

# Sophos Mobile Control Installation guide

Product version: 2

Document date: December 2011



# Contents

- 1 Introduction..... 3
- 2 The Sophos Mobile Control server..... 4
- 3 Set up Sophos Mobile Control..... 13
- 4 Updating from Sophos Mobile Control 1.1 ..... 30
- 5 Apple Push Notification service ..... 31
- 6 Technical support ..... 34
- 7 Legal notices ..... 35

# 1 Introduction

Sophos Mobile Control is a web based mobile device management platform for administrating smartphones and mobile devices. It consists of a server and a client component. The server handles the central management of data and devices. The client takes on communication with the server on each end user device and executes the transferred commands.

This document describes the installation steps for the Sophos Mobile Control server (SMC server).

## 1.1 Access data

The access data for the system is saved in a database that can be extended later on. All installation steps have to be executed as an **administrator** of Microsoft Windows Server 2003/2008 or as a user of the relevant group. The database user needs sysadmin rights.

## 1.2 Licenses

To use Sophos Mobile Control you need a valid license. After purchasing the software, you receive a license file named license.sql. It must be placed in the same directory as the setup file during installation.

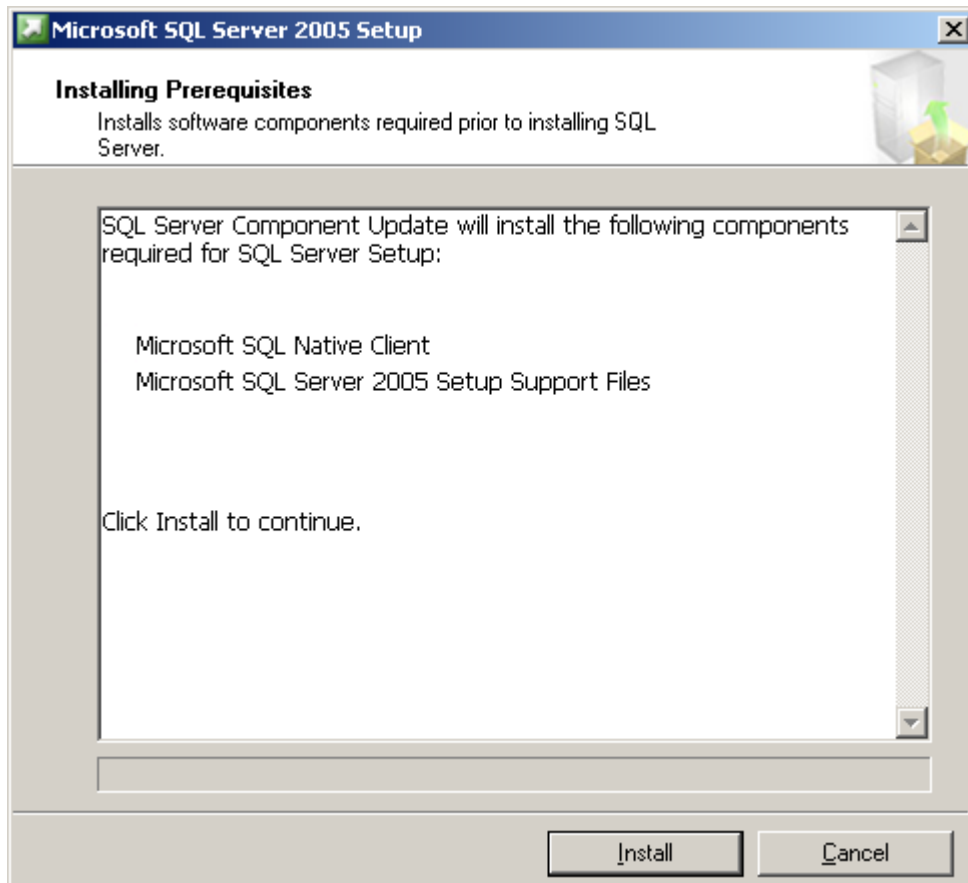
**Note:** If there is no valid license available, the SMC server can be installed, but you cannot register any mobile devices in the Sophos Mobile Control web interface.



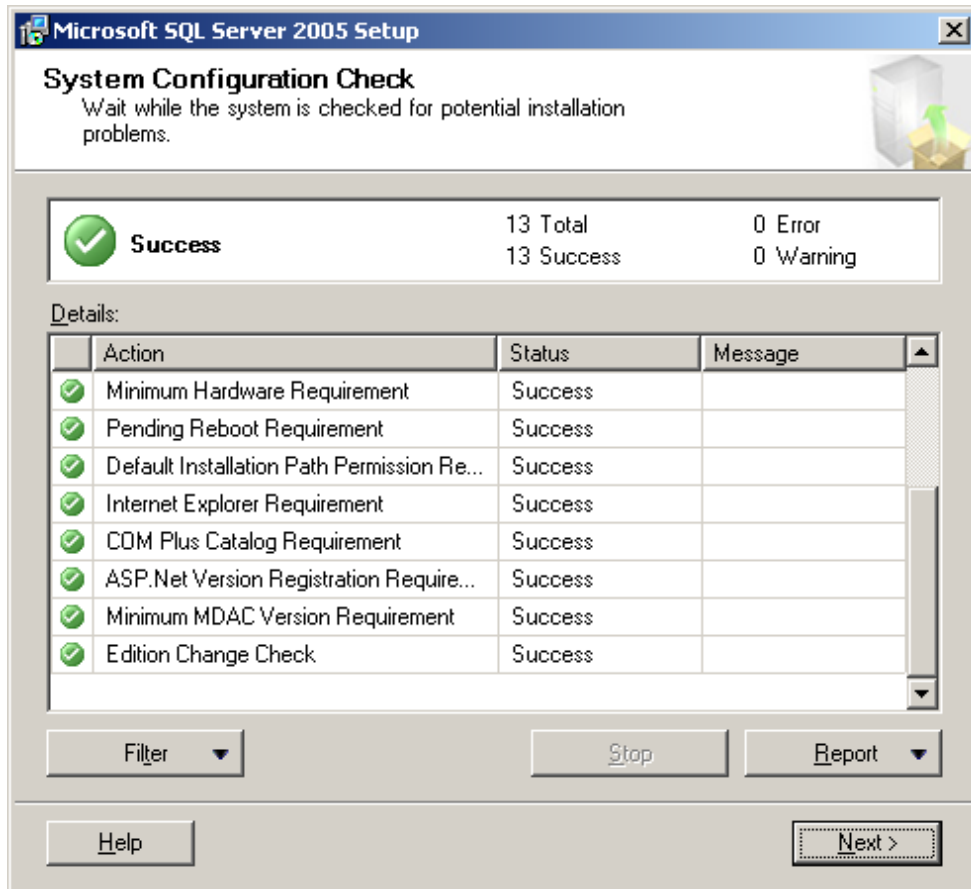
## 2.3 Install the database server Microsoft SQL Server

We recommend Microsoft SQL Server 2005 Express Edition for Windows with installer.

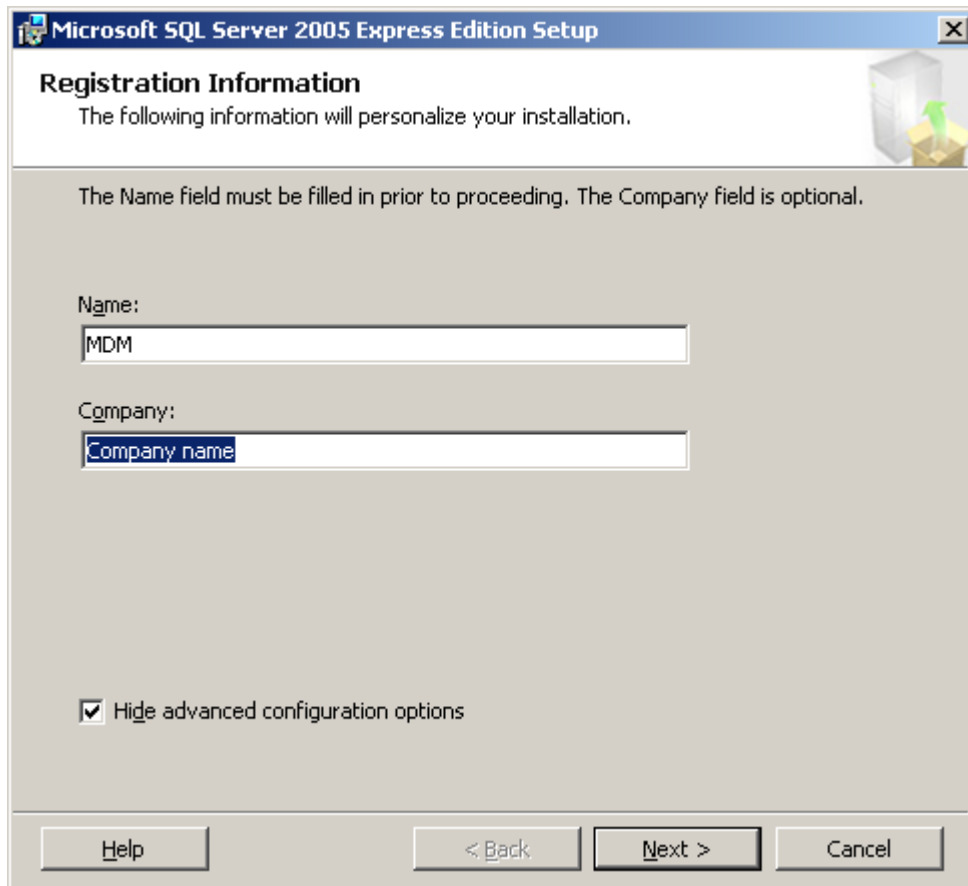
1. Execute the installer, select **I accept the licensing terms and conditions** and click **Next**. The **Installing Prerequisites** dialog is displayed.



2. Click **Install** to install the prerequisites. After installation has finished click **Next** to continue with the Microsoft SQL Server Installation Wizard.

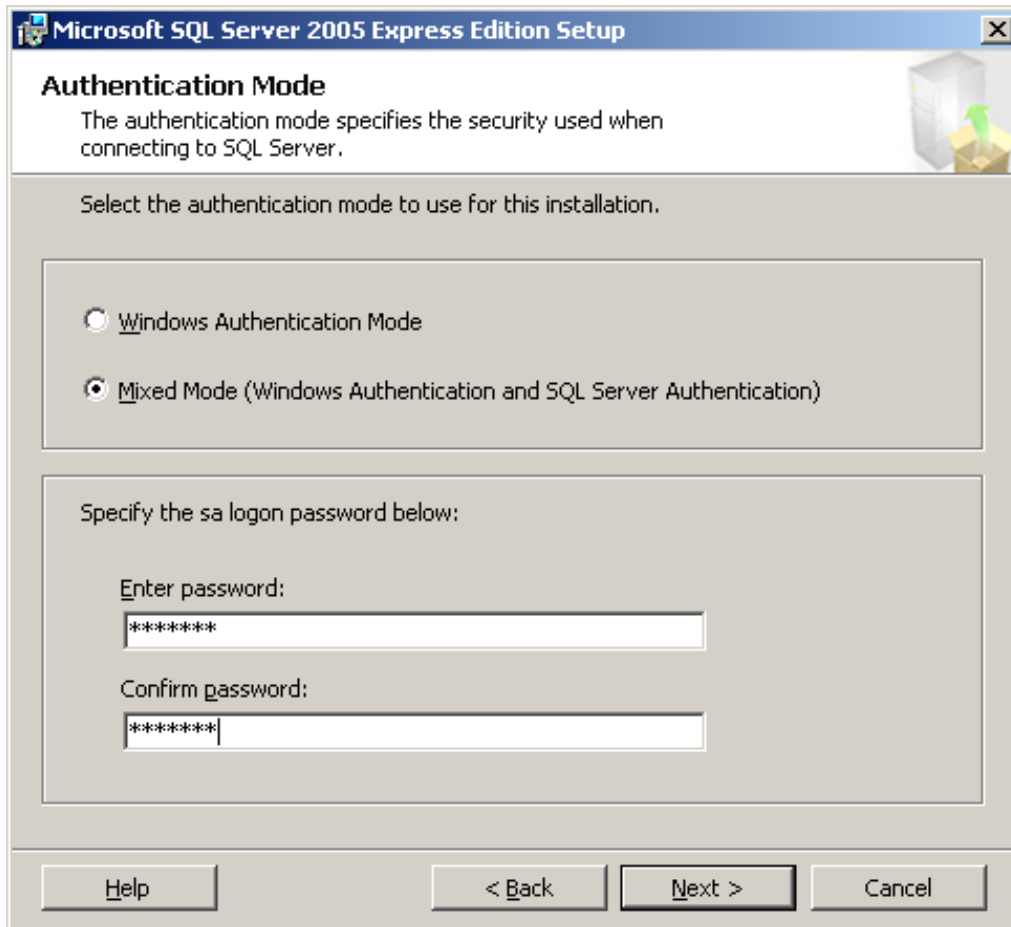


3. Start the Microsoft SQL Server installation. If the **System Configuration Check** was successful, click **Next**.  
The **Registration Information** dialog is displayed.



Enter **Name** and **Company** and click **Next** to continue.

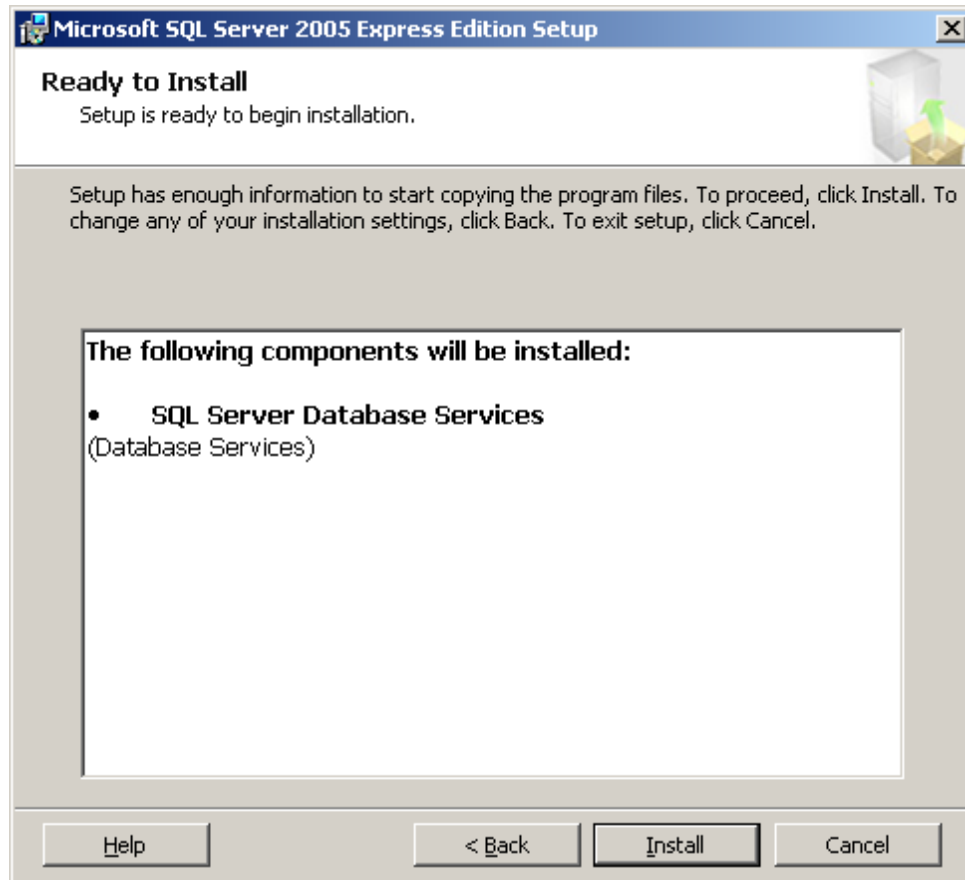
4. In Feature Selection, no changes need to be made. Click Next. The Authentication Mode dialog is displayed.



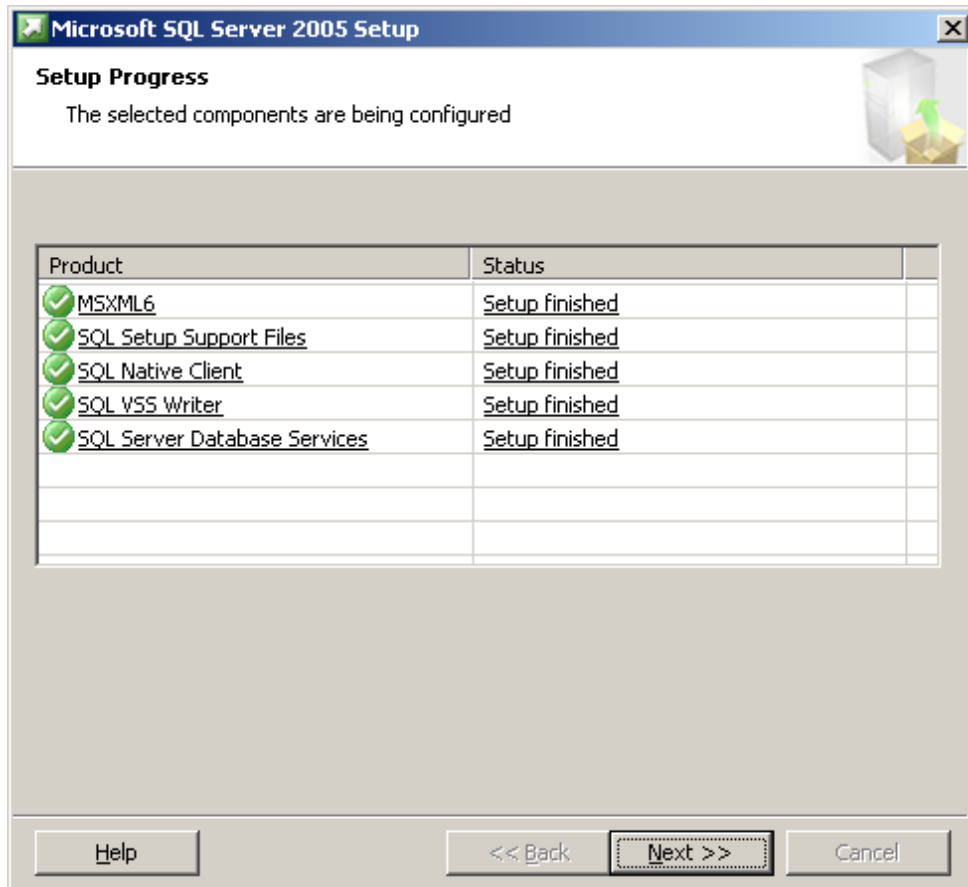
Select the authentication mode and fill in the Enter password and Confirm password fields. Click Next to continue.

**Note:** For the Windows authentication mode, the connecting user must have the SQL logon language set to English.

5. No further changes need to be made. Click the Next button until the Ready to Install dialog is displayed.

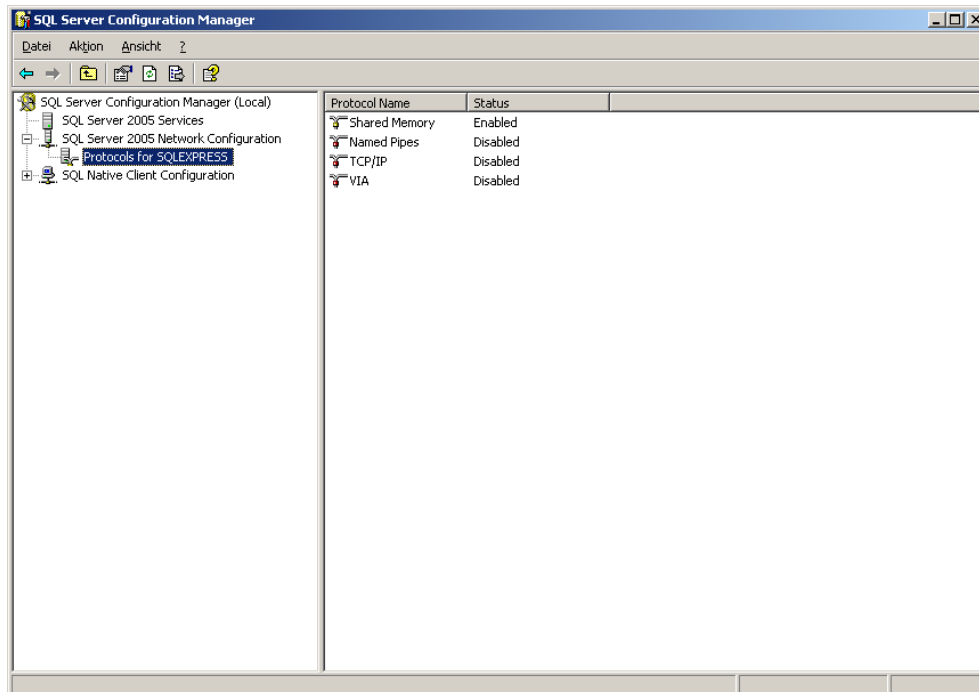


6. Click the **Install** button to start installation.

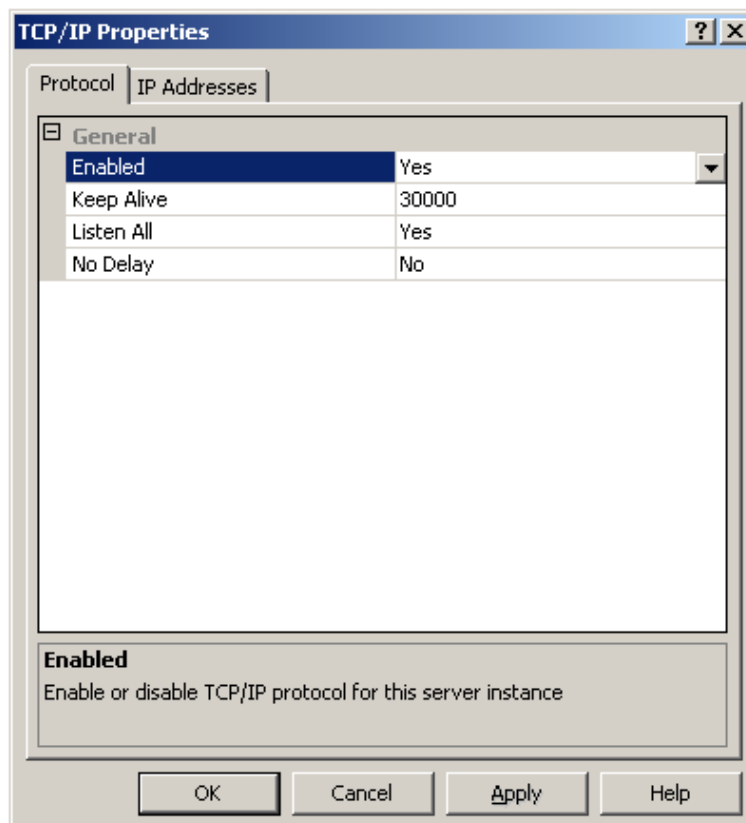


7. If all components were installed correctly, click **Next** and **Finish** to complete installation.

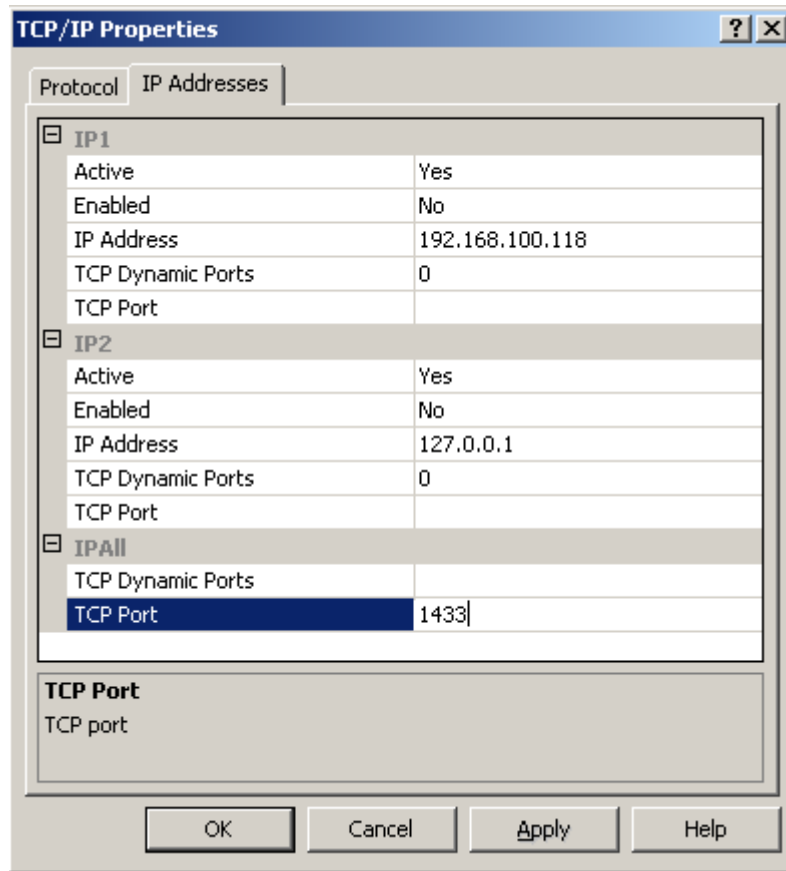
- Before Sophos Mobile Control can be installed, the TCP/IP Protocol for the SQL Server needs to be enabled and the TCP port needs to be set to 1433. Open the **Start Menu** and select **All Programs > Microsoft SQL Server 2005 > Configuration Tools** and click **SQL Server Configuration Manager**.



- Go to **Protocols for SQLEXPRESS** and double-click **TCP/IP**. The **TCP/IP Properties** dialog is displayed.



10. In the **Protocol** tab, set **Enabled** to **Yes** and click the **IP Addresses** tab.



11. Click **TCP Dynamic Ports** and make sure that the field is empty to disable this function. Now click **TCP Port**, enter **1433** and click **OK** to apply your settings.
12. For the new settings to take effect, the server needs to be restarted. Click **SQL Server 2005 Services**, right-click **SQL Server (SQLEXPRESS)** and select **Restart**.

## 3 Set up Sophos Mobile Control

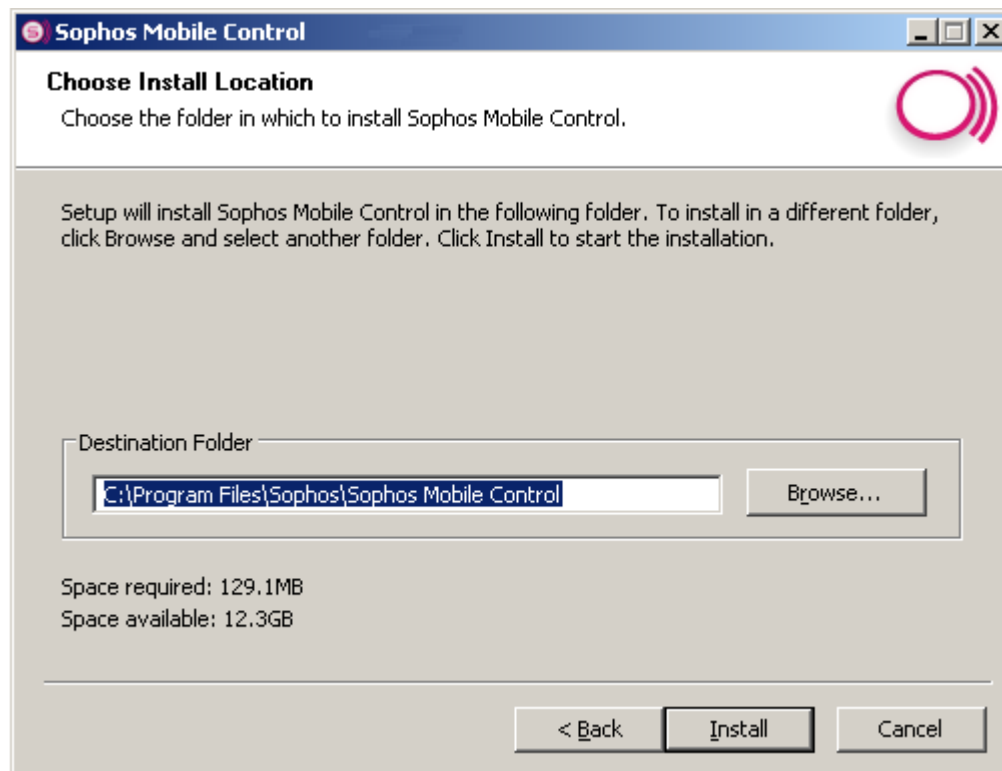
The key steps are:

- Execute the Sophos Mobile Control Installer
- Carry out the configuration steps in the Sophos Mobile Control Configuration Wizard
- Create a customer in the Sophos Mobile Control Customer Wizard

### 3.1 Install and configure Sophos Mobile Control

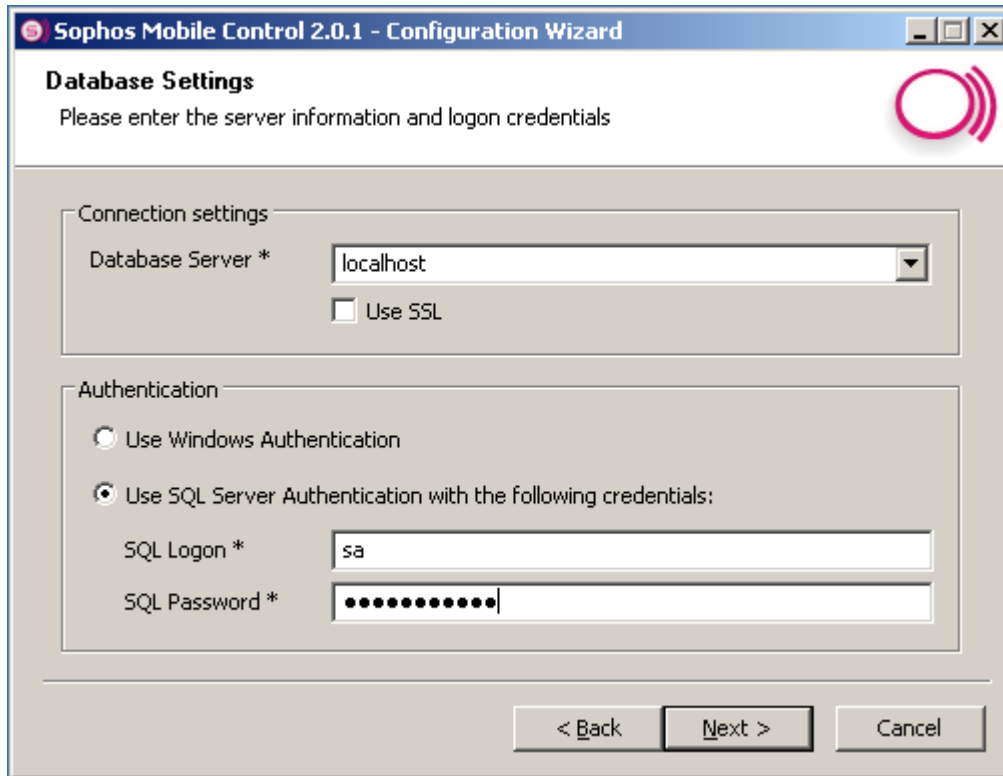
**Prerequisite:** Before you execute the Sophos Mobile Control installer, put the license file `license.sql` for the operation of the SMC server in the directory where the setup file is located. You can generate self-signed certificates during setup.

1. Execute the Sophos Mobile Control installer, review and agree to the **License Agreement**. The **Choose Install Location** dialog is displayed.



Choose the destination folder and click **Install** to start installation.

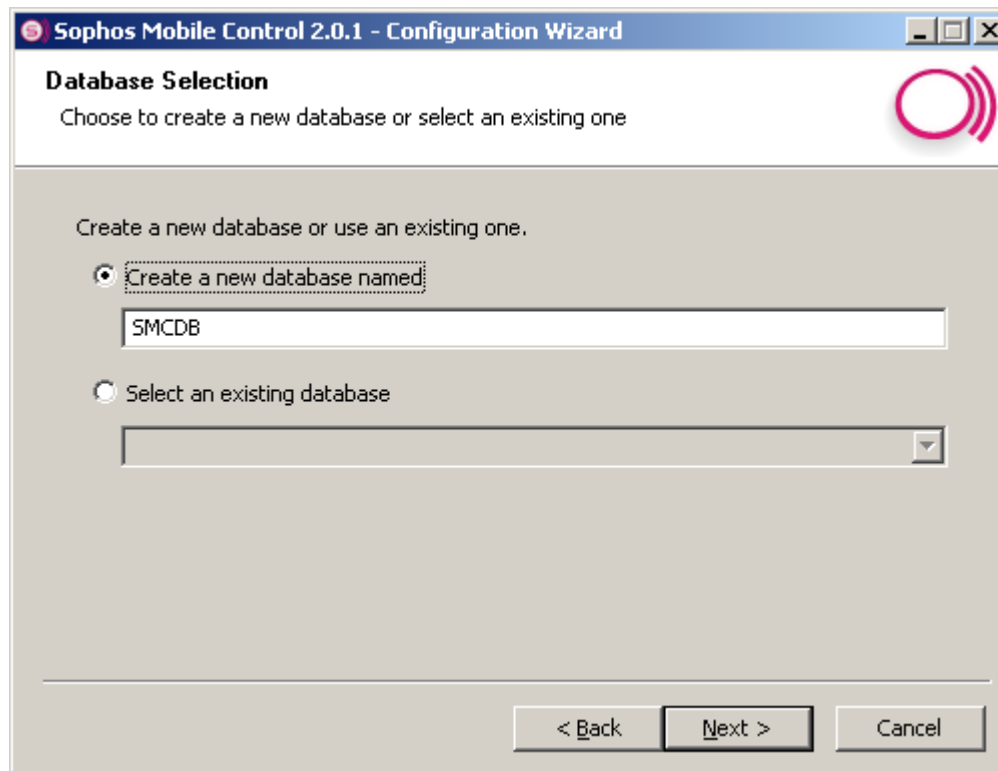
2. During setup, the **Sophos Mobile Control Configuration Wizard** is displayed. Select **Use Microsoft SQL Server** as database and click **Next**.  
In the next step, you specify server information and logon credentials



3. Select **Use Windows Authentication** to use your Windows user credentials for the SQL Server connection.

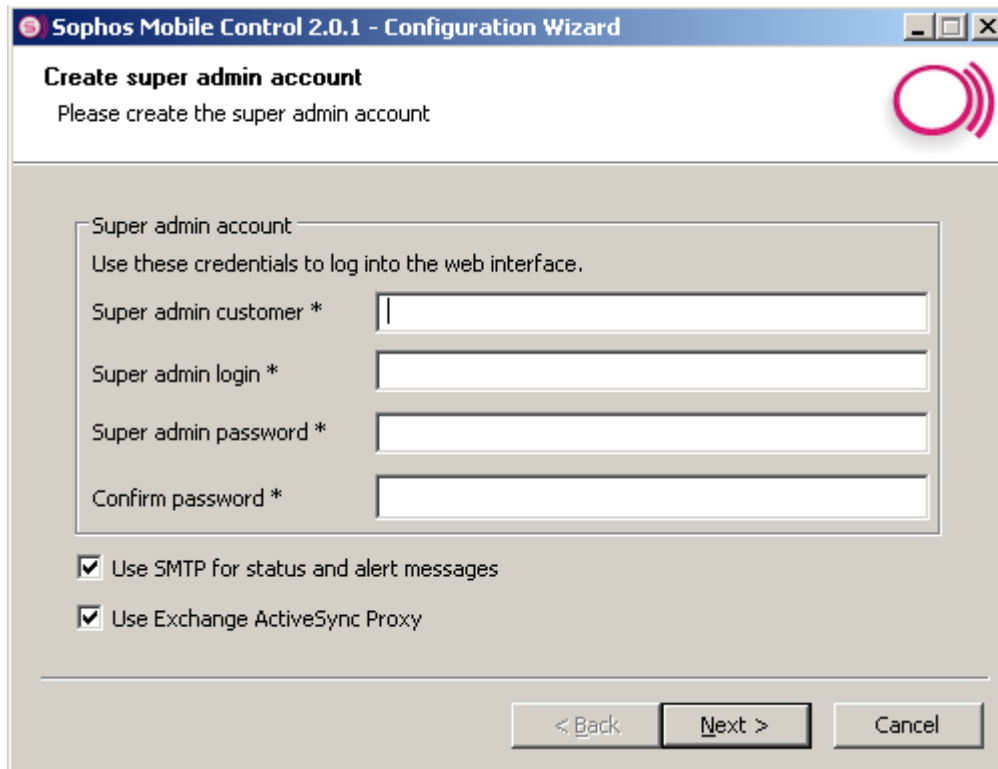
To use the user credentials specified during SQL server installation, select **Use SQL Server Authentication with the following credentials** and enter the required user name and password. Click **Next** to continue.

- In the next step, you select the database.



- Select **Create a new database named**, enter a name (for example SMCDB) and click **Next**. The dialog **Database Configuration** is displayed. It shows the relevant progress messages.

6. After the database has been successfully created and populated, click **Next**. In the next step, you create the super administrator account to be used.



The screenshot shows a Windows-style dialog box titled "Sophos Mobile Control 2.0.1 - Configuration Wizard". The main heading is "Create super admin account" with the instruction "Please create the super admin account". The dialog contains a section titled "Super admin account" with the text "Use these credentials to log into the web interface." Below this are four text input fields: "Super admin customer \*", "Super admin login \*", "Super admin password \*", and "Confirm password \*". At the bottom of the dialog, there are two checked checkboxes: "Use SMTP for status and alert messages" and "Use Exchange ActiveSync Proxy". At the very bottom, there are three buttons: "< Back", "Next >", and "Cancel".

The super administrator you create in this dialog can manage all customers created at a later stage and define template rules for new customers. In addition, the super administrator can export a list of all managed devices for all customers.

7. Enter **Super admin customer**, **Super admin login** and password information and click **Next**.

**Note:** These credentials are needed to log on to the web interface.

**Note:** The super admin should not be used in productive operation.

- In the next step, you can enter SMTP information and logon credentials. This step is optional.

**Sophos Mobile Control 2.0.1 - Configuration Wizard**

### Configure SMTP

Enter the SMTP server information and logon credentials

Enter SMTP server information

SMTP Host \*

SMTP User

SMTP Password

Enter Sophos Mobile Control server email information

Email Originator \*

Email Recipient(s) \*

Use ; to separate recipients

< Back   Next >   Cancel

Enter the SMTP information and click Next.

- After confirming the successful test and configuration of the SMTP, you can configure the Exchange Active Sync (EAS) Proxy information. This step is optional.

**Sophos Mobile Control 2.0.1 - Configuration Wizard**

### EAS-Proxy Setup

Please enter the EAS-Proxy configuration

ActiveSync enabled Exchange Server name or IP address (without http:// or https://) \*

Use SSL

Default mail access for new devices under management

Compliance check controlled email access

Allow email access

Deny email access

< Back   Next >   Cancel

Enter the relevant EAS-Proxy information and select **Use SSL**. Under **Default mail access for new devices under management**, specify how email access should be checked and handled:

- Select **Compliance check controlled email access** for an ongoing automatic check if devices comply with your corporate rules for mobile access. If devices are not compliant, further email access through EAS proxy may be denied depending on the compliance settings specified in the Sophos Mobile Control web interface.
- Select **Allow email access** if all new managed devices are to be granted email access through EAS proxy. The administrator has to deny access individually.
- Select **Deny email access** to deny new managed devices email access through EAS proxy. The administrator has to grant access individually.

Click Next.

- In the next step, you configure the compliance check. This step is optional.

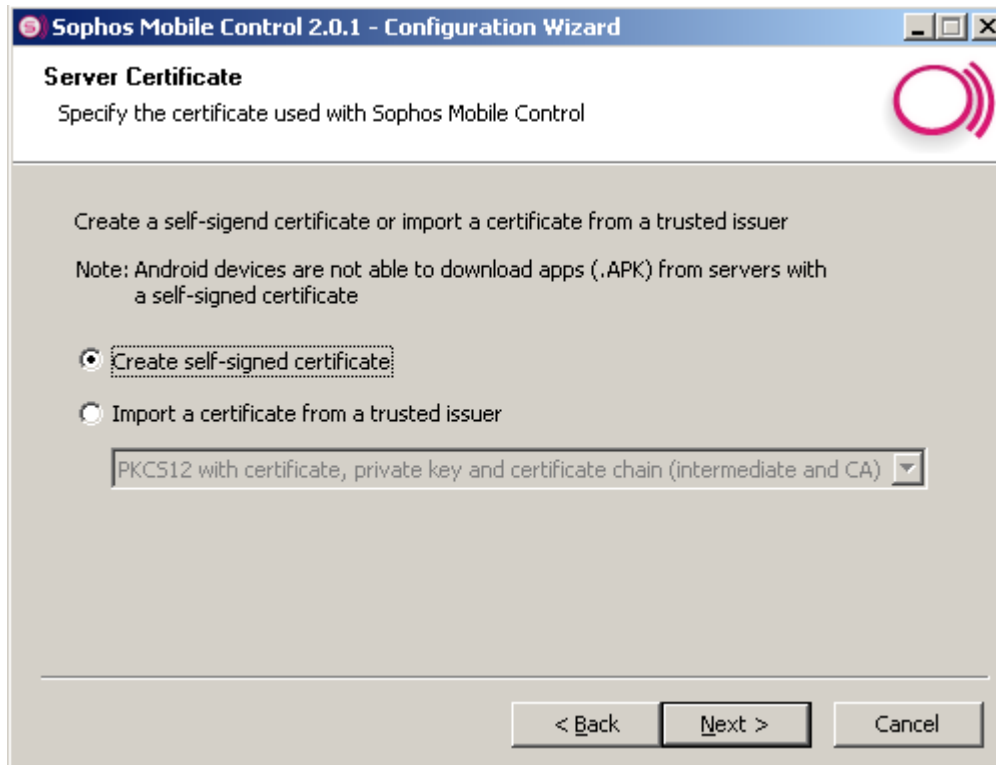
The screenshot shows a configuration wizard window for Sophos Mobile Control 2.0.1. The window title is "Sophos Mobile Control 2.0.1 - Configuration Wizard". The main heading is "Sophos Mobile Control - Configuration Wizard" and the instruction is "Please enter the compliance check information". Below this, there is a section titled "Enter compliance check configuration". It contains two input fields: "Compliance check interval (in minutes) \*" with the value "30" and "Device sync interval (in minutes) \*" with the value "1440". At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel".

For compliance check, you can configure the following:

- In the **Compliance check interval (in minutes)** field, enter the time interval in which the check is to be performed.
- In the **Device sync interval (in minutes)** field, enter the time interval after which the device synchronizes with the server.  
**Note:** The value you set in this field only applies to iOS devices. For Android and Windows Mobile devices a default of 24 hours applies. To define a different interval for these device types, use the command package Set MDM Sync Interval (in minutes).

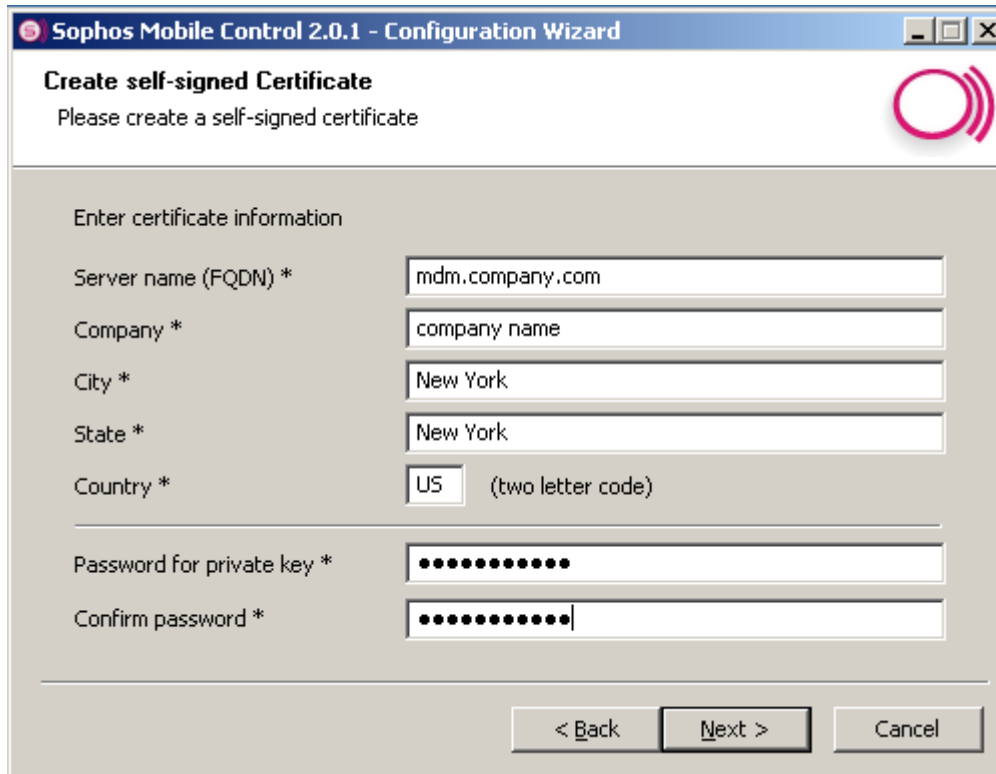
Click Next.

11. In the next step, certificates for HTTPS need to be created or imported.



- If you do not have a trusted certificate yet, select **Create self signed certificate**, click **Next** and continue with step 12.
- If you have a trusted certificate, click **Import a certificate from a trusted issuer**, select **PKCS12 with certificate, private key and certificate chain (intermediate and CA)** from the dropdown list, click **Next** and continue with step 13. You can also select **Separate files for certificate, private key, intermediate and CA** from the dropdown list, click **Next** and continue with step 14.

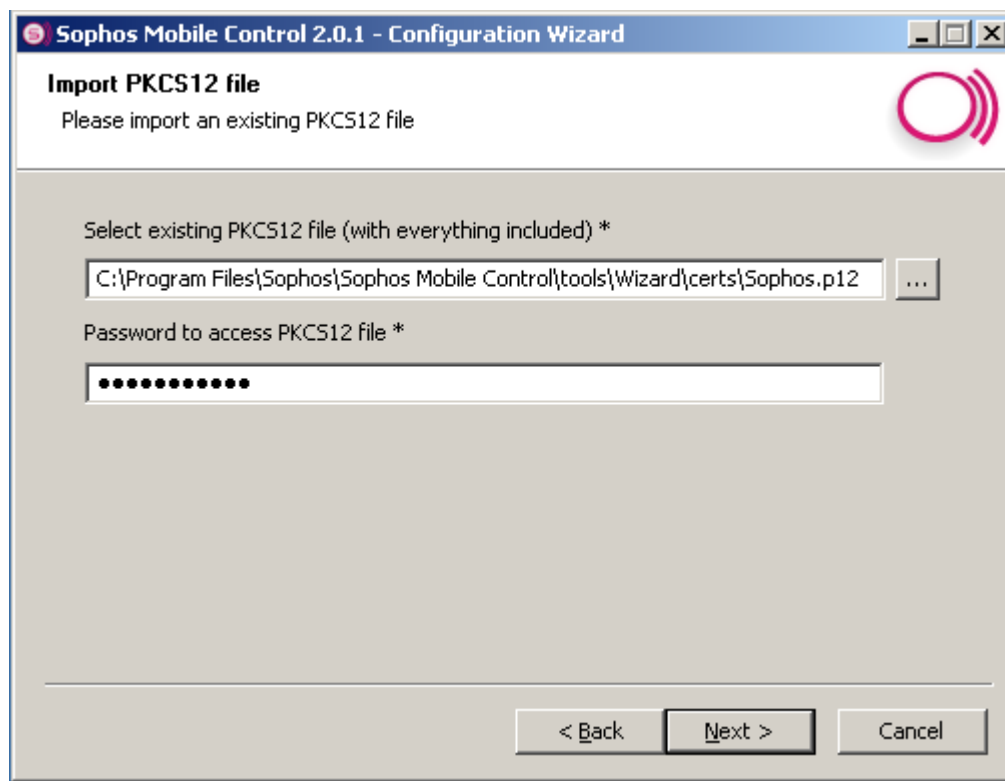
12. If you have selected **Create self signed Certificate**, the following dialog is shown. Enter the appropriate certificate information.



The screenshot shows a Windows-style dialog box titled "Sophos Mobile Control 2.0.1 - Configuration Wizard". The main heading is "Create self-signed Certificate" with the instruction "Please create a self-signed certificate". The dialog is divided into two sections. The first section, "Enter certificate information", contains several text input fields: "Server name (FQDN) \*" with the value "mdm.company.com", "Company \*" with "company name", "City \*" with "New York", "State \*" with "New York", and "Country \*" with "US" and a note "(two letter code)". The second section contains two password fields: "Password for private key \*" and "Confirm password \*", both filled with masked characters. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

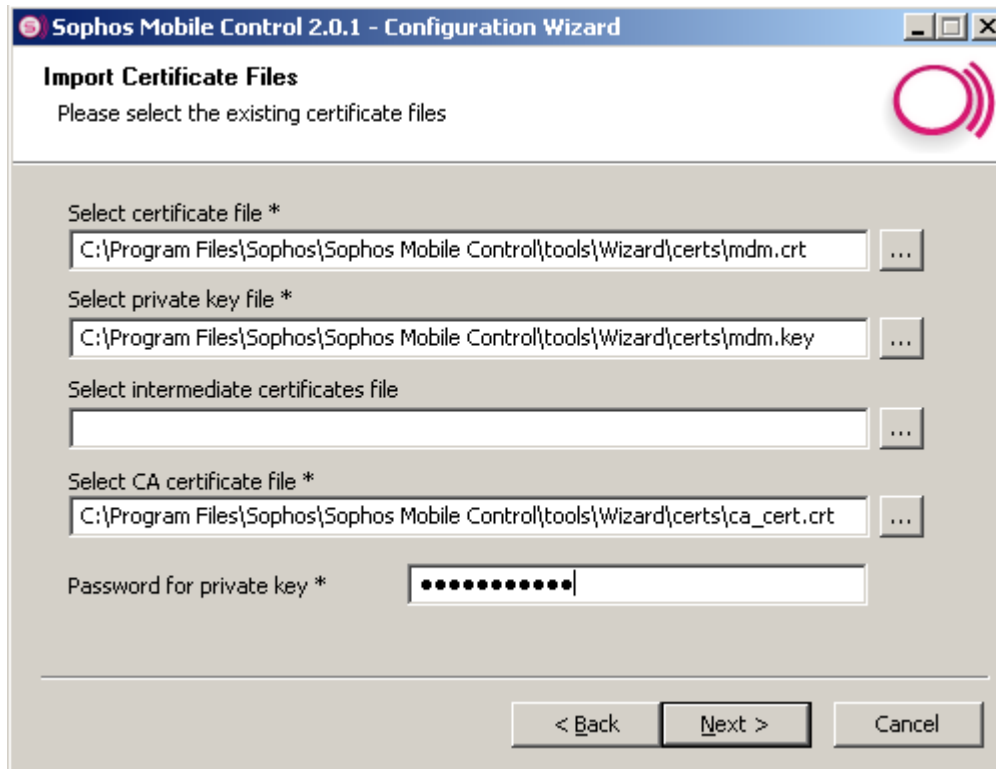
After you have entered all necessary information click Next to review and confirm the creation.

13. If you have selected PKCS12 with certificate, private key and certificate chain (intermediate and CA) under **Import a certificate from a trusted issuer**, the following dialog is shown. Select the appropriate file and enter a password.



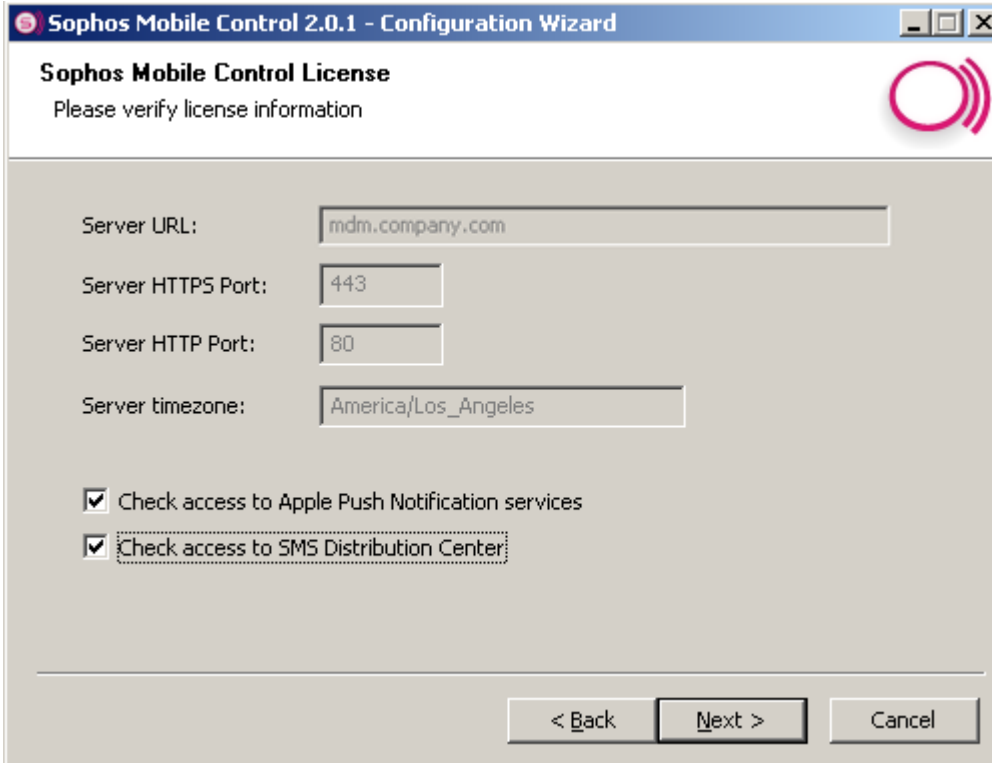
Click Next to review and confirm the import.

14. If you have selected **Separate files for certificate, private key, intermediate and CA** under **Import a certificate from a trusted issuer**, the following dialog is shown. Select the appropriate files and enter a password.



Click **Next** to review and confirm the import.

15. In the next step, you verify license information.



The screenshot shows the 'Sophos Mobile Control License' window of the configuration wizard. The title bar reads 'Sophos Mobile Control 2.0.1 - Configuration Wizard'. The main heading is 'Sophos Mobile Control License' with the instruction 'Please verify license information'. The window contains the following fields and options:

- Server URL:
- Server HTTPS Port:
- Server HTTP Port:
- Server timezone:
- Check access to Apple Push Notification services
- Check access to SMS Distribution Center

At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Select the check boxes displayed and click Next to confirm the licensing, configuration process and the access checks.

16. Configuration is now complete.



The screenshot shows the 'Sophos Mobile Control - Configuration Wizard finished' window. The title bar reads 'Sophos Mobile Control 2.0.1 - Configuration Wizard'. The window features the Sophos logo on the left and the following text:

**Sophos Mobile Control - Configuration Wizard finished**

The Sophos Mobile Control server has been successfully configured and licensed.  
Click Finish to close Wizard

At the bottom, there are three buttons: '< Back', 'Finish', and 'Cancel'.

Click **Finish** to close the **Configuration Wizard**.

In the **Configuration Wizard**, you have now created a template customer and an admin user (super administrator). This setup does not support the LDAP connection to a directory service such as Active Directory and the self-registration of end users with the Self Service Portal.

In the next step, you create a customer in the **Customer Wizard** to support these features.

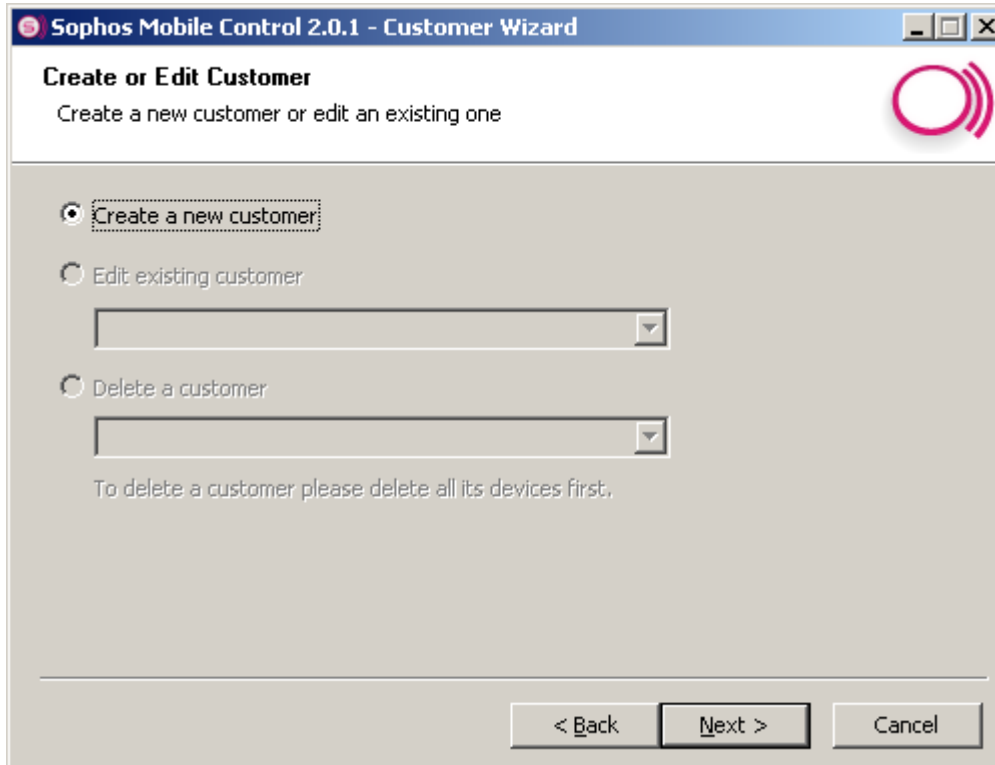
## 3.2 Create a customer

1. In the next setup step, the Sophos Mobile Control Customer Wizard is displayed.

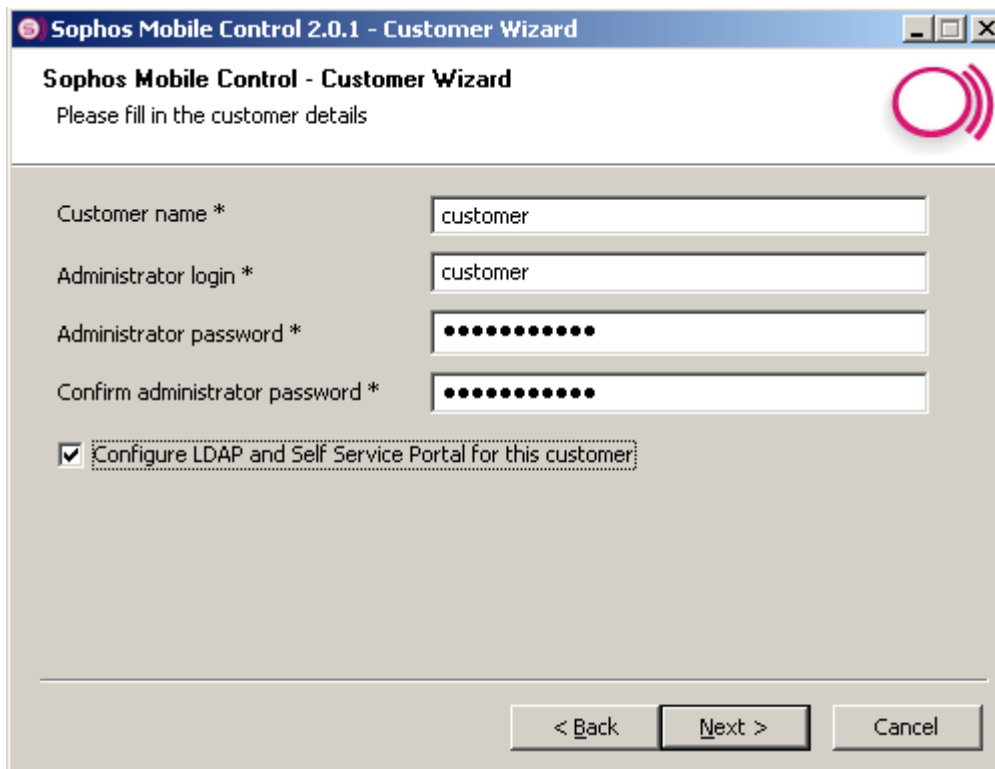


Click Next.

2. Make sure that **Create a new customer** is selected and click **Next**.

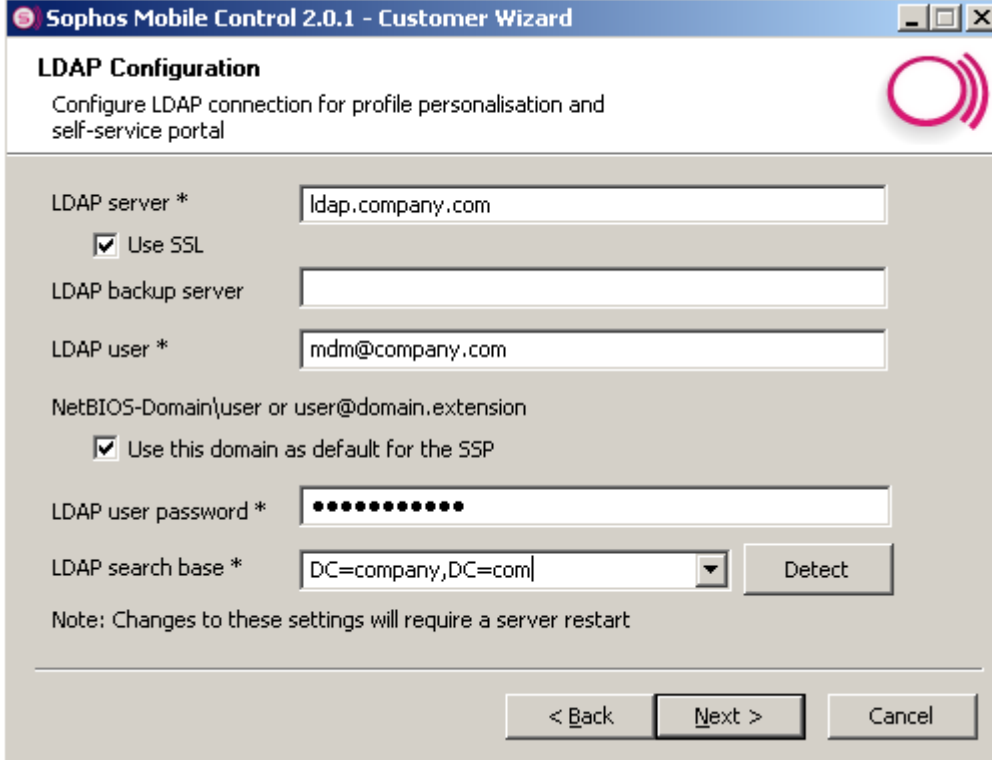


3. In the next step, you fill in the customer details. Enter a **Customer name**, **Administrator name** and password information. Select **Configure LDAP and Self Service Portal** for this customer if you want to use a directory service with the Self Service Portal.



If you have selected **Configure LDAP and Self Service Portal for this customer**, click **Next** and continue with step 4. Otherwise click **Next** to complete the customer setup.

4. Enter the relevant **LDAP server** and **LDAP user** information and click **Detect** to detect the LDAP search base automatically. Afterwards, click **Next** to continue.



The screenshot shows the 'LDAP Configuration' window in the Sophos Mobile Control 2.0.1 - Customer Wizard. The window title is 'Sophos Mobile Control 2.0.1 - Customer Wizard'. The main heading is 'LDAP Configuration' with a sub-heading 'Configure LDAP connection for profile personalisation and self-service portal'. The window contains several input fields and checkboxes:

- LDAP server \***: ldap.company.com
- Use SSL**
- LDAP backup server**: (empty)
- LDAP user \***: mdm@company.com
- NetBIOS-Domain\user or user@domain.extension**: (empty)
- Use this domain as default for the SSP**
- LDAP user password \***: (masked with dots)
- LDAP search base \***: DC=company,DC=com (with a dropdown arrow)
- Detect** button

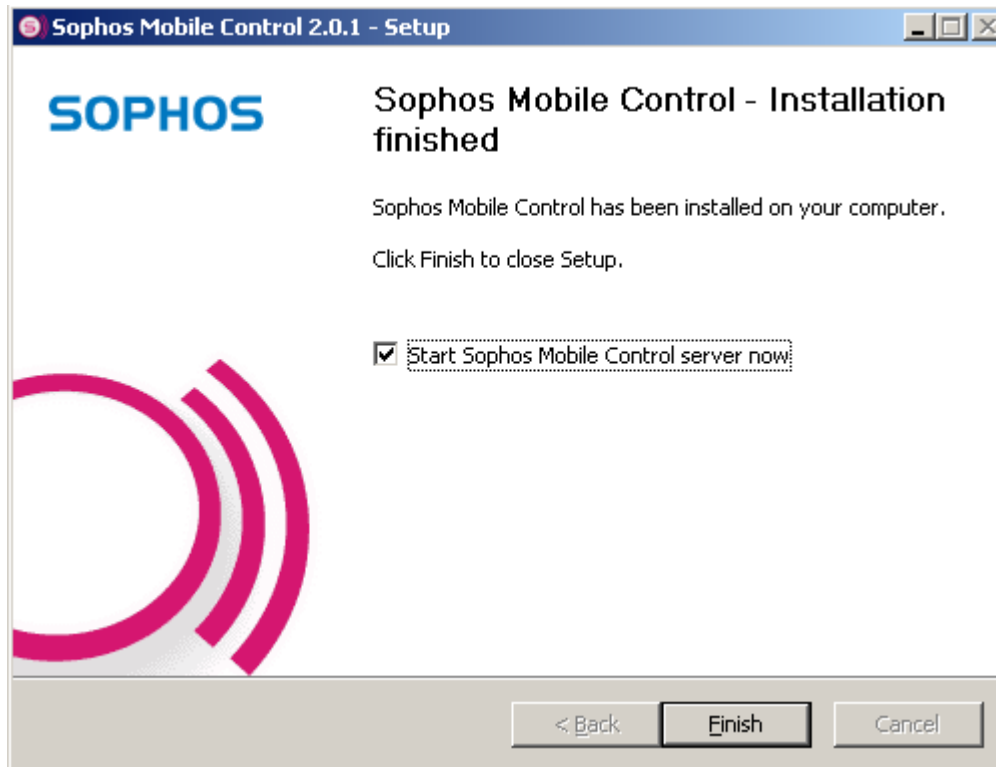
Note: Changes to these settings will require a server restart

At the bottom, there are three buttons: < Back, Next >, and Cancel.

- Customer setup is complete.  
Click **Finish** to close the Customer Wizard.



- Click **Finish** to complete the Sophos Mobile Control Setup.



7. Click **Finish** to complete the installation and start Sophos Mobile Control for the first time.

If you have selected SQL server authentication under during installation, the SMCSVC service is started automatically and the Sophos Mobile Control server is executed. If you have selected Windows authentication, you first have to enter logon details in the service and start it afterwards.

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

**Note:** If a different language than English is used for the SQL login, an error occurs and an error message is displayed. To solve this problem, first stop the SMCSVC service. Then open SQL Management Studio on the server, set the language used for login to English and start the SMCSVC service again.

## 4 Updating from Sophos Mobile Control 1.1

To update your SMC Server installation from version 1.1 to version 2.0, execute the Sophos Mobile Control 2.0 installer.

The installer automatically detects that an existing installation is to be updated to version 2.0. The basic process is the same as for new installations (see [Set up Sophos Mobile Control](#), page 13). A number of configuration settings from the old versions are maintained.

For security reasons, you are prompted to enter the passwords you have defined during first-time installation. In addition, you have to reenter some configuration settings. You can also define settings for new functionality in version 2.0.

## 5 Apple Push Notification service

To use the built-in Mobile Device Management (MDM) protocol of devices running Apple iOS 4 (or higher), Sophos Mobile Control must use Apple's Push Notification service (APNs) to trigger the iOS devices. 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.

**Note:** Please do NOT use the Internet Explorer for any Apple websites. Apple recommends their own Safari browser, but Mozilla Firefox, Opera or Google Chrome also work.

### 5.1 Requirements

Apple requires all device management customers to register with the iOS Developer Enterprise Program to generate their own Apple Push Notification service (APNs) certificate.

**Note:** This is not the Apple Developer Program.

For the registration, you need a DUNS number (Data Universal Numbering System from Dun & Bradstreet (D&B)).

- To register, follow the steps on the Apple website:  
<http://developer.apple.com/programs/ios/enterprise>
- Usually, your request will be checked by Apple within five working days.

For silent operations, all devices must have at least iOS version 4 installed. A free update is available from Apple for

- iPhone 3G, 3GS, 4
- iPad
- iPod touch 3rd or 4th generation

To notify iOS devices, the Sophos Mobile Control server needs to connect to the Apple Push Notification service. The notifications are sent SSL-encrypted to

- gateway.push.apple.com:2195 TCP (17.0.0.0/8)

iOS devices with Wifi only need a connection to the APNs

- Wifi iOS device → \*.push.apple.com:5223 TCP (17.0.0.0/8)

## 5.2 Creating a certificate for APNs

Once you are an official member of the iOS Developer Enterprise Program, you can create the APNs certificate for Sophos Mobile Control.

### 5.2.1 Generate a certification signing request

In the Tools folder located in the Sophos Mobile Control installation directory (for example C:\Program Files\Sophos\Mobile Control), you find the subfolder CreateAPNsCert. Open it and double-click the batch file step1\_create\_csr.bat. You must enter some required information, for example your country, company name and E-mail address.

Afterwards the files APNsCertificateSigningRequest.csr and ApnsPrivateKey.key are created automatically. You will need them later.

**Note:** Back up the file ApnsPrivateKey.key. You will need it for certificate renewal.

### 5.2.2 Create an App ID for your Sophos Mobile Control server

1. To log in to the Apple Member Center, open <http://developer.apple.com/membercenter> and log in with your Apple ID for the iOS Developer Enterprise Program.
2. Navigate to iOS Provisioning Portal, App ID.
3. Create a new App ID:
  - Description → Sophos Mobile Control Server App
  - Bundle Seed ID (App ID Prefix) → Generate new
  - Bundle Identifier (App ID Suffix) → com.apple.mgmt.sophos.mobile.control.<companyname>  
**Note:** The identifier must start with com.apple.mgmt.sophos.mobile.control.
  - Submit

### 5.2.3 Create certificate for Sophos Mobile Control

1. In the **App ID** section, locate the App ID for **Sophos Mobile Control Server App** and click **Configure**.
2. Select the **Enable for Apple Push Notification service** check box.
3. Click the **Configure** button for **Production Push SSL Certificate**.
4. In the assistant, press **Continue**.
5. Upload the certificate signing request file **APNsCertificateSigningRequest.csr** and press **Generate**.
6. Download the generated certificate to the **CreateAPNsCert** folder and close the assistant. It must be called **aps\_production\_identity.cer**.
7. Now run **step2\_convert\_pkcs12.bat** and enter a password for your certificate file. Remember the password as you will need it to upload the file to Sophos Mobile Control. Two files are created automatically:
  - **aps\_production\_identity.pem**
  - **Sophos Mobile Control\_apns\_certificate.pkcs12** (this will be uploaded to Sophos Mobile Control)

### 5.2.4 Upload the APNs certificate to Sophos Mobile Control

1. Log in to the Sophos Mobile Control web GUI as a user with administrator role.
2. Go to the **Settings** dialog.
3. Select the file **Sophos Mobile Control\_apns\_certificate.pkcs12**, enter the certificate password and press **Upload**.
4. To save your changed settings, click **Save**.

Now your Sophos Mobile Control server is able to trigger iOS devices with push notifications and you can use the built-in MDM protocol.

## 6 Technical support

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

- Visit the SophosTalk forum at <http://community.sophos.com/> and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at <http://www.sophos.com/support/>.
- Download the product documentation at <http://www.sophos.com/support/docs/>.
- Send an email to [support@sophos.com](mailto:support@sophos.com), including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

## **7 Legal notices**

Copyright © 2011 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.

Powered by DIALOGS Software GmbH