SOPHOS

Security made simple.

Sophos Mobile Control

SaaS startup guide

Product version: 6

Document date: January 2016

Contents

1 About this guide

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

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

This guide focuses on Apple iOS and Android as the most common mobile platforms. The settings apply to other 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. 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 registered mobile devices.

The client is an app to be installed on the mobile 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 register their own devices and 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 phones and tablets. 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 Apple iOS and Android 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. 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.

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 Apple iOS and Android 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 web 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, activate them in the web console.
3. Check your licenses.
4. Configure personal settings, password policies for web console users, technical support contact details, and settings for the Self Service Portal.
5. Get an Apple Push Notification service certificate.
6. Optionally, set up a standalone EAS proxy to filter email traffic from mobile devices to an email server.
7. Optionally, configure the interface to 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 web console for the first time.

1. Use your preferred web browser to open the web console URL.
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 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 web 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 web 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. Optionally, adjust the values of the remaining fields:
   - **First name**
   - **Last name**
   - **Email adress**
5. Click **Save**.

Your account details are changed. Remember to use the new login name next time you log in to the web 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. See About Sophos Mobile Control (page 5).

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 web 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:

- **Number of licenses**: Number of end users that can be managed from the web console.
- **Licenses used**: Number of licenses in use.
- **Valid until**: The license expiry date.
- **Licensed URL**: The URL of the Sophos Mobile Control server for which the license is issued.

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

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 by end users

8.1 Configure personal settings

To use the Sophos Mobile Control web 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 web console.
Timezone	Select the timezone in which dates are shown.
Unit of length	Select if you want to use **metric** or **imperial** units for length values.
Lines per page in tables	Select the maximum number of table lines you want to display per page in the web console.
Show extended device details	Select this check box to show all available information about the device. The tabs **Custom properties** and **Internal properties** will be added to the **Show device** view.
Activated platforms	Select the platforms you want to manage: ▪ **Android** ▪ **iOS** ▪ **Windows Mobile** (includes Windows Phone 8.x and Windows 10 Mobile operating systems) Based on your platform selection, the user interface of the web console will be 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 web 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 (up to 730 days), or enter **0** 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 will be 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** on the navigation bar.

3. On the **Agreement** 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 confirm that they have read 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 Get an Apple Push Notification service certificate

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

Sophos Mobile Control manages APNs certificates per customer. You have to create and upload the certificates for each customer that you use.

The following sections describe the requirements that have to 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 Apple iOS device with Wi-Fi only access needs to connect to `*.push.apple.com:5223 TCP (17.0.0.0/8)`

9.2 Create and upload an APNs certificate

To perform this task you need to have the **iOS** platform activated in the personal settings of the customer. See Configure personal settings (page 12).

Note: Do not use Internet Explorer to access any Apple websites. Apple recommends their own Safari browser, but Mozilla Firefox, Opera or Google Chrome also work.

1. You can use the APNs Certificate Wizard to create an APNs certificate. The wizard is included in your product delivery. It is also available for download from the web console. In the web console menu sidebar, under **SETTINGS**, go to the **Setup** > **System Setup** > **iOS APNS** tab, then click the download link.
2. Double-click the file `Sophos Mobile Control APNs Certificate Wizard.exe` to launch the **APNs Certificate Wizard**.
3. On the **License Agreement** page, click **I Agree** to accept the license terms.
4. On the **Create Certificate Signing Request** page, enter your **Company Name** and your **Country** code (for example **US** or **UK**).

   The directory in which the certificate request will be stored is shown on the **Create Certificate Signing Request** page. Make a note of this information, then click **Next**.
5. On the **Upload PLIST** page, you will upload the Certificate Signing Request to Apple. Follow the instructions in the dialog:

   a) Use a Firefox, Chrome or Safari browser to navigate to the Apple site that is shown.

We recommend that you use the latest browser version.

b) Log in with your Apple ID, or create an ID if you do not have one yet.
We recommend you create a corporate Apple ID and not a personal one.

c) On the first page of the **Apple Push Certificates Portal**, click **Create a Certificate**.

d) Accept the terms and conditions.

e) Browse for your Certificate Signing Request (`*.plist`) and click **Upload**.
On the **Upload PLIST** page, you can click the `Upload to Apple` link to open the directory in which the `*.plist` file has been created.

f) When your APNs certificate has been created, download and save the certificate file (`*.pem`) in the `PEM from Apple` directory.

6. Click **Next**.
7. On the **Create P12** page, you will create your APNs certificate for Sophos Mobile Control. Enter a password for the APNs certificate. You need this password later, when you upload the `.P12` certificate file to Sophos Mobile Control.

   The directory in which the certificate will be stored is shown on the **Create P12** page. Make a note of this information, then click **Next**.

   Note: We recommend that you create a backup copy of that directory.

8. On the **Sophos Mobile Control APNs Certificate Wizard finished** page, click **Finish**.
9. On the **iOS APNS** tab of the Sophos Mobile Control web console, click **Upload a file**. Browse for the `.p12` certificate file you have created and enter your password. Optionally you can also enter your Apple ID for future reference.

   After the file has been uploaded successfully, a confirmation message is displayed and the **Topic**, **Type** and **Expiry date** information of your APNs certificate is shown.

10. Click **Save** to complete the procedure.

10 Set up a standalone EAS proxy

10.1 Standalone EAS proxy

With Sophos Mobile Control, you can set up an EAS proxy to filter email traffic from mobile devices to an email server.

The mobile 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.

Features

- Support for multiple Microsoft Exchange or Lotus 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.

10.2 Usage scenarios for the standalone EAS proxy

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

You use Lotus Traveler for non-iOS devices

Microsoft Exchange and Lotus Traveler for iOS devices use the ActiveSync protocol for the communication between email server and client, while Lotus 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.

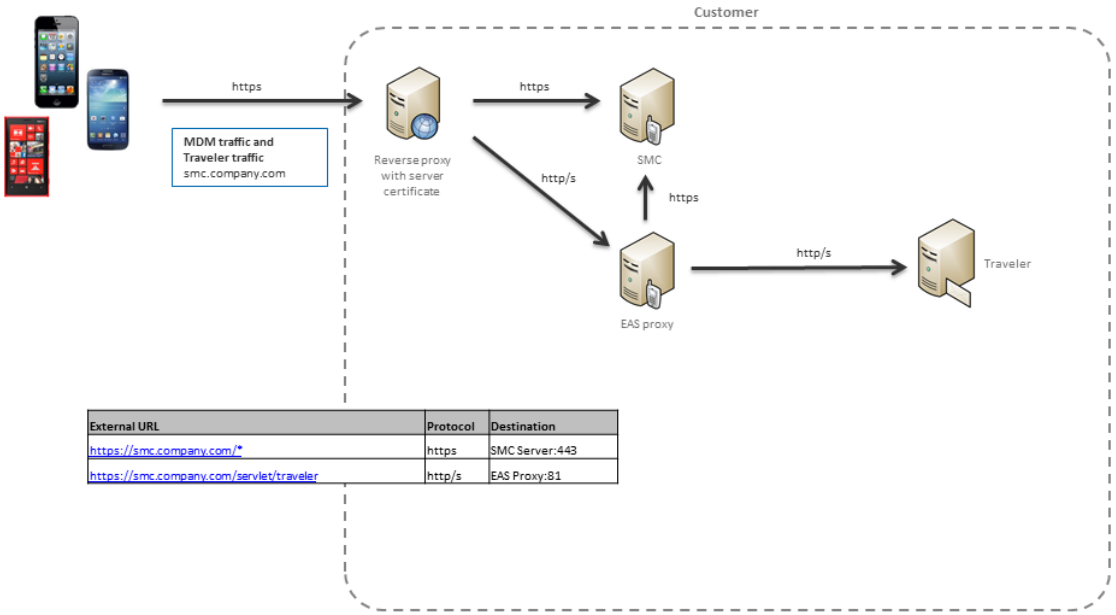


Figure 1: EAS proxy for Lotus Traveler

You want to support multiple backend servers

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

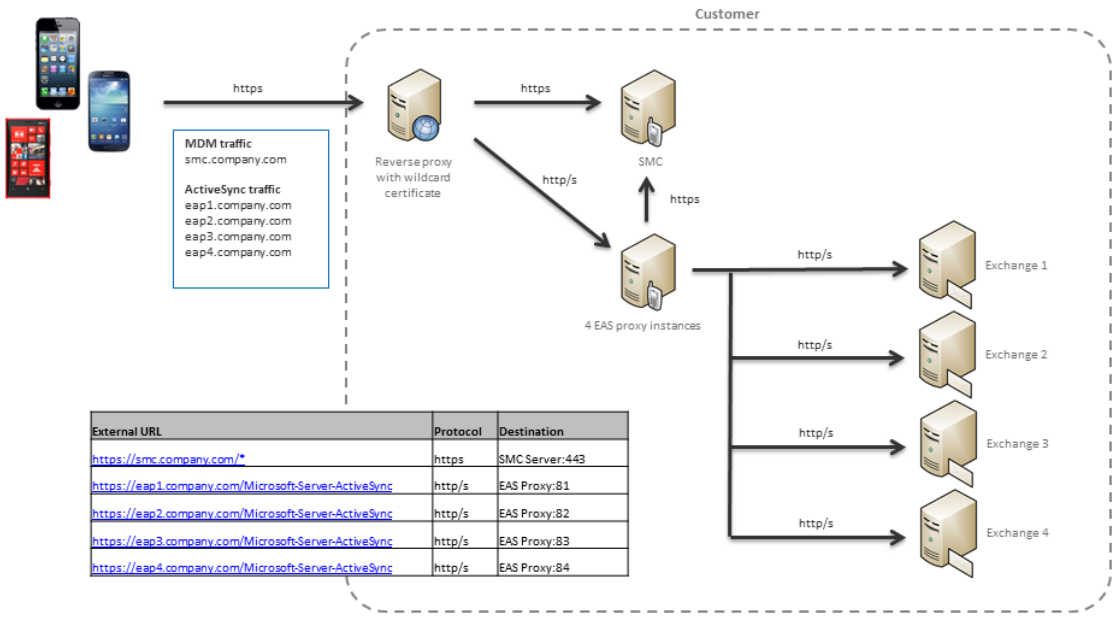
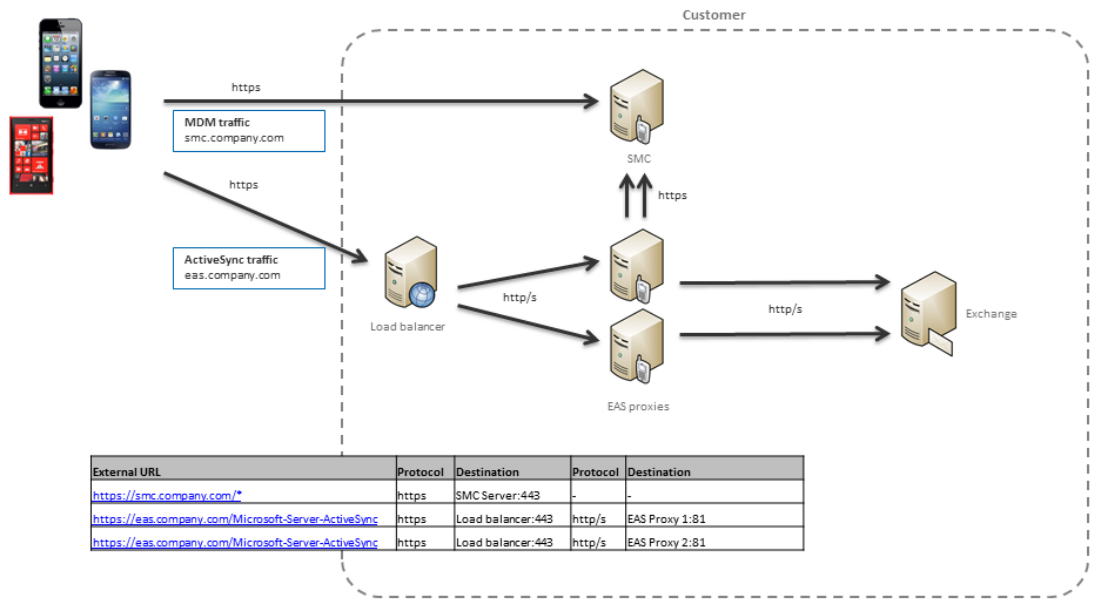


Figure 2: SMC and multiple EAS proxy instances

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.



External URL	Protocol	Destination	Protocol	Destination
https://smc.company.com/*	https	SMC Server:443	-	-
https://eas.company.com/Microsoft-Server-ActiveSync	https	Load balancer:443	http/s	EAS Proxy 1:81
https://eas.company.com/Microsoft-Server-ActiveSync	https	Load balancer:443	http/s	EAS Proxy 2:81

Figure 3: Load-balanced EAS proxies (can also be used behind reverse proxy)

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.

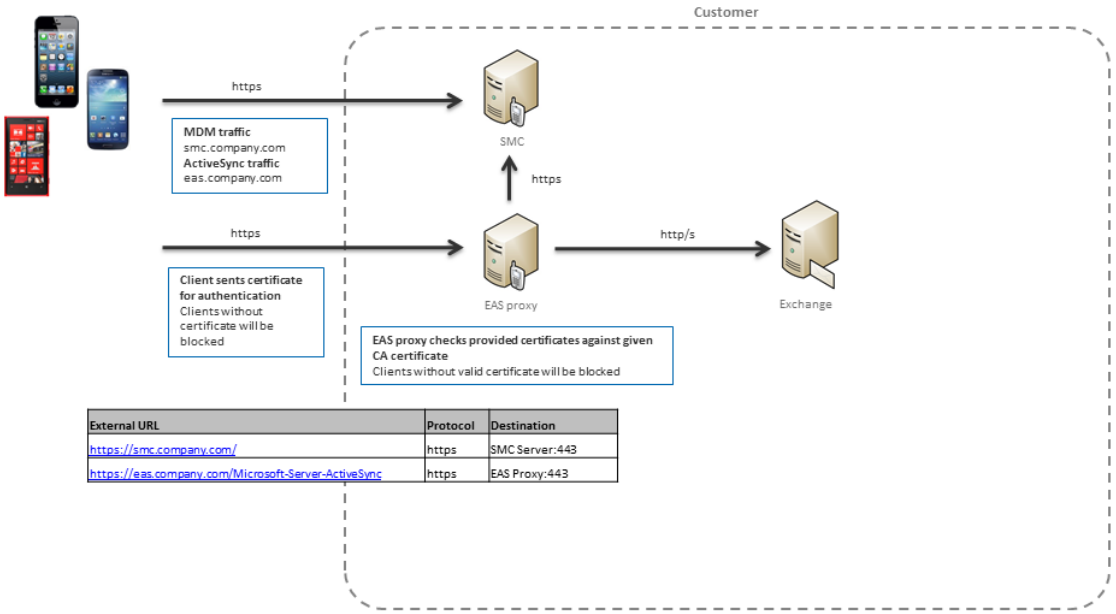


Figure 4: EAS proxy with client certificate authentication

10.3 Download the EAS proxy installer

1. Log on to the Sophos Mobile Control web console.
2. On the menu sidebar, under **SETTINGS**, click **Setup** and then click **System setup**.

   The **System setup** view is displayed.
3. Go to the **EAS proxy** tab and click the download link in the **External** section.

10.4 Install the standalone EAS proxy

Prerequisite:

- During the configuration of the EAS proxy instances, the installer will check if the specified mail servers are accessible. You need to make sure that these servers are available before running the installer.

To install and configure the standalone EAS proxy:

1. Run the `Sophos Mobile Control EAS Proxy Setup.exe` as administrator to launch the **Sophos Mobile Control EAS Proxy - Setup Wizard**.
2. Review and agree to the license terms.
3. 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 launched automatically and guides you through the configuration steps.

4. 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.
5. 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 the Sophos knowledge base article *Using your MySophos account to download your Sophos software*, which is available at https://www.sophos.com/support/knowledgebase/111195.aspx.

   - 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 box:
     - **PKCS12 with certificate, private key and certificate chain (intermediate and CA)**
     - **Separate files for certificate, private key, intermediate and CA certificate**

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

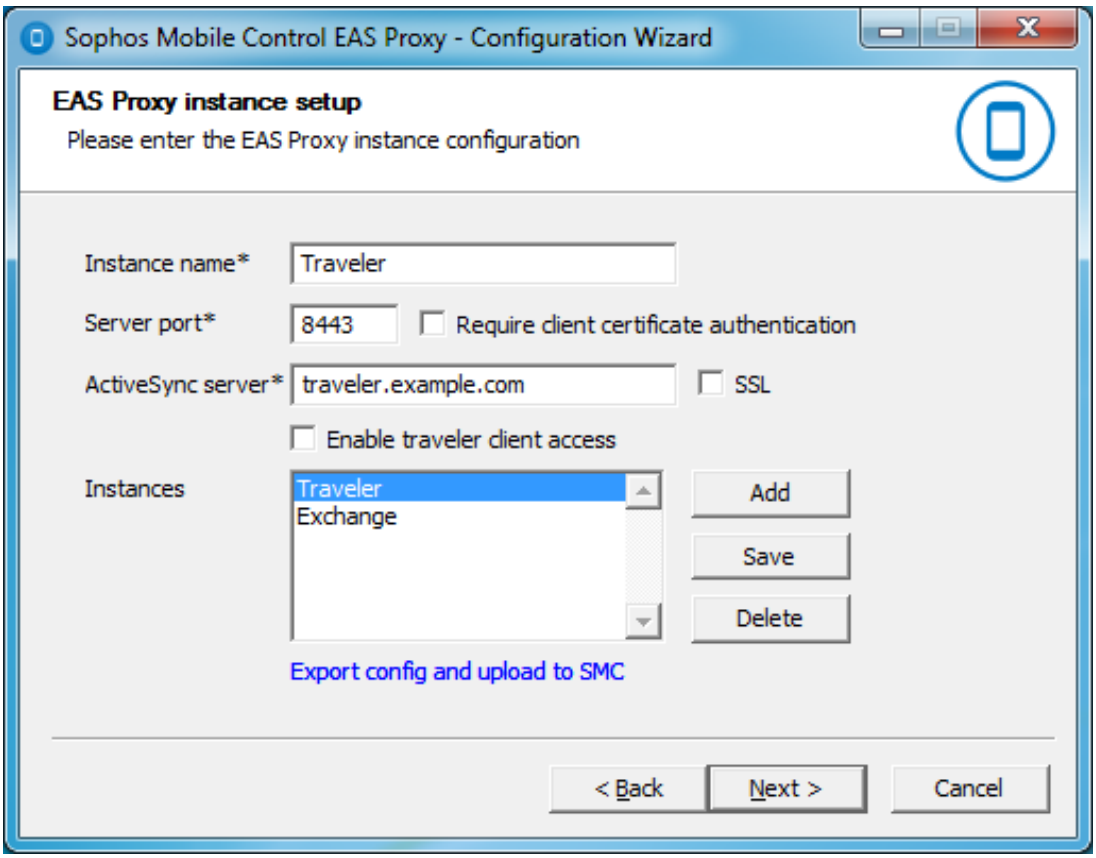
   Note: For a self-signed certificate, you need to specify a server that is accessible from the client devices.

7. 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.

8. On the **EAS Proxy instance setup** page, configure one or more EAS proxy instances. For every instance, enter an **Instance name**, the relevant **Server port** for incoming traffic and the **ActiveSync server** with which the proxy instance will connect. Select **Enable traveler client access** to enable Lotus Traveler client access. If required, you can enable SSL or client certificate authentication for certain instances.

   Note: If you set up more than one proxy instance, each of these must use a different server port.



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

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

10. 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.

11. Log in to the Sophos Mobile Control web console and navigate to **Setup** > **System setup** > **EAS proxy**.

12. In the **External** section, click **Upload a file** and select the certificate file that has been created for the EAS proxy instance. Do not forget to save these changes to the **EAS proxy** settings.

    Note: You need to upload the certificate before you start the EAS proxy. If the certificate is not available at startup, Sophos Mobile Control rejects the connection and the service will not be started.

13. If required, repeat steps 8 to 12 to configure additional instances of the EAS proxy. When finished, click **Next**.

    The server ports that you entered are tested and Inbound Rules for the Windows Firewall are configured.

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.

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.

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 criteria are not met.

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 drop-down list box:
   - **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.
Redirect page for disallowed 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 the ISE, you must configure the URL of the Sophos Mobile Server and the credentials that you entered here.

- **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.

  On the security gateway, you must configure some specific settings, as described in the Check Point Support Center article MDM cooperative enforcement for Mobile clients.

- **Custom**

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

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

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

  Note: The **Custom** option is deprecated. For certificate based access to the NAC interface, we recommend that you use the NAC web service interface.

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

12 Create compliance rules

With compliance rules you can:

- Allow, disallow or enforce certain features of a mobile 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 mobile devices, we recommend that you define separate sets of compliance rules for at least these two device types.

For detailed information on compliance rules, see the Sophos Mobile Control administrator help.

To create a set of 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 mobile 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 will not be checked for compliance.

5. Under **Rule**, configure the compliance criteria 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.

   If you have defined app groups, you can assign these to the compliance rules **Allowed apps**, **Not allowed apps** and **Mandatory apps**.

   For a detailed description of all settings, click **Help** on the navigation bar.

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 when you use the Sophos Mobile Control EAS Proxy server. See Set up a standalone EAS proxy (page 17).
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.
Deny network	Forbid network access. See Configure Network Access Control (page 24).
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, as described in step 8 below.
Transfer task bundle	Transfer a specific task bundle to the device. We recommend that you set this to **None** at this stage. 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. For further information, see the Sophos Mobile Control administrator help.

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 in the **Compliance rules** list view.

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 Create device groups

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.

Note: We recommend that you only group devices with the same operating system. This makes it easier to use groups for installations and other operating system specific tasks.

To create a new 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 **Company devices** and **Employee devices** list boxes to select the compliance rules you want to apply.
4. Click **Save**.

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

The new device group is created and shown in the **Device groups** view.

Note: If you delete a device group, the group's members are moved to another group that needs to be specified. If there is no other group left to move the devices to, the group cannot be deleted. Before a group is deleted a warning message is displayed.

14 Configure Apple iOS devices

14.1 Create profiles for Apple iOS devices

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 web console.
- Import profiles created with Apple Configurator.

This section describes how to create profiles in the web 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) **Version**: Optionally, enter a version number for the profile.
   d) **Description**: Enter a description for the profile, for example **`base profile`**.
   e) **User can remove profile**: Select whether users are allowed to remove the profile from their device. Possible values are:
      - **Always**
      - **With authentication**
      - **Never**

We recommend that you select **Never**.

f) **Automatically remove on**: Optionally, select a date for the automatic removal of the profile from the mobile devices.

We recommend that you do not set a date.

4. Click **Show** next to **Operating systems** and select the version of the operating system the profile applies to. Select all relevant iOS versions for this profile.

   The list shows the iOS versions of the devices that are already registered with the system, and a generic version **iOS** that covers all supported iOS versions.

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

   For a detailed description of the settings, click **Help** on the navigation bar.

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, select **Restrictions** and click **Next**.
9. 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** on the navigation bar.

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 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 bundles for Apple iOS devices

1. On the menu sidebar, under **CONFIGURE**, click **Task bundles** > **Apple iOS** to open the **Task bundles** page, and then click **Create task bundle**.

2. On the **Edit task bundle** page, configure the following settings:
   a) **Name**: Enter a name for the task bundle. We recommend that you use the name **`iOS SSP task bundle`** for task bundles that are applied during enrollment through the Self Service Portal.
   b) **Version**: Optionally, enter a version number for the task bundle.
   c) **Description**: Enter a description for the task bundle, for example **`base SSP task bundle`**.
   d) **Selectable for compliance actions**: When you select this option, the task bundle can be loaded onto a device when the device breaks a compliance rule. See Create compliance rules (page 26).
3. Click **Show** next to **Operating systems** and select the version of the operating system the task bundle applies to. Select all relevant iOS versions for this task bundle.
   The list shows the iOS versions of the devices that are already registered with the system, and a generic version **iOS** that covers all supported iOS versions.
4. 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 in the Self Service Portal while the task is processed.
5. 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 (**`iOS SSP profile`**, if you have used the suggested name). Click **Apply** to create the task.
6. If you have configured profiles for Exchange ActiveSync, VPN or Wi-Fi settings, repeat the previous step for each profile.
7. If required, 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.
8. After you have added all required tasks to the task bundle, click the **Save** button on the **Edit task bundle** page.

The task bundle is displayed on the **Task bundles** page and is available for transfer onto Apple iOS devices.

15 Configure Android devices

15.1 Create profiles for Android devices

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)

To create an Android device profile for password policies and restrictions:

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
4. 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) **Version**: Optionally, enter a version number for the profile.
   c) **Description**: Optionally, enter a description for the profile, for example **`base profile`**.
5. Click **Show** next to **Operating systems** and select the version of the operating system the profile applies to. Select all relevant Android versions for this profile.

   The list shows the Android versions of the devices that are already registered with the system, and a generic version **Android** that covers all supported Android versions.
6. To add password policies to the profile, click **Add configuration**, select **Password policies** and click **Next**.

   The **Password policies** page opens.
7. In **Password type**, select the type of password you want to define, for example **Complex**.
8. 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** on the navigation bar.
9. Click **Apply** to save your settings.

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

10. To add restrictions to the profile, click **Add configuration** again, select **Restrictions** and click **Next**.
11. 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** on the navigation bar.

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

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

13. 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 bundles for Android devices

1. On the menu sidebar, under **CONFIGURE**, click **Task bundles** > **Android** to open the **Task bundles** page, and then click **Create task bundle**.
2. On the **Edit task bundle** page, configure the following settings:

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

   b) **Version**: Optionally, enter a version number for the task bundle.

   c) **Description**: Enter a description for the task bundle, for example **`base SSP task bundle`**.

   d) **Selectable for compliance actions**: When you select this option, the task bundle can be loaded onto a device when the device breaks a compliance rule. See Create compliance rules (page 26).

3. Click **Show** next to **Operating systems** and select the version of the operating system the task bundle applies to. Select all relevant Android versions for this task bundle.

   The list shows the Android versions of the devices that are already registered with the system, and a generic version **Android** that covers all supported Android versions.

4. 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 in the Self Service Portal while the task is processed.

5. 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 (**`Android SSP profile`**, if you have used the suggested name). Click **Apply** to create the task.
6. If you have configured profiles for Exchange ActiveSync, VPN or Wi-Fi settings, repeat the previous step for each profile.

7. If required, 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.

8. After you have added all required tasks to the task bundle, click the **Save** button on the **Edit task bundle** page.

The task bundle is displayed on the **Task bundles** page and is available for transfer onto Android devices.

16 Update Self Service Portal settings

After you have created the task bundles to be transferred when users register their devices with the Sophos Mobile Control 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 opens.
3. From the **Task bundle/profile** list box, select the task bundles you have created for Apple iOS and Android devices.
4. Select the **Active** check box for the device types that should be available in the Self Service Portal:
5. From the **Add to device group** list box, select the group that devices will be added to when they are registered 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 web console and the Self Service Portal:

- Internal user management

  With internal user management you can create users by adding them manually through the web console or by importing them from a .csv file.

- External user management

  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 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 web 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 directory** 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 mobile platforms that you want to manage with Sophos Mobile Control.

For detailed information on how to use the Self Service Portal, see the Sophos Mobile Control user help.

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.

To import users from a list of account data:

1. On the menu sidebar, under **MANAGE**, click **Users**, and then click **Import users**.
2. To import users into Sophos Mobile Control, you need to create a .csv file with the user account data, formatted using *comma separated values* (CSV).

   If you do not have CSV formatted user account data yet, you can click the **Example CSV** link to download a sample file that shows the required data structure.

3. After you have prepared the .csv file with the user account data, click **Upload a file** and select it in the dialog.

   The user entries are read in from the file and are displayed on the **Import users** page.

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 user entries, correct the content of the .csv file accordingly and upload it again.

5. When all user entries are read in without errors, make sure that **Send welcome emails** is selected.
6. Click **Finish** to create the user accounts.

The users are imported and displayed in the **Show users** view. 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 web 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.

1. On the menu sidebar, under **SETTINGS**, click **Setup** > **System setup**, and then click the **User setup** tab.
2. Click **Configure external LDAP** to specify the server details.
3. On the **Server details** page, configure the following settings:
   a) Select the **LDAP type**. Sophos Mobile Control supports:
      - **Active Directory**
      - **Domino**
      - **eDirectory**
      - **Red Hat Directory**
      - **Zimbra**

   b) In the **Primary URL** field, enter the URL of the directory server. You can enter the server IP or the server name. Select **SSL** to use **SSL** for the server connection.
   c) In the **Backup URL** field, optionally enter the URL of the backup server. You can enter the server IP or the server name. Select **SSL** to use **SSL** for the server connection.
   d) In the **User** field, enter a user who has read rights for 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>`

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

   Click **Next**.
4. On the **Search base** page, enter the distinguished name of the search base object.

   The search base object defines the location in the external directory from which the search for the user or group that is trying to log in begins.

5. On the **Search fields** page, define which directory fields are to be used for resolving the *%_USERNAME_%* and *%_EMAILADDRESS_%* placeholders in profiles. Select the required fields from the **User name** and **Email** list boxes, or enter the values manually.

   Note: The list boxes only contain fields that are configured for the user that is currently connected to the LDAP directory, that is the user that you specified in step 3.d above. If that user does not have an email field configured, for example, you need to manually enter the required value in the **Email** field.

   For example for Active Directory, these field mappings apply:

   - **User name**: **`sAMAccountName`**
   - **First name**: **`givenName`**
   - **Last name**: **`sn`**
   - **Email**: **`mail`**

6. 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 complete 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 web console but not for the Self Service Portal.

   Note:

   The group that you specify here is not related to the directory group that 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 mobile platforms for each directory group.

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

7. Click **Apply**.
8. 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 test enrollments for all mobile platforms that you want to manage with Sophos Mobile Control.

For detailed information on how to use the Self Service Portal, see the Sophos Mobile Control user help.

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.
- Assign the device to a user (optional).
- Enroll the device.
- Transfer an enrollment task bundle to the device (optional).

To launch the device enrollment wizard:

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

   Tip: Alternatively, you can launch 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 type: either **Corporate** 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.

   When you are ready, click **Next**. This will add the device to Sophos Mobile Control.

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

21 Glossary

customer	The tenant that manages devices.
device	The mobile device to be managed (for example smartphone or tablet).
end user	The end user of the device.
enrollment	The registration of a device with Sophos Mobile Control.
provisioning	The process of installing the Sophos Mobile Control client on a device.
Self Service Portal (SSP)	The Sophos Mobile Control web interface that allows end users to enroll their own devices and carry out other tasks without having to contact the helpdesk.
SMC Advanced license	An SMC Advanced license adds functionality to a standard license by enabling you to manage Sophos Mobile Security, Sophos Secure Workspace and Sophos Secure Email through Sophos Mobile Control.
SMSec	Abbreviation for Sophos Mobile Security used in the Sophos Mobile Control web console user interface.
Sophos Mobile Control client	The Sophos Mobile Control app that is installed on the mobile device.
Sophos Mobile Security	A security app for Android phones and tablets. You can manage this app from Sophos Mobile Control, provided that an SMC Advanced license is available and activated in the Sophos Mobile Control web console.
Sophos Secure Email	An app for Apple iOS and Android devices that provides a secure container for managing your email, calendar and contacts. You can manage this app from Sophos Mobile Control, provided that an SMC Advanced license is available and activated in the Sophos Mobile Control web console.
Sophos Secure Workspace	An encryption app for Apple iOS and Android phones and tablets. You can manage this app from Sophos Mobile Control, provided that an SMC Advanced license is available and activated in the Sophos Mobile Control web console.
task bundle	A package you can create in the web console to bundle several tasks for mobile devices into one transaction. You can bundle all tasks necessary to have a device fully enrolled and running.

web console	The web interface of the server that is used to manage devices.

22 Technical support

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

- Visit the SophosTalk 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

Copyright © 2011 - 2016 Sophos Ltd. 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 Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.