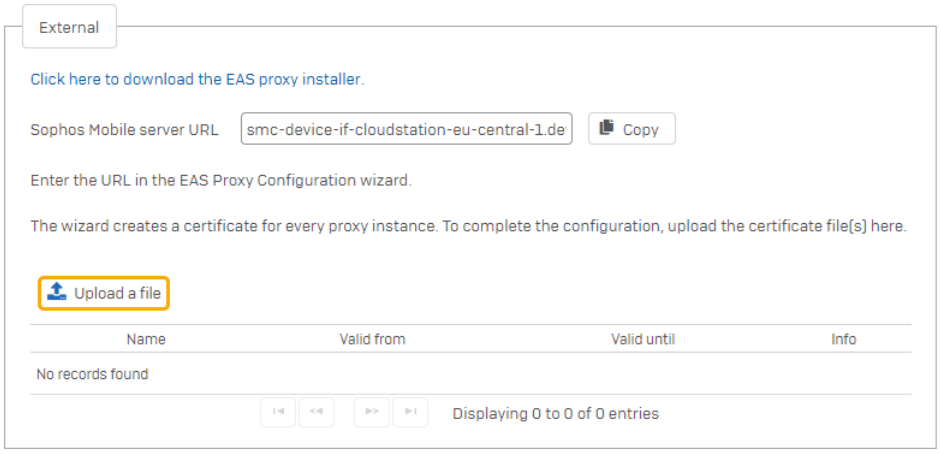




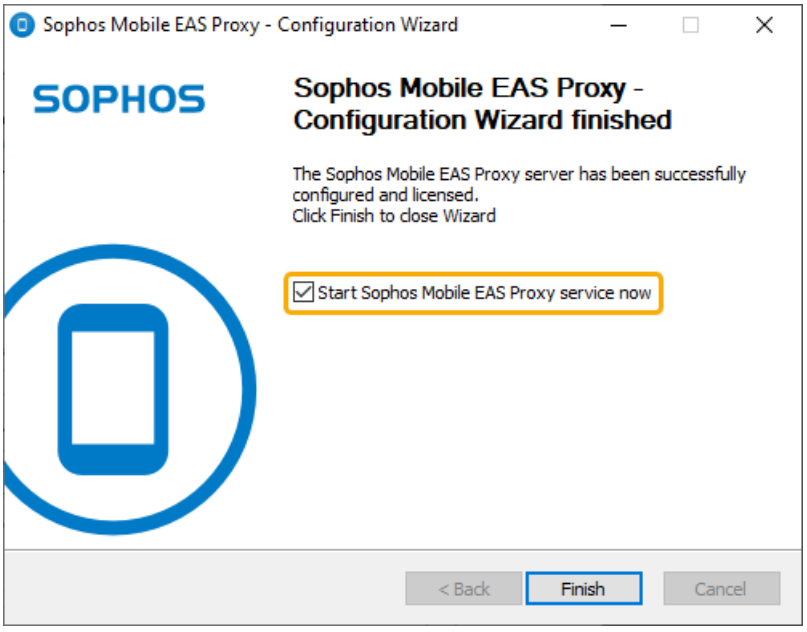
5. On the **EAS Proxy instance setup** page, click **Export config and upload to Sophos Mobile server**.

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

   On the Sophos Central Admin page, click **Upload a file**, go 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. On the last page of the configuration assistant, ensure that the option to start the EAS proxy service is selected.



9. If you turned off mail filtering before starting migration, turn it on again:
   - For the standalone EAS proxy in proxy mode:

     Open the EAS proxy's configuration file, `easproxy.conf.xml`, and change all occurrences of the text `verificationEnabled="false"` to `verificationEnabled="true"`.
   - For the standalone EAS proxy in PowerShell mode:

     Run the `Set-ActiveSyncOrganizationSettings` PowerShell command to set the `DefaultAccessLevel` parameter to the value you used before starting migration.

Related information

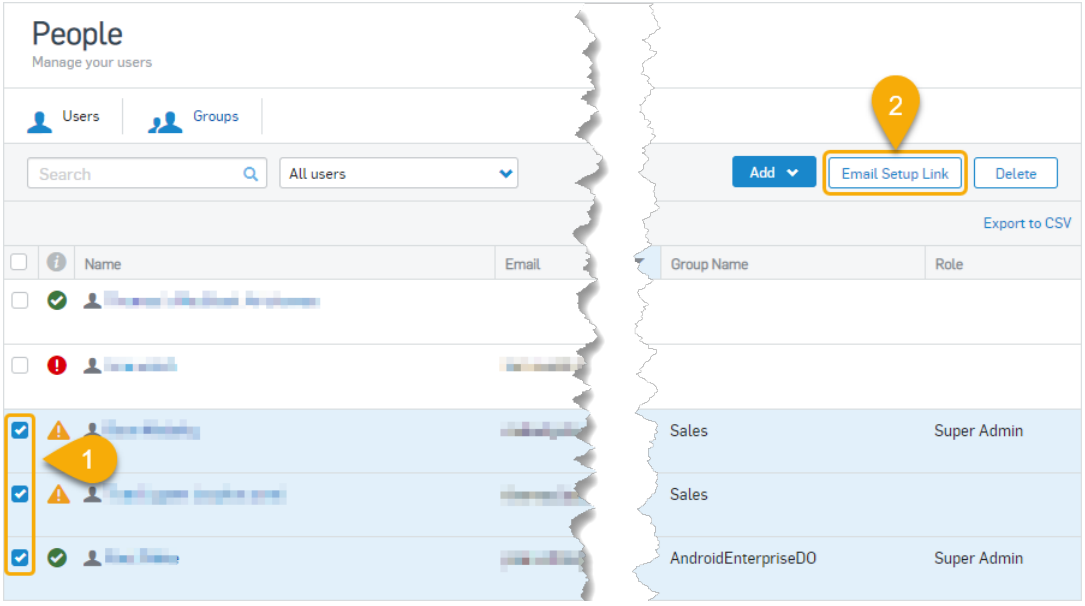
Standalone EAS proxy (Sophos Mobile administrator help)

6.10 Migrate Sophos Mobile Self Service Portal access

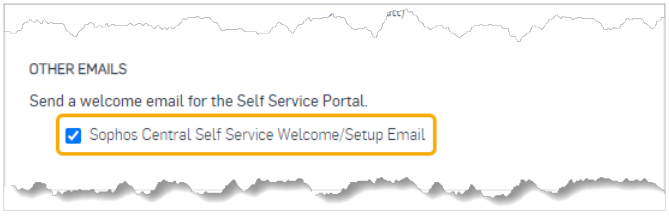
To give your users access to the Sophos Central Sophos Mobile Self Service Portal, send them a welcome email with their new credentials.

In Sophos Central Admin, do as follows:

1. Go to **People > Users**.
2. Select the users that you want to give access to the Sophos Mobile Self Service Portal.
3. Click **Email Setup Link**.



4. Select **Sophos Central Self Service Welcome/Setup Email**.



5. Click **Send**.

7 Migration issues

The **Preview export** and **Preview import** pages of the migration assistant show issues that require your attention.

Red exclamation mark next to an item

A condition that blocks migration. You must resolve the issue before you can start migration.

Hover over an item to display details about the issue.

Yellow warning sign next to an item

A condition where the migration assistant will modify your data. If you agree to the change, no action is required.

Hover over an item to display details about the issue.

You can’t migrate. You’ve set up Android Enterprise in Sophos Central.

In Sophos Central, unbind Android Enterprise. The migration assistant transfers your Android Enterprise configuration.

You can’t migrate. Synchronization with Google Play is in progress.

Wait for a few minutes. The warning disappears when synchronization with Google Play is complete.

You can’t migrate. You’ve set up Samsung Knox Mobile Enrollment.

Revoke the Knox Mobile Enrollment (KME) configuration.

After migration, set up KME in Sophos Central. See Migrate Knox Mobile Enrollment.

You can’t migrate. You’ve set up Android QR code enrollment.

Revoke the QR code.

After migration, set up Android QR code enrollment in Sophos Central. See Migrate Android Enterprise QR code enrollment.

You can’t migrate. You’ve set up Android zero-touch enrollment.

Revoke the Android zero-touch configuration.

After migration, set up zero-touch enrollment in Sophos Central. See Migrate Android zero-touch enrollment.

You can’t migrate. You’ve set up Sophos Chrome Security auto-enrollment.

Revoke the Google Workspace connection code.

After migration, set up Sophos Chrome Security auto-enrollment in Sophos Central. See Migrate Sophos Chrome Security auto-enrollment.

You can’t migrate. You’ve set up third-party EMM integration for Sophos Intercept X for Mobile.

Revoke the connection code for devices enrolled with a third-party Enterprise Mobile Management (EMM) program.

After migration, set up third-party EMM integration in Sophos Central. See Migrate third-party EMM integration.

You can’t migrate. You’ve set up federated authentication with Azure Active Directory.

Turn off federated authentication.

After migration, set up federated authentication for Sophos Central administrators and users. See Federated sign-in (Sophos Central Admin help).

You’re already managing <X> devices in Sophos Central.

Delete the devices that you added to Sophos Central. You can add them again after migration is completed.

Wrong Sophos Central license type.

Your Mobile license in Sophos Central doesn’t support the features that you’re trying to migrate.

Contact your Sophos sales representative.

Couldn’t transfer <X> app packages.

The migration assistant couldn’t transfer app packages that you uploaded to Sophos Mobile.

Click **Confirm manual transfer of app packages** to transfer the app packages manually. See Transfer app package files.

Couldn’t transfer <X> documents.

The migration assistant couldn’t transfer documents that you uploaded to Sophos Mobile.

Click **Confirm manual transfer of documents** to transfer the documents manually. See Transfer documents.

Error. Couldn’t copy objects from super administrator customer.

The migration assistant couldn’t copy items that were referenced from the super administrator customer. Please try again or contact Sophos Support.

Sophos Mobile apps out of date on <X> of <Y> Android devices.

Some Android devices have out-of-date Sophos Mobile apps installed. Update the following apps, where required: Sophos Mobile Control, Sophos Secure Workspace, Sophos Secure Email, Sophos Intercept X for Mobile.

Sophos Chrome Security out of date on <X> of <Y> Chrome devices.

Install the latest app version on all Chrome devices.

Sophos Mobile apps out of date on <X> iPhones and iPads.

Some iPhones and iPads have out-of-date Sophos Mobile apps installed. Update the following apps, where required: Sophos Mobile Control, Sophos Secure Workspace, Sophos Secure Email, Sophos Intercept X for Mobile.

Found <X> Windows Phone devices

Delete any Windows Phone and Windows Mobile devices in Sophos Mobile.

Can’t authenticate with Sophos Central. Check if your Sophos Central account exists.

The migration assistant can’t access the Sophos Central account from which you downloaded the migration token. Ensure that the account wasn’t removed.

This policy uses unavailable app groups. To export it, the super administrator must assign the following app groups to the customer: <X>

To resolve the issue, do as follows:

1. Sign in to Sophos Mobile with a super administrator account.
2. Open the app group for editing.
3. Click **Show** and select the customer that you’re trying to migrate.
4. On the **Edit app group** page, click **Save**.

Can’t connect to the Sophos Central account from the migration token.

The migration assistant can’t connect to Sophos Central.

Try again later or contact Sophos Support.

Sophos Mobile versions of source (<X>) and target (<Y>) systems don’t match.

The Sophos Mobile product in Sophos Central has a different version than the one you’re trying to migrate.

Contact Sophos Support to find out the required version.

This task bundle uses unavailable policies. To export it, the super administrator must assign the following policies to the customer: <X>

To resolve the issue, do as follows:

1. Sign in to Sophos Mobile with a super administrator account.
2. Open the policy that is displayed in the error message for editing.
3. Click **Show** and select the customer that you’re trying to migrate.
4. On the **Edit policy** page, click **Save**.
5. Repeat these steps for all policies that are displayed in the error message.

Email addresses aren’t unique.

Use a different email address for each user in Sophos Mobile.

Email addresses in Sophos Central aren’t unique.

Use a different email address for each user in Sophos Central.

Active Directory IDs aren’t unique.

Sophos Mobile uses the same ID for different Active Directory user accounts. Delete the users from Sophos Mobile.

Related information

Federated sign-in (Sophos Central Admin help)

8 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.

9 Legal notices