SOPHOS

Security made simple.

Sophos Mobile Control installation guide

Product version: 7

Contents

1 About this guide

This guide explains how to install and set up Sophos Mobile Control version 7. It also describes how to update an existing installation of Sophos Mobile Control.

Unless otherwise noted, all procedures must be performed as an administrator of Microsoft Windows Server or as a user of the relevant group.

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 Sophos Mobile Control licenses

Sophos Mobile Control offers two types of licenses:

- SMC Standard license
- 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.

For further information on managing Sophos Mobile Security, Sophos Secure Workspace and Sophos Secure Email with Sophos Mobile Control, see the Sophos Mobile Control administrator help.

As a super administrator, you can activate your purchased licenses in the super administrator customer and assign the required number of licensed users to individual customers.

3.1 Trial licenses

Sophos offers a free trial for Sophos Mobile Control. You can register for the trial on the Sophos website: http://www.sophos.com/en-us/products/free-trials/mobile-control.aspx.

A trial license allows you to manage up to five users and is valid for 30 days.

All you will need when you set up Sophos Mobile Control for evaluation is the email address you used to register when downloading the installer.

3.2 Upgrade trial licenses to full licenses

To upgrade trial licenses to full licenses you only have to enter your full license key in Sophos Mobile Control. For further information, see the Sophos Mobile Control administrator help.

3.3 Update licenses

To update your licenses you have to activate the new license key in Sophos Mobile Control. For further information, see the Sophos Mobile Control super administrator guide.

4 Set up Sophos Mobile Control

The key steps to set up Sophos Mobile Control are:

- Request an SSL Certificate, see Request an SSL certificate for Sophos Mobile Control (page 8).
- Run the Sophos Mobile Control installer, see Install and set up the Sophos Mobile Control server (page 9).

After the installation there are a few initial configuration steps that you need to perform:

- Log in to the Sophos Mobile Control console for the first time to start the configuration wizard.
- For iOS devices, you need to get an Apple Push Notification service certificate.
- Optionally, you can set up a standalone EAS Proxy for email filtering that has the following advantages over the internal EAS Proxy that is automatically installed with Sophos Mobile Control:
  - Support for certificate-based client authentication.
  - IBM Notes Traveler client support for non-iOS devices.
  - Support for multiple Exchange and IBM Notes Traveler servers.

For details on these configuration tasks, see the Sophos Mobile Control startup guide.

4.1 Deployment considerations

We recommend you read the Sophos Mobile Control deployment guide before performing the installation and deployment of the Sophos Mobile Control server. This guide provides guidance on the following aspects of a Sophos Mobile Control server installation:

- Architecture examples for the integration of the Sophos Mobile Control server into your company's infrastructure.
- Architecture examples for the integration of the standalone EAS proxy into your company's infrastructure.
- Dimensioning guidelines in terms of hardware (for example CPU and memory) and software (for example database and virtualization) requirements.
- Communication details (ports, protocols, destinations) of required inbound and outbound connections.

4.2 System environment requirements

The Sophos Mobile Control installer runs a series of test to verify that your system environment meets all the necessary requirements for Sophos Mobile Control.

These requirements are:

- You are an administrator on the computer.
- The computer's operating system is supported by Sophos Mobile Control.

  Supported operating systems are the 64-bit editions of:

  - Windows Server 2008 R2 SP1
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016

  (including additional service packs, if available)

- The computer has at least one network adapter.
- The computer has at least 4 GB of RAM.
- The Microsoft Internet Information Services (IIS) web server is disabled on the computer.
- The HTTP/S ports 80, 443 and 8080 are available on the computer.
- The computer can connect to the Apple Push Notification service (APNs).
- The computer can connect to the Google Cloud Messaging (GCM) service.
- The computer can connect to the Windows Push Notification service.
- The computer can connect to the Sophos services.
- Optional: The computer can connect to the Apple Volume Purchase Program (VPP) web service.
- Optional: The computer can connect to the Apple Device Enrollment Program (DEP) web service.
- Optional: The computer can connect to the Apple iTunes web service.
- Optional: The computer can connect to the Apple Activation Lock Bypass web service.
- Optional: The computer can connect to the Google webservice for Android Enterprise.

4.3 Request an SSL certificate for Sophos Mobile Control

In order to set up Sophos Mobile Control, you need an SSL web server certificate. In the setup process, you can select between creating a self-signed certificate and using a PKCS #12 with certificate, private key and certificate chain. For further information, see Install and set up the Sophos Mobile Control server (page 9). Your Sophos product delivery includes an SSL Certificate Wizard in the *%MDM_HOME%*`\tools\Wizard` folder which you can use to request your certificate or you can download the wizard from www.sophos.com/mysophos.

Note: If you use a self-signed certificate or a certificate that is issued by your own certificate authority (CA), you must manually install that self-signed certificate or your CA certificate on your devices before you enroll them with Sophos Mobile Control. If you do not do this, the Sophos Mobile Control app will not trust your server and will refuse to connect. Certificates issued by a globally trusted CA do not require this manual installation.

Note: You cannot install Android apps from APK files that are hosted on the Sophos Mobile Control server if you use a self-signed certificate or a certificate that is issued by your own CA.

To request your SSL certificate:

- Start the SSL Certificate Wizard by double-clicking the file *Sophos Mobile Control SSL Certificate Wizard.exe*.

  The wizard guides you through installation. Enter the required information, considering the following instructions:

  a) On the **Upload CSR** page, you can click the **Open CSR** button to open the CSR file if your certificate vendor supports copy and paste.

  b) On the **Import Certificate Files** page, enter the CA certificate downloaded on the **Upload CSR** page into the **Select CA certificate file** field.

  c) On the **Certificate created** page, the location of the certificate created is shown. You need to refer to this location when setting up Sophos Mobile Control, see Install and set up the Sophos Mobile Control server (page 9).

Note: You should create a backup of the folder containing the certificate files.

4.4 Install and set up the Sophos Mobile Control server

- If you plan to connect Sophos Mobile Control to an existing database, make sure you have the logon credentials for the database available before starting the installation, and that you have sufficient permissions to create new data stores, user accounts and data records.
- If the database is not held locally, you need access to TCP port 1433 (for Microsoft SQL Server) or 3306 (for MySQL). In addition, you need an admin account that the Sophos Mobile Control server can use to log in to the database.

1. Run the Sophos Mobile Control installer as administrator, and review and agree to the **License Agreement**.
2. On the **System Property Checks** page, click **Check** to run the tests to verify that your system environment meets all the necessary requirements for Sophos Mobile Control. See System environment requirements (page 7).

   You can click **Report** to generate a report of the test results.
3. On the **Choose Install Location** page, choose the destination folder for Sophos Mobile Control server.
4. On the **Database Type Selection** page, select the database type you want to use:
   - **Install and use Microsoft SQL Server 2016 Express**: Installs immediately SQL Server 2016 Express and configures it to be used with Sophos Mobile Control. This option is only available if you install Sophos Mobile Control on a Windows Server 2016 computer.
   - **Install and use Microsoft SQL Server 2014 Express**: Installs immediately SQL Server 2014 Express and configures it to be used with Sophos Mobile Control. This option is only available if you install Sophos Mobile Control on a Windows Server 2008 or 2012 computer.
   - **Use existing Microsoft SQL database**
   - **Use existing MySQL**

5. On the **Database Settings** page, enter the logon credentials for the database.

   Note: If you select the **Use SQL Server Authentification** option, you need to make sure that the SQL login language is set to English. See Change the SQL login language (page 11) for details.

6. On the **Database Selection** page, click **Create a new database named** and enter a name for the database to be created, for example SMCDB.
7. On the **Database Configuration** page, progress messages are displayed during the database creation.

   When the database has been successfully created and populated, click **Next** to continue.

8. If you have selected Windows authentication for the database access, there is a page **Set service credentials** where you set the Windows account under which the Sophos Mobile Control service runs.

   You can use the Local System account or a user account. In the latter case, specify the user account either as **`<computer name>\<user name>`** or as **`<domain>\<user name>`**.

   The installer will assign the database access rights to that account.

   Note: For security reasons, we recommend that you run the Sophos Mobile Control service as a user with limited access rights. The user account should have the following properties:

   - User account is a local Windows account on the computer on which Sophos Mobile Control is installed.
   - User is not a member of any group, not even of the *users* group.
   - User can access your SQL database with the necessary change rights. For an MS-SQL database, this means that the user must be a member of the *db_datareader* and *db_datawriter* roles.

9. On the **Configure super admin account** page, enter a name for the **Super admin customer** (a special customer that is only used by the super administrator), the **Super admin login** (the super administrator login name) and a **Super admin password**.

   The super administrator is primarily intended for customer management and should not be used for routine device management. In Sophos Mobile Control, customers are the tenants that manage the devices of their users. The super administrator logs in to the super administrator customer and can, for example, predefine settings for new customers and push settings and configurations to existing customers. For further information, see the Sophos Mobile Control super administrator guide.

   Note:

   - The super admin credentials are required for the first login to the Sophos Mobile Control console.
   - After installation, additional super administrators can be added in the Sophos Mobile Control console.

10. On the **Configure external server name** page, enter a Sophos Mobile Control server name (for example smc.mycompany.com).

    Note: The server name must be resolvable by the managed devices.

11. On the **Configure server certificate** page, import a certificate for secure (HTTPS) access to the web server.
    - If you have a trusted certificate, click **Import a certificate from a trusted issuer** and an option from the drop-down list.
    - If you do not have a trusted certificate yet, select **Create self-signed certificate**.

    Note: If you use a self-signed certificate or a certificate that is issued by your own certificate authority (CA), you must manually install that self-signed certificate or your CA certificate on your devices before you enroll them with Sophos Mobile Control. If you do not do this, the Sophos Mobile Control app will not trust your server and will refuse to connect. Certificates issued by a globally trusted CA do not require this manual installation.

    Note: You cannot install Android apps from APK files that are hosted on the Sophos Mobile Control server if you use a self-signed certificate or a certificate that is issued by your own CA.

    Note: Your Sophos product delivery includes an SSL Certificate Wizard that you can use to request your SSL certificate for Sophos Mobile Control. For further information, see Request an SSL certificate for Sophos Mobile Control (page 8).

12. 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 managed devices.

13. On the **Server Information** page, verify the server information, then click **Next** to confirm the server and configuration process.
14. After installation has finished, the **Sophos Mobile Control - Installation finished** dialog box is displayed. Make sure that the check box **Start Sophos Mobile Control server now** is selected and click **Finish** to start the Sophos Mobile Control service for the first time.

    Note: After the service has been started it can take a few minutes before the Sophos Mobile Control web interface is available.

After the installation there are a few initial configuration steps that you need to perform:

- Log in to the Sophos Mobile Control console for the first time to start the configuration wizard. See the Sophos Mobile Control startup guide.
- For iOS devices, you need to get an Apple Push Notification service certificate. See the Sophos Mobile Control startup guide.
- Optionally, you can set up a standalone EAS proxy for email filtering. See Standalone EAS proxy (page 13).

4.5 Change the SQL login language

If you have configured Sophos Mobile Control Server to use SQL Server authentication to connect to the database, the SQL login language must be set to English. Otherwise, an error occurs when the Sophos Mobile Control service is started.

This topic describes how to change the SQL login language to English.

1. Stop the Sophos Mobile Control service.
2. Open SQL Server Management Studio on the server and select **Security** > **Logins**.

3. On the **General** page of the **Login Properties**, set **Default language** to English, then click **OK** to save the changes.
4. Restart the Sophos Mobile Control service.

5 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.

There are two types of EAS proxy:

- The internal EAS proxy that is automatically installed with Sophos Mobile Control. It supports incoming ActiveSync traffic as used by Microsoft Exchange or IBM Notes Traveler for iOS and Samsung Knox devices.
- A standalone EAS proxy that can be downloaded and installed separately. 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

The standalone EAS proxy has additional features compared to the internal version:

- Support for IBM Notes Traveler for non-iOS devices (for example, Android). The Traveler client for these devices uses a protocol (not ActiveSync) that is not supported by the internal EAS proxy.
- 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 18).

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.

5.1 Usage scenarios for the standalone EAS proxy

Note: Additional to the information provided in this section, the Sophos Mobile Control deployment guide contains schematic diagrams for the integration of the standalone EAS proxy into your company's infrastructure. We recommend that you observe that information before performing the installation and deployment of 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

The internal EAS proxy is not suitable for this scenario because it only supports the ActiveSync protocol, which is used by Microsoft Exchange and by IBM Notes Traveler for iOS devices. IBM Notes Traveler for non-iOS devices (for example, Android) uses a different protocol that is supported by the standalone EAS proxy.

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.

5.2 Download the EAS proxy installer

1. Log in to the Sophos Mobile Control console as super administrator.
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.

5.3 Install the standalone EAS proxy

Prerequisite:

- Sophos Mobile Control has been installed and set up.
- 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: Your Sophos product delivery includes an SSL Certificate Wizard that you can use to request your SSL certificate for the Sophos Mobile Control EAS proxy. For further information, see Request an SSL certificate for Sophos Mobile Control (page 8).

   - 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 as super administrator.
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.

5.4 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.

Note: For a schematic of the PowerShell communication, see the Sophos Mobile Control deployment guide.

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 15).

Upload certificates

10. Log in to the Sophos Mobile Control console as a super administrator.
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.

6 Load balancing and high availability

Sophos Mobile Control (SMC) makes it possible to set up a high-availability environment. This ensures that the SMC service remains externally accessible and tasks can be further processed even after failure of a Sophos Mobile Control node. To achieve this, load balancing, that distributes client and browser sessions by using DNS Round Robin to the available nodes, is required.

The following describes setting up clustering for Sophos Mobile Control and configuring load balancing with Sophos UTM.

6.1 Requirements

- One separate Windows server for each Sophos Mobile Control node.
- All nodes must be on the same network.
- One Microsoft SQL or MySQL database server or cluster.
- Sophos UTM or Apache Reverse Proxy (mod_proxy) for load balancing. Load balancer must support permanent session cookies and official SSL web server certificates.

Note: For detailed information about the installation requirements see the Sophos Mobile Control 7 release notes and the Sophos Mobile Control installation prerequisites form.

Architecture

For an example of a three-node Sophos Mobile Control cluster see the Sophos Mobile Control deployment guide.

For multicast communication between the individual Sophos Mobile Control nodes, optionally a separate network can be used. The network interface to be used can be selected during cluster configuration, as described in Set up the first node (page 22). It may also be a VLAN.

Note: If you want to operate a second Sophos Mobile Control cluster for test purposes, a separate network is needed.

Ports and protocols

The following table shows the required ports and protocols for communication between the individual nodes of a Sophos Mobile Control server cluster.

Protocol	Ports	Destination
TCP	7600, 8181, 57600	*<Incoming>*
TCP	7600, 8181, 57600	*<Outgoing>*

Protocol	Ports	Destination
UDP	45700	*<Incoming>*

Server certificates

When you set up Sophos Mobile Control, you configure an SSL web server certificate that allows the Sophos Mobile Control app to establish a secure connection to the Sophos Mobile Control server. We recommend that you use a certificate that is issued by a globally trusted certificate authority (CA). In a clustered environment with several SMC server nodes behind a load balancer, this might not be practical. You might want to use a self-signed certificate instead. Sophos Mobile Control supports self-signed certificates, but the following restrictions apply:

- If you use a self-signed certificate or a certificate that is issued by your own certificate authority (CA), you must manually install that self-signed certificate or your CA certificate on your devices before you enroll them with Sophos Mobile Control. If you do not do this, the Sophos Mobile Control app will not trust your server and will refuse to connect. Certificates issued by a globally trusted CA do not require this manual installation.
- You cannot install Android apps from APK files that are hosted on the Sophos Mobile Control server if you use a self-signed certificate or a certificate that is issued by your own CA.

6.2 Set up cluster nodes

To set up a clustered environment you install the first node as described in Install and set up the Sophos Mobile Control server (page 9). Clustering itself is then activated using the **Configuration Wizard**.

For all other nodes, the database created during installation of the first node has to be selected and clustering has to be activated.

Note: It is also possible to configure an existing SMC server for clustering and to extend the environment by adding additional nodes.

6.2.1 Set up the first node

1. Install Sophos Mobile Control as described in Install and set up the Sophos Mobile Control server (page 9) and write down the name of the database you created. Specify this database when installing further nodes.
2. At the end of the installation deselect the **Start Sophos Mobile Control server now** option in the **Sophos Mobile Control - Installation finished** dialog.

   Note: If the SMC service has already been started it will automatically be stopped and restarted during the configuration described later in this section. Alternatively, you can manually stop the service from the menu of the Sophos Mobile Control system tray icon.

3. On the server, click **Start**, go to **Sophos Mobile Control** and click **Configuration Wizard**.

4. The **Welcome** page of the Sophos Mobile Control Configuration Wizard is displayed. Click **Next**.
5. On the **Database Selection** page, select **Skip database configuration** and click **Next**.
6. On the **Choose configuration steps** page, select **Configure cluster support** and click **Next**.
7. On the **Cluster Configuration** page, use the drop-down list of available network interfaces to select the interface that will be used for multicast communication between the server node that you are about to set up and the other nodes.
8. Click through the remaining pages of the configuration wizard. Make sure that you click **Yes** when asked to start the SMC service.

   The configuration of the first SMC server node is now complete. Click **Finish** in the **Sophos Mobile Control - Configuration Wizard finished** dialog.

6.2.2 Set up further nodes

1. Start the installation of Sophos Mobile Control as described in Install and set up the Sophos Mobile Control server (page 9).
2. On the **Database selection** page, select the database you created when you installed the first node and click **Next**.

   The **Database configuration** dialog box is displayed. It shows the progress of the configuration process.
3. On the **Database configuration** page, wait until the configuration process has finished, then click **Next**.
4. On the **Choose configuration steps** page, select **Configure cluster support** and click **Next**.
5. On the **Configure server certificate** page, create a self-signed certificate as described in Install and set up the Sophos Mobile Control server (page 9) and click **Next**.
6. On the **Cluster Configuration** page, use the drop-down list of available network interfaces to select the interface of the Sophos Mobile Control server node that you are about to set up, then click **Next**.
7. Click through the remaining pages of the configuration wizard. On the **Sophos Mobile Control - Installation finished** page, select **Start Sophos Mobile Control server now** to start the cluster node that you just configured.

The configuration of the SMC node is now complete. If required, repeat this procedure to configure additional nodes.

6.3 Set up load balancing with Sophos UTM

This topic describes how to set up Sophos UTM as a load balancer for a cluster of Sophos Mobile Control server nodes. For more information on configuring Sophos UTM, see the Sophos UTM documentation.

Note:

- In order to use Sophos UTM for clustering you need a Sophos UTM license with a **Sophos Webserver Protection** subscription.
- As described later in this section, you need to specify a certificate to protect the communication between the managed devices and the virtual web server that you set up in Sophos UTM. For

simplicity, we recommend that you use the same certificate that you used for the Sophos Mobile Control server (see Request an SSL certificate for Sophos Mobile Control (page 8)). If you used a self-signed certificate, it is mandatory that you use that same certificate.

1. Log into Sophos UTM WebAdmin.
2. From the WebAdmin menu section **Webserver Protection**, go to the **Web Application Firewall** > **Real Webservers** tab.
3. Click **New Real Webserver** to create an SMC node.
4. In the **Add Real Webserver** dialog, enter the following settings:
   a) **Name**: Enter a descriptive name for the web server (for example **`SMC node`**).
   b) **Host**: Select or add a host. Select a host by clicking the folder symbol next to the host edit field. Drag a host from the list of available hosts into the **Host** edit field.
      For additional information on how to add a definition, see the topic *Network Definitions* in the UTM Administration Guide.
   c) **Type**: Select **Encrypted (HTTPS)**.

   Click **Save** to save the configuration.

   Repeat the previous step for each Sophos Mobile Control server node.
5. From the WebAdmin menu section **Webserver Protection**, go to the **Certificate Management** > **Certificates** tab.
6. Click **New Certificate** to upload an SSL web server certificate.
7. In the **Add Certificate** dialog, enter the following settings:
   a) **Name**: Enter a descriptive name for the certificate.
   b) **Method**: Select **Upload**.
   c) **File type**: Select **PKCS#12(Cert+CA)**
   d) **Password**: Enter the password for your certificate file.
   e) **File**: Click the folder icon next to the **File** box, select the certificate you want to upload and click **Start Upload**.

   Click **Save** to save the configuration. The certificate is added to the **Certificates** list.
8. From the WebAdmin menu section **Webserver Protection**, go to the **Web Application Firewall** > **Virtual Webservers** tab.
9. Click **New Virtual Webserver** to add a virtual web server for the cluster.
10. In the **Add Virtual Webserver** dialog box, make the following settings:
    a) **Name**: Enter a descriptive name for the virtual web server (for example **`SMC cluster`**).
    b) In the **Interface** list, select the WAN interface over which the cluster should be accessible from outside.
    c) **Type**: Select **Encrypted (HTTPS) & redirect**.
    d) In the **Certificate** list, select the web server's certificate you uploaded beforehand.
    e) **Domains** (only with wildcard certificate, that is a public key certificate that can be used with multiple subdomains): Enter the domains the web server is responsible for, for example **`shop.example.com`**, or use the **Action** icon to import a list of domain names.

Domains must be entered as fully qualified domain names (FQDN).

You can use an asterisk (*) as a wildcard for the domain prefix, for example, **`*.mydomain.com`**. Domains with wildcards are considered as fallback settings: The virtual web server with the wildcard domain entry is only used when no other virtual web server with a more specific domain name is configured.

Example: A client request to **`a.b.c`** will match **`a.b.c`** before **`*.b.c`** before **`*.c`**.

f) **Real Webservers**: Select the SMC nodes you created beforehand.

Important: Do not select a firewall profile.

Click **Save** to save the configuration. The server is added to the **Virtual Webservers** list.

11. Enable the virtual web server.

    The new virtual web server is disabled by default. Click the toggle switch to enable the virtual web server. The toggle switch color should change from gray (disabled) to green (enabled).

12. Go to the **Site Path Routing** tab.
13. In the **Virtual Webservers** list, go to the virtual web server you added and click **Edit**.
14. In the **Edit Site Path Route** dialog box, click **Advanced** and select **Enable sticky session cookie**.

    Click **Save** to save the configuration.

7 Update Sophos Mobile Control

Sophos Mobile Control server installations can be updated directly from versions 6 or 6.1 to 7.

Older versions need to be updated to version 6 beforehand. For details, see the Sophos Mobile Control 6 documentation.

To update your Sophos Mobile Control server installation to version 7, start the Sophos Mobile Control 7 installer and follow the instructions. The installer automatically detects if an existing installation needs to be updated to version 7.

A system property check will be performed before the update starts. If all checks are passed you can proceed with the update. Database and files will be updated automatically without any user interaction. Once the update is complete, the Sophos Mobile Control service will be started again.

Note: If you used Windows Authentication during your initial Sophos Mobile Control server installation the **Start Sophos Mobile Control server now** option is grayed out. You have to start the service manually.

8 Technical reference

8.1 Sophos Mobile Control server features

The core component of the Sophos Mobile Control product is the Sophos Mobile Control server. Its main features include:

- The server is connected to the Internet.
- The server makes it possible to set up a high-availability environment.
- The administrator controls the server using the web interface.
- End users can register their devices by using the Self Service Portal, or get a device from the administrator that has already been prepared for auto-enrollment.
- The managed devices synchronize with the server through HTTPS.
- iOS clients get triggered by the server through APNs, Android clients through GCM. Windows devices use the Windows Notification Service (WNS).
- You can use an existing Microsoft SQL Server or MySQL database to store device and application information. Alternatively, you can let the Sophos Mobile Control installer create a new database using Microsoft SQL Server Express.
- The database can reside on the same or a separate computer. This allows the use of database clusters.
- The server supports multi-tenant setups to allow different customers on the same server.
- Email access is possible through an integrated or a standalone EAS proxy. For the standalone variant, HTTPS access to the SMC server is required.

The Sophos Mobile Control server has been developed for Java EE (Enterprise Edition). It installs and runs in the well-tested industry-standard WildFly application server.

The server may be installed in virtualized environments.

8.2 Sophos Mobile Control web interfaces

8.2.1 Mobile Control administration interface

Sophos Mobile Control is managed through a web interface that is secured by a login and a session mechanism. You can implement password policies. Access control allows different user roles. These roles have different sets of access rights. Each user can be assigned exactly one role.

For further information, see the Sophos Mobile Control administrator help.

8.2.2 Super administrator interface

The super administrator is primarily used to set up and manage customers for device management. The first super administrator account is created during Sophos Mobile Control setup, see Install and set up the Sophos Mobile Control server (page 9).

As a super administrator you log in to the super administrator customer which is also created during Sophos Mobile Control setup. For the super administrator customer, the Sophos Mobile Control console shows a customized view for super administrator tasks.

8.2.3 Self Service Portal

The Self Service Portal is secured by a login, session mechanism and a password policy. The account has to be set up by the Sophos Mobile Control administrator and can be associated with any tenant. The Self Service Portal is designed for end users to register their devices with Sophos Mobile Control. The end users are also allowed to perform tasks for their devices, for example remote lock or remote wipe. The tasks they can perform vary according to device platform and configuration. As an administrator you can configure the Self Service Portal functions available to end users.

For information on how to configure the Self Service Portal for end users, see the Sophos Mobile Control administrator help.

9 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.

10 Legal notices

Last update: 20170315