Contents

About this help..........................................................................................................................................................1
About Sophos Mobile..................................................................................................................................................2
About Sophos Mobile Admin.......................................................................................................................................3
    User interface..........................................................................................................................................................3
    Table views..........................................................................................................................................................3
    Prerequisites..........................................................................................................................................................4
    User roles............................................................................................................................................................4
    Log in to Sophos Mobile Admin..........................................................................................................................5
    Log out from Sophos Mobile Admin.....................................................................................................................6
    Change your password........................................................................................................................................6
    Password recovery...............................................................................................................................................6

Key steps for managing devices with Sophos Mobile............................................................................................7
Dashboard...............................................................................................................................................................8
Reports.....................................................................................................................................................................9
Tasks.......................................................................................................................................................................10
    Monitor tasks......................................................................................................................................................10
Alerts.......................................................................................................................................................................13
General settings.....................................................................................................................................................15
    Configure personal settings..............................................................................................................................15
    Configure password policies.............................................................................................................................16
    Configure SMC app settings...............................................................................................................................17
    Enable Baidu Cloud Push service......................................................................................................................17
    Configure iOS settings.....................................................................................................................................17
    Configure polling interval for Windows devices............................................................................................18
    Configure Email...............................................................................................................................................19
    Configure technical support contact details....................................................................................................19
    Define customer properties................................................................................................................................19

Configure Self Service Portal..................................................................................................................................21
    Create Self Service Portal groups with internal user management.................................................................21
    Configure Self Service Portal settings............................................................................................................22
    Available Self Service Portal actions...............................................................................................................23
    Manage Self Service Portal users....................................................................................................................26

System setup..........................................................................................................................................................32
    Check your licenses............................................................................................................................................32
    Apple Push Notification service certificates.....................................................................................................33
    Configure iOS AirPlay destinations....................................................................................................................37
    Register Samsung Knox license.......................................................................................................................37
    Simple Certificate Enrollment Protocol (SCEP)..................................................................................................37
    Configure user setup........................................................................................................................................38

Compliance policies................................................................................................................................................39
    Create compliance policy................................................................................................................................39
    Available compliance rules...............................................................................................................................41
    Assign a compliance policy to device groups..................................................................................................45
    Check devices for compliance..........................................................................................................................46

Devices....................................................................................................................................................................47
    Add devices.........................................................................................................................................................47
    Enroll devices.....................................................................................................................................................48
    Unenroll devices.................................................................................................................................................48
    Manage devices..................................................................................................................................................55
    Apple DEP.........................................................................................................................................................56
    Duo Security integration....................................................................................................................................74

Device groups.........................................................................................................................................................76
1 About this help

This help describes how to use Sophos Mobile Admin.

Further information is available in the following documents:

• For a description of Sophos Mobile installation, see the Sophos Mobile installation guide. This guide is not relevant for Sophos Mobile as a Service.
• For information on how to use Sophos Mobile Admin as a super administrator for customer management, see the Sophos Mobile super administrator guide. This guide is not relevant for Sophos Mobile as a Service.
• For a description of the key steps for initial configuration, see the Sophos Mobile startup guide and the Sophos Mobile as a Service startup guide.
• For information on the Self Service Portal, see the Sophos Mobile user help.

Document conventions

The following conventions are used in this help:

• Unless otherwise noted, Windows Mobile refers to Windows 10 Mobile and Mobile Enterprise editions and to Windows Phone 8.1.
• Unless otherwise noted, Windows or Windows 10 refers to Windows 10 Pro, Enterprise, Education, Home and S editions.
• Unless otherwise noted, Windows IoT refers to the Windows 10 IoT Core edition.
• Unless otherwise noted, all procedures assume that you are logged in to Sophos Mobile Admin using an administrator account.
About Sophos Mobile

Sophos Mobile

Sophos Mobile is the EMM solution for businesses that want to spend less time and effort to manage and secure mobile devices. Manage mobile devices with the easy-to-use, web-based, unified Sophos Central admin interface alongside endpoint, network, or server security from Sophos. Secure container apps and support for mobile OS containerization in iOS, Android enterprise, and Samsung Knox ensure sensitive company data stays separated from personal information on the device.

With its best-in-class data protection, comprehensive security, value-for-money, and flexible management options, Sophos Mobile is the best way to allow the use of mobile devices for work, keeping users productive, business data safe and personal data private.

Sophos Mobile Security


Sophos Secure Workspace

Sophos Secure Workspace is a containerized mobile content management app for iOS and Android that provides a secure way to protect, manage, and distribute business documents and web content. Edit Office format documents without leaving the container environment to ensure encrypted content remains secure. Anti-phishing technology protects users from malicious links in documents and content.

When managed by Sophos Mobile, admins can easily restrict access to content based on device compliance rules. In combination with Sophos SafeGuard Encryption, Sophos Secure Workspace provides seamless exchange of encrypted files—stored locally or in the cloud—between Windows, macOS, iOS and Android users.

Sophos Secure Email

Sophos Secure Email is a fully featured, secure, and containerized email app for Android and iOS that lets you isolate business email, calendar and contacts from private data on a mobile device when managed by Sophos Mobile. All company information is protected with AES-256 encryption and access can easily be revoked based on device compliance rules. Sophos Secure Email also lets IT provision business email securely and consistently across different devices and OS variations.
3 About Sophos Mobile Admin

Sophos Mobile Admin is the central instrument for managing devices with Sophos Mobile. It is the web interface of the server used for device management. With the web portal you can implement a corporate policy for the use of devices and apply it to the devices that are enrolled with Sophos Mobile.

In Sophos Mobile Admin you can:

- Configure the system, for example personal settings or platform-specific settings.
- Configure compliance policies and define actions to be taken if devices no longer comply with the rules specified. See Compliance policies (page 39).
- Enroll devices with Sophos Mobile. See Add devices (page 47).
- Provision new devices. See Enroll devices (page 48).
- Install apps on enrolled devices. See Apps (page 244).
- Define profiles and security policies for devices. See Profiles and policies (page 77).
- Create task bundles to bundle several tasks and transfer them to the devices in one transaction. See Task bundles (page 233).
- Carry out administrative tasks on devices, for example reset the password of devices, lock or wipe devices if they are lost or stolen, unenroll devices. See Manage devices (page 56).
- Create and view reports. See Reports (page 9).

3.1 User interface

The Sophos Mobile Admin user interface is divided into a header, a main menu, and the main frame. The main frame displays the different pages of Sophos Mobile Admin, based on the selected menu.

- **Header**
  The page header has these links on the right side:
  - Your account name and the customer name.
  - The Help button that opens online help in a separate browser window.
  - The Logout button that logs you off from Sophos Mobile Admin.

- **Main menu**
  The main menu on the left lets you access the main functions of Sophos Mobile.

---

**Note**
Your assigned administrator role affects what you can do. See User roles (page 4).

3.2 Table views

In Sophos Mobile Admin, many pages display information in a tabular form. These tables have common controls that you can interact with.

Above the table:
Sophos Mobile on Premise

- Use the **Show or hide columns** icon to configure which table columns are visible.
- Enter text in the **Search all fields** field to only display data rows that contain that text in any column.

In the table:
- Click a column header to sort the table rows by that property. Click again to revert the sort order.
- Click the blue triangle next to an entry name to perform actions on that entry, like **Show**, **Edit**, **Delete**.

Below the table:
- Use the navigation buttons to display a specific table page.
- Use the **Export** icon to export either the whole table or the current page to a Microsoft Excel file or a comma-separated values (CSV) file. If you have configured a row filter, only the currently visible rows are exported.

### 3.3 Prerequisites

Before using Sophos Mobile Admin:

- You need a computer connected to the internet and equipped with a web browser. For information on supported browsers and the relevant versions, see the *Sophos Mobile release notes*.
- The super administrator must have created a customer (a tenant whose devices are managed in Sophos Mobile). For further information, see the *Sophos Mobile super administrator guide*.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>For Sophos Mobile as a Service, a customer is predefined. Super administrators are not supported for Sophos Mobile as a Service.</td>
</tr>
</tbody>
</table>

- You need a Sophos Mobile user account and the relevant credentials for logging in to Sophos Mobile Admin. The credentials consist of customer, user and password. For further information, see **Log in to Sophos Mobile Admin** (page 5).

### 3.4 User roles

Sophos Mobile administrators have different roles. The role affects what an administrator can do.

The available roles are:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>This role has the rights to perform all available actions.</td>
</tr>
<tr>
<td>Limited Administrator</td>
<td>This role is allowed to perform all actions required for enrolling and managing a device, but cannot specify essential settings and cannot manage other administrators.</td>
</tr>
<tr>
<td>Reporting</td>
<td>This role can view the list of devices and is able to create reports. For example, an auditor or an employee who needs to document the settings in Sophos Mobile.</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Content admin</td>
<td>This role is intended for employees responsible for uploading, updating or removing documents. Usually this role is assigned to a person outside the IT department. The permissions are set to limit visibility and access only the content in the <em>Documents</em> menu.</td>
</tr>
<tr>
<td>Helpdesk</td>
<td>This role is intended for support purposes. It has only limited rights (for example installation of software packages). This role does not have access to critical functions, such as defining settings and creating, deleting or editing devices/device groups, packages and profiles.</td>
</tr>
<tr>
<td>Read-only</td>
<td>This role has read-only access to all settings that are available to the Administrator role.</td>
</tr>
<tr>
<td>App Group Administrator</td>
<td>This role can manage app groups. A typical user is an administrator that accesses the Sophos Mobile web service interface to create, update or read app groups.</td>
</tr>
<tr>
<td>Duo API</td>
<td>This role is required for integration with the Duo Security authentication software. Administrators with the <em>Duo API</em> role can access the Sophos Mobile web service interface for requesting the management status of devices.</td>
</tr>
</tbody>
</table>

*Tip*
Your Sophos Mobile product delivery includes the Role Editor. Role Editor lets you easily modify existing user roles or create your own custom roles. You can find it in the `%MDM_HOME%\tools\Wizard` folder, where `%MDM_HOME%` is the Sophos Mobile installation folder.

For information on how to use the Role Editor, see Sophos knowledgebase article [122066](#) or contact the Sophos support team.

**Related tasks**
Create administrators (page 281)

### 3.5 Log in to Sophos Mobile Admin

1. Open Sophos Mobile Admin in your web browser.
2. In the login dialog, enter your customer name and your user credentials (name and password), then click **Login**.

The customer’s *Dashboard* page is displayed.

**Note**
When you log in to Sophos Mobile Admin for the first time, you are prompted to change your password.
3.6 Log out from Sophos Mobile Admin

To log out from Sophos Mobile Admin, click **Logout** in the page header.

3.7 Change your password

You can change your password any time after you have logged in to Sophos Mobile Admin:

1. On the menu sidebar, under **SETTINGS**, click **Setup > General**, and then click the **Change password** tab.
2. Enter your old password, a new one and confirm it.
3. Click **Save**.

3.8 Password recovery

If you have forgotten your password for Sophos Mobile Admin, you can reset it.

1. In the **Login** dialog box of Sophos Mobile Admin, click **Forgot password?**
   The **Reset password** dialog box is displayed.
2. Enter your account information and click **Reset password**.
   You receive an email with a link for resetting your password.
3. Click the link.
   The **Change password** dialog box is displayed.
4. Enter a new password, confirm it and click **Change password**.

Your password has been changed and you are logged in to Sophos Mobile Admin.
4 Key steps for managing devices with Sophos Mobile

Sophos Mobile offers a wide range of Mobile Device Management functions depending on device types, corporate security policies and specific requirements in your company.

The key steps for managing devices with Sophos Mobile are:

• Configure compliance policies for devices. See Compliance policies (page 39).
• Create device groups. See Create device group (page 76).
  
  Device groups are used to categorize devices. We recommend that you put devices into groups. This helps you to manage them efficiently as you can carry out tasks on a group rather than on individual devices.
• Enroll and provision devices. See Add devices (page 47) and Enroll devices (page 48).
  
  Devices can either be enrolled and provisioned by administrators in Sophos Mobile Admin or by device users in the Self Service Portal.
• Set up profiles and security settings for devices. See Profiles and policies (page 77).
• Create task bundles. See Task bundles (page 233).
• Configure the available features of the Self Service Portal. See Configure Self Service Portal (page 21).
• Apply new or updated profiles and security settings to enrolled devices.
5 Dashboard

Note
This section applies to the Dashboard page of regular administrators. For the super administrator, the Dashboard page is used to manage customers. See the Sophos Mobile super administrator guide.

The customizable Dashboard is the regular start page of Sophos Mobile and provides access to the most important information at a quick glance. It consists of several widgets providing information about:

- Devices, all or per group
- Compliance status by platform or for all devices
- Managed status by platform or for all devices
- The SSP registration status
- The managed platform versions

There also is a special widget Add device to start the device enrollment wizard. See Use the device enrollment wizard to assign and enroll new devices (page 50).

The following options are available to customize the Dashboard:

- To add a widget to the page, click Add widget.
- To remove a widget from the page, click the Close button in its header.
- To reset the page to its default layout, click Restore default layout.
- To rearrange the widgets on the page, drag a widget header.
6 Reports

With Sophos Mobile you can create various reports from the following areas:
- Devices
- Apps and documents
- Compliance
- Malware
- Certificates

To create a report:
1. On the menu sidebar, under **INFORM**, click **Reports**, and then click the name of the required report.
2. In the **Choose format** dialog, click one of the available icons to select the output format:
   - Click ![Excel](image) to export the report to a Microsoft Excel file.
   - Click ![CSV](image) to export the report to a comma-separated values (CSV) file.

The report is saved to your local computer, using the download settings of your web browser.
7 Tasks

The Task view page gives you an overview of all tasks you created and started and displays their current state. You can monitor all your tasks and intervene in case of problems. For example, you can delete a task that cannot be completed but blocks the device.

To delete a task, click the Delete icon next to it.

You can filter tasks according to their type and state and sort them by device name, package name, creator and scheduled date.

7.1 Monitor tasks

In Sophos Mobile Admin, you can monitor all existing tasks for devices.

- The Tasks page shows all unfinished and failed tasks as well as the finished tasks of the last few days. The Task view page is refreshed automatically, so you can watch the states of the tasks evolve.
- The Task details page shows general information about a task from the Tasks page or the Task archive page.
- The Task archive page shows all tasks.

7.1.1 View unfinished, failed and latest finished tasks

1. On the menu sidebar, under INFORM, click Tasks.
2. On the Task view page, the State column shows the task status, for example, Completely failed.
3. In the Refresh interval (in sec.) field, you can select how often the Task view page is to be refreshed.
4. To view further details about a task, click the Show magnifier icon next to the required task.
   The Task details page is displayed. Besides general information on the task (for example, device name, package name and creator) it shows the states a specific task went through, including timestamps and error codes. If there are commands to be executed by the device, an additional Details button is available on the Task details page.
5. If available, click Details to view the commands to be executed by the device. The commands sent to the device are part of the task. They are executed by the SMC app or by the MDM client. Results indicating the success or failure are transferred back to the server. If there was no error, the error code is “0”. If a command has failed, the error code is displayed. In most cases there is also a description of what may have caused the command to fail.
6. To return to the Task details page, click Back.

7.1.2 View task archive

1. On the menu sidebar, under INFORM, click Tasks.
2. On the Task view page, click Task archive.
   The Task archive page is displayed. It shows all finished and failed tasks in the system.
3. On this page, you can:
• Click **Reload** to refresh the **Task archive** page.
• Delete a task from the archive by clicking the **Delete** icon next to the relevant task.
• Select several tasks and click **Delete selected** to delete them from the archive.

To go back to the **Task view** page, click **Tasks** on the menu sidebar.

### 7.1.3 Task states

The following table provides an overview of the task states shown on the **Task view** and on the **Task archive** pages.

Every state is associated with a color code that indicates the state category.

<table>
<thead>
<tr>
<th>Color code</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Accepted</td>
<td>Task has been created.</td>
</tr>
<tr>
<td></td>
<td>Will be retried</td>
<td>Task will be retried later.</td>
</tr>
<tr>
<td></td>
<td>Started</td>
<td>Task has been started.</td>
</tr>
<tr>
<td></td>
<td>In progress</td>
<td>Execution of the task is being prepared.</td>
</tr>
<tr>
<td></td>
<td>Task bundle in progress</td>
<td>Execution of the task bundle is being prepared.</td>
</tr>
<tr>
<td></td>
<td>Notified</td>
<td>SMC app was notified.</td>
</tr>
<tr>
<td></td>
<td>Commands sent</td>
<td>SMC app has received the package and/or the commands.</td>
</tr>
<tr>
<td></td>
<td>Result evaluation started</td>
<td>SMC app has answered and the evaluation of the result has been started.</td>
</tr>
<tr>
<td></td>
<td>Result incomplete</td>
<td>Result evaluation showed that not all commands’ results have been received by now.</td>
</tr>
<tr>
<td></td>
<td>Waiting for user interaction</td>
<td>There is a pending user action on the device.</td>
</tr>
<tr>
<td></td>
<td>Waiting for task completion</td>
<td>An installation task was sent to the device, but it may take some time to complete.</td>
</tr>
<tr>
<td></td>
<td>Device is locked</td>
<td>Task waits for the device to become unlocked (iOS only).</td>
</tr>
<tr>
<td>Color code</td>
<td>State</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td><strong>Successful</strong></td>
<td>Package has been installed or the commands have been successfully executed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For the initial provisioning of the Sophos Mobile Control app the task must finish with the state <em>Installed</em>.</td>
</tr>
<tr>
<td></td>
<td><strong>Installed</strong></td>
<td>The Sophos Mobile Control app has been installed successfully. The device is provisioned now.</td>
</tr>
<tr>
<td></td>
<td><strong>Result evaluation failed</strong></td>
<td>Result evaluation could not be executed.</td>
</tr>
<tr>
<td></td>
<td><strong>Task partly failed</strong></td>
<td>Not all commands of the task could be executed successfully.</td>
</tr>
<tr>
<td></td>
<td><strong>Delayed</strong></td>
<td>Task will be restarted later.</td>
</tr>
<tr>
<td></td>
<td><strong>Failed (retry queued)</strong></td>
<td>Task has failed and will be retried later.</td>
</tr>
<tr>
<td></td>
<td><strong>Task failed</strong></td>
<td>Task has failed and no further retries are queued.</td>
</tr>
<tr>
<td></td>
<td><strong>Completely failed</strong></td>
<td>Task has failed, and it is not possible to retry it.</td>
</tr>
<tr>
<td></td>
<td><strong>Not started</strong></td>
<td>Task is part of a task bundle and was not processed yet.</td>
</tr>
<tr>
<td></td>
<td><strong>Skipped</strong></td>
<td>Task is not supported by device. Task bundle execution continues with the next task.</td>
</tr>
<tr>
<td></td>
<td><strong>Unknown</strong></td>
<td>The server has no information about the task status.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Color code</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Open</strong></td>
</tr>
<tr>
<td></td>
<td><strong>In progress</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Success</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Failure</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Other</strong></td>
</tr>
</tbody>
</table>
8 Alerts

The Alerts page lists the alerts that require your attention.

For each alert, the list shows the event that caused the alert, when it occurred, and which user and device are affected.

The list also shows the severity of alerts:

- Gray info sign for informational alerts
- Orange warning sign for medium-priority alerts
- Red warning sign for high-priority alerts

Acknowledge alerts

Select one or more alerts and then click Mark as acknowledged to remove the selected alerts from the list. To display acknowledged alerts, select Show acknowledged alerts in the drop-down list above the table.

Note

Acknowledging an alert does not resolve the event that triggered it.

Important

Alerts are automatically deleted from the Sophos Mobile database after 90 days, even if you have not acknowledged them.

Set up email reports for alerts

Sophos Mobile sends email reports for all alerts that have not been acknowledged yet. For information on how to set up the list of recipients and the notification schedule, see Configure Email (page 19).

Which events trigger alerts?

Alerts are created for the following events:

- Compliance violations for which you have activated the Create alert action. See Create compliance policy (page 39).
- Resolved compliance violations
- Device lifecycle changes:
  - Add device
  - Enroll device
  - Unenroll device
Sophos Mobile on Premise

• Important device actions:
  — Wipe device
  — Lock device
  — Locate device
  — Reset password
• Exceeded thresholds of cellular data usage
• Successful and failed tasks
• Undefined placeholders that are used in profiles or policies
• Upcoming expirations of the following licenses and certificates:
  — Sophos Mobile license
  — Apple Volume Purchase Program (VPP) license
  — Apple Device Enrollment Program (DEP) license
  — Samsung Knox Premium license
  — Sophos Mobile server’s SSL/TLS certificates
  — Apple Push Notification service (APNs) certificate
  — Root and client certificates configured in profiles and policies
  — Device certificates
• Additional events for APNs certificates:
  — APNs certificate renewed
  — APNs certificate revoked
  — No APNs certificate configured
• Sophos Mobile Security events:
  — Malware detected or cleaned up
  — PUA detected or cleaned up
  — Low reputation app detected or cleaned up
• Android enterprise events:
  — Google communication errors
  — Unapprove work app used in task bundles
9 General settings

On the General settings page you can perform the following tasks:

- **Personal**  
  - Configure personal settings (page 15)
- **Change password**  
  - Change your password (page 6)
- **Password policies**  
  - Configure password policies (page 16)
- **SMC app**  
  - Configure SMC app settings (page 17)
- **Android**  
  - Enable Baidu Cloud Push service (page 17)
- **iOS**  
  - Configure iOS settings (page 17)
- **Windows**  
  - Configure polling interval for Windows devices (page 18)
- **Email configuration**  
  - Configure Email (page 19)
- **Technical contact**  
  - Configure technical support contact details (page 19)
- **Customer properties**  
  - Define customer properties (page 19)

9.1 Configure personal settings

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

**Note**

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

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language</td>
<td>Select the language for Sophos Mobile Admin.</td>
</tr>
<tr>
<td>Timezone</td>
<td>Select the timezone in which dates are shown.</td>
</tr>
</tbody>
</table>
### Sophos Mobile on Premise

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

**Note**  
The list of available platforms depends on your platform settings from the super administrator configuration.  
For further information, see the [Sophos Mobile super administrator guide](#).

3. Click **Save**.

### 9.2 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. For information on external user management, see the [Sophos Mobile super administrator guide](#).

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. Click **Save**.

### 9.3 Configure SMC app settings

On the **SMC app** tab of the **General settings** page, you configure settings for the Sophos Mobile Control app on Android, iOS and Windows Mobile devices.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable unenrollment through app</td>
<td>Remove the <strong>Unenroll</strong> button from the Sophos Mobile Control app to prevent users from unenrolling their device through the app.</td>
</tr>
</tbody>
</table>

**Note**

To completely prevent user-initiated unenrollment, also disable the **Unenroll device** option in the Self Service Portal settings. See Configure Self Service Portal settings (page 22).

3. Click **Save**.

### 9.4 Enable Baidu Cloud Push service

Sophos Mobile uses the Google Cloud Messaging (GCM) service to send push notifications to Android devices, to trigger them to contact the Sophos Mobile server. In China, GCM will likely not work. Therefore, Sophos Mobile can also use Baidu Cloud Push, which is a Chinese push notification service.

If you manage Android devices that are located in China, enable the Baidu Cloud Push service as follows:

1. On the menu sidebar, under **SETTINGS**, click **Setup > General**, and then click the **Android** tab.
2. In the **Baidu Cloud Push service** section, select **Enable Baidu Cloud Push service**.
3. Click **Save**.

When Baidu Cloud Push is enabled, Sophos Mobile sends all push notifications through GCM and through Baidu Cloud Push.

### 9.5 Configure iOS settings

On the **iOS** tab of the **General settings** page, you configure settings that are specific to iOS devices.

1. On the menu sidebar, under **SETTINGS**, click **Setup > General**, and then click the **iOS** tab.
2. Configure the following settings:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activation Lock bypass</td>
<td>Select Enable to be able to clear the Activation Lock on supervised devices. When this option is selected, Sophos Mobile retrieves a bypass code when syncing with a supervised device that has Activation Lock enabled. If required, you can perform the Activation Lock bypass action from the device’s Show device page to clear Activation Lock when the device needs to be erased and re-deployed. Activation Lock is an iOS security feature to prevent the reactivation of lost or stolen devices. Normally, you need the correct Apple ID and password to clear Activation Lock. With the Activation Lock bypass feature, you can clear Activation Lock by providing the bypass code only.</td>
</tr>
<tr>
<td>Synchronize device name</td>
<td>Select Enable to manage iOS devices under the name that is configured on the device. When this option is selected, the device name that Sophos Mobile uses is set every time the device synchronizes with Sophos Mobile. When this option is deselected, you set the device name during device enrollment.</td>
</tr>
</tbody>
</table>

3. Click Save.

### 9.6 Configure polling interval for Windows devices

For Windows devices, you can configure the polling interval at which the Windows MDM client contacts the Sophos Mobile server. Usually, the server contacts the client using push notifications. Polling is used as a safety measure when the push notification service is not available.

**Note**
The default values are sufficient in most cases. Using shorter intervals impacts battery life and data consumption and causes higher server load.

1. On the menu sidebar, under SETTINGS, click Setup > General, and then click the Windows tab.
2. Select polling intervals for the different Windows operating systems. You can configure individual settings for:
   - Windows 10 Mobile and Windows Phone 8.1 devices
   - Windows 10 computers
3. Click Save.
9.7 Configure Email

On the Email configuration tab, you configure settings for emails that are sent by Sophos Mobile.

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

2. In Language, select the email language.

3. In Originator name, enter the name that appears as email originator.

4. Optional: Under Alert email settings, configure alert reports that are sent to administrators:
   a) In Severity, select the severity levels that are included in the report.
   b) In Email recipients, specify the recipients by entering one or more valid email addresses.
   c) In Email schedule, enter a time of the day when the report is sent out, and then click Add.

   Repeat this to send out more than one report per day.

   **Note**
   Times are in the server time zone.

5. Click Save.

Related concepts

Alerts (page 13)

9.8 Configure technical support contact details

To support users who have questions or problems, you can provide them with details of how to contact technical support. The information that you enter here is displayed in the Sophos Mobile Control app and in the Self Service Portal.

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

2. Enter the required information for the technical contact.

3. Click Save.

9.9 Define customer properties

You can define customer-level properties.

When you define a property with name `my_property`, you can refer to the value of the property in profiles and policies by using the placeholder `%_CUSTPROP(my_property)_%`. For example, you can use this to refer to a domain that is specific to the customer.

For details on profile and policy placeholders, see Placeholders in profiles and policies (page 81).

To define a customer property:

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

2. Click Add customer property.
3. Enter a name and a value for the new property.
4. Click **Apply** to add the property.
5. Click **Save** to save the changes to the customer settings.
10 Configure Self Service Portal

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

On the menu sidebar, you can configure settings for the use of the Self Service Portal, for example:

- The platforms for which devices can be enrolled.
- The available functions.
- The users that are allowed to access the Self Service Portal.

The Self Service Portal is available for the following platforms:

- Android
- iOS
- Windows Mobile
- Windows

10.1 Create Self Service Portal groups with internal user management

Self Service Portal configurations are applied to groups of Self Service Portal users. With internal user management, you can create Self Service Portal groups and assign users to them. For further information on user management, see Manage Self Service Portal users (page 26).

Note

Internal user management is only available for a customer if it has been activated by the super administrator. For further information, see the Sophos Mobile super administrator guide. This does not apply to Sophos Mobile as a Service. Super administrators are not supported in Sophos Mobile as a Service. For information on how to define the user management methods for Sophos Mobile as a Service, see Configure Self Service Portal user management (page 26).

To create a Self Service Portal group:

1. On the menu sidebar, under MANAGE, click Users. The Show users page is displayed.
2. Click Show user groups. The Show user groups page is displayed.
3. Click Create group. The Edit group page is displayed.
4. In the Name field, enter a name for the new Self Service Portal user group.
5. Click Save.

The new Self Service Portal user group is displayed on the Show user groups page. When you create new users, you can assign them to the group. When you define Self Service Portal settings, you can select the group to assign the settings to it.
10.2 Configure Self Service Portal settings

Note
The Self Service Portal settings are not available when you have turned off internal and external user management. See Configure Self Service Portal user management (page 26).

1. On the menu sidebar, under SETTINGS, click Setup, and then click Self Service Portal. The Self Service Portal page is displayed.

2. On the Configuration tab, configure the following settings:
   a) In the Maximum number of devices list, select the maximum number of devices a user can enroll in the Self Service Portal. This ensures that the number of available licenses is not exceeded.
   b) In the Device owner preselection list, select if new devices are classified as corporate or personal devices, and if the users are able to change this classification when they enroll their devices in the Self Service Portal. You can select one of the following settings:
      • no preselection: The user can choose between Corporate device and Personal device.
      • corporate preselected: Corporate device is preselected. The user can change this to Personal device.
      • corporate fixed: Corporate device is selected and can’t be changed by the user.
      • personal preselected: Personal device is preselected. The user can change this to Corporate device.
      • personal fixed: Personal device is selected and can’t be changed by the user.
   c) Under Available functionality, select the functions that should be available for users of the Self Service Portal. The functions supported vary according to the device platform. See Available Self Service Portal actions (page 23).

3. On the Terms of use tab, you configure a mobile policy, disclaimer or agreement text that is displayed as a first step when users enroll their devices. Users must accept the text to be able to continue.
   You may use HTML markup to format the text.

4. On the Post-install text tab, you configure text to be displayed in the Self Service Portal after device enrollment. For example, use this to describe post-enrollment tasks.
   You may use HTML markup to format the text.

5. On the Group settings tab, you configure the group settings, for example, the device groups enrolled devices will be added to and the task bundle that will be transferred to the devices.

Important
Because of the complexity of the group settings configuration, we recommend that you test device enrollment for different user groups before you roll out the settings to your actual users.

a) Click Add.
   The Edit group settings page is displayed.

b) In the Name field, enter a name for the Self Service Portal configuration group.

c) In the User group field, enter a user group that you have defined (for internal user management), or an LDAP directory group with the full LDAP path or with wildcards (for
external user management). You can use an asterisk (*) as the first, the last or the only character in this field to specify several groups. For example: Enter Dev* to specify all group names that start with the string Dev. Enter * to specify all available groups.

**Note**
The value * represents all groups, not all users. Users that are not a member of any group are not included.

d) Select **Show terms of use during registration** to display the terms of use text that you configured before as the first step of the enrollment procedure.

e) Select **Show post-install text during registration** to display the post-install text that you configured before as the last step of the enrollment procedure.

f) In columns **Initial package - corporate device** and **Initial package - personal device**, select the task bundle (for Android, iOS, and macOS) or policy (for Windows and Windows Mobile) to be executed on corporate and personal devices.

g) In column **Active**, select the platforms that should be available in the Self Service Portal. You must select an initial package before you can select a platform.

h) In column **Add to device group**, select the group the device should be added to. For information on device groups, see Device groups (page 76).

i) Click **Apply**.

6. The **Self Service Portal** page is displayed. Click **Save**.

**Note**
As a super administrator, you can also define the default customer for the Self Service Portal. For further information, see the Sophos Mobile super administrator guide. Note that this does not apply to Sophos Mobile as a Service. Super administrators are not supported in Sophos Mobile as a Service.

### 10.3 Available Self Service Portal actions

This section lists the Self Service Portal actions that are available for the individual platforms.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Locate device</strong></td>
<td>With this function users can locate devices if they are lost or stolen.</td>
<td>Android, iOS, Windows Mobile, Windows</td>
</tr>
<tr>
<td><strong>Lock device</strong></td>
<td>With this function users can lock their devices if they are lost or stolen.</td>
<td>Android, iOS, macOS, Windows Mobile</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
<td>Platforms</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td><strong>Reconfigure device</strong></td>
<td>With this function users can reconfigure their devices if Sophos Mobile has been removed from the device, but the device is still enrolled.</td>
<td>Android</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iOS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>macOS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Mobile</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows</td>
</tr>
<tr>
<td><strong>Show compliance violations</strong></td>
<td>With this function users can view the compliance violations for their devices.</td>
<td>Android</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iOS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>macOS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Mobile</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows</td>
</tr>
<tr>
<td><strong>Refresh data</strong></td>
<td>With this function users can manually synchronize their devices with the Sophos Mobile server. This is useful, for example, if the device has been switched off for a long period of time and therefore has not been synchronized with the server. In this case, the device may be non-compliant and needs to be synchronized with the server to make it compliant again.</td>
<td>Android</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iOS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>macOS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Mobile</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This function is not available for devices on which Sophos Mobile only manages the Sophos container.</td>
<td></td>
</tr>
<tr>
<td><strong>Reset password</strong></td>
<td>With this function users can reset their lock screen password. For Android and iOS devices, a temporary password is displayed in the Self Service portal. The device can only be unlocked with this password. After unlocking their devices, users can set a new password. For iOS, the password is completely deleted. The user has to set a new password within 60 minutes.</td>
<td>Android</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iOS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Mobile</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
<td>Platforms</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td><strong>Wipe</strong></td>
<td>With this function users can reset their enrolled devices to their factory settings if devices are lost or stolen. All data on the device is deleted.</td>
<td>Android, iOS, macOS, Windows Mobile, Windows</td>
</tr>
<tr>
<td><strong>Wipe Android work profile</strong></td>
<td>With this function users can remove the work profile from their devices. This also unenrolls the devices from Sophos Mobile.</td>
<td>Android</td>
</tr>
<tr>
<td><strong>Unenroll device</strong></td>
<td>With this function users can decommission devices that they no longer use. This is useful, for example, if the number of devices users can enroll in the Self Service Portal is limited or users get new devices.</td>
<td>Android, iOS, macOS, Windows Mobile, Windows</td>
</tr>
<tr>
<td><strong>Delete unmanaged device</strong></td>
<td>With this function users can delete decommissioned devices.</td>
<td>Android, iOS, macOS, Windows Mobile, Windows</td>
</tr>
<tr>
<td><strong>Reset App Protection password</strong></td>
<td>With this function users can reset their App Protection password on Android devices. The App Protection password protects defined apps and has to be entered each time users start these apps. The password will be deleted and they have to set a new one.</td>
<td>Android</td>
</tr>
<tr>
<td><strong>Reset Sophos container password</strong></td>
<td>With this function users can reset their Sophos container password. The Sophos container password has to be entered each time users start one of the container apps. The password will be deleted and they have to set a new one.</td>
<td>Android, iOS</td>
</tr>
<tr>
<td><strong>Reconfigure the SMC app</strong></td>
<td>With this function users can reconfigure an already installed Sophos Mobile Control app.</td>
<td>iOS, Windows Mobile</td>
</tr>
<tr>
<td><strong>Managed Lost Mode</strong></td>
<td>Users can turn Managed Lost Mode on or off.</td>
<td>iOS</td>
</tr>
</tbody>
</table>
Sophos Mobile on Premise

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Play Lost Mode sound</td>
<td>Users can play a sound on their device in Managed Lost Mode.</td>
<td>iOS</td>
</tr>
</tbody>
</table>

Related tasks
Configure Self Service Portal settings [page 22]

10.4 Manage Self Service Portal users

Sophos Mobile offers different methods for managing Self Service Portal users:

- **Internal user management**: With internal user management you can create users by adding them manually to Sophos Mobile or by importing them from a comma-separated values (CSV) file.
- **External user management**: With external user management you can assign devices to groups and profiles based on external directory membership.

The user management method is customer-specific. For Sophos Mobile on Premise, it is defined by the super administrator when a customer is created. For Sophos Mobile as a Service, you must define it before adding users. See Configure Self Service Portal user management [page 26].

10.4.1 Configure Self Service Portal user management

**Note**
For Sophos Mobile on Premise, user management for the Self Service Portal is configured by the super administrator when a customer is created. See the Sophos Mobile super administrator guide.

1. On the menu sidebar, under **SETTINGS**, click **Setup**, and then click **System setup**. The **System setup** page is displayed.

2. Go to the **User setup** tab. On this tab, select the data source for the Self Service Portal (SSP) users to be managed by Sophos Mobile:
   - Select **None. No SSP, user-specific profiles, or LDAP administrators available.** to turn off user management.
   - Select **Internal directory** to use internal user management for Self Service Portal users.
   - Select **External LDAP directory** to use external user management for Self Service Portal users.
     - Click **Configure external LDAP** to specify the server details. See Configure external directory connection [page 27].

3. Click **Save**.
   If you have selected **Internal directory** or **External LDAP directory**, the selected option and the option **None. No SSP, user-specific profiles, or LDAP administrators available.** are displayed on the **User setup** tab. If you want to change your selection afterward, select **None. No SSP, user-specific profiles, or LDAP administrators available** first to make all options available.
Note
The user management configuration cannot be changed as long as there are any devices linked to the directory. If you try to change the configuration while devices are still connected, an error message is displayed.

10.4.2 Configure external directory connection

When you use an external LDAP directory for managing user accounts for Sophos Mobile Admin and the Self Service Portal, you must configure the directory connection so that Sophos Mobile can retrieve the user data from the LDAP server. For Sophos Mobile on Premise, this is done by the super administrator when the customer is created.

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 SETTNGS, click Setup > System setup, and then click the User setup tab.
2. Select External LDAP directory.
3. Click Configure external LDAP to specify the server details.
4. On the Server details page, configure the following settings:
   a) In the LDAP type field, select the LDAP server type:
      - Active Directory
      - IBM Domino
      - NetIQ eDirectory
      - Red Hat Directory Server
      - Zimbra
   b) In the Primary URL field, enter the URL of the primary directory server. You can enter the server IP or the server name. Select SSL/TLS to secure the server connection by SSL or TLS (depending on what the server supports). For Sophos Mobile as a Service, SSL/TLS cannot be deselected.
   c) Optional: In the Secondary URL field, enter the URL of a directory server that is used as fallback in case the primary server cannot be reached. You can enter the server IP or the server name. Select SSL/TLS to secure the server connection by SSL or TLS (depending on what the server supports). For Sophos Mobile as a Service, SSL/TLS cannot be deselected.
   d) In the User field, enter an account for lookup operations on the directory server. Sophos Mobile uses the account credentials when it connects to the directory server.

For Active Directory, you also need to enter the relevant domain. Supported formats are:
   - <domain>\<user name>
   - <user name>@<domain>.<domain code>
Note
For security reasons, we recommend you specify a user that only has read permissions for the directory server and not write permissions.

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

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 external directory from which the search for a user or user group begins.

6. On the **Search fields** page, define which directory fields are to be used for resolving the \$_USERNAME_\$ and \$_EMAILADDRESS_\$ placeholders in profiles and policies. Type the required field names or select them from the **User name** and **Email** lists.

Note
The lists only contain fields that are configured for the user that is currently connected to the LDAP directory, specified in step 4.d (page 27) earlier in this description. If, for example, an email field was not configured for that user, you need to manually enter the required value in the **Email** field.

In the case of Active Directory, these field mappings apply:

- **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 an asterisk *, members of all LDAP directory groups are allowed to log in to the Self Service Portal.

Note
The value * represents all groups, not all users. Users that are not a member of any LDAP directory group are not included.

- 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 **Resolve 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.
8. Click **Apply**.
9. On the **User setup** tab, click **Save**.

### 10.4.3 Create Self Service Portal users

This section only applies to internal user management, i.e. when you don’t use an LDAP directory for managing user accounts.

For information on how to configure user management for Sophos Mobile on Premise, see the [Sophos Mobile super administrator guide](#).

For information on how to configure user management for Sophos Mobile as a Service, see [Configure Self Service Portal user management](#) (page 26).

To create a user account for the Self Service Portal:

1. On the menu sidebar, under **MANAGE**, click **Users**. The **Show users** page is displayed.
2. Click **Create user**. The **Edit user** page is displayed.
3. Select the **Send registration email** check box.
4. Enter the following information:
   a) **User name**
   b) **First name**
   c) **Last name**
   d) **Email address**
   e) **Groups** (optional)

   **Note**
   The **User name** field must only contain letters (Latin alphabet), digits, spaces and the characters `\ ! \_ \- \#`.

5. Click **Save**.

   The new Self Service Portal user is displayed on the **Show users** page. A registration email is sent to the new user.

   If you click the blue triangle next to the required user, you can view the user details (**Show**), **Edit** or **Delete** the user.
10.4.4 Import Self Service Portal users

This section only applies to internal user management, i.e. when you don’t use an LDAP directory for managing user accounts.

For information on how to configure user management for Sophos Mobile on Premise, see the Sophos Mobile super administrator guide.

For information on how to configure user management for Sophos Mobile as a Service, see Configure Self Service Portal user management (page 26).

You can add new Self Service Portal users by importing a UTF-8 encoded comma-separated values (CSV) file with up to 500 users.

Note
Use a text editor for editing the CSV file. If you use Microsoft Excel, values entered may not be resolved correctly. Make sure that you save the file with extension .csv.

Tip
A sample file with the correct column names and column order is available for download from the Import users page.

To import users from a CSV file:
1. On the menu sidebar, under MANAGE, click Users, and then click Import users.
2. On the Import users page, select Send registration emails.
3. Click Upload a file and then navigate to the CSV file that you have prepared. The entries are read in from the file and are displayed.
4. 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.
5. Click Finish to create the user accounts.

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

10.4.5 View user details

1. On the menu sidebar, under MANAGE, click Users.
   The Show users page is displayed, showing all user accounts for the Self Service Portal.
2. Click the blue triangle next to the user whose details you want to display and then click Show.
   The account details and the devices the user is assigned to are displayed.
For internal user management, i.e. when you don’t use an LDAP directory for managing user accounts, you can click Edit to edit the account details.
11 System setup

On the System setup page you can perform the following tasks:

- **License**
  - Check your licenses [page 32]
- **APNs**
  - Create an APNs certificate [page 33]
  - Renew an APNs certificate [page 34]
  - Copy an APNs certificate to another customer [page 35]
- **iOS AirPlay**
  - Configure iOS AirPlay destinations [page 37]
- **Android enterprise**
  - Set up Android enterprise - Overview [page 265]
- **Apple VPP**
  - Set up a VPP sToken [page 255]
  - Automatically assign VPP apps [page 257]
  - Synchronize VPP license information [page 259]
- **Apple DEP**
  - Set up Apple DEP [page 68]
- **Apple DEP profiles**
  - Create DEP profile [page 69]
- **Samsung Knox license**
  - Register Samsung Knox license [page 37]
- **SCEP**
  - Configure SCEP [page 38]
- **User setup**
  - Configure user setup [page 38]
- **SGN**
  - Enable corporate keyring synchronization [page 290]

11.1 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.

To check your available licenses:
1. On the menu sidebar, under SETTINGS, click Setup > System setup.
2. On the System setup page, 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.
If the super administrator did not set a quota for the customer, the number of licenses is limited by the overall number for the Sophos Mobile server.

- **Used licenses**: Number of licenses in use.
- **Valid until**: The license expiration date.
- **Advanced license**: The super administrator has activated a Mobile Advanced license for the customer.

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

### 11.2 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.

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

#### 11.2.1 Requirements

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

- The Sophos Mobile server needs to connect to `gateway.push.apple.com:2195` TCP (17.0.0.0/8)
- Each iOS device with Wi-Fi only access needs to connect to `*.push.apple.com:5223` TCP (17.0.0.0/8)

#### 11.2.2 Create an APNs certificate

This procedure assumes that you have not uploaded a certificate for the Apple Push Notification service (APNs) to Sophos Mobile yet.

To renew an existing certificate, see [Renew an APNs certificate](#) (page 34).

**Tip**

You can use the same certificate for several customers. See [Copy an APNs certificate to another customer](#) (page 35).

1. On the menu sidebar, under **SETTINGS**, click **Setup > System setup** and then click the **APNs** tab. The description on that tab guides you through the steps you have to perform to request a certificate from Apple and to upload it to Sophos Mobile.
2. In the **Download certificate signing request** step, click **Download certificate signing request**. This saves the certificate signing request file `apple.csr` to your local computer. The signing request file is specific to the current customer.
3. You need an Apple ID. Even if you already have an ID, we recommend that you create a new one for use with Sophos Mobile. In the **Create Apple ID** step, click **Create a new Apple ID**. This opens an Apple web page where you can create an Apple ID for your company.
4. For your reference, enter your new Apple ID in the **Apple ID** field on the top of the **APNs** tab. When you renew the certificate each year, you must always use that same Apple ID.

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

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

7. Download the `.pem` APNs certificate file and save it to your computer.

8. In the **Upload APNs certificate** step, click **Upload certificate** and then browse for the `.pem` file that you received from the Apple Push Certificates Portal.

9. Click **Save** to add the APNs certificate to Sophos Mobile.

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

### 11.2.3 Renew an APNs certificate

This procedure assumes that you already have uploaded a certificate for the Apple Push Notification service (APNs) to Sophos Mobile that is about to expire and needs to be renewed.

To create and upload a new certificate, see [Create an APNs certificate](#) (page 33).

**Important**

In the Apple portal, it is important that you select the correct APNs certificate for renewal. If you renew the wrong certificate, you might need to re-enroll all iOS and macOS devices.

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

2. In the **Download certificate signing request** step, click **Download certificate signing request**. This saves the certificate signing request file `apple.csr` to your local computer.

3. Skip the step **Create Apple ID**. This step is only required if you are creating an APNs certificate for Sophos Mobile for the first time.

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

5. Log in with your Apple ID. This must be the same ID that you used for the creation of the initial APNs certificate.

6. In the Apple Push Certificates Portal, click **Renew** next to your Sophos Mobile APNs certificate.

7. Upload the certificate signing request file `apple.csr` you prepared before.

8. Download the `.pem` APNs certificate file and save it to your computer.

9. In the **Upload APNs certificate** step, click **Upload certificate** and then browse for the `.pem` file that you received from the Apple Push Certificates Portal.

10. Click **Save**.

11. When you are logged in as super administrator, there is an additional dialog that lists all customers that currently use the same APNs certificate as the super administrator customer, that is a certificate with the same **Topic** attribute.
• Click **Save for all customers concerned** to renew the APNs certificate for all of these customers.
• Click **Save only for super administrator customer** to renew the APNs certificate only for the super administrator customer.

**Important**
If the following message is shown, you are not renewing the correct certificate:

The topic of the new certificate does not correspond to the old one. If devices have been set up with the previous certificate, they have to be set up again. Do you really want to save your changes?

This message indicates that you are about to create a new APNs certificate with a different identifier. If you confirm the message, all existing iOS and macOS devices are not manageable any more and you have to re-enroll them.

For information on how to select the correct certificate, see Identify the correct APNs certificate for renewal (page 36).

### 11.2.4 Copy an APNs certificate to another customer

You can copy a certificate for the Apple Push Notification service (APNs) to another customer within the same or a different installation of Sophos Mobile.

**Important**
If there already exists an APNs certificate at the target location, it is important that the **Topic** property of the certificate that you want to copy is identical to the **Topic** of the existing certificate. If you copy the wrong certificate, you might need to re-enroll all iOS and macOS devices of the customer.

Download the certificate from the source location:

1. Log in to Sophos Mobile Admin as an administrator of the customer whose APNs certificate you want to copy.
2. On the menu sidebar, under **Settings**, click **Setup > System setup** and then click the **APNs** tab.
3. Make a note of the **Topic** value that is displayed in the certificate details.
4. Click **Download certificate as PKCS #12 file**.
5. In the confirmation dialog, the password for the certificate file is displayed. Make a note of that password and then click **Download**.
   
   This saves the certificate file `apns_cert.p12` to your local computer.

Upload the certificate to the target location:

6. Log in to Sophos Mobile Admin as an administrator of the customer to whom you want to upload the certificate.
7. On the menu sidebar, under **Settings**, click **Setup > System setup** and then click the **APNs** tab.
8. If there already exists an APNs certificate, verify that the **Topic** value is identical to the value of the certificate you are about to copy.
9. In the **Upload APNs certificate** step, click **Upload certificate** and then browse for the `apns_cert.p12` file that you downloaded before.
10. Enter the password and then click **Apply**.
11. Click **Save**.
11.2.5 Identify the correct APNs certificate for renewal

When you renew your Apple Push Notification service (APNs) certificate for the Sophos Mobile server as described in Renew an APNs certificate (page 34), it is important that on the Apple portal you select the correct APNs certificate for renewal.

This section describes how to identify the APNs certificate that is currently uploaded to the Sophos Mobile server.

Retrieve the certificate identifier:

1. Log in to Sophos Mobile Admin with an administrator account for the customer whose APNs certificate needs to be renewed.
2. On the menu sidebar, under SETTINGS, click Setup > System setup and then click the APNs tab.
3. In section Content of the Apple Push Notification keystore, the properties of the uploaded APNs certificate are displayed.
4. Make a note of the value that is displayed for Topic.
   This is the identifier of your APNs certificate.

Identify the certificate:

   If you are experiencing issues with certain features of the Apple portal when using Microsoft Internet Explorer, we recommend that you use the latest version of the Firefox, Opera, Chrome or Safari browser instead.
6. Log in with the Apple ID that you used for the creation of the initial APNs certificate.
7. In the list of APNs certificates, click the Certificate Info icon next to a certificate entry.
   This displays the certificate details.
8. In the Subject DN field, locate the value that follows the string UID=. If this matches the identifier that you determined in Sophos Mobile Admin, you have identified the correct certificate.

11.2.6 Check APNs connectivity of devices

Users of the Sophos Mobile Control app for iOS can check if their devices are able to connect to the Apple Push Notification service (APNs) server.

1. In the Sophos Mobile Control app, tap the Information icon to open the About screen.
2. Tap Check APNs.

The app tries to connect to the Apple APNs server. The expected server response time is 5 seconds or less.

If the app notifies you that the APNs server could be reached, the device is able to receive commands from Sophos Mobile server through APNs.

If the app notifies you that the APNs server could not be reached, your network does not allow APNs communication and thus Sophos Mobile is not able to manage iOS devices. To correct this, make sure that the requirements described in Requirements (page 33) are met.
11.3 Configure iOS AirPlay destinations

With Sophos Mobile you can remotely trigger AirPlay mirroring between an iOS device and predefined AirPlay destinations (for example AppleTV).

**Note**
AirPlay only works for devices within the same network.

You can define destinations for AirPlay mirroring.

1. On the menu sidebar, under **SETTINGS**, click **Setup** and then **System setup**, and go to the **iOS AirPlay** tab.
2. In the **AirPlay destinations** section, click **Create AirPlay destination**. The **AirPlay destination** page is displayed.
3. Enter the device name and, optionally, the MAC address of the AirPlay destination device. If required, enter the password of the device.
4. Click **Apply**. The device is shown under **AirPlay destinations** in the **iOS AirPlay** tab of the **System setup** page.
5. Click **Save**.

You can trigger AirPlay mirroring between an iOS device and this destination by clicking **Request AirPlay mirroring** from the **Actions** menu on the **Show device** page for the relevant device.

11.4 Register Samsung Knox license

If your company has purchased a Samsung Knox Premium license, you have to enter your license key, the number of licenses and the expiration date on the **Samsung Knox license** tab in order to manage the Knox container on your Samsung Knox devices with Sophos Mobile.

11.5 Simple Certificate Enrollment Protocol (SCEP)

You can configure Simple Certificate Enrollment Protocol (SCEP) to provide certificates. This allows devices to obtain certificates from a Certificate Authority by using SCEP.

You can configure all the settings required to access a Certificate Authority server with SCEP in Sophos Mobile Admin.

You define the settings required for devices in an **SCEP** configuration of a device profile (Android and iOS) or a policy (Windows Mobile).

11.5.1 Prerequisites

In order to use the Simple Certificate Enrollment Protocol, the following prerequisites must be fulfilled:
• An SCEP-enabled Windows CA exists in the environment.
• Login credentials for a user who can create a challenge code are available.
• The Sophos Mobile server has http or https access to the following sites:
  — https://YOUR-SCEP-SERVER/CertSrv/MSCEP_ADMIN
  — https://YOUR-SCEP-SERVER/CertSrv/MSCEP

11.5.2 Configure SCEP

1. On the menu sidebar, under SETTINGS, click Setup > System setup, and go to the SCEP tab.
2. Specify the following:
   a) In the SCEP server URL field, enter https://YOUR-SCEP-SERVER/CertSrv/MSCEP.
   b) In the Challenge URL field, enter https://YOUR-SCEP-SERVER/CertSrv/MSCEP_ADMIN.

   Note
   If you use a Windows 2003 server as the SCEP server, enter https://YOUR-SCEP-SERVER/CertSrv/MSCEP.

   c) In the User and Password fields, enter the user credentials of the user who can create a challenge code.

   Note
   In the User field, enter a user who has the necessary rights to enroll certificates. Use the logon format: username@domain

   d) In the Challenge characters field, select the character types that are used for the challenge password.
   e) In the Challenge length field, accept the default length.
   f) Optional: Clear the Use HTTP proxy option if you want Sophos Mobile to bypass the HTTP proxy when connecting to the SCEP server. This option is only available if the HTTP proxy is enabled.

   For Sophos Mobile on Premise, the super administrator can configure an HTTP proxy that Sophos Mobile uses for outbound HTTP and SSL/TLS connections. See the Sophos Mobile super administrator guide.

   For Sophos Mobile as a Service, the HTTP proxy is always enabled.
3. Click Save.
   Sophos Mobile tests the connection to your SCEP server.

   To deploy a profile using SCEP, you must add a SCEP configuration to an Android or iOS device profile or to a Windows Mobile policy.

11.6 Configure user setup

On the User setup tab you can change the user management settings. For further information, see Manage Self Service Portal users (page 26) and the Sophos Mobile super administrator guide.
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.

**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:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deny email</strong></td>
<td>Forbid email access. This action can only be taken if the super administrator has configured a connection to the internal or to the standalone EAS proxy. See the Sophos Mobile super administrator guide. This action is only available for Android, iOS, Windows and Windows Mobile devices.</td>
</tr>
<tr>
<td><strong>Lock container</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Deny network</strong></td>
<td>Forbid network access. This action can only be taken if the super administrator has configured Network Access Control. See the Sophos Mobile super administrator guide.</td>
</tr>
<tr>
<td><strong>Create alert</strong></td>
<td>Create an alert. The alerts are displayed on the Alerts page.</td>
</tr>
<tr>
<td><strong>Transfer task bundle</strong></td>
<td>Transfer a specific task bundle to the device. Select a task bundle from the list, or select None to transfer no task bundle when the compliance rule is violated. This action is only available for Android, iOS, macOS and Windows devices.</td>
</tr>
</tbody>
</table>

**Important**
When used incorrectly, task bundles may misconfigure or even wipe devices. To assign the correct task bundles to compliance rules, an in-depth knowledge of the system is required.

7. When you have made the settings for all required platforms, click **Save** to save the compliance policy under the name that you specified. The new compliance policy is displayed on the Compliance policies page.
## 12.2 Available compliance rules

This section lists the compliance rules that you can select for the individual platforms.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Managed required</strong></td>
<td>Define the action that will be executed when a device is no longer managed.</td>
<td>Android, Android Things, iOS, macOS, Windows Mobile, Windows, Windows IoT</td>
</tr>
<tr>
<td><strong>Minimum SMC app version</strong></td>
<td>Enter the minimum Sophos Mobile Control app version that has to be installed onto the device.</td>
<td>Android, Android Things, iOS, Windows Mobile</td>
</tr>
<tr>
<td><strong>Root access allowed</strong></td>
<td>Select whether devices with root rights are allowed.</td>
<td>Android</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>&lt;br&gt;For Sony devices with Enterprise API version 4 or above and for Samsung devices with Knox version 5.5 or below, this includes all devices that are classified <em>insecure</em> by the MDM API, for example because the bootloader is unlocked.</td>
<td></td>
</tr>
<tr>
<td><strong>Apps from unknown sources allowed</strong></td>
<td>Select whether apps from unknown sources are allowed.</td>
<td>Android</td>
</tr>
<tr>
<td></td>
<td>This rule only affects devices with Android 7.x or earlier. With Android 8, the system setting to restrict app installation sources was removed.</td>
<td></td>
</tr>
<tr>
<td><strong>Android Debug Bridge (ADB) allowed</strong></td>
<td>Select whether ADB (Android Debug Bridge) is allowed.</td>
<td>Android</td>
</tr>
<tr>
<td><strong>Allow jailbreak</strong></td>
<td>Select whether jailbroken devices are allowed.</td>
<td>iOS</td>
</tr>
<tr>
<td>Rule</td>
<td>Description</td>
<td>Platforms</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td><strong>Screen lock required</strong></td>
<td>Select whether a device password or other screen lock mechanism (like pattern or PIN) is required. For Android, this includes the display lock types <em>Pattern</em>, <em>PIN</em> and <em>Password</em>, but not <em>Swipe</em>. Windows Mobile devices that have no password policy assigned are always reported as non-compliant. This is a Windows limitation.</td>
<td>Android</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iOS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Mobile</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows</td>
</tr>
<tr>
<td><strong>Min. OS version</strong></td>
<td>Select the earliest operating system version required.</td>
<td>Android</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Android Things</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iOS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>macOS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Mobile</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows IoT</td>
</tr>
<tr>
<td><strong>Max. OS version</strong></td>
<td>Select the latest operating system version allowed.</td>
<td>Android</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Android Things</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iOS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>macOS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Mobile</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows IoT</td>
</tr>
<tr>
<td><strong>Mandatory OS updates</strong></td>
<td>Select if devices must have the latest available or the latest required update installed. Some iOS updates are classified as <em>required</em> by Apple. The latest available update might be newer than the latest required update.</td>
<td>iOS</td>
</tr>
<tr>
<td><strong>Max. synchronization gap</strong></td>
<td>Specify the maximum interval between synchronization processes for devices.</td>
<td>Android</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Android Things</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iOS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>macOS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Mobile</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows IoT</td>
</tr>
<tr>
<td>Rule</td>
<td>Description</td>
<td>Platforms</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td><strong>Maximum SMC app synchronization interval</strong></td>
<td>Specify the maximum interval between app synchronization processes for devices.</td>
<td>iOS, Windows Mobile</td>
</tr>
<tr>
<td><strong>Max. SMSec scan interval</strong></td>
<td>Specify the maximum scan interval for malware scans performed by the Sophos Mobile Security app on the device.</td>
<td>Android</td>
</tr>
<tr>
<td><strong>Denial of SMSec permissions allowed</strong></td>
<td>Sophos Mobile Security needs permissions on the device to work properly. The user has to grant these permissions when the app is installed. Select whether a denial of the required permissions results in a compliance violation.</td>
<td>Android</td>
</tr>
<tr>
<td><strong>Malware apps allowed</strong></td>
<td>Select whether malware apps that have been detected by Sophos Mobile Security are allowed.</td>
<td>Android</td>
</tr>
<tr>
<td><strong>Suspicious apps allowed</strong></td>
<td>Select whether suspicious apps that have been detected by Sophos Mobile Security are allowed.</td>
<td>Android</td>
</tr>
<tr>
<td><strong>PUAs allowed</strong></td>
<td>Select whether PUAs (Potentially Unwanted Apps) that have been detected by Sophos Mobile Security are allowed.</td>
<td>Android</td>
</tr>
<tr>
<td><strong>Encryption required</strong></td>
<td>Select whether encryption is required for devices. On devices with Android 5 or higher, users must additionally enable the <strong>Require PIN to start device</strong> or <strong>Require Password to start device</strong> setting when they set a screen lock. See Sophos knowledgebase article 123947. For macOS, this setting applies to FileVault full-disk encryption. For Windows Mobile, a violation is only reported if the restriction <strong>Forbid unencrypted device</strong> is set as well. This is a Windows limitation.</td>
<td>Android, iOS, macOS, Windows Mobile, Windows</td>
</tr>
<tr>
<td><strong>Data roaming allowed</strong></td>
<td>Select whether data roaming is allowed for devices.</td>
<td>Android, iOS</td>
</tr>
<tr>
<td>Rule</td>
<td>Description</td>
<td>Platforms</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Container configured</td>
<td>Select whether a container must be set up and enabled on the device. This can be a Sophos container, a Samsung Knox container or an Android work profile.</td>
<td>Android</td>
</tr>
<tr>
<td>Locate permission required</td>
<td>This setting refers to the <strong>Locate</strong> function. Select whether the user has to allow the Sophos Mobile Control app at installation time to retrieve location data in order to be compliant.</td>
<td>Android</td>
</tr>
<tr>
<td>Denial of SMC permissions allowed</td>
<td>The Sophos Mobile Control app needs permissions on the device to work properly. The user has to grant these permissions when the app is installed. Select whether a denial of the required permissions results in a compliance violation.</td>
<td>Android</td>
</tr>
<tr>
<td>App is able to locate</td>
<td>Location services must be turned on and the Sophos Mobile Control app must be allowed to use them. For Windows Mobile, this rule only affects Windows Phone 8.1 devices.</td>
<td>iOS</td>
</tr>
<tr>
<td>Firewall required</td>
<td>The macOS firewall must be turned on.</td>
<td>macOS</td>
</tr>
<tr>
<td>System Integrity Protection required</td>
<td>System Integrity Protection must be turned on.</td>
<td>macOS</td>
</tr>
<tr>
<td>Note</td>
<td>System Integrity Protection is a macOS security feature that limits the actions the root user can perform. System Integrity Protection can be configured when the Mac starts up from macOS Recovery.</td>
<td></td>
</tr>
<tr>
<td>Security updates required</td>
<td>Automatic installation of macOS security updates must be turned on.</td>
<td>macOS</td>
</tr>
</tbody>
</table>
**12.3 Assign a compliance policy to device groups**

1. On the menu sidebar, under **MANAGE**, click **Device groups**.
   The **Device groups** page is displayed.
2. Click the blue triangle next to the device group you want to assign a compliance policy to and then click **Edit**.
   There is always a **Default** device group available. For information on how to create your own device groups, see **Create device group** (page 76).
3. Under **Compliance policies**, select the compliance policies you want to apply to corporate and to personal devices.
4. Click **Save**.
The selected compliance policies are shown on the Device groups page for the relevant device group under Compliance policy (corporate) and Compliance policy (personal).

12.4 Check devices for compliance

After you have configured compliance policies, you can check if enrolled devices comply with these policies.
1. On the menu sidebar, under CONFIGURE, click Compliance policies.
2. Click Check now.

All enrolled devices are checked for compliance. The specified actions are carried out.
13 Devices

13.1 Add devices

Devices can be added to Sophos Mobile in the following ways:

- Add devices manually. See Add device (page 47).
- Import devices from a comma-separated values (CSV) file. See Import devices (page 48).
- Use the device enrollment wizard to add a device to Sophos Mobile, assign it to a user, enroll it, and transfer an enrollment task bundle. See Use the device enrollment wizard to assign and enroll new devices (page 50).
- Enable users to enroll devices on their own in the Self Service Portal. See Configure Self Service Portal (page 21). This portal reduces IT effort by allowing users to carry out tasks without contacting the helpdesk. The devices are provisioned by executing defined task bundles. See Task bundles (page 233).

We recommend that you use device groups to group devices for easier administration. See Device groups (page 76).

13.1.1 Add device

We recommend that you create one or more device groups before adding your first device to Sophos Mobile. You can then assign each device to a device group, to simplify device management. See Create device group (page 76).

To add a new device to Sophos Mobile:

1. On the menu sidebar, under MANAGE, click Devices. The Devices page is displayed.
2. Click Add and then select the platform from the Add device manually menu section. The Edit device page is displayed.
3. On the Edit device page, specify the following device details:
   a) In the Name field, enter a unique name for the new device.
   b) In the Description field, enter a description for the new device.
   c) Under Owner, select Corporate or Personal.
   d) In the Email address field enter an email address.
   e) In the Phone number field, enter the phone number of the new device. Enter the phone number in international format, for example +491701234567.
   f) Under Device group, select the device group the device is to be assigned to.
      For information on how to create device groups, see Create device group (page 76).
4. To assign a user to the device, click the Edit user assignment icon next to the User field and then click Assign user to device. For further information, see Assign a user to a device (page 60).
5. To add custom properties to the device, go to the Custom properties tab and click Add custom property. For further information, see Define custom properties for devices (page 61).
6. After you have specified all relevant device details, click Save.
The new device is added to Sophos Mobile and displayed on the Devices page under MANAGE. You can now provision and manage the device.

Note
For iOS devices, when you have configured Sophos Mobile to synchronize the device name with the device as described in Configure iOS settings (page 17), the name you entered in the Name field is replaced by the name set during synchronization.

13.1.2 Import devices

You can add new devices by importing a UTF-8 encoded comma-separated values (CSV) file with up to 500 devices.

Note
Use a text editor for editing the CSV file. If you use Microsoft Excel, values entered may not be resolved correctly. Make sure that you save the file with extension .csv.

Note
The users that are specified in your CSV file must already be available in Sophos Mobile.

Tip
A sample file with the correct column names and column order is available for download from the Import devices page.

To import devices from a CSV file:
1. On the menu sidebar, under MANAGE, click Devices.
3. On the Import devices page, click Upload a file and then navigate to the CSV file that you have prepared.
   The entries are read in from the file and are displayed.
4. 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.
5. Click Finish to create the devices.

The devices listed in the CSV file are imported and displayed on the Devices page. You can now enroll and configure the devices.

13.2 Enroll devices

After you have added new devices in Sophos Mobile Admin, they must be enrolled with Sophos Mobile.
Enrollment types

Sophos Mobile supports two enrollment types:

Device enrollment

This enrollment type provides full Mobile Device Management (MDM) capabilities. Sophos Mobile is able to manage the whole device.

Sophos container enrollment

Sophos Mobile only manages the Sophos container on the device, but not the device itself. The Sophos container is available for Android and iOS only.

Sophos container enrollment is useful in the following situations:

• You want to manage Bring Your Own Device (BYOD) scenarios. With Sophos container enrollment, your organization can only see very limited device information, and no personal apps or data.
• Your devices are managed by a non-Sophos MDM software, but you also want to use features provided by the Sophos container, for example corporate keyring synchronization with Sophos SafeGuard Enterprise.
• Your devices are managed by a non-Sophos MDM software, but you want to configure additional email accounts. For example when you are a consultant company and your employees need to access your customers’ Exchange servers.

Enrollment methods

The following options are available to enroll devices:

• You can enroll individual, unmanaged devices using the Devices function. For further information, see Enroll individual devices (page 50).
• You can use the device enrollment wizard to add a device to Sophos Mobile, assign it to a user, enroll it, and transfer an enrollment task bundle. See Use the device enrollment wizard to assign and enroll new devices (page 50).

Note

If required, you can use the device enrollment wizard or the auto-enrollment method to enroll iOS devices without Apple ID. This can be useful, for example to preconfigure the device before handing it over to a user. See Enroll iOS devices without Apple ID (page 53).
Recommendations

To enroll and configure multiple devices efficiently, the following methods are recommended:

- You can bundle the tasks that are necessary to enroll devices, apply required policies and install required apps (for example, managed apps for iOS devices). For further information, see Task bundles (page 233).
- You can enable users to enroll devices in the Self Service Portal. To do so, include a task bundle for enrollment when configuring the settings for Self Service Portal use. For further information on how to create the task bundles required for enrollment, see the Sophos Mobile startup guide or the Sophos Mobile as a Service startup guide. For further information on how to select the task bundle in the Self Service Portal settings, see Configure Self Service Portal settings (page 22).

13.2.1 Enroll individual devices

1. On the menu sidebar, under MANAGE, click Devices and then click the device that you want to enroll.
2. On the Show device page, select an enrollment type:
   - To enroll the device with Sophos Mobile, click Actions > Enroll.
   - To enroll the Sophos container, click Actions > Enroll Sophos container.
3. For Sophos container enrollment, select a task bundle or policy.

The enrollment task is started and displayed on the Task view page. An email with enrollment instructions is sent to the user.

**Note**

On Macs, the enrollment procedure must be performed by the user that will be managed by Sophos Mobile. To install the enrollment profile, the user must enter an administrator password.

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

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

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

To start the device enrollment wizard:

1. On the menu sidebar, under MANAGE, click Devices, and then click Add > Enrollment wizard.
Tip
Alternatively, you can start the wizard from the Dashboard page by clicking the Add device widget.

2. On the Enter user search parameters wizard page, you can 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. After you have entered search criteria, the wizard displays a list of matching users. Select the required user.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform</td>
<td>The device platform. You can only select a platform that is enabled for the customer that you logged in to.</td>
</tr>
<tr>
<td>Name</td>
<td>A unique name under which the device will be managed by Sophos Mobile.</td>
</tr>
<tr>
<td>Description</td>
<td>An optional description of the device.</td>
</tr>
<tr>
<td>Phone number</td>
<td>An optional phone number. Enter the number in international format, for example +491701234567.</td>
</tr>
<tr>
<td>Email address</td>
<td>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.</td>
</tr>
<tr>
<td>Owner</td>
<td>Select the device owner type: either Corporate or Personal.</td>
</tr>
<tr>
<td>Device group</td>
<td>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.</td>
</tr>
</tbody>
</table>

5. If you have configured Sophos container enrollment, select whether you want to enroll the device or only the Sophos container. See Configure Sophos container enrollment (page 287).

6. Select a task bundle that will be transferred to the device after it has been enrolled. Or select Only enroll device to enroll the device without transferring a task bundle.
   For Sophos container enrollment, you can select a policy instead of a task bundle.
   When you click Next, the device is added to Sophos Mobile.

7. On the Enrollment wizard page, follow the instructions to complete the enrollment process.
8. When enrollment has been completed successfully, click **Finish** to close the device enrollment wizard.

**Note**
- When you have made all the selections, you can close the wizard without having to wait for the **Finish** button to appear. An enrollment task is created and processed in the background.
- If you have selected a task bundle to be transferred to the device after enrollment, you can monitor the task status on the **Task view** page. See **View unfinished, failed and latest finished tasks** (page 10).
- For iOS devices, when you have configured Sophos Mobile to synchronize the device name with the device as described in **Configure iOS settings** (page 17), the name you entered in the **Name** field is ignored and the name that is configured on the device is used instead.

### 13.2.3 Auto-enroll iOS devices

You can configure iOS devices to auto-enroll with Sophos Mobile during device activation. To do so, you use Apple Configurator 2 to assign devices to the Sophos Mobile MDM server. When the users switch on their devices for the first time, the iOS setup assistant starts. During setup, the devices are automatically enrolled with Sophos Mobile.

**Note**
- For a detailed description of Apple Configurator 2, see the **Apple Configurator 2 online help**.

To configure auto-enrollment of iOS devices with Sophos Mobile:

1. As a one-time step to prepare auto-enrollment, create a device group that will be assigned to devices during auto-enrollment with Sophos Mobile. In the device group properties, select the **Enable iOS auto-enrollment** option. See **Create device group** (page 76).
2. Make a note of the URL that is displayed in the **Auto-enrollment URL** field of the device group. You need this URL when you configure devices with Apple Configurator 2.
3. Connect the iOS device you want to auto-enroll to an USB port of a Mac with Apple Configurator 2 installed.
4. In Apple Configurator 2, use the Prepare Assistant to set up the device configuration.
5. Select **Manual Enrollment** and then enter the auto-enrollment URL of the device group.
6. Follow the further steps of the Prepare Assistant. You can optionally configure the following aspects of the device activation:
   - Enable device supervision mode.
   - Configure host computers to which the device is allowed to connect with, using USB ports.
   - For supervised devices, generate or choose a "supervision identity".
• Disable configuration steps of the iOS setup assistant.

After you have completed the configuration, hand over the device to the user. When the user switches on the device for the first time, the iOS setup and the enrollment with Sophos Mobile are performed as configured.

Tip

By default, Sophos Mobile manages auto-enrolled devices under a name that is composed from the device ID and the device type. Alternatively, Sophos Mobile can use the name that is configured on the device. See the Synchronize device name option in Configure iOS settings (page 17).

13.2.4 Enroll iOS devices without Apple ID

You can enroll an iOS device with Sophos Mobile without having to associate the device with an Apple ID first. This can be useful for example to preconfigure the device before handing it over to a user.

The standard enrollment method includes the installation of the Sophos Mobile Control app onto the device. Because the app is installed from the App Store and an Apple ID is required to access the App Store, you need to associate the device with the ID before starting the enrollment.

Alternatively, you can enroll an iOS device without installing the Sophos Mobile Control app, so there is no need to associate the device with an Apple ID. This is provided by:

• The auto-enrollment method. See Auto-enroll iOS devices (page 52).
• The device enrollment wizard. See Use the device enrollment wizard to assign and enroll new devices (page 50).

In the Device enrollment wizard, do as follows:

1. On the Enrollment page, select the Enrollment without Apple ID tab.
2. Use the device's web browser to open the enrollment URL. This opens a Sophos Mobile enrollment form.
3. In that form, enter the token and then click Enroll.
4. Follow the instructions on the device to install the enrollment task bundle.

13.2.5 Enroll Android Things device

This section describes how to enroll an Android Things device using the device enrollment wizard.

Prerequisites:

• You have set up a computer (known as host computer) that is connected to your local IP network and that has the Android Debug Bridge command-line tool (adb) installed. adb is part of the Android SDK Platform-Tools package. This package can either be installed as part of the Android SDK or as a standalone package. For details, see the Android developer documentation.
• You have flashed an Android Things image file onto the device that you want to enroll.
• You have connected the device to your local IP network through Ethernet or Wi-Fi.

To enroll the Android Things device with Sophos Mobile:

1. On the menu sidebar, under MANAGE, click Devices, and then click Add > Enrollment wizard.
2. Use the device enrollment wizard as described in Use the device enrollment wizard to assign and enroll new devices (page 50) to start the enrollment procedure. For an Android Things device, do as follows:
   a) In the Device details wizard step, in the Platform field, select Android Things.
   b) In the Enrollment wizard step, click Open the Sophos Mobile download area, and then download the APK file of latest SMC Android Client version from there.
3. Copy the APK file to the host computer.

   **Tip**
   You can use the same APK file for all Android Things devices that you enroll.

4. On the host computer, use the `adb` command-line tool to connect to the Android Things device, where `<ip-address>` is the IP address of the device:

   ```
   adb connect <ip-address>
   connected to <ip-address>:5555
   ```

5. Install the Sophos Mobile Control app onto the Android Things device, using the following `adb` command:

   ```
   adb install <path-to-apk-file>
   ```

6. Reboot the device, for example by using the following `adb` command:

   ```
   adb reboot
   ```

   **Note**
   A reboot is required to grant the required permissions to the Sophos Mobile Control app.

7. After reboot, connect to the device again:

   ```
   adb connect <ip-address>
   ```

8. Configure the Sophos Mobile Control app, using the `adb` command that is displayed in the device enrollment wizard or in the instructions email:

   ```
   adb shell am start -d "<configuration-parameters>"
   ```

   **Note**
   You might receive a system message Warning: Activity not started, its current task has been brought to the front. This can be ignored.

The Sophos Mobile Control app on the Android Things device connects to your Sophos Mobile server. After the enrollment process has completed, the device is shown with status Managed in Sophos Mobile.

### 13.2.6 Enroll Windows IoT device

This section describes how to enroll a Windows IoT device using the device enrollment wizard.
Prerequisites:

- You have flashed Windows 10 IoT Core onto the device that you want to enroll.
- You have connected the device to your local IP network through Ethernet or Wi-Fi.

To enroll the Windows IoT device with Sophos Mobile:

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

2. Use the device enrollment wizard as described in **Use the device enrollment wizard to assign and enroll new devices** (page 50) to start the enrollment procedure. For a Windows IoT device, do as follows:
   a) In the **Device details** wizard step, in the **Platform** field, select **Windows IoT**.
   b) In the **Enrollment** wizard step, click **Download provisioning package** to download a .ppkg file with the provisioning package for Sophos Mobile. This link is also available from the instructions email.

3. On a Windows computer that is connected to the same local network as the Windows IoT device, use the Windows File Explorer to connect to the device.
   In the File Explorer address bar, enter the following address, where `<ip-address>` is the IP address of the device:
   \<ip-address>c$
   Enter your administrator user name and password for the device if prompted.

4. Copy the .ppkg file that you downloaded from the enrollment wizard to the **C:\Windows \Provisioning\Packages** folder on the device.

   **Note**
   There must only be one .ppkg file in that folder.

5. Reboot the device.

   After reboot, the Windows IoT device executes the provisioning package and connects to your Sophos Mobile server. After the enrollment process has completed, the device is shown with status **Managed** in Sophos Mobile.

   **Important**
   On the **Show device** page, don't perform the device actions **Set to "Not managed"** or **Delete** before you have unenrolled the device. If you do so, you have to wipe the device before you can enroll it again. To wipe it, you need to re-flash a Windows 10 IoT Core image onto the device.

### 13.3 Unenroll devices

You can unenroll devices that will no longer be used, for example, if a user gets a new device. This is useful, for example, if you have limited the number of devices a user can enroll in the Self Service Portal.

1. On the menu sidebar, under **MANAGE**, click **Devices**.
2. Select the desired device, click **Actions** and then click **Unenroll**.
   A message is displayed prompting you to confirm that you want to unenroll the device.
3. Click **Yes**.

The device is unenrolled. This results in the following:

- **Android devices:**
  - The Sophos Mobile Control device administrator is disabled.
  - The server login data and all other data received are removed.
  - The container apps (Sophos Secure Workspace and Sophos Secure Email) and the Sophos Mobile Security app are reset.

- **iOS devices:**
  - All profiles are removed.
  - All managed apps are removed.
  - All certificates received through Mobile Device Management are removed.
  - The container apps (Sophos Secure Workspace and Sophos Secure Email) are reset.

- **Macs:**
  - All policies are removed.
  - All certificates received through Mobile Device Management are removed.

---

**Note**

For devices enrolled with Sophos Mobile in Android enterprise device owner mode, there is no dedicated unenroll action. To unenroll such a device, wipe it.

---

### 13.4 Manage devices

On the menu sidebar, under **MANAGE > Devices** and **Device groups**, you can keep track of devices and device groups and carry out a number of administrative tasks. After adding devices to Sophos Mobile you can, for example:

- View and edit device details.
- Allow or forbid email access for devices.
- Lock or unlock devices remotely.
- Reset device passwords.
- Wipe the device remotely in case of loss or theft.
- Decommission devices (Android and iOS).
- Delete devices.

### 13.4.1 View devices

1. On the menu sidebar, under **MANAGE**, click **Devices**.
2. Go to the required device and click its name.
   - The **Show device** page is displayed for the selected device.
On the **Devices** page you can display additional information by pointing to certain elements:

- Point to the "Not managed" icon of a device to display the actual status like **Unenrolled** or **Checked out**.
- Point to the "Not compliant" icon of a device to display the severity level (high, medium, low).

### 13.4.2 The Show device page

On the **Show device** page, all relevant information for an individual device is displayed.

In the upper part of the page, you can see the most important device information at a glance.

In the lower part of the page, detailed device information is displayed on several tabs. The tabs and information shown depend on the device platform.

From the **Show device** page, you can directly switch to the **Edit device** page. To edit the device you are viewing, click **Edit**.

#### Status

Shows essential device information like management type, management status, and compliance status.

#### Profiles

Shows the profiles (including provisioning profiles) installed on the device.

The tab also contains commands to install profiles onto the device or to remove them.

**Note**

iOS device profiles that only contain the following configurations don’t appear on the **Profiles** tab:

- **Roaming/Hotspot**
- **Wallpaper**

These configurations are not installed as a profile onto the device. They only set settings that the user may change at a later time.

**Tip**

The search field of the table lets you search by profile IDs, even though the ID is not displayed in the table.

#### Policies

Shows the policies assigned to the device.
On this tab, the Assign policy button is available to assign a policy to the device.

**Device properties**

Shows device properties, for example, properties for model, model name, OS version. For Android devices, rooted smartphones are detected and the relevant property is shown. For iOS devices, jailbroken smartphones are detected and the relevant property is shown.

**Custom properties**

Shows custom device properties. These are the properties that you can create yourself. Custom device properties can, for example, be used in placeholders if no Active Directory connection is available. When you edit a device, you can also add user-specific information here.

**Internal properties**

Shows internal device properties, for example, ActiveSync traffic allowed, IMEI.

**Compliance violations**

This tab is only displayed for non-compliant devices. It shows the compliance violations of the device and the actions taken because of the violation.

For the configuration of these actions, see Create compliance policy (page 39).

**Installed apps**

Shows the software installed onto the device. Different information is displayed for each platform.

The Size column shows the disk space usage of an app itself. The Data column shows the additional disk space that an app uses for user data, configurations, and so on.

With the Install app button, you can install software onto the device. You can also remove apps from the device by clicking the Delete icon next to the relevant app.

**Note**

- For devices where Sophos Mobile only manages the Sophos container, apps outside the Sophos container are not listed. This includes apps that the user has installed from the Enterprise App Store.
- For iOS, apps marked as Managed can be silently removed. See Managed apps for iOS (page 253)
- For Macs, apps from all user accounts are listed.
- For Windows, you can only remove apps that have been installed by Sophos Mobile. If you try to remove an app installed by the user, the task fails.
System apps
Shows Android system apps on the device.

Note
System apps cannot be removed from the device.

Knox apps
This tab shows the apps that the user has installed in the Samsung Knox container.

Knox system apps
This tab shows the system apps that are installed in the Samsung Knox container.

Scan results
This tab shows the results of the last Sophos Mobile Security scan performed on the device.
The tab is only available if the Sophos Mobile Security app is managed by Sophos Mobile. See Manage Sophos Mobile Security (page 283).

Certificates
Shows the certificates in use on the device.
For Macs, device certificates are listed but user certificates are not.

Tip
In the table, point to the Subject or Issuer value to display the certificate details.

Tasks
This tab shows all unfinished and failed tasks for the device as well as the finished tasks of the last few days. You can also view these tasks, together with the tasks for all other devices, on the Task view page. See Monitor tasks (page 10).

13.4.3 Use the extended device filter
With the extended device filter, you can filter the device list according to your requirements. You can store filter criteria under a custom name to apply them later on.

To define a device filter:
1. On the Devices page, click Extended filter in the header bar.
2. Define your filter criteria.
3. To save the filter criteria under a custom name, enter that name in **Device filter** and click **Save**.
4. After you have selected the required criteria, click **Filter** to apply the filter to the device list.

When a filter is active, the filter icon in the header bar changes its color from blue to green.

**Tip**
Remember to reset a filter when it is no longer needed. Otherwise, lists or reports may not include the results you expect.

**Other device filter tasks:**

- To remove a filter from the device list, click **Extended filter** and then click **Reset**.
- To apply a saved filter, click **Saved filters** and then select the required filter.
- To delete a saved filter, click **Saved filters** and then click the trashcan icon next to the filter you want to delete.
- To edit a saved filter, first apply the filter, then click **Extended filter** and make the required changes, then save the filter again.

### 13.4.4 Edit devices

1. On the menu sidebar, under **MANAGE**, click **Devices**.
2. Click the blue triangle next to the required device and then click **Edit**.
   The **Edit device** page is displayed for the selected device.
3. Make the necessary changes (for example, install or remove software on the **Installed apps** tab) and click **Save**.

Your changes are applied to the edited device.

**Note**
Property changes only become valid after you have clicked **Save**. If you do not save the changes you have made, they do not have any effect.

### 13.4.5 Assign a user to a device

1. On the menu sidebar, under **MANAGE**, click **Devices**.
2. On the **Devices** page, click the blue triangle next to the required device and then click **Edit**.
3. On the **Edit device** page, click the **Edit user assignment** icon next to the **User** field and then click the relevant entry from the selection list:
   - To assign a user to a device that has no user assigned to it yet, click **Assign user to device**.
   - To assign a different user to a device that already has a user assigned to it, click **Reassign user to device**.
4. In the **Enter user search parameters** step of the assignment dialog, enter search strings in one or more fields to look up a user the device will be assigned to. For example, enter the user name or part of it.
5. In the **Select user** step, select the required user and then click **Apply**.
6. On the Edit device page, click Save.

### 13.4.6 Deassign a user from a device

1. On the menu sidebar, under MANAGE, click Devices.
2. On the Devices page, click the blue triangle next to the required device and then click Edit.
3. On the Edit device page, click the Edit user assignment icon next to the User field and then click Deassign user from device.
4. In the confirmation dialog, click Yes.
5. Click Save.

### 13.4.7 Define custom properties for devices

You can define custom properties for individual devices.

When you define a property with name `my property`, you can refer to the value of the property in profiles and policies by using the placeholder `%_DEVPROP(my property)_%`. For example, you can use this to refer to the user that is assigned to a device.

For details on profile and policy placeholders, see Placeholders in profiles and policies (page 81).

**Note**
- You cannot create a custom device property with the same name as a standard device property.
- As well as the device-level custom properties described here, you can also define customer-level custom properties. See Define customer properties (page 19).

To define a custom device property:
1. On the menu sidebar, under SETTINGS, click Setup > General. On the Personal tab, make sure that the Show extended device details option is selected.
2. On the menu sidebar, under MANAGE, click Devices.
3. Click the blue triangle next to the required device and then click Edit.
4. On the Edit device page, go to the Custom properties tab and click Add custom property.
5. Enter a name and a value for the new custom device property.
6. Click Apply to add the property.
7. Click Save to save the changes to the device.

### 13.4.8 Configure network access

Before you can configure network access for a device, Network Access Control (NAC) must be enabled in Sophos Mobile.

For Sophos Mobile on Premise, NAC is enabled by the super administrator. See the Sophos Mobile super administrator guide.

For Sophos Mobile as a Service, NAC is always enabled.

There are two options to configure network access for a device:
1. Allow or deny network access unconditionally.
2. Disable network access when the device violates a compliance rule, enable network access otherwise.

Note
Sophos Mobile does not control the network access by itself. Instead, it provides a Deny network status that can be used by external NAC software like Sophos UTM to block network communication.

To configure network access for a device:
1. On the menu sidebar, under MANAGE, click Devices.
2. On the Devices page, select the devices for which you want to set the network access mode.
3. Click Actions, and then click Set network access.
4. Select the network access mode:
   - **Allow**: Network access for the selected devices is allowed.
   - **Deny**: Network access for the selected devices is denied.
   - **Auto mode**: Network access for the selected devices is based on the compliance status of the devices.
5. Click Yes to save the changes.

Note
You can't deny network access for devices where Sophos Mobile only manages the Sophos container.

For information on how to configure network access in compliance rules, see Create compliance policy (page 39).

13.4.9 Lock device

You can remotely lock a device that is managed by Sophos Mobile. This activates the screen lock.

1. On the menu sidebar, under MANAGE, click Devices.
2. On the Devices page, click the blue triangle next to the device that you want to lock or unlock and then click Show.
3. On the Show device page, click Actions > Lock.
4. For macOS: Set a 6-digit PIN code that must be entered on the Mac to unlock it. A task to activate the lock screen is created and transferred to the device.
   - For all platforms except for macOS: The user must enter the device password (or the PIN or pattern, if configured) to unlock the device.
   - For macOS: The Mac restarts. The user must enter the PIN code you set to unlock the device.

You can display the task status on the Task view page.
**Note**
Even for devices where Sophos Mobile only manages the Android work profile, the Lock action locks the device, not just the work profile.

**Note**
You can't lock devices where Sophos Mobile only manages the Sophos container.

**Note**
You can't wipe a Mac that has been locked remotely.

**Tip**
In Sophos Mobile Admin, the macOS system lock PIN is displayed on the device page under Device properties > Unlock passcode and on the Task details page under Lock PIN.

### 13.4.10 Wipe device

You can remotely wipe a device that is managed by Sophos Mobile. This resets the device to its factory settings.

1. On the menu sidebar, under **MANAGE**, click **Devices**.
2. On the **Devices** page, click the blue triangle next to the device that you want to wipe and then click **Show**.
3. On the **Show device** page, click **Actions > Wipe**.
4. For macOS: Set a 6-digit PIN that must be entered on the Mac to unlock it.

A task to wipe the device is created and transferred to the device.

For macOS: When the task is transferred to a Mac, it restarts and then begins wiping the disk. The user must enter the system lock PIN on the Mac to unlock it.

You can display the task status on the **Task view** page.

**Note**
You can't wipe the following devices:

- Devices where Sophos Mobile only manages the Sophos container.
- Devices enrolled with Sophos Mobile in Android enterprise profile owner mode.
- Android Things or Windows IoT devices.
- Macs you’ve locked remotely.

**Tip**
In Sophos Mobile Admin, the macOS system lock PIN is displayed on the device page under Device properties > Unlock passcode and on the Task details page under Lock PIN.
13.4.11 Configure telecom expense management

With telecom expense management (TEM) you monitor cellular data usage of individual devices. This feature is available for Android and iOS devices.

1. On the menu sidebar, under MANAGE, click Devices.

2. On the Devices page, select the devices for which you want to configure telecom expense management.

   Note
   Only select devices with the same cellular data plan.

3. Click Actions > Configure telecom expense management.

4. Configure the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Turn on monitoring</td>
<td>If selected, monitoring cellular data usage is turned on for the selected devices.</td>
</tr>
<tr>
<td>Data volume of plan</td>
<td>The data volume in MB of your cellular data plan.</td>
</tr>
<tr>
<td>Alert threshold</td>
<td>A data volume threshold in MB. When the used data volume for a device exceeds this value, an alert is created. See Alerts (page 13).</td>
</tr>
<tr>
<td>Usage cycle reset date</td>
<td>A value between 1 and 31 to specify the day of the month when the data usage value is reset.</td>
</tr>
</tbody>
</table>

   Note
   If a month has fewer days than the value entered, the data usage value is reset on the last day of the month.

5. Click Save to apply the settings to the selected devices.

Cellular data usage is reported by a device every time it syncs with the Sophos Mobile server.

To view the current data usage of a device, open the device’s Show device page and then click Actions > Telecom expense management.

Important
The reported data usage might deviate from the values charged by your telecom provider. Data traffic caused by installed apps is reported, but not system updates, system app updates, or similar.
**Tip**
Use the **Cellular data usage** report to view the data usage for all devices that have telecom expense management turned on. See **Reports** (page 9).

**Note**
- The data usage value is reset at these times:
  - Regularly every month at the end of the day you configured.
  - When you turn off telecom expense management for the device.
  - When the device is unenrolled from Sophos Mobile.
- For iOS, data usage is not reported when the Sophos Mobile Control app is closed, e.g. when the user has not started the app after restarting the device.

### 13.4.12 Update the iOS software

You can update the iOS software for the following device types:

- Supervised devices with iOS 10.3 or higher
- Supervised Apple DEP devices

**Note**
This section describes how to update the iOS software for a single device. To update the iOS software for a device group, use a task bundle with an **Install latest iOS update** task. See **Available iOS task types** (page 237).

To update the iOS software on a device:
1. On the menu sidebar, under **MANAGE**, click **Devices**.
2. On the **Devices** page, click the blue triangle next to the device and then click **Show**.
3. On the **Show device** page, click **Actions > Show available updates**.
   
   A list of iOS updates that are available for the device is displayed. Updates labeled **Critical** are critical security updates as classified by Apple.

4. To install the latest available update, click **Install latest available update**.

A task to update the iOS software is created and transferred to the device.

You can display the task status on the **Task view** page.

**Tip**
- To check the update status of a single iOS device, open the device’s **Show device** page. A warning sign is displayed next to **Operating system** if the device does not have the latest available iOS version installed.
- To check the update status of all iOS devices, go to the **OsUpdateAvailable** column of the **Devices** report.
13.4.13 Configure iOS Managed Lost Mode

You can put a supervised iOS device into Managed Lost Mode. The device can’t be used until Managed Lost Mode is turned off again in Sophos Mobile.

In Managed Lost Mode, the only actions available on the device are:

- Dial a phone number you have configured.
- Make an emergency call.

**Note**

- Managed Lost Mode is a different lock mode from Lost Mode, which a user can turn on in iCloud. When you turn on Managed Lost Mode in Sophos Mobile, the device can’t be unlocked in iCloud.
- Locating the device is more reliable in Managed Lost Mode than in standard lock mode. The device location is reported by iOS system functionality which does not require the Sophos Mobile Control app to be active.
- Managed Lost Mode requires iOS 9.3 or later.

To turn on Managed Lost Mode:

1. On the menu sidebar, under `MANAGE`, click `Devices`.
2. On the `Devices` page, click the blue triangle next to the device that you want to put into Managed Lost Mode and then click `Show`.
3. On the `Show device` page, click `Actions > Turn on Managed Lost Mode`.
4. Configure the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lock screen message</td>
<td>Text that is displayed on the lock screen.</td>
</tr>
<tr>
<td>Phone number</td>
<td>A phone number that can be dialed from the lock screen.</td>
</tr>
<tr>
<td>Footnote</td>
<td>Footnote text that is displayed at the bottom of the lock screen.</td>
</tr>
<tr>
<td></td>
<td>If you don’t configure a footnote, a standard note to contact an administrator is displayed.</td>
</tr>
</tbody>
</table>

A task to turn on Managed Lost Mode is created and transferred to the device. Managed Lost Mode is turned on immediately after the device has received the task.

When a device is in Managed Lost Mode, you can perform the following actions on the `Show device` page:

- To locate the device, use `Actions > Locate`.
- To play a sound on the device, use `Actions > Play Lost Mode sound`. This requires iOS 10.3 or later.
- To turn off Managed Lost Mode, use `Actions > Turn off Managed Lost Mode`. 
Tip
To find out if Managed Lost Mode is turned on, check the device property IsMDMLostModeEnabled.

13.5 Apple DEP

With the Apple Device Enrollment Program (DEP), you can purchase iPhones, iPads, and Macs in volume for distribution within your company. DEP simplifies the deployment of mobile devices by providing the following features:

- Configurable activation process.
- Wireless enabling of supervision mode.
- Over-the-air configuration.
- Automatic enrollment of iOS devices with Sophos Mobile during device activation.

Note
Sophos Mobile currently supports Apple DEP for iPhones and iPads but not for Macs.

Tip
For detailed information on DEP, visit the Apple DEP website at http://www.apple.com/business/dep/.

Preparation steps

To prepare the management of DEP devices with Sophos Mobile, perform the following one-time steps:

1. In the Apple DEP web portal, create a virtual MDM server and link it to Sophos Mobile. See Set up Apple DEP (page 68).
2. In Sophos Mobile, create one or more DEP profiles that control various device attributes specific to DEP. With the DEP profile, you can also customize the iOS setup assistant that starts when a device is switched on for the first time. See Create DEP profile (page 69).

Deployment steps

When you purchase DEP devices, the typical deployment process includes the following steps:

1. Purchase the devices from Apple or an approved DEP vendor.
2. In the Apple DEP web portal, assign the devices to the Sophos Mobile MDM server. For this and the next step, see Deploy DEP devices (page 72).
3. In Sophos Mobile Admin, assign a DEP profile to the devices.
4. Distribute the devices to your users.
5. When the users switch on their devices for the first time, the customized iOS setup assistant starts. During setup, the devices are enrolled with Sophos Mobile and the user is assigned to the device.
6. If required, you can transfer additional task bundles to the devices to complete the provisioning.

13.5.1 Set up Apple DEP

**Prerequisite:** This procedure assumes that you have already enrolled in the Apple Device Enrollment Program (DEP) and set up an administrator account for the Apple DEP web portal.

**Note**
For detailed information on enrolling in DEP, visit the Apple DEP website at [http://www.apple.com/business/dep/](http://www.apple.com/business/dep/) or see the Apple Deployment Programs online help.

**Tip**
If you have already enrolled in the Apple Volume Purchase Program (VPP), you can use the same Apple ID for DEP.

To use Apple DEP with Sophos Mobile, you need to create a virtual MDM server in the Apple DEP web portal and link it to the Sophos Mobile server. This includes a verification process to establish a secure connection between Sophos Mobile and the Apple DEP web service.

To set up a virtual MDM server for Sophos Mobile:

1. On the menu sidebar, under **SETTINGS**, click **Setup > System setup**, and then click the **Apple DEP** tab.
2. Click **Download public key** to download the Sophos Mobile public key file for Apple DEP.
   The file is saved to your local computer, using the download settings of your web browser.
   You can do this by clicking the **Apple DEP web portal** link in Sophos Mobile.
4. Log in to the Apple DEP web portal with your company Apple ID.
5. In the portal, go to **Device Enrollment Program > Manage Servers**, and then click **Add MDM Server**.
6. Enter a name for MDM server, for example **Sophos Mobile**.
7. In the next step, upload the public key file that you downloaded from Sophos Mobile.
8. In the next step, download the server token.
   At this point, you may log out from the Apple DEP web portal.
9. On the **Apple DEP** tab of Sophos Mobile, click **Upload a file** and select the server token that you downloaded from the Apple DEP web portal.
   The details of your virtual MDM server are displayed.
10. Click **Save** to save your changes.

The DEP server token is valid for one year.

**Important**
When you create a new server token in the Apple DEP web portal, you must use the same Apple ID that you used for the creation of the initial token.
13.5.2 Create DEP profile

You need to set up the Apple Device Enrollment Program (DEP) before you can create DEP profiles. See Set up Apple DEP (page 68).

A DEP profile is assigned to a DEP device and provides information to the Apple server when the device is activated. This information includes:

- The MDM server (that is the Sophos Mobile server) assigned to manage the device.
- Configuration options for the enrollment with Sophos Mobile.
- A list of hosts that the device is allowed to pair with.
- Customization options for the iOS setup assistant that starts when the device is switched on for the first time.

If required, you can create several DEP profiles to use different setup and enrollment settings for your DEP devices.

To create a DEP profile:
1. On the menu sidebar, under SETTINGS, click Setup > System setup, and then click the Apple DEP profiles tab.
2. Click Add.
3. In the Edit DEP profile dialog, enter a name and optionally a description for the DEP profile.
4. Optional: In the Device group list, select a device group that will be assigned to devices when they are enrolled with Sophos Mobile. For information on device groups, see Device groups (page 76).

Note
To simplify device management, we recommend that you use a separate device group for DEP devices.

5. Optional: In the Task bundle list, select a task bundle that will be transferred onto the devices when they are enrolled with Sophos Mobile. The list includes all iOS task bundles that contain no enrollment task. For information on task bundles, see Task bundles (page 233).
6. On the Enrollment tab, you can configure the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervise device</td>
<td>Supervision mode is enabled.</td>
</tr>
<tr>
<td>User can remove MDM profile</td>
<td>The user is able to remove the Sophos Mobile enrollment profile through the iOS user interface. This option can only be deselected for supervised devices.</td>
</tr>
<tr>
<td>Install SMC app</td>
<td>Install the Sophos Mobile Control app onto the device. If you enable this option, you must also disable the Skip Apple ID option on the iOS setup tab to make sure that Sophos Mobile can install the app from the App Store.</td>
</tr>
</tbody>
</table>
User can skip MDM profile assignment | The user is able to skip the setup step that applies the Sophos Mobile enrollment profile.

Assign user to device | During the enrollment process with Sophos Mobile, users are asked for their Self Service Portal credentials and then assigned to the device. Use this option to auto-assign a user to the device.

7. On the **iOS setup** tab, you can disable configuration steps of the iOS setup assistant that starts when the device is switched on for the first time.

**Note**

These settings only affect the iOS setup. If you disable a configuration step, the user is still able to enable the relevant option later. To completely disable a feature, use a **Restrictions** configuration. See **Restrictions configuration (iOS device profile)** (page 144).

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skip Apps &amp; Data</td>
<td>The page <strong>Apps &amp; Data</strong> is not displayed. The user cannot restore data from an iCloud or iTunes backup, or transfer data from an Android device.</td>
</tr>
<tr>
<td>Disable &quot;Move Data from Android&quot;</td>
<td>On the <strong>Apps &amp; Data</strong> page, the option <strong>Move Data from Android</strong> is not available. The user cannot transfer data from an Android device. This can only be enabled when <strong>Skip Apps &amp; Data</strong> is also enabled.</td>
</tr>
<tr>
<td>Skip Diagnostics</td>
<td>The page <strong>Diagnostics</strong> is not displayed. Sending diagnostic and usage data to Apple is disabled.</td>
</tr>
<tr>
<td>Skip Location Services</td>
<td>The page <strong>Location Services</strong> is not displayed. The user cannot enable location services.</td>
</tr>
<tr>
<td>Skip Siri</td>
<td>The page <strong>Siri</strong> is not displayed. The user cannot set up Siri.</td>
</tr>
<tr>
<td>Skip Display Zoom</td>
<td>The page <strong>Display Zoom</strong> is not displayed. The user cannot change the display view.</td>
</tr>
<tr>
<td>Skip Apple ID</td>
<td>The page <strong>Apple ID</strong> is not displayed. The user cannot log in with their Apple ID to access Apple services.</td>
</tr>
</tbody>
</table>
8. On the **Support information** tab, you can configure the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>The department or location name associated with the profile. This name is included in the information that the user can access by clicking <strong>About Configuration</strong> during device setup.</td>
</tr>
<tr>
<td>Phone number</td>
<td>The support phone number for your company. This field is pre-populated with the phone number from the technical support contact details. See <a href="#">Configure technical support contact details</a> (page 19).</td>
</tr>
<tr>
<td>Email</td>
<td>The support email address for your company. This field is pre-populated with the email address from the technical support contact details. See <a href="#">Configure technical support contact details</a> (page 19).</td>
</tr>
</tbody>
</table>

**Note**
The phone number is stored internally in the DEP profile but is not available to the device user.

**Note**
The email address is stored internally in the DEP profile but is not available to the device user.

9. On the **USB pairing** tab, you configure host computers to which the device is allowed to connect with, using USB ports. This can be used to sync the device with iTunes or to manage it with Apple Configurator.

   - To allow USB connection with all hosts, select **Allow USB pairing with all hosts**.
   - To forbid USB connection or to restrict it to certain hosts, deselect **Allow USB pairing with all hosts** and then upload a certificate file for each host to which the device is allowed to connect with.

10. When you have configured all tabs of the **Edit DEP profile** dialog, click **Apply** to save the DEP profile.

11. To assign the profile to all new DEP devices to which no profile has been manually assigned to, select it in the **Default DEP profile assigned to new devices** list.
When you select None, you have to manually assign a DEP profile to new DEP devices as described in Deploy DEP devices (page 72). Otherwise, DEP devices will not be enrolled with Sophos Mobile when they are activated.

12. Click Save to save your changes.

### 13.5.3 Deploy DEP devices

Perform this procedure to connect your devices to Apple DEP and to enroll them with Sophos Mobile. You can manage devices that you have purchased from Apple or from an approved DEP vendor. Before you can connect devices to Apple DEP, you need to configure the device vendor in the Apple DEP portal.

**Note**

In a typical DEP workflow, you perform this procedure before handing over the devices to your users for activation and usage.

**Note**

For a detailed description of the Apple DEP portal, see the Apple Deployment Programs online help.

To assign your devices to Sophos Mobile and to assign a DEP profile to them:

1. Open the web portal for the Apple deployment programs at https://deploy.apple.com in your web browser and then log in with your company Apple ID.
2. In the portal, go to Device Enrollment Program > Manage Devices.
3. Under Choose Devices By, select your new devices by serial number, by order number, or upload a CSV file containing the serial numbers of your devices.

**Note**

If you have purchased your devices from a reseller, they are available in the DEP portal within 24 hours after the reseller posts your order to Apple.

4. Under Choose Action, select Assign to Server and then select the virtual MDM server that you have set up for Sophos Mobile as described in Set up Apple DEP (page 68).
5. Click OK to perform the assignment.

At this point, you may log out from the Apple DEP web portal.

You may skip the remaining steps if you have configured a default DEP profile as described in Create DEP profile (page 69).

6. Log in to Sophos Mobile Admin with an administrator account for the customer for which you want to manage the DEP devices.
7. On the menu sidebar, under MANAGE, click Devices and then click Apple DEP.
   The Apple DEP devices page lists all devices that you have assigned to Sophos Mobile in the Apple DEP web portal.
8. If the devices that you just assigned to Sophos Mobile do not appear in the list, click Synchronize with Apple DEP portal.
9. Select the new devices and then click **Actions > Assign profile**.

10. In the confirmation dialog, select the DEP profile you want to assign to the devices and then click **OK**.

When the purchased devices arrive at your company, you can hand them over to your users. No further configuration is required. When the users switch on their devices for the first time, the iOS setup and the enrollment with Sophos Mobile are performed as configured in the assigned DEP profile.

If you have selected the **Assign user to device** profile option as described in Create DEP profile (page 69), the users are automatically assigned to their device.

### 13.5.4 Manage DEP devices

DEP devices are managed in Sophos Mobile just as non-DEP devices are. See Manage devices (page 56).

Specifically to DEP, you can assign a DEP profile to a device. The DEP profile provides information to the Apple server when the device is activated. See Create DEP profile (page 69).

#### Note

The DEP profile that is displayed in Sophos Mobile might be different to the profile that is actually used on the device. If you change the assignment after the device was activated, the device continues to use the previously assigned profile until it is wiped and activated again.

To change the DEP profile of a device:

1. On the menu sidebar, under **MANAGE**, click **Devices** and then click **Apple DEP**.

   The **Apple DEP devices** page lists all devices that you have assigned to Sophos Mobile on the Apple DEP web portal.

2. Click **Synchronize with Apple DEP portal** to update the DEP information.

   **Note**

   To limit the load on the Apple DEP server, the **Synchronize with Apple DEP portal** option is disabled after a synchronization and becomes available again after a few minutes.

3. Select the devices to which you want to assign a different DEP profile.

4. Click **Actions** and then click the required action:

   - **Assign profile**: Select the DEP profile that will be assigned to the devices when they are activated the next time.
   - **Deassign profile**: Assign no DEP profile when the devices are activated the next time.

   The new profile assignment is displayed on the **Apple DEP devices** page. The changes are applied to the devices after they are wiped and activated again.
13.6 Duo Security integration

You can connect Sophos Mobile with the Duo Security authentication software. This allows Duo Security to identify trusted devices by their Sophos Mobile management status.

To determine the trust status of a device, Duo Security uses different approaches for Android and iOS:

- For Android devices, the trust status is retrieved through the Sophos Mobile web service interface.
- For iOS devices, the trust status is determined by the existence of a certain certificate on the device.

Note

For more information on trusted devices, see the Duo Security documentation.

13.6.1 Configure Duo Security integration for Android devices

Perform the following steps to let Duo Security determine the trust status of your Android devices.

1. In Sophos Mobile, create an administrator with role **Duo API**.
2. In the **Duo Admin Panel**, enter the user name and password of that administrator. See the Duo Security documentation for details.

To determine the trust status of an Android device, the **Duo Mobile** Android app reports the device ID to the Duo Security server. The Duo Security server then retrieves the device status through the Sophos Mobile web service interface and classifies managed devices as trusted.

Related concepts
User roles [page 4]

Related tasks
Create administrators (page 281)

13.6.2 Configure Duo Security integration for iOS devices

Perform the following steps to let Duo Security determine the trust status of your iOS devices.

1. From the menu sidebar, go to **Setup > System setup > Duo Security** and then configure the settings for the SCEP CA server as provided by Duo Security.
2. Add a **Duo device certificate** configuration to the iOS device profile you are using for your iOS devices.
3. Update the iOS device profile on the devices.

This installs a Duo device certificate on the devices. The **Duo Mobile** iOS app detects the certificate and classifies the devices as trusted.

Related tasks
Install a profile onto devices [page 81]
Related reference
Duo device certificate (iOS device profile) [page 165]
14 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.

14.1 Create device group

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

Note

The device group settings contain the Enable iOS auto-enrollment option. This option allows you to enroll iOS devices with the Apple Configurator. See Auto-enroll iOS devices (page 52).

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

14.2 Delete device groups

1. On the menu sidebar, under MANAGE, click Device groups.
2. On the Device groups page, click the blue triangle next to the device group that you want to delete, and then click Delete.
3. In the confirmation dialog, select one of the remaining device groups to which devices from the current device group will be re-assigned.
   This selection is not available when there are no devices assigned to the current device group.
4. Click Yes to delete the device group.

Note

When there is only one device group left and there are devices assigned to it, you cannot delete this device group.
15 Profiles and policies

Profiles

Profiles are settings that you define and then install onto a device or device group.

To install a profile on one or more devices, Sophos Mobile creates a task and executes it at the specified time. When you update a profile, you must install it again for the changed configurations to take effect on the device.

The following profile types are available:

- Configurations for Android device profiles (page 83)
- Configurations for Knox container profiles (page 137)
- Configurations for iOS device profiles (page 142)

Policies

Policies are settings that you define and then assign to a device or device group. You can only assign one policy of each type to one device.

If you assign a policy to a device, a sync is triggered and the settings take effect immediately. Assigned policies are updated on the device each time a device connects to the Sophos Mobile server. So when you update a policy, you do not have to explicitly re-apply it to the device.

The following policy types are available:

- Configurations for Android enterprise device policies (page 114)
- Configurations for Android enterprise work profile policies (page 102)
- Configurations for Sophos container policies for Android (page 127)
- Configurations for Mobile Security policies (page 137)
- Configurations for Android Things policies (page 142)
- Configurations for Sophos container policies for iOS (page 170)
- Configurations for macOS device policies (page 181)
- Configurations for macOS user policies (page 195)
- Configurations for Windows Mobile policies (page 212)
- Configurations for Windows policies (page 222)
- Configurations for Android Things policies (page 142)
- Configurations for Windows IoT policies (page 229)

15.1 Create profile or policy

Profiles and policies are made up of one or more configurations. By adding configurations, you define the scope of the profile or policy, that is, the areas that are managed on the devices.

1. On the menu sidebar, under CONFIGURE, click Profiles, policies and then click the platform for which you want to create the profile or policy.

2. On the Profiles and policies page, click Create. If there is more than one profile or policy type available for a platform, Create opens a menu from which you can select the required type.

For a list of available profile and policy types, see Profiles and policies (page 77).
3. Enter a name and a description.
4. For iOS and macOS device profiles, enter your organization name.
5. For Sophos container policies, a **General** configuration is mandatory and is automatically added to the policy. On the **Edit policy** page, click **General** to open the configuration and make the required changes.
6. For Android enterprise policies, a **Restrictions** configuration is mandatory and is automatically added to the policy. On the **Edit policy** page, click **Restrictions** to open the configuration and make the required changes.
7. To add more configurations to the profile or policy, click **Add configuration** and then select the configuration you want to add.

**Note**
The configurations supported may depend on the version of the operating system or on other device features. The requirements are indicated by a blue label.

8. In the settings page of the configuration, specify the required settings.
9. Optional: Repeat the previous steps to add more configurations.
10. After you have added all required configurations, click **Save**.

The profile or policy is created. For information on how to apply the profile or policy to devices, see **Install a profile onto devices** (page 81) or **Assign a policy to devices** (page 82).

**Tip**
When you update a profile, you can easily re-install it onto all devices on which it is installed: On the **Profiles and policies** page, click the blue triangle next to the profile and then click **Update devices**.

When you update a policy, it is automatically updated on all devices to which the policy is assigned.

### 15.2 Import iOS device profiles created with Apple Configurator

You can import profiles created with Apple Configurator into Sophos Mobile. Apple Configurator can be downloaded from the App Store.

**Note**
You import device profiles with the same procedure as provisioning profiles for your self-developed iOS apps. When you upload a profile file, Sophos Mobile analyzes its content in order to distinguish between the two profile types.

1. After you have created a profile in Apple Configurator, export it (unencrypted and unsigned) and save it on your computer.
2. On the menu sidebar, under **CONFIGURE**, click **Profiles, policies > iOS**.
3. On the **Profiles and policies** page, click **Create > Import profile**.

The **Edit profile** page is displayed.
4. Enter a name and a description for the new profile in the relevant fields.
5. Click **Upload a file** and navigate to the file you have saved on your computer, select it and click **Open**.
6. Click **Save**.

The profile is created. It can be installed onto devices. See *Install a profile onto devices* (page 81).

### 15.3 Import provisioning profiles for iOS apps

When you develop your own iOS apps, you create provisioning profiles so that your apps can be installed from an IPA file instead of the App Store. You can upload these provisioning profiles to the Sophos Mobile server to subsequently distribute them to your devices.

For details on provisioning profiles, see the *iOS Developer Library*.

**Note**

You import provisioning profiles with the same procedure as device profiles created with Apple Configurator. When you upload a profile file, Sophos Mobile analyzes its content in order to distinguish between the two profile types.

1. After you have generated a provisioning profile in your iOS development environment, save it on your computer.
2. On the menu sidebar, under **CONFIGURE**, click **Profiles, policies > iOS**.
3. On the **Profiles and policies** page, click **Create > Import profile**. The **Edit profile** page is displayed.
4. Enter a name and a description for the new profile in the relevant fields.
5. Click **Upload a file** and navigate to the file you have saved on your computer, select it and click **Open**.
6. Click **Save**.

The profile is created. It can be installed onto devices. See *Install a profile onto devices* (page 81).

### 15.4 About macOS policies

For Macs there are two types of policies:

- **Device policy**: When you assign a device policy to a Mac, the settings apply to all users that log in to the Mac, whether they are managed by Sophos Mobile or not.
- **User policy**: When you assign a user policy to a Mac, the settings apply to all managed users that log in to the Mac.

**Managed users are**:

- The local user that has enrolled the Mac with Sophos Mobile.
- All network users that are known to Sophos Mobile, i.e. users from the external LDAP directory you have configured for the Self Service Portal.
About device and user policies

• In addition to the enrollment policy (which is a device policy) you can assign one device policy and one user policy to a Mac.
• If there are conflicting configurations in a device policy and a user policy assigned to the same Mac, the more restrictive configuration is applied.
• On the Mac, the assigned policies are listed under System Preferences > Profiles.
• When you update a device policy, the changes take effect the next time the device syncs.
• When you update a user policy, the changes take effect the next time a user logs in to the Mac.
• Users may remove the user policy from the Mac but it is automatically re-assigned the next time the user logs in.
• Users can’t remove the device policy.
• When a user removes the enrollment policy, the Mac is unenrolled from Sophos Mobile. This requires administrator privileges.

Related concepts
Configurations for macOS device policies [page 181]
Configurations for macOS user policies [page 195]

15.5 Windows password complexity rules

Password complexity rules (for example length, number of uppercase and lowercase letters) for Windows computers are fixed and cannot be set by a Sophos Mobile policy. Different rules apply for local and for Microsoft accounts.

Local accounts

• Password must not contain the user’s account name or more than two consecutive characters from the user’s full name.
• Password must be six or more characters long.
• Password must contain characters from three of the following four categories:
  — Uppercase characters A-Z (Latin alphabet)
  — Lowercase characters a-z (Latin alphabet)
  — Digits 0-9
  — Special characters (!, $, #, %, etc.)

Microsoft accounts

• Password must be eight or more characters long.
• Password must contain characters from two of the following four categories:
  — Uppercase characters A-Z (Latin alphabet)
  — Lowercase characters a-z (Latin alphabet)
  — Digits 0-9
  — Special characters (!, $, #, %, etc.)
15.6 Samsung Knox support

You can manage your Samsung Knox devices with Sophos Mobile.

To activate Samsung Knox support, you must configure a Samsung Knox Premium license key in Sophos Mobile. See Register Samsung Knox license (page 37).

To configure the Knox container of Samsung devices, see Configurations for Knox container profiles (page 137).

To install apps in a Samsung Knox container, see Add app (page 244).

To manage your Samsung Knox devices you can create task bundles for the following actions:

- Knox container: lock
- Knox container: unlock
- Knox container: reset password
- Knox container: remove (removes the container and all related configuration from the device)

To create a task bundle for a Samsung Knox device, see Create task bundle (page 233).

15.7 Placeholders in profiles and policies

Profiles and policies may contain placeholders which are replaced by actual data at the time of task execution. The following placeholders can be used:

- Placeholders for user data:
  - %_EMAILADDRESS_
  - %_USERNAME_

- Placeholders for device properties:
  - %DEVPROP(property name)_%
    where property name can be either a standard property or a custom property of the device. See Define custom properties for devices (page 61).

- Placeholders for customer properties:
  - %CUSTPROP(property name)_%
    See Define customer properties (page 19).

For macOS, user data is replaced as follows:

- For the local Mac user, the data of the Sophos Mobile user assigned to the device is used.
- For network users, the data of the LDAP user account is used.

15.8 Install a profile onto devices

1. On the menu sidebar, under CONFIGURE, click Profiles, policies and then click one of the device platforms that support profiles:
   - Android
   - iOS

   The Profiles and policies page for the selected platform is displayed.
2. Click the blue triangle next to the profile to be installed and then click Install. The Select devices page is displayed.

3. On this page, you can:
   - Select individual devices onto which you want to install the profile.
   - Click Select device groups and select one or several device groups.

4. After you have made your selection, click Next. The Set execution date page is displayed.

5. Under Scheduled date, select Now or specify a date and time for the execution of the task.

6. Click Finish. The Task view page is shown.

The profile is installed onto the selected devices at the specified date and time.

**Tip**
You can also install a profile by using one of the following options:

- To update a profile on all devices on which the profile is installed: On the Profiles and policies page, click the blue triangle next to the profile and then click Update devices.
- To install a profile on a single device: On the device's Show device page, select the Profiles tab and click Install profile.
- To install a profile on several devices: On the Devices page, select the required devices and then click Actions > Install profile.
- To install a profile on one or more devices as part of a task bundle: Add an Install profile task to the task bundle and transfer it to the required devices or device groups.

### 15.9 Assign a policy to devices

1. On the menu sidebar, under CONFIGURE, click Profiles, policies and then click one of the device platforms that support policies:
   - Android
   - Android Things
   - iOS
   - macOS
   - Windows Mobile
   - Windows
   - Windows IoT

   The Policies page for the selected platform is displayed.

2. Click the blue triangle next to the policy to be assigned and then click Assign. The Select devices page is displayed.

3. On this page, you can:
   - Select individual devices you want to assign the policy to.
   - Click Select device groups and select one or several device groups for assigning the policy.

4. After you have made your selection, click Finish.

The policy is assigned to the selected devices and a synchronization process for the selected devices is triggered.
Note
Policies cannot be removed from a device. To disable a policy, you must assign a different policy to that device.

Tip
You can also assign a policy by using one of the following options:

• To assign a policy to a single device: On the device’s Show device page, select the Policies tab and click Assign policy.
• To assign a policy to several devices: On the Devices page, select the required devices and then click Actions > Install profile.
• To assign a policy to one or more devices as part of a task bundle: Add an Install profile task to the task bundle and transfer it to the required devices or device groups.

15.10 Uninstall profile

Use one of the following procedures to uninstall a profile from devices:

• To uninstall a profile from a single device: On the device’s Show device page select the Profiles tab. Click the blue triangle next to the profile you want to remove and then click Uninstall.
• To uninstall a profile from all devices it’s installed on: On the Profiles and policies page for a platform, click the blue triangle next to the profile you want to remove and then click Uninstall.
• To uninstall a profile from selected devices: Create a task bundle with a Uninstall Profile task and transfer it to the required devices or device groups.

15.11 Download profiles and policies

You can download profiles and policies that you have configured in Sophos Mobile Admin. This is useful, for example, if you need to pass the defined settings on to Sophos Support.

1. On the menu sidebar, go to Profiles, policies and click a device platform.
   The Profiles and policies page for the selected platform is displayed.
2. Click the name of the required profile or policy.
   The Show profile or Show policy page is displayed.
3. Click Download.
   The profile or policy is saved to your local computer.

15.12 Configurations for Android device profiles

With an Android device profile you configure various aspects of Android devices, like password policies, restrictions or Wi-Fi settings.

For information on how to create a device profile, see Create profile or policy (page 77).
15.12.1 Password policies configuration (Android device profile)

With the Password policies configuration you define requirements for the display lock password.

**Note**
The settings supported may depend on the version of the operating system or on other device features. The scope is indicated by a blue label in Sophos Mobile.

**Password type**

In the Password type list, select the type of password users are allowed to configure:

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pattern, PIN or password</td>
<td>Users must set a screen lock. They can choose a type Pattern, PIN or Password screen lock. No additional restrictions are imposed.</td>
</tr>
<tr>
<td>Simple password</td>
<td>Users must set a Password screen lock. Digits are allowed, but the password must contain at least one letter. You can define a minimum length. See the following table.</td>
</tr>
<tr>
<td>PIN or password</td>
<td>Users must set a PIN or Password screen lock. You can define a minimum length. See the following table.</td>
</tr>
<tr>
<td>Alphanumeric password</td>
<td>Users must set a Password screen lock. The password must contain both letters and digits. You can define a minimum length. See the following table.</td>
</tr>
<tr>
<td>Complex password</td>
<td>Users must set a Password screen lock. The password must contain both letters and digits. You can define a minimum length and a minimum number of digits, lowercase and uppercase letters and special characters. See the following two tables.</td>
</tr>
</tbody>
</table>

If you select Simple password, PIN or password, Alphanumeric password or Complex password, the following fields are displayed:

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum password length</td>
<td>The minimum number of characters a password must contain.</td>
</tr>
</tbody>
</table>
### Sophos Mobile on Premise

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Maximum idle time before password prompt</strong></td>
<td>The time after the device is locked if it has not been used. The device can be unlocked by entering the password.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The device might impose a shorter time period than what you configure here.</td>
</tr>
<tr>
<td><strong>Maximum password age in days</strong></td>
<td>Requires users to change their password in the specified interval. Value range: 0 (no password change required) to 730 days.</td>
</tr>
<tr>
<td><strong>Number of failed attempts until device wipe</strong></td>
<td>The number of failed attempts to enter the correct password before the device is wiped.</td>
</tr>
<tr>
<td><strong>Minimum history length</strong></td>
<td>The number of old passwords that are remembered and compared with new ones. When the user defines a new password, it is not accepted if it matches a previously used password. Value range: 1 to 5 or none.</td>
</tr>
</tbody>
</table>

If you select **Complex password**, the following additional fields are displayed:

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Minimum number of letters</strong></td>
<td>The minimum number of letters a password must contain.</td>
</tr>
<tr>
<td><strong>Minimum number of lowercase letters</strong></td>
<td>The minimum number of lowercase letters a password must contain.</td>
</tr>
<tr>
<td><strong>Minimum number of uppercase letters</strong></td>
<td>The minimum number of uppercase letters a password must contain.</td>
</tr>
<tr>
<td><strong>Minimum number of non-alphabetic characters</strong></td>
<td>The minimum number of non-alphabetic characters (for example &amp; or !) a password must contain.</td>
</tr>
<tr>
<td><strong>Minimum number of digits</strong></td>
<td>The minimum number of numerals a password must contain.</td>
</tr>
<tr>
<td><strong>Minimum number of special characters</strong></td>
<td>The minimum number of special characters (for example !&quot;$%&amp;/()=,:;&lt;&gt;@) a password must contain.</td>
</tr>
</tbody>
</table>
### Biometric authentication

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow fingerprint authentication</td>
<td>If supported by the device, the user can use fingerprint authentication to unlock the device.</td>
</tr>
<tr>
<td>Allow iris authentication</td>
<td>If supported by the device, the user can use iris authentication to unlock the device.</td>
</tr>
</tbody>
</table>

### 15.12.2 Restrictions configuration (Android device profile)

With the Restrictions configuration you define restrictions for devices.

#### Security

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Force encryption</td>
<td>Users must encrypt their devices.</td>
</tr>
<tr>
<td>Force SD card encryption</td>
<td>When the profile is installed onto a device, the user must encrypt the SD card.</td>
</tr>
<tr>
<td>Note</td>
<td>For some device types, users can choose to cancel the encryption. They will be reminded again on the next SD card mount.</td>
</tr>
<tr>
<td>Allow fast encryption</td>
<td>Users can change the fast encryption options in the device settings.</td>
</tr>
<tr>
<td>Allow factory reset</td>
<td>Users can reset their devices to factory state.</td>
</tr>
<tr>
<td>Allow &quot;Developer options&quot;</td>
<td>Users can change the developer options.</td>
</tr>
<tr>
<td>Allow safe mode</td>
<td>Users can boot the device in safe mode.</td>
</tr>
<tr>
<td>Allow USB debugging</td>
<td>Users can turn on USB debugging.</td>
</tr>
<tr>
<td>Note</td>
<td>For Sony devices with Enterprise API version 9 or above, clearing the Allow USB debugging check box makes all developer options unavailable.</td>
</tr>
</tbody>
</table>
### Setting/Field | Description
---|---
Allow firmware recovery | All types of firmware updates (like over-the-air, download etc.) are allowed.
Allow backup | Users can create system backups. If the check box is cleared, Google backup is turned off but other backup methods (for example Sophos Mobile backups) remain available.
Allow settings changes | Users can change device settings.
Allow clipboard | Users can copy any contents to the clipboard.
Enable shared clipboard | Allows users to copy clipboard content between apps. If the check box is cleared, each app has an individual clipboard.
This setting is only available if you select Allow clipboard.
Allow screen capture | Users can take a screenshot of the display.
Allow mock GPS locations | Users can select a mock location app in the Android developer options.
Allow over-the-air firmware updates | Over-the-air firmware updates are allowed.
Allow audio recording | Users can perform audio recording.
Allow video recording | Users can record videos. If the check box is cleared, users can still take pictures and stream videos.
Allow Activation Lock | Users can change the Activation Lock options in the device settings.
Allow S Beam | Users can start the Samsung S Beam app.
Allow S Voice | Users can start the Samsung S Voice app.
Allow "Share via" | The Share via feature is available.

### Accounts

| Setting/Field | Description |
---|---|
Allow multiple user accounts | If the check box is cleared, multi-user support is turned off. Users or other apps cannot create additional user accounts. |
### Allow adding email accounts
If the check box is cleared, users cannot add email accounts. This does not affect the account creation through a device profile.

### Allow removal of the Google account
If the check box is cleared, users cannot remove the Google account from the device.

### Allow auto-sync for Google accounts
If the check box is cleared, Google accounts are not synchronized automatically. Users are still able to perform a manual sync from inside some apps like Gmail.

### Network and communication

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow airplane mode</td>
<td>If the check box is cleared, users cannot enable airplane mode.</td>
</tr>
<tr>
<td>Allow sync while roaming</td>
<td>If the check box is cleared, synchronization while roaming is turned off.</td>
</tr>
<tr>
<td>Allow emergency calls only</td>
<td>Only emergency calls are allowed. All other calls will be blocked.</td>
</tr>
<tr>
<td>Force manual sync during roaming</td>
<td>Automatic data synchronization is turned off when the device is roaming. This affects all configured accounts, such as Google or Exchange.</td>
</tr>
<tr>
<td>Force mobile data connection</td>
<td>Users cannot turn off cellular data.</td>
</tr>
<tr>
<td>Allow SMS</td>
<td>If the check box is cleared, users cannot send text messages.</td>
</tr>
<tr>
<td>Allow mobile data connection while roaming</td>
<td>If the check box is cleared, mobile data connections while roaming are turned off.</td>
</tr>
<tr>
<td>Allow voice calls while roaming</td>
<td>If the check box is cleared, voice calls while roaming are turned off.</td>
</tr>
<tr>
<td>Allow user mobile data limit</td>
<td>If the check box is cleared, users cannot set a mobile data limit.</td>
</tr>
<tr>
<td>Allow VPN</td>
<td>If the check box is cleared, users cannot use VPN connections.</td>
</tr>
<tr>
<td>Allow Wi-Fi Direct</td>
<td>If the check box is cleared, data transfer through Wi-Fi Direct is turned off.</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allow Android Beam</td>
<td>If the check box is cleared, data transfer through Android Beam is turned off. This includes the Samsung S Beam app.</td>
</tr>
<tr>
<td>Allow Miracast policy</td>
<td>If the check box is cleared, data transfer through Miracast is turned off.</td>
</tr>
<tr>
<td>Allow Bluetooth</td>
<td>If the check box is cleared, Bluetooth is turned off.</td>
</tr>
<tr>
<td>Allow Advanced Audio Distribution Profile (A2DP)</td>
<td>To allow individual Bluetooth profiles, first select the Allow Bluetooth check box and then select the profiles you want to allow.</td>
</tr>
<tr>
<td>Allow Audio/Video Remote Control Profile (AVRCP)</td>
<td>If the <strong>Allow Bluetooth</strong> check box is cleared, the settings have no effect, i.e. all profiles are forbidden.</td>
</tr>
<tr>
<td>Allow Hands-Free Profile (HFP)</td>
<td></td>
</tr>
<tr>
<td>Allow Headset Profile (HSP)</td>
<td></td>
</tr>
<tr>
<td>Allow Phone Book Access Profile (PBAP)</td>
<td></td>
</tr>
<tr>
<td>Allow Serial Port Profile (SPP)</td>
<td></td>
</tr>
<tr>
<td>Allow NFC</td>
<td>If the check box is cleared, NFC (near-field communication) is turned off.</td>
</tr>
<tr>
<td>Allow Wi-Fi</td>
<td>If the check box is cleared, Wi-Fi is turned off.</td>
</tr>
</tbody>
</table>

### Tethering

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow tethering</td>
<td>If the check box is cleared, all tethering is turned off. This includes tethering over Wi-Fi, USB and Bluetooth.</td>
</tr>
<tr>
<td>Allow Wi-Fi tethering</td>
<td>If the check box is cleared, Wi-Fi tethering (<a href="#">Wi-Fi hotspot</a>) is turned off.</td>
</tr>
<tr>
<td>Allow USB tethering</td>
<td>If the check box is cleared, USB tethering is turned off.</td>
</tr>
<tr>
<td>Allow Bluetooth tethering</td>
<td>If the check box is cleared, Bluetooth tethering is turned off.</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allow configuring Wi-Fi tethering</td>
<td>The user can configure the settings of the Wi-Fi hotspot.</td>
</tr>
</tbody>
</table>

**Hardware**

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow camera</td>
<td>If the check box is cleared, the camera is unavailable.</td>
</tr>
<tr>
<td>Allow camera on lock screen</td>
<td>If the check box is cleared, the camera is unavailable when the screen is locked. To allow the camera on the lock screen you must also select the Allow camera option.</td>
</tr>
<tr>
<td>Force GPS for location queries</td>
<td>GPS information is used for device location.</td>
</tr>
<tr>
<td>Allow SD card</td>
<td>If the check box is cleared, SD cards cannot be used in devices.</td>
</tr>
<tr>
<td>Allow moving apps to the SD card</td>
<td>If the check box is cleared, users cannot move apps from the internal storage to the SD card.</td>
</tr>
<tr>
<td>Allow writing to unencrypted SD card</td>
<td>If the check box is cleared, it is not possible to write to unencrypted SD cards.</td>
</tr>
<tr>
<td>Allow microphone</td>
<td>If the check box is cleared, the microphone is unavailable.</td>
</tr>
<tr>
<td>Allow USB</td>
<td>The USB mass storage mode and the USB media device mode (MTP) are available on the device.</td>
</tr>
<tr>
<td>Allow USB media player</td>
<td>If the check box is cleared, the Media Transfer Protocol (MTP) is unavailable. Because Android uses MTP for USB file transfer, any file transfer over USB is blocked.</td>
</tr>
<tr>
<td>Allow power saving mode</td>
<td>If the check box is cleared, the device doesn't enter power saving mode.</td>
</tr>
<tr>
<td>Allow USB host storage</td>
<td>All external storage devices the user connects are mounted. This includes portable USB storage devices, external HD drives and SD card readers. If the check box is cleared, external storage devices are not mounted.</td>
</tr>
</tbody>
</table>
## Applications

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow app install</td>
<td>If the check box is cleared, users cannot install apps.</td>
</tr>
<tr>
<td>Allow app uninstall</td>
<td>If the check box is cleared, users cannot uninstall apps.</td>
</tr>
<tr>
<td>Allow unsigned app install</td>
<td>If the check box is cleared, users can only install signed APK files.</td>
</tr>
<tr>
<td>Allow Play Store</td>
<td>If the check box is cleared, the Google Play Store app is unavailable.</td>
</tr>
<tr>
<td>Allow apps from unknown sources</td>
<td>If the check box is cleared, users can only install apps through the Google Play Store app.</td>
</tr>
<tr>
<td>Allow native browser</td>
<td>If the check box is cleared, the native browser is unavailable. Third-party browser apps are not affected.</td>
</tr>
<tr>
<td>Allow app crash reports</td>
<td>If the check box is cleared, apps cannot send crash reports.</td>
</tr>
<tr>
<td>Allow wallpaper change</td>
<td>If the check box is cleared, users cannot change the wallpaper.</td>
</tr>
<tr>
<td>Allow widgets on lock screen</td>
<td>If the check box is cleared, widgets are unavailable when the screen is locked.</td>
</tr>
<tr>
<td>Allow Knox contact info for personal calls</td>
<td>By default, a Samsung Knox device displays contact information when the user receives a call from a Knox contact while in personal mode.</td>
</tr>
<tr>
<td></td>
<td>If the check box is cleared, Knox contact information is not displayed in personal mode.</td>
</tr>
<tr>
<td>Allow autofill in browser</td>
<td>The user can enable autofill in the settings of the native Android browser. If enabled, web pages can provide suggestions when the user is filling in form data.</td>
</tr>
<tr>
<td></td>
<td>If the check box is cleared, autofill is turned off and the browser setting is unavailable.</td>
</tr>
<tr>
<td>Allow cookies in browser</td>
<td>The user can enable cookies in the settings of the native Android browser. If enabled, web pages can store cookies on the device.</td>
</tr>
<tr>
<td></td>
<td>If the check box is cleared, cookies are turned off and the browser setting is unavailable.</td>
</tr>
</tbody>
</table>
### Setting/Field | Description
--- | ---
Allow JavaScript in browser | The user can enable JavaScript in the settings of the native Android browser. If enabled, web pages can execute JavaScript code on the device. 
If the check box is cleared, JavaScript is turned off and the browser setting is unavailable.

Allow pop-ups in browser | The user can enable pop-ups in the settings of the native Android browser. If enabled, web pages can open new browser windows. 
If the check box is cleared, pop-ups are turned off and the browser setting is unavailable.

Allow changing date and time settings | The user can change the date and time settings.

Allowed apps / Forbidden apps | You can configure either Allowed apps or Forbidden apps. Select the desired option from the first list and then select the app group containing the apps that should be allowed or forbidden from the second list.
App installations initiated by the Sophos Mobile server are not restricted by this setting.
For information on creating app groups, see App groups (page 261).

### 15.12.3 Knox Premium restrictions configuration (Android device profile)

With the Knox Premium restrictions configuration you define restrictions for Samsung Knox devices. These restrictions apply to the device, not to the Knox container.

| Option | Description |
--- | ---
Allow firmware auto update options | The device automatically checks for firmware updates. Users cannot change this in the device settings.

Enable ODE Trusted Boot verification | The device decrypts the data partition on boot only if the binary and the kernel are official, i.e. if the device is not rooted. 
If the check box is cleared, the device always decrypts the data partition on boot.

Prevent installation of another administrator app | The installation of apps that require device administrator privileges is prevented. This does not affect apps that are installed by Sophos Mobile.

Prevent activation of another administration app | The activation of device administrator privileges for apps is prevented.
### 15.12.4 App Protection configuration (Android device profile)

With the **App Protection** configuration you define password requirements for protecting apps. With App Protection in use, users must define a password when they start a protected app for the first time. After a failed login attempt a login delay is imposed.

If App Protection is active on a device, the command **Reset App Protection password** is available in the **Actions** menu of the **Show device** page. The user can also reset the App Protection password in the Self Service Portal.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password complexity</strong></td>
<td>The minimum complexity requirements for the password to be defined by users.</td>
</tr>
<tr>
<td><strong>Grace period in minutes</strong></td>
<td>After the grace period has expired, protected apps can only be unlocked by entering a password.</td>
</tr>
<tr>
<td><strong>App group</strong></td>
<td>Select the app group containing the apps that are password protected.</td>
</tr>
<tr>
<td></td>
<td>For creating app groups, see <a href="#">App groups</a> (page 261).</td>
</tr>
<tr>
<td><strong>Allow fingerprint authentication</strong></td>
<td>Users can use their fingerprint to unlock a protected app.</td>
</tr>
</tbody>
</table>
15.12.5 App Control configuration (Android device profile)

With the App Control configuration you define apps that users are not allowed to start. For example, you can use this to block apps that have been pre-installed by the device manufacturer and cannot be uninstalled.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>App group</td>
<td>Select the app group containing the blocked apps.</td>
</tr>
<tr>
<td></td>
<td>For information on creating app groups, see App groups (page 261).</td>
</tr>
</tbody>
</table>

15.12.6 App permissions configuration (Android)

With the App permissions configuration you configure what happens when an app requests a permission at runtime.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>App-specific runtime permissions</td>
<td>You can grant or deny certain runtime permissions for individual apps. Click Add and then configure the settings for an app:</td>
</tr>
<tr>
<td></td>
<td>In the App identifier field, enter the internal identifier of the app.</td>
</tr>
<tr>
<td></td>
<td>For each runtime permission, select the desired grant state:</td>
</tr>
<tr>
<td></td>
<td>• Selectable: The user can grant or deny the permission.</td>
</tr>
<tr>
<td></td>
<td>• Granted: Permission is granted and cannot be denied by the user.</td>
</tr>
<tr>
<td></td>
<td>• Denied: Permission is denied and cannot be granted by the user.</td>
</tr>
</tbody>
</table>

15.12.7 Exchange account configuration (Android device profile)

With the Exchange account configuration you set up a connection to a Microsoft Exchange Server email server.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account name</td>
<td>The account name.</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Exchange server</strong></td>
<td>The Exchange server address.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If you use the Sophos Mobile EAS proxy, enter the URL of the EAS proxy server.</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>The domain for this account.</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>The user for this account.</td>
</tr>
<tr>
<td></td>
<td>If you enter the variable <code>%_USERNAME_%</code>, the server replaces it with the actual user name.</td>
</tr>
<tr>
<td><strong>Email address</strong></td>
<td>The email address of the account.</td>
</tr>
<tr>
<td></td>
<td>If you enter the variable <code>%_EMAILADDRESS_%</code>, the server replaces it with the actual email address.</td>
</tr>
<tr>
<td><strong>Sender</strong></td>
<td>A sender name for this account.</td>
</tr>
<tr>
<td></td>
<td>If you enter the variable <code>%_EMAILADDRESS_%</code>, the server replaces it with the actual email address.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The password for this account.</td>
</tr>
<tr>
<td></td>
<td>If you leave this field empty, users must enter the password on their devices.</td>
</tr>
<tr>
<td><strong>Synchronization period</strong></td>
<td>The time period used for synchronizing emails.</td>
</tr>
<tr>
<td></td>
<td>Only the emails from within the specified period are synchronized to the inbox on the managed device.</td>
</tr>
<tr>
<td><strong>Synchronization interval</strong></td>
<td>The interval between email synchronization processes.</td>
</tr>
<tr>
<td><strong>SSL/TLS</strong></td>
<td>The connection to the Exchange server is secured by SSL or TLS (depending on what the server supports).</td>
</tr>
<tr>
<td></td>
<td>We recommend that you select this check box.</td>
</tr>
<tr>
<td><strong>Default account</strong></td>
<td>The account is used as the default email account.</td>
</tr>
<tr>
<td><strong>Allow all certificates</strong></td>
<td>Allow all certificates in transfer processes from the email server.</td>
</tr>
<tr>
<td><strong>Client certificate</strong></td>
<td>The client certificate for the connection to the Exchange server.</td>
</tr>
<tr>
<td><strong>Allow forwarding emails</strong></td>
<td>Allow forwarding of emails.</td>
</tr>
</tbody>
</table>
### Setting/Field Description

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow use of HTML format</td>
<td>Allow the use of HTML format in emails.</td>
</tr>
<tr>
<td>Maximum attachment size in MB</td>
<td>The maximum size of a single email message (1, 3, 5, 10, Unlimited).</td>
</tr>
<tr>
<td>Synchronize content types</td>
<td>The content types to be synchronized.</td>
</tr>
</tbody>
</table>

**Note**
For Sony devices with Enterprise API version 6.x or below, it is important that the Exchange account information matches the user that is assigned to the device.

On these devices, the Sophos Mobile Control app is not able to send the ActiveSync ID to the Sophos Mobile server. When the device contacts the EAS proxy for the first time, the ActiveSync ID that the email client sends is not known to Sophos Mobile. To verify the account details, the EAS proxy searches for a device with an unknown ActiveSync ID and an assigned user that matches the user information supplied by the email client. If such a device is found, the ActiveSync ID is assigned to that device and the email request is passed on to the Exchange server. Otherwise, the request is rejected.

For details, see [Sophos knowledgebase article 121360](#).

### 15.12.8 Wi-Fi configuration (Android device profile)

With the **Wi-Fi configuration** you specify settings for connecting to Wi-Fi networks.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
<td>The ID of the Wi-Fi network.</td>
</tr>
<tr>
<td>Security type</td>
<td>The security type of the Wi-Fi connection:</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td>• WEP</td>
</tr>
<tr>
<td></td>
<td>• WPA/WPA2 PSK</td>
</tr>
<tr>
<td></td>
<td>• EAP/PEAP</td>
</tr>
<tr>
<td></td>
<td>• EAP/TLS</td>
</tr>
<tr>
<td></td>
<td>• EAP/TTLS</td>
</tr>
<tr>
<td>Phase 2 authorization</td>
<td>The authentication method for phase 2 of the EAP negotiation:</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td>• PAP</td>
</tr>
<tr>
<td></td>
<td>• CHAP</td>
</tr>
<tr>
<td></td>
<td>• MSCHAP</td>
</tr>
<tr>
<td></td>
<td>• MSCHAPv2</td>
</tr>
<tr>
<td></td>
<td>This field is available for <strong>EAP/PEAP</strong> and <strong>EAP/TTLS</strong> connections.</td>
</tr>
</tbody>
</table>
**Setting/Field** | **Description**
---|---
**Identity** | The user identity. This field is available for EAP connections.
**Anonymous identity** | The pseudonym identity sent unencrypted in phase 1 of the EAP negotiation. This field is available for EAP connections.
**Password** | The password for the Wi-Fi network.
**Identity certificate** | The identity certificate for the connection to the Wi-Fi network. The list includes all certificates from Client certificate configurations of the current policy. This field is available for EAP connections.
**Trusted certificate** | The root CA for the certificate of the EAP server. The list includes all certificates from Root certificate configurations of the current policy. This field is available for EAP connections.
**Proxy server and port** | The name or IP address and the port number of a proxy server for the Wi-Fi connection.

**15.12.9 VPN configuration (Android device profile)**

With the VPN configuration you define VPN settings for network connections.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connection name</strong></td>
<td>The name of the connection shown on the device.</td>
</tr>
<tr>
<td><strong>Server</strong></td>
<td>The host name or the IP address of the server.</td>
</tr>
</tbody>
</table>
### Setting/Field | Description
---|---
**Connection type**| The type of the VPN connection:
- **L2TP/IPsec (PSK)**
  If you select this type, the fields **User**, **Password** and **L2TP/IPsec (PSK)** are displayed. Enter the user and password. In the **L2TP/IPsec (PSK)** field, enter the pre-shared key for authentication.
- **L2TP/IPsec (Certificate)**
  If you select this type, the fields **Client certificate**, **Root certificate**, **User** and **Password** are displayed. In the fields **Client certificate** and **Root certificate**, select the relevant certificates. In addition, enter the **User** and the relevant **Password**.
- **Cisco AnyConnect**
  If you select this type, you can upload XML files with an AnyConnect VPN profile and/or an NVM (Network Visibility Module) profile. See the Cisco AnyConnect administrator guide for information on these profiles.

### 15.12.10 Root certificate configuration [Android device profile]

With the **Root certificate** configuration you install a root certificate onto devices.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. The name of the certificate is shown in the **Certificate name** field. Enter the password for the selected certificate.

**Note**
The certificate you upload here is only available for this profile. If you require certificates in other profiles or policies, you have to upload them again.

### 15.12.11 Client certificate configuration [Android device profile]

With the **Client certificate** configuration you install a client certificate onto devices.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. The name of the certificate is shown in the **Certificate name** field. Enter the password for the selected certificate.

**Note**
The certificate you upload here is only available for this profile. If you require certificates in other profiles or policies, you have to upload them again.
15.12.12 SCEP configuration (Android device profile)

With the SCEP configuration you enable devices to request certificates from a Certificate Authority using the Simple Certificate Enrollment Protocol (SCEP).

**Note**
You must first add a Root certificate configuration to upload the CA certificate of the SCEP server before you can add a SCEP configuration.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>URL</strong></td>
<td>The web address of the Certificate Authority server.</td>
</tr>
<tr>
<td></td>
<td>Use the variable <code>%_SCEPPROXYURL_</code> to refer to the server URL that is</td>
</tr>
<tr>
<td></td>
<td>configured on the SCEP tab of the System setup page.</td>
</tr>
<tr>
<td><strong>Alias name</strong></td>
<td>The name under which the certificate will appear in selection dialogs.</td>
</tr>
<tr>
<td></td>
<td>This should be a memorable name to identify the certificate. For example,</td>
</tr>
<tr>
<td></td>
<td>use the same value as in the Subject field, but without the CN= prefix.</td>
</tr>
<tr>
<td><strong>Subject</strong></td>
<td>The name of the entity (for example person or device) that will receive the</td>
</tr>
<tr>
<td></td>
<td>certificate. You can use placeholders for user data or device properties.</td>
</tr>
<tr>
<td></td>
<td>The value that you enter (with placeholders replaced by the actual data)</td>
</tr>
<tr>
<td></td>
<td>must be a valid X.500 name.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>• Enter CN=%<em>USERNAME</em>% to specify a user.</td>
</tr>
<tr>
<td></td>
<td>• Enter CN=%<em>DEVPROP(serial_number)</em>% to specify a device.</td>
</tr>
<tr>
<td></td>
<td>For information on available placeholders, see Placeholders in profiles and</td>
</tr>
<tr>
<td></td>
<td>policies (page 81).</td>
</tr>
<tr>
<td><strong>Type of Subject Alternative Name</strong></td>
<td>To add a Subject Alternative Name (SAN) to the SCEP configuration, select the SAN type and then enter the SAN value. SAN types are:</td>
</tr>
<tr>
<td><strong>Value of Subject Alternative Name</strong></td>
<td>To add a Subject Alternative Name (SAN) to the SCEP configuration, select the SAN type and then enter the SAN value. SAN types are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>RFC 822 name</strong>: A valid email address.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DNS name</strong>: The DNS name of the CA server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Uniform resource identifier</strong>: The fully qualified URL of the CA server.</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AD user logon name</td>
<td>The <strong>User logon name</strong> value set in Active Directory, i.e. the user’s <strong>User Principal Name</strong> (UPN).</td>
</tr>
<tr>
<td>Challenge</td>
<td>The web address to obtain a challenge password from the SCEP server. Use the variable <code>%_CACHALLENGE_%</code> to refer to the challenge URL that is configured on the <strong>SCEP</strong> tab of the <strong>System setup</strong> page.</td>
</tr>
<tr>
<td>Root certificate</td>
<td>The CA certificate. Select the certificate from the list. The list contains all certificates that you have uploaded in <strong>Root certificate</strong> configurations of the current profile.</td>
</tr>
<tr>
<td>Key size</td>
<td>The size of the public key in the issued certificate. Make sure that the value matches the size configured on the SCEP server.</td>
</tr>
<tr>
<td>Use as digital signature</td>
<td>If you select this check box, the public key can be used as a digital signature.</td>
</tr>
<tr>
<td>Use for encryption</td>
<td>If you select this check box, the public key can be used for data encryption.</td>
</tr>
</tbody>
</table>

### 15.12.13 Access Point Name configuration (Android device profile)

With the **Access Point Name** configuration you specify an Access Point Name (APN) configuration for mobile devices. APN configurations define how devices connect to a mobile network.

**Important**  
We recommend that you ask your carrier for the required settings. If you select **Use as default APN** and the settings are not correct, the device cannot access data through cellular networks.

**Note**  
With the exception of the **APN** field, all settings are optional and should only be specified if required by your mobile network carrier.
<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>APN</strong></td>
<td>The APN that the device quotes when it opens a connection with the carrier. This must match an APN that the carrier accepts. Otherwise, the connection cannot be established.</td>
</tr>
<tr>
<td><strong>User-friendly name</strong></td>
<td>An optional name that is displayed on the device in addition to the APN.</td>
</tr>
<tr>
<td><strong>Proxy server and port</strong></td>
<td>The address and port of the HTTP server that is used for web traffic.</td>
</tr>
<tr>
<td><strong>User name, User password</strong></td>
<td>A user name and password for connecting to the APN.</td>
</tr>
<tr>
<td><strong>Server</strong></td>
<td>The WAP Gateway Server.</td>
</tr>
<tr>
<td><strong>MMSC</strong></td>
<td>The Multimedia Messaging Service Center (MMSC).</td>
</tr>
<tr>
<td><strong>MMS proxy server and port</strong></td>
<td>The address and port of a HTTP server that is used for communication with the MMSC.</td>
</tr>
<tr>
<td><strong>Mobile Country Code (MCC), Mobile Network Code (MNC)</strong></td>
<td>MCC and MNC for specifying the carrier. The APN is only used for this carrier.</td>
</tr>
<tr>
<td><strong>Authentication type</strong></td>
<td>The authentication method for PPP connections.</td>
</tr>
<tr>
<td><strong>APN type</strong></td>
<td>The types of data connection that this APN is used for. To use the APN for all data types, enter * or leave the field empty.</td>
</tr>
<tr>
<td><strong>Bearer</strong></td>
<td>The Radio Access Technology (RAT) that the carrier uses.</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>The network protocol that is supported by the carrier.</td>
</tr>
<tr>
<td><strong>Roaming protocol</strong></td>
<td>The network protocol that is supported by the carrier when in roaming mode.</td>
</tr>
<tr>
<td><strong>Use as default APN</strong></td>
<td>If selected, devices will use this APN as default. An error is raised when you try to select this option in more than one Access Point Name configuration.</td>
</tr>
</tbody>
</table>
15.12.14 Kiosk mode configuration (Android device profile)

With the Kiosk mode configuration you define restrictions for devices to put them into a kiosk mode. Click Select source and then do one of the following to specify an app that is started when the profile is transferred to a device:

- Select Custom and enter an app identifier.
- Select App list and then select an app from the App identifier list. The list contains all apps that you have configured on the Apps page. See Add app (page 244).
- Select None to configure kiosk mode without specifying an app. The kiosk mode restrictions are applied to the device, but no app is started.

Under Options, deselect hardware and software features you want to disable in kiosk mode. When the profile is transferred to a device, the app that you specified is started. However, if you have not turn off any of the available hardware or software features, the user will be able to leave the app and use the device as normal. To set the device into a true kiosk mode, you must clear at least the Allow Home button and Allow task manager check boxes.

**Note**

- The app that you specify must be installed on the device. If it is not, the transfer tasks will remain in state Incomplete until the app is installed. To install the app, create a task bundle with an Install app task, for example, and transfer it to your devices.
- If you want to specify an app for Samsung Knox devices, make sure it is a launcher app. This type of app provides an alternative desktop for Android.
- For Sony devices with Enterprise API version 9 or above, if you clear any of the Allow volume up, Allow volume down or Allow volume mute check boxes, all volume buttons of the device are disabled.

15.13 Configurations for Android enterprise work profile policies

With an Android enterprise work profile policy you configure settings that are related to the work profile of a device. The policy can be applied to devices that are enrolled with Sophos Mobile using the Android enterprise profile owner mode.

For information on how to create an Android enterprise work profile policy, see Create profile or policy (page 77).

15.13.1 “Password policies - Device” configuration (Android enterprise work profile policy)

With the Password policies - Device configuration you define requirements for the display lock password.
## Password type

In the **Password type** list, select the type of password users are allowed to configure:

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pattern, PIN or password</strong></td>
<td>Users must set a screen lock. They can choose a type <strong>Pattern, PIN</strong> or <strong>Password</strong> screen lock. No additional restrictions are imposed.</td>
</tr>
<tr>
<td><strong>Simple password</strong></td>
<td>Users must set a <strong>Password</strong> screen lock. Digits are allowed, but the password must contain at least one letter. You can define a minimum length. See the following table.</td>
</tr>
<tr>
<td><strong>PIN or password</strong></td>
<td>Users must set a <strong>PIN</strong> or <strong>Password</strong> screen lock. You can define a minimum length. See the following table.</td>
</tr>
<tr>
<td><strong>Alphanumeric password</strong></td>
<td>Users must set a <strong>Password</strong> screen lock. The password must contain both letters and digits. You can define a minimum length. See the following table.</td>
</tr>
<tr>
<td><strong>Complex password</strong></td>
<td>Users must set a <strong>Password</strong> screen lock. The password must contain both letters and digits. You can define a minimum length and a minimum number of digits, lowercase and uppercase letters and special characters. See the following two tables.</td>
</tr>
</tbody>
</table>

If you select **Simple password**, **PIN or password**, **Alphanumeric password** or **Complex password**, the following fields are displayed:

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Minimum password length</strong></td>
<td>The minimum number of characters a password must contain.</td>
</tr>
<tr>
<td><strong>Maximum idle time before password prompt</strong></td>
<td>The time after the device is locked if it has not been used. The device can be unlocked by entering the password.</td>
</tr>
</tbody>
</table>

**Note**

The device might impose a shorter time period than what you configure here.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Maximum password age in days</strong></td>
<td>Requires users to change their password in the specified interval. Value range: 0 (no password change required) to 730 days.</td>
</tr>
</tbody>
</table>
### Number of failed attempts until device wipe

The number of failed attempts to enter the correct password before the device is wiped.

### Minimum history length

The number of old passwords that are remembered and compared with new ones. When the user defines a new password, it is not accepted if it matches a previously used password. Value range: 1 to 5 or none.

If you select **Complex password**, the following additional fields are displayed:

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum number of letters</td>
<td>The minimum number of letters a password must contain.</td>
</tr>
<tr>
<td>Minimum number of lowercase letters</td>
<td>The minimum number of lowercase letters a password must contain.</td>
</tr>
<tr>
<td>Minimum number of uppercase letters</td>
<td>The minimum number of uppercase letters a password must contain.</td>
</tr>
<tr>
<td>Minimum number of non-alphabetic characters</td>
<td>The minimum number of non-alphabetic characters (for example &amp; or !) a password must contain.</td>
</tr>
<tr>
<td>Minimum number of digits</td>
<td>The minimum number of numerals a password must contain.</td>
</tr>
<tr>
<td>Minimum number of special characters</td>
<td>The minimum number of special characters (for example !&quot;#$%&amp;/()='_;:&lt;&gt;@) a password must contain.</td>
</tr>
</tbody>
</table>

### 15.13.2 “Password policies - Work profile” configuration (Android enterprise work profile policy)

With the **Password policies - Work profile** configuration you define requirements for the work profile password. The user must enter that password to open a work app when the work profile is locked.

#### Note

The settings supported may depend on the version of the operating system or on other device features. The scope is indicated by a blue label in Sophos Mobile.

#### Password type

In the **Password type** list, select the type of password users are allowed to configure:
<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pattern, PIN or password</strong></td>
<td>Users must set a screen lock. They can choose a type Pattern, PIN or Password screen lock. No additional restrictions are imposed.</td>
</tr>
<tr>
<td><strong>Simple password</strong></td>
<td>Users must set a Password screen lock. Digits are allowed, but the password must contain at least one letter. You can define a minimum length. See the following table.</td>
</tr>
<tr>
<td><strong>PIN or password</strong></td>
<td>Users must set a PIN or Password screen lock. You can define a minimum length. See the following table.</td>
</tr>
<tr>
<td><strong>Alphanumeric password</strong></td>
<td>Users must set a Password screen lock. The password must contain both letters and digits. You can define a minimum length. See the following table.</td>
</tr>
<tr>
<td><strong>Complex password</strong></td>
<td>Users must set a Password screen lock. The password must contain both letters and digits. You can define a minimum length and a minimum number of digits, lowercase and uppercase letters and special characters. See the following two tables.</td>
</tr>
<tr>
<td><strong>Weak biometric recognition</strong></td>
<td>Users are allowed to use weak biometric recognition methods, like face recognition, to unlock the work profile.</td>
</tr>
</tbody>
</table>

**Note**

Weak biometric recognition methods provide similar security as a 3-digit PIN. This means that unauthorized unlocking might happen in 1 of 1000 attempts.

If you select Simple password, PIN or password, Alphanumeric password or Complex password, the following fields are displayed:

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Minimum password length</strong></td>
<td>The minimum number of characters a password must contain.</td>
</tr>
</tbody>
</table>
### Maximum idle time before password prompt
The time after the work profile is locked if it has not been used. The profile can be unlocked by entering the password.

**Note**
The device might impose a shorter time period than what you configure here.

### Maximum password age in days
Requires users to change their password in the specified interval. Value range: 0 (no password change required) to 730 days.

### Number of failed attempts until device wipe
The number of failed attempts to enter the correct password before the work profile is wiped.

### Minimum history length
The number of old passwords that are remembered and compared with new ones. When the user defines a new password, it is not accepted if it matches a previously used password. Value range: 1 to 5 or none.

If you select **Complex password**, the following additional fields are displayed:

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum number of letters</td>
<td>The minimum number of letters a password must contain.</td>
</tr>
<tr>
<td>Minimum number of lowercase letters</td>
<td>The minimum number of lowercase letters a password must contain.</td>
</tr>
<tr>
<td>Minimum number of uppercase letters</td>
<td>The minimum number of uppercase letters a password must contain.</td>
</tr>
<tr>
<td>Minimum number of non-alphabetic characters</td>
<td>The minimum number of non-alphabetic characters (for example &amp; or !) a password must contain.</td>
</tr>
<tr>
<td>Minimum number of digits</td>
<td>The minimum number of numerals a password must contain.</td>
</tr>
<tr>
<td>Minimum number of special characters</td>
<td>The minimum number of special characters (for example !&quot;#$%&amp;/()=,-;:_@&lt;&gt; ) a password must contain.</td>
</tr>
</tbody>
</table>
### 15.13.3 Restrictions configuration (Android enterprise work profile policy)

With the Restrictions configuration you configure restrictions and related settings for Android work profiles.

#### Security

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow screen capture</td>
<td>Users can capture the screen content of work apps.</td>
</tr>
<tr>
<td>Allow user to configure credentials</td>
<td>Users can install or remove certificates in the work profile.</td>
</tr>
<tr>
<td>Allow work clipboard in personal apps</td>
<td>Users can copy text from a work app and paste it into a personal app.</td>
</tr>
<tr>
<td></td>
<td>Pasting clipboard text from a personal app into a work app is always possible.</td>
</tr>
<tr>
<td>Allow Smart Lock</td>
<td>Users can turn on the Android Smart Lock feature that automatically unlocks the device in certain situations.</td>
</tr>
<tr>
<td>Allow location sharing</td>
<td>Work apps can access the device’s location features.</td>
</tr>
<tr>
<td></td>
<td>If the check box is cleared, work apps cannot access the device's location features, even if the user has turned location sharing on.</td>
</tr>
<tr>
<td>Allow opening web links in personal apps</td>
<td>Web links that the user taps in a work app can be opened by a personal browser app.</td>
</tr>
<tr>
<td>Allow debugging</td>
<td>Users can turn on the debugging features in the Android developer options.</td>
</tr>
<tr>
<td>Allow unlocking device by fingerprint</td>
<td>Users can use the fingerprint sensor to unlock the device.</td>
</tr>
<tr>
<td>Allow work contact info for personal calls</td>
<td>The personal phone app displays the caller’s name for incoming calls from work contacts.</td>
</tr>
<tr>
<td>Allow work contact info for Bluetooth devices</td>
<td>Connected Bluetooth devices display the caller’s name for incoming personal calls from work contacts.</td>
</tr>
<tr>
<td>Allow searches of work contacts in personal profile</td>
<td>The personal phone app includes results from work contacts when searching for caller’s names.</td>
</tr>
</tbody>
</table>
### Accounts

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow managing accounts</td>
<td>Users can add or remove accounts from the work profile, but not the Google account.</td>
</tr>
</tbody>
</table>

### Network and communication

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow VPN</td>
<td>Users can use VPN connections for work apps.</td>
</tr>
<tr>
<td>Allow Android Beam</td>
<td>Users can send data from work apps through Android Beam (data transfer through NFC).</td>
</tr>
</tbody>
</table>

### Hardware

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow camera</td>
<td>Work apps can access the camera.</td>
</tr>
</tbody>
</table>

### Applications

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow app uninstall</td>
<td>Users can uninstall work apps.</td>
</tr>
<tr>
<td>Allow installing apps from unknown sources</td>
<td>If the check box is cleared, users can only install work apps from the Google Play Store, not from unknown sources or through Android Debug Bridge (ADB).</td>
</tr>
</tbody>
</table>
| Allow managing apps    | If the check box is cleared, users cannot perform the following tasks for work apps:  
  • Uninstall apps  
  • Disable apps  
  • Stop apps  
  • Clear app cache  
  • Clear app data  
  • Clear setting *Open by default* |
<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Allow disabling Google security scans | Users can turn off the Google security setting **Scan device for security threats**.  
                                              The setting is available in the **Settings** app, under **Google > Security > Google Play Protect**. |
| Short message                 | A company-specific support message that is displayed to the user when functionality has been turned off. |
|                               | **Note**  
                                              If you enter more than 200 characters, the message may be truncated. |
| Long message                  | Additional text to complement the short message. The text is displayed when the user taps **More details** in screens that display the short message. |
|                               | **Note**  
                                              This text is also displayed on the Android **Device administrator** screen for the Sophos Mobile Control app. |

**15.13.4 App Protection configuration (Android enterprise work profile policy)**

With the **App Protection** configuration you define password requirements for protecting work apps, i.e. the apps that are installed in the work profile.

With App Protection in use, users must define a password when they start a protected app for the first time. After a failed login attempt a login delay is imposed.

If App Protection is active on a device, the command **Reset App Protection password** is available in the **Actions** menu of the **Show device** page. The user can also reset the App Protection password in the Self Service Portal.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password complexity</td>
<td>The minimum complexity requirements for the password to be defined by users.</td>
</tr>
<tr>
<td>Grace period in minutes</td>
<td>After the grace period has expired, protected apps can only be unlocked by entering a password.</td>
</tr>
</tbody>
</table>
### 15.13.5 App Control configuration (Android enterprise work profile policy)

With the **App Control** configuration you define work apps that users are not allowed to start.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>App group</strong></td>
<td>Select the app group containing the blocked apps. For information on creating app groups, see <a href="#">App groups</a> (page 261).</td>
</tr>
</tbody>
</table>

### 15.13.6 App permissions configuration (Android enterprise work profile policy)

With the **App permissions** configuration you configure what happens when a work app requests a permission at runtime.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Default response for runtime permission requests** | The default response for future runtime permission requests of work apps:  
  - **Prompt**: Apps prompt the user to grant a permission.  
  - **Auto-accept**: All runtime permission requests are automatically granted.  
  - **Auto-deny**: All runtime permission requests are automatically denied.  
  The user cannot change the permissions later. |
**App-specific runtime permissions**

You can grant or deny certain runtime permissions for individual apps. Click **Add** and then configure the settings for an app:

In the **App identifier** field, enter the internal identifier of the app.

For each runtime permission, select the desired grant state:

- **Selectable**: The user can grant or deny the permission.
- **Granted**: Permission is granted and can’t be denied by the user.
- **Denied**: Permission is denied and can’t be granted by the user.

---

**15.13.7 Exchange account configuration (Android enterprise work profile policy)**

With the **Exchange account** configuration you set up a connection to a Microsoft Exchange Server email server. These settings are applied to the Gmail app in the work profile.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Account name</strong></td>
<td>The account name.</td>
</tr>
<tr>
<td><strong>Exchange server</strong></td>
<td>The Exchange server address.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>If you use the Sophos Mobile EAS proxy, enter the URL of the EAS proxy server.</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>The domain for this account.</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>The user for this account.</td>
</tr>
<tr>
<td></td>
<td>If you enter the variable <code>%USERNAME%</code>, the server replaces it with the actual user name.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>The password is entered by the user.</td>
</tr>
<tr>
<td><strong>Email address</strong></td>
<td>The email address of the account.</td>
</tr>
<tr>
<td></td>
<td>If you enter the variable <code>%EMAILADDRESS%</code>, the server replaces it with the actual email address.</td>
</tr>
</tbody>
</table>
### Setting/Field Description

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender</td>
<td>A sender name for this account. If you enter the variable <code>%_EMAILADDRESS_%</code>, the server replaces it with the actual email address.</td>
</tr>
<tr>
<td>Synchronization period</td>
<td>The time period used for synchronizing emails. Only the emails from within the specified period are synchronized to the inbox on the managed device.</td>
</tr>
<tr>
<td>SSL/TLS</td>
<td>The connection to the Exchange server is secured by SSL or TLS (depending on what the server supports). We recommend that you select this check box.</td>
</tr>
<tr>
<td>Allow all certificates</td>
<td>Allow all certificates in transfer processes from the email server.</td>
</tr>
<tr>
<td>Client certificate</td>
<td>The client certificate for the connection to the Exchange server.</td>
</tr>
</tbody>
</table>

#### 15.13.8 Root certificate configuration [Android enterprise work profile policy]

With the **Root certificate** configuration you install a root certificate onto devices. This certificate will be available to work apps, i.e. to apps that are installed in the work profile.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. The name of the certificate is shown in the **Certificate name** field. Enter the password for the selected certificate.

**Note**

The certificate you upload here is only available for this policy. If you require certificates in other profiles or policies, you have to upload them again.

#### 15.13.9 Client certificate configuration [Android enterprise work profile policy]

With the **Client certificate** configuration you install a client certificate onto devices. This certificate will be available to work apps, i.e. to apps that are installed in the work profile.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. The name of the certificate is shown in the **Certificate name** field. Enter the password for the selected certificate.
**Note**
The certificate you upload here is only available for this policy. If you require certificates in other profiles or policies, you have to upload them again.

### 15.13.10 SCEP configuration [Android enterprise work profile policy]

With the SCEP configuration you enable devices to request certificates from a Certificate Authority using the Simple Certificate Enrollment Protocol (SCEP). These certificates will be available to apps that are installed in the work profile.

**Note**
You must first add a **Root certificate** configuration to upload the CA certificate of the SCEP server before you can add a **SCEP** configuration.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>URL</strong></td>
<td>The web address of the Certificate Authority server. Use the variable <code>%_SCEPPROXYURL_</code> to refer to the server URL that is configured on the SCEP tab of the <strong>System setup</strong> page.</td>
</tr>
<tr>
<td><strong>Alias name</strong></td>
<td>The name under which the certificate will appear in selection dialogs. This should be a memorable name to identify the certificate. For example, use the same value as in the <strong>Subject</strong> field, but without the <code>CN=</code> prefix.</td>
</tr>
<tr>
<td><strong>Subject</strong></td>
<td>The name of the entity (for example person or device) that will receive the certificate. You can use placeholders for user data or device properties. The value that you enter (with placeholders replaced by the actual data) must be a valid X.500 name. For example:  * Enter <code>CN=%_USERNAME_</code> to specify a user.  * Enter <code>CN=%_DEVPROP(serial_number)_</code> to specify a device. For information on available placeholders, see <a href="#">Placeholders in profiles and policies</a> (page 81).</td>
</tr>
</tbody>
</table>
Setting/Field | Description
---|---
**Type of Subject Alternative Name** | To add a Subject Alternative Name (SAN) to the SCEP configuration, select the SAN type and then enter the SAN value. SAN types are:

- **RFC 822 name**: A valid email address.
- **DNS name**: The DNS name of the CA server.
- **Uniform resource identifier**: The fully qualified URL of the CA server.

**Value of Subject Alternative Name**

**AD user logon name** | The User logon name value set in Active Directory, i.e. the user’s User Principal Name (UPN).

**Challenge** | The web address to obtain a challenge password from the SCEP server.

Use the variable `%_CACHALLENGE_%` to refer to the challenge URL that is configured on the SCEP tab of the System setup page.

**Root certificate** | The CA certificate.

Select the certificate from the list. The list contains all certificates that you have uploaded in Root certificate configurations of the current profile.

**Key size** | The size of the public key in the issued certificate.

Make sure that the value matches the size configured on the SCEP server.

**Use as digital signature** | If you select this check box, the public key can be used as a digital signature.

**Use for encryption** | If you select this check box, the public key can be used for data encryption.

---

### 15.14 Configurations for Android enterprise device policies

With an Android enterprise device policy you configure various aspects of Android devices, like password policies, restrictions or Wi-Fi settings. The policy can be applied to devices that are enrolled with Sophos Mobile using the Android enterprise device owner mode.

For information on how to create an Android enterprise device policy, see Create profile or policy (page 77).
15.14.1 “Password policies” configuration (Android enterprise device policy)

With the Password policies configuration you define requirements for the display lock password.

Password type

In the Password type list, select the type of password users are allowed to configure:

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pattern, PIN or password</td>
<td>Users must set a screen lock. They can choose a type Pattern, PIN or Password screen lock. No additional restrictions are imposed.</td>
</tr>
<tr>
<td>Simple password</td>
<td>Users must set a Password screen lock. Digits are allowed, but the password must contain at least one letter. You can define a minimum length. See the following table.</td>
</tr>
<tr>
<td>PIN or password</td>
<td>Users must set a PIN or Password screen lock. You can define a minimum length. See the following table.</td>
</tr>
<tr>
<td>Alphanumeric password</td>
<td>Users must set a Password screen lock. The password must contain both letters and digits. You can define a minimum length. See the following table.</td>
</tr>
<tr>
<td>Complex password</td>
<td>Users must set a Password screen lock. The password must contain both letters and digits. You can define a minimum length and a minimum number of digits, lowercase and uppercase letters and special characters. See the following two tables.</td>
</tr>
</tbody>
</table>

If you select Simple password, PIN or password, Alphanumeric password or Complex password, the following fields are displayed:

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum password length</td>
<td>The minimum number of characters a password must contain.</td>
</tr>
</tbody>
</table>
## Maximum idle time before password prompt

The time after the device is locked if it has not been used. The device can be unlocked by entering the password.

**Note**
The device might impose a shorter time period than what you configure here.

## Maximum password age in days

Requires users to change their password in the specified interval. Value range: 0 (no password change required) to 730 days.

## Number of failed attempts until device wipe

The number of failed attempts to enter the correct password before the device is wiped.

## Minimum history length

The number of old passwords that are remembered and compared with new ones. When the user defines a new password, it is not accepted if it matches a previously used password. Value range: 1 to 5 or none.

If you select **Complex password**, the following additional fields are displayed:

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Minimum number of letters</strong></td>
<td>The minimum number of letters a password must contain.</td>
</tr>
<tr>
<td><strong>Minimum number of lowercase letters</strong></td>
<td>The minimum number of lowercase letters a password must contain.</td>
</tr>
<tr>
<td><strong>Minimum number of uppercase letters</strong></td>
<td>The minimum number of uppercase letters a password must contain.</td>
</tr>
<tr>
<td><strong>Minimum number of non-alphabetic characters</strong></td>
<td>The minimum number of non-alphabetic characters (for example &amp; or !) a password must contain.</td>
</tr>
<tr>
<td><strong>Minimum number of digits</strong></td>
<td>The minimum number of numerals a password must contain.</td>
</tr>
<tr>
<td><strong>Minimum number of special characters</strong></td>
<td>The minimum number of special characters (for example !&quot;$%&amp;/()=:_@&lt;&gt;) a password must contain.</td>
</tr>
</tbody>
</table>
15.14.2 Restrictions configuration [Android enterprise device policy]

With the Restrictions configuration you define restrictions for devices.

Security

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Force encryption</td>
<td>Users must encrypt their devices.</td>
</tr>
<tr>
<td>Allow factory reset</td>
<td>Users can reset the device to its factory settings.</td>
</tr>
<tr>
<td>Allow safe mode</td>
<td>Users can boot the device in safe mode.</td>
</tr>
<tr>
<td>Allow debugging</td>
<td>Users can turn on the debugging features in the Android developer options.</td>
</tr>
<tr>
<td>Allow screen capture</td>
<td>Users can take a screenshot of the display.</td>
</tr>
<tr>
<td>Allow user to configure credentials</td>
<td>Users can install or remove certificates.</td>
</tr>
<tr>
<td>Allow Smart Lock</td>
<td>Users can turn on the Android Smart Lock feature that automatically unlocks the device in certain situations.</td>
</tr>
<tr>
<td>Allow location sharing</td>
<td>Users can turn on location sharing.</td>
</tr>
<tr>
<td>Allow unlocking device by fingerprint</td>
<td>Users can use the fingerprint sensor to unlock the device.</td>
</tr>
<tr>
<td>Allow adding user</td>
<td>If supported by the device, users can add user accounts on the device.</td>
</tr>
<tr>
<td>Allow removing user</td>
<td>Users can remove user accounts from the device.</td>
</tr>
<tr>
<td>Allow changing the account picture</td>
<td>Users can change the photo used for their user account.</td>
</tr>
<tr>
<td>Hide sensitive information on lock screen</td>
<td>If notifications on the lock screen are turned on, sensitive notification content is hidden.</td>
</tr>
<tr>
<td>System update policy</td>
<td>Select when system updates are installed:</td>
</tr>
<tr>
<td></td>
<td>- <strong>No policy</strong>: The user can decide when to install system updates.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Install automatically</strong>: System updates are installed automatically as soon as they are available.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Install within maintenance window</strong>: System updates are installed automatically within a daily maintenance window. Enter start and end time of the day.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Postpone</strong>: System updates (except for security updates) are blocked for 30 days.</td>
</tr>
</tbody>
</table>
## Accounts

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow managing accounts</td>
<td>Users can add or remove accounts from the device, but not the Google account.</td>
</tr>
</tbody>
</table>

## Network and communication

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow SMS</td>
<td>If the check box is cleared, users cannot send text messages.</td>
</tr>
<tr>
<td>Allow mobile data connection while roaming</td>
<td>If the check box is cleared, mobile data connections while roaming are turned off.</td>
</tr>
<tr>
<td>Allow VPN</td>
<td>If the check box is cleared, users cannot use VPN connections.</td>
</tr>
<tr>
<td>Allow Android Beam</td>
<td>Users can send data from work apps through Android Beam (data transfer through NFC).</td>
</tr>
<tr>
<td>Allow Bluetooth</td>
<td>If the check box is cleared, Bluetooth is turned off.</td>
</tr>
<tr>
<td>Allow outgoing phone calls</td>
<td>Users can make phone calls.</td>
</tr>
<tr>
<td>Allow network reset</td>
<td>Users can reset network settings to their defaults.</td>
</tr>
<tr>
<td>Enable Wi-Fi settings</td>
<td>Users can change the Wi-Fi settings.</td>
</tr>
<tr>
<td>Allow configuring cell broadcasts</td>
<td>Users can turn cell broadcast (CB) messages on or off in their messaging app.</td>
</tr>
<tr>
<td>Enable cellular networks settings</td>
<td>Users can change the cellular network settings.</td>
</tr>
<tr>
<td>Enable tethering settings</td>
<td>Users can change the tethering and portable hotspot settings.</td>
</tr>
</tbody>
</table>

## Hardware

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow camera</td>
<td>If the check box is cleared, the camera is unavailable.</td>
</tr>
<tr>
<td>Allow microphone</td>
<td>If the check box is cleared, the microphone is unavailable.</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Allow external media</strong></td>
<td>Users can connect external media like USB storage to the device.</td>
</tr>
</tbody>
</table>

### Applications

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allow app uninstall</strong></td>
<td>Users can uninstall apps.</td>
</tr>
<tr>
<td><strong>Allow installing apps from unknown sources</strong></td>
<td>If the check box is cleared, users can only install apps from Google Play, not from unknown sources or through Android Debug Bridge (ADB).</td>
</tr>
<tr>
<td><strong>Allow wallpaper change</strong></td>
<td>If the check box is cleared, users cannot change the wallpaper.</td>
</tr>
<tr>
<td><strong>Allow managing apps</strong></td>
<td>If the check box is cleared, users can’t perform the following tasks for apps:</td>
</tr>
<tr>
<td></td>
<td>• Uninstall apps</td>
</tr>
<tr>
<td></td>
<td>• Disable apps</td>
</tr>
<tr>
<td></td>
<td>• Stop apps</td>
</tr>
<tr>
<td></td>
<td>• Clear app cache</td>
</tr>
<tr>
<td></td>
<td>• Clear app data</td>
</tr>
<tr>
<td></td>
<td>• Clear setting <strong>Open by default</strong></td>
</tr>
<tr>
<td><strong>Allow disabling Google security scans</strong></td>
<td>Users can turn off the Google security setting <strong>Scan device for security threats</strong>. The setting is available in the <strong>Settings</strong> app, under <strong>Google &gt; Security &gt; Google Play Protect</strong>.</td>
</tr>
<tr>
<td><strong>Allow setting date and time</strong></td>
<td>Users can set the date and time. If the check box is cleared, network date and time is used.</td>
</tr>
<tr>
<td><strong>Short message</strong></td>
<td>A company-specific support message that is displayed to the user when functionality has been turned off.</td>
</tr>
</tbody>
</table>

**Note**

If you enter more than 200 characters, the message may be truncated.
<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Long message</td>
<td>Additional text to complement the short message. The text is displayed when the user taps <strong>More details</strong> in screens that display the short message.</td>
</tr>
</tbody>
</table>

**Note**
This text is also displayed on the Android **Device administrator** screen for the Sophos Mobile Control app.

<table>
<thead>
<tr>
<th>Allowed accessibility services</th>
<th>Restrict the list of apps that can provide accessibility services:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• If you select <strong>All available apps</strong>, users can use all accessibility services.</td>
</tr>
<tr>
<td></td>
<td>• If you select <strong>Only system apps</strong>, users can only use accessibility services from system apps.</td>
</tr>
<tr>
<td></td>
<td>• If you select an app group, users can only use accessibility services from apps within that group, and from system apps.</td>
</tr>
</tbody>
</table>

### 15.14.3 App Protection configuration (Android enterprise device policy)

With the **App Protection** configuration you define password requirements for protecting work apps.

With App Protection in use, users must define a password when they start a protected app for the first time. After a failed login attempt a login delay is imposed.

If App Protection is active on a device, the command **Reset App Protection password** is available in the **Actions** menu of the **Show device** page. The user can also reset the App Protection password in the Self Service Portal.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password complexity</td>
<td>The minimum complexity requirements for the password to be defined by users.</td>
</tr>
<tr>
<td>Grace period in minutes</td>
<td>After the grace period has expired, protected apps can only be unlocked by entering a password.</td>
</tr>
<tr>
<td>App group</td>
<td>Select the app group containing the apps that are password protected. For creating app groups, see <a href="#">App groups</a> (page 261).</td>
</tr>
<tr>
<td>Allow fingerprint authentication</td>
<td>Users can use their fingerprint to unlock a protected app.</td>
</tr>
</tbody>
</table>
15.14.4 App Control configuration (Android enterprise device policy)

With the App Control configuration you define apps that users are not allowed to start. For example, you can use this to block apps that have been pre-installed by the device manufacturer and cannot be uninstalled.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>App group</td>
<td>Select the app group containing the blocked apps. For information on creating app groups, see App groups (page 261).</td>
</tr>
</tbody>
</table>

15.14.5 App permissions configuration (Android enterprise device policy)

With the App permissions configuration you configure what happens when an app requests a permission at runtime.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default response for runtime</td>
<td>The default response for future runtime permission requests of work apps:</td>
</tr>
<tr>
<td>permission requests</td>
<td>• <strong>Prompt</strong>: Apps prompt the user to grant a permission.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto-accept</strong>: All runtime permission requests are automatically granted.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto-deny</strong>: All runtime permission requests are automatically denied.</td>
</tr>
<tr>
<td></td>
<td>The user cannot change the permissions later.</td>
</tr>
<tr>
<td>App-specific runtime permissions</td>
<td>You can grant or deny certain runtime permissions for individual apps. Click Add and then configure the settings for an app:</td>
</tr>
<tr>
<td></td>
<td>In the <strong>App identifier</strong> field, enter the internal identifier of the app.</td>
</tr>
<tr>
<td></td>
<td>For each runtime permission, select the desired grant state:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Selectable</strong>: The user can grant or deny the permission.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Granted</strong>: Permission is granted and can’t be denied by the user.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Denied</strong>: Permission is denied and can’t be granted by the user.</td>
</tr>
</tbody>
</table>
15.14.6 Exchange account configuration (Android enterprise device policy)

With the Exchange account configuration you set up a connection to a Microsoft Exchange Server email server.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account name</td>
<td>The account name.</td>
</tr>
<tr>
<td>Exchange server</td>
<td>The Exchange server address.</td>
</tr>
</tbody>
</table>

**Note**

If you use the Sophos Mobile EAS proxy, enter the URL of the EAS proxy server.

<table>
<thead>
<tr>
<th>Domain</th>
<th>The domain for this account.</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>The user for this account.</td>
</tr>
</tbody>
</table>

**Note**

If you enter the variable `%_USERNAME_%`, the server replaces it with the actual user name.

<table>
<thead>
<tr>
<th>Email address</th>
<th>The email address of the account.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If you enter the variable <code>%_EMAILADDRESS_%</code>, the server replaces it with the actual email address.</td>
</tr>
<tr>
<td>Sender</td>
<td>A sender name for this account.</td>
</tr>
<tr>
<td></td>
<td>If you enter the variable <code>%_EMAILADDRESS_%</code>, the server replaces it with the actual email address.</td>
</tr>
<tr>
<td>Synchronization period</td>
<td>The time period used for synchronizing emails.</td>
</tr>
<tr>
<td></td>
<td>Only the emails from within the specified period are synchronized to the inbox on the managed device.</td>
</tr>
<tr>
<td>SSL/TLS</td>
<td>The connection to the Exchange server is secured by SSL or TLS (depending on what the server supports).</td>
</tr>
<tr>
<td></td>
<td>We recommend that you select this check box.</td>
</tr>
<tr>
<td>Allow all certificates</td>
<td>Allow all certificates in transfer processes from the email server.</td>
</tr>
</tbody>
</table>
## 15.14.7 Wi-Fi configuration (Android enterprise device policy)

With the Wi-Fi configuration you specify settings for connecting to Wi-Fi networks.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SSID</strong></td>
<td>The ID of the Wi-Fi network.</td>
</tr>
<tr>
<td><strong>Security type</strong></td>
<td>The security type of the Wi-Fi connection:</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td>• WEP</td>
</tr>
<tr>
<td></td>
<td>• WPA/WPA2 PSK</td>
</tr>
<tr>
<td></td>
<td>• EAP/PEAP</td>
</tr>
<tr>
<td></td>
<td>• EAP/TLS</td>
</tr>
<tr>
<td></td>
<td>• EAP/TTLS</td>
</tr>
<tr>
<td><strong>Phase 2 authorization</strong></td>
<td>The authentication method for phase 2 of the EAP negotiation:</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td>• PAP</td>
</tr>
<tr>
<td></td>
<td>• CHAP</td>
</tr>
<tr>
<td></td>
<td>• MSCHAP</td>
</tr>
<tr>
<td></td>
<td>• MSCHAPv2</td>
</tr>
<tr>
<td></td>
<td>This field is available for EAP/PEAP and EAP/TTLS connections.</td>
</tr>
<tr>
<td><strong>Identity</strong></td>
<td>The user identity.</td>
</tr>
<tr>
<td></td>
<td>This field is available for EAP connections.</td>
</tr>
<tr>
<td><strong>Anonymous identity</strong></td>
<td>The pseudonym identity sent unencrypted in phase 1 of the EAP negotiation.</td>
</tr>
<tr>
<td></td>
<td>This field is available for EAP connections.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The password for the Wi-Fi network.</td>
</tr>
<tr>
<td><strong>Identity certificate</strong></td>
<td>The identity certificate for the connection to the Wi-Fi network.</td>
</tr>
<tr>
<td></td>
<td>The list includes all certificates from Client certificate configurations of the current policy.</td>
</tr>
<tr>
<td></td>
<td>This field is available for EAP connections.</td>
</tr>
</tbody>
</table>
### Setting/Field | Description
--- | ---
Trusted certificate | The root CA for the certificate of the EAP server. The list includes all certificates from **Root certificate** configurations of the current policy. This field is available for EAP connections.

15.14.8 Root certificate configuration (Android enterprise device policy)

With the **Root certificate** configuration you install a root certificate onto devices.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. The name of the certificate is shown in the **Certificate name** field. Enter the password for the selected certificate.

**Note**
The certificate you upload here is only available for this policy. If you require certificates in other profiles or policies, you have to upload them again.

15.14.9 Client certificate configuration (Android enterprise device policy)

With the **Client certificate** configuration you install a client certificate onto devices.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. The name of the certificate is shown in the **Certificate name** field. Enter the password for the selected certificate.

**Note**
The certificate you upload here is only available for this policy. If you require certificates in other profiles or policies, you have to upload them again.

15.14.10 SCEP configuration (Android enterprise device policy)

With the **SCEP** configuration you enable devices to request certificates from a Certificate Authority using the Simple Certificate Enrollment Protocol (SCEP).

**Note**
You must first add a **Root certificate** configuration to upload the CA certificate of the SCEP server before you can add a **SCEP** configuration.
<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>The web address of the Certificate Authority server. Use the variable %<em>SCEPPROXYURL</em>% to refer to the server URL that is configured on the SCEP tab of the System setup page.</td>
</tr>
<tr>
<td>Alias name</td>
<td>The name under which the certificate will appear in selection dialogs. This should be a memorable name to identify the certificate. For example, use the same value as in the Subject field, but without the CN= prefix.</td>
</tr>
</tbody>
</table>
| Subject                             | The name of the entity (for example person or device) that will receive the certificate. You can use placeholders for user data or device properties. The value that you enter (with placeholders replaced by the actual data) must be a valid X.500 name. For example:  
  - Enter CN=%_USERNAME_% to specify a user.  
  - Enter CN=%_DEVPROP(serial_number)_% to specify a device. For information on available placeholders, see Placeholders in profiles and policies (page 81). |
| Type of Subject Alternative Name    | To add a Subject Alternative Name (SAN) to the SCEP configuration, select the SAN type and then enter the SAN value. SAN types are:  
  - RFC 822 name: A valid email address.  
  - DNS name: The DNS name of the CA server.  
  - Uniform resource identifier: The fully qualified URL of the CA server. |
| Value of Subject Alternative Name   |                                                                                                                                             |
| AD user logon name                  | The User logon name value set in Active Directory, i.e. the user’s User Principal Name (UPN).                                                                                                             |
| Challenge                           | The web address to obtain a challenge password from the SCEP server. Use the variable %_CACHALLENGE_% to refer to the challenge URL that is configured on the SCEP tab of the System setup page. |
### 15.14.11 Kiosk mode configuration [Android enterprise device policy]

With the **Kiosk mode** configuration you define restrictions for devices to put them into a kiosk mode.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Select source** | • **None**: Allow all apps. The kiosk mode restrictions are applied to the device, but the user can start any app available on the device.  
                    • **Custom**, **App list**: Lock a single app to the screen.  
                    • **App group**: Allow multiple apps to appear on the screen.  |
| **App identifier** | The app available in kiosk mode. Depending on your selection in **Select source**, either specify the app by its identifier, or select it from the list of available apps.  |
| **App group** | The apps available in kiosk mode. Select one of the configured app groups.  |
| **Allow volume change** | If the check box is cleared, the device’s volume buttons are disabled.  |
| **Turn off screen lock** | The device screen is never locked.  |
| **Stay on while charging** | The device screen stays on while the device is connected to a power supply.  |
15.15 Configurations for Sophos container policies for Android

With a Sophos container policy you configure settings that are related to the Sophos container apps Sophos Secure Email and Sophos Secure Workspace.

For information on how to create a Sophos container policy, see Create profile or policy (page 77).

15.15.1 General configuration (Android Sophos container policy)

With the General configuration you define settings that apply to all Sophos container apps, if applicable.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Sophos container password</td>
<td>Users must enter an additional password to be able to start a Sophos container app. The password has to be defined when the first container app is started after the configuration has been applied. This password applies to all container apps.</td>
</tr>
<tr>
<td>Password complexity</td>
<td>The required minimum complexity of the Sophos container password. More secure passwords are always allowed. Passwords (a mix of numeric and alphanumeric characters) are always seen as more secure than PINs (numeric characters only).</td>
</tr>
<tr>
<td>Always hide characters in password entry fields</td>
<td>Characters in password entry fields are not briefly displayed before they are masked.</td>
</tr>
<tr>
<td>Password age in days</td>
<td>The number of days that a password can be used before users are prompted to change it.</td>
</tr>
</tbody>
</table>

Copyright © 2018 Sophos Limited
<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Failed logins until lock</strong></td>
<td>The number of failed login attempts that are tolerated before the container apps are locked. Once they are locked an administrator needs to unlock the apps or, if allowed, users can use the Self Service Portal to do so.</td>
</tr>
<tr>
<td><strong>Allow fingerprint</strong></td>
<td>Users can use their fingerprint to unlock the app.</td>
</tr>
<tr>
<td><strong>Grace period in minutes</strong></td>
<td>The period of time within which no Sophos container password must be entered when a container app comes to the foreground again.</td>
</tr>
<tr>
<td></td>
<td>The grace period applies to all container apps. You can switch between the apps during the grace period without entering a password.</td>
</tr>
<tr>
<td><strong>Lock on device lock</strong></td>
<td>When the device is locked, the Sophos container is locked as well.</td>
</tr>
<tr>
<td></td>
<td>If the check box is cleared, the container is locked only after the grace period has expired.</td>
</tr>
<tr>
<td><strong>Last server connect</strong></td>
<td>The period of time within users can use a Sophos container app without a connection to the Sophos Mobile server.</td>
</tr>
<tr>
<td></td>
<td>When a Sophos container app becomes active and does not have contact with the server within the defined period of time, a lock screen will be displayed. Users can only unlock the app by tapping <strong>Retry</strong> on the lock screen. The app will then try to connect to the server. If the connection can be established, the app will be unlocked. If not, access will be denied.</td>
</tr>
<tr>
<td></td>
<td>• <strong>On access</strong>: Server connection is always required and the app is locked when the server cannot be reached.</td>
</tr>
<tr>
<td></td>
<td>• <strong>1 hour</strong>: Server connection is required when the app becomes active one hour or more after the last successful server connection.</td>
</tr>
<tr>
<td></td>
<td>• <strong>3 hours</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>6 hours</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>12 hours</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>1 day</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>3 days</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>1 week</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>none</strong>: No regular contact is required.</td>
</tr>
</tbody>
</table>
### Setting/Field

<table>
<thead>
<tr>
<th>Offline starts without server connection</th>
<th>In this field you define how often users can start one of the Sophos container apps without a server connection.</th>
</tr>
</thead>
</table>

**Note**

This setting requires the Sophos container password feature to be turned on.

A counter is incremented whenever users enter the Sophos container password. If the counter exceeds the defined number, the same lock screen as for the **Last server connect** setting will be displayed. The counter will be reset if a connection to the Sophos Mobile server is established.

- **Unlimited**: No server connection is required.
- **0**: Starting the app without a server connection is not possible.
- **1**: After one start of the app, a successful server connection is necessary.
  - **3**
  - **5**
  - **10**
  - **20**

| Root access allowed | Container apps are allowed to run on rooted devices. |

### App usage constraints

Here you can define constraints on using the Sophos container apps. Click **Add** to enter constraints.

<table>
<thead>
<tr>
<th>Geo-fencing</th>
<th>Lets you add latitude and longitude and a radius within which the Sophos container apps can be used.</th>
</tr>
</thead>
</table>

| Time-fencing | Lets you specify a start and end time within which the Sophos container apps can be used. Days of the week on which the apps can be used can be specified as well. |
**Wi-Fi fencing**

If you select **Wi-Fi connection required**, the Sophos container is locked when there is no active Wi-Fi connection.

If you add Wi-Fi networks to the list, the Sophos container is locked when the device is connected to a Wi-Fi network not listed.

**Important**

We recommend that you do not rely on Wi-Fi fencing as the only security mechanism because Wi-Fi names can be spoofed very easily.

---

### 15.15.2 Corporate Email configuration (Android Sophos container policy)

With the **Corporate Email** configuration you define user settings for your Microsoft Exchange Server. These settings are applied to the Sophos Secure Email app if it is installed in the Sophos container.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Exchange server</strong></td>
<td>The Exchange server address.</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>The user for this account.</td>
</tr>
<tr>
<td></td>
<td>If you enter the variable <code>%USERNAME%</code>, the server replaces it with the actual user name.</td>
</tr>
<tr>
<td><strong>Email address</strong></td>
<td>The email address of the account.</td>
</tr>
<tr>
<td></td>
<td>If you enter the variable <code>%EMAILADDRESS%</code>, the server replaces it with the actual email address.</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>The domain for this account.</td>
</tr>
<tr>
<td><strong>Support contact email</strong></td>
<td>The email address that will be used as the &quot;Contact Support&quot; email address.</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Export contacts to device</td>
<td>Users are allowed to export the Exchange contacts with a phone number to the local device contacts, so that they can identify company contacts in incoming calls. Sophos Secure Email keeps the information synchronized.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>The local contact information is automatically deleted in the following situations:</td>
</tr>
<tr>
<td></td>
<td>• When the <strong>Corporate Email</strong> configuration is removed from the Sophos container policy (requires a restart of the Secure Email app).</td>
</tr>
<tr>
<td></td>
<td>• When the Sophos container is removed from the device.</td>
</tr>
<tr>
<td></td>
<td>• When the device is unenrolled from Sophos Mobile.</td>
</tr>
<tr>
<td>Notification details</td>
<td>Select the amount of information that is displayed in email notifications. This setting also affects event reminders. If you select <strong>No notifications</strong>, event reminders are turned off. If you select any other value, event reminders are turned on and include time, location and title information.</td>
</tr>
<tr>
<td>Deny copy to clipboard</td>
<td>Users cannot copy or cut texts from the Sophos Secure Email app.</td>
</tr>
<tr>
<td>Deny screenshots</td>
<td>Users can’t take screenshots that show the Sophos Secure Email app.</td>
</tr>
<tr>
<td>Maximum email size</td>
<td>Email messages that are larger than the size you select (including attachments) are not retrieved from the Exchange server.</td>
</tr>
<tr>
<td>Allow viewing/sharing</td>
<td>Users are allowed to view or share email attachments.</td>
</tr>
<tr>
<td>View attachments</td>
<td>Select whether attachments can be viewed in all apps or only in the Sophos container apps Sophos Secure Workspace and Sophos Secure Email.</td>
</tr>
</tbody>
</table>
15.15.3 Corporate Documents configuration (Android Sophos container policy)

With the Corporate Documents configuration you define settings for the Corporate Documents feature of the Sophos Secure Workspace app.

Configure storage providers

For each storage provider you can define the following settings separately:

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>The storage provider is available in the app.</td>
</tr>
<tr>
<td>Offline</td>
<td>Users are allowed to add files from the storage provider to the app's Favorites list for offline use.</td>
</tr>
<tr>
<td>Open in (encrypted)</td>
<td>Users can share encrypted files with other apps via Open In.</td>
</tr>
<tr>
<td>Open in (unencrypted)</td>
<td>Users can share unencrypted files with other apps via Open In.</td>
</tr>
<tr>
<td>Clipboard</td>
<td>Users can copy parts of a document and paste them into other apps.</td>
</tr>
</tbody>
</table>

Enterprise provider settings

For WebDAV provider, also referred to as enterprise provider, you can centrally define server settings and login credentials. These cannot be changed by users.

Credential settings that you do not define centrally can be chosen by the users in the app’s provider credential screens.
For example you can centrally define the server and user account to be used but you can leave the password field undefined. Users then would have to know the password when accessing the storage provider.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>The name of the provider that is displayed in the Sophos Secure Workspace app.</td>
</tr>
</tbody>
</table>
| **Server**    | In this field, enter:  
  - The URL of the root folder on the Corporate Documents WebDAV server.  
  - The URL of the root folder on the WebDAV server.  
  Use the following format: https://server.company.com  
  Only the https protocol is supported. |
| **User name** | The user name for the relevant server. You can also use the %USERNAME% variable. |
| **Password**  | The password for the relevant account. |
| **Upload folder** | The upload folder for the relevant account. |

**Other settings**

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable Documents</strong></td>
<td>This turns on the Documents feature to securely distribute company documents.</td>
</tr>
</tbody>
</table>
| **Passphrase complexity** | The required minimum complexity of passphrases for encryption keys. More secure passphrases are always allowed.  
  You can select the following settings:  
  - 4 char password  
  - 6 char password  
  - 8 char password  
  - 10 char password |
| **Deny screenshots**  | Users can't take screenshots that show the Sophos Secure Workspace app.      |
15.15.4 Corporate Browser configuration (Android Sophos container policy)

With the Corporate Browser configuration you define settings for the Corporate Browser feature of the Sophos Secure Workspace app.

The Corporate Browser allows you to securely access corporate intranet pages and other allowed pages. You can define domains and bookmarks within a domain.

Every bookmarks belongs to a certain domain. When you add a bookmark, the domain entry is created automatically if it does not exist.

General settings

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny screenshots</td>
<td>Users can’t take screenshots that show the Sophos Secure Workspace app.</td>
</tr>
</tbody>
</table>

Domain settings

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>The domain that you want to allow.</td>
</tr>
<tr>
<td>Allow copy/paste</td>
<td>Users can copy and paste text from the Corporate Browser to other apps.</td>
</tr>
<tr>
<td>Allow open with</td>
<td>Users can download attachments or pass them on to other apps.</td>
</tr>
<tr>
<td>Allow save password</td>
<td>Users can save their passwords in the Corporate Browser.</td>
</tr>
</tbody>
</table>

Bookmark settings

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name for the bookmark.</td>
</tr>
<tr>
<td>URL</td>
<td>The web address for the bookmark.</td>
</tr>
</tbody>
</table>
15.15.5 Client certificate configuration (Android Sophos container policy)

With the Client certificate configuration you install a client certificate onto devices. This certificate will be available to the Sophos Secure Email and Sophos Secure Workspace apps if they are installed in the Sophos container.

In the File field, navigate to the relevant certificate and click Upload a file. The name of the certificate is shown in the Certificate name field. Enter the password for the selected certificate.

Note
The certificate you upload here is only available for this policy. If you require certificates in other profiles or policies, you have to upload them again.

15.15.6 Root certificate configuration (Android Sophos container policy)

With the Root certificate configuration you install a root certificate onto devices. This certificate will be available to the Sophos Secure Email and Sophos Secure Workspace apps if they are installed in the Sophos container.

In the File field, navigate to the relevant certificate and click Upload a file. The name of the certificate is shown in the Certificate name field. Enter the password for the selected certificate.

Note
The certificate you upload here is only available for this policy. If you require certificates in other profiles or policies, you have to upload them again.

15.15.7 SCEP configuration (Android Sophos container policy)

With the SCEP configuration you enable devices to request certificates from a Certificate Authority using the Simple Certificate Enrollment Protocol (SCEP). These certificates are available to the Sophos Secure Workspace app if it is installed in the Sophos container.

Note
You must first add a Root certificate configuration to upload the CA certificate of the SCEP server before you can add a SCEP configuration.
<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>URL</strong></td>
<td>The web address of the Certificate Authority server. Use the variable <code>%_SCEPPROXYURL_%</code> to refer to the server URL that is configured on the <strong>SCEP</strong> tab of the <strong>System setup</strong> page.</td>
</tr>
<tr>
<td><strong>Alias name</strong></td>
<td>The name under which the certificate will appear in selection dialogs. This should be a memorable name to identify the certificate. For example, use the same value as in the <strong>Subject</strong> field, but without the CN= prefix.</td>
</tr>
<tr>
<td><strong>Subject</strong></td>
<td>The name of the entity (for example person or device) that will receive the certificate. You can use placeholders for user data or device properties. The value that you enter (with placeholders replaced by the actual data) must be a valid X.500 name. For example:</td>
</tr>
<tr>
<td></td>
<td>• Enter CN=%<em>USERNAME</em>% to specify a user.</td>
</tr>
<tr>
<td></td>
<td>• Enter CN=%<em>DEVPROP(serial_number)</em>% to specify a device.</td>
</tr>
<tr>
<td></td>
<td>For information on available placeholders, see <strong>Placeholders in profiles and policies</strong> (page 81).</td>
</tr>
<tr>
<td><strong>Type of Subject Alternative Name</strong></td>
<td>To add a <strong>Subject Alternative Name</strong> (SAN) to the SCEP configuration, select the SAN type and then enter the SAN value. SAN types are:</td>
</tr>
<tr>
<td><strong>Value of Subject Alternative Name</strong></td>
<td>• <strong>RFC 822 name</strong>: A valid email address.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DNS name</strong>: The DNS name of the CA server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Uniform resource identifier</strong>: The fully qualified URL of the CA server.</td>
</tr>
<tr>
<td><strong>AD user logon name</strong></td>
<td>The <strong>User logon name</strong> value set in Active Directory, i.e. the user’s <strong>User Principal Name</strong> (UPN).</td>
</tr>
<tr>
<td><strong>Challenge</strong></td>
<td>The web address to obtain a challenge password from the SCEP server. Use the variable <code>%_CACHALLENGE_%</code> to refer to the challenge URL that is configured on the <strong>SCEP</strong> tab of the <strong>System setup</strong> page.</td>
</tr>
</tbody>
</table>

136 Copyright © 2018 Sophos Limited
## Setting/Field | Description
---|---
**Root certificate** | The CA certificate. Select the certificate from the list. The list contains all certificates that you have uploaded in *Root certificate* configurations of the current profile.

**Key size** | The size of the public key in the issued certificate. Make sure that the value matches the size configured on the SCEP server.

**Use as digital signature** | If you select this check box, the public key can be used as a digital signature.

**Use for encryption** | If you select this check box, the public key can be used for data encryption.

### 15.16 Configurations for Mobile Security policies

With a Mobile Security policy you configure settings that are related to the Sophos Mobile Security app.

For detailed information on Mobile Security policies, see these sections:
- Configure antivirus settings for Sophos Mobile Security [page 283]
- Configure web filtering settings for Sophos Mobile Security [page 284]

### 15.17 Configurations for Knox container profiles

With a Knox container profile you configure settings that are related to the Knox container of Samsung devices.

For information on how to create a Knox container profile, see Create profile or policy [page 77].

#### 15.17.1 Password policies configuration (Knox container profile)

With the *Password policies* configuration you define requirements for the Knox container password.

**Note**

The settings supported may depend on the version of the operating system or on other device features. The scope is indicated by a blue label in Sophos Mobile.

**Password type**

In the *Password type* list, select the type of password users are allowed to configure.
<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pattern, PIN or password</td>
<td>Users must set a screen lock. They can choose a type Pattern, PIN or Password screen lock. No additional restrictions are imposed.</td>
</tr>
<tr>
<td>Simple password</td>
<td>Users must set a Password screen lock. Digits are allowed, but the password must contain at least one letter. You can define a minimum length. See the following table.</td>
</tr>
<tr>
<td>PIN or password</td>
<td>Users must set a PIN or Password screen lock. You can define a minimum length. See the following table.</td>
</tr>
<tr>
<td>Alphanumeric password</td>
<td>Users must set a Password screen lock. The password must contain both letters and digits. You can define a minimum length. See the following table.</td>
</tr>
<tr>
<td>Complex password</td>
<td>Users must set a Password screen lock. The password must contain both letters and digits. You can define a minimum length and a minimum number of digits, lowercase and uppercase letters and special characters. See the following two tables.</td>
</tr>
</tbody>
</table>

If you select Simple password, PIN or password, Alphanumeric password or Complex password, the following fields are displayed:

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum password length</td>
<td>The minimum number of characters a password must contain.</td>
</tr>
<tr>
<td>Maximum idle time before password prompt</td>
<td>The time after the Knox container is locked if it has not been used. The container can be unlocked by entering the password.</td>
</tr>
</tbody>
</table>

**Note**

The device might impose a shorter time period than what you configure here.

<table>
<thead>
<tr>
<th>Maximum password age in days</th>
<th>Requires users to change their password in the specified interval. Value range: 0 (no password change required) to 730 days.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of failed attempts until device wipe</td>
<td>The number of failed attempts to enter the correct password before the Knox container is wiped.</td>
</tr>
</tbody>
</table>

138 Copyright © 2018 Sophos Limited
<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Minimum history length</strong></td>
<td>The number of old passwords that are remembered and compared with new ones. When the user defines a new password, it is not accepted if it matches a previously used password. Value range: 1 to 5 or none.</td>
</tr>
</tbody>
</table>

If you select **Complex password**, the following additional fields are displayed:

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Minimum number of letters</strong></td>
<td>The minimum number of letters a password must contain.</td>
</tr>
<tr>
<td><strong>Minimum number of lowercase letters</strong></td>
<td>The minimum number of lowercase letters a password must contain.</td>
</tr>
<tr>
<td><strong>Minimum number of uppercase letters</strong></td>
<td>The minimum number of uppercase letters a password must contain.</td>
</tr>
<tr>
<td><strong>Minimum number of non-alphabetic characters</strong></td>
<td>The minimum number of non-alphabetic characters (for example &amp; or !) a password must contain.</td>
</tr>
<tr>
<td><strong>Minimum number of digits</strong></td>
<td>The minimum number of numerals a password must contain.</td>
</tr>
<tr>
<td><strong>Minimum number of special characters</strong></td>
<td>The minimum number of special characters (for example !&quot;$%&amp;/()=,-;:_@&lt;&gt; ) a password must contain.</td>
</tr>
</tbody>
</table>

**Biometric authentication**

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allow fingerprint authentication</strong></td>
<td>If supported by the device, the user can use fingerprint authentication to unlock the Knox container.</td>
</tr>
<tr>
<td><strong>Allow iris authentication</strong></td>
<td>If supported by the device, the user can use iris authentication to unlock the Knox container.</td>
</tr>
<tr>
<td><strong>Allow face authentication</strong></td>
<td>If supported by the device, the user can use face authentication to unlock the Knox container.</td>
</tr>
</tbody>
</table>
15.17.2 Restrictions configuration (Knox container profile)

With the Restrictions configuration you configure restrictions and related settings for the Knox container of Samsung devices.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow screen capture</td>
<td>Users can capture the screen content of apps inside the Samsung Knox container.</td>
</tr>
<tr>
<td>Allow camera</td>
<td>Apps inside the Samsung Knox container can access the camera.</td>
</tr>
<tr>
<td>Allow clipboard</td>
<td>Users can copy any contents to the clipboard.</td>
</tr>
<tr>
<td>Allow &quot;Share via&quot;</td>
<td>The Share via feature that certain apps use is turned on.</td>
</tr>
<tr>
<td>Allow microphone</td>
<td>Apps inside the Samsung Knox container can access the microphone.</td>
</tr>
<tr>
<td>Enforce the use of the secure keypad</td>
<td>Users must use the secure keypad.</td>
</tr>
<tr>
<td>Allow addition of new email accounts</td>
<td>Users can add email accounts beyond the accounts that are configured by a Sophos Mobile profile.</td>
</tr>
<tr>
<td>Allow data export</td>
<td>Private apps can access data from within the Samsung Knox container.</td>
</tr>
<tr>
<td>Allow copying files into the container</td>
<td>Private files can be copied or moved into the Samsung Knox container.</td>
</tr>
<tr>
<td>Allow Bluetooth</td>
<td>Apps inside the Samsung Knox container can use Bluetooth connections.</td>
</tr>
<tr>
<td>Allow NFC</td>
<td>Apps inside the Samsung Knox container can use NFC (near-field communication) connections.</td>
</tr>
<tr>
<td>Enforce multi-factor authentication</td>
<td>More than one authentication method is required to unlock the Samsung Knox container, for example password and fingerprint.</td>
</tr>
<tr>
<td>Allowed apps / Forbidden apps</td>
<td>You can configure either Allowed apps or Forbidden apps. Select the desired option from the first list and then select the app group containing the apps that should be allowed or forbidden from the second list. App installations initiated by the Sophos Mobile server are not restricted by this setting. For information on creating app groups, see App groups (page 261).</td>
</tr>
</tbody>
</table>
### 15.17.3 Exchange account configuration (Knox container profile)

With the Exchange account configuration you set up a connection to a Microsoft Exchange Server email server. These settings are applied to the Samsung Knox container.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Account name</strong></td>
<td>The account name.</td>
</tr>
<tr>
<td><strong>Exchange server</strong></td>
<td>The Exchange server address.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If you use the Sophos Mobile EAS proxy, enter the URL of the EAS proxy server.</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>The domain for this account.</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>The user for this account.</td>
</tr>
<tr>
<td></td>
<td>If you enter the variable <code>%USERNAME%</code>, the server replaces it with the actual user name.</td>
</tr>
<tr>
<td><strong>Email address</strong></td>
<td>The email address of the account.</td>
</tr>
<tr>
<td></td>
<td>If you enter the variable <code>%EMAILADDRESS%</code>, the server replaces it with the actual email address.</td>
</tr>
<tr>
<td><strong>Sender</strong></td>
<td>A sender name for this account.</td>
</tr>
<tr>
<td></td>
<td>If you enter the variable <code>%EMAILADDRESS%</code>, the server replaces it with the actual email address.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The password for this account.</td>
</tr>
<tr>
<td></td>
<td>If you leave this field empty, users must enter the password on their devices.</td>
</tr>
<tr>
<td><strong>Synchronization period</strong></td>
<td>The time period used for synchronizing emails.</td>
</tr>
<tr>
<td></td>
<td>Only the emails from within the specified period are synchronized to the inbox on the managed device.</td>
</tr>
<tr>
<td><strong>Synchronization interval</strong></td>
<td>The interval between email synchronization processes.</td>
</tr>
<tr>
<td><strong>SSL/TLS</strong></td>
<td>The connection to the Exchange server is secured by SSL or TLS (depending on what the server supports).</td>
</tr>
<tr>
<td></td>
<td>We recommend that you select this check box.</td>
</tr>
</tbody>
</table>
### 15.18 Configurations for Android Things policies

With an Android Things policy you configure various aspects of Android Things devices. Currently, only Wi-Fi settings are supported.

For information on how to create an Android Things policy, see Create profile or policy (page 77).

#### 15.18.1 Wi-Fi configuration (Android Things policy)

With the Wi-Fi configuration you specify settings for connecting to Wi-Fi networks.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
<td>The ID of the Wi-Fi network.</td>
</tr>
<tr>
<td>Security type</td>
<td>The security type of the Wi-Fi network:</td>
</tr>
<tr>
<td></td>
<td>- None</td>
</tr>
<tr>
<td></td>
<td>- WEP</td>
</tr>
<tr>
<td></td>
<td>- WPA/WPA2</td>
</tr>
<tr>
<td></td>
<td>If you select WEP or WPA/WPA2, a Password field is displayed. Enter the relevant password.</td>
</tr>
</tbody>
</table>

### 15.19 Configurations for iOS device profiles

With an iOS device profile you configure various aspects of iOS devices, like password policies, restrictions or Wi-Fi settings.

For information on how to create a device profile, see Create profile or policy (page 77).
### 15.19.1 Password policies configuration (iOS device profile)

With the Password policies configuration you define requirements for the device password.

**Note**

When the Password policies configuration is assigned to a device, a grace period of 60 minutes starts. Within the grace period, the user is asked to change the password when they return to the Home screen to comply with the policies. After the grace period, the user may not start any apps on the device, including internal apps.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow simple value</td>
<td>Users are allowed to use sequential or repeated characters in their password, for example 1111 or abcde.</td>
</tr>
<tr>
<td>Require alphanumeric value</td>
<td>Passwords must contain at least one letter or number.</td>
</tr>
<tr>
<td>Minimum password length</td>
<td>Specifies the minimum number of characters a password must contain.</td>
</tr>
<tr>
<td>Minimum number of complex characters</td>
<td>Specifies the minimum number of non-alphanumeric characters (for example &amp; or !) a password must contain.</td>
</tr>
<tr>
<td>Maximum password age in days</td>
<td>Requires users to change their password in the specified interval. Value range: 0 (no password change required) to 730 days.</td>
</tr>
<tr>
<td>Maximum Auto-Lock (in minutes)</td>
<td>In this field, you can specify the maximum value the user is allowed to configure on the device. Auto-Lock specifies how soon (in minutes) the device will be locked if it has not been used.</td>
</tr>
<tr>
<td>Password history</td>
<td>In this field, you can specify how many old passwords are remembered and compared with new ones. When the user defines a new password, it is not accepted if it matches a previously used password. Value range: 1 to 50 or 0 (no password history).</td>
</tr>
<tr>
<td>Maximum grace period for device lock</td>
<td>In this field, you can specify the maximum value the user is allowed to configure on the device. The grace period for device lock specifies for how long the device can be unlocked after a lock without a password prompt. If you select None, the user can select any of the intervals available. If you select Immediately, users must enter a password every time they unlock their devices.</td>
</tr>
</tbody>
</table>
Number of failed attempts until device wipe

In this field, you can specify the number of failed attempts to enter the correct password before the device is wiped. After six failed attempts, a time delay is imposed before a password can be entered again. The delay increases with each failed attempt. After the final failed attempt, all data and settings are securely removed from the device. The time delay starts after the sixth attempt. So if you set this value to 6 or lower, no delay is imposed and the device is wiped when the attempt limit is exceeded.

15.19.2 Restrictions configuration (iOS device profile)

With the Restrictions configuration you define restrictions for devices.

Note
Some options are only available for certain versions of iOS or for supervised devices. This is indicated by blue labels in Sophos Mobile Admin.

Device

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow app installation</td>
<td>If the check box is cleared, the App Store is unavailable and its icon is removed from the Home screen. Users cannot install or update apps from the App Store, iTunes or Apple Configurator.</td>
</tr>
<tr>
<td>Allow app installation from device UI</td>
<td>If the check box is cleared, the App Store is unavailable and its icon is removed from the Home screen. Users can still install or update apps from iTunes or Apple Configurator.</td>
</tr>
<tr>
<td>Allow use of camera</td>
<td>If the check box is cleared, the camera is unavailable and the Camera icon is removed from the Home screen. Users cannot take pictures, record videos, or use FaceTime.</td>
</tr>
<tr>
<td>Allow FaceTime</td>
<td>Users can place or receive FaceTime video calls.</td>
</tr>
<tr>
<td>Allow screen capture</td>
<td>Users can take a screenshot of the display.</td>
</tr>
<tr>
<td>Allow automatic sync while roaming</td>
<td>If the check box is cleared, devices that are roaming will only sync when the user accesses an account.</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allow Siri</td>
<td>If the check box is cleared, users cannot use Siri, voice commands, or dictation.</td>
</tr>
<tr>
<td>Allow Siri while device is locked</td>
<td>If the check box is cleared, users must unlock their devices by entering their password before they use Siri.</td>
</tr>
<tr>
<td>Allow Siri querying content from the web</td>
<td>If the check box is cleared, Siri does not query content from the web.</td>
</tr>
<tr>
<td>Force Siri explicit language filter</td>
<td>If the check box is cleared, the Siri filter for explicit language is not enforced on the device.</td>
</tr>
<tr>
<td>Allow voice dialing while device is locked</td>
<td>If the check box is cleared, users cannot dial by using voice commands when the device is locked by a password.</td>
</tr>
<tr>
<td>Note</td>
<td>If the user has not configured a device password, voice dialing is always allowed.</td>
</tr>
<tr>
<td>Allow Passbook while device is locked</td>
<td>Passbook notifications are displayed when the device is locked.</td>
</tr>
<tr>
<td>Allow in-app purchase</td>
<td>Users can make in-app purchases.</td>
</tr>
<tr>
<td>Force user to enter store password for all purchases</td>
<td>Users must enter their Apple ID password to make any purchase. If the check box is cleared, there is a brief grace period during which users can make subsequent purchases without having to enter their password again.</td>
</tr>
<tr>
<td>Allow multiplayer gaming</td>
<td>Users can play multi-player games in Game Center.</td>
</tr>
<tr>
<td>Allow Game Center</td>
<td>If the check box is cleared, Game Center is unavailable.</td>
</tr>
<tr>
<td>Allow adding Game Center friends</td>
<td>Users can add friends in Game Center.</td>
</tr>
<tr>
<td>Allow find my friends modification</td>
<td>If the check box is cleared, modifications to the Find my Friends app are unavailable.</td>
</tr>
<tr>
<td>Allow host pairing</td>
<td>If the check box is cleared, host pairing is turned off with the exception of the supervision host. If no supervision host certificate is configured, all pairing is turned off.</td>
</tr>
<tr>
<td>Allow pairing with Apple Watch</td>
<td>If the check box is cleared, users cannot pair the device with an Apple Watch. Any currently paired Apple Watch is unpaired.</td>
</tr>
<tr>
<td>Allow AirDrop</td>
<td>Content sharing with AirDrop is turned on.</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allow Control Center on lock screen</td>
<td>If the check box is cleared, the Control Center is unavailable when the device screen is locked.</td>
</tr>
<tr>
<td>Allow Notification Center on lock screen</td>
<td>If the check box is cleared, the Notification Center is unavailable when the device screen is locked.</td>
</tr>
<tr>
<td>Allow Today view on lock screen</td>
<td>If the check box is cleared, the Today view is unavailable when the device screen is locked.</td>
</tr>
<tr>
<td>Allow News</td>
<td>The News app is available.</td>
</tr>
<tr>
<td>Allow over-the-air PKI updates</td>
<td>Over-the-air PKI updates are possible.</td>
</tr>
<tr>
<td>Allow iBooks Store</td>
<td>Users can purchase books in iBooks.</td>
</tr>
<tr>
<td>Allow explicit sexual content in iBooks Store</td>
<td>If the check box is cleared, explicit sexual content through iBooks Store is blocked.</td>
</tr>
<tr>
<td>Allow user to install configuration profiles</td>
<td>Users can install configuration profiles.</td>
</tr>
<tr>
<td>Allow iMessage</td>
<td>Users can use iMessage to send or receive text messages.</td>
</tr>
<tr>
<td>Allow app removal</td>
<td>Users can remove apps from the device.</td>
</tr>
<tr>
<td>Allow erase all contents and settings</td>
<td>If the check box is cleared, the Erase all Content And Settings option in the Reset UI is unavailable.</td>
</tr>
<tr>
<td>Allow internet search result for Spotlight</td>
<td>If the check box is cleared, Spotlight does not return internet search results.</td>
</tr>
<tr>
<td>Allow enabling of restrictions option</td>
<td>If the check box is cleared, the Enable Restrictions option in the Reset UI is unavailable.</td>
</tr>
<tr>
<td>Allow Handoff</td>
<td>Users can use the Apple Continuity feature Handoff. With Handoff, users can start to work on a document, email or message on one device and continue from another device.</td>
</tr>
<tr>
<td>Allow device name modification</td>
<td>Users can change the device name.</td>
</tr>
<tr>
<td>Allow wallpaper modification</td>
<td>Users can change the wallpaper.</td>
</tr>
<tr>
<td>Allow keyboard shortcuts</td>
<td>Users can use keyboard shortcuts.</td>
</tr>
<tr>
<td>Allow dictation for keyboard input</td>
<td>Users can turn on dictation in the keyboard settings.</td>
</tr>
<tr>
<td>Allow automatic app download</td>
<td>If the check box is cleared, the automatic downloading of apps purchased on other devices is turned off. This does not affect updates to existing apps.</td>
</tr>
</tbody>
</table>
### Sophos Mobile on Premise

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Apple Music</td>
<td>Users can access the Apple Music library.</td>
</tr>
<tr>
<td>Allow Apple Music Radio</td>
<td>Users can access Apple Music Radio.</td>
</tr>
<tr>
<td>Allow modification of Bluetooth settings</td>
<td>Users can modify the Bluetooth settings.</td>
</tr>
</tbody>
</table>

### Company data

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Allow documents to be shared only within managed apps/accounts | This restricts the opening of documents with apps or accounts managed by Sophos Mobile, for example a corporate email account.  
If users have an email account managed by Sophos Mobile and apps managed by Sophos Mobile on their devices, attachments from the managed email account can only be opened with managed apps.  
In this way you can prevent corporate documents from being opened in unmanaged apps. |
| Allow documents to be shared only within unmanaged apps/accounts | This restricts the opening of documents with apps/accounts not managed by Sophos Mobile, for example a private email account.  
If users have an email account and apps not managed by Sophos Mobile on their devices, attachments from the unmanaged email account can only be opened with unmanaged apps.  
In this way you can prevent personal documents from being opened in managed apps. |
| Force AirDrop documents to be used as unmanaged documents | AirDrop is considered an unmanaged drop target.                              |
| Allow managed apps to sync with iCloud            | Managed apps can use iCloud synchronization.                                 |
| Allow backup for enterprise books                  | Enterprise books are backed up.                                              |
| Allow enterprise books notes and highlights sync   | Enterprise books notes and highlights are synchronized.                      |
## Applications

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow use of the iTunes Store</td>
<td>If the check box is cleared, the iTunes Store is unavailable and its icon is removed from the Home screen. Users cannot preview, purchase or download content.</td>
</tr>
<tr>
<td>Allow use of Safari</td>
<td>If the check box is cleared, the Safari web browser is unavailable and its icon is removed from the Home screen. This also prevents users from opening Web Clips.</td>
</tr>
<tr>
<td>Enable auto-fill</td>
<td>If the check box is cleared, Safari does not auto-fill web forms with previously entered information.</td>
</tr>
<tr>
<td>Force fraud warning</td>
<td>The Safari security setting to warn the user when they visit a suspected phishing website is always turned on.</td>
</tr>
<tr>
<td>Block pop-ups</td>
<td>The Safari pop-up blocker is turned on.</td>
</tr>
<tr>
<td>Allow JavaScript in browser</td>
<td>Web pages can execute JavaScript code on the device.</td>
</tr>
<tr>
<td>Accept cookies</td>
<td>In this field, you specify if Safari accepts cookies. When you allow cookies, you can specify if only cookies from the current site, from previously visited sites, or from all sites are accepted.</td>
</tr>
<tr>
<td>Allow modification of cellular data usage per app</td>
<td>Users can change the cellular data usage per app.</td>
</tr>
<tr>
<td>Allowed apps / Forbidden apps</td>
<td>You can specify either Allowed apps or Forbidden apps. Select the desired option from the first list and then select the app group containing the apps that should be allowed or forbidden from the second list. For information on creating app groups, see App groups (page 261).</td>
</tr>
</tbody>
</table>

## iCloud

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow backup</td>
<td>Users can back up their devices to iCloud.</td>
</tr>
<tr>
<td>Allow document sync</td>
<td>Users can store documents and app configuration data in iCloud.</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Allow Photo Stream</strong></td>
<td>Users can upload photos to My Photo Stream.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If you clear the check box to forbid My Photo Stream, this also removes existing photos shared via My Photo Stream from all devices. If there are no other copies of these photos, they are lost.</td>
</tr>
<tr>
<td><strong>Allow iCloud Photo Library</strong></td>
<td>Users can use iCloud Photo Library.</td>
</tr>
<tr>
<td><strong>Allow shared photo streams</strong></td>
<td>Users can invite others to view their photo streams and can view photo streams shared by others.</td>
</tr>
<tr>
<td><strong>Allow iCloud Keychain sync</strong></td>
<td>Users can use iCloud Keychain to synchronize passwords across their iPhones, iPads, and Macs. If the check box is cleared, iCloud Keychain data is only stored locally on the device.</td>
</tr>
</tbody>
</table>

**Security and privacy**

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allow diagnostic data to be sent to Apple</strong></td>
<td>If the check box is cleared, iOS diagnostic information is not sent to Apple.</td>
</tr>
<tr>
<td><strong>Allow user to accept untrusted TLS certificates</strong></td>
<td>If the check box is cleared, users are not asked if they want to trust certificates that cannot be verified. This setting applies to Safari and to Mail contacts and Calendar accounts.</td>
</tr>
<tr>
<td><strong>Trust enterprise apps</strong></td>
<td>Enterprise apps are trusted.</td>
</tr>
<tr>
<td><strong>Allow password modification</strong></td>
<td>Users can add, change or remove the device password.</td>
</tr>
<tr>
<td><strong>Allow account modification</strong></td>
<td>If the check box is cleared, users cannot modify accounts. The Accounts menu is unavailable.</td>
</tr>
<tr>
<td><strong>Allow Touch ID to unlock device</strong></td>
<td>If the check box is cleared, the device can't be unlocked by Touch ID.</td>
</tr>
<tr>
<td><strong>Force limit ad-tracking</strong></td>
<td>Anonymous user data apps used for targeting ads are no longer provided.</td>
</tr>
<tr>
<td><strong>Force encrypted backups</strong></td>
<td>Users must encrypt backups in iTunes.</td>
</tr>
<tr>
<td><strong>Force configured Wi-Fi networks</strong></td>
<td>Devices can only connect to Wi-Fi networks that have been configured by a Sophos Mobile profile.</td>
</tr>
</tbody>
</table>
Content ratings

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow explicit music and podcasts</td>
<td>If the check box is cleared, explicit music or video content is hidden in the iTunes Store. Explicit content is flagged by content providers, for example record labels, when listed on the iTunes Store.</td>
</tr>
</tbody>
</table>

15.19.3 Roaming/Hotspot configuration (iOS device profile)

With the Roaming/Hotspot configuration you define settings for roaming and personal hotspots.

**Note**

Users can change these settings on their devices anytime.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable voice roaming</td>
<td>Voice roaming is available.</td>
</tr>
<tr>
<td>Enable data roaming</td>
<td>Data roaming is available.</td>
</tr>
<tr>
<td>Enable personal hotspot</td>
<td>The user can configure the device to serve as a personal hotspot.</td>
</tr>
</tbody>
</table>

15.19.4 Exchange account configuration (iOS device profile)

With the Exchange account configuration you set up a connection to a Microsoft Exchange Server email server.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account name</td>
<td>The account name.</td>
</tr>
<tr>
<td>Exchange server</td>
<td>The Exchange server address.</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain for this account.</td>
</tr>
</tbody>
</table>

**Note**

If you use the Sophos Mobile EAS proxy, enter the URL of the EAS proxy server.
<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>The user for this account. If you enter the variable <code>%_USERNAME_%</code>, the server replaces it with the actual user name.</td>
</tr>
<tr>
<td>Email address</td>
<td>The email address of the account. If you enter the variable <code>%_EMAILADDRESS_%</code>, the server replaces it with the actual email address.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for this account. If you leave this field empty, users must enter the password on their devices.</td>
</tr>
<tr>
<td>Synchronization period</td>
<td>The time period used for synchronizing emails. Only the emails from within the specified period are synchronized to the inbox on the managed device.</td>
</tr>
<tr>
<td>SSL/TLS</td>
<td>The connection to the Exchange server is secured by SSL or TLS (depending on what the server supports). We recommend that you select this check box.</td>
</tr>
<tr>
<td>Allow move</td>
<td>Users can move emails from this account to another. This also allows users to use a different account when replying to or forwarding a message from this account.</td>
</tr>
<tr>
<td>Allow recent address syncing</td>
<td>The account is included in the syncing of recently used addresses with other devices using iCloud.</td>
</tr>
<tr>
<td>Use in Mail only</td>
<td>The account can only be used to send messages from the Mail app. It cannot be selected as a sending account for messages created with other apps, for example Photos or Safari.</td>
</tr>
<tr>
<td>Identity certificate</td>
<td>Select the identity certificate for the connection to the Exchange server. The list includes all certificates from Client certificate configurations of the current profile.</td>
</tr>
<tr>
<td>Enable S/MIME</td>
<td>Support the S/MIME encryption standard.</td>
</tr>
<tr>
<td>Signing certificate</td>
<td>The certificates that are used for email signing and encryption. To select a certificate, you must first upload it in a Client certificate configuration of the current profile.</td>
</tr>
</tbody>
</table>
**Sophos Mobile on Premise**

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow user to send unencrypted emails</td>
<td>For each outgoing email, the user can choose to encrypt it or not.</td>
</tr>
</tbody>
</table>

**15.19.5 Wi-Fi configuration (iOS device profile)**

With the Wi-Fi configuration you specify settings for connecting to Wi-Fi networks.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
<td>The ID of the Wi-Fi network.</td>
</tr>
<tr>
<td>Connect automatically</td>
<td>Automatically connect to the target network.</td>
</tr>
<tr>
<td>Hidden network</td>
<td>The target network is not open or visible.</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Security type | The security type of the Wi-Fi network:  
  - None  
  - WEP (Personal)  
  - WPA/WPA2 (Personal)  
  - Any (Personal)  
  - WEP (Enterprise)  
  - WPA/WPA2 (Enterprise)  
  - Any (Enterprise)  
  
If you select a type with *Personal* in its name, a **Password** field is displayed. Enter the relevant password.  
If you select a type with *Enterprise* in its name, the tabs **Protocols**, **Authentication** and **Trust** are displayed.  
On the **Protocols** tab configure the following:  
  - Under **Accepted EAP types**, specify the EAP methods to be used for authentication. Depending on the types selected on this tab, the values in the **Internal identity** field on this tab become available for selection.  
  - Under **EAP-FAST**, configure the EAP-FAST Protected Access credential settings.  
On the **Authentication** tab, configure client authentication settings:  
  - In the **User** field, enter the user name for the connection to the Wi-Fi network.  
  - Select **Require password on each connect**, if the password is to be queried for each connection and transferred with the authentication.  
  - In the **Password** field, enter the relevant password.  
  - In the **Identity certificate** list, select the certificate for the connection to the Wi-Fi network.  

**Note**  
The certificate to be used has to be specified in a **Client certificate** configuration.  

- In the **External identity** field, enter the externally visible ID (for TTLS, PEAP and EAP-FAST).  
On the **Trust** tab, configure server authentication settings:  
Select the trusted certificates from the list.  

**Note**  
You must specify the certificates in a **Root certificate** configuration.
### Proxy

In this list, select the proxy settings for the Wi-Fi connection:

- **None**
- **Manually**
- **Automatic**

If you select **Manually**, the fields **Server and port**, **Authentication** and **Password** are displayed. Enter the required proxy information. If you select **Automatic**, the field **Proxy server URL** is displayed. Enter the URL of the proxy server.

### 15.19.6 VPN configuration (iOS device profile)

With the **VPN** configuration you define VPN settings for network connections.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connection name</strong></td>
<td>The name of the connection shown on the device.</td>
</tr>
<tr>
<td><strong>Connection type</strong></td>
<td>The type of the VPN connection:</td>
</tr>
<tr>
<td></td>
<td>- Cisco AnyConnect</td>
</tr>
<tr>
<td></td>
<td>- Cisco Legacy AnyConnect</td>
</tr>
<tr>
<td></td>
<td>- IPsec (Cisco)</td>
</tr>
<tr>
<td></td>
<td>- F5</td>
</tr>
<tr>
<td></td>
<td>- Check Point</td>
</tr>
<tr>
<td></td>
<td>- Custom SSL/TLS</td>
</tr>
<tr>
<td></td>
<td>Different entry fields are shown on the <strong>VPN</strong> page depending on the connection type you select here.</td>
</tr>
<tr>
<td><strong>Identifier (reverse DNS format)</strong></td>
<td>The custom identifier in reverse DNS format.</td>
</tr>
<tr>
<td><strong>Server</strong></td>
<td>The host name or the IP address of the server.</td>
</tr>
<tr>
<td><strong>Account</strong></td>
<td>The user account for the authentication of the connection.</td>
</tr>
<tr>
<td><strong>Third-party settings</strong></td>
<td>If your vendor has specified custom connection properties, you can enter them in this field.</td>
</tr>
<tr>
<td></td>
<td>To enter a property, click <strong>Add</strong> and then enter <strong>Key</strong> and <strong>Value</strong> of the property in the dialog box.</td>
</tr>
<tr>
<td><strong>Send all traffic through VPN</strong></td>
<td>All traffic is sent through VPN.</td>
</tr>
<tr>
<td><strong>Group</strong></td>
<td>The group that may be required for the authentication of the connection.</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>User authentication</strong></td>
<td>The type of user authentication for the connection:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Password</strong></td>
</tr>
<tr>
<td></td>
<td>If you select this option, the <strong>Password</strong> field is shown below the <strong>User authentication</strong> field. Enter the password for authentication.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Certificate</strong></td>
</tr>
<tr>
<td></td>
<td>If you select this option, the <strong>Certificate</strong> field is shown below the <strong>User authentication</strong> field. Select a certificate.</td>
</tr>
<tr>
<td><strong>Device authentication</strong></td>
<td>The type of device authentication:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Keys (Shared Secret)/Group name</strong></td>
</tr>
<tr>
<td></td>
<td>If you select this option, the fields <strong>Group name</strong>, <strong>Keys (Shared Secret)</strong>, <strong>Use hybrid authentication</strong> and <strong>Request password</strong> are displayed below the <strong>Device authentication</strong> field. Enter the required authentication information in the <strong>Group name</strong> and <strong>Keys (Shared Secret)</strong> fields. Select <strong>Use hybrid authentication</strong> and <strong>Request password</strong> as required.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Certificate</strong></td>
</tr>
<tr>
<td></td>
<td>If you select this option, the fields <strong>Certificate</strong> and <strong>Including user PIN</strong> are displayed below the <strong>Device authentication</strong> field. In the <strong>Certificate</strong> list, select the required certificate. Select <strong>Including user PIN</strong> to include the user PIN in device authentication.</td>
</tr>
<tr>
<td><strong>Proxy</strong></td>
<td>The proxy settings for the connection:</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Manually</strong></td>
</tr>
<tr>
<td></td>
<td>If you select this option, the fields <strong>Server and port</strong>, <strong>Authentication</strong> and <strong>Password</strong> are displayed. In the <strong>Server and port</strong> field, enter the valid address and the port of the proxy server. In the <strong>Authentication</strong> field, enter the user name for the connection to the proxy server. In the <strong>Password</strong> field, enter the password for the connection to the proxy server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Automatic</strong></td>
</tr>
<tr>
<td></td>
<td>If you select this option, the <strong>Proxy server URL</strong> field is displayed. Enter the URL of the server with the proxy setting in this field.</td>
</tr>
</tbody>
</table>
### Setting/Field | Description
--- | ---
**Provider type** | The VPN connection type.  
- **App proxy**: Network traffic is sent through a VPN tunnel at the application layer.  
- **Packet tunnel**: Network traffic is sent through a VPN tunnel at the network layer.

### 15.19.7 Per app VPN configuration (iOS device profile)

With the **Per app VPN** configuration you define VPN settings for individual apps.

You can configure apps to automatically connect to VPN when they are started. So you can, for example, ensure that data transmitted by managed apps travels through VPN.

After you have set up per app VPN configurations, you can select a configuration on the **Edit package** page of an app. See **Configure per app VPN and settings for iOS apps** (page 259).

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connection name</strong></td>
<td>The name of the connection shown on the device.</td>
</tr>
</tbody>
</table>
| **Connection type** | The type of the VPN connection:  
- **Cisco AnyConnect**  
- **Cisco Legacy AnyConnect**  
- **F5**  
- **Check Point**  
- **Custom SSL/TLS**  
Different entry fields are shown on the **VPN** page depending on the connection type you select here. |
| **Identifier (reverse DNS format)** | The custom identifier in reverse DNS format. |
| **Server** | The host name or the IP address of the server. |
| **Account** | The user account for the authentication of the connection. |
| **Third-party settings** | If your vendor has specified custom connection properties, you can enter them in this field.  
To enter a property, click **Add** and then enter **Key** and **Value** of the property in the dialog box. |
<p>| <strong>Send all traffic through VPN</strong> | All traffic is sent through VPN. |
| <strong>Group</strong> | The group that may be required for the authentication of the connection. |</p>
<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **User authentication** | The type of user authentication for the connection:  
  • **Password**  
    If you select this option, the **Password** field is shown below the **User authentication** field. Enter the password for authentication.  
  • **Certificate**  
    If you select this option, the **Certificate** field is shown below the **User authentication** field. Select a certificate. |
| **Proxy** | The proxy settings for the connection:  
  • **None**  
  • **Manually**  
    If you select this option, the fields **Server and port**, **Authentication** and **Password** are displayed. In the **Server and port** field, enter the valid address and the port of the proxy server. In the **Authentication** field, enter the user name for the connection to the proxy server. In the **Password** field, enter the password for the connection to the proxy server.  
  • **Automatic**  
    If you select this option, the **Proxy server URL** field is displayed. Enter the URL of the server with the proxy setting in this field. |
| **Provider type** | The VPN connection type.  
  • **App proxy**: Network traffic is sent through a VPN tunnel at the application layer.  
  • **Packet tunnel**: Network traffic is sent through a VPN tunnel at the network layer. |
### Safari domains

In this field, you can enter a list of domain strings. Use a new line for each domain string.

When a domain that matches one of the domain strings is opened in Safari or another browser app, the VPN connection is triggered.

The rule matching behavior is as follows:

- Leading and trailing dots are ignored. For example, the string `.example.com` matches the same domains as the string `example.com`.
- Each string component must match a whole domain component. For example, the string `example.com` matches the domain `www.example.com`, but not `www.myexample.com`.
- Strings with a single component only match that specific domain. For example, the string `example` matches the domain `example`, but not `www.example.com`.

---

#### 15.19.8 Single sign-on configuration (iOS device profile)

With the Single sign-on configuration you define settings for a single sign-on for third-party apps.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>A human-readable name for the account.</td>
</tr>
<tr>
<td><strong>Kerberos principal name</strong></td>
<td>The Kerberos principal name. If you do not enter a value, the user must enter the name during profile installation.</td>
</tr>
<tr>
<td><strong>Realm</strong></td>
<td>The Kerberos realm name. You must enter the name in upper-case.</td>
</tr>
<tr>
<td><strong>URLs</strong></td>
<td>A list of URL prefixes that must be matched to use the account for Kerberos authentication over HTTP. Values must begin with <code>http://</code> or <code>https://</code>. If a value doesn't end with <code>/</code>, the <code>/</code> is added by Sophos Mobile. For devices with iOS 9.0 or later, you may use a single asterisk (*) to match all values. For example, <code>https://*.example.com/</code> matches <code>https://www.example.com/</code> or <code>https://m.example.com/</code>.</td>
</tr>
</tbody>
</table>
### App identifiers

A list of bundle IDs of apps. Values must be either exact matches (e.g. `com.sophos.smsec`), or prefixes, using the characters `.*` at the end of the string (e.g. `com.sophos.*`).

### 15.19.9 Single app mode configuration (iOS device profile)

With the Single app mode configuration you define settings for the operation mode that locks devices into a single app and prevents users from changing to other apps.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select source</td>
<td>Select how you want to specify the app for the single app mode:</td>
</tr>
<tr>
<td></td>
<td>• <strong>App list</strong>: Select the app from a list of all available iOS apps.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Custom</strong>: Manually enter the bundle ID of the app.</td>
</tr>
<tr>
<td>App identifier</td>
<td>The app for the single app mode. Either select an app from the list or enter a bundle ID.</td>
</tr>
<tr>
<td>Disable touchscreen</td>
<td>Touch gestures are unavailable.</td>
</tr>
<tr>
<td>Disable rotation</td>
<td>The screen does not rotate.</td>
</tr>
<tr>
<td>Disable volume buttons</td>
<td>Volume buttons are unavailable.</td>
</tr>
<tr>
<td>Disable ringer switch</td>
<td>The ringer switch is unavailable.</td>
</tr>
<tr>
<td>Disable sleep wake button</td>
<td>The wake button is unavailable.</td>
</tr>
<tr>
<td>Disable Auto-Lock</td>
<td>The Auto-Lock feature that puts the device into sleep after an idle period is turned off.</td>
</tr>
<tr>
<td>Enable VoiceOver</td>
<td>VoiceOver is available.</td>
</tr>
<tr>
<td>Enable Zoom</td>
<td>The Zoom feature is available.</td>
</tr>
<tr>
<td>Enable Invert Colors</td>
<td>The Invert Colors feature is available.</td>
</tr>
<tr>
<td>Enable AssistiveTouch</td>
<td>AssistiveTouch is available.</td>
</tr>
<tr>
<td>Enable Speak Selection</td>
<td>The Speak Selection feature is available.</td>
</tr>
<tr>
<td>Enable Mono Audio</td>
<td>The Mono Audio feature is available.</td>
</tr>
<tr>
<td>VoiceOver</td>
<td>VoiceOver adjustments are available.</td>
</tr>
</tbody>
</table>
### 15.19.10 Web Clip configuration (iOS device profile)

With the **Web Clip** configuration you define Web Clips to be added to the Home screen of user devices. Web Clips provide fast access to favorite web pages. But you can also add a Web Clip with a support phone number for example, to provide a quick way to dial the helpdesk.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>A description for the Web Clip.</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td>The web address of the Web Clip.</td>
</tr>
<tr>
<td><strong>Can be removed</strong></td>
<td>If the check box is cleared, the user cannot remove the Web Clip. It cannot be deleted from the device unless the user removes the profile that installed it.</td>
</tr>
<tr>
<td><strong>Full screen</strong></td>
<td>The Web Clip is opened full screen on the device. A full screen Web Clip opens the URL as a web app.</td>
</tr>
<tr>
<td><strong>Icon</strong></td>
<td>Select an image to be used as the Web Clip icon on the Home screen. This must be a PNG, GIF or JPEG image with a maximum file size of 1 MB. The image is cropped to a square and scaled to match the display resolution. For best results, we recommend that you use an image of size 180 px by 180 px.</td>
</tr>
</tbody>
</table>

**Note**

When a **favicon** is defined in the HTML code of the web page, the device might display that favicon as Web Clip icon. This happens for certain web pages only, depending on how the favicon is configured in the web page code.
## 15.19.11 Wallpaper configuration (iOS device profile)

With the **Wallpaper** configuration you define background images for the lock screen and/or the Home screen of iOS devices.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Apply to</strong></td>
<td>Select whether the image is used for the Lock screen, for the Home Screen, or both.</td>
</tr>
<tr>
<td><strong>Image</strong></td>
<td>Select a PNG or JPEG image with a maximum file size of 5 MB that is used for the wallpaper. iOS crops and scales the image as required. For best results, use the following image sizes (in pixels):</td>
</tr>
<tr>
<td></td>
<td>• 640 × 1136 (iPhone 5)</td>
</tr>
<tr>
<td></td>
<td>• 750 × 1334 (iPhone 6/7)</td>
</tr>
<tr>
<td></td>
<td>• 1242 × 2208 (iPhone 6/7 Plus)</td>
</tr>
<tr>
<td></td>
<td>• 1536 × 2048 (iPad, iPad mini, iPad Air)</td>
</tr>
<tr>
<td></td>
<td>• 2048 × 2732 (iPad Pro)</td>
</tr>
</tbody>
</table>

**Note**

Users can change the wallpaper at any time.

## 15.19.12 Access Point Name configuration (iOS device profile)

With the **Access Point Name** configuration you specify an Access Point Name (APN) configuration for iOS devices. APN configurations define how devices connect to a mobile network.

**Note**

The **Access Point Name** configuration is deprecated in favor of the **Cellular** configuration. See [Cellular configuration (iOS device profile) (page 166)](#).

**Important**

If these settings are not correct, the device cannot access data using the cellular network. To undo settings changes, the profile must be removed from the device.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>APN</strong></td>
<td>The APN that the device quotes when it opens a GPRS connection with the carrier. This must match an APN that the carrier accepts. Otherwise, the connection cannot be established.</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>User name for access point</td>
<td>The user name for the access point.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>iOS supports APN user names of up to 64 characters.</td>
</tr>
<tr>
<td>Password for access point</td>
<td>The password for the access point.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>iOS supports APN passwords of up to 64 characters.</td>
</tr>
<tr>
<td>Proxy server and port</td>
<td>The address and the port of the proxy server.</td>
</tr>
</tbody>
</table>

### 15.19.13 Web content filter configuration (iOS device profile)

With the **Web content filter** configuration you define blocked URLs and allowed URLs with bookmarks.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Blocked URLs</strong></td>
<td>If you select the check box, you can define a list of blocked URLs that may not be accessed on the devices.</td>
</tr>
<tr>
<td></td>
<td><strong>Click Next</strong> to display the <strong>Web content filter</strong> page. On this page, you can add individual URLs. Use a new line for each URL.</td>
</tr>
<tr>
<td><strong>Allowed URLs with bookmarks</strong></td>
<td>If you select the check box, you can define allowed URLs with bookmarks to be added to the Safari browser on the devices. All other sites are blocked.</td>
</tr>
<tr>
<td></td>
<td><strong>Click Next</strong> to display the <strong>Web content filter</strong> page. <strong>Click Add</strong> to add individual URLs as bookmarks.</td>
</tr>
<tr>
<td><strong>Block adult content</strong></td>
<td>On the <strong>Web content filter</strong> page, use this to turn on an Apple filter that blocks adult content. For example, web pages that contain swearing or sexually explicit language.</td>
</tr>
</tbody>
</table>
15.19.14 Global HTTP proxy configuration (iOS device profile)

With the Global HTTP proxy configuration you define a corporate proxy server.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Global HTTP proxy** | Select the proxy settings for the connection:  
  - **Manually**  
    If you select this option, the fields **Server and port**, **Authentication** and **Password** are displayed. In the **Server and port** field, enter the valid address and the port of the proxy server. In the **Authentication** field, enter the user name for the connection to the proxy server. In the **Password** field, enter the password for the connection to the proxy server.  
  - **Automatic**  
    If you select this option, the **Proxy server URL** field is displayed. Enter the URL of the server with the proxy setting in this field. |

15.19.15 Root certificate configuration (iOS device profile)

With the Root certificate configuration you install a root certificate onto devices.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. The name of the certificate is shown in the **Certificate name** field. Enter the password for the selected certificate.

**Note**
The certificate you upload here is only available for this profile. If you require certificates in other profiles or policies, you have to upload them again.

15.19.16 Client Certificate configuration (iOS device profile)

With the Client certificate configuration you install a client certificate onto devices.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. The name of the certificate is shown in the **Certificate name** field. Enter the password for the selected certificate.

**Note**
The certificate you upload here is only available for this profile. If you require certificates in other profiles or policies, you have to upload them again.
### 15.19.17 SCEP configuration (iOS device profile)

With the SCEP configuration you enable devices to request certificates from a Certificate Authority using the Simple Certificate Enrollment Protocol (SCEP).

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>URL</strong></td>
<td>The web address of the Certificate Authority server. Use the variable <code>%_SCEPPROXYURL_%</code> to refer to the server URL that is configured on the <strong>SCEP</strong> tab of the <strong>System setup</strong> page.</td>
</tr>
<tr>
<td><strong>CA name</strong></td>
<td>A name that is understood by the Certificate Authority. The name can, for example, be used to distinguish between instances.</td>
</tr>
</tbody>
</table>
| **Subject**           | The name of the entity (for example person or device) that will receive the certificate. You can use placeholders for user data or device properties. The value that you enter (with placeholders replaced by the actual data) must be a valid X.500 name. For example:  
  - Enter `CN=%_USERNAME_%` to specify a user.  
  - Enter `CN=%_DEVPROP(serial_number)_%` to specify a device.  
  For information on available placeholders, see [Placeholders in profiles and policies](page 81). |
| **Type of Subject Alternative Name** | To add a Subject Alternative Name (SAN) to the SCEP configuration, select the SAN type and then enter the SAN value. SAN types are:  
  - **RFC 822 name**: A valid email address.  
  - **DNS name**: The DNS name of the CA server.  
  - **Uniform resource identifier**: The fully qualified URL of the CA server. |
<p>| <strong>Value of Subject Alternative Name</strong> |                                                                                                                                                                                                              |
| <strong>AD user logon name</strong> | The User logon name value set in Active Directory, i.e. the user’s User Principal Name (UPN).                                                                                                               |
| <strong>Challenge</strong>         | The web address to obtain a challenge password from the SCEP server. Use the variable <code>%_CACHALLENGE_%</code> to refer to the challenge URL that is configured on the <strong>SCEP</strong> tab of the <strong>System setup</strong> page.                     |
| <strong>Retries</strong>           | The number of retries if the server sends a response of type <em>pending</em>.                                                                                                                                       |</p>
<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retry delay</td>
<td>The number of seconds between retries.</td>
</tr>
<tr>
<td>Key size</td>
<td>The size of the public key in the issued certificate. Make sure that the</td>
</tr>
<tr>
<td></td>
<td>value matches the size configured on the SCEP server.</td>
</tr>
<tr>
<td>Use as digital signature</td>
<td>If you select this check box, the public key can be used as a digital</td>
</tr>
<tr>
<td></td>
<td>signature.</td>
</tr>
<tr>
<td>Use for encryption</td>
<td>If you select this check box, the public key can be used for data encryption.</td>
</tr>
</tbody>
</table>

**15.19.18 Duo device certificate (iOS device profile)**

With the **Duo device certificate** configuration you enable devices to request a certificate from the Duo Security SCEP server. If this certificate is installed on a device, the **Duo Mobile** iOS app classifies the device as trusted.

The required settings are common for all Duo Security accounts. Do not change the pre-populated values.

**15.19.19 Managed domains configuration (iOS device profile)**

With the **Managed domains** configuration you define managed domains for iOS devices.

**Email domains**

Enter email domains that are managed by your organization. In the Mail app, email addresses that don’t match one of the configured domains are highlighted as out-of-domain.

**Web domains**

When web domains are managed, files downloaded from specific websites in Safari can only be opened by managed apps. For information on managed apps, see **Managed apps for iOS** (page 253).

**Note**

If a managed web domain entry contains a port number, only addresses that specify that port number will be considered managed. Otherwise, only the standard ports will be considered managed (port 80 for http and 443 for https).
15.19.20 Cellular configuration (iOS device profile)

With the Cellular configuration you define cellular network settings for iOS devices.

**Note**
A Cellular configuration cannot be installed onto a device if an Access Point Name configuration is already installed.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>PAP, CHAP</td>
</tr>
<tr>
<td>APN</td>
<td>The APN that the device quotes when it opens a GPRS connection with the carrier. This must match an APN that the carrier accepts. Otherwise, the connection cannot be established.</td>
</tr>
<tr>
<td>User name for access point</td>
<td>The user name for the access point.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> iOS supports APN user names of up to 64 characters.</td>
</tr>
<tr>
<td>Password for access point</td>
<td>The password for the access point.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> iOS supports APN passwords of up to 64 characters.</td>
</tr>
<tr>
<td>Proxy server and port</td>
<td>The address and the port of the proxy server.</td>
</tr>
</tbody>
</table>

15.19.21 CalDAV configuration (iOS device profile)

With the CalDAV configuration you configure the synchronization of calendar data with a CalDAV server. For example, this can be used to sync Google Calendar with an iOS device.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account name</td>
<td>The display name of the CalDAV account on the device.</td>
</tr>
</tbody>
</table>
### Setting/Field | Description
---|---
**Account host and port** | The host name or IP address and optionally the port number of the CalDAV server. For example, for Google Calendar enter: `calendar.google.com:443`  
**Principal URL** | If required by the CalDAV server, enter the principal URL of the calendar resource. For example, to sync with a calendar other than the primary calendar in a Google account, enter:  
`https://apidata.googleusercontent.com/caldav/v2/calendar_id/user`  
where `calendar_id` is the ID of the calendar you want to sync with. In the Google Calendar web application, the calendar ID is displayed in the calendar settings. See the Google Calendar help for details.  
**User name, Password** | The login credentials for the CalDAV account. For example, for Google Calendar enter the credentials of the Google account.  
**SSL/TLS** | The connection to the CalDAV server is secured by SSL or TLS (depending on what the server supports). We recommend that you select this check box.

### 15.19.22 CardDAV configuration (iOS device profile)

With the CardDAV configuration you configure the synchronization of contact data with a CardDAV server. For example, this can be used to sync Google Contacts with an iOS device.

| Setting/Field | Description |
---|---|
**Account name** | The display name of the CardDAV account on the device.  
**Account host and port** | The host name or IP address and optionally the port number of the CardDAV server. For example, for Google Contacts enter: `google.com`
### Setting/Field Description

**Principal URL**
If required by the CardDAV server, enter the principal URL of the contacts resource.
For example, the Google CardDAV API supports the following principal URL:
https://www.googleapis.com/carddav/v1/principals/account_name@gmail.com
where `account_name` is the Google account name.

**User name, Password**
The login credentials for the CardDAV account.
For example, for Google Contacts enter the credentials of the Google account.

**SSL/TLS**
The connection to the CardDAV server is secured by SSL or TLS (depending on what the server supports).
We recommend that you select this check box.

---

### 15.19.23 IMAP/POP configuration (iOS device profile)

With the **IMAP/POP** configuration you add an IMAP or POP email account to the iOS device.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Account name</strong></td>
<td>The display name of the email account on the device.</td>
</tr>
<tr>
<td><strong>Account type</strong></td>
<td>The type of the email server for incoming email (either <strong>IMAP</strong> or <strong>POP</strong>).</td>
</tr>
<tr>
<td><strong>User display name</strong></td>
<td>The display name of the user for outgoing email. Use the variable <code>%_USERNAME_%</code> to refer to the name of the user that is assigned to the device.</td>
</tr>
<tr>
<td><strong>Email address</strong></td>
<td>The email address of the account. Use the variable <code>%_EMAILADDRESS_%</code> to refer to the email address of the user that is assigned to the device.</td>
</tr>
<tr>
<td><strong>Allow move</strong></td>
<td>Users can move emails from this account to another. This also allows users to use a different account when replying to or forwarding a message from this account.</td>
</tr>
<tr>
<td><strong>Allow recent address syncing</strong></td>
<td>The account is included in the syncing for the list of recent addresses.</td>
</tr>
<tr>
<td><strong>Use in Mail only</strong></td>
<td>The account can only be used to send messages from the Mail app. It cannot be selected as a sending account for messages created with other apps, for example Photos or Safari.</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Allow Mail Drop</strong></td>
<td>Allow Apple Mail Drop for this account.</td>
</tr>
<tr>
<td><strong>Enable S/MIME</strong></td>
<td>Support the S/MIME encryption standard.</td>
</tr>
<tr>
<td><strong>Signing certificate</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Encryption certificate</strong></td>
<td>The certificates that are used for email signing and encryption.</td>
</tr>
<tr>
<td></td>
<td>To select a certificate, you must first upload it in a <strong>Client certificate</strong> configuration of the current profile.</td>
</tr>
<tr>
<td><strong>Allow user to send unencrypted emails</strong></td>
<td>For each outgoing email, the user can choose to encrypt it or not.</td>
</tr>
<tr>
<td><strong>Incoming email</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Email server and port</strong></td>
<td>The host name or IP address and the port number of the server for incoming email (inbound server).</td>
</tr>
<tr>
<td><strong>User name</strong></td>
<td>The user name for connecting to the inbound server.</td>
</tr>
<tr>
<td><strong>Authentication type</strong></td>
<td>The authentication method for connecting to the inbound server.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The password for connecting to the inbound server (if required).</td>
</tr>
<tr>
<td><strong>SSL/TLS</strong></td>
<td>The connection to the inbound server is secured by SSL or TLS (depending on what the server supports).</td>
</tr>
<tr>
<td><strong>Outgoing email</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Email server and port</strong></td>
<td>The host name or IP address and the port number of the server for outgoing email (outbound server).</td>
</tr>
<tr>
<td><strong>User name</strong></td>
<td>The user name for connecting to the outbound server.</td>
</tr>
<tr>
<td><strong>Authentication type</strong></td>
<td>The authentication method for connecting to the outbound server.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The password for connecting to the outbound server (if required).</td>
</tr>
<tr>
<td><strong>Use same password as for incoming email</strong></td>
<td>Use the password that is specified for incoming email.</td>
</tr>
<tr>
<td><strong>SSL/TLS</strong></td>
<td>The connection to the outbound server is secured by SSL or TLS (depending on what the server supports).</td>
</tr>
</tbody>
</table>
**15.19.24 Network usage rules configuration (iOS device profile)**

With the Network usage rules configuration you specify how managed apps are allowed to use cellular data networks.

**General rules**

Under Rules for all managed apps, specify the settings for managed apps in general.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow cellular data</td>
<td>Managed apps are allowed to use data communication over cellular networks.</td>
</tr>
<tr>
<td>Allow data roaming</td>
<td>Managed apps are allowed to use data communication while the device is roaming on a foreign cellular network.</td>
</tr>
</tbody>
</table>

**Exceptions**

Exceptions override the general rules. Use Add exception to define rules that are specific to an app group.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>App group</td>
<td>Select an app group that contains the managed apps to which the exception applies.</td>
</tr>
<tr>
<td>Allow cellular data</td>
<td>Managed apps from the selected app group are allowed to use data communication over cellular networks.</td>
</tr>
<tr>
<td>Allow data roaming</td>
<td>Managed apps from the selected app group are allowed to use data communication while the device is roaming on a foreign cellular network.</td>
</tr>
</tbody>
</table>

**Note**

You cannot define multiple exceptions for the same app group.

**15.20 Configurations for Sophos container policies for iOS**

With a Sophos container policy you configure settings that are related to the Sophos container apps Sophos Secure Email and Sophos Secure Workspace.

For information on how to create a Sophos container policy, see Create profile or policy (page 77).
## 15.20.1 General configuration (iOS Sophos container policy)

With the **General** configuration you define settings that apply to all Sophos container apps, if applicable.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable Sophos container password</strong></td>
<td>Users must enter an additional password to be able to start a Sophos container app. The password has to be defined when the first container app is started after the configuration has been applied. This password applies to all container apps.</td>
</tr>
<tr>
<td><strong>Password complexity</strong></td>
<td>The required minimum complexity of the Sophos container password. More secure passwords are always allowed. Passwords (a mix of numeric and alphanumeric characters) are always seen as more secure than PINs (numeric characters only).</td>
</tr>
<tr>
<td>• Any: Sophos container passwords do not have restrictions.</td>
<td></td>
</tr>
<tr>
<td>• 4 digit PIN</td>
<td></td>
</tr>
<tr>
<td>• 6 digit PIN</td>
<td></td>
</tr>
<tr>
<td>• 4 char password</td>
<td></td>
</tr>
<tr>
<td>• 6 char password</td>
<td></td>
</tr>
<tr>
<td>• 8 char password</td>
<td></td>
</tr>
<tr>
<td>• 10 char password</td>
<td></td>
</tr>
<tr>
<td><strong>Always hide characters in password entry fields</strong></td>
<td>Characters in password entry fields are not briefly displayed before they are masked.</td>
</tr>
<tr>
<td><strong>Password age in days</strong></td>
<td>The number of days that a password can be used before users are prompted to change it.</td>
</tr>
<tr>
<td><strong>Failed logins until lock</strong></td>
<td>The number of failed login attempts that are tolerated before the container apps are locked. Once they are locked an administrator needs to unlock the apps or, if allowed, users can use the Self Service Portal to do so.</td>
</tr>
<tr>
<td><strong>Allow fingerprint</strong></td>
<td>Users can use their fingerprint to unlock the app.</td>
</tr>
<tr>
<td><strong>Grace period in minutes</strong></td>
<td>The period of time within which no Sophos container password must be entered when a container app comes to the foreground again. The grace period applies to all container apps. You can switch between the apps during the grace period without entering a password.</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Lock on device lock</strong></td>
<td>When the device is locked, the Sophos container is locked as well. If the check box is cleared, the container is locked only after the grace period has expired.</td>
</tr>
</tbody>
</table>
| **Last server connect**   | The period of time within users can use a Sophos container app without a connection to the Sophos Mobile server.  
When a Sophos container app becomes active and does not have contact with the server within the defined period of time, a lock screen will be displayed. Users can only unlock the app by tapping **Retry** on the lock screen. The app will then try to connect to the server. If the connection can be established, the app will be unlocked. If not, access will be denied.  
• **On access**: Server connection is always required and the app is locked when the server cannot be reached.  
• **1 hour**: Server connection is required when the app becomes active one hour or more after the last successful server connection.  
• **3 hours**  
• **6 hours**  
• **12 hours**  
• **1 day**  
• **3 days**  
• **1 week**  
• **none**: No regular contact is required. |
### Setting/Field | Description
--- | ---
**Offline starts without server connection** | In this field you define how often users can start one of the Sophos container apps without a server connection.

**Note**
This setting requires the Sophos container password feature to be turned on.

A counter is incremented whenever users enter the Sophos container password. If the counter exceeds the defined number, the same lock screen as for the **Last server connect** setting will be displayed. The counter will be reset if a connection to the Sophos Mobile server is established.

- **Unlimited**: No server connection is required.
- **0**: Starting the app without a server connection is not possible.
- **1**: After one start of the app, a successful server connection is necessary.
- **3**
- **5**
- **10**
- **20**

**Jailbreak allowed** | Container apps are allowed to run on jailbroken devices.

**App usage constraints**
Here you can define constraints on using the Sophos container apps. Click **Add** to enter constraints.

- **Geo-fencing**
  Lets you add latitude and longitude and a radius within which the Sophos container apps can be used.

- **Time-fencing**
  Lets you specify a start and end time within which the Sophos container apps can be used. Days of the week on which the apps can be used can be specified as well.
## Sophos Mobile on Premise

**Wi-Fi fencing**

If you select **Wi-Fi connection required**, the Sophos container is locked when there is no active Wi-Fi connection.

If you add Wi-Fi networks to the list, the Sophos container is locked when the device is connected to a Wi-Fi network not listed.

**Important**

We recommend that you do not rely on Wi-Fi fencing as the only security mechanism because Wi-Fi names can be spoofed very easily.

---

### 15.20.2 Corporate Email configuration (iOS Sophos container policy)

With the **Corporate Email** configuration you define user settings for your Microsoft Exchange Server. These settings are applied to the Sophos Secure Email app if it is installed in the Sophos container.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange server</td>
<td>The Exchange server address.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If you use the Sophos Mobile EAS proxy, enter the URL of the EAS proxy server.</td>
</tr>
<tr>
<td>User</td>
<td>The user for this account.</td>
</tr>
<tr>
<td></td>
<td>If you enter the variable <code>%_USERNAME_%</code>, the server replaces it with the actual user name.</td>
</tr>
<tr>
<td>Email address</td>
<td>The email address of the account.</td>
</tr>
<tr>
<td></td>
<td>If you enter the variable <code>%_EMAILADDRESS_%</code>, the server replaces it with the actual email address.</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain for this account.</td>
</tr>
<tr>
<td>Support contact email</td>
<td>The email address that will be used as the &quot;Contact Support&quot; email address.</td>
</tr>
<tr>
<td>Use secure text fields</td>
<td>The content of input fields is secured. Auto-complete and auto-correction are disabled within the Sophos Secure Email app to prevent sensitive words to be saved in the memory of the device.</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Export contacts to device</td>
<td>Users are allowed to export the Exchange contacts with a phone number to the local device contacts, so that they can identify company contacts in incoming calls. Sophos Secure Email keeps the information synchronized.</td>
</tr>
<tr>
<td>Note</td>
<td>The local contact information is automatically deleted in the following situations:</td>
</tr>
<tr>
<td>• When the Corporate Email configuration is removed from the Sophos container policy (requires a restart of the Secure Email app).</td>
<td></td>
</tr>
<tr>
<td>• When the Sophos container is removed from the device.</td>
<td></td>
</tr>
<tr>
<td>• When the device is unenrolled from Sophos Mobile.</td>
<td></td>
</tr>
<tr>
<td>Call identification</td>
<td>Contact information from Sophos Secure Email can be used to identify company contacts in incoming calls, without the need to export Sophos Secure Email contacts to the device contacts.</td>
</tr>
<tr>
<td></td>
<td>To use this, users must turn on the following device settings:</td>
</tr>
<tr>
<td></td>
<td>• In the Settings app: Phone &gt; Call Blocking &amp; Identification &gt; Email</td>
</tr>
<tr>
<td></td>
<td>• In the Sophos Secure Email app: Settings &gt; Contacts &gt; Call Identification</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Notifications</strong></td>
<td>The notification type for new email:</td>
</tr>
<tr>
<td></td>
<td>• <strong>System</strong>: Notifications are managed by iOS. They don’t include details like Sender or Subject.</td>
</tr>
<tr>
<td></td>
<td>• <strong>App</strong>: Notifications are managed by the Sophos Secure Email app. You can select how much detail is displayed. When the app is not running, no notifications are displayed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong>: No notifications are displayed. This setting also affects event reminders:</td>
</tr>
<tr>
<td></td>
<td>• <strong>System, None</strong>: Event reminders only include time information.</td>
</tr>
<tr>
<td></td>
<td>• <strong>App</strong>: Event reminders include time, location and title information.</td>
</tr>
<tr>
<td><strong>Deny copy to clipboard</strong></td>
<td>Users cannot copy or cut texts from the Sophos Secure Email app.</td>
</tr>
<tr>
<td><strong>Open attachments</strong></td>
<td>Select whether attachments can be opened in all apps or only in the Sophos container apps Sophos Secure Workspace and Sophos Secure Email.</td>
</tr>
<tr>
<td><strong>Maximum email size</strong></td>
<td>Email messages that are larger than the size you select (including attachments) are not retrieved from the Exchange server.</td>
</tr>
<tr>
<td><strong>Advanced settings</strong></td>
<td>Click <strong>Advanced settings</strong> to configure settings that a future version of the Sophos Secure Email app might require.</td>
</tr>
</tbody>
</table>

**Important**
Only configure these settings if instructed by the Sophos support team.

### 15.20.3 Corporate Documents configuration (iOS Sophos container policy)

With the **Corporate Documents** configuration you define settings for the Corporate Documents feature of the Sophos Secure Workspace app.

**Configure storage providers**

For each storage provider you can define the following settings separately:
Sophos Mobile on Premise

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>The storage provider is available in the app.</td>
</tr>
<tr>
<td>Offline</td>
<td>Users are allowed to add files from the storage provider to the app’s Favorites list for offline use.</td>
</tr>
<tr>
<td>Open in (encrypted)</td>
<td>Users can share encrypted files with other apps via Open In.</td>
</tr>
<tr>
<td>Open in (unencrypted)</td>
<td>Users can share unencrypted files with other apps via Open In.</td>
</tr>
<tr>
<td>Clipboard</td>
<td>Users can copy parts of a document and paste them into other apps.</td>
</tr>
</tbody>
</table>

Enterprise provider settings

For Egnyte and WebDAV provider, also referred to as enterprise provider, you can centrally define server settings and login credentials. These cannot be changed by users.

Credential settings that you do not define centrally can be chosen by the users in the app’s provider credential screens.

For example you can centrally define the server and user account to be used but you can leave the password field undefined. Users then would have to know the password when accessing the storage provider.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the provider that is displayed in the Sophos Secure Workspace app.</td>
</tr>
<tr>
<td>Server</td>
<td>In this field, enter:</td>
</tr>
<tr>
<td></td>
<td>• The URL of the root folder on the Corporate Documents WebDAV server.</td>
</tr>
<tr>
<td></td>
<td>• The URL of the root folder on the Egnyte server.</td>
</tr>
<tr>
<td></td>
<td>• The URL of the root folder on the WebDAV server.</td>
</tr>
<tr>
<td></td>
<td>Use the following format: <a href="https://server.company.com">https://server.company.com</a></td>
</tr>
<tr>
<td>User name</td>
<td>In this field, enter the user name for the relevant server.</td>
</tr>
<tr>
<td>Password</td>
<td>In this field, enter the password for the relevant account.</td>
</tr>
<tr>
<td>Upload folder</td>
<td>In this field, enter the upload folder for the relevant account.</td>
</tr>
</tbody>
</table>
**Other settings**

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Documents</td>
<td>This turns on the <strong>Documents</strong> feature to securely distribute company documents.</td>
</tr>
<tr>
<td>Passphrase complexity</td>
<td>The required minimum complexity of passphrases for encryption keys. More secure passphrases are always allowed. You can select the following settings:</td>
</tr>
<tr>
<td></td>
<td>• 4 char password</td>
</tr>
<tr>
<td></td>
<td>• 6 char password</td>
</tr>
<tr>
<td></td>
<td>• 8 char password</td>
</tr>
<tr>
<td></td>
<td>• 10 char password</td>
</tr>
</tbody>
</table>

**15.20.4 Corporate Browser configuration (iOS Sophos container policy)**

With the **Corporate Browser** configuration you define settings for the Corporate Browser feature of the Sophos Secure Workspace app.

The Corporate Browser allows you to securely access corporate intranet pages and other allowed pages. You can define domains and bookmarks within a domain.

Every bookmarks belongs to a certain domain. When you add a bookmark, the domain entry is created automatically if it does not exist.

**Domain settings**

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>The domain that you want to allow.</td>
</tr>
<tr>
<td>Allow copy/paste</td>
<td>Users can copy and paste text from the Corporate Browser to other apps.</td>
</tr>
<tr>
<td>Allow open with</td>
<td>Users can download attachments or pass them on to other apps.</td>
</tr>
<tr>
<td>Allow save password</td>
<td>Users can save their passwords in the Corporate Browser.</td>
</tr>
</tbody>
</table>
Bookmark settings

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name for the bookmark.</td>
</tr>
<tr>
<td>URL</td>
<td>The web address for the bookmark.</td>
</tr>
</tbody>
</table>

15.20.5 Client certificate configuration (iOS Sophos container policy)

With the **Client certificate** configuration you install a client certificate onto devices. This certificate will be available to the Sophos Secure Email and Sophos Secure Workspace apps if they are installed in the Sophos container.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. The name of the certificate is shown in the **Certificate name** field. Enter the password for the selected certificate.

**Note**
The certificate you upload here is only available for this policy. If you require certificates in other profiles or policies, you have to upload them again.

15.20.6 Root certificate configuration (iOS Sophos container policy)

With the **Root certificate** configuration you install a root certificate onto devices. This certificate will be available to the Sophos Secure Email and Sophos Secure Workspace apps if they are installed in the Sophos container.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. The name of the certificate is shown in the **Certificate name** field. Enter the password for the selected certificate.

**Note**
The certificate you upload here is only available for this policy. If you require certificates in other profiles or policies, you have to upload them again.
15.20.7 SCEP configuration (iOS Sophos container policy)

With the SCEP configuration you enable devices to request certificates from a Certificate Authority using the Simple Certificate Enrollment Protocol (SCEP). These certificates are available to the Sophos Secure Workspace app if it is installed in the Sophos container.

**Note**
You must first add a Root certificate configuration to upload the CA certificate of the SCEP server before you can add a SCEP configuration.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>URL</strong></td>
<td>The web address of the Certificate Authority server. Use the variable $SCEPPROXYURL$ to refer to the server URL that is configured on the SCEP tab of the System setup page.</td>
</tr>
<tr>
<td><strong>Alias name</strong></td>
<td>The name under which the certificate will appear in selection dialogs. This should be a memorable name to identify the certificate. For example, use the same value as in the Subject field, but without the CN= prefix.</td>
</tr>
</tbody>
</table>
| **Subject**                | The name of the entity (for example person or device) that will receive the certificate. You can use placeholders for user data or device properties. The value that you enter (with placeholders replaced by the actual data) must be a valid X.500 name. For example:  
  - Enter CN=\%USERNAME\% to specify a user.  
  - Enter CN=\%DEVPROP(serial_number)\% to specify a device.  
  For information on available placeholders, see Placeholders in profiles and policies (page 81). |
| **Type of Subject Alternative Name** | To add a Subject Alternative Name (SAN) to the SCEP configuration, select the SAN type and then enter the SAN value. SAN types are:  
  - RFC 822 name: A valid email address.  
  - DNS name: The DNS name of the CA server.  
  - Uniform resource identifier: The fully qualified URL of the CA server. |
<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD user logon name</td>
<td>The User logon name value set in Active Directory, i.e. the user’s User Principal Name (UPN).</td>
</tr>
<tr>
<td>Challenge</td>
<td>The web address to obtain a challenge password from the SCEP server. Use the variable <code>%_CACHALLENGE_%</code> to refer to the challenge URL that is configured on the SCEP tab of the System setup page.</td>
</tr>
<tr>
<td>Root certificate</td>
<td>The CA certificate. Select the certificate from the list. The list contains all certificates that you have uploaded in Root certificate configurations of the current profile.</td>
</tr>
<tr>
<td>Key size</td>
<td>The size of the public key in the issued certificate. Make sure that the value matches the size configured on the SCEP server.</td>
</tr>
<tr>
<td>Use as digital signature</td>
<td>If you select this check box, the public key can be used as a digital signature.</td>
</tr>
<tr>
<td>Use for encryption</td>
<td>If you select this check box, the public key can be used for data encryption.</td>
</tr>
</tbody>
</table>

### 15.21 Configurations for macOS device policies

With a macOS device policy you configure various aspects of Macs, like password policies, restrictions or Wi-Fi settings. Device policy settings apply to all users that log in to the Mac you assign the policy to, whether they are managed by Sophos Mobile or not.

**Related concepts**
- About macOS policies (page 79)
- Configurations for macOS user policies (page 195)

**Related tasks**
- Create profile or policy (page 77)
**15.21.1 Password policies configuration (macOS device policy)**

With the Password policies configuration you define requirements for the passwords of Mac user accounts.

**Note**
When the Password policies configuration is assigned to a device, a grace period of 60 minutes starts. Within the grace period, the user is asked to change the password when they return to the Home screen to comply with the policies. After the grace period, the user may not start any apps on the device, including internal apps.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow simple value</td>
<td>Users are allowed to use sequential or repeated characters in their password, for example 1111 or abcde.</td>
</tr>
<tr>
<td>Require alphanumeric value</td>
<td>Passwords must contain at least one letter or number.</td>
</tr>
<tr>
<td>Minimum password length</td>
<td>Specifies the minimum number of characters a password must contain.</td>
</tr>
<tr>
<td>Minimum number of complex characters</td>
<td>Specifies the minimum number of non-alphanumeric characters (for example &amp; or !) a password must contain.</td>
</tr>
<tr>
<td>Maximum password age in days</td>
<td>Requires users to change their password in the specified interval. Value range: 0 (no password change required) to 730 days.</td>
</tr>
<tr>
<td>Maximum Auto-Lock (in minutes)</td>
<td>In this field, you can specify the maximum value the user is allowed to configure on the device. Auto-Lock specifies how soon (in minutes) the device will be locked if it has not been used.</td>
</tr>
<tr>
<td>Password history</td>
<td>In this field, you can specify how many old passwords are remembered and compared with new ones. When the user defines a new password, it is not accepted if it matches a previously used password. Value range: 1 to 50 or 0 (no password history).</td>
</tr>
</tbody>
</table>
### Setting/Field

| **Maximum grace period for device lock** | In this field, you can specify the maximum value the user is allowed to configure on the device. The grace period for device lock specifies for how long the device can be unlocked after a lock without a password prompt. If you select **None**, the user can select any of the intervals available. If you select **Immediately**, users must enter a password every time they unlock their devices. |
| **Number of failed attempts until device wipe** | In this field, you can specify the number of failed attempts to enter the correct password before the device is wiped. After six failed attempts, a time delay is imposed before a password can be entered again. The delay increases with each failed attempt. After the final failed attempt, all data and settings are securely removed from the device. The time delay starts after the sixth attempt. So if you set this value to 6 or lower, no delay is imposed and the device is wiped when the attempt limit is exceeded. |

### 15.21.2 Restrictions configuration (macOS device policy)

With the **Restrictions** configuration you define restrictions for Macs.

**Note**

Some options are only available for certain versions of macOS. This is indicated by blue labels next to an option in Sophos Mobile Admin.

### Device

<table>
<thead>
<tr>
<th><strong>Setting/Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow use of camera</td>
<td>If the check box is cleared, the camera is unavailable and the Camera icon is removed from the Home screen. Users cannot take pictures, record videos, or use FaceTime.</td>
</tr>
<tr>
<td>Allow internet search result for Spotlight</td>
<td>If the check box is cleared, Spotlight does not return internet search results.</td>
</tr>
<tr>
<td>Allow Apple Music</td>
<td>Users can access the Apple Music library.</td>
</tr>
</tbody>
</table>
### iCloud

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow backup</td>
<td>Users can back up their devices to iCloud.</td>
</tr>
<tr>
<td>Allow iCloud Photo Library</td>
<td>Users can use iCloud Photo Library.</td>
</tr>
<tr>
<td>Allow iCloud Keychain sync</td>
<td>Users can use iCloud Keychain to synchronize passwords across their iPhones, iPads, and Macs. If the check box is cleared, iCloud Keychain data is only stored locally on the device.</td>
</tr>
<tr>
<td>Allow document sync</td>
<td>Users can store documents and app configuration data in iCloud.</td>
</tr>
<tr>
<td>Allow Back to My Mac</td>
<td>Users can use iCloud Back to My Mac, i.e. file and screen sharing between a remote and a local Mac.</td>
</tr>
<tr>
<td>Allow Find My Mac</td>
<td>Users can use iCloud Find My Mac to locate, lock, or wipe their Mac remotely.</td>
</tr>
<tr>
<td>Allow iCloud Bookmarks</td>
<td>Users can use iCloud Bookmarks to synchronize web bookmarks between browsers and platforms.</td>
</tr>
<tr>
<td>Allow iCloud Mail</td>
<td>Users can set up an iCloud Mail account on their Mac.</td>
</tr>
<tr>
<td>Allow iCloud Calendar</td>
<td>Users can use iCloud Calendar to share their calendars across their devices and with other iCloud users.</td>
</tr>
<tr>
<td>Allow iCloud Reminders</td>
<td>Users can use iCloud Reminders to share reminder lists across their devices and with other iCloud users.</td>
</tr>
<tr>
<td>Allow iCloud Address Book</td>
<td>Users can use iCloud Address Book to share contacts across their devices and with other iCloud users.</td>
</tr>
<tr>
<td>Allow iCloud Notes</td>
<td>Users can use iCloud Notes to take notes and to share them across their devices and with other users.</td>
</tr>
<tr>
<td>Allow iCloud Drive for Desktop and Documents</td>
<td>Users can store their Mac Desktop and their Documents folder in iCloud Drive and access them on other devices.</td>
</tr>
</tbody>
</table>

### Security and privacy

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Touch ID to unlock device</td>
<td>If the check box is cleared, the device can’t be unlocked by Touch ID.</td>
</tr>
</tbody>
</table>
### Setting/Field

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allow definition lookup</strong> Users can look up definitions for highlighted words.</td>
</tr>
<tr>
<td><strong>Allow Auto Unlock</strong> Users can use Auto Unlock to have their Mac automatically unlocked by their Apple Watch.</td>
</tr>
<tr>
<td><strong>Allow iTunes File Sharing</strong> Users can use File Sharing in iTunes to copy files between their Mac and an iPhone or iPad.</td>
</tr>
<tr>
<td><strong>Allow AirPrint</strong> Users can send files to AirPrint-enabled printers.</td>
</tr>
<tr>
<td><strong>Allow iBeacon discovery of AirPrint printers</strong> macOS uses iBeacon to discover AirPrint devices.</td>
</tr>
<tr>
<td><strong>Important</strong> If you allow this, malicious AirPrint devices can perform phishing attacks on network traffic.</td>
</tr>
<tr>
<td><strong>Force trusted certificates for AirPrint over TLS</strong> AirPrint over TLS is rejected if the AirPrint device uses an untrusted certificate.</td>
</tr>
</tbody>
</table>

### 15.21.3 Wi-Fi configuration (macOS device policy)

With the Wi-Fi configuration you specify settings for connecting to Wi-Fi networks.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SSID</strong></td>
<td>The ID of the Wi-Fi network.</td>
</tr>
<tr>
<td><strong>Connect automatically</strong></td>
<td>Automatically connect to the target network.</td>
</tr>
<tr>
<td><strong>Hidden network</strong></td>
<td>The target network is not open or visible.</td>
</tr>
</tbody>
</table>
### Setting/Field

<table>
<thead>
<tr>
<th>Security type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The security type of the Wi-Fi network:</td>
<td></td>
</tr>
<tr>
<td>• <strong>None</strong></td>
<td></td>
</tr>
<tr>
<td>• <strong>WEP (Personal)</strong></td>
<td></td>
</tr>
<tr>
<td>• <strong>WPA/WPA2 (Personal)</strong></td>
<td></td>
</tr>
<tr>
<td>• <strong>Any (Personal)</strong></td>
<td></td>
</tr>
<tr>
<td>• <strong>WEP (Enterprise)</strong></td>
<td></td>
</tr>
<tr>
<td>• <strong>WPA/WPA2 (Enterprise)</strong></td>
<td></td>
</tr>
<tr>
<td>• <strong>Any (Enterprise)</strong></td>
<td></td>
</tr>
</tbody>
</table>

If you select a type with *Personal* in its name, a **Password** field is displayed. Enter the relevant password.

If you select a type with *Enterprise* in its name, the tabs **Protocols**, **Authentication** and **Trust** are displayed.

On the **Protocols** tab configure the following:

- Under **Accepted EAP types**, specify the EAP methods to be used for authentication. Depending on the types selected on this tab, the values in the **Internal identity** field on this tab become available for selection.
- Under **EAP-Fast**, configure the EAP-Fast Protected Access credential settings.

On the **Authentication** tab, configure client authentication settings:

- In the **User** field, enter the user name for the connection to the Wi-Fi network.
- Select **Require password on each connect**, if the password is to be queried for each connection and transferred with the authentication.
- In the **Password** field, enter the relevant password.
- In the **Identity certificate** list, select the certificate for the connection to the Wi-Fi network.

**Note**
The certificate to be used has to be specified in a **Client certificate** configuration.

- In the **External identity** field, enter the externally visible ID (for TTLS, PEAP and EAP-Fast).

On the **Trust** tab, configure server authentication settings:

Select the trusted certificates from the list.

**Note**
You must specify the certificates in a **Root certificate** configuration.
### Proxy

In this list, select the proxy settings for the Wi-Fi connection:

- **None**
- **Manually**
- **Automatic**

If you select **Manually**, the fields **Server and port**, **Authentication**, and **Password** are displayed. Enter the required proxy information. If you select **Automatic**, the field **Proxy server URL** is displayed. Enter the URL of the proxy server.

---

### 15.21.4 VPN configuration (macOS device policy)

With the VPN configuration you define VPN settings for network connections.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection name</td>
<td>The name of the connection shown on the device.</td>
</tr>
<tr>
<td>Connection type</td>
<td>The type of the VPN connection:</td>
</tr>
<tr>
<td></td>
<td>- Cisco AnyConnect</td>
</tr>
<tr>
<td></td>
<td>- Cisco Legacy AnyConnect</td>
</tr>
<tr>
<td></td>
<td>- IPsec (Cisco)</td>
</tr>
<tr>
<td></td>
<td>- F5</td>
</tr>
<tr>
<td></td>
<td>- Check Point</td>
</tr>
<tr>
<td></td>
<td>- Custom SSL/TLS</td>
</tr>
<tr>
<td></td>
<td>Different entry fields are shown on the VPN page depending on the connection type you select here.</td>
</tr>
<tr>
<td>Identifier (reverse DNS format)</td>
<td>The custom identifier in reverse DNS format.</td>
</tr>
<tr>
<td>Server</td>
<td>The host name or the IP address of the server.</td>
</tr>
<tr>
<td>Account</td>
<td>The user account for the authentication of the connection.</td>
</tr>
<tr>
<td>Third-party settings</td>
<td>If your vendor has specified custom connection properties, you can enter them in this field. To enter a property, click <strong>Add</strong> and then enter <strong>Key</strong> and <strong>Value</strong> of the property in the dialog box.</td>
</tr>
<tr>
<td>Send all traffic through VPN</td>
<td>All traffic is sent through VPN.</td>
</tr>
<tr>
<td>Group</td>
<td>The group that may be required for the authentication of the connection.</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **User authentication** | The type of user authentication for the connection:  
• **Password**  
  If you select this option, the **Password** field is shown below the **User authentication** field. Enter the password for authentication.  
• **Certificate**  
  If you select this option, the **Certificate** field is shown below the **User authentication** field. Select a certificate. |
| **Device authentication** | The type of device authentication:  
• **Keys (Shared Secret)/Group name**  
  If you select this option, the fields **Group name**, **Keys (Shared Secret)**, **Use hybrid authentication** and **Request password** are displayed below the **Device authentication** field. Enter the required authentication information in the **Group name** and **Keys (Shared Secret)** fields. Select **Use hybrid authentication** and **Request password** as required.  
• **Certificate**  
  If you select this option, the fields **Certificate** and **Including user PIN** are displayed below the **Device authentication** field. In the **Certificate** list, select the required certificate. Select **Including user PIN** to include the user PIN in device authentication. |
| **Proxy** | The proxy settings for the connection:  
• **None**  
• **Manually**  
  If you select this option, the fields **Server and port**, **Authentication** and **Password** are displayed. In the **Server and port** field, enter the valid address and the port of the proxy server. In the **Authentication** field, enter the user name for the connection to the proxy server. In the **Password** field, enter the password for the connection to the proxy server.  
• **Automatic**  
  If you select this option, the **Proxy server URL** field is displayed. Enter the URL of the server with the proxy setting in this field. |
### Provider type

The VPN connection type.
- **App proxy**: Network traffic is sent through a VPN tunnel at the application layer.
- **Packet tunnel**: Network traffic is sent through a VPN tunnel at the network layer.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Filter name</strong></td>
<td>A custom name for the filter configuration.</td>
</tr>
<tr>
<td><strong>Filter ID</strong></td>
<td>The bundle ID of the third-party app.</td>
</tr>
<tr>
<td><strong>Server</strong></td>
<td>The server hosting the filtering service (host name, IP address, or URL).</td>
</tr>
<tr>
<td><strong>Organization</strong></td>
<td>The name of your organization. The value is passed to the filtering service.</td>
</tr>
<tr>
<td><strong>User name</strong></td>
<td>The credentials required for connecting to the filtering service.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Certificate</strong></td>
<td>A certificate for authenticating to the filtering service.</td>
</tr>
<tr>
<td><strong>Filter range</strong></td>
<td>The traffic to be filtered by the third-party app:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Filter browser traffic</strong>: WebKit browser traffic is filtered.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Filter socket traffic</strong>: Socket traffic is filtered.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Filter browser and socket traffic</strong>: WebKit and socket traffic is filtered.</td>
</tr>
<tr>
<td><strong>Third-party settings</strong></td>
<td>Additional configuration settings, if required by the third-party app.</td>
</tr>
</tbody>
</table>
15.21.6 Global HTTP proxy configuration (macOS device policy)

With the Global HTTP proxy configuration you define a corporate proxy server.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global HTTP proxy</td>
<td>Select the proxy settings for the connection:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Manually</strong></td>
</tr>
<tr>
<td></td>
<td>If you select this option, the fields <strong>Server and port</strong>, <strong>Authentication</strong> and <strong>Password</strong> are displayed. In the <strong>Server and port</strong> field, enter the valid address and the port of the proxy server. In the <strong>Authentication</strong> field, enter the user name for the connection to the proxy server. In the <strong>Password</strong> field, enter the password for the connection to the proxy server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Automatic</strong></td>
</tr>
<tr>
<td></td>
<td>If you select this option, the <strong>Proxy server URL</strong> field is displayed. Enter the URL of the server with the proxy setting in this field.</td>
</tr>
</tbody>
</table>

15.21.7 Root certificate configuration (macOS device policy)

With the Root certificate configuration you install a root certificate onto Macs.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. The name of the certificate is shown in the **Certificate name** field. Enter the password for the selected certificate.

**Note**
The certificate you upload here is only available for this policy. If you require certificates in other profiles or policies, you have to upload them again.

15.21.8 Client Certificate configuration (macOS device policy)

With the Client certificate configuration you install a client certificate onto Macs.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. The name of the certificate is shown in the **Certificate name** field. Enter the password for the selected certificate.

**Note**
The certificate you upload here is only available for this policy. If you require certificates in other profiles or policies, you have to upload them again.
### 15.21.9 SCEP configuration (macOS device policy)

With the SCEP configuration you enable devices to request certificates from a Certificate Authority using the Simple Certificate Enrollment Protocol (SCEP).

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>URL</strong></td>
<td>The web address of the Certificate Authority server. Use the variable <code>%_SCEPPROXYURL_%</code> to refer to the server URL that is configured on the SCEP tab of the System setup page.</td>
</tr>
<tr>
<td><strong>CA name</strong></td>
<td>A name that is understood by the Certificate Authority. The name can, for example, be used to distinguish between instances.</td>
</tr>
</tbody>
</table>
| **Subject**                | The name of the entity (for example person or device) that will receive the certificate. You can use placeholders for user data or device properties. The value that you enter (with placeholders replaced by the actual data) must be a valid X.500 name. For example:  
  - Enter `CN=%_USERNAME_%` to specify a user.  
  - Enter `CN=%DEVPROP(serial_number)_%` to specify a device.  
  For information on available placeholders, see Placeholders in profiles and policies [page 81]. |
| **Type of Subject Alternative Name** | To add a Subject Alternative Name (SAN) to the SCEP configuration, select the SAN type and then enter the SAN value. SAN types are:  
  - **RFC 822 name**: A valid email address.  
  - **DNS name**: The DNS name of the CA server.  
  - **Uniform resource identifier**: The fully qualified URL of the CA server.                                                                 |
### Setting/Field

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retry delay</td>
<td>The number of seconds between retries.</td>
</tr>
<tr>
<td>Key size</td>
<td>The size of the public key in the issued certificate. Make sure that the value matches the size configured on the SCEP server.</td>
</tr>
</tbody>
</table>

### 15.21.10 Directory service configuration (macOS device policy)

With the **Directory service** configuration you specify an Active Directory domain that a Mac joins when the policy is assigned to it.

**Note**
If the Active Directory domain you configure here is the same domain you use for the Self Service Portal, the macOS user policy assigned to the Mac is applied to all Active Directory users that log in to the Mac.

### General settings

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain host name</td>
<td>The DNS host name of the Active Directory domain to join.</td>
</tr>
<tr>
<td>AD administrator name</td>
<td>The credentials of the user account used for connecting to the Active Directory server.</td>
</tr>
<tr>
<td>Password</td>
<td>This user must have permissions to add devices to the Active Directory database.</td>
</tr>
<tr>
<td>Organizational unit</td>
<td>The organizational unit (OU) within the Active Directory database where the joining computer is added.</td>
</tr>
</tbody>
</table>

### User experience

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Create mobile account      | macOS creates a mobile account when a network user logs in for the first time.  
With a mobile account, users can log in to the Mac with their Active Directory credentials even when the Mac is not connected to the Active Directory server. |
### Setting/Field

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Require confirmation before creating a mobile account</strong></td>
<td>The user can decide whether to create a mobile account or not.</td>
</tr>
<tr>
<td><strong>Force local home folder</strong></td>
<td>Select this check box to force the creation of user profiles on the startup disk. This is required for mobile accounts. If you clear the check box, pure network home directories are used.</td>
</tr>
<tr>
<td><strong>Use UNC path from Active Directory</strong></td>
<td>macOS mounts the home folder specified in the Active Directory user account.</td>
</tr>
<tr>
<td><strong>Network protocol</strong></td>
<td>The protocol for mounting the home folder.</td>
</tr>
<tr>
<td><strong>Default user shell</strong></td>
<td>The command-line shell for the user. If you leave this field empty, <code>/bin/bash</code> is used.</td>
</tr>
</tbody>
</table>

### Mapping

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UID attribute</strong></td>
<td>The Active Directory attribute that is mapped to the unique user ID (UID) in macOS.</td>
</tr>
<tr>
<td><strong>User GID attribute</strong></td>
<td>The Active Directory attribute that is mapped to the primary group ID in macOS user accounts.</td>
</tr>
<tr>
<td><strong>Group GID attribute</strong></td>
<td>The Active Directory attribute that is mapped to the group ID in macOS group accounts.</td>
</tr>
</tbody>
</table>

**Important**

If you change these mapping settings later, users might lose access to previously created files.

### Administrative

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Preferred DC server</strong></td>
<td>The Active Directory domain controller (DC) that is consulted first. If you leave this field empty, macOS selects the domain controller by site information and controller responsiveness.</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Password trust interval in days</strong></td>
<td>Specify how often macOS changes the password of its Active Directory computer account. If you leave this field empty, macOS changes its password every 14 days. If you set a value of 0, macOS doesn’t change the password automatically.</td>
</tr>
</tbody>
</table>
| **Namespace**                                    | • **Forest**  
  Namespace support is turned on. Multiple users with the same login name that exist in different domains of the Active Directory forest can log in.  
  Users must enter their login name as `DOMAIN\name`.  
  • **Domain**  
  Namespace support is turned off. Users must have a unique login name. |
| **Packet signing**                               | macOS can sign and encrypt the LDAP connections used for Active Directory communication. |
| **Packet encryption**                            | • **Allow**: macOS decides if to sign and/or encrypt the LDAP connections.  
  • **Disable**: macOS doesn’t sign or encrypt the LDAP connections.  
  • **Require**: macOS always signs and encrypts LDAP connections.  
  • **SSL/TLS**: macOS always uses LDAP over SSL/TLS. |
| **Multi-domain authentication**                  | Users from all domains in the Active Directory forest can log in. |
| **Domain administrator groups**                  | A list of Active Directory groups. Members of these groups are granted administrative privileges on the Mac. To enter more than one group, press Enter after each entry. |
| **Restrict DDNS**                                | A list of network interfaces. By default, macOS uses Dynamic DNS (DDNS) for all network interfaces. To restrict DDNS to certain interfaces, enter their BSD names. For example to restrict DDNS to the built-in Ethernet port, enter `en0`. To enter more than one interface, press Enter after each entry. |
15.21.11 Managed domains configuration (macOS device policy)

With the Managed domains configuration you define managed domains for Macs.

Email domains

Enter email domains that are managed by your organization. In the Mail app, email addresses that don't match one of the configured domains are highlighted as out-of-domain.

15.21.12 Gatekeeper configuration (macOS device policy)

With the Gatekeeper configuration you configure macOS Gatekeeper, which blocks apps installed from forbidden sources.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow apps downloaded from</td>
<td>Select the required setting:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Anywhere</strong>: Users can open all apps, regardless of where they were installed from.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Mac App Store</strong>: Users can only open apps from Mac App Store.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Mac App Store and identified developers</strong>: Users can only open apps from Mac App Store or from identified developers, i.e. developers approved by Apple.</td>
</tr>
</tbody>
</table>

15.22 Configurations for macOS user policies

With a macOS user policy you configure various aspects of Macs, like password policies, restrictions or Wi-Fi settings. User policy settings apply to all managed users of the Mac you assign the policy to.

Related concepts
About macOS policies [page 79]
Configurations for macOS device policies [page 181]

Related tasks
Create profile or policy [page 77]
**15.22.1 Password policies configuration (macOS user policy)**

With the **Password policies** configuration you define requirements for the passwords of Mac user accounts.

**Note**

When the **Password policies** configuration is assigned to a device, a grace period of 60 minutes starts. Within the grace period, the user is asked to change the password when they return to the Home screen to comply with the policies. After the grace period, the user may not start any apps on the device, including internal apps.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow simple value</td>
<td>Users are allowed to use sequential or repeated characters in their password, for example 1111 or abcde.</td>
</tr>
<tr>
<td>Require alphanumeric value</td>
<td>Passwords must contain at least one letter or number.</td>
</tr>
<tr>
<td>Minimum password length</td>
<td>Specifies the minimum number of characters a password must contain.</td>
</tr>
<tr>
<td>Minimum number of complex characters</td>
<td>Specifies the minimum number of non-alphanumeric characters (for example &amp; or !) a password must contain.</td>
</tr>
<tr>
<td>Maximum password age in days</td>
<td>Requires users to change their password in the specified interval. Value range: 0 (no password change required) to 730 days.</td>
</tr>
<tr>
<td>Maximum Auto-Lock (in minutes)</td>
<td>In this field, you can specify the maximum value the user is allowed to configure on the device. Auto-Lock specifies how soon (in minutes) the device will be locked if it has not been used.</td>
</tr>
<tr>
<td>Password history</td>
<td>In this field, you can specify how many old passwords are remembered and compared with new ones. When the user defines a new password, it is not accepted if it matches a previously used password. Value range: 1 to 50 or 0 (no password history).</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Maximum grace period for device lock</td>
<td>In this field, you can specify the maximum value the user is allowed to configure on the device. The grace period for device lock specifies for how long the device can be unlocked after a lock without a password prompt. If you select None, the user can select any of the intervals available. If you select Immediately, users must enter a password every time they unlock their devices.</td>
</tr>
<tr>
<td>Number of failed attempts until device wipe</td>
<td>In this field, you can specify the number of failed attempts to enter the correct password before the device is wiped. After six failed attempts, a time delay is imposed before a password can be entered again. The delay increases with each failed attempt. After the final failed attempt, all data and settings are securely removed from the device. The time delay starts after the sixth attempt. So if you set this value to 6 or lower, no delay is imposed and the device is wiped when the attempt limit is exceeded.</td>
</tr>
</tbody>
</table>

### 15.22.2 Restrictions configuration (macOS user policy)

With the Restrictions configuration you define restrictions for Macs.

**Note**

Some options are only available for certain versions of macOS. This is indicated by blue labels next to an option in Sophos Mobile Admin.

---

### Device

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow use of camera</td>
<td>If the check box is cleared, the camera is unavailable and the Camera icon is removed from the Home screen. Users cannot take pictures, record videos, or use FaceTime.</td>
</tr>
<tr>
<td>Allow internet search result for Spotlight</td>
<td>If the check box is cleared, Spotlight does not return internet search results.</td>
</tr>
<tr>
<td>Allow Apple Music</td>
<td>Users can access the Apple Music library.</td>
</tr>
</tbody>
</table>
### iCloud

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow backup</td>
<td>Users can back up their devices to iCloud.</td>
</tr>
<tr>
<td>Allow iCloud Photo Library</td>
<td>Users can use iCloud Photo Library.</td>
</tr>
<tr>
<td>Allow iCloud Keychain sync</td>
<td>Users can use iCloud Keychain to synchronize passwords across their iPhones, iPads, and Macs. If the check box is cleared, iCloud Keychain data is only stored locally on the device.</td>
</tr>
<tr>
<td>Allow document sync</td>
<td>Users can store documents and app configuration data in iCloud.</td>
</tr>
<tr>
<td>Allow Back to My Mac</td>
<td>Users can use iCloud Back to My Mac, i.e. file and screen sharing between a remote and a local Mac.</td>
</tr>
<tr>
<td>Allow Find My Mac</td>
<td>Users can use iCloud Find My Mac to locate, lock, or wipe their Mac remotely.</td>
</tr>
<tr>
<td>Allow iCloud Bookmarks</td>
<td>Users can use iCloud Bookmarks to synchronize web bookmarks between browsers and platforms.</td>
</tr>
<tr>
<td>Allow iCloud Mail</td>
<td>Users can set up an iCloud Mail account on their Mac.</td>
</tr>
<tr>
<td>Allow iCloud Calendar</td>
<td>Users can use iCloud Calendar to share their calendars across their devices and with other iCloud users.</td>
</tr>
<tr>
<td>Allow iCloud Reminders</td>
<td>Users can use iCloud Reminders to share reminder lists across their devices and with other iCloud users.</td>
</tr>
<tr>
<td>Allow iCloud Address Book</td>
<td>Users can use iCloud Address Book to share contacts across their devices and with other iCloud users.</td>
</tr>
<tr>
<td>Allow iCloud Notes</td>
<td>Users can use iCloud Notes to take notes and to share them across their devices and with other users.</td>
</tr>
<tr>
<td>Allow iCloud Drive for Desktop and Documents</td>
<td>Users can store their Mac Desktop and their Documents folder in iCloud Drive and access them on other devices.</td>
</tr>
</tbody>
</table>

### Security and privacy

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Touch ID to unlock device</td>
<td>If the check box is cleared, the device can’t be unlocked by Touch ID.</td>
</tr>
</tbody>
</table>
### Setting/Field

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow definition lookup</td>
<td>Users can look up definitions for highlighted words.</td>
</tr>
<tr>
<td>Allow Auto Unlock</td>
<td>Users can use Auto Unlock to have their Mac automatically unlocked by their Apple Watch.</td>
</tr>
<tr>
<td>Allow iTunes File Sharing</td>
<td>Users can use File Sharing in iTunes to copy files between their Mac and an iPhone or iPad.</td>
</tr>
<tr>
<td>Allow AirPrint</td>
<td>Users can send files to AirPrint-enabled printers.</td>
</tr>
<tr>
<td>Allow iBeacon discovery of AirPrint printers</td>
<td>macOS uses iBeacon to discover AirPrint devices.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong>&lt;br&gt;If you allow this, malicious AirPrint devices can perform phishing attacks on network traffic.</td>
</tr>
<tr>
<td>Force trusted certificates for AirPrint over TLS</td>
<td>AirPrint over TLS is rejected if the AirPrint device uses an untrusted certificate.</td>
</tr>
</tbody>
</table>

#### 15.22.3 Exchange account configuration (macOS user policy)

With the Exchange account configuration you set up a connection to a Microsoft Exchange Server email server.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account name</td>
<td>The account name.</td>
</tr>
<tr>
<td>Exchange server</td>
<td>The Exchange server address.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>&lt;br&gt;If you use the Sophos Mobile EAS proxy, enter the URL of the EAS proxy server.</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain for this account.</td>
</tr>
<tr>
<td>User</td>
<td>The user for this account.</td>
</tr>
<tr>
<td></td>
<td>If you enter the variable <code>%USERNAME%</code>, the server replaces it with the actual user name.</td>
</tr>
<tr>
<td>Email address</td>
<td>The email address of the account.</td>
</tr>
<tr>
<td></td>
<td>If you enter the variable <code>%EMAILADDRESS%</code>, the server replaces it with the actual email address.</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Password</td>
<td>The password for this account. If you leave this field empty, users must enter the password on their devices.</td>
</tr>
<tr>
<td>SSL/TLS</td>
<td>The connection to the Exchange server is secured by SSL or TLS (depending on what the server supports). We recommend that you select this check box.</td>
</tr>
</tbody>
</table>

### 15.22.4 Wi-Fi configuration (macOS user policy)

With the Wi-Fi configuration you specify settings for connecting to Wi-Fi networks.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
<td>The ID of the Wi-Fi network.</td>
</tr>
<tr>
<td>Connect automatically</td>
<td>Automatically connect to the target network.</td>
</tr>
<tr>
<td>Hidden network</td>
<td>The target network is not open or visible.</td>
</tr>
</tbody>
</table>
Security type

The security type of the Wi-Fi network:

- None
- WEP (Personal)
- WPA/WPA2 (Personal)
- Any (Personal)
- WEP (Enterprise)
- WPA/WPA2 (Enterprise)
- Any (Enterprise)

If you select a type with *Personal* in its name, a **Password** field is displayed. Enter the relevant password.

If you select a type with *Enterprise* in its name, the tabs **Protocols**, **Authentication** and **Trust** are displayed.

On the **Protocols** tab configure the following:

- Under **Accepted EAP types**, specify the EAP methods to be used for authentication. Depending on the types selected on this tab, the values in the **Internal identity** field on this tab become available for selection.
- Under **EAP-FAST**, configure the EAP-FAST Protected Access credential settings.

On the **Authentication** tab, configure client authentication settings:

- In the **User** field, enter the user name for the connection to the Wi-Fi network.
- Select **Require password on each connect**, if the password is to be queried for each connection and transferred with the authentication.
- In the **Password** field, enter the relevant password.
- In the **Identity certificate** list, select the certificate for the connection to the Wi-Fi network.

**Note**
The certificate to be used has to be specified in a **Client certificate** configuration.

- In the **External identity** field, enter the externally visible ID (for TTLS, PEAP and EAP-FAST).

On the **Trust** tab, configure server authentication settings:

Select the trusted certificates from the list.

**Note**
You must specify the certificates in a **Root certificate** configuration.
Sophos Mobile on Premise

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Proxy**     | In this list, select the proxy settings for the Wi-Fi connection:  
|               | • None  
|               | • Manually  
|               | • Automatic  

If you select **Manually**, the fields **Server and port**, **Authentication**, and **Password** are displayed. Enter the required proxy information. If you select **Automatic**, the field **Proxy server URL** is displayed. Enter the URL of the proxy server.

### 15.22.5 VPN configuration (macOS user policy)

With the VPN configuration you define VPN settings for network connections.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connection name</strong></td>
<td>The name of the connection shown on the device.</td>
</tr>
</tbody>
</table>
| **Connection type**                  | The type of the VPN connection:  
|                                      | • Cisco AnyConnect  
|                                      | • Cisco Legacy AnyConnect  
|                                      | • IPsec (Cisco)  
|                                      | • F5  
|                                      | • Check Point  
|                                      | • Custom SSL/TLS  

Different entry fields are shown on the VPN page depending on the connection type you select here.

<table>
<thead>
<tr>
<th><strong>Identifier (reverse DNS format)</strong></th>
<th>The custom identifier in reverse DNS format.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server</strong></td>
<td>The host name or the IP address of the server.</td>
</tr>
<tr>
<td><strong>Account</strong></td>
<td>The user account for the authentication of the connection.</td>
</tr>
</tbody>
</table>
| **Third-party settings**            | If your vendor has specified custom connection properties, you can enter them in this field.  
<p>|                                     | To enter a property, click <strong>Add</strong> and then enter <strong>Key</strong> and <strong>Value</strong> of the property in the dialog box. |
| <strong>Send all traffic through VPN</strong>    | All traffic is sent through VPN. |
| <strong>Group</strong>                           | The group that may be required for the authentication of the connection. |</p>
<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User authentication</strong></td>
<td>The type of user authentication for the connection:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Password</strong></td>
</tr>
<tr>
<td></td>
<td>If you select this option, the Password field is shown below the User authentication field. Enter the password for authentication.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Certificate</strong></td>
</tr>
<tr>
<td></td>
<td>If you select this option, the Certificate field is shown below the User authentication field. Select a certificate.</td>
</tr>
<tr>
<td><strong>Device authentication</strong></td>
<td>The type of device authentication:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Keys (Shared Secret)/Group name</strong></td>
</tr>
<tr>
<td></td>
<td>If you select this option, the fields Group name, Keys (Shared Secret), Use hybrid authentication and Request password are displayed below the Device authentication field. Enter the required authentication information in the Group name and Keys (Shared Secret) fields. Select Use hybrid authentication and Request password as required.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Certificate</strong></td>
</tr>
<tr>
<td></td>
<td>If you select this option, the fields Certificate and Including user PIN are displayed below the Device authentication field. In the Certificate list, select the required certificate. Select Including user PIN to include the user PIN in device authentication.</td>
</tr>
<tr>
<td><strong>Proxy</strong></td>
<td>The proxy settings for the connection:</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Manually</strong></td>
</tr>
<tr>
<td></td>
<td>If you select this option, the fields Server and port, Authentication and Password are displayed. In the Server and port field, enter the valid address and the port of the proxy server. In the Authentication field, enter the user name for the connection to the proxy server. In the Password field, enter the password for the connection to the proxy server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Automatic</strong></td>
</tr>
<tr>
<td></td>
<td>If you select this option, the Proxy server URL field is displayed. Enter the URL of the server with the proxy setting in this field.</td>
</tr>
</tbody>
</table>
### 15.22.6 Single sign-on configuration (macOS user policy)

With the **Single sign-on** configuration you define settings for a single sign-on for third-party apps.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>A human-readable name for the account.</td>
</tr>
<tr>
<td><strong>Kerberos principal name</strong></td>
<td>The Kerberos principal name. If you do not enter a value, the user must enter the name during profile installation.</td>
</tr>
<tr>
<td><strong>Realm</strong></td>
<td>The Kerberos realm name. You must enter the name in upper-case.</td>
</tr>
<tr>
<td><strong>URLs</strong></td>
<td>Values must begin with http:// or https://. If a value doesn’t end with /, the / is added by Sophos Mobile.</td>
</tr>
<tr>
<td><strong>App identifiers</strong></td>
<td>A list of bundle IDs of apps. Values must be either exact matches [e.g. com.sophos.smsec], or prefixes, using the characters .* at the end of the string [e.g. com.sophos.*].</td>
</tr>
</tbody>
</table>

### 15.22.7 Web Clip configuration (macOS user policy)

With the **Web Clip** configuration you define Web Clips to be added to the macOS desktop. Web Clips provide fast access to favorite web pages. But you can also add a Web Clip with a support phone number for example, to provide a quick way to dial the helpdesk.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>A description for the Web Clip.</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td>The web address of the Web Clip.</td>
</tr>
</tbody>
</table>
### Setting/Field

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Can be removed</strong></td>
<td>If the check box is cleared, the user cannot remove the Web Clip. It cannot be deleted from the device unless the user removes the profile that installed it.</td>
</tr>
<tr>
<td><strong>Full screen</strong></td>
<td>The Web Clip is opened full screen on the device. A full screen Web Clip opens the URL as a web app.</td>
</tr>
<tr>
<td><strong>Icon</strong></td>
<td>Select an image to be used as the Web Clip icon on the Home screen. This must be a PNG, GIF or JPEG image with a maximum file size of 1 MB. The image is cropped to a square and scaled to match the display resolution. For best results, we recommend that you use an image of size 180 px by 180 px.</td>
</tr>
</tbody>
</table>

**Note**
When a favicon is defined in the HTML code of the web page, the device might display that favicon as Web Clip icon. This happens for certain web pages only, depending on how the favicon is configured in the web page code.

### 15.22.8 Web content filter configuration (macOS user policy)

With the **Web content filter** configuration you define settings for a third-party app for filtering internet content.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Filter name</strong></td>
<td>A custom name for the filter configuration.</td>
</tr>
<tr>
<td><strong>Filter ID</strong></td>
<td>The bundle ID of the third-party app.</td>
</tr>
<tr>
<td><strong>Server</strong></td>
<td>The server hosting the filtering service (host name, IP address, or URL).</td>
</tr>
<tr>
<td><strong>Organization</strong></td>
<td>The name of your organization. The value is passed to the filtering service.</td>
</tr>
<tr>
<td><strong>User name</strong></td>
<td>The credentials required for connecting to the filtering service.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>A certificate for authenticating to the filtering service.</td>
</tr>
<tr>
<td><strong>Certificate</strong></td>
<td>A certificate for authenticating to the filtering service.</td>
</tr>
</tbody>
</table>
### Filter range

The traffic to be filtered by the third-party app:

- **Filter browser traffic**: WebKit browser traffic is filtered.
- **Filter socket traffic**: Socket traffic is filtered.
- **Filter browser and socket traffic**: WebKit and socket traffic is filtered.

### Third-party settings

Additional configuration settings, if required by the third-party app.

---

### 15.22.9 Global HTTP proxy configuration (macOS user policy)

With the **Global HTTP proxy** configuration you define a corporate proxy server.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global HTTP proxy</td>
<td>Select the proxy settings for the connection:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Manually</strong></td>
</tr>
<tr>
<td></td>
<td>If you select this option, the fields <strong>Server and port</strong>, <strong>Authentication</strong> and <strong>Password</strong> are displayed. In the <strong>Server and port</strong> field, enter the valid address and the port of the proxy server. In the <strong>Authentication</strong> field, enter the user name for the connection to the proxy server. In the <strong>Password</strong> field, enter the password for the connection to the proxy server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Automatic</strong></td>
</tr>
<tr>
<td></td>
<td>If you select this option, the <strong>Proxy server URL</strong> field is displayed. Enter the URL of the server with the proxy setting in this field.</td>
</tr>
</tbody>
</table>

---

### 15.22.10 Root certificate configuration (macOS user policy)

With the **Root certificate** configuration you install a root certificate onto Macs.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. The name of the certificate is shown in the **Certificate name** field. Enter the password for the selected certificate.

**Note**

The certificate you upload here is only available for this policy. If you require certificates in other profiles or policies, you have to upload them again.
15.22.11 Client Certificate configuration (macOS user policy)

With the **Client certificate** configuration you install a client certificate onto Macs.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. The name of the certificate is shown in the **Certificate name** field. Enter the password for the selected certificate.

**Note**
The certificate you upload here is only available for this policy. If you require certificates in other profiles or policies, you have to upload them again.

15.22.12 SCEP configuration (macOS user policy)

With the **SCEP** configuration you enable devices to request certificates from a Certificate Authority using the Simple Certificate Enrollment Protocol (SCEP).

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>URL</strong></td>
<td>The web address of the Certificate Authority server. Use the variable %_SCEP_PROXYURL% to refer to the server URL that is configured on the <strong>SCEP</strong> tab of the <strong>System setup</strong> page.</td>
</tr>
<tr>
<td><strong>CA name</strong></td>
<td>A name that is understood by the Certificate Authority. The name can, for example, be used to distinguish between instances.</td>
</tr>
</tbody>
</table>
| **Subject**   | The name of the entity (for example person or device) that will receive the certificate. You can use placeholders for user data or device properties. The value that you enter [with placeholders replaced by the actual data] must be a valid X.500 name. For example:  
  • Enter CN=%_USERNAME_% to specify a user.  
  • Enter CN=%_DEVPROP(serial_number)_% to specify a device. For information on available placeholders, see **Placeholders in profiles and policies** [page 81]. |
<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type of Subject Alternative Name</strong></td>
<td>To add a <em>Subject Alternative Name</em> (SAN) to the SCEP configuration, select the SAN type and then enter the SAN value. SAN types are:</td>
</tr>
<tr>
<td><strong>Value of Subject Alternative Name</strong></td>
<td><em>RFC 822 name</em>: A valid email address.</td>
</tr>
<tr>
<td></td>
<td><em>DNS name</em>: The DNS name of the CA server.</td>
</tr>
<tr>
<td></td>
<td><em>Uniform resource identifier</em>: The fully qualified URL of the CA server.</td>
</tr>
<tr>
<td><strong>AD user logon name</strong></td>
<td>The <em>User logon name</em> value set in Active Directory, i.e. the user's <em>User Principal Name</em> (UPN).</td>
</tr>
<tr>
<td><strong>Challenge</strong></td>
<td>The web address to obtain a challenge password from the SCEP server.</td>
</tr>
<tr>
<td></td>
<td>Use the variable <code>%_CACHALLENGE_%</code> to refer to the challenge URL that is configured on the SCEP tab of the <em>System setup</em> page.</td>
</tr>
<tr>
<td><strong>Retries</strong></td>
<td>The number of retries if the server sends a response of type <em>pending</em>.</td>
</tr>
<tr>
<td><strong>Retry delay</strong></td>
<td>The number of seconds between retries.</td>
</tr>
<tr>
<td><strong>Key size</strong></td>
<td>The size of the public key in the issued certificate. Make sure that the value matches the size configured on the SCEP server.</td>
</tr>
</tbody>
</table>

### 15.22.13 Managed domains configuration (macOS user policy)

With the Managed domains configuration you define managed domains for Macs.

**Email domains**

Enter email domains that are managed by your organization. In the Mail app, email addresses that don't match one of the configured domains are highlighted as out-of-domain.

### 15.22.14 CalDAV configuration (macOS user policy)

With the CalDAV configuration you configure the synchronization of calendar data with a CalDAV server. For example, this can be used to sync Google Calendar with a Mac.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Account name</strong></td>
<td>The display name of the CalDAV account on the device.</td>
</tr>
</tbody>
</table>
### Account host and port
The host name or IP address and optionally the port number of the CalDAV server.
For example, for Google Calendar enter:
calendar.google.com:443

### Principal URL
If required by the CalDAV server, enter the principal URL of the calendar resource.
For example, to sync with a calendar other than the primary calendar in a Google account, enter:
https://apidata.googleusercontent.com/caldav/v2/calendar_id/user
where `calendar_id` is the ID of the calendar you want to sync with. In the Google Calendar web application, the calendar ID is displayed in the calendar settings. See the Google Calendar help for details.

### User name, Password
The login credentials for the CalDAV account.
For example, for Google Calendar enter the credentials of the Google account.

### SSL/TLS
The connection to the CalDAV server is secured by SSL or TLS (depending on what the server supports).
We recommend that you select this check box.

### 15.22.15 CardDAV configuration (macOS user policy)
With the CardDAV configuration you configure the synchronization of contact data with a CardDAV server. For example, this can be used to sync Google Contacts with a Mac.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Account name</strong></td>
<td>The display name of the CardDAV account on the device.</td>
</tr>
</tbody>
</table>
| **Account host and port** | The host name or IP address and optionally the port number of the CardDAV server.  
For example, for Google Contacts enter:  
google.com |
**Setting/Field** | **Description**
--- | ---
Principal URL | If required by the CardDAV server, enter the principal URL of the contacts resource. For example, the Google CardDAV API supports the following principal URL: https://www.googleapis.com/carddav/v1/principals/account_name@gmail.com where account_name is the Google account name.

User name, Password | The login credentials for the CardDAV account. For example, for Google Contacts enter the credentials of the Google account.

SSL/TLS | The connection to the CardDAV server is secured by SSL or TLS (depending on what the server supports). We recommend that you select this check box.

15.22.16 IMAP/POP configuration (macOS user policy)

With the IMAP/POP configuration you add an IMAP or POP email account to Macs.

| Setting/Field | Description |
--- | ---|
Account name | The display name of the email account on the device. |
Account type | The type of the email server for incoming email (either IMAP or POP). |
User display name | The display name of the user for outgoing email. Use the variable %USERNAME% to refer to the name of the user that is assigned to the device. |
Email address | The email address of the account. Use the variable %EMAILADDRESS% to refer to the email address of the user that is assigned to the device. |
Incoming email | |
Email server and port | The host name or IP address and the port number of the server for incoming email (inbound server). |
User name | The user name for connecting to the inbound server. |
Authentication type | The authentication method for connecting to the inbound server. |
<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>The password for connecting to the inbound server (if required).</td>
</tr>
<tr>
<td>SSL/TLS</td>
<td>The connection to the inbound server is secured by SSL or TLS (depending on what the server supports).</td>
</tr>
<tr>
<td>Outgoing email</td>
<td></td>
</tr>
<tr>
<td>Email server and port</td>
<td>The host name or IP address and the port number of the server for outgoing email (outbound server).</td>
</tr>
<tr>
<td>User name</td>
<td>The user name for connecting to the outbound server.</td>
</tr>
<tr>
<td>Authentication type</td>
<td>The authentication method for connecting to the outbound server.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for connecting to the outbound server (if required).</td>
</tr>
<tr>
<td>Use same password as for incoming email</td>
<td>Use the password that is specified for incoming email.</td>
</tr>
<tr>
<td>SSL/TLS</td>
<td>The connection to the outbound server is secured by SSL or TLS (depending on what the server supports).</td>
</tr>
</tbody>
</table>

**15.22.17 LDAP configuration (macOS user policy)**

With the LDAP configuration you add user information from an LDAP directory to the macOS Address Book app.

**Note**

To configure a Mac to join an Active Directory domain, use the Directory service configuration. See Directory service configuration (macOS device policy) (page 192).

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account description</td>
<td>A description of the LDAP connection.</td>
</tr>
<tr>
<td>Host name</td>
<td>The host name or IP address of the LDAP server.</td>
</tr>
<tr>
<td>User name</td>
<td>The login credentials of the user Sophos Mobile uses to connect to the LDAP server.</td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
<tr>
<td>Use SSL/TLS</td>
<td>The connection to the LDAP server is secured by SSL or TLS (depending on what the server supports).</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Search settings</td>
<td>The nodes in the LDAP tree where to start searching from, and what scope to search in.</td>
</tr>
<tr>
<td>Base</td>
<td>The path to the node the search starts from. For example: ou=users,o=my company</td>
</tr>
<tr>
<td>Scope</td>
<td>The scope of sub-nodes to include in the search:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Base node only</strong>: Only the base node.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Base node and direct child nodes</strong>: The base node and its child nodes, i.e. the first-level sub-nodes.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Base node and all sub-nodes</strong>: The base node and all sub nodes to infinite depth.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the search setting.</td>
</tr>
</tbody>
</table>

### 15.23 Configurations for Windows Mobile policies

With a Windows Mobile policy you configure various aspects of Windows Mobile devices, like password policies, restrictions or Wi-Fi settings.

For information on how to create a Windows Mobile policy, see Create profile or policy [page 77].

### 15.23.1 Password policies configuration (Windows Mobile policy)

With the **Password policies** configuration you define requirements for the device password.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password type</td>
<td>The type of password users must define:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Alphanumeric</strong>: Password must contain both digits and letters</td>
</tr>
<tr>
<td></td>
<td>• <strong>Numeric</strong>: Password must only contain digits</td>
</tr>
<tr>
<td></td>
<td>For Windows Phone 8.1, <strong>Alphanumeric</strong> covers passwords that contain digits and/or letters.</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Minimum complexity of alphanumeric passwords</strong></td>
<td>This defines the character classes that must be used in an alphanumeric password.</td>
</tr>
<tr>
<td></td>
<td><strong>For Windows 10 Mobile:</strong></td>
</tr>
<tr>
<td></td>
<td>• 1: Not applicable [if selected, 2 is used]</td>
</tr>
<tr>
<td></td>
<td>• 2: Digits and lowercase letters are required</td>
</tr>
<tr>
<td></td>
<td>• 3: Digits, lowercase letters, and uppercase letters are required</td>
</tr>
<tr>
<td></td>
<td>• 4: Digits, lowercase letters, uppercase letters, and special characters are required</td>
</tr>
<tr>
<td></td>
<td><strong>For Windows Phone 8.1, the value you select is the number of different character classes that must be used in a password. Character classes are:</strong></td>
</tr>
<tr>
<td></td>
<td>• Digits</td>
</tr>
<tr>
<td></td>
<td>• Lowercase letters</td>
</tr>
<tr>
<td></td>
<td>• Uppercase letters</td>
</tr>
<tr>
<td></td>
<td>• Special characters</td>
</tr>
<tr>
<td><strong>Allow simple password</strong></td>
<td>Passwords can contain sequential or repeated characters, for example abcd or 1111.</td>
</tr>
<tr>
<td><strong>Minimum password length</strong></td>
<td>The minimum number of characters a password must contain.</td>
</tr>
<tr>
<td><strong>Maximum number of failed attempts</strong></td>
<td>The number of failed login attempts to enter the correct password before the device is wiped. Enter a value between 1 and 999, or 0 for no restriction.</td>
</tr>
<tr>
<td><strong>Time in minutes until the device is locked</strong></td>
<td>The time period [in minutes] after which the device is locked if it has not been used. The user can unlock the device. Enter a value between 1 and 999, or 0 for no restriction.</td>
</tr>
<tr>
<td><strong>Password history</strong></td>
<td>The number of old passwords that are remembered and compared with new ones. When the user defines a new password, it is not accepted if it matches a previously used password. Enter a value between 1 and 999, or 0 for no restriction.</td>
</tr>
<tr>
<td><strong>Maximum password age in days</strong></td>
<td>The number of days after which users must change their password. Enter a value between 1 and 730, or 0 for no restriction.</td>
</tr>
</tbody>
</table>
### Setting/Field Description

| Allow the password grace period to be set | Users are allowed to set the password grace period. |

### 15.23.2 Restrictions configuration (Windows Mobile policy)

With the **Restrictions** configuration you define restrictions for devices.

#### Device

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Forbid SD card</strong></td>
<td>Users cannot access the storage card. This does not prevent apps from accessing the storage card.</td>
</tr>
<tr>
<td><strong>Forbid unencrypted device</strong></td>
<td>Internal storage encryption is turned on.</td>
</tr>
<tr>
<td><strong>Important</strong></td>
<td>After internal storage encryption has been turned on on a device, you cannot turn it off again through a policy.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You must enable BitLocker on the device before applying the policy.</td>
</tr>
<tr>
<td><strong>Forbid action center notifications above lock screen</strong></td>
<td>No Action Center notifications are displayed above the device lock screen.</td>
</tr>
<tr>
<td><strong>Forbid manual addition of non-Microsoft email accounts</strong></td>
<td>Forbids adding all types of email accounts, as well as Exchange, Office 365 and Outlook.com accounts.</td>
</tr>
<tr>
<td><strong>Forbid Microsoft account connection</strong></td>
<td>The Microsoft account is the system account used for synchronization, backup and the Store.</td>
</tr>
<tr>
<td><strong>Forbid developer mode</strong></td>
<td>The Windows developer mode is turned off.</td>
</tr>
<tr>
<td><strong>Forbid Microsoft Store</strong></td>
<td>The app store is unavailable.</td>
</tr>
<tr>
<td><strong>Forbid native browser</strong></td>
<td>The Microsoft Edge browser is unavailable.</td>
</tr>
<tr>
<td><strong>Forbid camera</strong></td>
<td>The Privacy setting <strong>Let apps use my camera</strong> is turned off.</td>
</tr>
</tbody>
</table>
### Setting/Field

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Telemetry level</strong></td>
<td>The amount of Windows diagnostic and usage data that devices are allowed to send.</td>
</tr>
<tr>
<td>Windows 10:</td>
<td></td>
</tr>
<tr>
<td>• <strong>Full</strong>: All data required to identify and analyze issues.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Enhanced</strong>: Data about how Windows and apps are used and how they perform.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Basic</strong>: A limited set of data that’s critical for understanding the device and its configuration.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Disabled (Windows Phone 8.1 only)</strong>: Not supported on Windows 10 devices. If you select this, the <strong>Basic</strong> level is used.</td>
<td></td>
</tr>
</tbody>
</table>

**Note**
Levels are cumulative from bottom to top, e.g. **Enhanced** includes all data from **Basic**.

**Tip**
For detailed information on the telemetry levels, see the Microsoft article [Configure Windows telemetry in your organization](#).[external link]

Windows Phone 8.1 doesn’t support different telemetry levels:
- **Full, Enhanced, Basic**: Users can turn telemetry on or off.
- **Disabled (Windows Phone 8.1 only)**: No telemetry data is submitted.

### Various

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Forbid copy and paste</strong></td>
<td>The clipboard is unavailable.</td>
</tr>
<tr>
<td><strong>Forbid Cortana</strong></td>
<td>Cortana is turned off.</td>
</tr>
<tr>
<td><strong>Forbid &quot;Save as&quot; for Office files</strong></td>
<td>Users cannot save a file on the device as an Office file.</td>
</tr>
<tr>
<td><strong>Forbid screen capture</strong></td>
<td>Screen captures are turned off.</td>
</tr>
<tr>
<td><strong>Forbid sharing of Office files</strong></td>
<td>Users cannot share Office files.</td>
</tr>
<tr>
<td><strong>Forbid &quot;Sync my settings&quot;</strong></td>
<td>Device settings cannot be synchronized to and from other Windows devices.</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Forbid voice recording</td>
<td>Voice recording is turned off.</td>
</tr>
</tbody>
</table>

**Wi-Fi**

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forbid Wi-Fi</td>
<td>Wi-Fi connections are turned off.</td>
</tr>
<tr>
<td>Forbid internet sharing</td>
<td>Internet Connection Sharing (ICS) is turned off.</td>
</tr>
<tr>
<td>Forbid Wi-Fi Sense (hotspot auto-connect)</td>
<td>The device does not automatically connect to Wi-Fi hotspots.</td>
</tr>
<tr>
<td>Forbid hotspot reporting</td>
<td>The device does not send information about Wi-Fi connections.</td>
</tr>
<tr>
<td>Forbid manual configuration</td>
<td>Users cannot configure Wi-Fi connections beyond the connections that are configured by Sophos Mobile.</td>
</tr>
</tbody>
</table>

**Connectivity**

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forbid NFC</td>
<td>NFC (near-field communication) is turned off.</td>
</tr>
<tr>
<td>Forbid Bluetooth</td>
<td>Bluetooth is turned off.</td>
</tr>
<tr>
<td>Forbid USB connection</td>
<td>USB connection between the device and a computer to sync files or to use developer tools to deploy or debug apps is forbidden. This does not affect USB charging.</td>
</tr>
</tbody>
</table>

**Roaming and costs**

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forbid cellular data roaming</td>
<td>Data connections over foreign cellular networks are turned off.</td>
</tr>
<tr>
<td>Forbid VPN over cellular</td>
<td>VPN connections over cellular networks are turned off.</td>
</tr>
<tr>
<td>Forbid VPN roaming over cellular</td>
<td>VPN connections over foreign cellular networks are turned off.</td>
</tr>
</tbody>
</table>
## Security and privacy

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forbid Bing Vision to store images from Bing Vision search</td>
<td>Bing Vision does not store the contents of the images captured when performing Bing Vision search.</td>
</tr>
<tr>
<td>Forbid use of location when searching</td>
<td>The search cannot utilize location information.</td>
</tr>
<tr>
<td>Forbid manual installation of root certificates</td>
<td>Users cannot manually install root and intermediate CA certificates.</td>
</tr>
<tr>
<td>Forbid locating</td>
<td>All location privacy settings on the device are turned off. No apps can use the location service. This also forbids Sophos Mobile to locate the device.</td>
</tr>
<tr>
<td>SafeSearch permission</td>
<td>The level of search result filtering that is enforced on the device:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Moderate</strong>: Moderate filtering against adult content. Valid search results are not filtered.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Strict</strong>: Highest filtering against adult content.</td>
</tr>
</tbody>
</table>

### Unenrollment

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forbid user to reset the phone</td>
<td>Users cannot factory reset the device through the control panel or hardware key combinations.</td>
</tr>
<tr>
<td>Forbid manual MDM unenrollment</td>
<td>Users cannot delete the workplace account.</td>
</tr>
</tbody>
</table>

### 15.23.3 Exchange account configuration (Windows Mobile policy)

With the Exchange account configuration you set up a connection to a Microsoft Exchange Server email server.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account name</td>
<td>The account name.</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Exchange server</strong></td>
<td>The Exchange server address.</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>The domain for this account.</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>The user for this account.</td>
</tr>
<tr>
<td><strong>Email address</strong></td>
<td>The email address of the account.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The password for this account.</td>
</tr>
<tr>
<td><strong>Synchronization period</strong></td>
<td>The time period used for synchronizing emails. Only the emails from within the specified period are synchronized to the inbox on the managed device.</td>
</tr>
<tr>
<td><strong>Synchronization interval</strong></td>
<td>The interval between email synchronization processes.</td>
</tr>
<tr>
<td><strong>SSL/TLS</strong></td>
<td>The connection to the Exchange server is secured by SSL or TLS (depending on what the server supports). We recommend that you select this check box.</td>
</tr>
<tr>
<td><strong>Synchronize content types</strong></td>
<td>The content types to be synchronized.</td>
</tr>
</tbody>
</table>

**Note**
If you use the Sophos Mobile EAS proxy, enter the URL of the EAS proxy server.

---

**15.23.4 Wi-Fi configuration (Windows Mobile policy)**

With the Wi-Fi configuration you specify settings for connecting to Wi-Fi networks.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SSID</strong></td>
<td>In this field, enter the ID of the Wi-Fi network.</td>
</tr>
<tr>
<td><strong>Connect automatically</strong></td>
<td>The connection will be established automatically.</td>
</tr>
<tr>
<td><strong>Hidden network</strong></td>
<td>The target network is not open or visible.</td>
</tr>
</tbody>
</table>
### 15.23.5 App restrictions configuration [Windows Mobile policy]

With the **App restrictions** configuration you specifically allow or block apps on the devices.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allowed apps</strong></td>
<td>Contains a set of individual apps that users are allowed to install and use on the device. Users will be unable to install or use any apps that are not explicitly listed. Use <strong>Allowed apps</strong> when you know the list of apps that you want to allow and want to block all other apps.</td>
</tr>
<tr>
<td><strong>Forbidden apps</strong></td>
<td>Contains a set of individual apps that users are prevented from installing on the device. Users will be able to install any apps that are not explicitly listed. Use <strong>Forbidden apps</strong> when you know the list of apps that you want to block and want to allow all other apps.</td>
</tr>
<tr>
<td><strong>App group</strong></td>
<td>Select the app group that contains the list of apps you want to allow or block.</td>
</tr>
</tbody>
</table>

**Note**

The app group has to be created beforehand. See **App groups** (page 261).

### 15.23.6 Root certificate configuration [Windows Mobile policy]

With the **Root certificate** configuration you install a root certificate onto devices.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. The name of the certificate is shown in the **Certificate name** field. Enter the password for the selected certificate.
**Note**

The certificate you upload here is only available for this policy. If you require certificates in other profiles or policies, you have to upload them again.

---

### 15.23.7 SCEP configuration (Windows Mobile policy)

With the **SCEP** configuration you enable devices to request certificates from a Certificate Authority using the Simple Certificate Enrollment Protocol (SCEP).

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>A description for the configuration.</td>
</tr>
<tr>
<td>URL</td>
<td>The web address of the Certificate Authority server. Use the variable %_SCEPPROXYURL% to refer to the server URL that is configured on the <strong>SCEP</strong> tab of the System setup page.</td>
</tr>
<tr>
<td>Subject</td>
<td>The name of the entity (for example person or device) that will receive the certificate. You can use placeholders for user data or device properties. The value that you enter (with placeholders replaced by the actual data) must be a valid X.500 name. For example: • Enter CN=%_USERNAME% to specify a user. • Enter CN=%_DEVPROP(serial_number)% to specify a device. For information on available placeholders, see Placeholders in profiles and policies [page 81].</td>
</tr>
<tr>
<td>Subject Alternative Name</td>
<td>Optionally, configure one or more Subject Alternative Name (SAN) values. Click <strong>Add</strong> and then enter a SAN type and a SAN value.</td>
</tr>
<tr>
<td>Challenge</td>
<td>The web address to obtain a challenge password from the SCEP server. Use the variable %_CACHALLENGE% to refer to the challenge URL that is configured on the <strong>SCEP</strong> tab of the System setup page.</td>
</tr>
</tbody>
</table>
### Setting/Field | Description
---|---
**Root certificate** | The CA certificate. Select the certificate from the list. The list contains all certificates that you have uploaded in **Root certificate** configurations of the current profile.

**Retries** | The number of retries if the server sends a response of type *pending*.

**Retry delay** | The number of seconds between retries.

**Key size** | The size of the public key in the issued certificate. Make sure that the value matches the size configured on the SCEP server.

**Use as digital signature** | If you select this check box, the public key can be used as a digital signature.

**Use for encryption** | If you select this check box, the public key can be used for data encryption.

**Hash algorithm** | Select one or more hash algorithms that are supported by the SCEP server.

*Warning*
We recommend that you don’t use the SHA-1 algorithm because it is considered unsafe.

---

### 15.23.8 IMAP/POP configuration (Windows Mobile policy)

With the **IMAP/POP** configuration you add an IMAP or POP email account to the device.

| Setting/Field | Description |
---|---|
**Account type** | The type of the email server for incoming email (either **IMAP** or **POP**).

**Account name** | The display name of the email account on the device.

**Email address** | The email address of the account. Use the variable `%_EMAILADDRESS_%` to refer to the email address of the user that is assigned to the device.

**User display name** | The display name of the user for outgoing email. Use the variable `%_USERNAME_%` to refer to the name of the user that is assigned to the device.
<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User name</strong></td>
<td>The user name for connecting to the inbound server.</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>The domain part of the credentials for the inbound server (if required).</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The password for connecting to the inbound server (if required).</td>
</tr>
</tbody>
</table>
| **Server for incoming email** | The host name (or the IP address) and the port number of the server for incoming email (inbound server). Format: server name:port number You don’t need to specify the port number if the standard port is used:  
  • 143 (IMAP)  
  • 993 (IMAP with SSL)  
  • 110 (POP3)  
  • 995 (POP3 with SSL) |
| **Use SSL/TLS for incoming email** | Use Secure Sockets Layer for incoming email transfer.                      |
| **Server for outgoing email** | The host name (or the IP address) and the port number of the server for outgoing email (outbound server). Format: server name:port number |
| **Use SSL/TLS for outgoing email** | Use Secure Sockets Layer for outgoing email transfer.                   |
| **Authentication required for outgoing connection** | The outbound server requires authentication. The same credentials as for the inbound server are used, as specified in the **User name**, **Domain** and **Password** fields. |
| **Synchronization period**    | The time period used for synchronizing emails. Only the emails from within the specified period are synchronized to the inbox on the managed device. |
| **Automatic synchronization** | The interval for automatic email synchronization.                           |

### 15.24 Configurations for Windows policies

With a Windows policy you configure various aspects of Windows computers, like password policies, restrictions or Wi-Fi settings.

For information on how to create a Windows policy, see Create profile or policy (page 77).
15.24.1 Password policies configuration (Windows policy)

With the Password policies configuration you define requirements for the passwords of Windows user accounts.

Note
Password complexity rules (for example length, number of uppercase and lowercase letters) for Windows computers are fixed and cannot be set by a Sophos Mobile policy. For details see Windows password complexity rules (page 80).

Note
Password policies can't be assigned to Windows computers if the following conditions are both met:

- There are other local users configured on the device in addition to the user that is enrolled with Sophos Mobile.
- One or more of these other users are not allowed to change their password.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of failed attempts</td>
<td>The number of failed login attempts to enter the correct password before the device is wiped. Enter a value between 1 and 999, or 0 for no restriction.</td>
</tr>
<tr>
<td>Time in minutes until the device is locked</td>
<td>The time period (in minutes) after which the device is locked if it has not been used. The user can unlock the device. Enter a value between 1 and 999, or 0 for no restriction.</td>
</tr>
<tr>
<td>Password history</td>
<td>The number of old passwords that are remembered and compared with new ones. When the user defines a new password, it is not accepted if it matches a previously used password. Enter a value between 1 and 999, or 0 for no restriction.</td>
</tr>
<tr>
<td>Maximum password age in days</td>
<td>The number of days after which users must change their password. Enter a value between 1 and 730, or 0 for no restriction.</td>
</tr>
</tbody>
</table>
15.24.2 Restrictions configuration (Windows policy)

With the Restrictions configuration you define restrictions for devices.

### Device

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Forbid SD card</strong></td>
<td>Users cannot access the storage card. This does not prevent apps from accessing the storage card.</td>
</tr>
<tr>
<td><strong>Forbid manual addition of non-Microsoft email accounts</strong></td>
<td>Forbids adding all types of email accounts, as well as Exchange, Office 365 and Outlook.com accounts.</td>
</tr>
<tr>
<td><strong>Forbid developer mode</strong></td>
<td>The Windows developer mode is turned off.</td>
</tr>
<tr>
<td><strong>Forbid camera</strong></td>
<td>The Privacy setting Let apps use my camera is turned off.</td>
</tr>
<tr>
<td><strong>Disable Edge autofill</strong></td>
<td>The Save form entries setting in the Edge web browser is turned off and cannot be turned on by the user.</td>
</tr>
<tr>
<td><strong>Disable Edge F12 Developer Tools</strong></td>
<td>The F12 Developer Tools of the Edge web browser are unavailable.</td>
</tr>
<tr>
<td><strong>Disable Edge pop-up blocker</strong></td>
<td>The Block pop-ups setting in the Edge web browser is turned off and cannot be turned on by the user.</td>
</tr>
<tr>
<td><strong>Disable AutoPlay settings</strong></td>
<td>The relevant sections of the Windows Control Panel are unavailable. The user cannot change any of these settings after the policy has been assigned to the device.</td>
</tr>
<tr>
<td><strong>Disable Date &amp; Time settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Disable Language settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Disable Power &amp; Sleep settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Disable Region settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Disable Sign-in settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Disable VPN settings</strong></td>
<td>Note Disable AutoPlay settings does not affect connected devices, like for example mobile phones.</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Disable Workplace settings</td>
<td></td>
</tr>
<tr>
<td>Disable Account settings</td>
<td></td>
</tr>
<tr>
<td>Telemetry level</td>
<td>The amount of Windows diagnostic and usage data that devices are allowed to send.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Full</strong>: All data required to identify and analyze issues.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enhanced</strong>: Data about how Windows and apps are used and how they perform.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Basic</strong>: A limited set of data that’s critical for understanding the device and its configuration.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Security</strong>: Information that is required to keep the device protected with the latest security updates.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Levels are cumulative from bottom to top, e.g. <strong>Enhanced</strong> includes all data from <strong>Basic</strong> and <strong>Security</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong></td>
</tr>
<tr>
<td></td>
<td>For detailed information on the telemetry levels, see the Microsoft article <a href="https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-telemetry">Configure Windows telemetry in your organization</a>.</td>
</tr>
</tbody>
</table>

### Various

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forbid Cortana</td>
<td>Cortana is turned off.</td>
</tr>
<tr>
<td>Forbid &quot;Sync my settings&quot;</td>
<td>Device settings cannot be synchronized to and from other Windows devices.</td>
</tr>
<tr>
<td>Disable Windows tips</td>
<td>The Windows notification setting <strong>Show me tips about Windows</strong> is cleared and unavailable.</td>
</tr>
</tbody>
</table>

### Wi-Fi

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forbid internet sharing</td>
<td>Internet Connection Sharing (ICS) is turned off.</td>
</tr>
<tr>
<td>Forbid Wi-Fi Sense (hotspot auto-connect)</td>
<td>The device does not automatically connect to Wi-Fi hotspots.</td>
</tr>
</tbody>
</table>
Connectivity

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forbid Bluetooth</td>
<td>Bluetooth is turned off.</td>
</tr>
</tbody>
</table>

Security and privacy

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forbid use of location when searching</td>
<td>The search cannot utilize location information.</td>
</tr>
</tbody>
</table>

Unenrollment

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forbid manual MDM unenrollment</td>
<td>Users cannot delete the workplace account.</td>
</tr>
</tbody>
</table>

15.24.3 Exchange account configuration (Windows policy)

With the Exchange account configuration you set up a connection to a Microsoft Exchange Server email server.

**Important**

If you use multiple configurations to set up Exchange email accounts, the devices might only be able to retrieve mail for one account. This typically happens when the accounts are located on different Exchange servers and there are different mailbox policies defined on these servers. Because Windows computers can only enforce a single mailbox policy, they will fail to connect to the accounts that use a different policy.

**Note**

Windows allows the user to reject all changes that you make to the Exchange configuration.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account name</td>
<td>The account name.</td>
</tr>
</tbody>
</table>
### Setting/Field | Description
--- | ---
**Exchange server** | The Exchange server address.  
  **Note**  
  If you use the Sophos Mobile EAS proxy, enter the URL of the EAS proxy server.
**Domain** | The domain for this account.  
**User** | The user for this account.  
  If you enter the variable `%USERNAME%`, the server replaces it with the actual user name.
**Email address** | The email address of the account.  
  If you enter the variable `%EMAILADDRESS%`, the server replaces it with the actual email address.
**Password** | The password for this account.  
  If you leave this field empty, users must enter the password on their devices.
**Synchronization period** | The time period used for synchronizing emails.  
  Only the emails from within the specified period are synchronized to the inbox on the managed device.
**Synchronization interval** | The interval between email synchronization processes.
**SSL/TLS** | The connection to the Exchange server is secured by SSL or TLS (depending on what the server supports).  
  We recommend that you select this check box.
**Synchronize content types** | The content types to be synchronized.

### 15.24.4 Wi-Fi configuration (Windows policy)

With the Wi-Fi configuration you specify settings for connecting to Wi-Fi networks.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SSID</strong></td>
<td>In this field, enter the ID of the Wi-Fi network.</td>
</tr>
<tr>
<td><strong>Connect automatically</strong></td>
<td>The connection will be established automatically.</td>
</tr>
<tr>
<td><strong>Hidden network</strong></td>
<td>The target network is not open or visible.</td>
</tr>
</tbody>
</table>
15.24.5 Root certificate configuration (Windows policy)

With the **Root certificate** configuration you install a root certificate onto devices. In the **File** field, navigate to the relevant certificate and click **Upload a file**. The name of the certificate is shown in the **Certificate name** field. Enter the password for the selected certificate.

**Note**
The certificate you upload here is only available for this policy. If you require certificates in other profiles or policies, you have to upload them again.

15.24.6 IMAP/POP configuration (Windows policy)

With the **IMAP/POP** configuration you add an IMAP or POP email account to Windows computers.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Account type</strong></td>
<td>The type of the email server for incoming email (either <strong>IMAP</strong> or <strong>POP</strong>).</td>
</tr>
<tr>
<td><strong>Account name</strong></td>
<td>The display name of the email account on the device.</td>
</tr>
<tr>
<td><strong>Email address</strong></td>
<td>The email address of the account. Use the variable <code>%_EMAILADDRESS_%</code> to refer to the email address of the user that is assigned to the device.</td>
</tr>
<tr>
<td><strong>User display name</strong></td>
<td>The display name of the user for outgoing email. Use the variable <code>%_USERNAME_%</code> to refer to the name of the user that is assigned to the device.</td>
</tr>
<tr>
<td><strong>User name</strong></td>
<td>The user name for connecting to the inbound server.</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>The domain part of the credentials for the inbound server (if required).</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The password for connecting to the inbound server (if required).</td>
</tr>
</tbody>
</table>
### Setting/Field Description

**Server for incoming email**

The host name (or the IP address) and the port number of the server for incoming email (inbound server).

*Format:* `server name:port number`

You don’t need to specify the port number if the standard port is used:

- 143 (IMAP)
- 993 (IMAP with SSL)
- 110 (POP3)
- 995 (POP3 with SSL)

**Use SSL/TLS for incoming email**

Use Secure Sockets Layer for incoming email transfer.

**Server for outgoing email**

The host name (or the IP address) and the port number of the server for outgoing email (outbound server).

*Format:* `server name:port number`

**Use SSL/TLS for outgoing email**

Use Secure Sockets Layer for outgoing email transfer.

**Authentication required for outgoing connection**

The outbound server requires authentication.

The same credentials as for the inbound server are used, as specified in the User name, Domain and Password fields.

**Synchronization period**

The time period used for synchronizing emails.

Only the emails from within the specified period are synchronized to the inbox on the managed device.

**Automatic synchronization**

The interval for automatic email synchronization.

---

### 15.25 Configurations for Windows IoT policies

With a Windows IoT policy you configure various aspects of Windows IoT devices, like restrictions or Wi-Fi settings.

For information on how to create a Windows IoT policy, see Create profile or policy (page 77).
## 15.25.1 Restrictions configuration (Windows IoT policy)

With the **Restrictions** configuration you define restrictions for devices.

### Device

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Forbid SD card</strong></td>
<td>Users cannot access the storage card. This does not prevent apps from accessing the storage card.</td>
</tr>
<tr>
<td><strong>Forbid developer mode</strong></td>
<td>The Windows developer mode is turned off.</td>
</tr>
<tr>
<td><strong>Forbid camera</strong></td>
<td>The Privacy setting <strong>Let apps use my camera</strong> is turned off.</td>
</tr>
<tr>
<td><strong>Disable Edge autofill</strong></td>
<td>The <strong>Save form entries</strong> setting in the Edge web browser is turned off and cannot be turned on by the user.</td>
</tr>
<tr>
<td></td>
<td>If the check box is cleared, the setting is turned on and cannot be turned off by the user.</td>
</tr>
<tr>
<td><strong>Disable Edge pop-up blocker</strong></td>
<td>The <strong>Block pop-ups</strong> setting in the Edge web browser is turned off and cannot be turned on by the user.</td>
</tr>
<tr>
<td></td>
<td>If the check box is cleared, the setting is turned on and cannot be turned off by the user.</td>
</tr>
</tbody>
</table>
### Telemetry level

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telemetry level</td>
<td>The amount of Windows diagnostic and usage data that devices are allowed to send.</td>
</tr>
<tr>
<td><strong>Full</strong></td>
<td>All data required to identify and analyze issues.</td>
</tr>
<tr>
<td><strong>Enhanced</strong></td>
<td>Data about how Windows and apps are used and how they perform.</td>
</tr>
<tr>
<td><strong>Basic</strong></td>
<td>A limited set of data that’s critical for understanding the device and its configuration.</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>Information that is required to keep the device protected with the latest security updates.</td>
</tr>
</tbody>
</table>

**Note**
Levels are cumulative from bottom to top, e.g. **Enhanced** includes all data from **Basic** and **Security**.

**Tip**
For detailed information on the telemetry levels, see the Microsoft article [Configure Windows telemetry in your organization](https://docs.microsoft.com/en-us/windows/security/identity-validation/configure-windows-telemetry-in-your-organization).

### Wi-Fi

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forbid internet sharing</td>
<td>Internet Connection Sharing (ICS) is turned off.</td>
</tr>
<tr>
<td>Forbid Wi-Fi Sense (hotspot auto-connect)</td>
<td>The device does not automatically connect to Wi-Fi hotspots.</td>
</tr>
</tbody>
</table>

### Connectivity

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forbid Bluetooth</td>
<td>Bluetooth is turned off.</td>
</tr>
</tbody>
</table>

### 15.25.2 Wi-Fi configuration (Windows IoT policy)

With the **Wi-Fi** configuration you specify settings for connecting to Wi-Fi networks.

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
<td>In this field, enter the ID of the Wi-Fi network.</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Connect automatically</td>
<td>The connection will be established automatically.</td>
</tr>
<tr>
<td>Hidden network</td>
<td>The target network is not open or visible.</td>
</tr>
<tr>
<td>Security type</td>
<td>Select the security type from the list. If you select <strong>WPA (Personal)</strong> or <strong>WPA2 (Personal)</strong> you must specify the password.</td>
</tr>
</tbody>
</table>

### 15.25.3 Root certificate configuration (Windows IoT policy)

With the **Root certificate** configuration you install a root certificate onto devices.

In the **File** field, navigate to the relevant certificate and click **Upload a file**. The name of the certificate is shown in the **Certificate name** field. Enter the password for the selected certificate.

**Note**

The certificate you upload here is only available for this profile. If you require certificates in other profiles or policies, you have to upload them again.
16 Task bundles

By using task bundles you can bundle several tasks in one transaction. So you can bundle all tasks necessary to have a device enrolled and configured:

- Enroll the device.
- Apply required policies.
- Install required apps (for example managed apps for iOS devices).
- Apply required profiles.

You can also include wipe commands in task bundles to automatically wipe non-compliant (for example jailbroken or rooted) devices. For further information, see Compliance policies (page 39).

Task bundles are available for the following platforms:

- Android
- iOS
- macOS
- Windows

16.1 Create task bundle

1. On the menu sidebar, under CONFIGURE, click Task bundles and then click the platform for which you want to create a task bundle.
2. On the Task bundles page, click Create task bundle.
The Edit task bundle page is displayed.
3. Enter a name and, optionally, a description for the new task bundle in the relevant fields.
The version is automatically incremented every time you save the task bundle.
4. Optional: Select Selectable for compliance actions to transfer the task bundle onto a device when it violates a compliance rule. See Compliance policies (page 39).

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

5. Optional: For iOS task bundles, select Ignore app installation failures to continue the task bundle processing even if an app installation fails. This option is disabled when the task bundle contains no Install app task.
6. Click Create task.
7. Select the task type and click Next.
The next view depends on the task type you have selected. In each view you can specify your own meaningful task names. These task names are shown during installation on the Self Service Portal.
8. Follow the wizard steps to add the required task and click Apply to create the task.
For Android task bundles, you can't mix Android and Android enterprise tasks. For example, you can't install an Android device profile and an Android work app with the same task bundle.

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

After you have added all required tasks to the task bundle, click Save on the Edit task bundle page. The task bundle is available for transfer. It is displayed on the Task bundles page.

When you edit an existing task bundle which is used as Initial package in the Self Service Portal settings, the enrollment task cannot be deleted. See Configure Self Service Portal settings (page 22).

The following task types are available for Android task bundles:

**Enroll**

When the task is transferred to devices, an enrollment email is sent to the email address that is configured for each device. Users must perform the steps that are described in the email to enroll their device.

When the task is transferred to a device that is already enrolled, no enrollment email is sent.

**Enroll Sophos container**

When the task is transferred to devices, an enrollment email is sent to the email address that is configured for each device. Users must perform the steps that are described in the email to enroll their device.

When the task is transferred to a device that is already enrolled, no enrollment email is sent.
Install profile

Select a profile or policy from the list of available profiles and policies. For information on how to add profiles or policies to this list, see Profiles and policies (page 77).

When the task is transferred to devices, the profile is silently installed or the policy is silently assigned.

Uninstall Profile

Under Select source, select Profiles and then select a profile from the list.

In addition to the profiles that are available on the Sophos Mobile server, the list includes profiles that are in use on the managed devices.

You can also uninstall a profile that is not contained in the list. Select Identifier and then enter the identifier of the profile you want to uninstall from devices.

When the task is transferred to devices, the profile is silently uninstalled.

Note

You cannot directly uninstall a Sophos container policy or a Mobile Security policy from devices. Instead, use the device action Unenroll Sophos container or Unenroll SMSec. This will also remove the related policies from the device.

Install app

Select an app from the list of all available apps. For information on how to add apps to this list, see Add app (page 244).

When the task is transferred to devices, users receive a notification on their devices that Sophos Mobile wants to install the app. Users can tap OK to start the process, or Not now to be notified again after a short period of time.

If users tap OK but then tap Cancel in the subsequent Android dialog, the task fails.

If the app is already installed on a device that receives the task, it is updated.

Install Android work app

This task type is available if you have configured Android enterprise for the customer.

Select an app from list of all available work apps. For information on how to add apps to this list, see Edit work app (page 276).

The installation task is sent to a Google service. Google then manages the installation of the app onto the device. On the Task view page, the task is displayed with state successful when it has been sent to Google.

Alternatively, you can install work apps from the Android work apps page. See Install work app (page 278).

For information on how to uninstall a work app from devices, see Uninstall work app (page 278).
**Remove app**

Under **Select source**, select **Apps** to select an app for removal from the list of available apps.

In addition to the apps that are available on the Sophos Mobile server, the list includes apps that are in use on the managed devices - with the exception of Android system apps and apps that have been pre-installed by the device manufacturer.

You can also remove an app that is not contained in the list. Select **Identifier** and then enter the package name of the app you want to remove from devices. If you select **Knox container app**, the app will be removed from the Samsung Knox container.

When the task is transferred to devices, users receive a notification on their devices that Sophos Mobile wants to remove the app. Users can tap **OK** to start the process, or **Not now** to be notified again after a short period of time.

If users tap **OK** but then tap **Cancel** in the subsequent Android dialog, the task fails.

If the app is not installed on a device that receives the task, no notification is displayed.

**Send message**

Enter a plain text to be displayed on the devices.

When the task is transferred to devices, the message text is displayed in a notification window. Users can display past messages on the **Messages** page of the Sophos Mobile Control app.

**Unenroll**

When the task is transferred to devices, they are unenrolled from Sophos Mobile. See **Unenroll devices** (page 55). Device users do not need to confirm the operation.

You can’t add an **Unenroll** task and a **Wipe** task to the same task bundle.

**Wipe**

When the task is transferred to devices, they are reset to their factory settings. Device users do not need to confirm the operation.

**Important**

Use this task type with care. All data on the devices that receive the task is deleted without user confirmation.

**Note**

When a **Wipe** task is transferred to a device enrolled with Sophos Mobile in Android Enterprise profile owner mode, only the work profile and all work apps are removed.

You can’t add an **Unenroll** task and a **Wipe** task to the same task bundle.
**Knox container: lock**

When the task is transferred to a Samsung device that supports Samsung Knox, the Knox container is locked.

**Knox container: unlock**

When the task is transferred to a Samsung device that supports Samsung Knox, the Knox container is unlocked.

**Knox container: reset password**

When the task is transferred to a Samsung device that supports Samsung Knox, the Knox container password is reset. Users must set a new password to unlock the Knox container.

**Knox container: remove**

When the task is transferred to a Samsung device that supports Samsung Knox, the Knox container (including any container-related configuration) is removed.

**Trigger SMSec scan**

When the task is transferred to devices, the Sophos Mobile Security app is silently triggered to perform a scan against malware and potentially unwanted apps (PUAs).

This task requires that Sophos Mobile Security is managed from Sophos Mobile, that is, a Mobile Security policy is assigned to the device. See Manage Sophos Mobile Security (page 283).

If Sophos Mobile Security is not managed by Sophos Mobile on a device that receives the task (that is, if a Mobile Security policy is not assigned to the device), the task remains in the state Will be retried.

### 16.3 Available iOS task types

The following task types are available for iOS task bundles:

**Enroll**

When the task is transferred to devices, an enrollment email is sent to the email address that is configured for each device. Users must perform the steps that are described in the email to enroll their device.

When the task is transferred to a device that is already enrolled, no enrollment email is sent.
**Enroll Sophos container**

When the task is transferred to devices, an enrollment email is sent to the email address that is configured for each device. Users must perform the steps that are described in the email to enroll their device.

When the task is transferred to a device that is already enrolled, no enrollment email is sent.

**Install profile**

Select a profile or policy from the list of available profiles and policies. For information on how to add profiles or policies to this list, see Profiles and policies (page 77).

When the task is transferred to devices, the profile is silently installed or the policy is silently assigned.

**Uninstall Profile**

Under Select source, select Profiles and then select a profile from the list.

In addition to the profiles that are available on the Sophos Mobile server, the list includes profiles that are in use on the managed devices.

You can also uninstall a profile that is not contained in the list. Select Identifier and then enter the identifier of the profile you want to uninstall from devices.

When the task is transferred to devices, the profile is silently uninstalled.

Note

You cannot directly uninstall a Sophos container policy from devices. Instead, use the device action Unenroll Sophos container. This will also remove the related policy from the device.

**Install provisioning profile**

Select an app provisioning profile from the list of available profiles. For information on how to add profiles to this list, see Import provisioning profiles for iOS apps (page 79).

When the task is transferred to devices, the provisioning profile is silently installed.

**Uninstall provisioning profile**

Under Select source, select Profiles and then select a provisioning profile from the list.

In addition to the profiles that are available on the Sophos Mobile server, the list includes profiles that are in use on the managed devices.

You can also remove a provisioning profile that is not contained in the list. Select Identifier and then enter the identifier of the profile you want to remove from devices.

When the task is transferred to devices, the provisioning profile is silently removed.
Reconfigure SMC app

When the task is transferred to a device, the user is asked to scan a QR code or to enter configuration details manually. This reconnects a previously uninstalled Sophos Mobile Control app to the server.

Note
This task should be preceded by an Install app task for the Sophos Mobile Control app.

Install app

Select an app from the list of all available apps. For information on how to add apps to this list, see Add app (page 244).

When the task is transferred to devices, users receive a notification on their devices that Sophos Mobile wants to install the app. Users can tap Install to start the process, or Cancel to reject the installation.

If users reject the installation, the task fails.

If the app is already installed on a device that receives the task, it is updated.

Remove app

Under Select source, select Apps to select an app for removal from the list of available apps.

In addition to the apps that are available on the Sophos Mobile server, the list includes apps that are in use on the managed devices - with the exception of iOS system apps.

You can also remove an app that is not contained in the list. Select Identifier and then enter the bundle ID of the app you want to remove from devices.

When the task is transferred to devices, the app is removed silently.

Install latest iOS update

When the task is transferred to devices, the latest available update of the iOS software is installed. Depending on the iOS device model, different updates might be installed.

You can update the iOS software for the following device types:

- Supervised devices with iOS 10.3 or higher
- Supervised Apple DEP devices

For other devices, the task will fail.

Send message

Enter a plain text to be displayed on the devices.

When the task is transferred to devices, the message text is displayed in a notification window. Users can display past messages on the Messages page of the Sophos Mobile Control app.
**Unenroll**

When the task is transferred to devices, they are unenrolled from Sophos Mobile. See [Unenroll devices](#) (page 55). Device users do not need to confirm the operation.

You can't add an **Unenroll** task and a **Wipe** task to the same task bundle.

**Wipe**

When the task is transferred to devices, they are reset to their factory settings. Device users do not need to confirm the operation.

**Important**

Use this task type with care. All data on the devices that receive the task is deleted without user confirmation.

You can't add an **Unenroll** task and a **Wipe** task to the same task bundle.

### 16.4 Available macOS task types

The following task types are available for macOS task bundles:

**Enroll**

When the task is transferred to devices, an enrollment email is sent to the email address that is configured for each device. Users must perform the steps that are described in the email to enroll their device.

When the task is transferred to a device that is already enrolled, no enrollment email is sent.

**Assign device policy**

Select a policy from the list of available macOS device policies. For information on how to add policies to this list, see [Profiles and policies](#) (page 77).

When the task is transferred to devices, the policy is silently assigned to the device. If a device policy is already assigned, it is replaced.

**Assign user policy**

Select a policy from the list of available macOS user policies. For information on how to add policies to this list, see [Profiles and policies](#) (page 77).

When the task is transferred to devices, the policy is silently assigned to the device. If a user policy is already assigned, it is replaced.

User policies are applied to users the next time they log in to the Mac.
Unenroll

When the task is transferred to devices, they are unenrolled from Sophos Mobile. See Unenroll devices (page 55). Device users do not need to confirm the operation.

You can’t add an Unenroll task and a Wipe task to the same task bundle.

Wipe

Set a 6-digit system lock PIN.

When the task is transferred to a Mac, macOS restarts and then begins wiping the disk. The user must enter the system lock PIN on the Mac to unlock it.

You can’t add an Unenroll task and a Wipe task to the same task bundle.

Important

Use this task type with care. All data on the devices that receive the task is deleted without user confirmation.

Tip

In Sophos Mobile Admin, the macOS system lock PIN is displayed on the device page under Device properties > Unlock passcode and on the Task details page under Lock PIN.

16.5 Available Windows task types

The following task types are available for Windows task bundles:

Enroll

When the task is transferred to devices, an enrollment email is sent to the email address that is configured for each device. Users must perform the steps that are described in the email to enroll their device.

When the task is transferred to a device that is already enrolled, no enrollment email is sent.

Assign policy

Select a policy from the list of available device policies. For information on how to add policies to this list, see Profiles and policies (page 77).

When the task is transferred to devices, the policy is silently assigned to the device. If a device policy is already assigned, it is replaced.
Install app

Select an app from the list of all available apps. For information on how to add apps to this list, see Add app (page 244).
When the task is transferred to devices, the app is installed silently.
If the app is already installed on a device that receives the task, it is updated.

Remove app

Select an app for removal.
The list of available apps includes apps you have configured on the Sophos Mobile server and apps installed on any of the managed Windows computers - with the exception of Windows system apps.
When the task is transferred to devices, the selected app is removed silently.

Note
You can only remove apps that have been installed by Sophos Mobile. If you try to remove an app installed by the user, the task fails.

Unenroll

When the task is transferred to devices, they are unenrolled from Sophos Mobile. See Unenroll devices (page 55). Device users do not need to confirm the operation.
You can’t add an Unenroll task and a Wipe task to the same task bundle.

Wipe

When the task is transferred to devices, they are reset to their factory settings. Device users do not need to confirm the operation.

Important
Use this task type with care. All data on the devices that receive the task is deleted without user confirmation.
You can’t add an Unenroll task and a Wipe task to the same task bundle.

16.6 Duplicate task bundles

Since creating a task bundle can be time-consuming, you can duplicate finished task bundles. This function is helpful if several extensive task bundles with similar tasks are required. Then only a few tasks need to be deleted or added.
1. On the menu sidebar, under CONFIGURE, click Task bundles and then click Android or iOS. The Task bundles page is displayed.
2. Click the blue triangle next to the task bundle you want to duplicate and then click Duplicate. The task bundle is duplicated and shown on the Task bundles page. You can now edit the duplicated task bundle as required. To edit the task bundle, click the blue triangle next to it and then click Edit.

16.7 Transfer task bundles to individual devices or to device groups

1. On the menu sidebar, under CONFIGURE, click Task bundles and then click Android or iOS. The Task bundles page is displayed.
2. Click the blue triangle next to the required task and then click Transfer. The Select devices page is displayed.
3. On this page, you can:
   - Select individual devices you want to transfer the task bundle to.
   - Click Select device groups, to open the Select device groups page and select one or several device groups for transferring the task bundle.
4. After you have made your selection, click Next. The Set execution date page is displayed.
5. Under Scheduled date, select Now or specify a date and time for the execution of this task.
6. Click Finish. The Task view page is shown.

The task bundle is transferred to the selected devices at the specified date and time.
17 Apps

You configure apps to make them available for installation from Sophos Mobile Admin (administrator-initiated) or from the Sophos Mobile Control app (user-initiated).

App management is available for the following platforms:

- Android
- iOS
- Windows Mobile

To make an app available in Sophos Mobile, you can do one of the following:

- Upload the app package to the Sophos Mobile server. This option is not available for Windows Mobile apps or for devices where Sophos Mobile only manages the Sophos container.
- Provide a link to the app in the relevant app store.

For both options, see section Add app (page 244).

To install an app on a device, create a task bundle that contains an Install app task. For Android and iOS devices, you can create such task bundles directly from the Apps page. See Install app (page 245).

Note

To be able to install app packages that are stored on the Sophos Mobile server (in contrast to the installation from the app store), the following conditions must be met:

- For Android, the Android security setting Unknown sources must be enabled on the devices. When you try to install an APK file when Unknown sources is disabled, the Sophos Mobile Control app will direct the users to the page where they can enable the setting. This restriction does not apply to devices with LG GATE, Samsung Knox or Sony Enterprise API.
- For iOS, the installation of apps from IPA files is only possible for self-developed apps. When the app is ready for distribution, you must create a provisioning profile for the app and make it available on the devices, either installed separately beforehand or included in the app's IPA file. You can use Sophos Mobile to distribute provisioning profiles to your iOS devices. See Import provisioning profiles for iOS apps (page 79). For details on provisioning profiles, see the iOS Developer Library.

17.1 Add app

You make an app available for installation either by uploading the app package or by linking to the app in the relevant app store.

1. On the menu sidebar, under CONFIGURE, click Apps and then click the platform for which you want to add the app.

2. Click Add app and then select the required option:
   - **Android package**: Add an Android app by uploading the APK file to Sophos Mobile.
   - **iOS package**: Add an iOS app by uploading the IPA file to Sophos Mobile.
   - **Android link**: Add an Android app by linking to it in Google Play.
• **iOS link**: Add an iOS app by linking to it in the App Store.
• **Windows Mobile link**: Add a Windows Mobile app by linking to it in Microsoft Store.
• **Windows MSI link**: Add a Windows app by linking to its MSI installation file.
• **Microsoft Store link**: Add a Windows app by linking to it in Microsoft Store.

3. Configure the app settings as required.
4. Click **Save** to save the app settings and to return to the **Apps** page.

The app is available for installation. It is displayed on the **Apps** page. If you have configured the **Available to device groups** field, the app is also displayed in the Enterprise App Store of the Sophos Mobile Control app from where users can install it. The installation process runs unattended or with very little user interaction.

**Note**
On devices where Sophos Mobile only manages the Sophos container, apps that you added by uploading the APK file (for Android apps) or IPA file (for iOS apps) are not available.

**Related reference**
- [App settings (Android)](page 247)
- [App settings (iOS)](page 249)
- [App settings (Windows Mobile)](page 250)
- [App settings (Windows)](page 251)

### 17.2 Install app

**Note**
This section does not apply to Android work apps. To install work apps, see [Install work app](page 278).

**Note**
This section does not apply to devices where Sophos Mobile only manages the Sophos container.

When you have added an app to Sophos Mobile as described in [Add app](page 244), you can manually install it on selected devices or device groups.

1. On the menu sidebar, under **CONFIGURE**, click **Apps** and then click the platform for which you want to install an app.
2. On the **Apps** page, click the blue triangle next to the required app and then click **Install**.
3. Select the devices on which you want to install the app. Do one of the following:
   - Select individual devices.
   - Click **Select device groups** and then select one or more device groups.
   
   When you are ready, click **Next**.
4. On the **Set execution date** page, specify the date when the app will be installed:
   - Select **Now** for an immediate execution.
Select Date and then enter a date and a time for a scheduled execution.

5. Click Finish.

The selected app is installed onto the selected devices at the specified date.

**Note**

On the following devices apps are installed silently, that is without user interaction:

- Supervised iOS devices
- Android devices with Samsung Knox Standard SDK 5.1 or higher
- Android devices with LG GATE
- Android devices with Sony Enterprise API version 8 or higher
- Windows computers, if you have configured the `/quiet` installation option for the app.

**Tip**

You can display the status of the installation task on the Task view page.

**Tip**

You can also install an app by using one of the following options:

- To install an app on a single device: On the device’s Show device page, select the Installed apps tab and click Install app.
- To install an app on several devices: On the Devices page, select the required devices and then click Actions > Install app.
- To install an app on one or more devices as part of a task bundle: Add an Install app task to the task bundle and transfer it to the required devices or device groups.

### 17.3 Uninstall app

**Note**

This section does not apply to Android work apps. To uninstall work apps, see Uninstall work app (page 278).

**Note**

This section does not apply to devices where Sophos Mobile only manages the Sophos container.

When you have added an app to Sophos Mobile as described in Add app (page 244), you can manually uninstall it from selected devices or device groups.

1. On the menu sidebar, under **CONFIGURE**, click **Apps** and then click the platform for which you want to uninstall an app.
2. On the **Apps** page, click **Uninstall**.
3. Select the devices from which you want to uninstall an app. Do one of the following:
   • Select individual devices.
   • Click Select device groups and then select one or more device groups.
   When you are ready, click Next.
4. On the Select app page, select the required app.
5. On the Set execution date page, specify the date when the app will be uninstalled:
   • Select Now for an immediate execution.
   • Select Date and then enter a date and a time for a scheduled execution.
6. Click Finish.
   The selected app is uninstalled from the selected devices at the specified date.

Note
On the following devices apps are uninstalled silently, that is without user interaction:
   • Managed apps on supervised iOS devices
   • Windows computers, if you have configured the /quiet installation option for the app.

Tip
Alternatively, you can use the following procedure to uninstall an app from a single device: Open the device’s Show device page, go to the Installed apps tab and then click the trash can icon next to the app name.

17.4 App settings (Android)

General settings

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the app.</td>
</tr>
<tr>
<td>Version</td>
<td>For app packages, the version that is displayed in the Enterprise App Store. For app links, Sophos Mobile uses the version from Google Play.</td>
</tr>
<tr>
<td>App identifier</td>
<td>The internal identifier of the app. Leave this field empty if you do not know the exact identifier. In most cases, Sophos Mobile can read the value from the app itself and then fills in this field automatically.</td>
</tr>
</tbody>
</table>
## Settings for app links

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Link</strong></td>
<td>The URL of the app in Google Play. To determine the URL, click Go to Google Play to open Google Play in a new browser tab and navigate to the app page. Then copy the URL from the tab's address bar and paste it into the Link field.</td>
</tr>
</tbody>
</table>

## Settings for app packages

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Upload a file</strong></td>
<td>Click <strong>Upload a file</strong> to upload the app to the Sophos Mobile server. Navigate to the APK file and click <strong>Open</strong>.</td>
</tr>
</tbody>
</table>

**Related tasks**

Add app (page 244)
## 17.5 App settings (iOS)

### General settings

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the app.</td>
</tr>
<tr>
<td>Version</td>
<td>For app packages, the version that is displayed in the Enterprise App Store. For app links, Sophos Mobile uses the version from the App Store.</td>
</tr>
<tr>
<td>App identifier</td>
<td>The internal identifier of the app. Leave this field empty if you do not know the exact identifier. In most cases, Sophos Mobile can read the value from the app itself and then fills in this field automatically.</td>
</tr>
<tr>
<td>App category</td>
<td>A category name, for example <em>Productivity</em>. When you make the app available in the Enterprise App Store, the app will be listed in a section with that name.</td>
</tr>
<tr>
<td>Available to device groups</td>
<td>You can make the app available in the Enterprise App Store so that its installation can be initiated by the user. Click <strong>Show</strong> and select one or more device groups for which the app will be listed in the Enterprise App Store.</td>
</tr>
<tr>
<td>Sophos Mobile managed installation</td>
<td>The app is installed as a managed app. See [Managed apps for iOS](page 253). This setting only affects apps that are installed by the user from the Enterprise App Store. Apps that you install from Sophos Mobile Admin are always managed.</td>
</tr>
<tr>
<td>Description</td>
<td>The app description displayed in the Enterprise App Store. You may use the placeholder <code>%_appstoretext_%</code> anywhere in your description text. In the Enterprise App Store, this is replaced by the actual app description from the App Store.</td>
</tr>
<tr>
<td>Settings and VPN</td>
<td>Click <strong>Show</strong> to configure a VPN connection that is used when the app is started, or to configure settings for the app that will be deployed on the device during the app installation.</td>
</tr>
</tbody>
</table>
### Settings for app links

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Search in iTunes  | Click **Search in iTunes** to search for the app in the iTunes database. When you select an app in the search results list, the following fields are filled out automatically:  
  - **App identifier**  
  - **App category**  
  - **Link** |
| Link              | The URL of the app in the App Store. To determine the URL, click **Obtain link** to open iTunes Link Maker in a new browser tab. Navigate to the app in Link Maker, and then copy the URL displayed under **Direct Link** into the **Link** field in Sophos Mobile Admin. |

### Settings for app packages

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upload a file</td>
<td>Click <strong>Upload a file</strong> to upload the app to the Sophos Mobile server. Navigate to the IPA file and click <strong>Open</strong>.</td>
</tr>
</tbody>
</table>

### Related tasks

Add app [page 244]

### 17.6 App settings (Windows Mobile)

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the app.</td>
</tr>
<tr>
<td>Version</td>
<td>The app version. Sophos Mobile uses the version from Microsoft Store.</td>
</tr>
<tr>
<td>App category</td>
<td>A category name, for example <em>Productivity</em>. When you make the app available in the Enterprise App Store, the app will be listed in a section with that name.</td>
</tr>
</tbody>
</table>
### Setting/Field

**Description**

The app description displayed in the Enterprise App Store. You may use the placeholder `%_appstoretext_%` anywhere in your description text. In the Enterprise App Store, this is replaced by the actual app description from Microsoft Store.

**Available to device groups**

You can make the app available in the Enterprise App Store so that it’s installation can be initiated by the user. Click **Show** and select one or more device groups for which the app will be listed in the Enterprise App Store.

**Link**

The URL of the app in Microsoft Store. To determine the URL, click **Go to Microsoft Store** to open Microsoft Store for Windows Phone apps in a new browser tab and navigate to the app page. Then copy the URL from the tab’s address bar and paste it into the **Link** field.

### Related tasks

- Add app (page 244)

### 17.7 App settings (Windows)

#### General settings

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>A name for the app.</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>The app version.</td>
</tr>
<tr>
<td><strong>App category</strong></td>
<td>A category name, for example <strong>Productivity</strong>.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>A description of the app.</td>
</tr>
</tbody>
</table>
## Settings for MSI links

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>If you enter a wrong GUID value, the app can't be uninstalled.</td>
</tr>
<tr>
<td>Link</td>
<td>The URL of the MSI file.</td>
</tr>
<tr>
<td>SHA-256 file hash</td>
<td>The SHA-256 hash value of the MSI file.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>If you enter a wrong hash value, the app can't be installed.</td>
</tr>
<tr>
<td>Installation options</td>
<td>The command-line options for the \texttt{msiexec.exe} installer executable.</td>
</tr>
<tr>
<td></td>
<td>The default option /quiet installs the app without user interaction.</td>
</tr>
</tbody>
</table>

For more information on these settings, see Determine settings for Windows MSI links \(\text{page 253}\).

## Settings for Microsoft Store links

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Store ID</td>
<td>The Store ID of the app in Microsoft Store. The value is entered automatically when you click \textbf{Get data}.</td>
</tr>
<tr>
<td>SKU ID</td>
<td>The app's SKU ID (stock-keeping unit ID) in the Microsoft Store catalog.</td>
</tr>
<tr>
<td></td>
<td>Apps might have different SKU IDs for full and trial versions, or for different market regions.</td>
</tr>
<tr>
<td></td>
<td>If you don't know the SKU ID for an app, use the default value 0010.</td>
</tr>
<tr>
<td>Package Family Name</td>
<td>The Package Family Name (PFN) of the app.</td>
</tr>
<tr>
<td></td>
<td>The value is entered automatically when you click \textbf{Get data}.</td>
</tr>
</tbody>
</table>
### 17.8 Determine settings for Windows MSI links

This section provides guidance on how to determine the app settings for Windows MSI links.

- **ProductCode GUID** — If you already have the Microsoft Windows SDK installed, use the included Orca program to get the ProductCode value of an MSI file. For an example, see the description on the web page Use Orca to find MSI file GUID product code.

  Alternatively, use a PowerShell script. Such scripts can be found on the internet, for example on the web page How to get MSI file information with PowerShell.

  **Note**
  
  The value you enter in the **ProductCode GUID** field must not include surrounding brackets.

- **SHA-256 file hash** — Use the `Get-FileHash` PowerShell command to get the SHA-256 hash value of an MSI file:

  ```powershell
  PS> Get-FileHash <path-to-MSI-file>
  
  For more information on the `Get-FileHash` command, see the Microsoft web page Get-FileHash.

- **Installation options** — For information on the available command-line options for installing MSI files, see the Microsoft web page Standard Installer Command-Line Options.

### 17.9 Managed apps for iOS

For iOS apps that you add to Sophos Mobile, you can choose to have the app installed as *managed* or *unmanaged* on the users' devices.
Managed apps have the following characteristics:

- When users select a managed app in the Enterprise App Store, an installation task is created and processed in Sophos Mobile. In contrast, when users select an unmanaged app, they are redirected to the Apple App Store to install the app from there.
- You can uninstall managed apps in Sophos Mobile Admin. This is not possible for unmanaged apps.
- On supervised iOS devices, managed apps are installed and uninstalled silently, that is without user interaction.
- Certain settings in iOS device profiles are only available for managed apps.
- When an iOS device is unenrolled from Sophos Mobile, all managed apps are automatically removed from the device. Unmanaged apps will remain on the device.

The following rules determine if an app is installed managed or unmanaged:

- Apps that you install from Sophos Mobile Admin are always managed.
- Apps that the user installs from the App Store are always unmanaged.
- Apps that the user installs from the Enterprise App Store are managed if you have activated the SMC managed installation setting in the app properties, as described in Add app (page 244).

To check the app status on a device, open the Show device page for that device and go to the Installed apps tab. See The Show device page (page 57).

**Tip**

If a user has installed an unmanaged app you can convert it into a managed app. To do this, configure the app in Sophos Mobile as managed, and then create an installation task for it. Because the app is already installed, it is not installed again, but its status changes from unmanaged to managed.

17.10 Manage Apple VPP apps

With the Apple Volume Purchase Program (VPP), you can buy iOS apps in volume for distribution within your company.

After an order placed with Apple VPP has been completed, you can download an sToken (service token) that contains the licenses for the apps purchased.


For detailed information on how to assign VPP apps to users or devices, see Automatically assign VPP apps (page 257) and Manually assign VPP apps (page 258).

Assigning VPP apps to users

In Sophos Mobile, you can provide the licenses included in the sToken to users by inviting them to become authorized Apple VPP users. After users have accepted their invitation, they become authorized VPP users and you can assign VPP apps to them. Users can install assigned VPP apps onto their devices using iTunes.

The process for inviting users to become authorized VPP users differs depending on whether you use internal or external user management in Sophos Mobile. The instructions in the subsequent sections cover both.
Assigning VPP apps to devices

You can also assign VPP apps to devices. You do not need to invite devices to VPP. You install an assigned VPP app on a device through Sophos Mobile.

Note
- When a VPP app is uninstalled from a device, Sophos Mobile revokes the VPP app assignment.
- When a device is unenrolled from Sophos Mobile, Sophos Mobile revokes all VPP app assignments.

17.10.1 Set up a VPP sToken

To provide licenses for apps purchased through the Apple Volume Purchase Program (VPP) in Sophos Mobile, you need to set up an sToken (service token).

1. On the menu sidebar, under SETTINGS, click Setup > System setup.
2. On the System setup page, click the Apple VPP tab.
3. Click the Apple iTunes VPP Portal link. This opens the Apple VPP web portal in a new browser window.
4. On that page, select Business.
5. In the Business Store Sign In dialog, enter your Apple ID and your password.
6. Go to the Account Summary page and click Download Token. The sToken is generated and saved to your local computer in a text file with extension .vpptoken, using the download settings of your web browser.
7. Optional: Move the sToken file to a location that you can access from Sophos Mobile Admin.
8. In Sophos Mobile Admin, go back to the Apple VPP tab, click Upload a file, select the sToken file and then click Open. Sophos Mobile reads in the file and populates the Organization and Expiry date fields from the sToken details.
9. In the Automatically assign VPP apps on installation list, you can configure the automatic assignment of VPP apps. See Automatically assign VPP apps (page 257).
10. Optional: Fill in the remaining fields of the Apple VPP tab. In the Country field, enter your two-letter country code, for example US for the United States.
11. Click Save.

17.10.2 Invite users to Apple VPP

You need to set up an sToken before you can invite users to the Apple Volume Purchase Program (VPP). See Set up a VPP sToken (page 255).

1. On the menu sidebar, under MANAGE, click Users.
2. On the Show users page, you can invite all users or individual users to Apple VPP:
   - To invite all users:
a) Click Invite users to Apple VPP at the top of the Show users page.
b) Click Yes in the confirmation dialog box.

• To invite a single user:
  a) Click the required user name.
  b) On the Show user page, click Invite user to VPP.
  c) Click Yes in the confirmation dialog box.

• To invite a single user, when using external user management and the user has no devices enrolled yet:
  a) Click Search and invite a user to Apple VPP at the top of the Show users page.
  b) In the Search user dialog, search for the user either by name or by email address.
  c) In the search result list, select the user that you want to invite to Apple VPP.
  d) Click Apply.

Sophos Mobile sends an invitation email to all relevant users.

Users must follow the link in their invitation email to connect their Apple iTunes account with Apple VPP. Afterward, they can install and use the apps that are licensed by your company.

Note
When you are using external user management and invite all users to Apple VPP, users that do not have an email address assigned will be registered for Apple VPP, but do not receive the link to connect their Apple iTunes account with Apple VPP.

For information on how to complete the VPP registration process in this case, see Invite users without email address to Apple VPP (page 256).

17.10.3 Invite users without email address to Apple VPP

Prerequisite: This procedure requires a super administrator account, so it does not apply to Sophos Mobile as a Service.

When you invite users from an external user directory to Apple VPP as described in Invite users to Apple VPP (page 255), users that do not have an email address assigned will be registered for Apple VPP, but will not receive the link to connect their Apple iTunes account with Apple VPP.

If this happens, perform the following steps to complete the Apple VPP registration process.

1. As Sophos Mobile super administrator, download the server log files.
   See the Sophos Mobile super administrator guide.
2. Identify the affected user accounts from the log files.
3. On the menu sidebar of Sophos Mobile Admin, under MANAGE, click Users.
4. On the Show users page, click one of the affected user names.
5. On the Show user page, click Show invitation link.
   For external users without email address, this function does not send an invitation email, but instead shows the invitation link in a message box.
6. Copy the link from the message box and communicate it to the user.
7. Repeat this for all affected users.

The users need to follow the link to connect their Apple iTunes account with Apple VPP.
17.10.4 Manage Apple VPP users

When you have set up an Apple VPP sToken as described in Set up a VPP sToken (page 255), the Show user page of each user includes an Apple Volume Purchase Program (VPP) section.

In this section, you can perform the following tasks to view or edit the Apple VPP status of the user:

- View the Apple VPP user status. This can be:
  - Not registered: The user has not been invited to Apple VPP.
  - Registered: The user has been invited to Apple VPP, but has not connected their Apple iTunes account with Apple VPP.
  - Associated: The user has connected their Apple iTunes account with Apple VPP and can install VPP apps.
- View the Apple VPP apps that the user has installed.
- Invite the user to Apple VPP by clicking Invite user to VPP.
  
  In most cases, an email with an invitation link is sent to the user. If the user account does not contain an email address, an invitation link will be displayed in a message box.
- Send another invitation email if the user did not receive or lost the initial email, by clicking Resend invitation email.
- Deregister the user from Apple VPP by clicking Delete VPP registration.

17.10.5 Automatically assign VPP apps

By default, apps that you purchased through the Apple Volume Purchase Program (VPP) are automatically assigned to the device on which the app is installed. If the device does not support the assignment of VPP apps, the app is assigned to the user that is assigned to the device.

**Note**

To support the assignment of VPP apps, the device must have the status managed.

You can invert the order of precedence and favor user assignment over device assignment, or you can disable automatic assignment and instead assign VPP apps manually, as described in Manually assign VPP apps (page 258).

The automatic assignment of VPP apps is configured per customer.

1. On the menu sidebar, under SETTINGS, click Setup > System setup.
2. On the System setup page, click the Apple VPP tab.
3. In the list Automatically assign VPP apps on installation, select the desired option:

   - Preferably to device: If the device supports it, the VPP app is assigned to the device. Otherwise, the VPP is assigned to the user that is assigned to the device. If there is no user assigned to the device, app assignment will fail.

   - Preferably to user: If a user is assigned to the device, the VPP app is assigned to that user. Otherwise, the app is assigned to the device. If the device does not support it, app assignment will fail.

   - Disabled: VPP apps are not assigned automatically. If you select this option, VPP apps must be assigned manually.
17.10.6 Manually assign VPP apps

This section describes the manual assignment of individual VPP apps. By default, apps that you purchased through the Apple Volume Purchase Program (VPP) are automatically assigned to the device on which the app is installed. See Automatically assign VPP apps (page 257).

You can assign apps that you purchased through the Apple Volume Purchase Program (VPP) to users or to devices. After you assign a VPP app to users that are associated with Apple VPP, they can install it on all iOS devices that are associated with their Apple ID. After you assign a VPP app to devices, you can push it to the devices through Sophos Mobile.

To assign a VPP app to users or devices:
1. On the menu sidebar, under CONFIGURE, click Apps > iOS.
   This opens the Apps page that displays a list of all apps that you have added to Sophos Mobile.
2. To add apps you purchased through Apple VPP to the app list, click Import VPP apps.
   This retrieves the app information from the Apple VPP server and creates app entries in Sophos Mobile, if required.
3. Click the blue triangle next to the VPP app you want to assign to users or devices and then click Edit.
   Tip
   VPP apps are marked by a check mark icon in the VPP column.
4. On the Edit iOS link page, click Show next to the VPP licenses option.
   This opens the VPP licenses dialog.
5. To assign the app to one or more users, click VPP users and then select the required users.
   The list contains all users that are registered for or associated with Apple VPP.
6. To assign the app to one or more devices, click Devices and then select the required devices.
   The list contains all iOS devices with status Managed.
7. Click Apply to confirm the changes and to close the VPP licenses dialog.
8. By default, VPP apps are not assigned to any device groups. To assign an app to one or more device groups, click Show next to Available to device groups and then select one or more device groups for which the app is listed in the Enterprise App Store.
9. By default, VPP apps are installed as managed on the users’ devices. To install an app as unmanaged, clear the Sophos Mobile managed installation check box.
   For information on managed apps, see Managed apps for iOS (page 253).
10. Click Save to save the changes and to synchronize the app assignment with the Apple VPP server.
   Tip
   To discard assignment changes that you made in the VPP licenses dialog, click Apply to close the dialog box and then click Back to leave the Edit iOS link page without saving the changes to the database.

To install the assigned app on a device:
After the app is assigned to users, it is listed in the Purchased view of the iTunes app on their devices. The users can install it from there.

After the app is assigned to devices, you can install it through Sophos Mobile. See Install app (page 245).

To deassign an app:

- Open the VPP licenses dialog box as described before and then clear the selection of the required users or devices.

**Note**
Because the status of VPP apps is managed by the Apple VPP server, it may take some time until changes that you make in Sophos Mobile are visible on the devices.

### 17.10.7 Synchronize VPP license information

For performance reasons, Sophos Mobile keeps a local copy of VPP license information. You can trigger Sophos Mobile to synchronize its VPP data with the Apple VPP server.

**Note**
You only need to synchronize the VPP data if the displayed license information for an app is incorrect.

1. On the menu sidebar, under SETTINGS, click Setup > System setup and then click the Apple VPP tab.
2. Click Clear VPP cache.

Sophos Mobile discards its local VPP information for the customer and synchronizes the data with the Apple VPP server.

**Note**
For information on how to display the license information for a VPP app, see Manually assign VPP apps (page 258).

### 17.11 Configure per app VPN and settings for iOS apps

For iOS apps, you can configure a VPN connection that is used when the app is started. You can also configure settings for the app that will be deployed on the device during the app installation.

**Prerequisites:**

- To be able to select a per app VPN, you need to define a Per app VPN configuration in an iOS configuration profile. See Per app VPN configuration (iOS device profile) (page 156).
- To define settings, you need to know the required parameter and the parameter type.

1. On the menu sidebar, under CONFIGURE, click Apps > iOS.
2. On the Apps page, click the blue triangle next to the required app and then click Edit.
3. On the Edit iOS link or Edit iOS package page, click Show next to the Settings and VPN field.

4. On the Edit settings and VPN page, select the required configuration from the Per app VPN list to define the VPN the app is supposed to connect to.

5. To add custom settings, click Create parameter.

6. In the Configuration parameter dialog, configure the following:
   a) In the Parameter field, enter the required parameter, for example, SMC_URL.
   b) In the Value field, enter the parameter value, for example, smc.sophos.com.
   c) In the Type list, select the parameter type: String, Bool, Integer or Real.
   d) Click Apply.

   The set of custom settings is displayed on the Edit Settings and VPN page.

7. On the Edit settings and VPN page, click Apply.

8. Click Save.

The selected per app VPN will be used when the app connects to VPN. The settings will be provided to the devices during the app installation.
18 App groups

In Sophos Mobile you create app groups to define list of apps for profiles, policies and compliance policies.

App groups are used in the following settings:

- In the **App Protection** configuration of Android device profiles.
- In the **App Control** configuration of Android device profiles.
- In the **Restrictions** configuration of Android device profiles, iOS device profiles and Knox container profiles.
- In the **App restrictions** configuration of Windows Mobile policies.
- In compliance policies to specify lists of allowed, forbidden and mandatory apps.

18.1 Create app group

1. On the menu sidebar, under **SETTINGS**, click **App groups** and then click the platform for which you want to create the app group.
2. On the **App group** page, click **Create app group**.
3. On the **Edit app group** page, enter a **Name** for the new app group and then click **Add app**.
4. In the **Edit app** dialog box you can either select an app from a list or enter custom app data.

- To select an app from a list, click **App list** and then select an app from the list of all apps that are currently installed on the managed devices for the platform you selected.
- To enter custom app data for an Android app, click **Custom** and then configure the following information:
  - **App name**: An arbitrary name that is used to identify the app.
  - **Identifier**: The package name of the app. The package name can be retrieved from the app's URL in Google Play. For example for the Sophos Mobile Control Android app, the Google Play URL is play.google.com/store/apps/details?id=com.sophos.mobilecontrol.client.android and the package name is com.sophos.mobilecontrol.client.android.
  - **Link**: For your reference, the URL of the app in Google Play.
- To enter custom app data for an iOS app, click **Custom** and then configure the following information:
  - **App name**: An arbitrary name that is used to identify the app.
  - **Identifier**: The bundle ID of the app.
  - **Link**: For your reference, the URL of the app in the App Store.
- To enter custom app data for a macOS app, click **Custom** and then configure the following information:
  - **App name**: An arbitrary name that is used to identify the app.
  - **Identifier**: The bundle ID of the app.
  - **Link**: For your reference, the URL of the app in the App Store.
- To enter custom app data for a Windows Mobile app, click **Custom** and then configure the following information:
  - **App name**: An arbitrary name that is used to identify the app.
Sophos Mobile on Premise

- **Link:** The URL of the app in Microsoft Store. For example, the URL of the Sophos Mobile Control Windows Mobile app is https://www.microsoft.com/en-us/store/p/mobile-control-2017/9nblggh51qsj.

- **GUID:** If you know the GUID of the app, you can enter it instead of the link. Otherwise, leave this field empty.

  - To enter custom app data for a Windows app, click **Custom** and then configure the following information:
    - **App name:** An arbitrary name that is used to identify the app.
    - **Identifier:** The ID of the app as reported by Windows. For MSI apps, this is the ProductCode GUID of the MSI file. For Microsoft Store apps, this is the Package Family Name (PFN) of the app.
    - **Link:** For your reference, the URL of the app in Microsoft Store. For example, the URL of the Wikipedia Windows app is https://www.microsoft.com/en-us/store/p/wikipedia/9wzdncrfhwm4.

5. After you have selected an app from the list or entered custom app data, click **Add** to add it to the app group.

6. Optional: Add more apps to the app group.

7. When you are ready, click **Save** to save the app group.

### 18.2 Import app group

You can create an app group by importing a UTF-8 encoded comma-separated values (CSV) file with up to 10,000 apps.

**Note**

Use a text editor for editing the CSV file. If you use Microsoft Excel, values entered may not be resolved correctly. Make sure that you save the file with extension `.csv`.

**Tip**

A sample file with the correct column names and column order is available for download from the **Import apps** page.

To import apps from a CSV file and add them to an app group:

1. On the menu sidebar, under **SETTINGS**, click **App groups** and then click the platform for which you want to create the app group.

2. On the **App group** page, click **Create app group**.

3. On the **Edit app group** page, enter a **Name** for the new app group and then click **Import apps**.

4. On the **Import apps** page, click **Upload a file** and then navigate to the CSV file that you have 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. Click **Finish** to add the apps to the app group.

7. On the **Edit app group** page, click **Save**.
19 Corporate documents

Note
This feature requires a license of type Mobile Advanced.

In Sophos Mobile, you can upload files for distribution to the devices of your users.

- Documents managed in Sophos Mobile are automatically added to the Corporate Documents storage provider in Sophos Secure Workspace.
- You can assign a category to each document from the Corporate Documents storage provider.
- Documents from the Corporate Documents storage provider are read only.
- If Sophos Secure Workspace is not managed by Sophos Mobile, the Corporate Documents storage provider is not available.

To distribute corporate documents:
1. Install the Sophos Secure Workspace app onto the devices. See Apps (page 244).
2. Assign a Sophos container policy with a Corporate Documents configuration.
3. Upload documents to Sophos Mobile.

19.1 Add corporate documents

Note
This feature requires a license of type Mobile Advanced.

To distribute documents to devices:
1. On the menu sidebar, under CONFIGURE, click Documents. The Documents page is displayed.
2. Click Add document. The Edit document page is displayed.
3. In the Category field, enter the category under which the document is displayed in the Corporate Documents storage provider on the device.
   If you leave this field blank, the file will be shown in the root folder of the Corporate Documents storage provider.
4. Define settings for the document:
   - Select Copy to clipboard to allow users to copy the document to the clipboard.
   - Select Share document to allow users to share the document.
   - Select Use document offline to allow users to add the document to the Favorites list.
     When an unencrypted document from Corporate Documents is added to the Favorites list, the local copy is stored encrypted. When sharing the document is allowed, the file is automatically decrypted before it is forwarded to other apps. If you clear the Use document offline check box, local copies are automatically removed during the next synchronization.
5. Click Show next to Assigned groups and select the group that should have access to the document.
6. Add a description for the document.
7. Click **Upload a file** and navigate to the document. Select it and click **Open**.
8. Repeat this step for each document you want to distribute.

The document is added to the documents list. It is distributed to the users, who can view it in the Sophos Secure Workspace app.
20 Android enterprise

Android includes functionality that simplifies the integration of devices into your company environment and helps your users to separate personal and corporate data on their device. This is referred to as Android enterprise (formerly Android for Work).

Note
Sophos Mobile supports Android enterprise for devices with Android 6 or higher.

Sophos Mobile supports the Android enterprise enrollment modes Device owner and Profile owner.

Device owner

When a device is enrolled in device owner mode, device ownership is assigned to Sophos Mobile. Sophos Mobile can monitor and manage settings, apps and data on the whole device.

Device owner mode differs from a standard enrollment as follows:

- Users have a simplified enrollment experience.
- Users don’t need to set up a personal Google account on the device.
- Users can only install apps from managed Google Play, and you can configure the store layout.
- Only a minimum set of apps is enabled by default: Google Play Store, Contacts, Messages, Phone.
- You can install, uninstall or update apps without user interaction.
- You can configure app permissions so that users are not asked to grant permissions at runtime.
- For apps that support it, you can configure custom app settings.
- You can reset the screen lock password. With standard enrollment, this is not possible for Android 7.0 or later.
- You can configure a kiosk mode that restricts app usage to a selection of apps, not just a single app.
- You can only enroll devices that have not been set up yet, or that have been reset to their factory settings.
- There is no dedicated unenroll action. To unenroll a device, wipe it.

Profile owner

When a device is enrolled in profile owner mode, a work profile is created on the device. Sophos Mobile can only monitor and manage settings, apps and data within the work profile.

The profile owner mode is suitable for BYOD [bring your own device] scenarios.

Related information
Android enterprise help (external link)

20.1 Set up Android enterprise - Overview

To set up Android enterprise for your organization, you can choose between two different scenarios:
**Managed Google Play Account scenario**

This is the easiest method to set up Android enterprise for your organization.

- Sophos Mobile guides you through the process of setting up an Android enterprise account for your organization.
- If required, you can create multiple Android enterprise accounts for your organization.
- Sophos Mobile manages the whole user account lifecycle.

See Set up Android enterprise (Managed Google Play Account scenario) (page 266).

**Managed Google Domain scenario**

Use this method if you already have a Managed Google Domain or if you want to manage the accounts of your Android enterprise users outside of Sophos Mobile.

- You register a Managed Google Domain with Google and prove domain ownership.
- You bind Sophos Mobile as a third-party EMM (Enterprise Mobility Management) to your Managed Google Domain.
- Sophos Mobile creates user accounts as needed. Other than that, Sophos Mobile does not manage the account lifecycle.

See Set up Android enterprise (Managed Google Domain scenario) (page 267).

### 20.2 Set up Android enterprise (Managed Google Play Account scenario)

For the 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, click **Setup > System setup**, and then click the **Android enterprise** tab.
2. Click **Configure**.
3. Select “Managed Google Play Account” scenario and then click **Next**.
4. Select **Register account**.
   - This redirects you to a Google website where you register your organization with Android enterprise.
5. Log 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.
When specifying your organization name, include the term SMC and your Sophos Mobile customer name, like My organisation name (SMC/My customer name). The account properties don’t mention any information about the account being connected to Sophos Mobile.

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

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

This completes the procedure to set up Android enterprise for your organization.

### 20.3 Set up Android enterprise (Managed Google Domain scenario)

For the *Managed Google Domain* scenario, to set up Android enterprise for your organization, you:

1. Register a Managed Google Domain with Google.
2. Create an enterprise service account and configure the APIs that are required to communicate with the Google services.
3. Bind Sophos Mobile as a third-party EMM (*Enterprise Mobility Management*) to your Managed Google Domain.

#### 20.3.1 Register domain with Google

In the first stage of the procedure to set up Android enterprise for your organization, you register a domain with Google (*Managed Google Domain*), create a domain administrator (*Managed Google Account*) and verify your domain ownership.

**Note**

If you already have a Managed Google Domain, for example because you have signed up for G Suite (formerly Google Apps), you can skip this section.

1. Click the following link `https://www.google.com/a/signup/?enterprise_product=ANDROID_WORK` to sign up for a Managed Google Domain.
2. Fill the web form with the required information.
   - Under **About your business**, enter the domain that will be used as the Managed Google Domain in the **Business domain address** field. For example, you could use the domain of your Sophos Mobile server.

**Note**

If you want to configure Android enterprise for more than one customer in Sophos Mobile, you need a separate domain for each customer.

- Under **Your Google admin account**, enter the credentials for a new domain administrator.
3. Click the button to create the domain administrator account.
   This opens the Google Admin console.
4. In the Google Admin console, start the procedure to verify your domain ownership.
   Follow the instructions provided by Google to verify your domain.

After your domain ownership is verified, you receive a token to connect your Managed Google Domain with your third-party EMM provider, that is, with Sophos Mobile.

Next, you must create a Google service account and configure the relevant Google APIs. See Configure Google service account (page 268).

### 20.3.2 Configure Google service account

In the second stage of the procedure to set up Android enterprise for your organization, you create and configure a Google service account.

**Prerequisite:** You have a domain administrator account for your Managed Google Domain.

A Google service account is a special type of Google account for an application. This account is used by Sophos Mobile to communicate with the Google APIs.

Create a project:
1. Click the following link https://console.developers.google.com/apis/library to open the Google API console. Log in with the credentials of your domain administrator account.
2. In the header bar of the Google API console, click **Project > Create project**.
   If you already have a project, the header bar shows the project name instead of the word **Project**.
3. In the **New project** dialog, enter a project name, for example **Android enterprise**, and then click **Create**.

Enable the required APIs:
4. On the menu sidebar, click **Library**, and then enter the string **admin sdk** in the search field.
5. In the search result list, click **Admin SDK**.
6. At the top of the **Admin SDK** page, click **Enable**.
7. Repeat the previous three steps for the **Google Play EMM API**:
   a) On the menu sidebar, click **Library**, and then enter the string **emm** in the search field.
   b) In the search result list, click **Google Play EMM API**.
   c) At the top of the **Google Play EMM API** page, click **Enable**.

Create a service account:
8. On the **Google Play EMM API** page, click **Create credentials**.
9. In step one of the **Add credentials to your project** page, click the service account link.
10. On the **Service Accounts** page, click **Create Service Account**.
11. In the **Create service account** dialog box, enter the following settings:
    a) In **Name**, enter a name to identify the service account, for example **Android enterprise**.
    b) Select **Furnish a new private key** and then select **JSON**.
    c) Select **Enable G Suite Domain-wide Delegation**.
    d) In **Product name for the consent screen**, enter for example **Android enterprise**.
When you click **Create**, the private key for your service account is generated and saved to your computer in a JSON file.

**Note**
Store the JSON file in a secure location. You need it to bind Sophos Mobile to your Managed Google Domain.

Configure API access:
12. Click the following link [https://admin.google.com](https://admin.google.com) to open the Google Admin console and log in with the credentials of your domain administrator account.
13. Click **Security** and then click **Advanced settings**.

**Tip**
You may need to click **Show more** to display **Advanced settings**.

14. Click **Manage API client access**.
15. Open the JSON file in a text editor and copy the `client_id` value into the **Client Name** field. For example, if your JSON file contains a line

```json
"client_id": "123456789",
```

then enter `123456789` in the **Client Name** field.
16. In the **One or more API Scopes** field, enter the following two URLs, separated by a comma:

```bash
https://www.googleapis.com/auth/admin.directory.user,
https://www.googleapis.com/auth/androidenterprise
```
17. Click **Authorize**.

You can now bind Sophos Mobile to your Managed Google Domain. See [Bind Sophos Mobile to your domain](page 269).

### 20.3.3 Bind Sophos Mobile to your domain

In the third stage of the procedure to set up Android enterprise for your organization, you bind Sophos Mobile to your Managed Google Domain.

**Prerequisites:**
- You have a domain administrator account for your Managed Google Domain.
- You have verified your domain ownership.
- You have enabled the relevant Google APIs.
- You have created a Google service account.

1. On the menu sidebar, under **SETTINGS**, click **Setup > System setup**, and then click the **Android enterprise** tab.
2. Click **Configure**.
3. Select “**Managed Google Domain**” scenario and then click **Next**.
4. In the dialog box that opens, configure the following settings:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business domain</td>
<td>Your Managed Google Domain that has been verified to Google.</td>
</tr>
<tr>
<td>Domain administrator</td>
<td>The name of your domain administrator account. This is the administrator that you created when you registered your domain with Google.</td>
</tr>
<tr>
<td>EMM token</td>
<td>The token that you received from Google after you verified your domain ownership. You can view the token when you log in to the Google admin console [<a href="https://admin.google.com">https://admin.google.com</a>] with your domain administrator credentials and navigate to Security &gt; Manage EMM provider for Android.</td>
</tr>
</tbody>
</table>

5. Click **Upload a file** and then navigate to the JSON file that you downloaded from Google when creating the service account. The JSON file that you select must have an extension `.json`.

6. Click **Bind**.

Sophos Mobile contacts the Google web service to bind itself as an EMM provider to your Managed Google Domain.

In the final stage of the procedure to set up Android enterprise for your organization, you must configure the Google EMM settings. See Configure EMM settings (page 270).

### 20.3.4 Configure EMM settings

In the final stage of the procedure to set up Android enterprise for your organization, you configure the Google EMM settings.

**Prerequisite:** You have bound Sophos Mobile to your Managed Google Domain.

1. Click the following link [https://admin.google.com](https://admin.google.com) to open the Google Admin console and log in with the credentials of your domain administrator account.

2. Click **Security** and then click **Manage EMM provider for Android**.

   **Tip**
   
   You may need to click **Show more** to display **Manage EMM provider for Android**.

3. Under **General Settings**, select **Enforce EMM policies on Android devices**.

   This completes the procedure to set up Android enterprise for your organization.

### 20.4 Configure Android enterprise device enrollment

**Prerequisites**

- You have configured Android enterprise for the customer.
Complete the following steps to configure device enrollment for Android enterprise.

1. Create a policy for each Android enterprise enrollment mode you want to support.
   - For device owner mode, create a policy of type **Android enterprise device policy**.
   - For profile owner mode, create a policy of type **Android enterprise work profile policy**.
   
   For a general description of how to create policies, see Create profile or policy (page 77).

2. Create a task bundle for each Android enterprise enrollment mode you want to support.
   
   The task bundle must contain at least an **Enroll** task and an **Install profile or assign policy** task for the policy you have created before.
   
   For a general description of how to create task bundles, see Create task bundle (page 233).

3. In the Self Service Portal group settings, configure the task bundle you have created as the initial package.
   
   You can configure different packages for corporate and personal devices. For example, use device owner enrollment for corporate devices and profile owner enrollment for personal devices.
   
   For a general description of how to configure Self Service Portal group settings, see Configure Self Service Portal settings (page 22).

After you’ve configured device enrollment, Self Service Portal users can enroll their Android devices with Sophos Mobile. Based on your configuration, the enrollment mode (device owner or profile owner mode) is defined by the device type (corporate or personal device).

**Note**

If you configure Android enterprise enrollment for corporate and/or personal devices as described in this section, standard enrollment of Android devices is not available for that device type in the Self Service Portal.

### 20.5 Manage users for Android enterprise (Managed Google Domain scenario)

**Note**

This topic describes the management of Google user accounts if you have set up Android enterprise using the **Managed Google Domain** scenario.

For the **Managed Google Play Account** scenario, Sophos Mobile transparently manages the Google accounts of your users.

A user must have a **Managed Google Account** to enroll an Android enterprise device. This account is connected to the domain that you registered with Google.

Account names are formed like an email addresses, for example user@your_managed_Google_domain.

When a user enrolls a device in the Self Service Portal, Sophos Mobile checks if a Managed Google Account for the user already exists on the Google server. For this, the left part of the user’s email address in Sophos Mobile is combined with your Managed Google Domain. If an account with that name does not exist, Sophos Mobile creates it.
Example: If the user's email address in Sophos Mobile is user@your_company.com and your Managed Google Domain is your_managed_Google_domain, Sophos Mobile checks the Google server for an account user@your_managed_Google_domain.

Other than creating a Managed Google Account for the user during enrollment, Sophos Mobile does not manage the account lifecycle. If you delete the user account in Sophos Mobile, the user’s Managed Google Account remains.

You can manage the accounts for your Managed Google Domain from the Google Admin console. If required, you can create accounts from your LDAP directory, using Google Apps Directory Sync (GADS).

Related information
Google Admin console (external link)
About Google Apps Directory Sync (external link)

20.6 Create work profile

A work profile is created when users enroll their devices in the Self Service Portal in Android enterprise profile owner mode.

You can delete the work profile in Sophos Mobile Admin, for example to delete corporate data from the device in case of lost or theft.

20.7 Lock work profile

You can lock or unlock the work profile in Sophos Mobile Admin. When the work profile is locked, all work apps are unavailable and no notifications are displayed for work apps.

Note
This section does not apply to devices that are enrolled with Sophos Mobile in Android enterprise device owner mode. See Android enterprise (page 265)

1. On the menu sidebar, under MANAGE, click Devices.
2. Click the blue triangle next to the device for which you want to lock or unlock the work profile and then click Show.
3. Click Actions > Set container access.
4. Select the access permissions.
   - Deny: The work profile is locked. Users can no longer access apps or data within the work profile.
   - Allow: The work profile is unlocked.
   - Auto mode: The work profile is locked if the device violates a compliance rule that contains a Lock container action. This is the default behavior if you have not set an access permission.
5. Click Yes.

The device is synchronized with the Sophos Mobile server. Once this is complete the setting is applied to the device.
To lock the whole device instead of just the work profile, use Actions > Lock.

Users can lock the work profile from the Quick Settings panel on their device, for example when they are on leave.

20.8 Remove work profile from device

You can remove the work profile in Sophos Mobile Admin to delete corporate data from the device in case of lost or theft.

When you remove the work profile from the device, all work apps, including the Sophos Mobile Control app, are also removed. In Sophos Mobile Admin, the device is displayed with status Unenrolled.

1. On the menu sidebar, under MANAGE, click Devices.
2. Click the blue triangle next to the device from which you want to remove the work profile and then click Show.
3. Click Actions > Wipe Android work profile.

A task to remove the work profile is created and transferred to the device. You can display the task status on the Task view page.

If the user has already removed the work profile manually, the task fails as the device cannot receive it anymore.

To re-create the work profile, the user must repeat the enrollment procedure in the Self Service Portal.

20.9 User-initiated work profile removal

Users can remove the work profile from their device, either accidentally or intentionally. Sophos Mobile is unable to detect this type of removal. It continues to display the device management status as Android enterprise (profile owner).

After the user has removed the work profile, the device cannot synchronize with the Sophos Mobile server.
**Tip**
You can use the **Devices not synchronized in last 7 days** report to identify potentially affected devices.

If the work profile was removed accidentally, it can be re-enrolled as follows:

1. You delete the device from Sophos Mobile.
2. The user repeats the device enrollment procedure in the Self Service Portal.

## 20.10 Work apps

Work apps are apps that can be installed onto a device that is enrolled with Sophos Mobile using Android enterprise device owner or profile owner mode.

**Note**
For profile owner mode, work apps are installed inside the work profile and are marked with a briefcase badge.

You must perform the following tasks in managed Google Play and in Sophos Mobile to make work apps available to your users:

1. In managed Google Play, you select the apps for your organization. To do this:
   - Approve the app.
   - Purchase app licenses.
   - Accept the app permissions.
   
   See **Approve work app** (page 274).

2. In Sophos Mobile, you configure the app. To do this:
   - Define the location of the app in the managed Google Play Store app on the users’ devices.
   - For apps that support it, configure custom app settings.
   - For paid apps, assign users a license for the app.

   See **Edit work app** (page 276).

### 20.10.1 Approve work app

2. Select the app you want to make available to your users.
3. Either click **Approve** (for free apps) or **Buy** (for paid apps).

**Note**
Paid work apps are currently only available in the United States and in Canada.

4. If the app requires permissions, accept these on behalf of your company.
When your users install that app, they are not asked to grant permissions.

5. For paid apps, enter the number of licenses and the payment method.

**Note**
If you receive an error when trying to buy an app, check in the Google Admin console that Google payment services are enabled for your domain or your account.

At this stage, the app is approved for your domain but users are not able to install it yet. You must complete the allocation process in Sophos Mobile. See [Edit work app](#) (page 276).

**Note**
If an update to your work app includes additional app permissions, you must accept these before your users can install the update. In the Google Play menu, click **Update** to view and approve pending updates.

**Related information**
Managed Google Play (external link)
Google Admin console (external link)
Managed Google Play help (external link)

### 20.10.2 Unapprove work app

1. Open managed Google Play (https://play.google.com/work) and log in with your Android enterprise administrator account.
2. Click **My managed apps** to view the work apps you have approved.
3. Select the app you want to remove from your managed Google Play Store.
4. Click **Unapprove**.
5. To synchronize the change with Sophos Mobile, log in to the Sophos Mobile Admin.
6. On the menu sidebar, under **CONFIGURE**, click **Apps > Android**.
7. On the **Apps** page, click **Android work apps**.
8. Click **Retrieve app list from Google**.

**Note**
You must also remove the app from your Android task bundles.

**Related concepts**
Task bundles (page 233)

**Related information**
Managed Google Play (external link)
Google Admin console (external link)
Managed Google Play help (external link)
20.10.3 Edit work app

After you have approved an app in managed Google Play, you must configure the app in Sophos Mobile to make it available to your users.

1. On the menu sidebar, under CONFIGURE, click Apps > Android.
2. On the Apps page, click Android work apps.

   This opens the Android work apps page that displays a list of all work apps that you have approved in managed Google Play.

3. Click Retrieve app list from Google to synchronize the changes you made in managed Google Play. After synchronization, users can install the apps through the managed Google Play Store app.

4. Click the blue triangle next to the required app and then click Edit.
5. On the Edit Android work app page, configure the settings as required. See Work app settings (page 276).
6. Click Save to save your changes.
7. On the Android work apps page, click Send configuration to Google to send the updated layout information and app configuration to Google.

   Note
   If you skip this last step, the app configuration is only stored locally in Sophos Mobile. It is not transferred to the Google server and is not available to your users.

After the data is synchronized to the Google server, the work app is available through the managed Google Play Store app. Free apps are available to all of your users, while paid apps are only available to users that have a license assigned.

Related reference
Work app settings (page 276)

20.10.4 Work app settings

<table>
<thead>
<tr>
<th>Setting/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>The external app name as displayed in managed Google Play.</td>
</tr>
<tr>
<td>Product ID</td>
<td>The internal app name.</td>
</tr>
<tr>
<td>Pricing</td>
<td>The pricing type:</td>
</tr>
<tr>
<td></td>
<td>• Free</td>
</tr>
<tr>
<td></td>
<td>• Free with in-app purchases</td>
</tr>
<tr>
<td></td>
<td>• Paid</td>
</tr>
<tr>
<td>Setting/Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Distribution type</strong></td>
<td>• <strong>Public (Google-hosted):</strong> The app is available to the general public in managed Google Play.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Private (Google-hosted):</strong> The app is developed by you and only available to users within your Managed Google Domain. The APK file was uploaded to managed Google Play.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Private (self-hosted):</strong> Like <strong>Private (Google-hosted),</strong> but the APK file is installed from your local server. Managed Google Play is only used to manage the distribution.</td>
</tr>
<tr>
<td><strong>Managed Google Play URL, Google Play URL</strong></td>
<td>The web address of the app in managed Google Play and Google Play. Click the link to open that page in a new browser window.</td>
</tr>
<tr>
<td><strong>Page</strong></td>
<td>The page on which the app will appear in the users' Google Play Store app. The values are pre-configured by Sophos Mobile and cannot be changed.</td>
</tr>
<tr>
<td><strong>App category</strong></td>
<td>The name of a category under which the app will appear in the users' Google Play Store app. When you start to type, a list of matching categories is displayed. If you enter a category that is not available, it is created.</td>
</tr>
<tr>
<td><strong>Licenses</strong></td>
<td>Click <strong>Show</strong> next to <strong>Licenses</strong> to view or edit the number of used and remaining licenses for the app, and the users that have a license assigned. This setting is only available for paid apps.</td>
</tr>
<tr>
<td><strong>App settings</strong></td>
<td>Click <strong>App settings</strong> to view or edit app-specific settings. For information on the available settings, see the documentation provided by the app developer. This setting is only available if the app offers managed configuration.</td>
</tr>
</tbody>
</table>

**Tip**
You can use the placeholders `%USERNAME%` and `%EMAILADDRESS%` which are replaced by the actual user name and email address.
20.10.5 Install work app

After you have approved a work app in managed Google Play and have assigned app licenses to your users, you can install the app to selected devices or device groups.

Note
Users can install approved apps through the managed Google Play Store app.

1. On the menu sidebar, under **CONFIGURE**, click Apps > Android.
2. On the Apps page, click Android work apps.
3. Click the blue triangle next to the required app and then click Install.
4. Select the devices on which you want to install the app. Do one of the following:
   - Select individual devices.
   - Click Select device groups and then select one or more device groups.

   When you are ready, click Next.
5. On the **Set execution date** page, specify the date when the app will be installed:
   - Select Now for an immediate execution.
   - Select Date and then enter a date and a time for a scheduled execution.
6. Click Finish.

The installation task is sent to a Google service. Google then manages the installation of the app onto the device. On the Task view page, the task is displayed with state successful after it has been sent to Google.

20.10.6 Uninstall work app

You can uninstall a work app from selected devices or device groups.

1. On the menu sidebar, under **CONFIGURE**, click Apps and then click Android.
2. On the Apps page, click Android work apps.
3. On the Android work apps page, click Uninstall.
4. Select the devices from which you want to uninstall an app. Do one of the following:
   - Select individual devices.
   - Click Select device groups and then select one or more device groups.

   When you are ready, click Next.
5. On the Select app page, select the required app.
6. On the **Set execution date** page, specify the date when the app will be uninstalled:
   - Select Now for an immediate execution.
   - Select Date and then enter a date and a time for a scheduled execution.
7. Click Finish.

A task to uninstall the app is sent to a Google service. Google then manages the removal of the app from the device. On the Task view page, the task is displayed with state successful after it has been sent to Google.
Tip
Alternatively, you can use the following procedure to uninstall an app from a single device: Open the device's Show device page, go to the Installed apps tab and then click the trash can icon next to the app name.

20.10.7 Licenses for work apps

By assigning licenses for paid work apps to users, you define which apps are available to a user. You only assign licenses for paid work apps to users. Free apps that you have approved in managed Google Play are automatically available to all of your users after you synchronize the app list from Google to Sophos Mobile.

You configure the license assignment on the Edit Android work app page. See Edit work app (page 276).

Tip
You do not need to assign a license for administrator-initiated app installations. When you install a work app as described in Install work app (page 278), a license from your pool of purchased licenses will automatically be assign to the relevant users.

20.10.8 Layout of managed Google Play

You can define the location of each work app in the managed Google Play Store app on the users’ devices.

The configurable layout elements are Pages and Categories.

- Pages are named, vertically scrollable views. Pages and their names are pre-defined by Sophos Mobile.
- Categories are named, horizontally scrollable subsections of a page that you define. In the Google documentation, categories are also called clusters.
- Each category is specific to a certain page, and each app appears within a certain category.
- Pages that do not contain any apps are not displayed.
- You can configure up to 30 categories per page and up to 100 apps per category.

For each app, you define the page and, optionally, the category in which the app is displayed in the managed Google Play Store app on the users’ devices. By default, apps are placed on a page named Other.

You configure the store layout on the Edit Android work app page. See Edit work app (page 276).

20.10.9 Configurable work apps

A work app can offer a managed configuration. This feature is included by the app developer and allows you to configure custom settings for the app.

If an app supports managed configuration, a note This app offers managed configuration is displayed on the app’s page in managed Google Play.
You configure the app settings on the **Edit Android work app** page. See [Edit work app](page 276).

## 20.10.10 Private and self-hosted work apps

All work apps that you want to make available to your users must be distributed through managed Google Play.

- **Public work apps** are apps that are available to all users with a Managed Google Account.
- **Private work apps** are apps developed by you that are only available to users inside your Managed Google Domain.
- **Self-hosted work apps** are private apps for which the app package (that is the APK file) is located on a server belonging to your organization instead of the Google server. However, the app store metadata for self-hosted apps must be uploaded to Google so that the app can be distributed through managed Google Play.

For information on private work apps, see the [Android in the enterprise developer information](external link).
21 Create administrators

1. On the menu sidebar, under SETTINGS, click Setup > Administrators to open the Show administrators page, and then click Create administrator.

2. On the Edit administrator page, configure the account details for the administrator.
   - When External LDAP directory is selected as the user directory for the customer, you can click Lookup user via LDAP to select an existing LDAP account.
   - If you do not use an external user directory enter the relevant data for Login name, First name, Last name, Email address and Password.

   The password that you specify is a one-time password. When the administrator logs in for the first time they are prompted to change it.

   **Note**
   The Login name field must only contain letters (Latin alphabet), digits, spaces and characters !._-#.

3. In the Role list, select one of the available roles.
   - The role defines the type of access rights the new administrator will have to Sophos Mobile. See User roles (page 4).

4. Click Save to create the administrator account.

   The new administrator is created and shown on the Show administrators page. Forward the user credentials (user, customer and one-time password) to the new user. The new user can log in to Sophos Mobile Admin and is prompted to change the password.
You can send a custom message to managed devices.

1. On the menu sidebar, under **MANAGE**, click **Devices**. The **Devices** page is displayed.
2. Select one or more devices, click **Actions** and then click **Send message**.
3. In the **Enter message** dialog, enter the message you want to send. The message can contain up to 500 characters.
4. Click **Finish**.
23 Manage Sophos Mobile Security

**Note**
This feature requires a license of type Mobile Advanced.

Sophos Mobile Security is a security app for Android devices that protects devices from malicious apps and assists users in detecting app permissions that could be a security risk. Its web filtering capability allows you to filter websites by category and lets you block inappropriate content.

In Sophos Mobile Admin, you can manage the Sophos Mobile Security app on devices that are enrolled with Sophos Mobile as follows:

- You can configure settings for the Sophos Mobile Security app remotely and centrally.
- You can make sure that the Sophos Mobile Security app is installed and runs scans at defined intervals. You can define this as a compliance rule.
- You can trigger scans for specific devices.
- You can view scan results for devices.

For further information on Sophos Mobile Security, see the *Sophos Mobile Security help*.

### 23.1 Configure antivirus settings for Sophos Mobile Security

**Prerequisite:** You have activated a Mobile Advanced license.

1. On the menu sidebar, under **CONFIGURE**, click **Profiles, policies** and then click **Android**. The **Profiles and policies** page is displayed.
2. Click **Create** and select **Mobile Security policy**. The **Edit policy** page is displayed.
3. Enter a name for the new profile.
4. In the **Description** field, enter a description for the profile.
5. Click **Add configuration**. The **Available configurations** page is displayed.
6. Select **Antivirus** and click **Next**. The settings view of the configuration is displayed.
7. Go to the **Antivirus** tab.
8. Under **General**, you can specify the following:
   a) In the **Cloud scan mode** field, define when Sophos Mobile Security should scan for the latest malware information. Select one of the following options to define when the app should use a cloud lookup:
      - **Always**
      - **Not while roaming**
      - **Wi-Fi only**

      With this setting you can control the data traffic of the app. If you set the **Cloud scan mode** option to **Wi-Fi only**, the cloud lookup will only be performed when the device has a Wi-Fi
connection. If you set the **Cloud scan mode** option to **Not while roaming**, a cloud lookup will never be performed while the device is roaming on a foreign network.

b) In the **Scheduled scan interval** list, select how often scans are carried out.
   If you select **Daily while charging**, a scan is performed when the device is connected to a power supply for more than 30 minutes.

9. Under **Targets**, you can select the following:
   a) Select **Scan system apps** to include system apps in scans.
      System apps are not scanned by default as they are protected by the Android OS and cannot be removed by the user. But you can activate the scanning of system apps here.
   b) Select **Scan storage** to scan all files on internal shared storage, SD card, and connected USB devices for threats, in addition to the default scanning of all installed apps.

10. Under **PUAs**, you can do as follows:
    a) Select **Detect PUAs** to scan for Potentially Unwanted Applications.
       Potentially Unwanted Applications (PUAs) are apps that, while not malicious, are generally considered unsuitable for business networks. PUAs include adware, dialers, system monitors, remote administration tools, and hacking tools. However, certain apps that can fall into the PUA category might be considered useful by some users.

    If you select this option, Sophos Mobile Security will detect PUAs during scans and notify the device user accordingly.

    b) Select **Enable user to allow PUAs** to enable users to allow apps although they have been identified as PUAs. The user can mark them as ignored. In subsequent scans, these apps will not be shown as PUAs.

11. Under **Apps with low reputation**, you can specify how to deal with these apps. Classification of apps is based on Sophos Live Protection data. Under **Mode**, you can do as follows:
    a) Select **Allow** to turn off scanning for low reputation apps.
    b) Select **Warn** to display a warning on the device when a low reputation app is detected. Users can then choose how to deal with the app. They can add it to a list of allowed apps so that no further warning is displayed if this app is detected.
    c) Select **Block** in order to prevent low reputation apps from being started. A warning will be displayed but the user cannot start the app.

12. Under **Sophos Live Protection**, you can do as follows:
    a) Make sure that the **Scan notification** check box is selected to receive scan notifications.
    b) Select **Monitor storage** to monitor internal shared storage, SD card, and connected USB devices for changes. When new files are stored in these locations, they are scanned.

13. If your scan results include apps that should be allowed to start, you can add them to the list of allowed apps. Apps on this list will always be allowed to start. The apps will not be reported.
    To identify such an app, you can use the scan results of Sophos Mobile Security. See **View Sophos Mobile Security scan results** (page 286). Before you can allow these apps to start on the devices, you must add them to an app group as described in **App groups** (page 261).

14. To add allowed apps, select the app group containing the allowed apps.

15. Click **Apply**.

## 23.2 Configure web filtering settings for Sophos Mobile Security

**Prerequisite:** You have activated a Mobile Advanced license.
The Sophos Mobile Security app protects you from browsing sites with malicious, undesirable or illegal content.

**Note**
Web filtering only works with the Android web browser or with Google Chrome.

1. On the menu sidebar, under **CONFIGURE**, click **Profiles, policies** and then click **Android**. The **Profiles and policies** page is displayed.
2. Click **Create** and select **Mobile Security policy**. The **Edit policy** page is displayed.
3. Enter a name for the new profile.
4. In the **Description** field, enter a description for the profile.
5. Click **Add configuration**. The **Available configurations** page is displayed.
6. Select **Web filtering** and click **Next**. The **Web filtering** page is displayed.
7. In the **Filter malicious websites** field, configure the access to websites with malicious content.
8. Under **Filter websites by category**, configure the access to websites based on their category. Websites are categorized based on data from SophosLabs. The data is updated constantly.
9. Under **Website exceptions**, you can define:
   a) **Allowed domains**: add domains or IP addresses that are allowed, even though the category they belong to is blocked.
   b) **Blocked domains**: add domains or IP addresses that are blocked, even though the category they belong to is allowed.
   You can insert domain names or IP addresses. Examples: www.company.com, *.company.com, 10.2.0.1, 10.2.0.1/24
10. Click **Apply**.

Users cannot change the settings that you specified in Sophos Mobile.

### 23.3 Define Sophos Mobile Security compliance rules

**Prerequisite**: You have activated a Mobile Advanced license.

You can configure compliance rules that relate to Sophos Mobile Security.

1. Add a new compliance policy or open an existing policy for editing. For further information, see **Compliance policies** (page 39).
2. Go to the **Android** tab.
3. In the **Max. SMSec scan interval** field, you can specify the maximum scan interval for malware scans performed by the Sophos Mobile Security app.
4. In the **Denial of SMSec permissions allowed** list, select whether a denial of the required permissions results in a compliance violation.
5. In the **Malware apps allowed** list, select whether detected malware apps are allowed.
6. In the **Suspicious apps allowed** list, select whether detected suspicious apps are allowed.
7. In the **PUAs allowed** list, select whether detected PUAs (Potentially Unwanted Apps) are allowed.
8. After you have configured all required settings, click **Save**.
23.4 View Sophos Mobile Security scan results

**Note**
This feature requires a license of type Mobile Advanced.

1. On the menu sidebar, under **MANAGE**, click **Devices**.
2. Click the blue triangle next to the required device and then click **Edit** or click its name. The **Show device** or the **Edit device** page is displayed.
3. Go to the **Scan results** tab. The tab shows the Sophos Mobile Security scan results. The non-clean packages, for example, Potentially Unwanted Apps, are shown in a table. Under **Threat name**, you can click the links to display further information from Sophos Labs about the relevant threat.
4. Go to the **Compliance violations** tab to view the compliance violations related to the scan results. The violations shown depend on the Sophos Mobile Security compliance rules.

23.4.1 Create a list of allowed PUAs and apps with low reputation

**Note**
This feature requires a license of type Mobile Advanced.

You can use the scan results of the Sophos Mobile Security app to create a list of allowed apps.

1. On the menu sidebar, under **MANAGE**, click **Devices**.
2. Click the blue triangle next to the device whose scan results you want to use, and then click **Edit**.
3. Go to the **Scan results** tab. The non-clean packages are shown in a table. The **Threat name** column indicates whether the displayed package is a low reputation app, a PUA or malware. You can click the links to display further information on the relevant threat from SophosLabs.
   
   Detected low reputation apps and PUAs have a blue check mark icon to the left of the package name. Only these apps can be added to the allowed apps list.
4. Click the blue check mark icon to add the app to the allowed apps list.
5. In the dialog box, click **Yes** to confirm the operation. The app is added to the allowed apps list.
6. Repeat this step for all apps you want to add.
7. To view the list, go to **Settings** and click **General**.
8. Click **Show allow list**. All apps you added are displayed. Apps on this list will be allowed to start on all managed devices. The apps are not reported anymore.

When you click **Clear allow list**, all entries in the list are deleted.
24 Sophos container

Note
This feature requires a license of type Mobile Advanced.

The Sophos container is a logical area on a device containing the Sophos Secure Workspace, Sophos Secure Email and Sophos Mobile Security apps when they are managed by Sophos Mobile.

The Sophos container is available on the following platforms:

- Android
- iOS

24.1 Configure Sophos container enrollment

Note
This feature requires a license of type Mobile Advanced.

To enroll devices with Sophos Mobile using the Sophos container enrollment type, you need to perform the following configuration steps. You need to do this for each platform (Android, iOS) for which you want to use Sophos container enrollment.

1. Create a container policy. See Configurations for Sophos container policies for Android (page 127) and Configurations for Sophos container policies for iOS (page 170).

2. Use this container policy in a task bundle.
   The task bundle must contain at least an Enroll Sophos container task and an Install profile task. See Create task bundle (page 233).

3. Use this task bundle as an initial package for enrollments through the Self Service Portal:
   In the Self Service Portal settings, in the Group settings tab, select that task bundle in the Initial package - corporate devices or Initial package - personal devices field. See Configure Self Service Portal settings (page 22).

24.2 Mobile Advanced license

When you activate a Mobile Advanced license, you can use these additional features:

- Manage the Sophos Secure Workspace and Sophos Secure Email apps. See Manage Sophos container apps (page 288).
- For Android devices, manage the Sophos Mobile Security app. See Manage Sophos Mobile Security (page 283).

After you have received your license key you need to activate the license.
Activate a Mobile Advanced license for Sophos Mobile on Premise

For Sophos Mobile on Premise, licenses are managed by the super administrator in customer management. For further information, see the Sophos Mobile super administrator guide.

Activate a Mobile Advanced license for Sophos Mobile as a Service

In Sophos Mobile Admin, go to SETTINGS > Setup > System setup > License and enter your license key in the Advanced license key field.

24.3 Manage Sophos container apps

Note
This feature requires a license of type Mobile Advanced.

For better data separation on the managed devices, Sophos Mobile provides the Sophos container apps Sophos Secure Email and Sophos Secure Workspace:

• Sophos Secure Email is an app for Android and iOS devices that provides a secure container for managing your email, calendar and contacts.
• Sophos Secure Workspace is an app for Android and iOS devices that allows users to access encrypted files stored in the cloud. Files can be decrypted and viewed in a seamless way. Encrypted files can be handed over by other apps and uploaded to one of the supported cloud storage providers. Alternatively, the documents can be stored locally within the app.

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

The Sophos container provides:

• Centrally defined password rules
• Password rules for all container apps
• Single-Sign-On for all container apps
• Sophos Secure Workspace document settings
• Sophos Secure Workspace browser settings
• Sophos Secure Email settings

You can manage the Sophos apps with Sophos Mobile as follows:

• You can configure settings for the Sophos container apps on all managed devices remotely and centrally in Sophos Mobile. See Configurations for Sophos container policies for Android (page 127) and Configurations for Sophos container policies for iOS (page 170).
• Using compliance policies, you can make sure that the Sophos container apps are installed on the devices.
• You can enable secure distribution of documents using the Corporate Documents storage provider. See Corporate documents (page 263).
You can enable corporate keyring synchronization between the Sophos Secure Workspace app and Sophos SafeGuard Enterprise. This makes the keys from a user's SafeGuard keyring available in the Sophos Secure Workspace keyring. See Enable corporate keyring synchronization (page 290).

Note
In order to manage the Sophos container apps, they must be distributed using Sophos Mobile. If users already have an unmanaged version of Sophos Secure Workspace installed on their devices, they must uninstall it first and then install the managed version.

For further information on Sophos Secure Workspace, see the Sophos Secure Workspace help.

24.4 Reset Sophos container password

Note
This feature requires a license of type Mobile Advanced.

Note
This section applies to devices that have an assigned Sophos container policy.

You can reset the Sophos container password. This is useful, for example, when users forget their password. If you reset a Sophos container password, users will be asked to define a new container password.

1. On the menu sidebar, under MANAGE, click Devices. The Devices page is displayed.
2. Click the device for which you want to reset the Sophos container password. The Show device page is displayed.
3. Click Actions. The Actions menu is displayed.
4. Click Reset Sophos container password.
5. In the dialog box, click Yes to confirm the operation.

The Sophos container password is reset. The user has to enter a new Sophos container password.

24.5 Lock and unlock the Sophos container

Note
This feature requires a license of type Mobile Advanced.

Note
This section applies to devices that have an assigned Sophos container policy.
You can lock or unlock the Sophos container, that is, set the access permissions for the Sophos container apps and for data within the Sophos container.

1. On the menu sidebar, under **MANAGE**, click **Devices**.
2. On the **Devices** page, click the blue triangle next to the device for which you want to lock or unlock the Sophos container and then click **Show**.
3. On the **Show device** page, click **Actions > Set Sophos container access**.
4. In the dialog box for setting the access permissions, select one of the following:
   - **Deny**: The Sophos container is locked. Users can no longer use it.
   - **Allow**: The Sophos container is unlocked.
   - **Auto mode**: The Sophos container is locked as long as the device violates a compliance rule for which **Lock container** is activated. This is the default behavior if you have not set an access permission.
5. Click **Yes**.

The device is triggered to synchronize with the Sophos Mobile server. On synchronization, the setting is applied to the device.

### 24.6 Corporate keyring synchronization

Corporate keyring synchronization adds the following features to the Sophos Secure Workspace app:

- The keys from a user’s SafeGuard Enterprise keyring are available in the Sophos Secure Workspace keyring (SSW keyring).
- Users of the app can then use the keys to decrypt and view documents, or encrypt documents.
- Users can continue to use local keys that were available in their SSW keyring when you enabled keyring synchronization.
- Users cannot create new local keys.
- For security reasons, the keys from the SafeGuard keyring are removed from a device when the Sophos container is locked.

### 24.6.1 Enable corporate keyring synchronization

**Prerequisites:**

- You use Sophos SafeGuard Enterprise 8.0.
- You have configured external user management for the Self Service Portal, using the same Active Directory user database that is configured in SafeGuard Enterprise.
- Sophos Secure Workspace is managed by Sophos Mobile. This requires a Mobile Advanced license.
- Sophos Mobile Security must be able to communicate with your SafeGuard Enterprise server over HTTPS.

To enable corporate keyring synchronization, you set up a connection between Sophos Mobile and Sophos SafeGuard Enterprise as follows:

1. On the menu sidebar, under **SETTINGS**, click **Setup > System setup**, and then click the **SGN** tab.
2. Click the **Certificate** link to download the certificate of the Sophos Mobile server.
3. Open SafeGuard Management Center and go to **Tools > Configuration Package Tool**.
4. On the **Servers** tab, click **Add**, browse for the certificate file and then click **OK**. Do not change the value of the **Server name** field.
5. Optional: Select **Recovery via mobile** to enable the synchronization of BitLocker and FileVault recovery keys with the Sophos Secure Workspace app.

6. On the **Managed client packages** tab, configure the following settings:
   - In the **Configuration Package Name** field, select **Managed Client (Default)**.
   - In the **Primary Server** field, select your SGN server.
   - In the **Transport Encryption** field, select **SSL**.

7. Click **Create Configuration Package**.

8. On the **SGN** tab of Sophos Mobile Admin, click **Upload a file** to upload the configuration package that you created in the SafeGuard Management Center to Sophos Mobile.

9. Click **Save** to save the SafeGuard integration settings.
25 Transfer data from Sophos Mobile to Sophos Mobile in Central

You can export data from Sophos Mobile on Premise or Sophos Mobile as a Service and then import it into Sophos Mobile in Central.

The following items can be transferred:

- Profiles
- Policies
- App groups

To export your data, perform these steps in Sophos Mobile on Premise or Sophos Mobile as a Service:

1. On the menu sidebar, under SETTINGS, click Setup > Export.
2. Under Export preview, the items that will be exported are listed.
3. Click Export and then enter a password for the exchange file used to transfer data to Sophos Mobile in Central.
4. Click Download.
   The exchange file is downloaded to your computer.

To import your data into Sophos Mobile in Central, perform these steps in Sophos Central Admin:

5. On the menu sidebar, under My Products, click Mobile.
6. On the menu sidebar of the Mobile view, under SETTINGS, click Setup > Import.
7. Click Upload exchange file and then select the exchange file.
   Enter the password you set when exporting the data.
8. Click Upload to upload the exchange file.
9. Under Import preview, the items that will be imported are listed. Check if there are any warnings.

**Important**
If there are existing items with the same name as items to be imported, they will be overridden.

10. Click Import to import the data into your Sophos Mobile in Central account.
## 26 Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>customer</strong></td>
<td>The tenant that manages devices.</td>
</tr>
<tr>
<td><strong>device</strong></td>
<td>The device to be managed (for example smartphone, tablet or Windows 10 device).</td>
</tr>
<tr>
<td><strong>enrollment</strong></td>
<td>The registration of a device with Sophos Mobile.</td>
</tr>
<tr>
<td><strong>Enterprise App Store</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>provisioning</strong></td>
<td>The process of installing the Sophos Mobile Control app on a device.</td>
</tr>
<tr>
<td><strong>Self Service Portal</strong></td>
<td>The web interface that allows users to enroll their own devices and carry out other tasks without having to contact the helpdesk.</td>
</tr>
<tr>
<td><strong>Mobile Advanced license</strong></td>
<td>With a license of type Mobile Advanced you can manage the Sophos Mobile Security, Sophos Secure Workspace and Sophos Secure Email apps through Sophos Mobile.</td>
</tr>
<tr>
<td><strong>SMSec</strong></td>
<td>Abbreviation for Sophos Mobile Security.</td>
</tr>
<tr>
<td><strong>Sophos Mobile client</strong></td>
<td>The Sophos Mobile Control app that is installed onto devices managed by Sophos Mobile.</td>
</tr>
<tr>
<td><strong>Sophos Mobile console</strong></td>
<td>The web interface that you use to manage devices.</td>
</tr>
<tr>
<td><strong>Sophos Mobile Security</strong></td>
<td>A security app for Android devices. You can manage this app with Sophos Mobile, provided that a license of type Mobile Advanced is activated.</td>
</tr>
<tr>
<td><strong>Sophos Secure Email</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Sophos Secure Workspace</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>task bundle</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
27 Technical support

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

• Visit the Sophos Community at community.sophos.com/ and search for other users who are experiencing the same problem.
• Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.
28 Legal notices

Copyright © 2011-2018 Sophos Limited. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos is a registered trademark of Sophos Limited and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

Last update: 20180115