SOPHOS

Cybersecurity made simple.

Sophos Mobile

startup guide (SaaS)

product version: 9.5

Contents

1 About this document

This document explains how to set up Sophos Mobile step by step to manage your devices.

The descriptions apply to Sophos Mobile as a Service.

For other versions of this document, see the Sophos Mobile documentation web page.

2 What are the key steps?

To start using Sophos Mobile:

1. Reset your password, log in to Sophos Mobile Admin and change your administrator user name.
2. Optional: Activate your Mobile Advanced licenses to manage Sophos Intercept X for Mobile, Sophos Secure Workspace, and Sophos Secure Email.
3. Check your licenses.
4. Configure personal settings, password policies for administrator accounts, technical support contact details, and settings for the Self Service Portal.
5. Upload an Apple Push Notification service certificate to manage iPhones, iPads, and Macs.
6. Optional: Set up a standalone EAS proxy to filter email traffic from the managed devices to an email server.
7. Optional: Configure the interface for third-party Network Access Control systems.
8. Create compliance policies.
9. Create device groups.
10. Configure devices.
11. Update Self Service Portal settings.
12. Configure user management.
13. If you use internal user management: Add users either by creating them or by uploading your user list.
14. If you use external user management: Configure the connection to your LDAP directory.
15. Test device enrollment in the Self Service Portal.

3 Change your password

For security reasons, we recommend that you reset your password before you log in to Sophos Mobile Admin for the first time.

1. Open Sophos Mobile Admin in your web browser.
2. In the **Login** dialog, click **Forgot password?**.
3. In the **Reset password** dialog, enter your **Customer** and **User** information from the email you have received for the activation of your Sophos Mobile as a Service account, and then click **Reset password**.
   You will receive an email with a link to reset your password.
4. Click the link to open the **Change password** dialog.
5. Enter a new password, and then click **Change password**.
   Your password is changed. Remember to use this password next time you log in to the console.

Note
We recommend that you modify the password policies to enforce stronger passwords, for example by requiring a minimum number of lower-case, upper-case or special characters. See Configure password policies (page 8).

4 Change your login name

For security reasons, we recommend that you change your login name after the first login to Sophos Mobile Admin.

1. On the menu sidebar, under **SETTINGS**, click **Setup > Administrators**.
2. Click your login name.
3. On the **Edit administrator** page, enter a new value in the **Login name** field.
4. Optional: Adjust the values of the remaining fields:
   - **First name**
   - **Last name**
   - **Email address**
5. Select **Save**.

Your account details are changed. Remember to use the new login name next time you log in to Sophos Mobile Admin.

5 Activate Mobile Advanced licenses

With Mobile Advanced licenses you can use Sophos Mobile to manage Sophos Intercept X for Mobile, Sophos Secure Workspace, and Sophos Secure Email.

You activate Mobile Advanced licenses in Sophos Mobile Admin:

1. On the menu sidebar, under **SETTINGS**, click **Setup > Sophos setup**, and then click the **License** tab.
2. Enter your license key in the **Advanced license key** field and click **Activate**.

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

6 Check your licenses

Sophos Mobile uses a user-based license scheme. One user license is valid for all devices assigned to that user. Devices that are not assigned to a user require one license each.

On the menu sidebar, under **SETTINGS**, click **Setup > Sophos setup**, and then click the **License** tab.

The following information is displayed:

- **Maximum number of licenses**: Maximum number of device users (and unassigned devices) that can be managed.
- **Used licenses**: Number of licenses in use.
- **Valid until**: The license expiration date.

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

7 Configure settings

Configure the following settings:

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

7.1 Configure personal settings

You can adjust the appearance of Sophos Mobile Admin to your personal preferences. For example, you can set the language, the time zone, or the visible device platforms.

Note
These settings only affect the administrator account you're currently signed in with.

1. On the menu sidebar, under **SETTINGS**, click **Setup > General**, and then click the **Personal** tab.
2. Configure the following settings:

Option	Description
Language	The user interface language.
Time zone	The time zone in which dates are shown.
Unit system	The unit system for lengths (**Metric** or **Imperial**).
Lines per page in tables	The maximum number of entries displayed per table page.
Expert mode	This setting turns on additional features: • The **Show device** page includes the **Custom properties** tab with your custom device properties. • The **Show device** page includes the **Internal properties** tab with additional properties the device reports. • Several policy configuration pages include the **Extra settings** section to configure optional settings.
Activated platforms	The device platforms you want to view. In Sophos Mobile Admin, only pages and settings relevant for the selected platforms are shown.

3. Select **Save**.

7.2 Configure password policies

To enforce password security, configure password policies for Sophos Mobile Admin users and the Self Service Portal.

Note
The password policies do not apply to users from an external LDAP directory.

1. On the menu sidebar, under **SETTINGS**, click **Setup > General**, and then click the **Password policies** tab.
2. Under **Rules**, you can define password requirements, like a minimum number of lower-case, upper-case or numerical characters that a password must contain to be valid.
3. Under **Settings**, configure the following settings:
   a) **Password change interval (days)**: Enter the number of days until a password expires (between `1` and `730`), or leave the field empty to disable password expiration.
   b) **Number of previous passwords which must not be reused**: Select a value between `1` and `10`, or select `---` to disable this restriction.
   c) **Maximum number of failed login attempts**: Select the number of failed login attempts until the account gets locked (between `1` and `10`), or select `---` to allow an unlimited number of failed login attempts.
4. Select **Save**.

7.3 Configure IT contact

Provide your IT contact details so that users can get help with questions or problems.

The information you enter here is displayed in the Self Service Portal and on the users' devices.

1. On the menu sidebar, under **SETTINGS**, click **Setup > General**, and then click the **IT contact** tab.
2. Enter the contact information.
3. Select **Save**.

8 Set Android management mode

For Android devices, you can choose between the **Android Enterprise** and **Device administrator (legacy feature)** management modes.

We recommend you use Android Enterprise.

1. On the menu sidebar, under **SETTINGS**, select **Setup > Android setup** and then the **Android** tab.
2. In **Management mode**, select **Android Enterprise**.
3. Select **Save**.

Next, set up Android Enterprise for your organization.

8.1 Set up Android Enterprise - Overview

To set up Android Enterprise for your organization, you can choose between different scenarios. The Managed Google Play Account scenario is the easiest method to set up Android Enterprise and is described in this document.

For details on other Android Enterprise scenarios, see the Sophos Mobile administrator help.

Related information

Sophos Mobile administrator help

8.2 Set up Android Enterprise (Managed Google Play Account scenario)

Sophos Mobile guides you through the procedure to set up Android Enterprise for your organization.

1. On the menu sidebar, under **SETTINGS**, select **Setup > Android setup** and then the **Android Enterprise** tab.
2. Select **Configure**.
3. Select **“Managed Google Play Account” scenario** and then **Next**.
4. Select **Register account**.

   This redirects you to a Google website where you register your organization with Android Enterprise.
5. Sign in to the Google website with your Google account.

   Note
   We recommend that you create a new Google account for this purpose.

6. On the Google website, follow the steps to register your organization.

Tip
When specifying your organization name, we recommend that you include the term `Sophos Mobile`. For example:

```
Organization name (Sophos Mobile)
```

After you have completed the registration steps, the Google website redirects you back to Sophos Mobile.

7. In Sophos Mobile, select **Finalize setup** to complete the registration process.

Note
After you've set up Android Enterprise you can't change the user management mode, for example from internal user management to an external LDAP directory.

9 Apple Push Notification service certificates

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

APNs certificates have a validity period of one year.

9.1 Create APNs certificate

1. On the menu sidebar, under **SETTINGS**, click **Setup > Apple setup**, and then click the **APNs** tab.
2. Click **APNs certificate wizard**.
3. On the **Mode** page, click **Create a new APNs certificate**.
4. On the **CSR** page, click **Download certificate signing request**.
   This saves the certificate signing request file `apple.csr` to your local computer.
5. 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. On the **Apple ID** page, click **Create Apple ID in the Apple portal**.
   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.

6. In the wizard, enter your new Apple ID in the **Apple ID** field.
7. On the **Certificate** page, click **Create certificate on the Apple portal**.
   This opens the Apple Push Certificates Portal.
8. Log in with your Apple ID and upload the certificate signing request file `apple.csr`.
9. Download the `.pem` APNs certificate file and save it to your computer.
10. On the **Upload** page, click **Upload certificate** and then browse for the `.pem` file that you received from the Apple Push Certificates Portal.
11. Select **Save**.

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

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

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

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 15).
- The EAS proxy remembers the device status for 24 hours. If the Sophos Mobile server is offline, for example during an update, email traffic is filtered based on the last known device status. After 24 hours, all email traffic is blocked.

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.

10.1 Download the EAS proxy installer

1. Sign in to Sophos Mobile Admin.

2. On the menu sidebar, under **SETTINGS**, click **Setup > Sophos setup**, and then click the **EAS proxy** tab.
3. Under **External**, click the link to download the EAS proxy installer.

The installer file is saved to your local computer.

10.2 Install the standalone EAS proxy

Prerequisites:

- 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.
- You know the URL of the Sophos Mobile server. See Determine the Sophos Mobile server URL (page 18).

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 EAS Proxy Setup.exe` to start the **Sophos Mobile 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 EAS Proxy - Configuration Wizard** is started automatically and guides you through the configuration steps.
3. In the **Sophos Mobile server configuration** dialog, enter the URL of the Sophos Mobile server the EAS proxy will connect to.

   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.
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 the SSL Certificate Wizard from MySophos to request your SSL/TLS certificate for the Sophos Mobile EAS proxy.

   For general information about how to download Sophos software, see Sophos knowledge base 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 Exchange ActiveSync Server instance with which the proxy instance will connect.
   - **SSL**: Communication between the proxy instance and Exchange ActiveSync Server is secured by SSL or TLS (depending on what the server supports).
   - **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.

     — For information on how to configure EWS for your Exchange server, see Sophos knowledge base article 127137.

   - **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 Sophos Mobile server** 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 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 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. Sign in to Sophos Mobile Admin.
17. On the menu sidebar, under **SETTINGS**, click **Setup > Sophos setup**, and then click the **EAS proxy** tab.
18. Under **External**, click **Upload a file**. Upload the certificate that the configuration wizard created.
    If you have set up more than one instance, repeat this for all instance certificates.
19. Select **Save**.
20. 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.

10.3 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.

Note
Because macOS doesn't support the ActiveSync protocol, you can't use PowerShell to control email access by Macs.

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 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 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. On wizard page **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.
   - **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. 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 13).

Upload certificates

10. Sign in to Sophos Mobile Admin.
11. On the menu sidebar, under **SETTINGS**, click **Setup > Sophos setup**, and then click the **EAS proxy** tab.
12. Optional: Under **General**, select **Restrict to Sophos Secure Email** to restrict email access to the Sophos Secure Email app, available for Android and iOS.

    This prevents other email apps from connecting to your email server.
13. Under **External**, click **Upload a file**. Upload the certificate that the configuration wizard created.

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

10.4 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.

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 > Sophos setup**, and then click the **EAS proxy** tab.
2. Optional: Under **General**, select **Restrict to Sophos Secure Email** to restrict email access to the Sophos Secure Email app, available for Android and iOS.

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

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

10.5 Determine the Sophos Mobile server URL

You need the Sophos Mobile server URL to configure the standalone EAS proxy. The value is displayed in the Sophos Mobile system settings.

1. Sign in to Sophos Mobile Admin.
2. On the menu sidebar, under **SETTINGS**, click **Setup > Sophos setup**, and then click the **EAS proxy** tab.

Under **External**, the URL of the Sophos Mobile server is displayed.

11 Configure Network Access Control

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

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

To configure Network Access Control:

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

   - **Sophos UTM**

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

   - **Cisco ISE**

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

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

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

   - **Check Point**

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

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

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

- **Web service**

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

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

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

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

- **Custom**

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

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

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

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

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

12 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.

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.

12.1 Create compliance policy

1. On the menu sidebar, under **CONFIGURE**, click **Compliance policies**.
2. On the **Compliance policies** page, click **Create compliance policy**, and then select the template the policy will be based on:
   - **Default template**: A selection of compliance rules, with no actions defined.
   - **PCI template**, **HIPAA template**: Compliance rules and actions based on the HIPAA and the PCI DSS security standard, respectively.

   Your choice of template doesn't restrict your subsequent configuration options.
3. Enter a name and, optionally, a description for the compliance policy.

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.

Option	Description
	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 18). This action is only available for Android, iOS, Windows and Windows Mobile devices.
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 action is only available for Android and iOS devices.
Deny network	Forbid network access. This action can only be taken if you have configured Network Access Control. See Configure Network Access Control (page 19). This action is not available for devices where Sophos Mobile only manages the Sophos container.
Create alert	Trigger an alert. The alerts are displayed on the **Alerts** page.
Transfer task bundle	Transfer a specific task bundle to the device. This action is only available for Android, iOS, macOS and Windows devices. We recommend that you set this to **None** at this stage. For further information, see the Sophos Mobile administrator help. **CAUTION** 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
When an Android Enterprise fully managed device becomes non-compliant, all apps are disabled.

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

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

13 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.

13.1 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. Select **Save**.

Note
The device group settings contain the **Enable iOS auto-enrollment** option. This option allows you to enroll iOS devices with the Apple Configurator. For further information, see the Sophos Mobile administrator help.

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

14 Get started with device policies

The **Policies startup** wizard helps you create basic device policies for all platforms. You can enhance the policies later.

Restriction
These instructions don't apply to Chrome devices.

To create policies with the **Policies startup** wizard:

1. On the dashboard, click **Policies startup wizard** in the **Getting started tasks** widget.

   Tip
   If you don't see the widget, click **Add widget > Getting started**.

2. On the **Platforms** page, select the device platforms for which you want to create a policy.
   Select **Android** and **iOS**.
3. For **Android**, you can select a management mode.
   This setting affects which policy types are available. We recommend you use the **Android Enterprise** mode.
4. On the **Policies** page, configure the following settings:
   a) Enter a name for the policy.
      For each platform, a policy with this name is created.
   b) Select the areas the policy manages.
      If you clear a check box, the corresponding wizard page is skipped. You can configure the skipped areas (and more) later.
      We suggest you select at least **Password requirements** and **Restrictions**.
5. On the **Passwords** page, configure requirements for the device password.
6. On the **Restrictions** page, configure restrictions applied to devices, like turning off the camera or other device features that could be a security risk.
7. On the **Wi-Fi** page, configure the connection to your corporate Wi-Fi network.
   If your Wi-Fi network uses a different security type than **WPA/WPA2 PSK**, you can change that setting later.
8. On the **Email** page, configure the connection to your corporate Microsoft Exchange email server.
   The placeholders `%_USERNAME_%` and `%_EMAILADDRESS_%` are replaced by the name and the email address of the user assigned to the device.
9. Click **Finish**.

For each platform you've selected, the wizard creates a policy.

To view the policy, click **Policies** in the menu sidebar and then click the device platform.

To change the areas managed, click the policy's name and then click **Add configuration**.

If you've selected the **Android Enterprise** mode, you must set up Android Enterprise for your organization before you can enroll devices. See the Sophos Mobile administrator help.

15 Create task bundle for Android devices

You create separate task bundles for Android, iOS, and other device platforms you want to manage.

To create an enrollment task bundle for your Android devices:

1. On the menu sidebar, under **CONFIGURE**, select **Task bundles > Android**.
2. On the **Task bundles** page, select **Create task bundle**.
3. On the **Edit task bundle** page, enter a name and, optionally, a description for the task bundle.

   The version is automatically incremented every time you save the task bundle.
4. Optional: If you select **Selectable for compliance actions**, you can transfer the task bundle to devices when they become non-compliant.

   You configure this in a compliance policy.
5. Select **Add task > Enroll**. You're guided through adding an enrollment task to the task bundle.
   a) Optional: Change the name of the task.

      The name will be displayed in the Self Service Portal when the device is enrolled.
   b) Select the enrollment type.

      To enroll Android Enterprise fully managed devices with this task bundle, select **Android Enterprise full device management**.
   c) On the next page, select the policy that will be assigned to the device when it's enrolled.

      Only policies that match the enrollment type you've selected are displayed.
   d) Select **Finish**.
6. Optional: Select **Add task > Assign policy** to add more policies to the task bundle, for example if you've configured separate policies for Exchange, VPN, or Wi-Fi settings.
7. Optional: Add more tasks to the task bundle, for example to install apps or to display a message on the device.
8. Optional: Change the installation order of the tasks by using the arrow icons on the right-hand side of the tasks list.

16 Create task bundle for iOS devices

You create separate task bundles for Android, iOS, and other device platforms you want to manage.

To create an enrollment task bundle for your iPhones and iPads:

1. On the menu sidebar, under **CONFIGURE**, select **Task bundles > iOS**.
2. On the **Task bundles** page, select **Create task bundle**.
3. On the **Edit task bundle** page, enter a name and, optionally, a description for the task bundle.

   The version is automatically incremented every time you save the task bundle.
4. Optional: If you select **Selectable for compliance actions**, you can transfer the task bundle to devices when they become non-compliant.

   You configure this in a compliance policy.
5. Optional: Select **Ignore app installation failures** to continue the task bundle processing even if an app installation fails.

   This option is only available if the task bundle contains an **Install app** task.
6. Select **Add task > Enroll**. You're guided through adding an enrollment task to the task bundle.
   a) Optional: Change the name of the task.

      The name will be displayed in the Self Service Portal when the device is enrolled.
   b) Select the enrollment type.

      To enroll fully managed devices with this task bundle, select **Full MDM**.
   c) On the next page, select the policy that will be assigned to the device when it's enrolled.

      Only policies that match the enrollment type you've selected are displayed.
   d) Select **Finish**.
7. Optional: Select **Add task > Assign policy** to add more policies to the task bundle, for example if you've configured separate policies for Exchange, VPN, or Wi-Fi settings.
8. Optional: Add more tasks to the task bundle, for example to install apps or to display a message on the device.
9. Optional: Change the installation order of the tasks by using the arrow icons on the right-hand side of the tasks list.

17 Create Self Service Portal configurations

With a Self Service Portal configuration, you configure the types of devices that users can enroll, the enrollment details, and the device actions they can perform in the Self Service Portal.

You can use different Self Service Portal configurations for different users. To do so, add users to a user group and associate the group with a configuration. You can find details on user groups in related information.

If a user belongs to several groups that are all associated with Self Service Portal configurations, the configuration with the highest priority applies.

To create a Self Service Portal configuration:

1. On the menu sidebar, under **SETTINGS**, select **Setup > Self Service Portal**.
2. Select **Enrollment texts** and then add a terms of use text and a post-enrollment text.

   When you assign these texts to your Self Service Portal configuration, they are displayed before and after the enrollment, respectively.
3. On the **Self Service Portal configurations** page, select **Add** to create a configuration.
4. Configure the following settings:

Option	Description
Name	The name of the configuration. In the Self Service Portal, users select a configuration by this name.
User groups	Select **Add** and then enter a user group. The configuration is applied to all members of that group.
Maximum number of devices	The maximum number of devices a user can enroll in the Self Service Portal.
Actions	Select **Show** and then select the management actions a user can perform in the Self Service Portal.

5. Select **Add > Android**.
6. In the **Configure platform settings** dialog, configure the following settings:

Option	Description
Display name	The name of the platform settings. In the Self Service Portal, users select an enrollment type by this name.
Description	A description of the platform settings. This description is displayed in the Self Service Portal next to the name.

Option	Description
Owner	The owner mode (corporate or personal) of devices enrolled with this configuration.
Device group	The device group the device is added to.
Enrollment package	Select the Android task bundle you've created.
Terms of use	The text to be displayed in the Self Service Portal before the enrollment. Leave this field empty to display no text. Users must agree to the text to proceed with the enrollment.
Post-enrollment text	The text to be displayed in the Self Service Portal after the enrollment. Leave this field empty to display no text.

7. Select **Apply** to add the platform settings to the Self Service Portal configuration.
8. Select **Add > iOS**, and then repeat the configuration steps you performed for Android.
9. On the **Edit Self Service Portal configuration** page, select **Save**.

There always is a **Default** configuration. This configuration has the lowest priority, so that it is only used when no other configuration matches a user.

18 Configure user management

Sophos Mobile offers two different methods for managing user accounts for Sophos Mobile Admin and the Self Service Portal:

- With **internal user management** you can create users by adding them manually in Sophos Mobile Admin or by importing them from a CSV file.
- With **external user management** you can connect to an existing LDAP directory and assign devices to groups and profiles based on directory membership.

Note

- You cannot change the user management method after devices have been assigned to users.
- For external user management, an LDAPS (LDAP over SSL/TLS) environment must be available. Sophos Mobile connects to the LDAP server using the default LDAPS port 636.

To select the user management method:

1. On the menu sidebar, under **SETTINGS**, click **Setup > Sophos setup**, and then click the **User setup** tab.
2. Select the data source for the user accounts for Sophos Mobile Admin and the Self Service Portal (SSP):
   - Select **Internal directory** to use internal user management.
   - Select **External LDAP directory** to use external user management instead of or in combination with internal user management.
3. If you selected **External LDAP directory**, click **Configure external LDAP** to specify the server details. See Configure external directory connection (page 32).
4. Select **Save**.

Note

After you have saved your settings, only the selected user management method is available on the **User setup** tab. To change your selection afterward, select and save **None. No SSP, user-specific profiles, or LDAP administrators available.** first to make all options available again.

19 Use internal user management

19.1 Create a Self Service Portal test user

To test provisioning through the Self Service Portal, create a Self Service Portal user account for yourself. You will use this account to log in to the Self Service Portal and test device enrollment.

To create a test user account for the Self Service Portal:

1. On the menu sidebar, under **MANAGE**, select **People**.
2. Click **Create user**.
3. Configure the required account details.

   Make sure that **Send registration email** is selected.
4. Select **Save**.

The user is added to the list of Self Service Portal users and a registration email is sent to the email address that you specified in the account details.

19.2 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 the test user account you created for yourself in Create a Self Service Portal test user (page 30) and perform test enrollments for all platforms that you want to manage with Sophos Mobile.

19.3 Import users

After you have tested device enrollment through the Self Service Portal, you can import your user list into Sophos Mobile.

The import of users is only relevant for internal user management. For external user management, all users that are assigned to a certain LDAP group can log in to the system.

You can import up to 500 users.

If you specify a group that doesn't exist, Sophos Mobile creates it.

The CSV file must have the following specification:

- The first row is treated as a header and is not imported.
- Values must be separated by semicolon, not by comma.
- All rows must have the correct number of semicolon characters, even if you leave out optional values.
- The file extension must be `.csv`.
- To ensure that non-English characters are imported correctly, the file must be UTF-8 encoded.

Tip
On the **Import users** page, select **Example CSV** to download a sample file.

To import users from a CSV file:

1. On the menu sidebar, under **MANAGE**, select **People**.
2. Select **Import users**.
3. On the **Import users** page, select **Send registration emails**.
4. Select **Upload a file** and then navigate to the CSV file you've prepared.
   The entries are read in from the file and are displayed.
5. If the data is not formatted correctly or is inconsistent, the file as a whole cannot be imported. In this case, follow the error messages that are displayed next to the relevant entries, correct the content of the CSV file accordingly and upload it again.
6. Select **Finish** to create the user accounts.

The users are imported and displayed on the **People** page. They receive emails with their login credentials for the Self Service Portal.

20 Use external user management

20.1 Configure external directory connection

To manage user accounts for Sophos Mobile Admin and the Self Service Portal in an external LDAP user directory, you must configure the connection to your LDAP server.

Sophos Mobile can connect to the following LDAP servers:

- **Active Directory**
- **Google Cloud Directory**
- **IBM Domino**
- **NetIQ eDirectory**
- **Red Hat Directory Server**
- **Zimbra**

For supported versions, see the Sophos Mobile 9.5 release notes.

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

1. On the menu sidebar, under **SETTINGS**, click **Setup > Sophos setup**, and then click the **User setup** tab.
2. Select **External LDAP directory**.
3. Click **Configure external LDAP**.

Configuration depends on the LDAP server type. The following instructions apply to Active Directory.

4. On the **Server details** page, configure the following settings:
   a) In the **LDAP type** field, select the LDAP server type.
   b) In the **Primary URL** field, enter the IP address or name of the primary directory server.
      Select **SSL/TLS** to secure the server connection by SSL or TLS (depending on what the server supports).
   c) Optional: In the **Secondary URL** field, enter the IP address or name of a directory server Sophos Mobile uses as fallback in case the primary server isn't available.
   d) In the **User** and **Password** fields, enter the credentials Sophos Mobile uses to authenticate with the LDAP server.
      Use one of the following formats:
      - `<domain>\<user name>`
      - `<user name>@<domain>.<domain code>`

Note
For security reasons, we recommend you select an account with no write permissions for the directory.

5. On the **Search base** page, enter the distinguished name (DN) of the search base object.
   The search base object defines the location in the directory from which the LDAP search begins.
6. On the **Search fields** page, configure the attributes of the directory service that contain the user properties Sophos Mobile uses.
   Select the attribute names from the list or enter them manually.
   Use the following mappings for Active Directory:

Property in Sophos Mobile	Attribute in Active Directory
User name	`sAMAccountName`
First name	`givenName`
Last name	`sn`
Email	`mail`

7. On the **SSP configuration** page, specify the users that are allowed to log in to the Self Service Portal. Enter the relevant information in the **LDAP directory group** field, using one of the following options:
   - If you enter the name of a group that is defined on the directory server, all members of that group are allowed to log in to the Self Service Portal. After you have entered the group name, click **Test group** to resolve the group name into a Distinguished Name (DN).
   - If you leave the field empty, no users from the directory server are allowed to log in to the Self Service Portal. Use this option if you want to enable external user management for Sophos Mobile Admin but not for the Self Service Portal.

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

8. Select **Apply**.
9. On the **User setup** tab, click **Save**.

Related information

How to connect a Sophos Mobile 8.0 server with an Azure Active Directory (Sophos knowledge base article 128081)

Connecting Sophos Mobile to Google Cloud Identity / Google Cloud Directory using Secure LDAP (Sophos knowledge base article 132870)

20.2 Test device enrollment for LDAP users

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

Log in to the Self Service Portal with your LDAP credentials and perform enrollment tests on all the platforms that you want to manage with Sophos Mobile.

21 Use the **Add device** wizard

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

- Add a new device to Sophos Mobile.
- Optional: Assign a user to the device.
- Enroll the device.
- Optional: Transfer a task bundle to the device.

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

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

2. On the **User** page, either enter search criteria to look up a user the device will be assigned to, or select **Skip user assignment** to enroll a device that will not be assigned to a user yet.
3. On the **User selection** page, select the required user from the list of users matching your search criteria.
4. On the **Device details** 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. If user management is configured for the customer, this is the email address of the user assigned to the device. If no user management is configured, enter an email address here.
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. On the **Enrollment type** page, select whether you want to enroll the device or only the Sophos container.

   Select **Enroll device**.
6. Select the task bundle you've configured for the device platform.
7. On the **Enrollment** page, follow the instructions to complete the enrollment process.
8. When enrollment has been completed successfully, click **Finish**.

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.

22 Glossary

ad hoc provisioning profile	A distribution provisioning profile you add to a self-developed iOS app. This allows you to install the app on designated devices without having to publish it to the App Store.
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 Sophos Mobile Admin 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 Sophos Intercept X for Mobile, Sophos Secure Workspace, and Sophos Secure Email.
provisioning	The process of installing the Sophos Mobile Control app on a device.
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 console	The web interface that you use to manage devices.
Sophos Intercept X for Mobile	A security app for Android and iOS 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.

Team ID	Every iOS and macOS app is signed by a Team ID. The Team ID is supplied by Apple and is unique to a specific development team.

23 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.

24 Legal notices