SOPHOS
Security made simple.

Sophos Mobile Control

SaaS startup guide

Product version: 7

Contents

1 About this guide

This guide explains how to initially configure Sophos Mobile Control as a Service to manage your devices.

Further information is available in the Sophos Mobile Control administrator help.

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

2 About Sophos Mobile Control

Sophos Mobile Control

Sophos Mobile Control is a management tool for mobile devices like smartphones and tablets, and also for Windows 10 desktop devices. It helps to keep corporate data safe by managing apps and security.

The Sophos Mobile Control system consists of a server and a client component.

The server is the core component of the Sophos Mobile Control product. It provides a web interface to administer Sophos Mobile Control and to manage the enrolled devices.

The client is an app to be installed onto the devices. It supports over-the-air setup and configuration through the web interface of the Sophos Mobile Control server.

With the Sophos Mobile Control Self Service Portal for your users, you can reduce IT effort by allowing users to enroll devices on their own and to carry out other tasks without contacting the helpdesk.

Sophos Mobile Control can also be used to manage the Sophos Mobile Security, Sophos Secure Workspace and Sophos Secure Email mobile apps. This requires an SMC Advanced license.

Sophos Mobile Security

Sophos Mobile Security is a security app for Android devices. Using up-to-the-minute intelligence from SophosLabs, your apps will be automatically scanned as you install them. This antivirus functionality protects you from malicious software which can lead to data loss and unexpected costs.

Sophos Secure Workspace

Sophos Secure Workspace is 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. It is designed to prevent any data loss even when your device is lost or stolen or when you send a document to an unintended destination.

Files can be decrypted and viewed in a seamless way. Files that are handed over by other apps can be encrypted and either uploaded to one of the supported cloud storage providers or stored locally within Sophos Secure Workspace.

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.

Sophos Secure Workspace also includes Corporate Browser, a web browser that lets you securely access corporate intranet pages and other allowed pages, as defined by a Sophos Mobile Control policy.

Sophos Secure Email

Sophos Secure Email is an app for Android and iOS devices that provides a secure container for managing your email, calendar and contacts. All data is encrypted and is protected from third-party access.

3 What are the key steps?

To start using Sophos Mobile Control:

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

4 Change your password

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

1. Open the address of the Sophos Mobile Control console in your web browser.
2. In the **Login** dialog, click **Forgot password?**.
3. In the **Reset password** dialog, enter your **Customer** and **User** information from the email you have received for the activation of your Sophos Mobile Control as a Service account, and then click **Reset password**.

   You will receive an email with a link to reset your password.

4. Click the link to open the **Change password** dialog.
5. Enter a new password, and then click **Change password**.

   Your password is changed. Remember to use this password next time you log in to the console.

Note: We recommend that you modify the password policies to enforce stronger passwords, for example by requiring a minimum number of lower-case, upper-case or special characters. See Configure password policies (page 13).

5 Change your login name

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

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

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

6 Activate SMC Advanced licenses

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

If SMC Advanced licenses have not been activated during the initial configuration of Sophos Mobile Control, you can activate them later from the Sophos Mobile Control console:

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

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

7 Check your licenses

Sophos Mobile Control 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.
- **Used licenses**: Number of licenses in use.
- **Valid until**: The license expiry date.

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

Note: To notify when the license is about to expire, Sophos Mobile Control sends several email reminders to all administrators, starting 30 days prior to the expiry date.

8 Configure settings

The following settings need to be configured:

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

8.1 Configure personal settings

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

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

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

2. Configure the following settings:

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

3. Click **Save**.

8.2 Configure password policies

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

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

1. On the menu sidebar, under **SETTINGS**, click **Setup** > **General**, and then click the **Password policies** tab.
2. Under **Rules**, you can define password requirements, like a minimum number of lower-case, upper-case or numerical characters that a password must contain to be valid.

3. Under **Settings**, configure the following settings:

   a) **Password change interval (days)**: Enter the number of days until a password expires (between `1` and `730`), or leave the field empty to disable password expiration.

   b) **Number of previous passwords which must not be reused**: Select a value between `1` and `10`, or select `---` to disable this restriction.

   c) **Maximum number of failed login attempts**: Select the number of failed login attempts until the account gets locked (between `1` and `10`), or select `---` to allow an unlimited number of failed login attempts.

4. Click **Save**.

8.3 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 on 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**.

8.4 Configure Self Service Portal settings

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

   The **Self Service Portal** page opens.

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

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

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

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

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

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

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

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

5. Click **Save**.

9 Apple Push Notification service certificates

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

APNs certificates have a validity period of one year. To notify when the certificate is about to expire, Sophos Mobile Control sends several email reminders to the administrators, starting 30 days prior to the expiry date.

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.

9.1 Requirements

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

- The Sophos Mobile Control 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)`

9.2 Create an APNs certificate

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

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

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 Control. In the **Create Apple ID** step, click **Create a new Apple ID**.

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

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

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

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

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

   This opens the Apple Push Certificates Portal.

6. Log in with your Apple ID and upload the certificate signing request file `apple.csr`.
7. Download the `.pem` APNs certificate file and save it to your computer.
8. In the **Upload APNs certificate** step, click **Upload certificate** and then browse for the `.pem` file that you received from the Apple Push Certificates Portal.
9. Click **Save** to add the APNs certificate to Sophos Mobile Control.

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

10 Standalone EAS proxy

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

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

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

Note: For performance reasons, we recommend you use the standalone EAS proxy server instead of the internal version when email traffic for more than 500 client devices must be managed.

Features

- Support for multiple Microsoft Exchange or IBM Notes Traveler email servers. You can set up one EAS proxy instance per email server.
- Load balancer support. You can set up standalone EAS proxy instances on several computers and then use a load balancer to distribute the client requests among them.
- Support for certificate-based client authentication. You can select a certificate from a certification authority (CA), from which the client certificates must be derived.
- Support for email access control through PowerShell. In this scenario, the EAS proxy service communicates with the email server through PowerShell to control the email access of your managed devices. Email traffic happens directly from the devices to the email server and is not routed through a proxy. See Set up email access control through PowerShell (page 21).

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

10.1 Usage scenarios for the standalone EAS proxy

A standalone EAS proxy server should be used for the following scenarios.

You use IBM Notes Traveler (formerly IBM Lotus Notes Traveler) for non-iOS devices

Microsoft Exchange and IBM Notes Traveler for iOS devices use the ActiveSync protocol for the communication between email server and client, while IBM Notes Traveler for non-iOS devices (for example, Android) uses a different protocol. The standalone EAS proxy supports that protocol.

For non-iOS devices, dedicated Traveler client software is required. This software is available through `<traveler-server>/servlet/traveler` or the Traveler file system. The *Install App* and *Uninstall App* features of Sophos Mobile Control can be used to install and uninstall the Traveler client software. Configuration has to be performed manually.

You want to support multiple backend servers

With the standalone EAS proxy you can set up multiple instances of backend email systems. Each instance needs an incoming TCP port. Each port can connect to a different backend. You need one URL per EAS proxy instance.

You want to set up load balancing for EAS

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

For this scenario an existing load balancer for HTTP is required.

You want to use client certificate based authentication

For this scenario an existing PKI is required and the public part of the CA certificate has to be set in the EAS proxy.

You need to manage more than 500 devices

For performance reasons, we recommend you use the standalone EAS proxy server instead of the internal version when email traffic for more than 500 client devices must be managed.

10.2 Download the EAS proxy installer

1. Log in to the Sophos Mobile Control console.
2. On the menu sidebar, under **SETTINGS**, click **Setup** > **System setup** and then click the **EAS proxy** tab.
3. Under **External**, click the link to download the EAS proxy installer.

The installer file is saved to your local computer.

10.3 Install the standalone EAS proxy

Prerequisite:

- All required email servers are accessible. The EAS proxy installer will not configure connections to servers that are not available.
- You are an administrator on the computer where you install the EAS proxy.

1. Run `Sophos Mobile Control EAS Proxy Setup.exe` to start the **Sophos Mobile Control EAS Proxy - Setup Wizard**.
2. On the **Choose Install Location** page, choose the destination folder and click **Install** to start installation.

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

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

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

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

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

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

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

   Note:

   You can download an SSL Certificate Wizard from MySophos that you can use to request your SSL certificate for the Sophos Mobile Control EAS proxy.

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

   - If you do not have a trusted certificate yet, select **Create self-signed certificate**.
   - If you have a trusted certificate, click **Import a certificate from a trusted issuer** and select one of the following options from the list:
     - **PKCS12 with certificate, private key and certificate chain (intermediate and CA)**
     - **Separate files for certificate, private key, intermediate and CA certificate**

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

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

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

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

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

   - **Instance type**: Select **EAS proxy**.
   - **Instance name**: A name to identify the instance.
   - **Server port**: The port of the EAS proxy for incoming email traffic. If you set up more than one proxy instance, each of these must use a different port.
   - **Require client certificate authentication**: Email clients must authenticate themselves when connecting to the EAS proxy.
   - **ActiveSync server**: The name or IP address of the server with which the proxy instance will connect.
   - **SSL**: Communication between the proxy instance and the ActiveSync server is secured by SSL.
   - **Allow EWS subscription requests from Secure Email**: Select this to allow the Sophos Secure Email app on iOS to subscribe to push notifications through Exchange Web Services (EWS). Push notifications inform the device when there are messages for Secure Email, even if the app is closed.

     Note: By default, the EAS proxy blocks all requests to the Exchange server's EWS interface for security reasons. If you select this checkbox, subscription requests are allowed. Other requests remain blocked.

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

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

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

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

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

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

10. Make a note of the certificate folder. You need this information when you upload the certificate to Sophos Mobile Control.
11. Optional: Click **Add** again to configure additional EAS proxy instances.
12. When you have configured all required EAS proxy instances, click **Next**.

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

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

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

14. On the **Sophos Mobile Control EAS Proxy - Configuration Wizard finished** page, click **Finish** to close the Configuration Wizard and return to the Setup Wizard.
15. In the Setup Wizard, make sure that **Start Sophos Mobile Control EAS Proxy server now** is selected, then click **Finish** to complete the configuration and to start the Sophos Mobile Control EAS proxy for the first time.

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

16. Log in to the Sophos Mobile Control console.
17. On the menu sidebar, under **SETTINGS**, click **Setup** > **System setup** and then click the **EAS proxy** tab.
18. Under **External**, click **Upload a file** and upload the certificate that the **Sophos Mobile Control EAS Proxy - Setup Wizard** has created for the PowerShell connection.

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

19. Click **Save**.
20. In Windows, open the **Services** dialog and restart the **EASProxy** service.

This completes the initial setup of the standalone EAS proxy.

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

10.4 Set up email access control through PowerShell

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

The PowerShell scenario has these advantages:

- Devices communicate directly with the Exchange server.
- You do not need to open a port on your server for incoming email traffic from your managed devices.

Supported email servers are:

- Exchange Server 2010
- Exchange Server 2013
- Exchange Server 2016

- Office 365 with an Exchange Online plan

To set up PowerShell:

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

Configure PowerShell

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

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

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

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

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

   Note: This step is not required for Office 365.

Create a service account

3. Log in to the relevant admin console:
   - For Exchange Server 2010: **Exchange Management Console**
   - For Exchange Server 2013/2016: **Exchange Admin Center**
   - For Office 365: **Office 365 Admin Center**

4. Create a user account. This account is used as a service account by Sophos Mobile Control to execute PowerShell commands.
   - Use a user name like **`smc_powershell`** that identifies the account purpose.
   - Turn off the setting to make the user change their password the next time they log in.
   - Remove any Office 365 license that was automatically assigned to the new account. Service accounts don’t require a license.

5. Create a new role group and assign it the required permissions.
   - Use a role group name like **`smc_powershell`**.
   - Add the **Mail Recipients** and **Organization Client Access** roles.
   - Add the service account as a member.

Set up PowerShell connections

6. Use the **Sophos Mobile Control EAS Proxy - Setup Wizard** as if you would set up a standalone EAS Proxy. In wizard step **EAS Proxy instance setup**, configure the following settings:
   - **Instance type**: Select **PowerShell Exchange/Office 365**.
   - **Instance name**: A name to identify the instance.
   - **Exchange server**: The name or IP address of the Exchange server (for a local Exchange server installation) or `outlook.office365.com` (for Office 365). Don't include a prefix `https://` or a suffix `/powershell`. These are added automatically.
   - **Allow all certificates**: The certificate that the Exchange server presents is not verified. Use this for example if you have a self-signed certificate installed on your Exchange server. Because the **Allow all certificates** option reduces the security level of the server communication, we strongly recommend that you select it only if required by your network environment.
   - **Allow EWS subscription requests from Secure Email**: Select this to allow the Sophos Secure Email app on iOS to subscribe to push notifications through Exchange Web Services (EWS). Push notifications inform the device when there are messages for Secure Email, even if the app is closed.

     Note: By default, the EAS proxy blocks all requests to the Exchange server's EWS interface for security reasons. If you select this checkbox, subscription requests are allowed. Other requests remain blocked.
   - **Service account**: The name of the user account you created in the Exchange or Office 365 admin console.
   - **Password**: The password of the user account.
7. Click **Add** to add the instance to the **Instances** list.
8. **Optional:** Repeat the previous steps to set up PowerShell connections to other Exchange or Office 365 servers.
9. Complete the **Sophos Mobile Control EAS Proxy - Setup Wizard** as described in Install the standalone EAS proxy (page 19).

Upload certificates

10. Log in to the Sophos Mobile Control console.
11. On the menu sidebar, under **SETTINGS**, click **Setup** > **System setup** and then click the **EAS proxy** tab.
12. Under **External**, click **Upload a file**. Upload the certificate that the **Sophos Mobile Control EAS Proxy - Setup Wizard** created for the PowerShell connection.

    If you have set up more than one instance, repeat this for all instance certificates.
13. Click **Save**.
14. In Windows, open the **Services** dialog and restart the **EASProxy** service.

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

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

10.5 Configure a connection to the internal EAS proxy server

1. On the menu sidebar, under **SETTINGS**, click **Setup** > **System setup**.
2. On the **System setup** page, click the **EAS proxy** tab.
3. In the **Internal** section, enter the Exchange or groupware server URL in the **Exchange/groupware server URL** text field.
4. Select **Use SSL** to use a secure connection.
5. Select **Allow EWS subscription requests from Secure Email** to allow the Sophos Secure Email app on iOS to subscribe to push notifications through Exchange Web Services (EWS). Push notifications inform the device when there are messages for Secure Email, even if the app is closed.

   By default, the EAS proxy blocks all requests to the Exchange server's EWS interface for security reasons. If you select this checkbox, subscription requests are allowed. Other requests remain blocked.
6. Click **Check connection** to test the connection.

   A message will be displayed if the server can be accessed.
7. Click **Save**.

10.6 Configure a connection to the external EAS proxy server

To configure the connection between Sophos Mobile Control and the standalone EAS proxy, you upload the certificate of the EAS proxy server to Sophos Mobile Control. The certificate was generated when you configured the EAS proxy instance.

Important: If the EAS proxy service is started before you have uploaded the certificate, Sophos Mobile Control rejects the connection to the server and the service fails to start.

To upload the certificate of the external EAS proxy:

1. On the menu sidebar, under **SETTINGS**, click **Setup** > **System setup**, and then click the **EAS proxy** tab.
2. In the **External** section, click **Upload a file** and navigate to the certificate file.

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

11 Configure Network Access Control

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

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

To configure Network Access Control:

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

     This option enables Sophos UTM integration (for version 9.2 and higher). The integration requires you to set the SMC server URL and admin user credentials in the UTM WebAdmin under **Management** > **Sophos Mobile Control**, as described in the *Sophos UTM online help*.
   - **Cisco ISE**

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

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

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

- **Check Point**

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

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

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

- **Web service**

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

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

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

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

- **Custom**

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

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

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

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

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

12 Compliance rules

With compliance rules 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 various sets of compliance rules 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 sets of compliance rules for at least these two device types.

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

12.1 Create compliance rules

To create compliance rules:

1. On the menu sidebar, under **CONFIGURE**, click **Compliance rules**.
2. On the **Compliance rules** page, click **Create compliance rules**.
3. Enter a **Name** and an optional **Description** for the new set of compliance rules.

The **Compliance rules** page contains individual tabs for the device platforms that are activated for the customer. 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.

   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.

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

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

Option	Description
Deny email	Forbid email access. This action can only be taken if you have configured a connection to the internal or to the standalone EAS Proxy. See Configure a connection to the internal EAS proxy server (page 24) or Configure a connection to the external EAS proxy server (page 24).
Lock container	Disable the Sophos Secure Workspace and Secure Email apps. This affects document, email and web access that is managed by these apps. This action can only be taken when you have activated an SMC Advanced license. This option is only relevant for Android and iOS devices.
Deny network	Forbid network access. This action can only be taken if you have configured Network Access Control. See Configure Network Access Control (page 25).
Notify admin	Send compliance emails to selected recipients. The list of recipients and the time schedule is specified collectively for all sets of compliance rules that you create. See the instructions later in this section.
Transfer task bundle	Transfer a specific task bundle to the device. We recommend that you set this to **None** at this stage. For further information, see the Sophos Mobile Control administrator help. **Important:** When used incorrectly, task bundles may misconfigure or even wipe devices. To assign the correct task bundles to compliance rules, an in-depth knowledge of the system is required.

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

   The new set is displayed on the **Compliance rules** page.

8. If you have selected the **Notify admin** action for one of the compliance rules, click **Compliance email settings** to specify the recipients that will receive compliance emails and the times when compliance emails are sent.

   You can specify the recipients either by entering the name of an administrator or by entering a valid email address.

   Note: These are common settings that apply to all compliance rules that have a **Notify admin** action.

9. Click **Save** to save the compliance email settings.

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

13 Device groups

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

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

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

13.1 Create device group

1. On the menu sidebar, under **MANAGE**, click **Device groups**, and then click **Create device group**.
2. On the **Edit device group** page, enter a **Name** and a **Description** for the new device group.
3. In the **Compliance rules** section, use the **Corporate devices** and **Personal devices** lists to select the compliance rules you want to apply.
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. For further information, see the Sophos Mobile Control administrator help.

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

14 Configure iOS devices

14.1 Create iOS device profile

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

We recommend that you set up separate profiles for:

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

Note:

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

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

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

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

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

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

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

   c) Optional: **Version**: Enter a version number for the profile.

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

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

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

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

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

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

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

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

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

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

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

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

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

14.2 Create task bundle for iOS devices

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

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

3. Enter a name and, optionally, a version and a description for the new task bundle in the relevant fields.
4. When you select the **Selectable for compliance actions** option, the task bundle can be transferred onto a device when the device breaks a compliance rule. See Compliance rules (page 27).

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

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

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

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

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

9. 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.

15 Configure Android devices

15.1 Create Android device profile

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

We recommend that you set up separate profiles for:

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

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

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

   b) Optional: **Version**: Enter a version number for the profile.

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

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

   The **Password policies** page opens.

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

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

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

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

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

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

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

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

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

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

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

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

15.2 Create task bundle for Android devices

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

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

3. Enter a name and, optionally, a version and a description for the new task bundle in the relevant fields.
4. When you select the **Selectable for compliance actions** option, the task bundle can be transferred onto a device when the device breaks a compliance rule. See Compliance rules (page 27).

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

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

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

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

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

9. 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.

16 Update Self Service Portal settings

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

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

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

17 Configure user management

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

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

Note:

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

To select the user management method:

1. On the menu sidebar, under **SETTINGS**, click **Setup** > **System setup**, and then click the **User setup** tab.
2. Select the data source for the user accounts for the Sophos Mobile Control console and the Self Service Portal (SSP):
   - Select **Internal directory** to use internal user management.
   - Select **External LDAP directory** to use external user management instead of or in combination with internal user management.
3. If you selected **External LDAP directory**, click **Configure external LDAP** to specify the server details. See Configure external directory connection (page 39).
4. Click **Save**.

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

18 Use internal user management

18.1 Create a Self Service Portal test user

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

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

1. On the menu sidebar, under **MANAGE**, click **Users**, and then click **Create user**.
2. Configure the required account details.

   Make sure that **Send welcome email** is selected.
3. Click **Save**.

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

18.2 Test device enrollment through the Self Service Portal

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

Log in to the Self Service Portal with the test user account you created for yourself in Create a Self Service Portal test user (page 37) and perform test enrollments for all platforms that you want to manage with Sophos Mobile Control.

18.3 Import users into Sophos Mobile Control

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

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

You add new Self Service Portal users by importing a UTF-8 encoded comma-separated values (CSV) file with up to 300 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 welcome 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.

19 Use external user management

19.1 Configure external directory connection

When you use an external LDAP directory for managing user accounts for the Sophos Mobile Control console and the Self Service Portal, you must configure the directory connection so that Sophos Mobile Control can retrieve the user data from the LDAP server.

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

1. On the menu sidebar, under **SETTINGS**, 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) Select the **LDAP type**. Sophos Mobile Control supports:

   - **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** to use SSL for the server connection. For Sophos Mobile Control as a Service, **SSL** 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** to use SSL for the server connection. For Sophos Mobile Control as a Service, **SSL** cannot be deselected.

   d) In the **User** field, enter an account for lookup operations on the directory server. Sophos Mobile Control 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 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 **SSP group** field, using one of the following options:

   - If you enter an asterisk **`*`**, all authenticated directory users are allowed to log in to the Self Service Portal.
   - 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 the Sophos Mobile Control console but not for the Self Service Portal.

   Note:

   The group you specify here is not related to the directory group you define on the **Group settings** tab of the **Self Service Portal** page. With those settings, you define task bundles, Sophos Mobile Control group membership and available device platforms for each directory group.

   For further information on the Self Service Portal group settings, see the Sophos Mobile Control administrator help.

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

19.2 Test device enrollment for LDAP users

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

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

20 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 Control.
- 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.

   Click **Next** to continue.

3. When you have entered search criteria, the wizard displays a list of matching users.

   Select the required user and click **Next**.

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

Option	Description
Platform	The device platform. You can only select a platform that is enabled for the customer that you logged in to.
Name	A unique name under which the device will be managed by Sophos Mobile Control.
Description	An optional description of the device.
Phone number	An optional phone number. Enter the number in international format, for example **`+491701234567`**.
Email address	The email address to which the enrollment instructions will be sent.
Owner	Select the device owner: either **Company** or **Employee**.
Device group	Select the device group the device will be assigned to. If you have not created a device group yet, you can select the device group **Default**, which is always available.

   When you are ready, click **Next**.

5. On the **Bundle selection** wizard page, 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.

   Note: Only task bundles that contain an *Enroll* task are displayed.

   When you are ready, click **Next**. The device is added to Sophos Mobile Control.

6. On the **Enrollment** wizard page, follow the instructions to install the Sophos Mobile Control app onto the device and to complete the enrollment and provisioning.
7. When enrollment has been completed successfully, click **Finish** to close the device enrollment wizard.

Note:

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

21 Glossary

device
The device to be managed (for example smartphone, tablet or Windows 10 device).

enrollment
The registration of a device with Sophos Mobile Control.

Enterprise App Store
An app repository that is hosted on the Sophos Mobile Control server. The administrator can use the Sophos Mobile Control console to add apps to the Enterprise App Store. Users can then use the Sophos Mobile Control app to install these apps onto their devices.

provisioning
The process of installing the Sophos Mobile Control app on a device.

Self Service Portal
The web interface that allows users to enroll their own devices and carry out other tasks without having to contact the helpdesk.

SMC Advanced license
With a license of type SMC Advanced you can manage the Sophos Mobile Security, Sophos Secure Workspace and Sophos Secure Email apps through Sophos Mobile Control.

SMSec
Abbreviation for Sophos Mobile Security.

Sophos Mobile Control client
The Sophos Mobile Control app that is installed onto the managed device.

Sophos Mobile Security
A security app for Android devices. You can manage this app with Sophos Mobile Control, provided that a license of type SMC Advanced is activated.

Sophos Secure Email
An app for Android and iOS devices that provides a secure container for managing your email, calendar and contacts. You can manage this app with Sophos Mobile Control, provided that a license of type SMC Advanced is activated.

Sophos Secure Workspace
An app for Android and iOS devices that provides a secure workspace where you can browse, manage, edit, share, encrypt and decrypt documents from various storage providers or distributed by your company. You can manage this app with Sophos Mobile Control, provided that a license of type SMC Advanced is activated.

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

Sophos Mobile Control console The web interface that you use to manage devices.

22 Technical support

You can find technical support for Sophos products in any of these ways:

- Visit the Sophos Community at community.sophos.com/ and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at www.sophos.com/en-us/support.aspx.
- Download the product documentation at www.sophos.com/en-us/support/documentation.aspx.
- Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.

23 Legal notices

Last update: 20170315