SOPHOS

Cybersecurity made simple.

# SafeGuard Enterprise for Mac user help

product version: 8.3

# Contents

# 1 About SafeGuard Enterprise for Mac

Sophos SafeGuard runs on Macs to protect them. It has two parts:

- SafeGuard Native Device Encryption (page 1) protects your computer with the help of FileVault encryption technology.
- SafeGuard File Encryption (page 1) lets you encrypt files with a key or password.

You may not have all the features described in this Help. This depends on your license and the policies you received from your security officer.

Sophos SafeGuard is configured and managed centrally from the Sophos SafeGuard Management Center. For more information on managing Sophos Safeguard Enterprise, see the documentation page.

To access general information on your installation of Sophos SafeGuard, click the Sophos SafeGuard icon in the system menu and open the Sophos SafeGuard preference pane (page 5).

The most important options for encrypting and decrypting files are available in a right-click menu in the Finder.

**Important**
Before you update your operating system, make sure that your version of Sophos SafeGuard supports the newest version of the operating system, see SafeGuard Enterprise release notes. If you update your operating system first, you may lose access to your data.

## 1.1 SafeGuard Native Device Encryption

Sophos SafeGuard Native Device Encryption builds on the FileVault disk encryption technology included in your operating system. It encrypts the entire hard disk, so that your data is safe even if the computer is lost or stolen.

SafeGuard Native Device Encryption works in the background. You will not see any prompts for encryption or decryption when opening, editing, and saving files.

To view details about your installation, open the Disk Encryption tab (page 7) in the Sophos SafeGuard preference pane.

SafeGuard Native Device Encryption allows you to:

- Encrypt a computer (page 8)
- Decrypt a computer (page 8)
- SafeGuard Native Device Encryption and SafeGuard File Encryption (page 9)
- Check your connection to the SafeGuard Enterprise Server (page 14)

## 1.2 SafeGuard File Encryption

SafeGuard File Encryption allows your security officer to define which files on your computer are encrypted and who can read them. There are two ways of defining which files are encrypted:

- Location-based file encryption (page 3)
- Application-based file encryption (page 3)

File Encryption policies are assigned to users, not to computers. Typically, File Encryption policies specify that files in your user folders such as **Documents** are encrypted. However, your security officer may specify folders, where files remain unencrypted. To find out which locations on your computer are encrypted, see the Policies tab (page 6) in the preference pane.

In Finder, encrypted files are marked with a green lock symbol. Files with no symbol are usually unencrypted.

**Note**
Files that have been saved as bundles or packages may not display an overlay icon even though they are encrypted. For example, when you insert an encrypted image file into an encrypted text file in TextEdit and save it as a Rich Text Document with Attachments, the resulting file appears to be unencrypted. It is encrypted, nevertheless.

After the encryption software has been installed and the communication with the SafeGuard Enterprise server has been established, you are requested to enter your macOS password. Moreover, you need a personal certificate. This certificate is generated on the SafeGuard Enterprise server when you enter the password. This is only required after product installation, first login, or password reset.

Once SafeGuard File Encryption is installed, make sure you enforce all policies your security officer assigned to you, see Encrypt files according to policy (page 10).

SafeGuard File Encryption allows you to:

- Encrypt files according to policy (page 10)
- Encrypt/Decrypt files manually (page 10)
- Send encrypted files via email (page 11)
- Use a password to protect a file (page 11)
- Encrypt files on removable devices (page 12)
- Recover encrypted files (page 14)

## User consent on macOS 10.14

From macOS 10.14, applications need user consent before they can control other applications. After installation, macOS shows a message **"Sophos SafeGuard" wants access to control "Finder"**, prompting you to allow or deny. Click **OK** because the Finder functionality is necessary for SafeGuard File Encryption to work properly.

This adds an entry in the **Automation** section of your **Privacy** settings, allowing SafeGuard File Encryption to automate Finder.

If you click **Don't allow**, this dialog will not be shown again and SafeGuard File Encryption will not be able to use the Finder functionality.

If you want to change the settings later, go to the **Automation** section of your **Privacy** settings and select **Finder** below **Sophos SafeGuard** to allow SafeGuard File Encryption to control Finder.

## 1.2.1 Location-based file encryption

Location-based file encryption allows your security officer to define locations where files are encrypted. We call these locations Secured Folders (page 3). To find out which locations on your computer are encrypted, see the Policies tab (page 6) in the preference pane.

- New files in a location that is specified for encryption are encrypted automatically.
- If you move an unencrypted file to a location that is specified for encryption, it is encrypted.
- If you move an encrypted file to a location that is excluded from encryption, it is decrypted.
- If you have the key for an encrypted file, you can read and modify the content.
- If you do not have the key for an encrypted file, you can neither read its content nor move it to a different location.
- If you access an encrypted file from a computer where File Encryption is not installed, you cannot read its content.

## 1.2.2 Application-based file encryption

Application-based file encryption encrypts files created or modified with specific applications (for example, Microsoft Word). A policy defines a list of applications for which file encryption is executed automatically. Application-based file encryption extends to all Secured Folders (page 3). In addition, your security officer can exclude specific locations from encryption. To find out which locations on your computer are encrypted, see the Policies tab (page 6) in the preference pane.

- New files created with specific apps are encrypted automatically.
- Files modified with specific apps are encrypted automatically.
- If you have the key for an encrypted file, you can read and modify the content.
- If you do not have the key for an encrypted file, you cannot read its content.
- If you access an encrypted file from a computer where File Encryption is not installed, you cannot read its content.
- If you access an encrypted file with an application that is not defined in your policy, you cannot read its content.

## 1.2.3 Secured Folders

Secured Folders are locations on your Mac, on network shares, or on removable devices where files are encrypted. Your security officer defines your Secured Folders in a policy. Typically, these are folders such as Documents and temporary folders where Microsoft Outlook or Apple Mail stores email attachments.

With macOS Catalina, SafeGuard Enterprise needs your permission for accessing folders like Documents, Desktop, Pictures and Apple Mail.

Follow these steps to allow SafeGuard Enterprise to access these folders:

1. Open **Security & Privacy**.
2. Unlock to make changes.
3. Select **Full Disk Access**.

4. Click the + button to add these two SafeGuard apps to your **Full Disk Access** panel:
   - sgd from the folder `/usr/local/bin/`
   - Sophos SafeGuard from the folder `/Library/Sophos SafeGuard FS`

## Limitations

- **Encrypted files only accessible in Secured Folders**

  You cannot access an encrypted file that is located outside a Secured Folder. You must either move it to a Secured Folder or decrypt it manually first.
- **Permanent version storage unavailable in Secured Folders**

  For files in Secured Folders, the standard functionality **Browse All Versions...** is not available.
- **Searching for files**
  - By default, searching for files in Secured Folders using Spotlight is not possible. To turn on Spotlight support, see Search for encrypted files (page 13).
  - Searching for labeled files does not work in Secured Folders.
- **Sharing Secured Folders**

  A Secured Folder cannot be shared over the network.

# 2 Sophos SafeGuard preference pane

After installing Sophos SafeGuard Enterprise for Mac, the Sophos SafeGuard icon appears in the **System Preferences**.

Click on the icon to open the Sophos SafeGuard preference pane.

The **About** tab is displayed. It contains information on the product version installed on your Mac.

## 2.1 Server tab

The **Server** tab contains the following information and functionality related to the SafeGuard Enterprise Server:

**Server Info**

- **Contact Interval:** Time between synchronisations with the server.
- **Last Contacted:** Date of the last synchronisation with the server.
- **Primary Server URL:** URL of the main server connection.
- **Secondary Server URL:** URL of the secondary server connection.
- **Server Verification:** Indicates whether SSL server verification for communication with the server is enabled.

**Drag configuration zip file here**

Drag the configuration zip file to this drop zone in order to apply configuration information from the SafeGuard Enterprise Server to the Mac.

**Synchronize**

Click this button to manually synchronize with the SafeGuard Enterprise Server.

**Check Connection**

Click this button to check your connection with the SafeGuard Enterprise Server.

**Company Certificate**

- **Valid from:** the date the certificate has become valid
- **Valid to:** the date the certificate validity expires
- **Issuer:** the instance which has issued the certificate
- **Serial:** the serial number of the company certificate

## 2.2 User tab

The **User** tab displays the following information:

- Your **Username**.
- The **Domain** directory your Mac belongs to. For local users, the local computer name is displayed.
- The **SafeGuard User GUID** that was generated during your first logon.

- The **SafeGuard User State** indicates, whether you are an **SGN user** or an **Unconfirmed user**. As an unconfirmed user, you cannot access or create encrypted files. In this case, ask your security officer to confirm your account.

The second window section displays information about the **User Certificate**. This is only relevant for File Encryption.

- **Valid from:** the date the certificate has become valid
- **Valid to:** the date the certificate validity expires
- **Issuer:** the instance which has issued the certificate
- **Serial:** the serial number of the certificate

In the third window section, you can choose to display an icon in the system menu for each component. These options are only available when the corresponding component is installed.

- **Show System Menu for Native Device Encryption**
- **Show System Menu for File Encryption**

# 2.3 Keys tab

This tab is only displayed when SafeGuard File Encryption is installed.

The **Keys** tab displays all existing key names in a list view.

Click on the list icon in the lower right corner next to **Number of Keys** to hide or show the GUID information of the key(s).

You can list and sort the keys using one of the header elements **Key Name** or **Key GUID**.

If a key is displayed in blue, it's your personal key. Local keys are displayed in green (see Use local keys (page 13)). All other (standard) keys are displayed in black.

# 2.4 Policies tab

This tab is only displayed when SafeGuard File Encryption is installed.

In the **Policies** tab, click on one of the icons in the lower right corner to switch between the **Locally Translated Path** view and the **Received Policies** view.

- The **Locally Translated Path** view displays only those policies which currently apply to the logged-on user on a specific Mac. The columns in the table contain the following information:
  - @: During initial encryption or when encrypting larger files, you can see a rotating wheel in the first column.
  - **Locally Translated Path**: Displays the location on your Mac.
  - **Mode**: Indicates whether a location is defined to be encrypted or excluded from encryption.
  - **Scope**: Indicates whether subfolders in a location are to be encrypted.
  - **Key Name**: Displays the name of the key assigned to the specified location.

    Your personal key is displayed in blue.

    A key that is displayed in orange means it has been configured in a policy that was assigned to you. But, you do not own the key, as it was not assigned to your keyring. This can cause trouble when accessing data. In this case contact your security officer.

- The **Received Policies** view displays all policies which are received from the server. The table lists the following information:
  - **Received Policies**: Specifies which files or folders to encrypt.
  - All other columns contain the information described above for the **Locally Translated Path** view.

### Enforce policies in the Locally Translated Path view

- When no policy is selected, you can click the **Enforce all Policies** button to start initial encryption. For more information, see Encrypt files according to policy (page 10).
- When you select a policy, you can click the **Enforce Policy** button to apply the selected policy only.
- When you select a policy, you can click the **Show in Finder** button to open the selected Secured Folder in the Finder.

### Possible results from enforcing policies

- Plain files are encrypted with the key assigned by a policy.
- Files already encrypted with the key specified in the policy remain encrypted.
- Files already encrypted with a different key are either
  - unchanged if the user does not have the required key in their keyring or
  - re-encrypted with the key assigned by a policy if the user has this encryption key in their keyring.
- Files in folders that are excluded from the encryption policy are decrypted.
- Files that are not accessible because of missing permissions (read-only) are left unchanged.

## 2.5 Disk Encryption tab

This tab is only displayed when SafeGuard Native Device Encryption is installed.

The **Disk Encryption** tab contains information about the current policies and the encryption status of your Mac.

The first window section tells you whether the system disk should be encrypted according to the policy set by the security officer.

The second window section displays the status of the Mac. This can be one of the following:

- The system disk is encrypted and a centrally stored recovery key is available.
- The system disk is encrypted but there is no centrally stored recovery key available.
- The system disk is not encrypted.

At the bottom, the **Decrypt System Disk** button is displayed. It is available if the security officer has set a policy defining that no encryption is necessary for the endpoint.

# 3 How to ...

## 3.1 Encrypt a computer

When your security officer assigns you a Device Encryption policy, a dialog prompts you to enter your macOS password. After that, the encryption of your computer starts.

1. Enter your macOS password.
2. Click **Enable** or **Enable and Restart**.

   Macs using Apple File System (APFS) formatting do not require a restart, so only the **Enable** option is shown.

Disk encryption operates in the background, so you can continue with your work. For more information, see SafeGuard Native Device Encryption (page 1).

If turning on the encryption fails, contact your system administrator.

## 3.2 Decrypt a computer

Usually, it is not necessary to decrypt. If the security officer sets a policy that specifies no encryption for your Mac that is already encrypted, it remains encrypted. However, in this case you have the choice to decrypt. Use the corresponding button in the preference pane. See Disk Encryption tab (page 7).

## 3.3 Reset a forgotten password

The process to reset a forgotten password depends on the type of encryption installed on your Mac:

- SafeGuard Native Device Encryption (page 8)
- SafeGuard Native Device Encryption and SafeGuard File Encryption (page 9)

### 3.3.1 SafeGuard Native Device Encryption

If you forget your macOS password, proceed as follows:

1. Switch on your Mac.
2. Click the question mark icon in the **Password** field.
   Your password hint is displayed and you are asked whether you want to reset your password using your recovery key.
3. Click the arrow icon next to the message to switch to the recovery key field.
4. Contact your security officer and ask for your recovery key.
5. Enter your recovery key in the corresponding field and click the arrow icon on the right-hand side.
   The Mac starts and the **Reset Password** dialog is displayed.
6. If you are an Active Directory user, ask your administrator to reset your password and request a new password.

   a) Make sure your computer is connected to the Active Directory Domain Services.

b) In the **Reset Password** dialog, click **Cancel** and enter your new password.

c) Change your password once again, if required.

7. If you are a local macOS user, enter a new password and a password hint and click **Reset Password**.
8. If the system cannot unlock your login keychain, click **Create New Keychain**.
9. A mac with macOS 10.13 and APFS formatted system disk might need the new password in order to create a new recovery password. When prompted, enter the password.

   The dialog is only shown if you are connected to the SafeGuard Enterprise Server. If there is no connection, it is shown the next time a connection is established.

## 3.3.2 SafeGuard Native Device Encryption and SafeGuard File Encryption

These instructions assume you have both SafeGuard Native Device Encryption and SafeGuard File Encryption installed on your Mac. If you are using only one of the above, steps may vary.

If you forget your macOS password, proceed as follows:

1. Switch on your Mac.
2. Click the question mark icon in the **Password** field.
   Your password hint is displayed and you are asked whether you want to reset your password using your recovery key.
3. Click the arrow icon next to the message to switch to the recovery key field.
4. Contact your security officer and ask for your recovery key. Additionally, your security officer must remove your user certificate in the SafeGuard Management Center.
5. Enter your recovery key in the corresponding field and click the arrow icon on the right-hand side.
   The Mac starts and the **Reset Password** dialog is displayed.
6. If you are an Active Directory user, ask your administrator to reset your password and request a new password.

   a) Make sure your computer is connected to the Active Directory Domain Services.

   b) In the **Reset Password** dialog, click **Cancel** and enter your new password.

   c) Change your password once again, if required.
7. If you are a local macOS user, enter a new password and a password hint and click **Reset Password**.
8. Click **Create New Keychain**.
   A new login keychain is created. Note that all existing entries of your keychain remain valid.
9. A mac with macOS 10.13 and APFS formatted system disk might need the new password in order to create a new recovery password. When prompted, enter the password.

   The dialog is only shown if you are connected to the SafeGuard Enterprise Server. If there is no connection, it is shown the next time a connection is established.
10. Enter your new password to create the SafeGuard user certificate.
    If you are an Active Directory user, your keys are loaded into the SafeGuard Enterprise keyring automatically. You can access your documents as before.
11. If you are a local user, ask your security officer to confirm the user registration.
12. Open the **Server** tab in the Preference Pane and click **Synchronize**.

Your keys are restored and you have access to your encrypted documents again.

## 3.4 Save the Device Encryption recovery key centrally

If there is no centrally stored recovery key available, the helpdesk cannot assist you with password recovery. To make the recovery key centrally available, import it using the command line tool: `sgdeadmin --import-recoverykey`. Then, the security officer can provide you with the recovery key when you need it.

If you do not know the recovery key, contact your security officer. This is important because if you forget your logon password and there is no recovery key available, all data stored on the encrypted disk will be lost.

## 3.5 Encrypt files according to policy

Your security officer uses policies to define which files need to be encrypted and what key needs to be used. To make sure that sensitive files on your computer are encrypted, we recommend that you perform an initial encryption. This means that all policies your security officer assigned to you will be enforced. To start an initial encryption:

1. Open the **System Preferences**.
2. Click the Sophos SafeGuard icon.
3. Select the **Policies** tab.
4. Switch to **Locally Translated Path** view and click on **Enforce all policies**.

All files in Secured Folders (page 3) are encrypted or re-encrypted with the key specified in the policy.

If you want to enforce a single policy, select the policy and click **Enforce Policy**.

If you want to encrypt individual files or folders according to policy, right-click a file or folder and select **Encrypt According to Policy**.

## 3.6 Encrypt/Decrypt files manually

SafeGuard File Encryption allows you to encrypt or decrypt individual files manually. Right-click a file to do one of the following:

- **Show Encryption State**: Indicates whether or not the file is encrypted as well as the key used.
- **Encrypt According to Policy**: The selected files are encrypted or re-encrypted with the key specified in a policy.
- **Decrypt Selected File** (only for application-based file encryption): Allows you to decrypt your file and store it in plaintext. We recommend decrypting your file only if it does not contain any sensitive data.
- **Encrypt Selected File** (only for application-based file encryption): Allows you to manually encrypt files with the key specified in your policy.
- **Create Password Protected File**: Here you can define a password to encrypt individual files manually. This is useful if you want to securely share your file with someone outside your corporate network, see Use a password to protect a file (page 11). This option is only available for files that are either not encrypted or encrypted with a key available in your keyring.

# 3.7 See where files are encrypted

Your security officer uses policies to define locations on your computer where files are encrypted and where they are not. To find out about your policies:

1. Open the **System Preferences**.
2. Click the Sophos SafeGuard icon.
3. Select the **Policies** tab, see Policies tab (page 6).

# 3.8 Send encrypted files via email

When you send encrypted files to recipients in your corporate network, you do not need to worry about encryption and decryption. If your recipient has the appropriate key, they will be able to read the file.

When sending emails to recipients outside your corporate network, we recommend that you encrypt your file with a password, see Use a password to protect a file (page 11).

If you are sending files to recipients outside your corporate network and you do not want to use password protection, make sure that you decrypt the file first. Otherwise, recipients will not be able to access encrypted files.

# 3.9 Use a password to protect a file

When sending emails to recipients outside your corporate network, we recommend that you encrypt your file with a password. This allows the recipients to access encrypted files without having SafeGuard Enterprise installed.

Do the following:

1. Right-click the file you want to send and select **Create Password Protected File**.
   If you receive an error message, select **View > Hide Preview** in the Finder and try again.
2. Follow the on-screen instructions and create a password. We recommend that you use a strong password and don't send it in the same email as the files.
   Your file is encrypted and saved as an HTML file. You can now safely attach the HTML file to emails.

   **Note**
   - You need free disk space for the encryption.
   - The encrypted HTML file is bigger than the original file.
   - The maximum supported file size is 50 MB.
   - To send several files at once, you can compress them into a .zip file and then encrypt the .zip file.

3. Give your recipients the password by phone or through any other means of communication.
   Recipients can use one of the following browsers to open the password protected attachment:
   - Mozilla Firefox
   - Google Chrome

- Microsoft Internet Explorer 11
- Microsoft Edge

4. Instruct your recipients to double-click the file and follow the on-screen instructions to do one of the following:
   - Enter the password and click **Enter** to access the file.
   - Click **Password protect a new file** to protect a different file with a password.

Recipients can access a file you protected with a password. They can protect the file with a password when sending it back to you. They may use the same password or a new password. They can even protect a new file with a password.

# 3.10 Encrypt files in the cloud

Sophos SafeGuard encrypts your files in the cloud automatically if the following conditions are met:

- Your administrator specified that files in cloud storage folders are encrypted.
- The cloud storage folder is located outside a Secured Folder (see Secured Folders (page 3)).
- You are using one of the supported cloud storage providers:
  - Box
  - Dropbox
  - Google Drive
  - Microsoft OneDrive
  - Microsoft OneDrive for Business

To see if your cloud storage folder is encrypted, check the **Policies** tab in the preference pane, see Policies tab (page 6).

**Note**

- You will see Sophos SafeGuard overlay icons on the encrypted files, instead of the cloud storage provider's icons.
- You can't view or edit encrypted files in the cloud simultaneously with other users.

# 3.11 Encrypt files on removable devices

When you insert a removable device into your computer, a dialog prompts you to decide how to handle the files on the device. You have the following options:

1. Select **Remember setting and do not show this dialog again** and click **No**.
   No files will be encrypted at any time on this device.
2. Select **Remember setting and do not show this dialog again** and click **Yes**.
   Whenever you save a new file on this device, it is encrypted automatically.
3. Select **Encrypt existing files** and click **Yes**.
   Existing files on your device will be encrypted and new files are encrypted as long as the device is connected to your computer.
4. Select **Remember setting and do not show this dialog again** and **Encrypt existing files** and click **Yes**.

Both existing files and new files on your device will always be encrypted automatically.

## 3.12 Exchange encrypted files on removable devices

You can use removable devices such as USB flash drives or external hard drives to exchange encrypted files.

To exchange and modify data on removable devices between two parties, both parties must have the appropriate policy and key assigned.

For the exchange between macOS and Windows endpoints, the device should be formatted with FAT32. Other file formats may work with limited functionality. Since the file format cannot be displayed in the Finder, you have to use Disk Utility to check the file system.

If you exchange larger files on removable devices, make sure you have more free space available than twice the largest file size to be exchanged.

On removable devices that are also used for Time Machine backups, the `Backups.backupdb` directory is excluded from encryption automatically.

## 3.13 Use local keys

Local keys are only available for Location-based file encryption (page 3).

Local keys can be used for encrypting files in specified folders on a removable device or a cloud storage provider. These locations must be included in an encryption policy already.

To create a local key:

1. Make sure your endpoint is connected to the SafeGuard Enterprise Server, see Server tab (page 5).
2. Right-click on a file or selection of files and select **Create New Key**.
3. Choose a name and a passphrase for your key and click **OK**.

   The key name is prefixed with "Local_" and postfixed with date and time.

The local key is created and added to your keyring. You can now apply the local key to a removable device or a cloud storage folder.

## 3.14 Search for encrypted files

If you want to search for encrypted files, you need to turn Spotlight on manually.

1. To turn on Spotlight search, run the following Terminal command:

   ```
   sgfsadmin --enable-spotlight
   ```
2. To turn off Spotlight search, run the following Terminal command:

   ```
   sgfsadmin --disable-spotlight
   ```

**Note**
Using Spotlight together with Sophos SafeGuard may reduce the search speed.

## 3.15 Recover encrypted files

If a file is encrypted with a key that is not available in your keyring, you cannot open the file. This might be the case because you are not supposed to access this file according to company policy. However, in some cases, you may be allowed access to the file but you just happen not to have the required key. In this case, you need to find out which key was used and ask your security officer to assign the key to your keyring. Proceed as follows:

1. Right-click the file and select **Show Encryption State** from the context menu.
   The key used for encrypting this file is displayed.
2. Contact your security officer and provide them with the key name.
3. Ask your security officer to assign the key to your keyring.
4. As soon as your security officer confirms that your user policy has been updated, go to **System Preferences > Sophos SafeGuard > Server**.
5. Click the **Synchronize** button.
6. Open the **Keys** tab and check whether the required key is displayed in the list.

If the key that was used for encrypting the file in question is listed in the **Keys** tab, you can now access the file.

## 3.16 Check your connection to the SafeGuard Enterprise Server

If you are having trouble synchronizing your endpoint with the SafeGuard Enterprise Server, do the following:

1. Open the Sophos SafeGuard preference pane (page 5) and click on the Server tab (page 5).
2. Click the **Check Connection** button.
   The **Check SafeGuard Enterprise Client-Server Connectivity** window opens.
3. Click **Run**.
   The system checks the connection to the SafeGuard Enterprise Server.
4. Click the **Export** button on the bottom of the window to save the results as a text file.
5. If the connection to the SafeGuard Enterprise Server fails, contact your administrator.

# 4 Support

## Full release

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 knowledge base 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.

# 5 Legal notices