

SOPHOS

Security made simple.

SafeGuard Enterprise upgrade guide

Product version: 7

Document date: December 2014



Contents

1 About this guide.....	3
2 Check the system requirements.....	4
3 Download installers.....	5
4 About upgrading.....	6
4.1 Upgrade the SafeGuard Enterprise Database and database schema.....	6
4.2 Upgrade SafeGuard Enterprise Server.....	8
4.3 Upgrade SafeGuard Management Center.....	8
4.4 Upgrade endpoints.....	9
4.5 Upgrade endpoint configuration packages.....	10
5 About migrating	12
5.1 Migrating from SafeGuard Easy.....	12
5.2 Modify the SafeGuard installation on endpoints.....	14
5.3 Migrate endpoints to a different operating system	14
6 Technical support.....	15
7 Legal notices.....	16

1 About this guide

This guide covers upgrading from previous versions of SafeGuard Enterprise as well as migration scenarios that may also involve a change in your Sophos encryption software license.

Both server-side and endpoint software upgrade/migration are covered.

This guide tells you how to directly upgrade from SafeGuard Enterprise 6.0 or later.

Note: 5.6x clients can still be managed with SafeGuard Enterprise 7.0.

The guide contains information on:

- Migrating from SafeGuard Easy 6.0 or later to SafeGuard Enterprise 7.0.
- Migrating endpoints to different encryption modules or operating systems.

2 Check the system requirements

For hardware and software requirements, service packs and disk space required during installation as well as for effective operation, see the current release notes version on the Sophos SafeGuard release notes landing page <http://www.sophos.com/en-us/support/knowledgebase/112776.aspx>.

3 Download installers

1. Using the web address and download credentials provided by your system administrator, go to the Sophos website and download the installers.
2. Store them in a location where you can access them for installation.

4 About upgrading

SafeGuard Enterprise 6.0 or later can be directly upgraded to the latest version of SafeGuard Enterprise without changing any previous settings. If you want to upgrade from older versions, you must first upgrade to version 6.0.

During an upgrade you cannot make changes to the installed features or modules. If changes are required, run the installer of the version already in place again and modify the installation (see [About migrating](#) (page 12)).

The following components are upgraded during an upgrade to the latest version of SafeGuard Enterprise. Carry out the upgrade in the order shown below:

1. SafeGuard Enterprise Database
2. SafeGuard Enterprise Server
3. SafeGuard Management Center
4. SafeGuard Enterprise protected endpoints
5. SafeGuard Enterprise configuration packages

Note: Once all SafeGuard Enterprise components and endpoints have been upgraded to version 7.0, we recommend that you switch to the more secure algorithm **SHA-256** to sign SafeGuard Enterprise-generated certificates.

Only do so if all SafeGuard Enterprise components and endpoints have been upgraded to version 6.1 or later. **SHA-256** is not supported in mixed environments where, for example, SafeGuard Enterprise 6.x endpoints are managed by SafeGuard Management Center 7.0.

For further information, see the *SafeGuard Enterprise Administrator help*, section *Change algorithm for self-signed certificates*.

4.1 Upgrade the SafeGuard Enterprise Database and database schema

Prerequisites:

- A SafeGuard Enterprise Database version 6.0 or later must be installed. Older versions must first be upgraded version by version to version 6.0.
- SQL migration scripts are needed for the upgrade. You find them in the Tools directory of your software delivery, under Database scripts > Migration scripts. Make sure that they are present on the database computer.
- .NET Framework 4 is required. It must be installed before the upgrade. It is provided in the SafeGuard Enterprise software delivery.
- Make sure that you have Windows administrator rights.

To upgrade the SafeGuard Enterprise Database and database schema:

1. Close all instances of SafeGuard Management Center.
2. Take all SafeGuard Enterprise Servers (IIS) offline, for example by stopping the website.
3. Create a backup of the SafeGuard Enterprise Database.
4. Open Microsoft SQL Server Management Studio.
5. In the Object Explorer, right-click the SafeGuard Enterprise Database and click **Properties**.
6. In the **Database Properties** window, select the **Options** page on the left. Under **State, Restrict Access**, select **SINGLE_USER** mode for running the SQL migration scripts.
7. In the Object Explorer, right-click the SafeGuard Enterprise Database and click **New Query**.
8. Use the SQL migration scripts to upgrade the database schema. Depending on the version installed, start the respective SQL scripts, for example:
 - a) From 6.0x to 7.0: Run **MigrateSGN600_SGN700.sql**
 - b) From 6.1 to 7.0: Run **MigrateSGN610_SGN700.sql**

If you have changed the default database name during installation, change the **USE SafeGuard** command in the script so that it reflects the current name accordingly.

9. In the **Database Properties** window, select the **Options** page on the left. Under **State, Restrict Access**, select **MULTI_USER** mode again.
10. Upgrade one instance of SafeGuard Management Center by installing the latest version of the SafeGuard Management Center installation package (`SGNManagementCenter.msi`).
11. Start the upgraded SafeGuard Management Center.

The database consistency is now checked automatically. If the cryptographic checksums of some tables are found incorrect, warning messages are displayed. To repair the tables select **Repair** in the relevant dialog. The checksums for the modified tables are recalculated.

12. Upgrade the SafeGuard Enterprise Server. For further information, see [Upgrade SafeGuard Enterprise Server](#) (page 8).
13. Upgrade the remaining instances of SafeGuard Management Center.

The latest version of the SafeGuard Enterprise Database is ready for use.

4.1.1 Upgrade SafeGuard Enterprise replicated databases

When the SafeGuard Enterprise Database is to be upgraded and replicated databases are in use, we recommend that you uninstall the replicated databases before starting the upgrade on the master database.

Upgrading the SafeGuard Enterprise Database requires running special SQL migration scripts which might otherwise conflict with replicated databases.

To upgrade the replicated database:

1. Uninstall the replicated databases.
2. Carry out the steps for upgrading the master database and database schema, see [Upgrade the SafeGuard Enterprise Database and database schema](#) (page 6).
3. Set up the replication databases again.

4.2 Upgrade SafeGuard Enterprise Server

Prerequisites

- SafeGuard Enterprise Server 6.0 or later must be installed. Versions below 6.0 must first be upgraded to SafeGuard Enterprise Server 6.0.
- .NET Framework 4 with ASP.NET 4 is required. It must be installed before the upgrade. It is provided in the SafeGuard Enterprise product delivery. You can also download it for free from: <http://www.microsoft.com/downloads>
- Make sure that you have Windows administrator rights.

To upgrade SafeGuard Enterprise Server:

1. Install the latest version of the SafeGuard Enterprise Server installation package using SGNServer_upgrade.exe.

SafeGuard Enterprise Server is upgraded to the latest version. It is automatically restarted and is ready for use.

4.3 Upgrade SafeGuard Management Center

Prerequisites:

- SafeGuard Management Center 6.0 or later must be installed. Versions below 6.0 must first be upgraded to SafeGuard Management Center 6.0.
- SafeGuard Enterprise Database and SafeGuard Enterprise Server must have been upgraded to the latest version. For successful operation, version numbers of SafeGuard Enterprise Database, SafeGuard Enterprise Server and SafeGuard Management Center must match.
- SafeGuard Management Center 7.0 can manage SafeGuard Enterprise-protected endpoints 5.60 and later.
- .NET Framework 4 is required. It must be installed before the upgrade. It is provided in the SafeGuard Enterprise product delivery.
- Make sure that you have Windows administrator rights.
- When upgrading from SafeGuard Enterprise 5.x to SafeGuard Enterprise 7.0, you need to manually import the default evaluation license for SafeGuard Cloud Storage and SafeGuard File Encryption. This license file is provided in your product delivery.

To upgrade SafeGuard Management Center:

1. Install the latest version of the SafeGuard Management Center installation package with the required features, see [About migrating](#) (page 12).
2. Start the SafeGuard Management Center.

3. In the SafeGuard Management Center, import the new license file: In **Users and Computers**, click the root node in the left-hand navigation tree. In the action area, switch to the **Licenses** tab. Click the **Import license file** button, browse for the respective license file and click **Open**. In the **Apply license?** dialog, click **Apply license**.
4. In the SafeGuard Management Center, import the default evaluation license *DefaultLicense_CSFS.xml* for SafeGuard Cloud Storage and SafeGuard File Encryption from the following Sophos product folder: *Sophos\SafeGuard Enterprise\Management Center*.

SafeGuard Management Center is upgraded to the latest version.

After upgrading SafeGuard Management Center to the latest version, do not transfer existing POA users to SafeGuard Enterprise-protected endpoints 5.x or later. They would be interpreted as normal users in this case and registered as users on the respective endpoints.

If you have exported policies for backup reasons, export them again after upgrading SafeGuard Management Center. Policies exported using older versions cannot be imported.

4.4 Upgrade endpoints

This section applies to both managed and unmanaged endpoints.

Prerequisites

- SafeGuard Enterprise encryption software version 6.0 or later must be installed. Older versions must first be upgraded to version 6.0.
- SafeGuard Enterprise Database, SafeGuard Enterprise Server, and SafeGuard Management Center must have been upgraded to the latest version. For successful operation, version numbers of SafeGuard Enterprise Database, SafeGuard Enterprise Server and SafeGuard Management Center must match.
- SafeGuard Management Center 7.0 and SafeGuard Enterprise Server 7.0 can manage SafeGuard Enterprise protected endpoints version 5.60 or later.

However, we recommend that you avoid a mixture of endpoint encryption software versions for general use.

- Make sure that you have Windows administrator rights.

To upgrade SafeGuard Enterprise-protected endpoints:

1. Log on to the computer as an administrator.
2. Install the latest pre-installation package *SGxClientPreinstall.msi* that provides the endpoint with the necessary requirements for a successful installation of the new encryption software.

Do not uninstall previous pre-installation packages.

3. Install the latest version of the respective SafeGuard Enterprise encryption software. Depending on your installed version, a direct upgrade might not be supported. Older versions must be upgraded version by version until version 6.0 is reached.

Windows Installer recognizes the features that are already installed and only upgrades these. If Power-on Authentication is installed, an updated POA kernel is also available after a successful update (policies, keys, etc.). SafeGuard Enterprise is automatically restarted on the computer.

If your old client version included configuration protection and you upgrade to a version that no longer supports it, for example, when you upgrade from version 6.0 to 7.0, you need to uninstall configuration protection. Confirm this in the user interface if you do a manual upgrade or provide the parameter CONFIRMCPREMOVAL=1 if you upgrade centrally.

4. To remove configuration protection completely, it is also necessary to uninstall SGNCPCClient.msi (or SGNCPCClient_x64.msi).
5. After installation is completed, restart the endpoint when prompted.

The latest version of the SafeGuard Enterprise encryption software is installed on the endpoints. Next, upgrade the endpoint configuration.

Note: To upgrade SafeGuard Enterprise-protected endpoints centrally and uninstall configuration protection at the same time, use a command in the following format:

```
msiexec /i SGNCClient_x64.msi /qn /log C:\Temp\SGNCClient.log  
CONFIRMCPREMOVAL=1
```

```
msiexec /x SGNCPCClient_x64.msi /qn /log C:\Temp\SGNCP.log
```

For further information, see the *SafeGuard Enterprise 7.0 installation guide*.

Note: You cannot make changes to your installed modules during an upgrade. If changes are required, see [About migrating](#) (page 12).

4.5 Upgrade endpoint configuration packages

After upgrading the encryption software, we strongly recommend to delete all old configuration packages for security reasons. Only install configuration packages created with SafeGuard Management Center 7.0 on endpoints upgraded to 7.0. Configuration packages generated with a previous version of the SafeGuard Management Center are not supported and cannot be used on upgraded endpoints.

We recommend that you create and distribute a new configuration package in the following case:

In mixed environments, in which individual components or endpoints are not upgraded to the latest version, only the hash algorithm SHA-1 can be used to sign certificates generated by SafeGuard Enterprise. As of SafeGuard Enterprise 6.1, the more secure hash algorithm SHA-256 can be used. Once all components and endpoints have been upgraded to the latest version, we recommend that you switch to the more secure algorithm. In this case, you need to create a new configuration package and distribute it to the endpoints.

Note: For further information, see the *SafeGuard Enterprise Administrator help*, section *Change algorithm for self-signed certificates*.

Note: You cannot downgrade an endpoint from the managed to standalone mode by uninstalling the managed configuration package and installing an unmanaged configuration package.

5 About migrating

Migration means a change of installed products, modules or features. As of version 7.0 this can only be done within the same version. Therefore it might be necessary to either migrate your product within your old version or to upgrade the installation first and do the migration afterwards.

Note: If you do not find your currently installed product or version in this guide, direct upgrade or migration is not supported. Please refer to the documentation for your product or version for possible upgrade or migration paths.

Note: If your migration scenario involves a change in your Sophos encryption software license, make sure that your new license is available for the migration.

5.1 Migrating from SafeGuard Easy

You can migrate the standalone solution SafeGuard Easy to the SafeGuard Enterprise suite with central management to make use of comprehensive management features, for example, user and computer management or extensive logging functionality.

- Set up the latest version of SafeGuard Enterprise Server. For further information, see the *SafeGuard Enterprise 7.0 Installation guide*.
- Migrate the management console.
- Migrate the endpoints to a managed configuration.

5.1.1 Migrate the management console

Prerequisites

- You do not have to uninstall SafeGuard Policy Editor.
- .NET Framework 4 with ASP.NET 4 must be installed. It is provided in the SafeGuard Enterprise product delivery.
- Make sure that you have Windows administrator rights.

To migrate the management console:

1. On the computer on which SafeGuard Policy Editor is installed, start `SGNManagementCenter.msi`. A wizard guides you through installation. Accept the default options.
2. If prompted, restart the computer.
3. Start SafeGuard Management Center to carry out initial configuration.
4. Configure the SafeGuard Enterprise policies to your needs.

SafeGuard Policy Editor has been migrated to SafeGuard Management Center.

5.1.2 Migrate endpoints to a managed configuration

You can migrate unmanaged endpoints to a managed configuration. They can thus be managed in the SafeGuard Management Center and have a connection to the SafeGuard Enterprise Server.

Note: If you have already upgraded an endpoint to the latest version and just want to change the configuration, start with step 6.

Prerequisites

- Back up the endpoint.
- Make sure that you have Windows administrator rights.
- Sophos SafeGuard encryption software on the endpoints does not have to be uninstalled. Sophos SafeGuard version 6.0 or later must be installed on the endpoints. Older versions must be upgraded version by version until version 6.0 is reached.

To migrate endpoints locally:

1. Log on to the endpoint as an administrator.
2. Install the latest pre-installation package `SGxClientPreinstall.msi` that provides the endpoint with the necessary requirements for a successful installation of the new encryption software.

Do not uninstall previous pre-installation packages.

3. Install the latest version of the respective Sophos SafeGuard encryption software.

Windows Installer recognizes the features that are already installed and only upgrades these. If Power-on Authentication is installed, an updated POA kernel is also available after a successful update (policies, keys etc.). Sophos SafeGuard is automatically restarted on the endpoint.

4. After installation is completed, restart the endpoint when prompted.
5. In SafeGuard Management Center, on the **Tools** menu, click **Configuration Package Tool**. Click **Managed client packages** and create a configuration package for managed endpoints.
6. Assign this package to the endpoint using a group policy.

Important: Authentication is disabled as the User Machine Assignment is not upgraded. After upgrading, the endpoints are therefore unprotected.

7. The user needs to restart the endpoint. The first logon is still achieved with Autologon. New keys and certificates are assigned to the user.
8. The user needs to restart the endpoint for a second time and log on at the Power-on Authentication. The endpoints are protected again only after the second restart.
9. Delete old and unused configuration packages.

The endpoint is now connected to the SafeGuard Enterprise Server.

5.2 Modify the SafeGuard installation on endpoints

If changes to the installed modules are required, run the installer of the version already in place again and modify the installation. The following restrictions apply:

- A change from SafeGuard volume-based encryption to BitLocker Encryption or the other way round requires the product to be uninstalled and reinstalled (data needs to be decrypted).
- A change from BitLocker support to BitLocker with Challenge/Response or the other way round requires the product to be uninstalled and reinstalled (data needs to be decrypted).

See the *SafeGuard Enterprise Administrator help* and the Release Notes for the system requirements for each module.

For information on migration of the operating system see [Migrate endpoints to a different operating system](#) (page 14).

5.3 Migrate endpoints to a different operating system

Once SafeGuard Enterprise is installed, it is only possible to update the Service Pack version of the operating system series installed. You can, for example, install a Windows 8 Service Pack update.

However, you cannot migrate from one operating system series to a different one when SafeGuard Enterprise is installed. For example, you cannot migrate from Windows 7 to Windows 8 when SafeGuard Enterprise is installed.

6 Technical support

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

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

7 Legal notices

Copyright © 1996 - 2014 Sophos Limited. All rights reserved. SafeGuard is a registered trademark of Sophos Limited and Sophos Group.

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, Sophos Anti-Virus and SafeGuard are registered trademarks of Sophos Limited, Sophos Group and Utimaco Safeware AG, as applicable. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

You find copyright information on third party suppliers in the *Disclaimer and Copyright for 3rd Party Software* document in your product directory.