

SafeGuard Enterprise administrator help

administrator help

Version: 8.3

Contents

1. About SafeGuard Enterprise.....	11
2. Installation.....	14
2.1 SafeGuard Enterprise components.....	14
2.2 Getting started.....	18
2.2.1 What are the key steps?.....	18
2.2.2 Compatibility with other Sophos products.....	20
2.3 Setting up SafeGuard Enterprise Server.....	21
2.3.1 Prerequisites.....	22
2.3.2 Installing and configuring Microsoft Internet Information Services (IIS).....	23
2.3.3 Install SafeGuard Enterprise Server.....	25
2.4 Setting up SafeGuard Enterprise Database.....	26
2.4.1 Database authentication.....	27
2.4.2 Generating the SafeGuard Enterprise Database.....	31
2.4.3 Change access rights for the SafeGuard Enterprise Database.....	32
2.4.4 Check SQL Services, named pipes, and TCP/IP settings.....	33
2.4.5 Create Windows Firewall rule on Windows Server.....	33
2.4.6 Configure Windows authentication for SQL Server logon.....	34
2.5 Setting up SafeGuard Management Center.....	35
2.5.1 Prerequisites.....	35
2.5.2 Install SafeGuard Management Center.....	35
2.5.3 Configuring SafeGuard Management Center.....	36
2.5.4 Setting up the organizational structure in the SafeGuard Management Center.....	42
2.5.5 Importing the license file.....	43
2.6 Testing communication.....	43
2.6.1 Ports/connections.....	43
2.6.2 Authentication method.....	44
2.6.3 Set proxy server settings.....	45
2.6.4 Check connection.....	45
2.7 Securing transport connections with SSL.....	45
2.7.1 Certificates.....	46

2.7.2 Activate SSL encryption in SafeGuard Enterprise.....	47
2.7.3 Configure the SGNSRV web page for SSL.....	48
2.7.4 Configure endpoints to use SSL.....	49
2.7.5 Assign the SSL certificate to Windows endpoints.....	49
2.7.6 Import the SSL certificate on Macs.....	50
2.8 Registering and configuring SafeGuard Enterprise Server.....	51
2.8.1 Register and configure SafeGuard Enterprise Server for the current computer.....	51
2.8.2 Register and configure SafeGuard Enterprise Server for a different computer.....	52
2.8.3 Edit SafeGuard Enterprise Server properties.....	53
2.8.4 Register SafeGuard Enterprise Server with Sophos firewall enabled.....	54
2.9 Creating configuration packages.....	54
2.9.1 Create configuration package for managed computers.....	55
2.9.2 Create configuration package for unmanaged computers (Windows only).....	56
2.10 Setting up SafeGuard Enterprise on endpoints.....	57
2.10.1 About managed and unmanaged endpoints.....	57
2.10.2 Restrictions.....	58
2.10.3 Check the availability of the SSL certificate on Windows endpoints.....	58
2.10.4 Prepare for BitLocker Drive Encryption support.....	59
2.10.5 Prepare for SafeGuard Full Disk Encryption with POA.....	59
2.10.6 Prepare for Cloud Storage.....	60
2.11 Installing the encryption software on Windows.....	61
2.11.1 Installing packages and features.....	61
2.11.2 Install the encryption software locally.....	63
2.11.3 Installing the encryption software centrally.....	65
2.11.4 Installations on self-encrypting, Opal-compliant hard drives.....	71
2.12 Installing the encryption software on macOS.....	72
2.12.1 Automated installation of SafeGuard Native Device Encryption.....	73
2.12.2 Manual installation of SafeGuard Native Device Encryption.....	73
2.12.3 Automated installation of SafeGuard File Encryption.....	74
2.12.4 Manual installation of SafeGuard File Encryption.....	75
2.13 Setting up Web Helpdesk.....	76
2.13.1 Server Requirements.....	76

2.13.2 Configure the web server with SSL/TLS.....	76
2.13.3 Language support.....	77
2.14 About upgrading.....	77
2.14.1 Upgrade SafeGuard Management Center.....	78
2.14.2 Upgrade SafeGuard Enterprise Server and Web Helpdesk.....	79
2.14.3 Upgrade endpoints.....	79
2.14.4 Upgrade endpoint configuration packages.....	80
2.15 About migrating.....	81
2.15.1 Modify the SafeGuard installation on endpoints.....	81
2.15.2 Migrate endpoints to a different operating system.....	82
3. SafeGuard Management Center.....	83
3.1 Logging on to the SafeGuard Management Center.....	84
3.1.1 Log on in Single Tenancy mode.....	84
3.2 SafeGuard Management Center user interface.....	84
3.2.1 Language settings.....	87
3.2.2 Check database integrity.....	87
3.3 Working with policies.....	88
3.3.1 Create policies.....	88
3.3.2 Edit policy settings.....	89
3.3.3 Policy groups.....	90
3.3.4 Back up policies and policy groups.....	91
3.3.5 Restore policies and policy groups.....	92
3.3.6 Assign policies.....	92
3.3.7 Manage policies in Users and Computers.....	94
3.4 Working with configuration packages.....	94
3.4.1 Create configuration package for managed endpoints.....	95
3.4.2 Create configuration package for unmanaged endpoints.....	96
3.4.3 Create configuration package for Macs.....	97
3.5 Enhanced authentication - the .Unconfirmed Users group.....	98
3.5.1 Confirm users.....	99
3.5.2 Automatically confirm users.....	100
3.6 User Machine Assignment.....	100

3.6.1 User types.....	101
3.6.2 User Machine Assignment in the SafeGuard Management Center.....	102
3.6.3 Assignment of user and computer groups.....	106
3.7 Improve Sophos SafeGuard by sending anonymous usage data.....	107
3.7.1 Create policy to disable sending anonymous usage data.....	107
3.8 SafeGuard Management Center advanced.....	107
3.8.1 Database maintenance.....	107
3.8.2 Working with multiple database configurations (Multi Tenancy).....	109
3.8.3 Warning when company certificate expires.....	114
3.8.4 Search for users, computers and groups in the SafeGuard Enterprise Database.....	115
3.8.5 Display object properties in Users and Computers.....	116
3.8.6 Disabling policy deployment.....	116
3.8.7 Rules for assigning and analyzing policies.....	116
3.8.8 Inventory and status data.....	122
3.8.9 SafeGuard Enterprise Security Officers.....	129
3.8.10 Managing the organizational structure.....	146
3.8.11 Keys and Certificates.....	157
3.8.12 Company Certificate Change Orders.....	168
3.8.13 Licenses.....	172
3.8.14 Tokens and smartcards.....	177
3.8.15 Scheduling tasks.....	194
3.8.16 Auditing.....	204
3.8.17 Policy types and their fields of applications.....	230
3.8.18 Repair a corrupted Management Center installation.....	276
3.8.19 Troubleshooting.....	276
4. Managing Windows endpoints.....	289
4.1 Manage BitLocker Drive Encryption.....	289
4.1.1 Authentication with BitLocker Drive Encryption.....	290
4.1.2 Best practice: Policy settings and user experience.....	291
4.1.3 Prerequisites for managing BitLocker on endpoints.....	293
4.1.4 Manage BitLocker Drive Encryption with SafeGuard Enterprise.....	294
4.1.5 Encrypting with BitLocker managed by SafeGuard Enterprise.....	295

4.1.6 BitLocker To Go.....	299
4.1.7 Recovery for BitLocker encrypted endpoints.....	299
4.2 Location-based File Encryption.....	302
4.2.1 Configuring encryption rules in location-based File Encryption policies.....	303
4.2.2 Configuring location-based File Encryption settings in General Settings policies.....	309
4.2.3 Outlook Add-in for location-based encryption.....	311
4.2.4 Multiple location-based File Encryption policies.....	313
4.2.5 Evaluation of location-based File Encryption rules on endpoints.....	314
4.2.6 Conflicting location-based File Encryption Rules.....	315
4.2.7 Location-based File Encryption and SafeGuard Data Exchange.....	315
4.3 Cloud Storage.....	315
4.3.1 Requirements for Cloud Storage vendor software.....	316
4.3.2 Create Cloud Storage Definitions (CSDs).....	316
4.3.3 Create a device protection policy with a Cloud Storage Definition target.....	321
4.4 SafeGuard Data Exchange.....	322
4.4.1 Best practice.....	322
4.4.2 Group keys.....	328
4.4.3 Local keys.....	328
4.4.4 Media passphrase.....	329
4.4.5 Configure trusted and ignored applications for SafeGuard Data Exchange.....	330
4.4.6 Configure ignored devices for SafeGuard Data Exchange.....	331
4.4.7 Configure persistent encryption for SafeGuard Data Exchange.....	331
4.4.8 SafeGuard Data Exchange and File Encryption.....	331
4.5 SafeGuard Enterprise and self-encrypting, Opal-compliant hard drives.....	332
4.5.1 How does SafeGuard Enterprise integrate Opal-compliant hard drives?.....	332
4.5.2 Enhancement of Opal-compliant hard drives with SafeGuard Enterprise.....	332
4.5.3 Manage endpoints with Opal-compliant hard drives with SafeGuard Enterprise.....	333
4.5.4 Encryption of Opal-compliant hard drives.....	333
4.5.5 Lock Opal-compliant hard drives.....	334
4.5.6 Enable users to unlock Opal-compliant hard drives.....	334
4.5.7 Logging of events for endpoints with Opal-compliant hard drives.....	334

4.6 SafeGuard Configuration Protection.....	335
4.7 About uninstallation.....	335
4.7.1 Start uninstallation.....	335
4.7.2 Preventing uninstallation on the endpoints.....	336
5. Managing Mac endpoints.....	337
5.1 Create configuration package for Macs.....	337
5.2 About SafeGuard Native Device Encryption for Mac.....	338
5.2.1 Manage FileVault 2 endpoints with SafeGuard Management Center.....	338
5.2.2 Encryption policies for FileVault 2 full disk encryption.....	338
5.2.3 Policies.....	339
5.2.4 How does encryption work?.....	339
5.2.5 Initial encryption.....	340
5.2.6 Decryption.....	340
5.2.7 Add FileVault 2 user.....	341
5.2.8 Remove FileVault 2 user.....	341
5.2.9 Synchronization with backend.....	341
5.2.10 Command line options.....	342
5.2.11 Recovery key for Mac endpoints.....	344
5.2.12 Recovery key handling.....	345
5.2.13 Password handling.....	346
5.3 About SafeGuard File Encryption for Mac.....	346
5.3.1 Centrally administered configuration options.....	349
5.3.2 Policies.....	350
5.3.3 Encrypting files in cloud storage.....	350
5.3.4 Initial encryption.....	352
5.3.5 Fast user switching.....	353
5.3.6 Use local keys.....	353
5.3.7 Command line options.....	354
5.3.8 Using Time Machine.....	357
5.3.9 Working with removable media.....	357
5.4 Troubleshooting.....	358
5.4.1 Reset forgotten password.....	358

5.4.2 Problems with accessing data.....	359
5.4.3 Problems with using virtual machines.....	360
5.4.4 SafeGuard recovered files.....	360
5.4.5 Missing Secure Token.....	360
5.5 Inventory and status data of Macs.....	361
5.6 Uninstall Native Device Encryption from Mac endpoints.....	361
5.7 Uninstall File Encryption from Mac endpoints.....	362
6. Synchronized Encryption.....	363
6.1 Best Practice: multi-key support for Synchronized Encryption.....	364
6.1.1 Creating a multi-key file encryption policy.....	364
6.2 Requirements.....	366
6.2.1 Install endpoints.....	366
6.2.2 Upgrade endpoints.....	367
6.2.3 Migration from existing File Encryption module on Windows.....	367
6.2.4 Migration from existing File Encryption module on macOS.....	368
6.2.5 Partial rollout of Synchronized Encryption.....	369
6.3 Encrypt data.....	372
6.3.1 Synchronized Encryption key.....	373
6.3.2 Automatically encrypt files according to policy with asynchronous encryption.....	373
6.3.3 Application Lists.....	374
6.3.4 Initial encryption.....	377
6.3.5 Create policies for application-based file encryption.....	379
6.4 Outlook Add-in for Synchronized Encryption.....	389
6.4.1 Create policies for activating the SafeGuard Enterprise Outlook Add-in.....	389
6.5 Integration with Sophos Central Endpoint Protection.....	390
6.5.1 Creating policies for removing keys on compromised machines.....	391
6.6 Share SafeGuard Enterprise key ring with mobile devices managed by Sophos Mobile....	392
6.6.1 Set up key ring synchronization.....	393
6.7 Configure trusted applications and ignored devices.....	394
6.7.1 Configure trusted applications for Application-based File Encryption.....	394
6.7.2 Configuring ignored devices.....	395
6.8 Application-based File Encryption policies in the RSOP.....	396

7. Advanced management.....	397
7.1 Best practices and recommendations.....	397
7.1.1 Rollout.....	397
7.1.2 Backend.....	402
7.1.3 Policies.....	403
7.1.4 Endpoints - all platforms.....	405
7.1.5 Windows endpoints.....	408
7.1.6 macOS endpoints.....	409
7.2 Security recommendations.....	410
7.3 Replicating the SafeGuard Enterprise Database.....	412
7.4 Web Helpdesk.....	412
7.4.1 Scope of Web Helpdesk.....	413
7.4.2 Allow Web Helpdesk logon for users without SafeGuard Enterprise.....	414
7.4.3 Authentication.....	417
7.4.4 Recovery for managed endpoints (managed SafeGuard Enterprise clients).....	419
7.4.5 Recovery using Virtual Clients.....	422
7.4.6 Recovery for unmanaged endpoints (Sophos SafeGuard clients standalone).....	426
7.4.7 Logging Web Helpdesk events.....	428
7.5 Recovery.....	429
7.5.1 Challenge/Response workflow.....	430
7.5.2 Launch the Recovery Wizard.....	430
7.5.3 Recovery via mobile devices.....	431
7.6 Tools.....	432
7.6.1 Client/Server Connectivity Check tool for Windows.....	432
7.6.2 Displaying Synchronized Encryption policies on endpoints.....	432
7.6.3 Displaying the system status with SGNState.....	434
7.6.4 Reverting an unsuccessful installation with SGNRollback.....	436
7.6.5 Recovering access to computers with the KeyRecovery tool.....	439
7.6.6 Restoring Windows BIOS SafeGuard full disk encryption systems.....	439
7.6.7 Restoring Windows UEFI BitLocker Challenge/Response systems.....	443
7.6.8 Decommissioning encrypted volumes.....	445
7.6.9 Decommissioning self-encrypting, Opal-compliant hard drives.....	447

8. Support.....	449
9. Legal notices.....	450

1. About SafeGuard Enterprise

SafeGuard Enterprise is a comprehensive data security solution that uses a policy-based encryption strategy to provide reliable data protection on workstations, network shares, and mobile devices. It allows users to securely share information and work with files on Windows, macOS, iOS, and Android devices with the help of the Sophos Secure Workspace app, see [SafeGuard Enterprise components \(page 14\)](#).

In the SafeGuard Management Center, you manage security policies, keys, and certificates using a role-based administration strategy. Detailed logs and report functions ensure that you always have an overview of all events.

On the user side, data encryption and protection against unauthorized access are the main security functions of SafeGuard Enterprise. SafeGuard Enterprise can be seamlessly integrated into the user's normal environment.

Synchronized Encryption - application-based File Encryption

Synchronized Encryption is built on two assertions – that all data is important and must be protected (encrypted) and that encryption should be persistent wherever the data is located. In addition, important data should be encrypted automatically and transparently so that a user need not be bothered with having to decide whether or not to encrypt a file based on its perceived importance. This very basic premise, that all data is important and must be protected, ensures that all data is encrypted seamless without user intervention. This allows the user to remain productive, have their data secure and follow their existing workflows, see [Synchronized Encryption \(page 363\)](#).

Location-based File Encryption

- **Cloud Storage**

Cloud storage services are useful to help users access their data, wherever they are, on whatever device they're using. Improving productivity of users is important, but it's equally critical to ensure your sensitive information stays secure once it moves to the cloud. SafeGuard Enterprise automatically and invisibly encrypts/decrypts files as they are uploaded or downloaded from cloud services.

- Encrypts files uploaded to cloud storage services
- Allows secure data sharing everywhere

- Automatically detects and supports most popular cloud storage services such as Box, Dropbox, OneDrive and Egnyte
- Reads encrypted files using our free Sophos Secure Workspace app for iOS and Android

- **File Encryption**

Encryption isn't only for making sure data stays safe from prying eyes outside your business. It's also useful for enabling secure collaboration and controlling files inside it. SafeGuard Enterprise goes beyond simple folder permissions and guarantees that only the right people can read the right files while still allowing IT to manage files and backups.

- Configures file encryption for shared folders
- Makes sure only certain users or groups are able to access data
- Doesn't require any interaction from your users
- Provides an extra layer of protection if/when your corporate servers move to the cloud

- **Data Exchange**

- SafeGuard Enterprise automatically and transparently encrypts files on removable media such as USB sticks, memory cards and CDs/DVDs.
- Share encrypted data on removable media easily across your organization without impacting your users
- Using a portable application and password, easily and securely share encrypted removable media with users not using SafeGuard Enterprise
- Removable media whitelisting makes encryption management easier and more flexible

Full disk encryption with BitLocker

Allows you to manage BitLocker on Windows 8.1 and Windows 10 endpoints.

Protect your Macs

Data on a Mac is as valuable as data on a Windows PC, which makes it vital to include Macs in your data encryption strategy. SafeGuard Enterprise protects your Macs with file and disk encryption

and ensures that the data on your Macs is secure at all times. It includes encryption capability for removable media, network file shares and cloud on Mac.

- Manage file or disk encryption for Macs in the same Management Center as other devices
- Manage FileVault 2 encrypted devices
- Works in the background without impacting performance
- Complete visibility and reporting on encryption status

For Mac endpoints the following modules are available:

	Synchronized Encryption - application-based	Sophos SafeGuard File Encryption - location-based	Sophos SafeGuard Native Device Encryption - FileVault 2 management
macOS 10.13	YES	YES	YES
macOS 10.14	YES	YES	YES
macOS 10.15	YES	YES	YES

Sophos Secure Workspace

Encryption keys from the SafeGuard Enterprise key ring can be made available in the Sophos Secure Workspace (SSW) app managed by Sophos Mobile. Users of the app can then use the keys to decrypt and view documents, or to encrypt documents. These files can then be securely shared between all SafeGuard Enterprise and SSW users. For more information, see the [Sophos Secure Workspace documentation](#).

2. Installation

Available features depend on the type of license you have. For information on what is included in your license, contact your sales partner.

2.1 *SafeGuard Enterprise components*

A Microsoft SQL database stores information about the clients (endpoints) on the company network. The Master Security Officer (MSO) uses the SafeGuard Management Center to manage the database contents and to create new security instructions (policies).

The endpoints read the policies from the database and report to the database. The communication between the database and the endpoints is maintained by an Internet Information Services (IIS) based web server which has the SafeGuard Enterprise Server installed on it.

SafeGuard Enterprise Web Helpdesk is an optional component that provides a web-based recovery solution for managed clients.

SafeGuard Enterprise consist of three major modules:

- Backend
- Software for Windows endpoints
- Software for macOS endpoints

Each module contains several components.

SafeGuard Enterprise Backend BKD

The backend provides the policies for managing SafeGuard Enterprise endpoints. It consists of:

Srv	SafeGuard Enterprise Server: It is maintained by an Internet Information Services (IIS) based web server and manages the communication between the database and the endpoints. Installation package: SGNServer.msi. SafeGuard Enterprise Server runs as an application on a Microsoft Internet Information Services (IIS) based web server and enables communication between the SafeGuard Enterprise database and the SafeGuard Enterprise endpoint. On request, the SafeGuard Enterprise Server sends policy settings to the endpoints. It requires .NET Framework 4.5 and ASP.NET 4.5.
------------	---

	<p>For SSL as default transport encryption method for the client-server communication, the <i>Basic Authentication</i> role needs to be installed.</p> <p>It comes with two subcomponents:</p>
	<p>Web Helpdesk (optional)</p> <p>WHD</p> <p>Web Helpdesk is a web-based recovery solution for managed clients. Web Helpdesk offers help to users who fail to log on or to access SafeGuard Enterprise encrypted data by providing a user-friendly Challenge/Response mechanism, see Web Helpdesk (page 412).</p>
	<p>Server Task Scheduler</p> <p>STS</p> <p>The SafeGuard Management Center offers the Task Scheduler to create and schedule periodic tasks based on scripts, for example to synchronize your Active Directory and the SafeGuard Enterprise Management Center.</p> <p>The tasks are automatically run by a service on the SafeGuard Enterprise Server to execute the scripts specified.</p>
MC	<p>SafeGuard Management Center</p> <p>The Master Security Officer (MSO) uses the SafeGuard Management Center to manage the database content and to create new security instructions (policies).</p> <p>Central management tool for SafeGuard Enterprise protected endpoints, used for managing keys and certificates, users and computers, and for creating SafeGuard Enterprise policies. The SafeGuard Management Center communicates with the SafeGuard Enterprise Database. .NET Framework 4.5 is required.</p> <p>Installation package: SGNManagementCenter.msi</p>
	<p>Multi tenancy mode</p> <p>MTM</p> <p>The SafeGuard Management Center installation package comes with an option to install it in multi tenancy mode.</p> <p>If you do so, it supports multiple databases by using tenant-specific database configurations (Multi Tenancy). You can set up and maintain different SafeGuard</p>

	<p>Enterprise Databases for different tenants such as company locations, organizational units or domains.</p> <p>For each database (tenant), you need to set up a separate SafeGuard Enterprise Server instance. Each database must be the same version. For example, it is not possible to manage SGN 7 databases and SGN 8.3 databases with a single SGN 8.3 Management Center.</p>
DB	<p>SafeGuard Enterprise Database</p> <p>The SafeGuard Enterprise Database(s) hold all relevant data such as keys/certificates, information about users and computers, events and policy settings. The database needs to be accessed by the SafeGuard Enterprise Server and by only one security officer through the SafeGuard Management Center, usually the Master Security Officer. The SafeGuard Enterprise Database(s) can be generated and configured using a wizard or scripts.</p> <p>You can create the database during the initial configuration of the SafeGuard Management Center using a wizard or via script and establish the connection between SafeGuard Management Center, database and SafeGuard Enterprise Server manually.</p>

- **Microsoft Active Directory Services** (optional):

You can import your company's organizational structure with users and computers from Active Directory.

Windows endpoints	WinClient
SafeGuard Enterprise provides installer packages for full disk encryption and file encryption.	
Depending on your requirements you can choose from several file encryption packages. You have to decide whether you want to encrypt all files saved by specific applications anywhere on the computer (application-based) or if you want to encrypt files in certain locations only (location-based).	
You cannot install Synchronized encryption (application-based) and the location-based file encryption packages (CS, FE, DX) on one computer.	
SafeGuard Enterprise protected endpoints can either be connected to a SafeGuard Enterprise Server (managed) or they are operated without any connection to a SafeGuard Enterprise Server (unmanaged). Managed endpoints receive their policies directly from the SafeGuard Enterprise Server. Unmanaged endpoints receive their policies and policy updates inside configuration packages that have to be installed on the computers.	

CBM	Client Base Module The Client Base Module provides the required core services and authentication modules.
BL	BitLocker (Windows Native Device Encryption) Allows you to manage BitLocker on Windows 8.1 and Windows 10 endpoints.
SyncEnc	Synchronized Encryption Encrypts files regardless of where they are stored. (application-based). You can define a list of applications which files are encrypted automatically.
CS	Cloud Storage Offers file-based encryption of data stored in the cloud (location-based).
FE	File Encryption Offers location-based file encryption on local drives and network locations, mainly for work groups on network shares.
DX	Data Exchange Offers file-based encryption of data stored on removable media connected to a computer and allows to securely exchange this data with other Windows users.

macOS endpoints macClient	
SafeGuard Enterprise provides installer packages for managing FileVault 2 full disk encryption and for file encryption. If you want to encrypt files and share them with Windows endpoints, you have to use SafeGuard File Encryption for macOS.	
FV2	FileVault 2 (SafeGuard Native Device Encryption for Mac) Allows you to manage FileVault2 on Macs.
macOSFE	SafeGuard File Encryption Offers file-based encryption on local drives, network shares, removable drives, and in the cloud.

With SafeGuard File Encryption for Mac, you can safely encrypt and decrypt files and exchange these files with other users on Macs or Windows PCs.

To read files encrypted by SafeGuard Enterprise on mobile devices, use Sophos Secure Workspace for iOS or Android.

Recommendations for practice operation

In order to ensure high-performance operation, you should consider the following when positioning the components in the network:

- The SafeGuard Enterprise Management Center should be positioned as close to the SQL database as possible.
- The same applies to the SafeGuard Enterprise Server.
- Both components should have the ability to access a domain controller at the same network location to ensure fast synchronization between Active Directory and SafeGuard Enterprise.

2.2 *Getting started*

This section guides you through a typical SafeGuard Enterprise installation with best practice examples and recommendations. It is designed for system/network/database administrators installing SafeGuard Enterprise (SGN) and describes a setup that is focused on the best possible security and performance with regards to the communication between the single components.

The document describes a domain situation in which all machines are members of the same domain. As a result of this, specific tasks may differ when using a workgroup environment.

- First-time installation: The SGN Install Advisor simplifies the first time installation of the management components including default policies. To launch the SGN Install Advisor for a new SafeGuard Enterprise installation, start SGNInstallAdvisor.bat from your product delivery. A wizard guides you through installation.
- Update installation: Follow the steps described here: [About upgrading \(page 77\)](#).

2.2.1 *What are the key steps?*

Before you can deploy any SafeGuard Enterprise client, a working backend is required. Consequently, we recommend adhering to the installation steps described below.

You find all SafeGuard Enterprise components (.msi packages) in the product delivery.

Step	Description	Package to be installed / tool to be used
1	<p>Check system requirements</p> <p>See the current release notes on the SafeGuard release notes landing page for hardware and software requirements, service packs and disk space required during installation as well as for effective operation.</p>	N/A
2	<p>Download installers</p> <p>Use the web address and download credentials provided by your system administrator, go to the Sophos website and download the installers. Store them in a location where you can access them for installation.</p> <p>For more information, see Sophos knowledge base article 111195.</p>	N/A
3	<p>Make sure that the Windows server has the latest Windows updates applied.</p> <p>Install .NET Framework and ASP.NET 4.6.1.</p>	N/A
4	<p>Set up Internet Information Services (IIS) for SafeGuard Enterprise, see Installing and configuring Microsoft Internet Information Services (IIS) (page 23) and install the <i>Basic Authentication</i> role.</p>	N/A
	<p>For Basic Authentication role, see the Microsoft document Basic Authentication.</p> <p>Make sure that .NET Framework 4.5 is installed on all computers where you install SafeGuard Enterprise components.</p>	
5	Install SafeGuard Enterprise Server.	SGNServer.msi
6	Configure Microsoft SQL Server database authentication for the SafeGuard Enterprise Master Security Officer, see Database authentication (page 27) .	N/A

Step	Description	Package to be installed / tool to be used
7	<p>Optional: Generate the SafeGuard Enterprise Database(s) with a script.</p> <p>The SafeGuard Management Center Configuration Wizard can create the database automatically after the installation of the SafeGuard Management Center (step 9).</p>	Scripts in product delivery
8	Install the SafeGuard Management Center for central management of users, computers, policies, keys, and reports.	SGNManagementCenter.msi
9	Configure SafeGuard Management Center: database and database server connections, certificates, Master Security Officer credentials.	SafeGuard Management Center Configuration Wizard
10	Register and configure SafeGuard Enterprise Server: Create server configuration package and deploy it on the web server.	SafeGuard Management Center Configuration Package Tool
11	Create the organizational structure from Active Directory or manually.	SafeGuard Management Center
12	Prepare endpoints for encryption.	SGxClientPreinstall.msi
13	Create initial client configuration package for endpoint configuration.	SafeGuard Management Center Configuration Package Tool
14	Install encryption software and initial configuration package on endpoints.	For available packages, see About managed and unmanaged endpoints (page 57) .

2.2.2 Compatibility with other Sophos products

This section describes the compatibility of SafeGuard Enterprise with other Sophos products.

2.2.2.1 Compatibility with Sophos Central

- SafeGuard Enterprise Device Encryption cannot coexist with Sophos Central Device Encryption on Windows endpoints and Macs.
- SafeGuard Enterprise 8.3 File Encryption can coexist with Sophos Central Device Encryption on Windows endpoints and Macs.

2.2.2.2 Compatibility with SafeGuard LAN Crypt

SafeGuard Enterprise 8.3 cannot coexist with SafeGuard LAN Crypt on one endpoint.

2.2.2.3 Compatibility with Sophos Enterprise Console

If you use Sophos Enterprise Console (SEC) to manage encryption, do not install the SafeGuard Enterprise Server and its subcomponents Web Helpdesk and Server Task Scheduler or a SafeGuard Management Center on the server where the SEC management server is installed.

2.2.2.4 Compatibility with Sophos Mobile

SafeGuard Enterprise collaborates with Sophos Mobile by sharing a common key ring. This means that users can securely access files that are encrypted with any SGN key on their mobile devices. Conversely, users can create files on their Secure Workspace app and open them on an SGN-protected computer.

Prerequisites:

- Register the Sophos Mobile server with its certificate at the SGN server in the Management Center (**Tools > Configuration Package Tool > Servers**).
- Establish a secure SSL/TLS connection between the servers. We strongly recommend using TLS 1.2 encryption protocol to avoid known SSL attacks.
- Use Active Directory so mobile users can be identified in SGN via their AD information.

2.3 *Setting up SafeGuard Enterprise Server*

The SafeGuard Enterprise Server acts as the interface to the SafeGuard Enterprise Clients. Like the SafeGuard Management Center, it accesses the database. It runs as an application on a web server based on Microsoft Internet Information Services (IIS). Make sure you use the most recent version of IIS with the latest updates applied.

For ideal security and performance, we recommend that you install SafeGuard Enterprise Server on a dedicated machine. This also ensures that other applications cannot conflict with SafeGuard Enterprise.

SafeGuard Enterprise Server also includes the Task Scheduler to create and schedule periodic tasks that can be based on scripts. The tasks are automatically run on the SafeGuard Enterprise Server. You find several scripts for different use cases in the SafeGuard Enterprise product delivery. You can use these as templates for your environment.

Starting with version 8.1 the SafeGuard Enterprise Web Helpdesk is part of the SGNServer.msi install package, see [Web Helpdesk \(page 412\)](#).

2.3.1 Prerequisites

The following prerequisites must be met:

- You need Windows administrator rights.
- Microsoft Internet Information Services (IIS) must be available.
IIS is available for download on the Microsoft website.
- If you use SSL transport encryption between SafeGuard Enterprise Server and SafeGuard Enterprise client, you have to set up the IIS for it in advance, see [Securing transport connections with SSL \(page 45\)](#).
 - A certificate must be issued and the IIS server configured to use SSL and point to the certificate.
 - The server name specified when configuring the SafeGuard Enterprise Server must be the same as the one specified in the SSL certificate. Otherwise, client and server cannot communicate. Alias DNS names are not supported because they may conflict with the SSL implementation.
 - For each SafeGuard Enterprise Server, a separate SSL certificate is needed.

If you manage Windows and macOS endpoints, SSL certificates should be issued by a CA since starting with macOS 10.12 Apple does no longer allow self signed certificates for SSL connections.

- If you use Network Load Balancer, make sure that the port range includes the SSL port.
- .NET Framework 4.5 and ASP.NET 4.5 (provided in the SafeGuard Enterprise product delivery) must be installed.

2.3.2 *Installing and configuring Microsoft Internet Information Services (IIS)*

The section explains how to prepare Microsoft Internet Information Services (IIS) to run with SafeGuard Enterprise Server.

2.3.2.1 Install and configure IIS 7/7.5 on Microsoft Windows Server 2008 R2

IIS is available for download on the Microsoft website.

1. On the **Start** menu, click **All Programs > Administrative Tools > Server Manager**.
2. In the **Server Manager**, click **Roles > Add Roles**.
3. In the **Add Roles Wizard**, on the **Before you Begin** page, verify the following:
 - The administrator account has a strong password.
 - The network settings, for example IP addresses, are configured.
 - The latest security updates from Windows Update are installed.
4. Select **Select Roles** on the right, and then select **Web server (IIS)**. On the next page, click **Add Required Features**. **Web Server (IIS)** is listed in the navigation area of the **Add Roles Wizard**.
5. Click **Web Server (IIS)**, then click **Roles Services**. Keep the default roles services.
6. On the right, additionally select the following: **ASP.NET**, which also selects the necessary sub-role services.
7. Select **IIS Management Scripts and Tools** that is needed for correct IIS configuration.
8. Click **Next > Install > Close**.

IIS is installed with a default configuration for hosting ASP.NET.

9. Check that the web page is displayed properly using `http://< server name>`. For further information, see: <http://support.microsoft.com>.

Check .NET Framework registration on IIS 7

.NET Framework version 4.5 is required. You can find the program in the SafeGuard Enterprise product delivery.

To check whether it is installed correctly on IIS 7:

1. From the **Start** menu, select **Run....**
2. Enter the following command: Appwiz.cpl. All programs installed on the computer are displayed.
3. Check if .NET Framework Version 4.5 is displayed. If it is not displayed, install this version. Follow the steps in the installation wizard and confirm all defaults.
4. To test that the installation is correctly registered, go to C:\Windows\Microsoft.NET\|Framework. Each installed version must be visible as a separate folder showing the version as folder name, for example "v 4.5".

Check ASP.NET registration on IIS 7

ASP.NET Version 4.5 is required.

To check that ASP.NET is installed and registered with the correct version, enter the command **aspnet_regiis.exe -lv** at the command prompt.

Version 4.5 should be displayed for ASP.NET.

2.3.2.2 Install and configure IIS 8 on Microsoft Windows Server 2012/2012 R2 and Windows Server 2016

IIS is available for download on the Microsoft website.

1. On the **Server Manager Dashboard**, select **Manage > Add Roles and Features**.
2. In the **Add Roles and Features Wizard**, on the **Before you Begin** page, verify the following:
 - The administrator account has a strong password.
 - The network settings, for example IP addresses, are configured.
 - The latest security updates from Windows Update are installed.
3. Select **Server Roles** on the left hand pane and then select **Web server (IIS)**. Click **Add Features** in the displayed window. **Web Server Role (IIS)** is listed on the left hand pane of the **Add Roles and Features Wizard**.

4. In the left hand pane select **Role Services** under **Web Server Role (IIS)**. Keep the default roles services.
5. Scroll down to the **Application Development** node and select:
 - **ASP.NET 4.5**
 - **ISAPI Extensions**
 - **ISAPI Filters**

Necessary sub-role services are selected automatically.

6. Under the **Security** node, select:

- **Basic Authentication**
- **Windows Authentication**

7. Click **Next > Install > Close**.

IIS is now installed with a default configuration for hosting ASP.NET on the Windows Server.

Confirm that the web server works using [http://\(Enter machine name without brackets\)](http://(Enter machine name without brackets)). If the web page is not shown properly, please consult the Microsoft Knowledge Base (<http://support.microsoft.com>) for further information.

2.3.3 Install SafeGuard Enterprise Server

After the IIS is configured, you can install SafeGuard Enterprise Server on the IIS server. You can find the install package SGNServer.msi in the product delivery. It allows you to install the following modules:

- the server
- the Scheduler Service (optional)
- the Web Helpdesk (optional)

1. On the server where you want to install SafeGuard Enterprise Server, double-click SGNServer.msi. A wizard guides you through the necessary steps.
2. Select the additional components to be installed:
 - **Task Scheduler**

Task Scheduler is automatically installed with an installation of type **Typical**.

- **Web Helpdesk**

Starting with version 8.1 the SafeGuard Enterprise Web Helpdesk is part of the SGNServer.msi install package, see [Web Helpdesk \(page 412\)](#).

3. Click **Install**.

SafeGuard Enterprise Server and selected additional components are installed.

To ensure that the installation has completed successfully, open the **Internet Information Services Manager** (run `inetmgr`) and check if a web page named SGNSRV is now available.

2.3.3.1 Logged events on the server

After installation of SafeGuard Enterprise Server, the connection of logged events is deactivated for the SafeGuard Enterprise Database by default in order to enhance performance. However, the connection of logged events is necessary for integrity protection of logged events. All entries in the event table are concatenated so that if an entry is removed this is evident and can be verified with an integrity check. To make use of integrity protection, you need to set the connection of logged events manually. For further information, see [Reports \(page 208\)](#).

You have to install a SafeGuard client installation package to enable the server to forward events to the SafeGuard Enterprise Database

2.4 *Setting up SafeGuard Enterprise Database*

SafeGuard Enterprise stores all relevant data such as keys, certificates, information about users and computers, events, and policy settings in a database. The SafeGuard Enterprise Database is based on Microsoft SQL Server.

Check the list of currently supported SQL Server types in the system requirements section of the current [release notes](#).

When using the SQL Express Edition, remember the maximum file size limitation of the database given by Microsoft. In large environments, using the SQL Express Edition might be inappropriate.

You can set up the database either automatically during first-time configuration in the SafeGuard Management Center or manually using the SQL scripts provided in your product delivery. Depending on your enterprise environment, check which method to choose. In both cases, you must first make sure that you have the necessary database access rights, see [Database access rights \(page 27\)](#).

Multiple SafeGuard Enterprise Databases can be created and maintained for different tenants such as different company locations, organizational units or domains (multi tenancy). For multi tenancy

mode all tenants must have installed the same version of SafeGuard Enterprise. To configure multi-tenancy, see [Working with multiple database configurations \(Multi Tenancy\) \(page 109\)](#).

To communicate to SQL over a firewall, TCP/IP ports 1433 and 1434 are required.

2.4.1 Database authentication

To access the SafeGuard Enterprise Database, the SafeGuard Management Center's first security officer must be authenticated at the SQL Server. This can be done in the following ways:

- Windows authentication: promote an existing Windows user to SQL user
- SQL authentication: create an SQL user account

Find out from your SQL administrator which authentication method is appropriate for you, as a security officer. You need this information before generating the database and before first-time configuration in the SafeGuard Management Center Configuration Wizard.

Use SQL authentication for computers that are not part of a domain, but otherwise use Windows authentication. If you use SQL authentication, we highly recommend that you secure the connection to and from the database server with SSL. For further information, see [Securing transport connections with SSL \(page 45\)](#).

2.4.1.1 Database access rights

SafeGuard Enterprise is set up in such a way that, to work with the SQL database, it only needs a single user account with minimum access rights for the database.

The SafeGuard Enterprise Database can either be created manually or automatically during first-time configuration in the SafeGuard Management Center. If it is created automatically, extended access rights for the SQL database (db_creator) are needed for the first SafeGuard Management security officer. However, these rights can be revoked afterwards by the SQL administrator until the next install/update.

While SafeGuard Enterprise is running, a single SafeGuard Management Center security officer only needs read/write permission for the SafeGuard Management Center Database.

If extending permissions during SafeGuard Management Center configuration is undesirable, the SQL administrator can generate the SafeGuard Enterprise Database with a script. The two scripts included in the product delivery, **CreateDatabase.sql** and **CreateTables.sql**, can be run for this purpose.

The following table shows the necessary SQL permissions for Microsoft SQL Server.

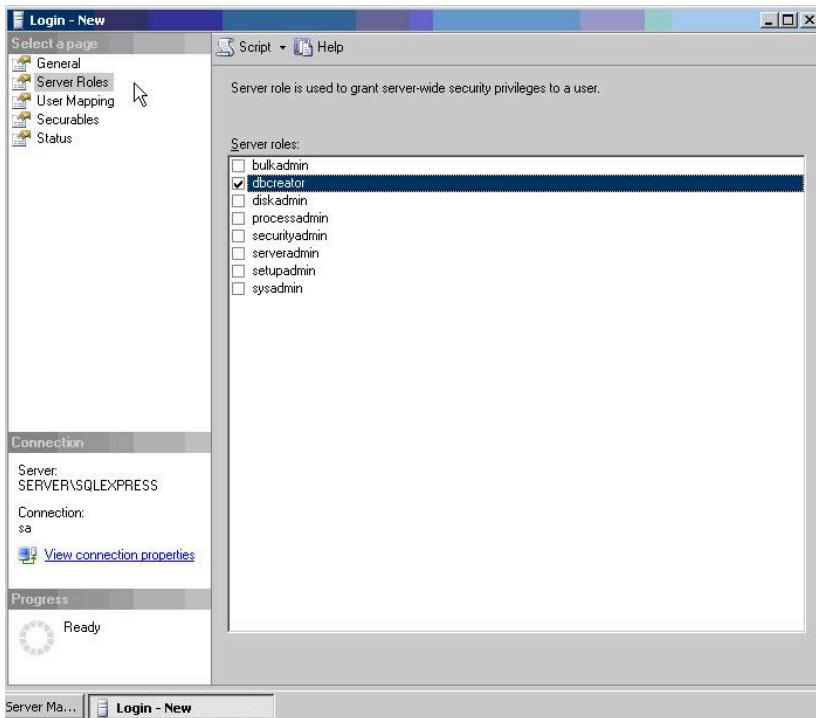
SQL Server	Access Right
Create database	
Server	db_creator
Master database	None
SafeGuard Enterprise Database	db_ownerpublic (default)
Use database	
Server	None
Master database	None
SafeGuard Enterprise Database	db_datareader db_datawriter public (default)

2.4.1.2 Configure a Windows account for SQL Server logon

The description of the individual configuration steps below is aimed at SQL administrators and relates to Microsoft Windows Server 2008 R2 and Microsoft SQL Server Standard or Express Edition.

As an SQL administrator, you need the right to create user accounts.

1. Open SQL Server Management Studio. Log on to the SQL Server with your credentials.
2. Open the **Object Explorer**, right-click **Security**, point to **New** and then click **Login**.
3. In **Login - New** on the **General** page, select **Windows authentication**.
4. Click **Search**. Find the respective Windows user name and click **OK**. The user name is displayed as **Login name**.
5. In **Default Database**, if a script has not been used to create a SafeGuard Enterprise Database yet, select **Master**.
6. Click **OK**.
7. To create the database automatically during SafeGuard Management Center first-time configuration, you have to change the access rights as follows: In **Login - New**, assign the access rights/roles by clicking **Server Roles** on the left. Select **dbcreator**. Once SafeGuard Enterprise has been installed, the database role can be reset to **dbowner**.



2.4.1.3 Create an SQL account for SQL Server logon

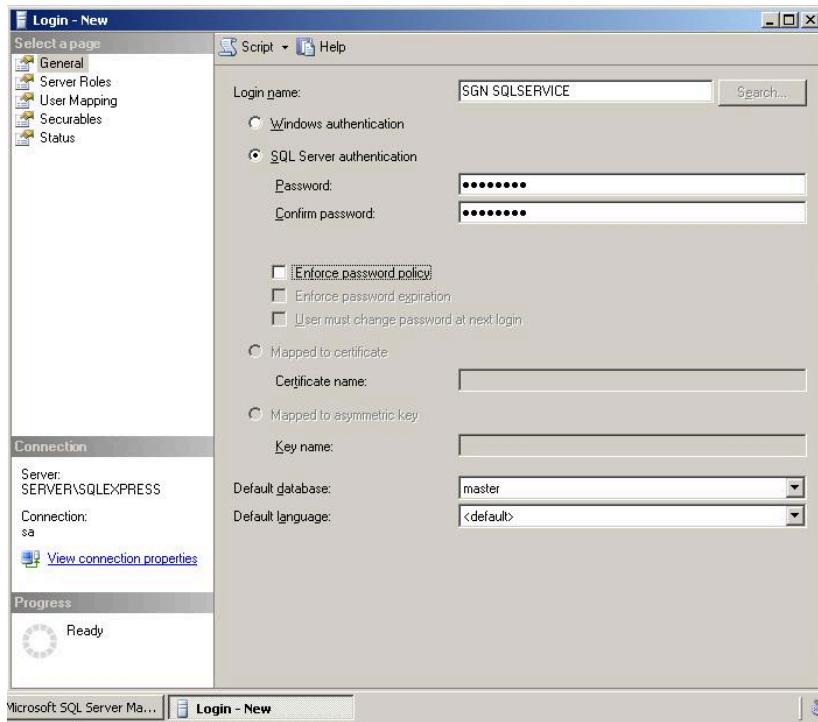
Every user that should be able to use the SafeGuard Management Center must have a valid SQL User account when using Windows authentication to connect to the SafeGuard database.

The description of the individual configuration steps below is aimed at SQL administrators. It relates to Microsoft Windows Server 2008 R2 with Microsoft SQL Server Standard Edition.

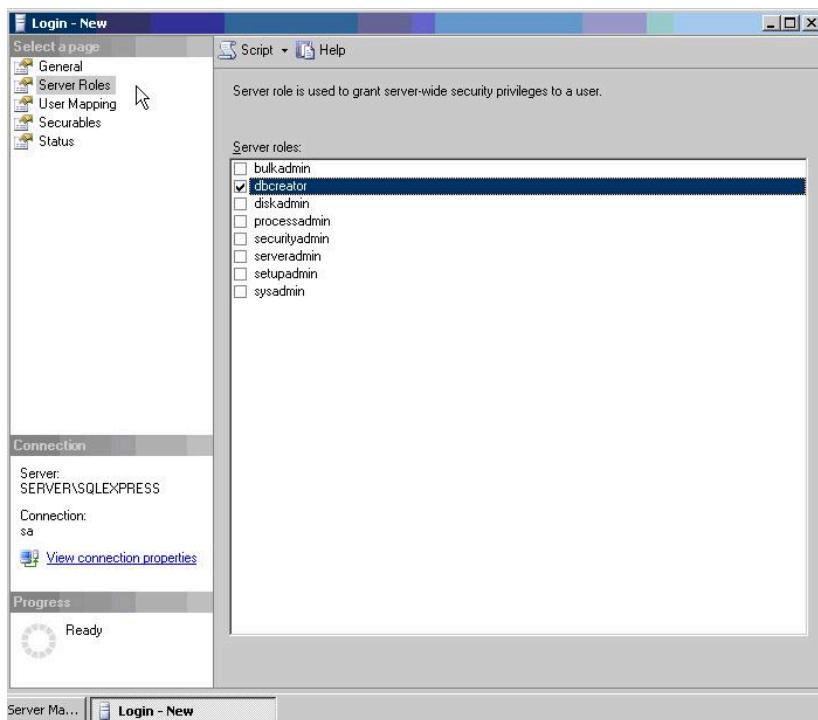
As an SQL administrator, you need the right to create an SQL user account.

1. Open SQL Server Management Studio. Log on to the SQL Server with your credentials.
2. Open the **Object Explorer**, right-click **Security** and select **New > Login**.
3. In **Login - New** on the **General** page, select **SQL Server authentication**.
4. On the **General** page, in **Login name**, do the following:
 - a. Enter the name of the new user, for example SGN SQLSERVICE.
 - b. Enter and confirm a password for the account.
 - c. Clear **Enforce password policy**.
 - d. In **Default Database**, if a script has not been used to create a SafeGuard Enterprise Database yet, select **Master**. Click **OK**.

Take a note of the authentication method and the credentials. You have to inform the SafeGuard Management Center security officer about them.



5. To create the database automatically during SafeGuard Management Center first-time configuration, you have to change the access rights as follows: In **Login - New** on the **General** page, assign the access rights/roles by clicking **Server Roles** on the left. Select **dbcreator**. Once SafeGuard Enterprise has been installed, the database role can be reset to **dbowner**.



The SQL user account and the access rights are now set up for the SafeGuard Enterprise security officer.

2.4.2 Generating the SafeGuard Enterprise Database

After setting up the user account for the SQL Server logon you need to generate the SafeGuard Enterprise Database. There are two ways to do so:

- Using SafeGuard Management Center Configuration Wizard

As a security officer, you can easily create the SafeGuard Enterprise Database during first-time configuration in the SafeGuard Management Center. The SafeGuard Management Center Configuration Wizard takes you through the basic configuration, which also includes database creation. To do so, install and configure SafeGuard Management Center, see [Setting up SafeGuard Management Center \(page 35\)](#), and then change the relevant access rights, see [Change access rights for the SafeGuard Enterprise Database \(page 32\)](#).

- Using SQL scripts provided in the product delivery

This procedure is preferable if extended SQL permissions during SafeGuard Management Center configuration are not desirable.

It depends on your enterprise environment which method should be applied. It is best to agree this between SQL administrator and SafeGuard Enterprise security officer.

2.4.2.1 Prerequisites

The following prerequisites must be met:

- Microsoft SQL Server must already be installed and configured. Microsoft SQL Express Edition is suitable for use in smaller companies, as there are no license fees.
- For performance reasons Microsoft SQL Server should not be installed on the computer on which SafeGuard Enterprise Server is installed.
- Database authentication methods and database access rights should be clarified.

2.4.2.2 Generate SafeGuard Enterprise Database with a script

If you want to create the SafeGuard Enterprise Database automatically during SafeGuard Management Center configuration, you can skip this step. If extended SQL permissions during SafeGuard Management Center configuration are not desirable, carry out this step. Two database scripts are provided in the product delivery (Tools folder) for this purpose:

- CreateDatabase.sql
- CreateTables.sql

The description of the steps below is aimed at SQL administrators and relates to Microsoft SQL Server Standard Edition.

As SQL administrator, you need to have the right to create a database.

1. Copy the scripts CreateDatabase.sql and CreateTables.sql from the SafeGuard Enterprise product delivery to the SQL Server.
2. Double-click the **CreateDatabase.sql** script. Microsoft SQL Server Management Studio is launched.
3. Log on to the SQL Server with your credentials.
4. Check that the two target paths at the beginning of the script, under **FILENAME** (MDF, LDF), exist on the local hard drive. Correct them if necessary.
5. Click **Execute** from the toolbar to generate the database. You have created the database **SafeGuard**. Next use the CreateTables.sql script in the product delivery to generate the tables.
6. Double-click **CreateTables.sql**. A further pane is opened in Microsoft SQL Server Management Studio.
7. At the top of the script, enter use SafeGuard to select the SafeGuard Enterprise Database in which the tables are to be created.
8. Click **Execute** from the Toolbar to generate the tables.

The SafeGuard Enterprise Database and the associated tables have been created.

2.4.3 Change access rights for the SafeGuard Enterprise Database

When the SafeGuard Enterprise Database has been created, the user account must be granted access to the database. These access rights are required for all security officers who work with the SafeGuard Management Center when Windows NT authentication is used. As it is possible to assign different roles and permissions to a user on a database, only the minimum required ones are described.

1. Open the SQL Server Management Studio. Log on to the SQL Server with your credentials.
2. Open the **Object Explorer**, double-click **Security**, and then double-click **Logins**.

3. Right-click the respective user name and click **Properties**.
4. Select **User Mapping** on the left. Under **Users mapped to this login**, select the database **SafeGuard**.
5. Under **Database role membership for** set the minimum access rights to use the SafeGuard Enterprise Database: select **db_datareader**, **db_datawriter** and **public**.
6. Click **OK**.

2.4.4 Check SQL Services, named pipes, and TCP/IP settings

In order to install the SafeGuard Management Center, it is required that the SQL Browser Service is running and that **Named Pipes** and **TCP/IP** are enabled. These settings are required to access the SQL server from other machines. This can be checked in the **SQL Server Configuration Manager**. The description relates to Microsoft Windows Server 2008 (R2) and Microsoft SQL Server 2012 Standard or Express Edition.

1. Open **SQL Server Configuration Manager**.
2. From the navigation tree on the left, select **SQL Server Services**.
3. Make sure that the **State** of both **SQL Server** and **SQL Server Browser** is **Running** and that **Start mode** is set to **Automatic**.
4. From the navigation tree on the left, select **SQL Server Network Configuration** and select the current instance.
5. Right-click the protocol **Named Pipes** and click **Enabled**.
6. Right-click the protocol **TCP/IP** and click **Enabled**.
7. Additionally, right-click the protocol **TCP/IP** and click **Properties**. On the **IP Addresses** tab, under **IPAll**, leave **TCP Dynamic Ports** blank. Set **TCP Port** to **1433**.
8. Restart the SQL Services.

2.4.5 Create Windows Firewall rule on Windows Server

This section relates to Microsoft Windows Server with Microsoft SQL Server 2012 Standard or Express Edition. When you use this configuration, carry out the steps below to ensure that a connection between SafeGuard Enterprise Database and SafeGuard Management Center can be established.

1. On the computer hosting the SQL Server instance, click **Start**, select **Administrative Tools** and then click **Windows Firewall with Advanced Security**.
2. From the navigation tree on the left, select **Inbound Rules**.
3. Click **Action** from the menu bar, and then click **New Rule**. The **New Inbound Rule Wizard** is launched.
4. On the **Rule Type** page, select **Custom** and click **Next**.
5. On the **Program** page, select the program and services this rule should apply to, and then click **Next**.

6. On the **Protocol and Ports** page, select **TCP** as **Protocol type**. For **Local port**, select **Specific Ports** and enter **1433, 1434**. For **Remote Port**, select **All Ports**. Click **Next**.
7. On the **Scope** page, you can specify that the rule applies only to network traffic to or from the IP addresses entered on this page. Configure as appropriate, and then click **Next**.
8. On the **Action** page, select **Allow the connection**, and click **Next**.
9. On the **Profile** page, select where to apply the rule, and click **Next**.
10. On the **Name** page, type a name and description for your rule, and click **Finish**.

2.4.6 Configure Windows authentication for SQL Server logon

This section relates to Microsoft Windows Server with Microsoft SQL Server 2012 Standard Edition and IIS 7.

To enable communication between SafeGuard Enterprise Server and SafeGuard Enterprise Database when using Windows authentication, the user must be made a member of Active Directory groups. Local file permissions must be adjusted, and the SQL user account must be populated to the Application Pool of the IIS.

1. Select **Start** and then **Run**. Enter **dsa.msc**. Open the Active Directory Users and Computers snap-in.
2. In the navigation tree on the left, expand the domain tree and select **Builtin**.
3. Add the respective Windows user to the following groups: **IIS_IUSRS**, **Performance Log Users**, **Performance Monitor Users**.
4. Exit the snap-in.
5. On the local file system, in Windows Explorer, right-click the **C:\Windows\Temp** folder and select **Properties**. In **Properties**, select the **Security** tab.
6. In **Security**, click **Add**, and enter the respective Windows user name in the **Enter the object names to select** field. Click **OK**.
7. In **Security**, under **Permissions** click **Advanced**. In **Advanced Security Settings for Temp** dialog, on the **Permission** tab, click **Edit**. Then set the following permissions in the **Object** dialog to **Allow: List folders / read data, Create files / write data, Delete**.
8. Click **OK**, exit **Temp Properties** and then Windows Explorer.
9. Open **Internet Information Services Manager**.
10. In the **Connections** pane on the left, select **Application Pools** of the relevant server node.
11. From the **Application Pools** list on the right, select **SGNSRV-Pool**.
12. In the **Actions** pane on the left, select **Advanced Settings**.
13. In **Advanced Settings**, under **Process Model**, for the **Identity** property, click the **...** button.
14. In **Application Pool Identity**, select **Custom account** and click **Set**.
15. In **Set Credentials**, type the relevant Windows user name in the following form: **Domain \<Windows user name>**. Type and confirm the respective Windows password and then click **OK**.
16. In the **Connections** pane on the left, select the relevant server node and click **Restart** from the **Actions** pane.

17. In the **Connections** pane on the left, under the relevant server node, under **Sites, Default Web Sites**, select **SGNSRV**.
18. On the SGNSRV home page, double-click **Authentication**.
19. Right-click **Anonymous authentication** and select **Edit**.
20. For **Anonymous user identity**, select **Specific user** and check that the user name is **IUSR**.
Correct it, if necessary.
21. Click **OK**.

Additional configuration when using a Windows account for SQL Server logon is now completed.

2.5 *Setting up SafeGuard Management Center*

This section describes how to install and configure SafeGuard Management Center.

SafeGuard Management Center is the central administrative tool for SafeGuard Enterprise. You install it on the administrator computers that you intend to use for managing SafeGuard Enterprise. SafeGuard Management Center can be installed on any computer on the network from which the SafeGuard Enterprise Databases can be accessed.

SafeGuard Management Center supports multiple databases by using tenant-specific database configurations (Multi Tenancy). You can set up and maintain different SafeGuard Enterprise Databases for different tenants such as company locations, organizational units or domains. To make management easier, these database configurations can also be exported to and imported from files.

2.5.1 *Prerequisites*

The following prerequisites must be met:

- Make sure that you have Windows administrator rights.
- .NET Framework 4.5 or higher must be installed. It is provided in the SafeGuard Enterprise product delivery.
- If you want to create a new SafeGuard Enterprise Database during SafeGuard Management Center configuration, you need the necessary SQL access rights and credentials, see [Database access rights \(page 27\)](#).

2.5.2 Install SafeGuard Management Center

1. Start SGNManagementCenter.msi from the install folder of your product delivery. A wizard guides you through the necessary steps.
2. Accept the defaults in the subsequent dialogs except as follows: On the **Select Installation Type** page, do one of the following:
 - For SafeGuard Management Center to support one database only, select **Typical**.
 - The **Custom** option allows users to choose which features will be installed.
 - For SafeGuard Management Center to support multiple databases (**Multi Tenancy**), select **Complete**. For further information, see [Working with multiple database configurations \(Multi Tenancy\) \(page 109\)](#).

SafeGuard Management Center is installed. If necessary, restart your computer. Next you carry out initial configuration in the SafeGuard Management Center.

2.5.3 Configuring SafeGuard Management Center

The SafeGuard Management Center Configuration Wizard provides help with specifying the basic SafeGuard Management Center settings and the database connections during the initial configuration. The wizard opens automatically when you start the SafeGuard Management Center for the first time after installation.

The SafeGuard Management Center **Help** provides context-sensitive help as well as a full-text search. It is configured for full functionality of the help system content pages with JavaScript enabled in your browser. If JavaScript is disabled, you can still display and navigate the SafeGuard Management Center help system. However, certain functionality such as the search cannot be displayed.

2.5.3.1 Prerequisites

The following prerequisites must be met:

- Make sure that you have Windows administrator rights.
- The firewall must be configured properly.
- Have the following information at hand. Where necessary, you can obtain this information from your SQL administrator.
 - SQL credentials.

- The name of the SQL Server which the SafeGuard Enterprise Database is to run on.
- The name of the SafeGuard Enterprise Database, if it has already been created.

2.5.3.2 Start initial SafeGuard Management Center configuration

After installation of the SafeGuard Management Center, you need to carry out initial configuration. You need to do so in Single Tenancy as well as in Multi Tenancy mode.

To start the SafeGuard Management Center Configuration Wizard:

1. Select **SafeGuard Management Center** from the **Start** menu. The Configuration Wizard is launched and guides you through the necessary steps.
2. On the **Welcome** page, click **Next**.

2.5.3.3 Configure the database server connection

A database is used to store all SafeGuard Enterprise specific encryption policies and settings. For the SafeGuard Management Center and the SafeGuard Enterprise Server to be able to communicate with this database, you must specify an authentication method for the database access, either Windows NT authentication or SQL authentication. If you want to connect to the database server with SQL authentication, make sure that you have the required SQL credentials at hand. Where necessary, you may obtain this information from your SQL administrator.

On the **Database Server Connection** page, do the following:

1. Under **Connection settings**, select the SQL database server from the **Database Server** list. All computers on a network on which a Microsoft SQL Server is installed are listed. If you cannot select the server, enter the server name or IP address with the SQL instance name manually.
2. Select **Use SSL** to secure the connection between SafeGuard Management Center and SQL database server. We strongly recommend that you do so if you select **Use SQL Server Authentication with the following credentials** under **Authentication**, because this setting will encrypt the transport of the SQL credentials. SSL encryption requires a working SSL environment on the SQL database server which you have to set up in advance, see [Securing transport connections with SSL \(page 45\)](#).
3. Under **Authentication**, select the type of authentication to be used to access the database server instance.
 - Select **Use Windows NT Authentication** to use your Windows credentials.

Use this type when your computer is part of a domain. However, additional mandatory configuration is required as the user needs to be authorized to connect to the database, see [Configure a Windows account for SQL Server logon \(page 28\)](#) and [Configure Windows authentication for SQL Server logon \(page 34\)](#).

- Select **Use SQL Server Authentication with the following credentials** to access the database with the relevant SQL credentials. Enter the credentials for the SQL user account that your SQL administrator has created. Where necessary, you may obtain this information from your SQL administrator.

 **Note** Use this type when your computer is not part of a domain. Make sure that you have selected **Use SSL** to secure the connection to and from the database server.

4. Click **Next**.

The connection to the database server has been established.

2.5.3.4 Create or select a database

On the **Database Settings** page, it is possible to either create a new database or to use an existing one. When the database has already been created by the SQL scripts, the wizard will automatically select the existing database. In this case, no further configuration is required.

If the database was not created beforehand, do the following:

1. Select **Create a new database named** and enter a name for the new database. To do this, you need the relevant SQL access rights, see [Database access rights \(page 27\)](#). SafeGuard Enterprise database names should only consist of the following characters to prevent localization issues: characters (A-Z, a-z), numbers (0-9), underscores (_).
2. Click **Next**.

2.5.3.5 Define Active Directory authentication

Before creating a new database, you can define all settings that are necessary to access an Active Directory. In this step, you define server name and user credentials.

We recommend that you provide the Active Directory credentials at this stage so that the base structure of the Active Directory can be imported automatically. This import includes all containers that are synchronized with the SafeGuard Enterprise database including organizational units and groups. No computers or users are imported with this initial directory import, but all keys are created and assigned to the corresponding containers. After the import, security officers can assign policies to different containers without executing a complete AD synchronization. Computers and users will receive their policies as soon as they are registered at the SGN server.

If you do not yet have your credentials, you may skip this step and you can manually configure your Active Directory import later.

For large enterprises with complex AD structures as well as for the handling of removed, changed, or moved objects, you need to use the **LDAP Authentication** wizard, see [Import an Active Directory structure \(page 148\)](#).

1. On the **Directory Authentication** page, enter the server name or IP address.
2. We recommend using SSL for securing the connection between the SafeGuard Enterprise Server and endpoints.
3. Define your user credentials.
4. Click **Next**.

After the SafeGuard Enterprise database has been created and the Initial Configuration wizard is complete, the base structure of the defined directory is imported to the database. All necessary keys are created and assigned to the corresponding containers.

2.5.3.6 Create the Master Security Officer (MSO)

As a security officer, you access the SafeGuard Management Center to create SafeGuard Enterprise policies and configure the encryption software for the users.

The Master Security Officer (MSO) is the top-level administrator with all the rights.

1. On the **Security Officer Data** page under **Master Security Officer ID**, enter a name for the Master Security Officer, for example, **MSO**.
2. Under **Certificate for Master Security Officer**, do one of the following:
 - [Create the Master Security Officer certificate \(page 39\)](#)
 - [Import the MSO certificate \(page 40\)](#)
 - [Export the MSO certificate \(page 40\)](#)

[Create the Master Security Officer certificate](#)

In **Create Master Security Officer Certificate**, you create a password for the personal certificate store. The SafeGuard Enterprise Certificate store is a virtual store for SafeGuard Enterprise certificates. This store is not related to Microsoft functionality. The password defined in this step is the password that is used to log on to the Management Center afterwards.

1. Under **Master Security Officer ID**, confirm the Master Security Officer name.
2. Enter a password for the certificate store twice and click **OK**.

The MSO certificate is created and saved locally (<mso_name>.cer).

We recommend that you make a note of the password and keep it in a safe place. You need it to access the SafeGuard Management Center.

Import the MSO certificate

If an MSO certificate is already available, you need to import it into the SafeGuard certificate store.

The certificate cannot be imported from a Microsoft PKI. An imported certificate must have a minimum of 1024 bits and a maximum of 4096 bits. We recommend a certificate length of at least 2048 bits.

1. In **Import authentication key file**, click [...] and select the key file.
2. Enter the password for the key file.
3. Enter the password for the certificate store.
4. Confirm the password for the certificate store.
5. Click **OK**.

Certificates and private keys are now contained in the certificate store. Logging on to SafeGuard Management Center then requires the password to the certificate store.

Export the MSO certificate

The MSO certificate is exported to a private key file (P12). In **Export certificate**, you define a password to protect this private key file. The private key file is needed to restore a broken SafeGuard Management Center installation.

To export an MSO certificate:

1. In **Export certificate**, enter and confirm a password for the private key (P12 file). The password must consist of 8 alphanumeric characters.
2. Click **OK**.
3. Enter a storage location for the private key file.

The private key is created and the file is stored in the defined location (mso_name.p12).

 **Important** Create a backup of the private key (p12 file) and store it in a safe place right after initial configuration. In case of PC failure the key is otherwise lost and SafeGuard Enterprise has to be reinstalled. This applies to all SafeGuard generated security officer certificates.

As soon as the security officer certificate is exported and the certificate store and the security officer are created, the wizard proceeds with the creation of the company certificate.

2.5.3.7 Create the company certificate

The company certificate is used to differentiate between SafeGuard Management installations. In combination with the MSO certificate, it allows you to restore a broken SafeGuard Enterprise Database configuration.

1. On the **Company Certificate** page, select **Create a new company certificate**.

2. Enter your company name.

 **Note** Certificates generated by SafeGuard Enterprise, such as the company, machine, security officer, and user certificates are signed with hash algorithm **SHA-256** for enhanced security in a first-time installation.

For endpoints with SafeGuard Enterprise older than 6.1, you must select **SHA-1** under **Hash algorithm for generated certificates**. For further information, see [Change algorithm for self-signed certificates \(page 165\)](#).

3. Click **Next**.

The newly created company certificate is stored in the database.

Create a backup of the company certificate and store it in a safe place right after initial configuration.

To restore a broken database configuration, see [Repair a corrupted database configuration \(page 108\)](#).

2.5.3.8 Complete initial SafeGuard Management Center configuration

Click **Finish** to complete the initial configuration of SafeGuard Management Center.

A configuration file is created.

You have created the following:

- A connection to the SafeGuard Enterprise Server.
- A SafeGuard Enterprise Database.
- A Master Security Officer account to log on to SafeGuard Management Center.

- All necessary certificates to restore a corrupt database configuration or SafeGuard Management Center installation.

SafeGuard Management Center is launched once the configuration wizard has closed, see [Logging on to the SafeGuard Management Center \(page 84\)](#).

2.5.4 Setting up the organizational structure in the SafeGuard Management Center

Note

Importing the organizational structure or creating it manually is only necessary if you skipped the initial import triggered by the SafeGuard Management Center Configuration Wizard.

There are two ways of mapping your organization in SafeGuard Enterprise:

- Importing an Active Directory structure.

During the synchronization with the Active Directory, objects such as computers, users, and groups are imported into the SafeGuard Management Center and stored in the SafeGuard Enterprise Database.

- Creating the company structure manually.

If there is no directory service available or if there are only few organizational units so that no directory service is needed, you can create new domains/workgroups which the user or computer can log on to.

You can use either one of these two options or combine them. For example, you can import an Active Directory (AD) either partially or entirely, and create other organizational units (OUs) manually.

When combining the two methods, the organizational units created manually are not mapped in the AD. If you want organizational units created in SafeGuard Enterprise to be mapped in the AD, you must add them to the AD separately.

For information on how to import or create an organization structure, see [Managing the organizational structure \(page 146\)](#).

2.5.4.1 Prevent deletion of domains, OU nodes and workgroups

You can configure SafeGuard Enterprise to prevent deletion of imported OU nodes. If configured this way only a Master Security Officer can delete OU nodes in the SafeGuard Management Center. The option is activated by default.

To prevent the deletion of OU nodes:

1. In the Management Center, select **Options** from the **Tools** menu.
2. Go to the **Directory** tab.
3. Activate the **Prevent deletion of domains, OU nodes and workgroups** option.
4. Click **OK**.

If an officer with insufficient rights tries to delete a domain, OU node or workgroup, a message is displayed, indicating that deletion of domains, OU nodes and workgroups is deactivated and has to be activated by a Master Security Officer or an officer with appropriate rights.

For logged events, see [Auditing \(page 204\)](#).

2.5.5 Importing the license file

SafeGuard Enterprise has an integrated license counter. When you download the product you can download a test license. This evaluation license includes five licenses for each module and needs to be imported into the SafeGuard Management Center. This enables the evaluation of other SafeGuard Enterprise components easily without any side effects. When purchasing SafeGuard Enterprise, every customer receives a personalized license file for their company which needs to be imported into the SafeGuard Management Center.

For further information, see [Licenses \(page 172\)](#).

2.6 Testing communication

When the SafeGuard Enterprise Server, the database, and the Management Center have been set up, we recommend running a connection test. This section contains the prerequisites and required settings for the connection test.

2.6.1 Ports/connections

The endpoints must create the following connections:

SafeGuard endpoint connection to	Port
SafeGuard Enterprise Server	Port 443 when using SSL transport connection Port 80/TCP  Note The ports must be open for bi-directional communication.

The SafeGuard Management Center must create the following connections:

SafeGuard Management Center connection to	Port
SQL database	SQL Server dynamic port: Port 1433/TCP and Port 1434/TCP
Active Directory	Port 389/TCP
SLDAP	Port 636 for the Active Directory import

The SafeGuard Enterprise Server must create the following connections:

SafeGuard Enterprise Server connection to	Port
SQL database	Port 1433/TCP and Port 1434/TCP for SQL (Express) dynamic port
Active Directory	Port 389/TCP

2.6.2 Authentication method

1. On the computer with SafeGuard Enterprise Server installed, open **Internet Information Services (IIS) Manager**.
2. In the tree structure, select the relevant server and click **Sites > Default Web Site > SGNSRV**.
3. Under **IIS**, double-click the **Authentication** icon and check the following settings:
 - Set **Anonymous Authentication** to **Enabled**.
 - Set **Windows Authentication** to **Disabled**.

2.6.3 Set proxy server settings

Set the proxy server settings for web server and endpoint as follows:

1. In Internet Explorer, on the **Tools** menu, click **Internet options**. Then click **Connections** and click **LAN settings**.
2. In **LAN Settings**, under **Proxy servers**, clear **Use a proxy server for your LAN**.

If a proxy server is required, click **Bypass proxy server for local addresses**.

2.6.4 Check connection

1. On the computer with SafeGuard Enterprise Server installed, open **Internet Information Services (IIS) Manager**.
2. In the tree structure, select the relevant server and click **Sites > Default Web Site > SGNSRV**.
3. Right-click **SGNSRV**, select **Manage Application** and click **Browse** to open the **Sophos SafeGuard Web Service** page.
4. On the **Sophos SafeGuard Web Service** page, a list of possible actions is displayed. Click **CheckConnection > Invoke**.

The following output indicates a successful connection test:

```
<DataRoot><WebService>OK</WebService><DBAuth>OK</DBAuth>
```

If communication between the SafeGuard Enterprise client and server is not working properly, see [Sophos knowledge base article 109662](#).

2.7 Securing transport connections with SSL

SafeGuard Enterprise supports encrypting the transport connections between its components with SSL. You can use SSL to encrypt transport between the following components:

- Database Server <-> SafeGuard Enterprise Server with IIS
- Database Server <-> SafeGuard Management Center
- SafeGuard Enterprise Server with IIS <-> managed endpoints

Before you activate SSL in SafeGuard Enterprise, you must set up a working SSL environment.

The following general tasks must be carried out for setting up SSL:

- Optional: install a Certificate Authority for issuing certificates used by SSL encryption.
- A certificate must be issued and the IIS server must be configured to use SSL and point to the certificate.
- The server name specified when configuring the SafeGuard Enterprise Server must be the same as the one specified in the SSL certificate. Otherwise client and server cannot communicate. For each SafeGuard Enterprise Server a separate certificate is needed.
- If you use Network Load Balancer, make sure that the port range includes the SSL port.

For further information, contact our technical support or see:

- The Microsoft document [How To Set Up an HTTPS Service in IIS](#)
- The Microsoft document [How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console](#)

SafeGuard specific transport encryption for test setups

For demo or test setups, you can alternatively secure the connection between the SafeGuard Enterprise Server and the SafeGuard Enterprise managed endpoints by SafeGuard specific encryption. For ideal security and performance, we strongly recommend that you use SSL encrypted communication. If, for some reason, this is not possible and SafeGuard-specific encryption is used, there is an upper limit of 1000 clients that connect to a single server instance.

 **Note** If you manage Macs, you must use SSL encryption.

2.7.1 Certificates

For securing the communication between the SafeGuard Enterprise Server and the SafeGuard Enterprise protected endpoint with SSL, a valid certificate is required. You can use the following certificate types:

A self-signed certificate

If you manage Mac and Windows endpoints, you have to use a certificate with proper key usage extensions. Starting with macOS 10.12, Apple only allows certificates that meet these requirements for establishing an SSL connection.

You can create a certificate with proper extensions in IIS when you configure the SGNSRV web page for SSL, see [Configure the SGNSRV web page for SSL \(page 48\)](#).

A certificate issued by a PKI with a private or a public root certificate

Technically it makes no difference whether you use a certificate with a public or a private root certificate.

If a certificate created by a public PKI is available but not the PKI infrastructure, you cannot use this certificate to secure communication with SSL. In this case you need to set up a PKI infrastructure or create a self-signed certificate.

If you want to use a PKI-generated certificate for SSL communication, create a certificate for the machine that is running the SafeGuard Enterprise Server. The following requirements apply:

- The certificate name must correspond to the machine that is shown at the top node in the Internet Information Services (IIS) Manager.
- The certificate must be issued to the machine using its FQDN name. Make sure that the client is capable of resolving the FQDN per DNS.

2.7.2 Activate SSL encryption in SafeGuard Enterprise

- Connection between web server and database server:

Activate SSL encryption when registering the SafeGuard Enterprise Server in the SafeGuard Management Center Configuration Package Tool. For more information, see [Configure the database server connection \(page 37\)](#) or see [Sophos knowledge base article 109012](#).

- Connection between the database server and SafeGuard Management Center:

Activate SSL encryption in the SafeGuard Management Center Configuration Wizard, see [Configure the database server connection \(page 37\)](#).

- Connection between SafeGuard Enterprise Server and the SafeGuard Enterprise protected endpoint:

Activate SSL encryption when creating the configuration package for the managed endpoints in the SafeGuard Management Center Configuration Package Tool, see [Create configuration package for managed computers \(page 55\)](#).

For information on how to configure the SafeGuard Enterprise Server to use SSL for securing communication, see [Configure the SGNSRV web page for SSL \(page 48\)](#).

Make certificates available on endpoints:

- For Windows endpoints, see [Assign the SSL certificate to Windows endpoints \(page 49\)](#).

- For macOS endpoints, see [Import the SSL certificate on Macs \(page 50\)](#)

We recommend that you set SSL encryption for SafeGuard Enterprise during first-time configuration of the SafeGuard Enterprise components. If you do it later, you need to create a new configuration package and install it on the relevant server or managed endpoints.

2.7.3 Configure the SGNSRV web page for SSL

The following description refers to Microsoft Windows Server 2012.

1. Open **Internet Information Services (IIS) Manager**.
2. In the **Connections** pane, select the server that hosts the SGNSRV web page.
3. In the right-hand pane, double-click **Server certificates** from the **IIS** section.
 - You can create a self-signed certificate to be used for SSL transport encryption.
 - You can import an existing certificate. Continue with step 5.
4. To create a certificate click **Create Self-Signed Certificate** in the **Actions** pane on the right.
 - a. Enter the name of the server that hosts the SGNSRV web page as friendly name and click **OK**.
The certificate is displayed in the **Servers Certificates** pane.
 - b. Double-click the certificate to export the public part.
You have to distribute the public part of the certificate to all your endpoints, see [Assign the SSL certificate to Windows endpoints \(page 49\)](#) and [Import the SSL certificate on Macs \(page 50\)](#).
 - c. In the **Certificate** dialog select the **Details** tab.
 - d. Click **Copy to file**.
 - e. In the **Certificate Export Wizard** click **Next**.
 - f. Select **No, do not export the private key** and click **Next**.
 - g. Keep the default selection for the export file format and click **Next**.
 - h. Click **Browse**, select a location, enter a file name for the certificate file, and click **Save**.
 - i. Click **Next**, and then **Finish**.
 - j. Continue with step 6.
5. To import a certificate click **Import** in the **Actions** pane on the right.
 - a. Browse to the certificate file.

- b. Select the file of type **Personal Information Exchange** and click **Open**.
- c. Enter the password and click **OK**.
The certificate is displayed in the **Servers Certificates** pane.

6. From the **Connections** pane on the left, select the name of the server on which the certificate is installed.
7. Under **Sites**, select the site to be secured with SSL.
8. From the **Actions** pane on the right, select **Bindings**.
9. In the **Site Bindings** dialog, click **Add**.
10. Under **Type:**, select **https** and under **SSL certificate:**, select the certificate you installed before.
11. Click **OK** and close the **Site Bindings** dialog box.
12. In the navigation pane select the server and click **Restart** in the **Actions** pane.

2.7.4 Configure endpoints to use SSL

To use SSL on the SafeGuard Enterprise protected endpoints:

1. Assign the SSL certificate to Windows endpoints and import SSL certificates on Macs, see [Assign the SSL certificate to Windows endpoints \(page 49\)](#) and [Import the SSL certificate on Macs \(page 50\)](#).
2. Create a client configuration package that includes SSL, see [Create configuration package for managed computers \(page 55\)](#).

2.7.5 Assign the SSL certificate to Windows endpoints

WinClient

There are several ways of assigning a certificate to an endpoint. One way is to assign it by using a Microsoft Group Policy, which is described in this section. If you want to use a different method, make sure that the certificate is stored in the local machine certificate store.

To assign a certificate by using Group Policy:

1. Open **Group Policy Management** console (gpedit.msc).
2. Create a new group policy object (GPO) to contain the certificate settings. Ensure that the GPO is associated with the domain, site, or organizational unit which contains the users you want to manage with the policy.
3. Right-click the GPO, and then select **Edit**.

Group Policy Management Editor opens, and displays the current contents of the policy object.

4. In the navigation pane, open **Computer Configuration > Windows Settings > Security Settings > Public Key Policies > Trusted Publishers**.
5. Click the **Action** menu, and then click **Import**.
6. Follow the instructions in the **Certificate Import Wizard** to find and import the certificate.
7. If the certificate is self-signed and cannot be traced back to a certificate that is in the Trusted Root Certification Authorities certificate store, then you must also copy the certificate to that store. In the navigation pane, click **Trusted Root Certification Authorities**, and then repeat steps 5 and 6 to install a copy of the certificate to that store.

2.7.6 Import the SSL certificate on Macs

Before you start the installation, make sure the SafeGuard Enterprise-SSL server certificate has been imported into the **system** keychain and is set to **Always Trust** for SSL.

1. Ask your SafeGuard Server Administrator to provide you with the SafeGuard Enterprise server certificate for SSL (file *<certificate name>.cer*).
2. Import the *<certificate name>.cer* file into your keychain. To do so, go to **Applications > Utilities** and double-click the **Keychain Access.app**.
3. In the left pane, select **System**.
4. Open a Finder window and select the *<certificate name>.cer* file.
5. Drag and drop the certificate file into the **System Keychain Access** window.
6. Enter your macOS password when prompted.
7. Click **Modify Keychain** to confirm your action.
8. In the **Keychain Access.app**, double-click the *<certificate name>.cer*.
9. Click the arrow next to **Trust** to display the trust settings.
10. For **Secure Sockets Layer (SSL)**, select the option **Always Trust**.
11. Close the dialog.
12. Enter your macOS password and confirm by clicking **Update Settings**.
A blue plus symbol in the lower right corner of the certificate icon indicates that this certificate is marked as trusted for all users.



13. Open a web browser and enter `https://<servername>/SGNSRV` to verify that your SafeGuard Enterprise Server is available.

Now you can start the installation.

2.7.6.1 Automated deployment

You can use the following command to import certificates:

```
sudo /usr/bin/security add-trusted-cert -d -k /Library/Keychains/System.keychain -r trustAsRoot -p ssl "<folder>/<certificate name>.cer".
```

This can be used for automated deployment via script. Change folder and certificate names according to your settings.

2.8 Registering and configuring SafeGuard Enterprise Server

The SafeGuard Enterprise Server needs to be registered and configured to implement the communication information between IIS server, database, and SafeGuard protected endpoint. The information is stored in a server configuration package.

You carry out this task in the SafeGuard Management Center. The workflow depends on whether SafeGuard Enterprise Server is installed on the same computer as the SafeGuard Management Center or on a different one.

You may set further properties such as add additional security officers for the selected server, or configure the connection to the database.

2.8.1 Register and configure SafeGuard Enterprise Server for the current computer

When SafeGuard Management Center and SafeGuard Enterprise Server are installed on the computer you are currently working on, register and configure SafeGuard Enterprise Server:

1. Start SafeGuard Management Center.
2. On the **Tools** menu, click **Configuration Package Tool**.
3. Select the **Servers** tab and then select **Make this computer an SGN Server**. This option is not available if Multi Tenancy is installed.

The Setup Wizard is started automatically.

4. Accept the defaults in all subsequent dialogs.

The SafeGuard Enterprise Server is registered. A server configuration package called <Server>.msi is created and directly installed on the current computer. The server information is displayed on the **Servers** tab. You may carry out additional configuration.

 **Note**

If you want to install a new server configuration package (MSI) on the SafeGuard Enterprise Server, make sure that you uninstall the old one first. Additionally, manually delete the local cache so that it can be updated correctly with new configuration data, such as SSL settings. Then install the new configuration package on the server.

2.8.2 Register and configure SafeGuard Enterprise Server for a different computer

When the SafeGuard Enterprise Server is installed on a computer other than the one where the SafeGuard Management Center is installed, register and configure SafeGuard Enterprise Server:

1. Start SafeGuard Management Center.
2. On the **Tools** menu, click **Configuration Package Tool**.
3. Select **Servers** tab and then click **Add....**
4. In **Server Registration** click [...] to select the server's machine certificate which can be found under C:\Program Files (x86)\Sophos\SafeGuard Enterprise\MachCert on the IIS server that runs the SafeGuard Enterprise Server. Its file name is <Computername>.cer. When the SafeGuard Enterprise Server is installed on a computer other than the one where the SafeGuard Management Center is installed, this .cer file must be accessible as a copy or by using a network permission.

Do not select the MSO certificate.

The fully qualified name (FQDN), for example server.mycompany.com and certificate information are displayed. When using SSL as transport encryption between an endpoint and the server, the server name specified here must be identical to the one specified in the SSL certificate. Otherwise they cannot communicate.

5. Click **OK**.

The server information is displayed on the **Servers** tab.

6. Click the **Server packages** tab. The available servers are displayed. Select the required server. Specify the output path for the server configuration package. Click **Create Configuration Package**.

A server configuration package (MSI) called <Server>.msi is created in the specified location.

7. Click **OK** to confirm the success message.

8. On the **Servers** tab, click **Close**.

You have finished registering and configuring SafeGuard Enterprise Server.

Next steps:

- Install the server configuration package (MSI) on the computer running the SafeGuard Enterprise Server.
- Restart the IIS in order to load the new configuration.

You may change the server configuration on the **Servers** tab any time.

2.8.3 Edit SafeGuard Enterprise Server properties

You can edit the properties and settings for any registered server and its database connection at any time.

1. On the **Tools** menu, click **Configuration Package Tool**.
2. Select **Servers** tab and then select the required server.
3. Carry out any of the following:

Element	Description
Scripting allowed	Click to enable the use of the SafeGuard Enterprise Management API. This allows scripting of administrative tasks.
Win. Auth. WHD	Click to enable Windows Authentication for Web Helpdesk. By default, the option is disabled.
Recovery via mobile	Click to enable sending recovery keys for full disk encryption to your Sophos Mobile Server.
Server roles	Click to select/deselect an available security officer role for the selected server.
Add server role...	Click to add further specific security officer roles for the selected server if required. You are prompted to select the server

Element	Description
Database connection	<p>certificate. The security officer role is added and can be displayed under Server roles.</p> <p>Click [...] to configure a specific database connection for any registered web server, including database credentials and transport encryption between the web server and the database server. For further information, see Configure the database server connection (page 37). Even if the database connection check has not been successful, a new server configuration package can be created.</p>

 **Note** You do not have to rerun the SafeGuard Management Center Configuration Wizard to update the database configuration. Simply make sure that you create a new server configuration package afterwards and distribute it to the respective server. When the updated server package is installed on the server, the new database connection can be used.

4. Create a new server configuration package on the **Server packages** tab.
5. Uninstall the old server configuration package, then install the new one on the respective server.

The new server configuration becomes active.

2.8.4 Register SafeGuard Enterprise Server with Sophos firewall enabled

A SafeGuard Enterprise protected endpoint is unable to connect to SafeGuard Enterprise Server when a Sophos firewall with default settings is installed on the endpoint. By default, the Sophos firewall blocks NetBIOS connections which are needed for resolving the SafeGuard Enterprise Server network name.

As a workaround, do one of the following:

- Unblock NetBIOS connections in the firewall.
- Include the fully qualified name of the SafeGuard Enterprise Server in the server configuration package. For further information, see [Register and configure SafeGuard Enterprise Server for a different computer \(page 52\)](#).

2.9 *Creating configuration packages*

Depending on the required configuration, create the appropriate configuration packages for the endpoints in the SafeGuard Management Center:

- For managed endpoints (Windows and macOS) - Managed client packages
- For unmanaged endpoints (Windows only) - Standalone client packages

Whenever you create a managed client package, the system produces both a package for Windows and a package (ZIP format) for Mac. The ZIP package is also used for the Sophos Mobile server to connect to the SafeGuard Enterprise backend.

The initial configuration package has to be installed on the endpoints with the encryption software.

2.9.1 *Create configuration package for managed computers*

1. In the SafeGuard Management Center, on the **Tools** menu, click **Configuration Package Tool**.
2. Select **Managed client packages**.
3. In the **Primary Server** drop-down box, switch to the server which was registered.
4. If required, specify a policy group to be applied to the computer. It must have been created beforehand in the SafeGuard Management Center. If you want to use service accounts for post-installation tasks on the computer, make sure that you include the respective policy setting in this first policy group. See the [SafeGuard Enterprise 8 administrator help](#).
5. Select the **Transport Encryption** mode defining how the connection between SafeGuard Enterprise Client and SafeGuard Enterprise Server is to be encrypted. For further information, see [Securing transport connections with SSL \(page 45\)](#).
6. Specify an output path for the configuration package (MSI).
7. Click **Create Configuration Package**.

If you have selected SSL encryption as the **Transport Encryption** mode, the server connection is validated. If the connection fails, a warning message is displayed. You can ignore the message and create the client configuration package anyway. However, you have to ensure that the communication between the SafeGuard Client and the SafeGuard Server is possible using SSL.

The configuration package (MSI) has now been created in the specified directory. You now need to distribute and deploy this package to the endpoints.

2.9.2 Create configuration package for unmanaged computers (Windows only)

1. In the SafeGuard Management Center, on the **Tools** menu, click **Configuration Package Tool**.
2. Select **Standalone client packages**.
3. Click **Add Configuration Package**.
4. Enter a name of your choice for the configuration package.
5. Specify a **Policy Group** which must have been created beforehand in the SafeGuard Management Center to be applied to the computers.
6. Under **Key Backup Location**, specify or select a shared network path for storing the key recovery file. Enter the share path in the following form: \\network computer\\, for example \\mycompany.edu\\. If you do not specify a path here, the end user is prompted to name a storage location for this file when first logging on to the endpoint after installation.

The key recovery file (XML) is needed to enable recovery of SafeGuard Enterprise protected computers and is generated on each SafeGuard Enterprise protected computer.

Make sure that you save this key recovery file at a file location accessible to the helpdesk. Alternatively, the files can be provided to the helpdesk in a different way. This file is encrypted by the company certificate. It can therefore be saved to any external media or to the network to provide it to the helpdesk for recovery purposes. It can also be sent by e-mail.

7. Under **POA Group**, you can select a POA user group to be assigned to the endpoint. POA users can access the endpoint for administrative tasks after the Power-on Authentication has been activated. To assign POA users, the POA group must have been created beforehand in the **Users and Computers** area of the SafeGuard Management Center.
8. Specify an output path for the configuration package (MSI).
9. Click **Create Configuration Package**.

The configuration package (MSI) has now been created in the specified directory. You now need to distribute and deploy this package to the endpoints.

2.10 Setting up SafeGuard Enterprise on endpoints

As soon as the back-end is running, the deployment and installation of the SafeGuard Enterprise Clients can begin. We recommend following the preliminary steps described in this section to ensure a smooth implementation.

The SafeGuard Enterprise client can be installed on different kinds of hardware and on different operating systems. A list of all supported operating systems and the minimum system requirements can be found in the [release notes](#).

General recommendations for the preparation of your system for the installation of SafeGuard Enterprise can be found in [Sophos knowledge base article 108088](#).

2.10.1 About managed and unmanaged endpoints

SafeGuard Enterprise endpoints can be configured as follows:

- **Managed**

Central server-based management in SafeGuard Management Center.

For managed endpoints, a connection to the SafeGuard Enterprise Server exists. They receive their policies through the SafeGuard Enterprise Server.

- **Unmanaged**

Local management through configuration packages created in SafeGuard Management Center.

Limitations:

- Local management is not possible with macOS.
- Synchronized Encryption is not available on unmanaged endpoints.

Unmanaged endpoints are not connected to the SafeGuard Enterprise Server and thus operate in standalone mode. They receive SafeGuard Enterprise policies by way of configuration packages instead.

SafeGuard Enterprise policies are created in the SafeGuard Management Center and exported to configuration packages. The configuration packages then need to be deployed by company software distribution mechanisms or installed manually on the endpoints.

Different installation packages and modules are provided for each type of endpoint.

2.10.2 Restrictions

Note the following restrictions for managed endpoints:

- **Restrictions for initial encryption:**

Initial configuration of managed endpoints may involve the creation of encryption policies that may be distributed inside a configuration package to the SafeGuard Enterprise protected endpoints. However, when the endpoint is not connected to a SafeGuard Enterprise Server immediately after the configuration package is installed, but is temporarily offline, only encryption policies with the following specific settings become immediately active:

Volume-based full disk encryption that uses the **Defined Machine Key** as encryption key.

For all other policies involving encryption with user-defined keys to become active on the SafeGuard Enterprise protected endpoint, the respective configuration package has to be reassigned to the endpoint's organizational unit as well. The user-defined keys are then only created after the endpoint is connected to SafeGuard Enterprise Server again.

This is because the **Defined Machine Key** is created directly on the SafeGuard Enterprise protected endpoint at the first restart after installation, whereas user-defined keys can only be created after the endpoint has been registered at the SafeGuard Enterprise Server.

- **Restrictions for BitLocker Drive Encryption support:**

Either SafeGuard Enterprise volume-based encryption or BitLocker Drive Encryption can be used, but not both simultaneously. If you want to change the encryption type, you must first decrypt all encrypted drives, uninstall the SafeGuard Enterprise encryption software and then reinstall it with the features you want to use. The installer prevents the deployment of both features at the same time. Uninstallation and reinstallation is necessary even if no configuration package intended to trigger encryption has been installed.

2.10.3 Check the availability of the SSL certificate on Windows endpoints

The certificate must be assigned to the computer and not to the user. The certificate file must be available in the Microsoft Certificate Store under Trusted Root Certification Authorities.

1. Log on to the endpoint as an administrator.

2. Click **Run** > mmc.
3. In the **Console1** window, click the **File** menu and then click the **Add/Remove Snap-in** command.
4. In the **Add/Remove Snap-in** dialog box, select **Certificates** in the left pane and click **Add**.
5. On the Certificates snap-in page, select the **Computer account** option.
6. On the **Select Computer** page, select **Local computer: (the computer this console is running on)** and click **Finish**.
7. Click **OK** in the **Add/Remove Snap-in** dialog box.
8. In the left pane, click **Console Root > Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates**.
9. In the right pane, check if the certificate which was created before is available in the store. If the certificate appears in the list, this step is completed. If not, do the following:
 10. Click **Run** > gpupdate /force.
A Windows command box is displayed.
11. Wait until the box has closed and perform the above steps again starting at step 1.

2.10.4 Prepare for BitLocker Drive Encryption support

If you want to use SafeGuard Enterprise to manage BitLocker endpoints, carry out the following specific preparations on the endpoint:

- Windows 7 or higher must be installed on the endpoint.
- BitLocker Drive Encryption must be installed and activated.
- BitLocker Drive Encryption Service must be running.
 **Note** Run `services.msc` and check if the **BitLocker Drive Encryption Service** is running.
- If TPM is to be used for authentication, TPM must be initialized, owned and activated.

2.10.5 Prepare for SafeGuard Full Disk Encryption with POA

Before you deploy SafeGuard Enterprise, we recommend that you prepare as follows.

- A user account must be set up and active on the endpoints.
- Make sure that you have Windows administrator rights.
- Create a full backup of the data on the endpoint.
- Drives to be encrypted must be completely formatted and have a drive letter assigned to them.
- Sophos provides a hardware configuration file to minimize the risk of conflicts between the POA and your endpoint hardware. The file is contained in the encryption software package. We recommend that you install an updated version of this file before any significant deployment of SafeGuard Enterprise. For more information, see [Sophos knowledge base article 65700](#).

You can help us improve hardware compatibility by executing a tool that we provide to collect hardware relevant information only. The tool is very easy to use. The collected information is added to the hardware configuration file. For more information, see [Sophos knowledge base article 110285](#).

- Check the hard disk(s) for errors with this command: chkdsk %drive% /F /V /X

After that, you need to reboot your system.

⚠ Important Do not start the SafeGuard Enterprise installation without completing this reboot!

- Use the Windows built-in defrag tool to locate and consolidate fragmented boot files, data files, and folders on local volumes.
- Uninstall third party boot managers, such as PROnetworks Boot Pro and Boot-US.
- If an imaging tool was used to install the operating system, we recommend you to "re-write" the master boot record (MBR).
- If the boot partition on the endpoint has been converted from FAT to NTFS and the endpoint has not been restarted since, restart the endpoint once. Otherwise the installation might not be completed successfully.
- For SafeGuard Enterprise clients (managed) only: Check whether there is a connection to the SafeGuard Enterprise Server. Select this web address in Internet Explorer on the endpoints: <http://<ServerIPAddress>/sgnsrv>. If the **Trans** page shows **Check Connection**, connection to SafeGuard Enterprise Server has been successfully established.

For further information, see [Sophos knowledge base article 108088](#).

2.10.6 Prepare for Cloud Storage

The SafeGuard Enterprise Cloud Storage module offers file-based encryption of data stored in the cloud. It only encrypts new data stored in the cloud. If data was already stored in the cloud before

installing Cloud Storage, this data is not automatically encrypted. If it is to be encrypted, users first have to remove it from the cloud and then enter it again after Cloud Storage has been installed.

Cloud Storage makes sure that local copies of cloud data are encrypted transparently and remain encrypted when stored in the cloud.

The way users work with data stored in the cloud is not changed. The vendor-specific cloud software remains unaffected and can be used in the same way as before to send data to or receive data from the cloud.

To prepare endpoints for Cloud Storage:

- The cloud storage software provided by the vendor must be installed on the endpoints where you want to install Cloud Storage.
- The cloud storage software provided by the vendor must have an application or system service stored on the local file system that synchronizes data between the cloud and the local system.
- The cloud storage software provided by the vendor must store the synchronized data on the local file system.

2.11 Installing the encryption software on Windows

Setting up SafeGuard Enterprise encryption software on endpoints can be done in two ways:

- Install encryption software locally (attended). This is advisable for a trial installation, for example.
- Install encryption software centrally (unattended). This ensures a standardized installation on multiple endpoints.

Before you start, check the available installation packages and features for managed and unmanaged endpoints. Installation steps for both variants are identical except that you assign a different configuration package for each of them.

The behavior of the endpoints when first logging on after installing SafeGuard Enterprise and the activation of the Power-on Authentication is described in the *SafeGuard Enterprise user help*.

2.11.1 Installing packages and features

The following table shows the installation packages and features of the SafeGuard Enterprise encryption software on endpoints. You find the installation packages in the **Installers** folder of your product delivery.

The default installation contains full disk encryption only. On endpoints running Windows 7, SafeGuard Full Disk Encryption is installed. On endpoints running Windows 8 or newer, BitLocker is installed. If you want to install a file encryption module, you need to select a **Custom** installation and select the required components. Note that you can only install either Synchronized Encryption or location-based File Encryption, not both.

When the operating system of the endpoint is Windows 64-bit, install the 64-bit variant of the installation packages (<package name>_x64.msi).

Package	Content	Available for managed endpoints	Available for unmanaged endpoints
SGxClientPreinstall.msi (Windows 7 only)	<p>Pre-installation package</p> <p>The package must be installed before installing any encryption installation package. Provides endpoints with necessary requirements for successful installation of the current encryption software.</p>	 mandatory	 mandatory
vstor-redist.exe SGNClient.msi SGNClient_x64.msi	<p>Optional: only necessary if not all current Windows updates are installed.</p> <p>SafeGuard client installation package</p> <p>Provides endpoints with necessary requirements for successful installation of the current encryption software. For full disk encryption for internal and external hard disks, SafeGuard Enterprise offers the alternatives SafeGuard Full Disk Encryption or BitLocker.</p>		
	<p>BitLocker or BitLocker C/R</p> <p>SafeGuard Enterprise manages the Microsoft BitLocker encryption engine. On UEFI platforms, BitLocker pre-boot authentication comes with a SafeGuard Challenge/Response mechanism whereas the BIOS version allows the retrieval of the recovery key from the SafeGuard Management Center.</p>		

Package	Content	Available for managed endpoints	Available for unmanaged endpoints
	<p>SafeGuard Full Disk Encryption (only Windows 7 BIOS)</p> <p>SafeGuard Full Disk Encryption includes SafeGuard Power-on Authentication.</p> <p>Synchronized Encryption</p> <p>Includes application-based file encryption and self-encrypting HTML functionality for automatically encrypting email attachments using Microsoft Outlook.</p> <p>Cloud Storage</p> <p>File-based encryption of data stored in the cloud. Local copies of data stored in the cloud are always encrypted transparently. To send data to or receive data from the cloud, vendor-specific software must be used.</p> <p>File Encryption</p> <p>File-based encryption of data on local hard disks and network shares, especially for workgroups.</p> <p>Data Exchange</p> <p>SafeGuard Data Exchange: file-based encryption of data on removable media on all platforms without re-encryption.</p>	     	    

2.11.2 Install the encryption software locally

Prerequisites:

- Endpoints must have been prepared for encryption, see [Setting up SafeGuard Enterprise on endpoints \(page 57\)](#).
- Decide which encryption package and features you need to install. For example, the SGxClientPreinstall.msi package is no longer required for Windows 8 or later. The steps

related to the POACFG file are only relevant for Device Encryption with POA and BitLocker with Challenge/Response.

To install the encryption software locally:

1. Log on to the endpoint as an administrator.
2. Copy the `SGNClient_x64.msi` package and the `SGxClientPreinstall.msi` package to the client.
3. Install the `SGxClientPreinstall.msi` package to provide the endpoint with the necessary requirements for a successful installation of the current encryption software.
As an alternative to the `SGxClientPreinstall.msi`, you can install the Microsoft `vcredist_x86.exe` package that is also available in the product delivery.
4. Install the `vcredist14_x86.exe` from the product delivery.
5. Download the current POACFG file as described in [Sophos knowledge base article 65700](#).
6. Save the latest version of the POACFG file centrally so that it is accessible from every endpoint.
7. Open a new administrative command line box on the client.
8. Change to the folder containing the SafeGuard installation files.
9. Start the installation using this command: `MSIEXEC /i <client.msi> POACFG=<path of the POA configuration file>`
The SafeGuard Enterprise Client installation wizard starts.
10. In the wizard, accept the defaults on all subsequent dialogs.
In a first-time installation, we recommend that you select a **Complete** installation from the start.
To only install a subset of features, choose a **Custom** installation.
11. Go to the location where you saved the relevant configuration package (MSI) created beforehand in the SafeGuard Management Center. Specific configuration packages need to be installed for managed and unmanaged endpoints, see [Creating configuration packages \(page 54\)](#).
12. Install the relevant configuration package (MSI) on the computer.
13. To activate Power-on Authentication, restart the endpoint twice.
14. Restart once more to perform a backup of the kernel data on every Windows boot. Make sure that the computer is not put into hibernation, sleep or hybrid sleep mode before the third restart to successfully complete the kernel backup.

SafeGuard Enterprise is set up on the endpoint. For more information on the computer's logon behavior after SafeGuard Enterprise installation, see the [SafeGuard Enterprise user help](#).

2.11.3 *Installing the encryption software centrally*

Installing encryption software centrally ensures a standardized installation on multiple endpoints.

 **Note** Within central software distribution, the installation and configuration packages can only be assigned to an endpoint, they cannot be assigned to a user.

For a central installation, do the following:

- Check the available encryption packages and features for managed and unmanaged endpoints, see [Installing packages and features \(page 61\)](#).
- Check the command-line options.
- Check the list of feature parameters for the ADDLOCAL command-line option.
- Check the sample commands.
- Prepare the installation script.

2.11.3.1 *Installing the encryption software centrally through Active Directory*

Make sure that you do the following when installing the encryption software centrally using group policy objects (GPO) in an Active Directory:

 **Note** Within central software distribution, the installation and configuration packages can only be assigned to an endpoint, they cannot be assigned to a user.

- Use a separate group policy object (GPO) for each installation package and sort them in the following order:
 1. pre-installation package
 2. encryption software package
 3. endpoint configuration package

For further information on the packages, see [Prepare the installation script \(page 65\)](#).

- When the endpoint language is not set to German, additionally do the following: in the Group Policy Editor, select the respective group object and then **Computer Configuration > Software Settings > Advanced**. In the **Advanced Deployment Options** dialog, select **Ignore language when deploying this package** and click **OK**.

2.11.3.2 Prepare the installation script

Prerequisites:

- Endpoints must have been prepared for encryption.
- Decide which encryption package and features you want to install.

To install the encryption software centrally:

1. Create a folder called Software to use as a central store for all applications.
2. Use your own tools to create a package to be installed on the endpoints. The package must include the following in the order mentioned:

Package	Description
Pre-installation package SGxClientPreinstall.msi	The mandatory package provides the endpoints with the necessary requirements for a successful installation of the current encryption software, for example the required DLL MSVCR100.dll.
(Windows 7 only)	 Note If this package is not installed, installation of the encryption software is aborted.
Encryption software package	For a list of available packages see Installing packages and features (page 61) .
Configuration package for endpoints	Use the configuration packages created before in SafeGuard Management Center. Different configuration packages need to be installed for managed and unmanaged endpoints, see Creating configuration packages (page 54) . Make sure that you delete any old ones first.

3. Create a script with the commands for the pre-configured installation. The script must list which features of the encryption software you want to install, see [Feature parameters for ADDLOCAL option \(page 68\)](#). Open a command prompt, and then type the scripting commands. For the command-line syntax, see [Command line options for central installation \(page 67\)](#).
4. Distribute this package to the endpoints using company software distribution mechanisms.

The installation is executed on the endpoints. The endpoints are then ready to be used with SafeGuard Enterprise.

5. To activate Power-on Authentication, restart the endpoint twice. Restart once more to perform a backup of the kernel data on every Windows boot. Make sure that the computer is not put

into hibernation, sleep or hybrid sleep mode before the third restart to successfully complete the kernel backup.

Additional configuration may be required to ensure that Power-on Authentication (POA) functions correctly on each hardware platform. Most hardware conflicts can be resolved using the **Hotkeys** built into the POA. Hotkeys can be configured in the POA after installation or by an additional configuration setting passed to the Windows Installer command msieexec. For further information, see Sophos knowledge base articles [107781](#) and [107785](#).

2.11.3.3 Prepare for Synchronized Encryption

For the Synchronized Encryption module to work properly, the Microsoft runtime `vstor-redist.exe` must be installed. The file installs Microsoft Visual Studio 2010 Tools for Office Runtime and is included in the installation package.

We recommend installing the components in the following order:

1. `vstor-redist.exe`
2. `SGNclient.msi`
3. configuration package

 **Note** You cannot deploy the configuration package before the installation of `vstor-redist.exe` is finished.

2.11.3.4 Command line options for central installation

For a central installation, we recommend that you prepare a script using the Windows Installer component msieexec, which automatically carries out a pre-configured SafeGuard Enterprise installation. msieexec is included in Windows. For further information, see [https://msdn.microsoft.com/en-us/library/aa372024\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/aa372024(v=vs.85).aspx).

Command line syntax

```
msieexec /i <path+msi package name> / ADDLOCAL=<SGN Features>
```

The command line syntax consists of:

- Windows Installer parameters, which, for example, log warnings and error messages to a file during the installation.

- SafeGuard Enterprise features to be installed, for example, full disk encryption.

Command line options

You can select all available options using msieexec.exe in the prompt. The main options are described below.

Option	Description
/i	Specifies the fact that this is an installation.
/qn	Installs with no user interaction and does not display a user interface.
ADDLOCAL=	<p>Lists the SafeGuard Enterprise features that are to be installed. If the option is not specified, all features intended for a standard installation are installed.</p> <p>For a list of SafeGuard Enterprise features in each installation package and availability according to endpoint configuration, see Installing packages and features (page 61). For list of feature parameters for the ADDLOCAL option, see Feature parameters for ADDLOCAL option (page 68).</p>
ADDLOCAL=ALL	Under Windows 7 (BIOS) ADDLOCAL=ALL installs the SafeGuard volume-based encryption and all other available features. Under Windows 8 or higher, ADDLOCAL=ALL installs BitLocker support and Synchronized Encryption.
REBOOT=NORESTART ReallySuppress	Forces or suppresses a restart after installation. If nothing is specified, the restart is forced after installation.
/L*VX <path + filename>	Logs all warnings and error messages in the specified log file. The parameter /Le <path + filename> only logs error messages.

2.11.3.5 Feature parameters for ADDLOCAL option

You need to define in advance which features are to be installed on the endpoints. The feature names are added as parameters to the command-line option ADDLOCAL. List the features after typing the option ADDLOCAL in the command prompt:

- Separate the features with a comma.
- Observe uppercase and lowercase.
- If you select a feature, you also need to add all feature parents to the command line.
- Please note that the names of the features may differ from the corresponding module names. You find them in the table below in brackets.

- You must always list the features **Client** and **CredentialProvider**.

The following tables list the features that can be installed on the endpoints. For further information, see: [Installing packages and features \(page 61\)](#).

Feature Parents	Feature
Client	CredentialProvider Mandatory. The feature enables logon with the Credential Provider.
Client, BaseEncryption	SectorBasedEncryption (SafeGuard volume-based encryption)
Client, BaseEncryption	BitLockerSupport Win 7 only: SectorBasedEncryption BitLockerSupport (BitLocker)
Client, BaseEncryption, BitLockerSupport Client, NextGenDataProtection Client, LocationBasedEncryption	BitLockerSupportCR (BitLocker C/R) NextGenDataProtection (Synchronized Encryption) SecureDataExchange (Data Exchange)
Client, LocationBasedEncryption Client, LocationBasedEncryption	FileShare (File Encryption) CloudStorage (Cloud Storage)

2.11.3.6 Sample commands: Installing SafeGuard File Encryption only

```
msiexec /i C:\Software\SGxClientPreinstall.msi /qn /L*VX C:\Temp
\SGxClientPreinstall.log
```

The endpoints are provided with the necessary requirements for successful installation of the current encryption software. A log file SGxClientPreinstall.log is created in C:\Temp\.

Use the /L*VX option if you have a problem with an installation package. It is not mandatory.

```
msiexec /i C:\Software\SGNClient.msi
ADDLOCAL=Client,CredentialProvider,LocationBasedEncryption,FileShare
```

The following components are installed:

- Support for logon to endpoints with Windows Credential Provider.
- SafeGuard File Encryption with file-based encryption of data on local hard disk and network shares.

Installation directory is C:\Program Files\Sophos\SafeGuard Enterprise.

```
msiexec /i C:\Software\SGNConfig_managed.msi
```

Installs the configuration package that configures the endpoint as a managed endpoint and enables the connection to the SafeGuard Enterprise Server.

2.11.3.7 Sample commands: Installing SafeGuard BitLocker Support

```
msiexec /i C:\Software\SGxClientPreinstall.msi
```

The endpoints are provided with the necessary requirements for successful installation of the current encryption software.

```
msiexec /i C:\Software\SGNClient_x64.msi  
ADDLOCAL=Client,CredentialProvider,BaseEncryption,BitLockerSupport
```

The following components are installed:

- Support for logon to endpoints with Windows Credential Provider.
- SafeGuard BitLocker Support.

Installation directory is C:\Program Files\Sophos\SafeGuard Enterprise.

```
msiexec /i C:\Software\SGNConfig_managed.msi
```

Installs the configuration package that configures the endpoint as a managed endpoint and enables the connection to the SafeGuard Enterprise Server.

2.11.3.8 Sample commands: Installing SafeGuard BitLocker Support and File Encryption

```
msiexec /i C:\Software\SGxClientPreinstall.msi
```

The endpoints are provided with the necessary requirements for successful installation of the current encryption software.

```
msiexec /i C:\Software\SGNClient_x64.msi  
ADDLOCAL=Client,CredentialProvider,BaseEncryption,BitLockerSupport,LocationBasedEncryption
```

The following components are installed:

- Support for logon to endpoints with Windows Credential Provider.
- SafeGuard BitLocker Support.

- SafeGuard File Encryption with file-based encryption of data on local hard disk and network shares.

Installation directory is C:\Program Files\Sophos\SafeGuard Enterprise.

```
msiexec /i C:\Software\SGNConfig_managed.msi
```

Installs the configuration package that configures the endpoint as a managed endpoint and enables the connection to the SafeGuard Enterprise Server.

2.11.4 Installations on self-encrypting, Opal-compliant hard drives

SafeGuard Enterprise supports the vendor-independent Opal standard for self-encrypting hard drives and offers management of endpoints with hard drives of this type.

To ensure that the support of self-encrypting, Opal-compliant hard drives follows the standard closely, two types of check are carried out at the installation of SafeGuard Enterprise on the endpoint:

- **Functional checks**

These include, among others, checking whether the drive identifies itself as an "OPAL" hard drive, whether communication properties are correct, and whether all Opal features required for SafeGuard Enterprise are supported by the drive.

- **Security checks**

Security checks ensure that only SafeGuard Enterprise users are registered on the drive and that only SafeGuard Enterprise users own the keys used to software-encrypt non-self-encrypting drives. If other users are found to be registered at installation, SafeGuard Enterprise automatically tries to disable these users. This is a functionality required by the Opal standard with the exception of a few default "authorities" which are required to run an Opal system.

 **Note** The security checks are repeated when an encryption policy for the drive is applied after successful Opal-mode installation. If they fail, drive management must have been manipulated outside of SafeGuard Enterprise since the first check at installation. In this case, SafeGuard Enterprise does not lock the Opal hard drive. A corresponding message will be displayed.

If any of these checks fail in an unrecoverable way, the installation does not fall back to software-based encryption. Instead all volumes on the Opal drive remain unencrypted.

From SafeGuard Enterprise version 7 onwards, no Opal checks are performed by default. This means that, although an Opal drive is present, SafeGuard Enterprise will encrypt volumes on this drive using software-based encryption.

If you want to force Opal checks, use the following command line syntax:

```
MSIEXEC /i SGNClient.msi OPALMODE=0
```

 **Note** An upgrade from SafeGuard Enterprise 7.0 or 8.0 to SafeGuard Enterprise 8.3 on a system with an Opal HDD used in Opal HW-encryption mode will preserve the Opal HW-encryption mode.

Some Opal hard drives may have potential security issues. There is no way to automatically determine which privileges have been assigned to an unknown user/authority that has already been registered on the drive when SafeGuard Enterprise installation/encryption is carried out. If the drive refuses the command to disable such users, SafeGuard Enterprise falls back to software encryption to ensure maximum security for the SafeGuard Enterprise user. As we cannot give any security guarantees for the hard drives themselves, we have implemented a special installation switch to enable you to use drives which may have potential security risks at your own discretion. For a list of hard drives for which this installation switch is necessary and for further information on supported hard drives, see the [release notes](#).

To apply the installation switch, use the following command line syntax:

```
MSIEXEC /i SGNClient.msi IGNORE_OPAL_AUTHORITYCHECK_RESULTS=1
```

The internal property of the .msi has the same name, if you want to install it using a transform.

2.12 *Installing the encryption software on macOS*

The following chapter describes the installation of Sophos encryption software for macOS clients. The following products are available:

- Sophos SafeGuard Native Device Encryption
- Sophos SafeGuard File Encryption

For both products, two installation types are possible:

- automated (unattended) installation
- manual (attended) installation

If you want to use SafeGuard File Encryption and SafeGuard Native Device Encryption, both need to be version 8.

2.12.1 Automated installation of SafeGuard Native Device Encryption

An automated (unattended) installation does not require any user interaction during the installation process.

This section describes the basic steps for an automated installation of SafeGuard Native Device Encryption for Mac. Use the management software installed on your system. Depending on the management solution you are using, the actual steps may vary.

To install SafeGuard Native Device Encryption for Mac on client computers, perform the following steps:

1. Download the installer file *Sophos SafeGuard DE.dmg*.
2. Copy the file to the target machines.
3. Install the file on the target machines. If you use Apple Remote Desktop, steps 2 and 3 are one single step.
4. Select the configuration zip file and copy it to the target machines, see [Create configuration package for Macs \(page 97\)](#).
5. Run the following command on the target machines:
`/usr/bin/sgdeadmin --import-config /full/path/to/SGNConfig_managed.zip`
6. Change */full/path/to/file* according to your settings. This command needs to be run with administrator privileges. If you are using Apple Remote Desktop, then enter `root` in the field **user name** to specify which user issues the above stated command.

For further information, see [Sophos knowledge base article 120507](#).

2.12.2 Manual installation of SafeGuard Native Device Encryption

A manual (or attended) installation allows you to control and test the installation while proceeding step by step. It is performed on a single Mac.

1. Open *Sophos SafeGuard DE.dmg*.
2. After reading through the readme file, double-click *Sophos SafeGuard DE.pkg* and follow the installation wizard. You will be prompted for your password to allow the installation of new software. The product will be installed to the folder */Library/Sophos SafeGuard DE/*.
3. Click **Close** to complete the installation.

4. After a restart, log on with your Mac password.
5. Open the **System Preferences** and click the Sophos Encryption icon to show the product settings.

6. Click the **Server** tab.
7. If server and certificate details are shown, skip the next steps go to step 11. If no information is shown, continue with the next step.
8. Select the configuration zip file and copy it to the target machines, see [Create configuration package for Macs \(page 97\)](#).
9. Drag the zip file to the **Server** dialog and drop it into the drop zone.
10. You will be prompted to enter a Mac administrator password. Enter the password and click **OK** to confirm.
11. Check the connection to the SafeGuard Enterprise Server: Company certificate details are shown in the lower part of the **Server** dialog. Then click **Synchronize**. A successful connection will result in an updated "Last Contacted" time stamp (Tab **Server**, **Server Info** area, **Last Contacted:**). An unsuccessful connection will display the following icon:


For further information, refer to the system log file.

2.12.3 Automated installation of SafeGuard File Encryption

An automated (unattended) installation does not require any user interaction during the installation process.

This section describes the basic steps for an automated installation of SafeGuard File Encryption for Mac. Use the management software installed on your system. Depending on the management solution you are using, the actual steps may vary.

To install SafeGuard File Encryption for Mac on client computers, perform the following steps:

1. Download the installer file *Sophos SafeGuard FE.pkg*.
2. Copy the file to the target machines.
3. Install the file on the target machines. If you use Apple Remote Desktop, steps 2 and 3 are one single step.

4. Select the configuration zip file and copy it to the target machines, see [Creating configuration packages \(page 54\)](#).
5. Run the following command on the target machines:
`/usr/bin/sgdeadmin --import-config /full/path/to/file.zip`
6. Change `/full/path/to/file` according to your settings. This command needs to be run with administrator privileges. If you are using Apple Remote Desktop, then enter `root` in the field **user name** to specify which user issues the above stated command.
7. You can add additional steps to your workflow, based on your specific settings, for example shutting down the target machines.
For further information, see [Sophos knowledge base article 120507](#).

2.12.4 Manual installation of SafeGuard File Encryption

A manual (or attended) installation allows you to control and test the installation while proceeding step by step. It is performed on a single Mac.

1. Open *Sophos SafeGuard FE.dmg*.
2. After reading through the readme file, double-click *Sophos SafeGuard FE.pkg* and follow the installation wizard. You will be prompted for your password to allow the installation of new software. The product will be installed to the folder */Library/Sophos SafeGuard FS/*.
3. Click **Close** to complete the installation.
4. Open the **System Preferences** and click the Sophos Encryption icon to show the product settings.

5. Click the **Server** tab.
6. If server and certificate details are shown, skip the next steps go to step 11. If no information is shown, continue with the next step.
7. Select the configuration zip file and copy it to the target machines, see [Creating configuration packages \(page 54\)](#).
8. Drag the zip file to the **Server** dialog and drop it into the drop zone.
9. You will be prompted to enter a Mac administrator password. Enter the password and click **OK** to confirm.

10. Enter your Mac password to request your SafeGuard user certificate.
11. Check the connection to the SafeGuard Enterprise Server: Company certificate details are shown in the lower part of the **Server** dialog. Then click **Synchronize**. A successful connection will result in an updated "Last Contacted" time stamp (Tab **Server**, **Server Info** area, **Last Contacted:**). An unsuccessful connection will display the following icon:



For further information, refer to the system log file.

2.13 Setting up Web Helpdesk

Web Helpdesk is part of the SafeGuard Enterprise Server installation, see [Install SafeGuard Enterprise Server \(page 25\)](#).

After Web Helpdesk installation you need to configure the web server.

On the Web Helpdesk officer's computer, only a web browser needs to be installed.

2.13.1 Server Requirements

Detailed system requirements for the server are described in the release notes.

- Make sure that you have Windows administration rights.
- Microsoft Internet Information Services (IIS) must be installed.
- .NET Framework 4.5 with ASP.NET 4.5 must be installed.
- For Windows Server 2012: The ASP.NET role must be installed (Server Roles > Web Server (IIS) > Web Server > Application Development > ASP.NET 4.5).

 **Note** For Windows Server 2012 the following applies: ASP.NET applications come pre-wired with a handlers section in the web.config. Within feature delegation in IIS this is set to read only. In the IIS Manager, check under the server name > feature delegation. If the handler mappings are set to read only and your site web.configs have a handlers section, change the value to read/write.

2.13.2 Configure the web server with SSL/TLS

1. Deploy Web Helpdesk to the intranet only.
For security reasons, do not put Web Helpdesk on the internet.

2. Establish an SSL/TLS connection.

You can limit the availability of Web Helpdesk to defined users using the standard IIS configuration shipped with IIS. Make sure that you have SSL/TLS Security Certificate installed on the IIS server. Then all communications with Web Helpdesk will be carried out using SSL/TLS.

The following general tasks must be carried out to set up the web server for SSL/TLS:

- a. Certificate Authority must be installed for issuing certificates used by SSL/TLS encryption.
- b. A certificate must be issued and the IIS server configured to use SSL/TLS and point to the certificate.
- c. The server name specified when configuring the SafeGuard Enterprise Server must be the same as the one specified in the SSL/TLS certificate. Otherwise client and server cannot communicate. For each SafeGuard Enterprise Server a separate certificate is needed.
- d. The worker processes for the application pool SGNWHD-Pool must not be increased to more than 1 (default). Otherwise authorization to Web Helpdesk will fail.

For further information, contact our technical support or see:

- <http://msdn2.microsoft.com/en-us/library/ms998300.aspx>
- <http://support.microsoft.com/default.aspx?scid=kb;en-us;316898>
- https://blogs.msdn.com/sql_protocols/archive/2005/11/10/491563.aspx

2.13.3 Language support

Web Helpdesk supports several languages. You can dynamically change the language of the application in the Web Helpdesk Logon screen. Click the desired language, and the application is displayed in the requested language immediately.

2.14 About upgrading

SafeGuard Enterprise 8.0 or newer can be directly upgraded to the latest version of SafeGuard Enterprise. If you want to upgrade from older versions, you must first upgrade to version 8.0.

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 \(page 81\)](#).

For successful operation, version numbers of SafeGuard Enterprise Database, SafeGuard Enterprise Server and SafeGuard Management Center must match. They must be of the same or a higher version as the clients. Managing newer clients (for example 8.10) with older backend components (for example 8.0) is not supported.

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 Management Center (includes the successful upgrade of the database)
2. SafeGuard Enterprise Server and Web Helpdesk
3. SafeGuard Enterprise protected endpoints
4. SafeGuard Enterprise configuration packages

By default, all **File Encryption** policies are converted to or treated as policies with **Encryption type** set to **Location-based**.

 **Note** Once all SafeGuard Enterprise components and endpoints have been upgraded, we recommend that you switch to the more secure algorithm **SHA-256** to sign SafeGuard Enterprise-generated certificates, see [Change algorithm for self-signed certificates \(page 165\)](#).

2.14.1 Upgrade SafeGuard Management Center

Prerequisites:

- SafeGuard Management Center 8.0 or later must be installed. Versions below 8.0 must first be upgraded to SafeGuard Management Center 8.0.
- For successful operation, version numbers of SafeGuard Enterprise Database, SafeGuard Enterprise Server and SafeGuard Management Center must match.
- SafeGuard Management Center 8.30 can manage SafeGuard Enterprise-protected endpoints 6.0 and later.
- .NET Framework 4.5 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.

To upgrade SafeGuard Management Center:

1. Install the latest version of the SafeGuard Management Center installation package with the required features, see [About migrating \(page 81\)](#).
2. Start the SafeGuard Management Center.
3. The system checks the version of the SafeGuard Enterprise database and upgrades to the new version automatically.
4. The system prompts you to back up your database prior to the update.

The SafeGuard Management Center and database are upgraded to the latest version.

After upgrading, do not transfer existing POA users to SafeGuard Enterprise-protected endpoints. 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.

2.14.2 Upgrade SafeGuard Enterprise Server and Web Helpdesk

Starting with version 8.10 the Web Helpdesk is part of the SafeGuard Enterprise Server installation package. When you upgrade the SafeGuard Enterprise Server the Web Helpdesk is automatically updated.

Prerequisites

- SafeGuard Enterprise Server 8.0 or later must be installed. Older versions must first be upgraded to SafeGuard Enterprise Server 8.0.
- .NET Framework 4.5 and ASP.NET 4.5 (provided in the SafeGuard Enterprise product delivery) must be installed.
- Make sure that you have Windows administrator rights.

To upgrade SafeGuard Enterprise Server:

Install the latest version of the SafeGuard Enterprise Server installation package using `SGNServer.msi`.

As soon as all SafeGuard Enterprise components (Management Center, Server, Web Helpdesk) have been upgraded, you must restart the SafeGuard Enterprise Server.

2.14.3 Upgrade endpoints

This section applies to both managed and unmanaged endpoints.

Prerequisites

- SafeGuard Enterprise encryption software version 8.0 or later must be installed. Older versions must first be upgraded to version 8.0.
- 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 8.30 and SafeGuard Enterprise Server 8.30 can manage SafeGuard Enterprise protected endpoints version 6.0 or newer. However, we recommend that you use the same version of encryption software on every endpoint.
- 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 as they are updated automatically.
3. Install the latest version of the 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 8.0 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.

4. After installation is completed, restart the endpoint when prompted.

 **Important** Restart the system according to the prompt. As long as you do not restart, the SafeGuard Credential Provider is not available. Under Windows 10 shutting down and starting the endpoint does not replace the necessary restart. You need to explicitly restart the system.

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

 **Note** You cannot make changes to your installed modules during an upgrade. If changes are required, see [About migrating \(page 81\)](#).

2.14.4 Upgrade endpoint configuration packages

After upgrading the SafeGuard backend software, we strongly recommend to delete all old configuration packages for security reasons. New installations of the SafeGuard Client have to be done with an endpoint configuration package that was created using SafeGuard Management Center version 8.30. Configuration packages generated with a previous version of the SafeGuard Management Center are not supported.

Endpoint configuration packages on existing (already configured) endpoints need to be upgraded in the following cases:

- At least one of the configured SafeGuard Servers has changed (applies to managed endpoints only).
- The policies need to be changed (applies to standalone endpoints only).
- To apply Certificate Change Orders (CCO).
- When the hash algorithm that is used to sign the self-signed certificates is changed from SHA-128 to SHA-256.

For further information, see [Change algorithm for self-signed certificates \(page 165\)](#)

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

2.15 *About migrating*

Migration means a change of installed products, modules, or features 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.

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.

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

2.15.1 *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.

Note the following:

- **Synchronized Encryption** cannot be installed on endpoints with **File Encryption** (location-based file encryption) already in place.
- A change from **SafeGuard Full Disk Encryption** (volume-based encryption) to **BitLocker** or the other way round requires the product to be uninstalled and reinstalled. Encrypted files must 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. Encrypted files must be decrypted.

- A change from **Data Exchange** to **File Encryption** requires two restarts and a logon to activate transparent encryption on network shares.

See the release notes for the system requirements for each module.

For information about migrating to a different operating system, see [Migrate endpoints to a different operating system \(page 82\)](#).

2.15.2 Migrate endpoints to a different operating system

Endpoints with SafeGuard Enterprise can be migrated from Windows 7/8 to Windows 10. Only for endpoints running Windows 7 and SafeGuard Full Disk Encryption, the latter has to be uninstalled before migrating to Windows 10. SafeGuard Full Disk Encryption is not supported on Windows 10. For information on uninstallation, see [About uninstallation \(page 335\)](#). For information on using BitLocker, see [Prepare for BitLocker Drive Encryption support \(page 59\)](#).

It is not possible to migrate endpoints from Windows 7 to Windows 8 when SafeGuard Enterprise is installed. If you are using operating systems older than Windows 10, it is only possible to update the Service Pack version of the operating system series installed.

3. SafeGuard Management Center

The SafeGuard Management Center is the console for managing computers encrypted with SafeGuard Enterprise. With SafeGuard Management Center you can implement a company-wide security strategy and apply it to the endpoints. SafeGuard Management Center enables you to:

- Create or import the organizational structure.
- Create security officers.
- Define policies.
- Export and import configurations.
- Monitor computers through comprehensive logging functionality.
- Recover passwords and access to encrypted endpoints.

With the SafeGuard Management Center you have Multi Tenancy support for managing multiple domains and databases. You can manage different SafeGuard Enterprise Databases and maintain different configurations.

 **Note** Some features are not included in all licenses. For information on what is included in your license, contact your sales partner.

Only privileged users - security officers - can access the SafeGuard Management Center. Several security officers can work with the data simultaneously. The various security officers can perform actions in accordance with the roles and rights assigned to them.

You can customize SafeGuard Enterprise policies and settings to your needs. After new settings have been saved to the database, they can be transferred to the endpoints where they become active.

Tip

This section provides information about the key procedures for managing endpoints. For advanced management, see [SafeGuard Management Center advanced \(page 107\)](#).

3.1 Logging on to the SafeGuard Management Center

During SafeGuard Enterprise initial configuration, an account is created for a Master Security Officer. This account is required the first time you log on to SafeGuard Management Center. To start SafeGuard Management Center, the user must know the password for the certificate store and have the certificate's private key.

For further information see [Create the Master Security Officer \(MSO\) \(page 39\)](#).

The logon procedure varies depending on whether you run the SafeGuard Management Center as connected to one database (Single Tenancy) or to multiple databases (Multi Tenancy).

 **Note** Two security officers must not use the same Windows account on the same computer. Otherwise it is not possible to separate their access rights properly.

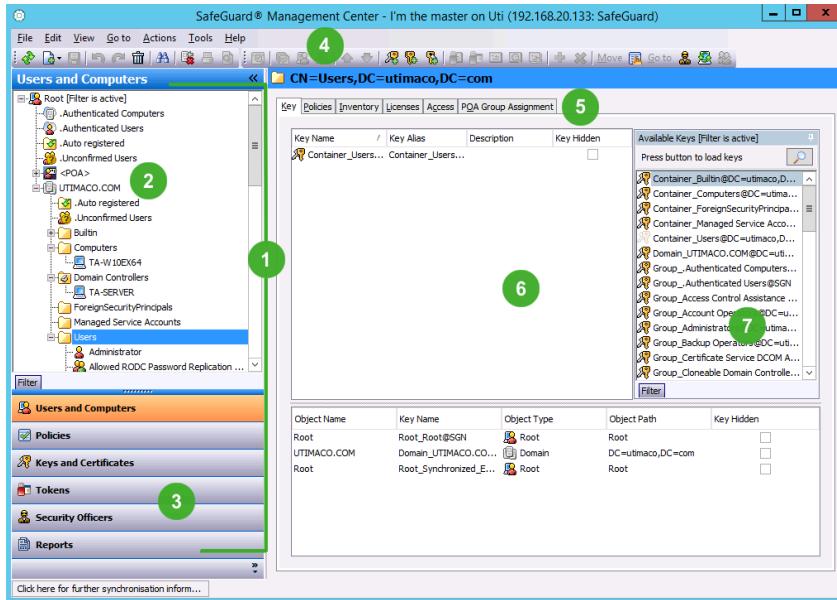
3.1.1 Log on in Single Tenancy mode

1. Start the SafeGuard Management Center. A logon dialog is displayed.
2. Log on as MSO (Master Security Officer) and enter the certificate store password specified during initial configuration. Click **OK**.

SafeGuard Management Center is launched.

 **Note** If you enter an incorrect password, an error message is displayed and a delay is imposed for the next logon attempt. The delay period is increased with each failed logon attempt. Failed attempts are logged.

3.2 SafeGuard Management Center user interface



1. **Navigation area**
2. **Navigation window** with administrative objects.
3. **Buttons for all administrative tasks**
4. **Toolbar**
5. **Tabs** to select different tasks or to display information.
6. **Action area** displays depend on the selection in the navigation area.
7. **Associated views** can contain essential elements or information for administration of the object currently being processed.

Navigation area

The navigation area contains buttons for all administrative actions:

- **Users and Computers**

To import groups and users from an active directory, from the domain or from an individual computer.

- **Policies**

To create policies.

- **Keys and Certificates**

To manage keys and certificates.

- **Tokens**

To manage tokens and smartcards.

- **Security Officers**

To create new security officers or roles and define actions which require additional authorization.

- **Reports**

To create and manage records of all security-related events.

Navigation window

Objects which are to be processed or can be created are displayed in the navigation window (Active Directory objects such as OUs, users and computers, policy items etc.). The objects displayed depend on the selected task.

 **Note** In **Users and Computers**, the objects shown in the navigation window directory tree depend on the security officer's access rights for directory objects. The directory tree only shows objects the logged on security officer has access to. Objects that are denied are not shown, except if there are nodes lower in the tree that the security officer has access rights for. In this case the denied objects are greyed out. If the security officer has **Full access** rights, the object is displayed in black. Objects with **Read only** access are displayed in blue.

Action area

In the action area, you define settings for the objects selected in the navigation window. The action area contains various tabs for processing objects and specifying settings.

The action area also includes information about the selected objects.

Associated views

In these views, additional objects and information are displayed. They provide useful information for system administration and make use of the system easier. You can for example assign keys to objects by using drag-and-drop.

Toolbar

Contains symbols for the different SafeGuard Management Center actions. Symbols are displayed as and when they are available for the selected object.

After logon, the SafeGuard Management Center always opens with the view in which it was closed.

3.2.1 Language settings

The language settings for the setup wizards and the different SafeGuard Enterprise components are as follows:

Wizards

The installation and configuration wizards of the different installation packages use the language setting of the operating system. If the operating system language is not available for these wizards, they default to English automatically.

SafeGuard Management Center

You can set the language of the SafeGuard Management Center as follows:

- In SafeGuard Management Center, click **Tools > Options > General**. Select **Use user defined language** and select an available language.
- Restart SafeGuard Management Center. It is displayed in the selected language.

SafeGuard Enterprise on endpoints

You set the language of SafeGuard Enterprise on endpoints in a policy of the type **General Settings** in the SafeGuard Management Center, setting **Customization > Language used on client**:

- If the language of the operating system is selected, SafeGuard Enterprise uses the language setting of the endpoint's operating system. If the operating system language is not available in SafeGuard Enterprise, the SafeGuard Enterprise language defaults to English.
- If one of the available languages is selected, SafeGuard Enterprise functions are displayed in the selected language on the endpoint.

3.2.2 Check database integrity

When you log on to the database, database integrity is automatically verified. If this check results in any errors, the **Verify Database Integrity** dialog is displayed.

You can also start the database integrity check manually any time after logon and display the **Verify Database Integrity** dialog:

1. In the SafeGuard Management Center, select **Tools > Database integrity**.

2. Check the tables by clicking **Check all** or **Check selected**.

Erroneous tables are marked in the dialog. To repair them, click **Repair**.

To repair tables you have to be a **Master Security Officer** or a **Database Recovery Officer**, see, [Predefined roles \(page 130\)](#)).

 **Note** After a SafeGuard Enterprise backend update (SQL) the database integrity check will always be started. The check only needs to be performed once per SafeGuard Enterprise Database to finish the update.

3.3 *Working with policies*

The following sections describe the administrative tasks concerning policies, for example creating, grouping and backing up policies.

For assigning, removing or editing policies, you need **Full access** rights to the relevant objects as well as to any group that is activated for the policies involved.

For a description of all policy settings available with SafeGuard Enterprise, see [Policy types and their fields of applications \(page 230\)](#).

3.3.1 *Create policies*

1. Log on to the SafeGuard Management Center with the password set during initial configuration.
2. In the navigation area, click **Policies**.
3. In the navigation window, right-click **Policy Items** and select **New**.
4. Select the policy type.

A dialog for naming the new policy is displayed.

5. Enter a name and optionally a description for the new policy.

Policies for Device Protection:

If you create a policy for device protection, you must also specify the target for device protection. Possible targets are:

- Mass storage (boot volumes/other volumes)
- Removable media
- Optical drives

- Storage device models
- Distinct storage devices
- Cloud storage

For each target, a separate policy has to be created. Later on you can combine the individual policies in a policy group named *Encryption*, for example.

6. Click **OK**.

The new policy is displayed in the navigation window below **Policy Items**. In the action area, all settings for the selected policy type are displayed and can be changed.

3.3.2 Edit policy settings

When you select a policy in the navigation window, you can edit the policy settings in the action area.

 **Note**

 not configured	A red icon in front of a not configured setting indicates that for this policy setting a value has to be defined. To be able to save the policy, you first have to select a setting other than not configured .
---	---

Setting policy settings to default values

In the toolbar the following icons are available for setting policy settings:

Icon	Policy setting
	Displays default values for policy settings that have not been configured (setting not configured). The default values for policy settings are displayed by default. Click the icon to hide the default values.
	Sets the marked policy setting to not configured .
	Sets all policy settings in an area to not configured .
	Sets the default value for the marked policy.
	Sets all policy settings in an area to the default value.

Differentiating between machine- and user-specific policies

Policy displayed in blue	Policy is applied to machines only, not users.
Policy displayed in black	Policy is applied to machines and users.

3.3.3 Policy groups

SafeGuard Enterprise policies can be combined in policy groups. A policy group may contain different policy types. In the SafeGuard Management Center, a **Default** policy group is available that is assigned to **Root** under **Users and Computers** by default.

If you put policies of the same type in a group, the settings are merged automatically. In this case, you can define priorities for using the settings. The settings of a policy with a higher priority overwrite the settings of a policy with a lower priority.

A defined policy setting will overwrite settings from other policies, if

- the policy with that setting has a higher priority.
- the policy setting has not been defined yet (**not configured**).

 **Note** Overlapping policies assigned to a group might result in incorrect calculation of the priorities. Ensure that you use disjunctive policy settings.

Policy groups must always contain at least one policy. Policy groups with no content disrupt the use of other policies. Make sure that you use policy groups only if they also contain a policy.

Exception concerning device protection:

Policies for device protection are only merged, if they were defined for the same target (for example boot volume). If they are for different targets, the settings will be added.

Unmanaged endpoints

The most common reason for using policy groups is to use them for initial configuration of unmanaged Windows SafeGuard Enterprise endpoints.

3.3.3.1 Combine policies into groups

Prerequisite: The individual policies of different types must have been created beforehand.

1. In the navigation area, click **Policies**.
2. In the navigation window, right-click **Policy Groups** and select **New**.
3. Click **New Policy Group**. A dialog for naming the policy group is displayed.
4. Enter a name and optionally a description for the policy group. Click **OK**.

5. The new policy group is displayed in the navigation window under **Policy Groups**.
6. Select the policy group. The action area shows all elements required for grouping the policies.
7. To add the policies to the group, drag them from the list of available policies to the policy area.
8. You can define a **priority** for each policy by arranging the policies in order using the context menu.

If you put policies of the same type in a group, the settings are merged automatically. In this case, you can define priorities for using the settings. The settings of a policy with a higher priority overwrite the settings of a policy with a lower priority. If an option is set to **not configured**, the setting is **not overwritten** in a policy of a lower priority.

Exception concerning device protection:

Policies for device protection are only merged, if they were defined for the same target (for example boot volume). If they are for different targets, the settings are added.

9. Save the policy with **File > Save**.

The policy group now contains the settings of all the individual policies.

3.3.3.2 Policy grouping results

The result of policy grouping is displayed separately.

To display the result, click the **Resulting** tab.

- For each policy type a separate tab is shown.

The settings resulting from combining the individual policies into a group are displayed.

- For policies for device protection, a tab is shown for each policy target (for example boot volumes, drive X etc.).

3.3.4 Back up policies and policy groups

You can create backups of policies and policy groups as XML files. If necessary, the relevant policies/policy groups can then be restored from these XML files.

1. In the navigation window, select the policy/policy group under **Policy Items** or **Policy Groups**.
2. Right-click to display the context menu and select **Backup Policy**.

 **Note** The **Backup Policy** command is also available in the **Actions** menu.

3. In the **Save As** dialog, enter a file name for the XML file and select the a storage location for the file. Click **Save**.

The backup of the policy/policy group is stored as an XML file in the specified directory.

When you add policies to a backed-up policy group, they will automatically be added to the backup.

3.3.5 Restore policies and policy groups

The policy/policy group backup to be restored must have been created using the same SafeGuard Enterprise version as the one you use for restoring it. For example: you cannot restore a policy group backup that has been created with SafeGuard Enterprise 7.0 with SafeGuard Enterprise 8.1.

To restore a policy/policy group from an XML file:

1. In the navigation window, select **Policy Items/Policy Groups**.
2. Right-click to display the context menu and select **Restore Policy**.

 **Note** The **Restore Policy** command is also available in the **Actions** menu.

3. Select the XML file from which the policy/policy group is to be restored and click **Open**.

The policy/policy group is restored.

3.3.6 Assign policies

To assign policies, you need **Full access** rights to the objects involved.

1. Click **Users and Computers**.
2. In the navigation window, select the required container object (for example OU or domain).
3. Switch to the **Policies** tab.

All items required for policy assignment are displayed in the action area.

4. To assign a policy, drag the policy from the list into the **Policies** tab.
5. You can define a **Priority** for each policy by arranging the policies in order using the context menu. The settings of higher-ranked policies override those below. If you select **No Override** for a policy, its settings will not be overridden by those from other policies.

 **Note**

If you select **No Override** for a low-priority policy, this policy will take higher priority than a higher-ranking policy.

To change the **Priority** or the **No Override** setting for policies in **Users and Computers**, you need **Full Access** rights for all objects the policies are assigned to. If you do not have **Full Access** rights for all objects, the settings are not editable. If you try to edit these fields, an info message is displayed.

6. The **.Authenticated users** and **.Authenticated computers** are displayed in the activation area.

The policy applies to all groups within the OU and/or domain.

3.3.6.1 Activate policies for individual groups

Policies are always assigned to an OU, a domain or a workgroup. They apply by default to all groups in those container objects (**.Authenticated users** and **.Authenticated computers** groups are displayed in the activation area).

However, you can also define policies and activate them for one or more groups. These policies then apply exclusively to these groups.

 **Note** To activate policies for individual groups, you need **Full access** rights for the relevant group.

1. Assign the policy to the OU the group is contained in.
2. **.Authenticated Users** and **.Authenticated Computers** are displayed in the activation area.
3. Drag these two groups from the activation area to **Available Groups** list. In this constellation, the policy is neither effective for users nor computers.
4. Now drag the required group (or multiple groups) from the **Available Groups** list into the activation area.

This policy now applies exclusively to this group.

If policies have also been assigned to the higher-ranking OU, this policy applies to this group in addition to those defined for the whole OU.

3.3.7 Manage policies in Users and Computers

Apart from the **Policies** area in the SafeGuard Management Center, you can also view and modify the contents of a policy where policy assignment is done, in **Users and Computers**.

1. Click **Users and Computers**.
2. In the navigation area, select the required container object.
3. You can open policies for viewing/modifying them from two locations.
 - Switch to the **Policies** tab, or
 - switch to the **RSOP** tab.
4. Right-click the required assigned or available policy and select **Open** from the context menu.
The policy dialog is displayed and you can view and edit the policy settings.
5. Click **OK** to save your changes.
6. To display the policy properties, right-click the required policy and select **Properties** from the context menu.
The **Properties** dialog for the policy is displayed. Here you can view **General** and **Assignment** information.

3.4 Working with configuration packages

In the SafeGuard Management Center, you can create the following types of configuration packages:

- **Configuration package for the SafeGuard Enterprise Server**

For successful operation, you need to create a configuration package for the SafeGuard Enterprise Server, defining the database and SSL connection, enabling the scripting API or using SafeGuard Enterprise together with Sophos Mobile.

- **Configuration package for managed endpoints**

Endpoints that have a connection to the SafeGuard Enterprise Server receive their policies through this server. For successful operation after installation of the SafeGuard Enterprise client

software, you need to create a configuration package for managed computers and deploy it to them.

After the first configuration of the endpoint by the configuration package, the endpoint receives policies through the SafeGuard Enterprise Server after you have assigned them in the **Users and Computers** area of the SafeGuard Management Center.

• Configuration package for Macs

Macs receive the server address and the company certificate through this package. They report their status information which is displayed in the SafeGuard Management Center. For information on how to create configuration packages for Macs, see [Create configuration package for Macs \(page 97\)](#).

• Configuration package for unmanaged endpoints

Unmanaged endpoints are never connected to the SafeGuard Enterprise Server at any point in time, they operate in standalone mode. They receive their policies by configuration packages. For successful operation, you need to create a configuration package containing the relevant policy groups and distribute it to the endpoints by company distribution mechanisms. Whenever you change any policy settings, you have to create new configuration packages and distribute them to the endpoints.

 **Note** Configuration packages for unmanaged endpoints can only be used on Windows endpoints.

Check your network and computers in regular intervals for old or unused configuration packages and make sure that you delete them for security reasons. Always make sure that you uninstall the old configuration packages before installing the new one on the computer/server.

3.4.1 *Create configuration package for managed endpoints*

Prerequisites

- In the **Users and Computers** navigation area, under the **Inventory** tab, check if a company certificate change is required for the endpoints that should receive the new configuration package. If the field **Current Company Certificate** is not checked, the currently active company certificates in the SafeGuard Enterprise Database and on the computer differ and a company certificate change is therefore required.

1. In the SafeGuard Management Center, on the **Tools** menu, click **Configuration Package Tool**.
2. Select **Managed client packages**.

3. Click **Add Configuration Package**.
4. Enter a name of your choice for the configuration package.
5. Assign a primary SafeGuard Enterprise Server (the secondary server is not necessary).
6. If required, specify a policy group which must have been created beforehand in the SafeGuard Management Center to be applied to the endpoints. If you want to use service accounts for post-installation tasks on the endpoint, make sure that you include the respective policy setting in this first policy group. See the [SafeGuard Enterprise 8 administrator help](#).
7. If the currently active company certificate in the SafeGuard Enterprise Database differs from the one on the endpoints that should receive the new configuration package, select the appropriate **CCO** (Company Certificate Change Order). In **Users and Computers**, in the **Inventory** tab of the relevant domain, OU or computer a missing check mark under **Current Company Certificate** indicates that a company certificate change is required. You can find information on the required CCO in the **CCOs** tab of the **Configuration Package Tool** in the **Tools** menu.

 **Note** Deployment of the new configuration package on the endpoint will fail, if the currently active company certificates in the SafeGuard Enterprise Database and on the endpoint do not match and no appropriate **CCO** is included.

8. Select the **Transport Encryption** mode defining how the connection between SafeGuard Enterprise Client and SafeGuard Enterprise Server is to be encrypted, either Sophos encryption or SSL encryption.

The advantage of SSL is that it is a standard protocol and that a faster connection can be achieved as when using SafeGuard transport encryption. SSL encryption is selected by default.

9. Specify an output path for the configuration package (MSI).

10. Click **Create Configuration Package**.

If you have selected SSL encryption as the **Transport Encryption** mode, the server connection is validated. If the connection fails, a warning message is displayed.

The configuration package (MSI) has now been created in the specified directory. You now need to distribute and deploy this package to the endpoints.

3.4.2 Create configuration package for unmanaged endpoints

1. In the SafeGuard Management Center, on the **Tools** menu, click **Configuration Package Tool**.
2. Select **Standalone client packages**.

3. Click **Add Configuration Package**.
4. Enter a name of your choice for the configuration package.
5. Specify a **Policy Group** which must have been created beforehand in the SafeGuard Management Center to be applied to the endpoints.
6. Under **POA Group**, you can select a POA user group to be assigned to the endpoint. POA users can access the endpoint for administrative tasks after the SafeGuard Power-on Authentication has been activated. To assign POA users, the POA group must have been created beforehand in the **Users and Computers** area of the SafeGuard Management Center.
7. If the currently active company certificate in the SafeGuard Enterprise Database differs from the one on the endpoints that should receive the new configuration package, select the appropriate **CCO** (Company Certificate Change Order).

 **Note** Deployment of the new configuration package on the endpoint will fail, if the currently active company certificates in the SafeGuard Enterprise Database and on the endpoint do not match and no appropriate **CCO** is included.

8. Under **Key Backup Location**, specify or select a shared network path for storing the key recovery file. Enter the share path in the following form: \\network computer\\, for example \\mycompany.edu\\. If you do not specify a path here, the end user is prompted to name a storage location for this file when first logging on to the endpoint after installation.

The key recovery file (XML) is needed to enable recovery of Sophos SafeGuard protected endpoints and is generated on each Sophos SafeGuard protected endpoint.

 **Note** Make sure to save this key recovery file at a file location accessible to the helpdesk. Alternatively, the files can be provided to the helpdesk by different mechanisms. This file is encrypted by the company certificate. It can therefore be saved to any external media or to the network to provide it to the helpdesk for recovery purposes. It can also be sent by e-mail.

9. Specify an output path for the configuration package (MSI).
10. Click **Create Configuration Package**.

The configuration package (MSI) has now been created in the specified directory. You now need to distribute and deploy this package to the endpoints.

3.4.3 Create configuration package for Macs

A configuration package for a Mac contains the server information and the company certificate. The Mac uses this information to report status information (SafeGuard POA on/off, encryption state and so on). The status information is displayed in the SafeGuard Management Center.

1. In the SafeGuard Management Center, on the **Tools** menu, click **Configuration Package Tool**.
2. Select **Managed client packages**.
3. Click **Add Configuration Package**.
4. Enter a name of your choice for the configuration package.
5. Assign a primary SafeGuard Enterprise Server (the secondary server is not necessary).
6. Select **SSL** as **Transport Encryption** for the connection between the endpoint and SafeGuard Enterprise Server. **Sophos** as **Transport Encryption** is not supported for Mac.
7. Specify an output path for the configuration package (ZIP).
8. Click **Create Configuration Package**.
The server connection for the **SSL Transport Encryption** mode is validated. If the connection fails, a warning message is displayed.

The configuration package (ZIP) has now been created in the specified directory. You now need to distribute and deploy this package to your Macs.

3.5 Enhanced authentication - the .Unconfirmed Users group

Users who log on to SafeGuard Enterprise need to be authenticated against Active Directory before they have access to their key rings.

If users cannot be authenticated when they log on, they will be moved to the **.Unconfirmed Users** group. This group is displayed in the global root node and in every domain or workgroup. Enhanced authentication applies to Windows and macOS users.

Possible reasons for which users cannot be authenticated when they log on are:

- The user provided credentials that do not match the credentials stored in Active Directory.
- The user is a local user on the endpoint.

Since only Active Directory users can be authenticated using a domain controller, a local user will always be moved to the **.Unconfirmed Users** group when they log on for the first time.

- The Active Directory authentication server is not reachable.
- The user belongs to a domain that is not imported from Active Directory.

In this case users will be added to the global **.Unconfirmed Users** group that is displayed directly below the **Root** node in **Users and Computers**.

- The authentication failed due to an unexpected error.

See also [Sophos knowledge base article 124328](#).

As long as users reside in the **.Unconfirmed Users** group they do not have access to their key rings.

If you click on an **.Unconfirmed Users** group, details of the users in the group (for example, the reason why a user is in the group) are displayed in the **Unconfirmed Users** tab in the right-hand pane.

On Windows endpoints, the **Client Status** dialog displays **unconfirmed user** under **SGN user state**.

On macOS endpoints, the **User** tab of the Sophos SafeGuard Preference pane displays **Unconfirmed user** under **SafeGuard User State**.

For logged events, see [Auditing \(page 204\)](#).

Enhanced Authentication and BitLocker

If you use BitLocker managed by SafeGuard Enterprise, you need to allow registration of new SGN users for **Everybody**:

1. In the **Policies** navigation area, create a new policy of the type **Specific Machine Settings** or select an existing one.
2. In the **User Machine Assignment (UMA)** section, go to the **Allow registration of new SGN users for** setting and select **Everybody** from the drop-down list.
3. Go to **Users and Computers** and assign the policy to your user groups.

3.5.1 Confirm users

As a security officer you have to verify users in the **.Unconfirmed Users** group. If they are authorized users, you have to explicitly confirm them to allow access to their key rings. Without their key ring users cannot access encrypted data.

To confirm users in the **.Unconfirmed Users** group:

1. In the Management Center, select the **.Unconfirmed Users** group.

Users who have not been authenticated against Active Directory are listed. You can click on individual users to display detailed information in the right-hand pane.

2. Verify if users are allowed to access the SafeGuard Enterprise key ring.

3. If they are, right-click on the user in the left-hand pane under **.Unconfirmed Users** and click **Confirm user**.

You can confirm all users in the **.Unconfirmed Users** group by selecting the group itself and clicking **Confirm all users** in the context menu.

Confirmed users will be moved to the correct Active Directory structure and will be able to access their key ring.

Confirmation of users can also be performed via scripting API calls.

3.5.2 Automatically confirm users

You can configure SafeGuard Enterprise to automatically confirm users that cannot be authenticated against Active Directory.

To confirm users in the **.Unconfirmed Users** group automatically:

1. In the Management Center, select **Options** from the **Tools** menu.

2. Go to the **Directory** tab.

3. Activate the **Automatically confirm users that cannot be authenticated against Active Directory** option.

4. Click **OK**.

All users that are moved to the **.Unconfirmed Users** group when they log on are confirmed automatically and get access to their key rings.

3.6 User Machine Assignment

SafeGuard Enterprise manages the information about the users who are allowed to log on to a particular machine in a list which is referred to as the User Machine Assignment (UMA).

For a user to be included in the UMA, they must have logged on once to a computer on which SafeGuard Enterprise has been installed and be registered in the SafeGuard Management Center as a "full" user in terms of SafeGuard Enterprise. A "full" user is one for whom a certificate has been generated after the first logon and for whom a key ring has been created. Only then can this user

data be replicated on other computers. After replication, the user can log on to this computer at the SafeGuard POA.

If the default setting applies, the first user to log on to the computer after the installation of SafeGuard Enterprise is entered as the owner of that computer in the UMA.

This attribute allows the user, after they have authenticated at SafeGuard Power-on Authentication, to enable other users to log on to that computer. See the [SafeGuard Enterprise 8 administrator help](#). They will also be added to the UMA for this computer.

An automatic list is generated which determines which user is allowed to log on to which computer. This list can be edited in the SafeGuard Management Center.

3.6.1 User types

There are various types of user in SafeGuard Enterprise. For more information on how the default behavior of these user types can be changed, see [Policy types and their fields of applications \(page 230\)](#).

- **Owner:** The first user to log on to an endpoint after the installation of SafeGuard Enterprise is not just entered as an SGN user, but also as the owner of that endpoint. Provided that the default settings have not been changed, an owner has the right to enable other users to log on to the endpoint and become SGN users.
- **SGN user:** A "full" SGN user is allowed to log on at the SafeGuard Power-on Authentication, is added to the UMA (User Machine Assignment) and is provided with a user certificate and a key ring for accessing encrypted data.
- **SGN Windows user:** A SGN Windows user is not added to the SafeGuard POA, but has a key ring for accessing encrypted files, just as a SGN user. He is also added to the UMA, which means that he is allowed to log on to Windows on that endpoint.
- **SGN guest user:** A SGN guest user is not added to the UMA, is not provided with rights to log on to the SafeGuard POA, is not assigned a certificate or a key ring and is not saved to the database. See [Specific machine settings - basic settings \(page 266\)](#) for information on how to prevent a SGN guest user from logging on to Windows.
- **Service account:** With service accounts, users (for example rollout operators, members of the IT team) can log on to endpoints after the installation of SafeGuard Enterprise without activating the SafeGuard POA and without being added as SGN users (owners) to the endpoints. Users included on a service account list are treated as SGN guest users after their Windows logon at the endpoint.

- **POA user:** After activation of the POA it might still be necessary to perform administrative tasks. POA users are predefined local accounts that are allowed to pass the POA. There is no automatic logon to Windows. The users logging on with POA user accounts log on to Windows with their existing Windows accounts. The accounts are defined in the **Users and Computers** area of the SafeGuard Management Center (user ID and password) and assigned to the endpoint in POA groups. For further information, see the [SafeGuard Enterprise 8 administrator help](#).

3.6.2 User Machine Assignment in the SafeGuard Management Center

Users can be allocated to specific computers in the SafeGuard Management Center. If a user is assigned to a computer in the SafeGuard Management Center (or vice versa) this allocation is incorporated into the UMA. The user data (certificate, key, etc.) is replicated on this computer and the user can log on to this computer. When a user is removed from the UMA, all user data is automatically deleted from the SafeGuard POA. The user can no longer log on at the SafeGuard POA with their user name and password.

 **Note** In **Users and Computers**, to view the assignment of users and computers you need at least **Read only** access rights for one of the objects (user or computer) involved. To define or change the assignment, you need **Full access** rights for both of the objects involved. The UMA display showing available users/machines is filtered according to your access rights. In the UMA grid display, which shows the users assigned to computers and vice versa, objects for which you do not have the required access rights are shown for your information, but the assignment cannot be modified.

When you assign a user to a computer, you can also specify who can allow other users to log on to this computer.

Under **Type** the SafeGuard Management Center indicates how the user was added to the SafeGuard Enterprise Database. **Adopted** means that the user has been added to the UMA on an endpoint.

If no one is assigned in the SafeGuard Management Center and no user is specified as the owner, the first user to log on after the installation of SafeGuard Enterprise on the computer is entered as the owner. This user can allow further users to log on to this computer. If users are assigned to this computer in the SafeGuard Management Center at a later date, they can log on at the SafeGuard Power-on Authentication. Nevertheless, such users must be full users (with existing certificate and key). The owner of the computer does not need to assign access entitlements in this case.

The following settings are used to specify who is allowed to add users to the UMA:

- **Can Become Owner:** If this setting is selected, the user can be registered as the owner of a computer.

- **User is Owner:** This setting means that this user is entered in the UMA as the owner. Only one user per computer can be entered in the UMA as the owner.

The **Allow registration of new SGN users for** policy setting in policies of the type **Specific Machine Settings** determines who is allowed to add further users to the UMA. The **Enable registration of SGN Windows users** setting in **Specific Machine Settings** policies determines whether SGN Windows users may be registered on the endpoint and added to the UMA.

- **Allow registration of new SGN users for**

Nobody

Even the user entered as the owner cannot add more users to the UMA. The option for an owner to add further users is deactivated.

Owner (default setting)

 **Note** A security officer can always add users in the SafeGuard Management Center.

Everybody

Lifts the restriction that users may only be added by the owner.

 **Note** For endpoints that do not have the Device Encryption module installed the **Allow registration of new SGN users for** setting must be set to **Everybody** if it should be possible on the endpoint to add more than one user to the UMA with access to their key ring. Otherwise users can only be added in the Management Center. This setting is only evaluated on managed endpoints. For more information, see [Sophos knowledge base article 110659](#).

- **Enable registration of SGN Windows users**

If you select **Yes**, SGN Windows users can be registered on the endpoint. An SGN Windows user is not added to the SafeGuard POA, but has a key ring for accessing encrypted files, just as an SGN user. If you select this setting, all users, that would have otherwise become SGN guest users, will become SGN Windows users. The users are added to the UMA as soon as they have logged on to Windows. SGN Windows users can be removed from the UMA automatically on managed endpoints and manually on unmanaged endpoints. For further information, see [Specific machine settings - basic settings \(page 266\)](#).

Example:

The following example shows how you can assign logon entitlements in the SafeGuard Management Center to just three users (User_a, User_b, User_c) for Computer_ABC.

First: Specify the response you require in the SafeGuard Management Center. SafeGuard Enterprise is installed on all endpoints during the night. In the morning, the users should be able to log on to the computer with their credentials.

1. In the SafeGuard Management Center, assign User_a, User_b and User_c to Computer_ABC. (**Users and Computers** -> Select computer_ABC -> Assign user by drag-and-drop). By doing this, you have specified a UMA.
2. In a policy of the type **Specific Machine Settings**, set **Allow registration of new SGN users for to Nobody**. Since User_a, User_b and User_c are not allowed to add new users is not necessary to specify a user as an owner.
3. Assign the policy to the computer and/or to a point within the directory structure at which it will be active for the computer.

When the first user logs on to Computer_ABC, an autologon is implemented for the SafeGuard POA. The computer policies are sent to the endpoint. Since User_a is included in the UMA and will become a full user when logging on to Windows. The user's policies, certificates and keys are sent to the endpoint. The SafeGuard POA is activated.

 **Note** The user can check the status message in the SafeGuard System Tray Icon (balloon tool tip) when this process has completed.

User_a is now a full user in terms of SafeGuard Enterprise and after the first logon can authenticate at the SafeGuard POA and is automatically logged on.

User_a now leaves the computer and User_b wants to log on. As the SafeGuard POA is activated, there is no more autologon.

User_b and User_c have two options for gaining access to this computer.

- User_a deactivates the **Pass through to Windows** option in the SafeGuard POA logon dialog and logs on.
- User_b uses Challenge/Response to log on at the SafeGuard POA.

In both cases, the Windows logon dialog is displayed.

User_b can enter their Windows credentials. The user's policies, certificates and keys are sent to the endpoint. The user is activated in the SafeGuard POA. User_b is now a full user in terms of SafeGuard Enterprise and after the first logon can authenticate themselves at the SafeGuard POA and will be automatically logged on.

While the computer policy specifies that no one can import users to this computer, since these users are already in the UMA, User_b and User_c nevertheless gain "full" user status at the Windows logon and are activated in the SafeGuard POA.

No other users will be added to the UMA or will ever be able to authenticate themselves at the SafeGuard Power-on Authentication. Any users logging on to Windows who are not User_a, User_b or User_c are excluded from the UMA in this scenario and will never be active in the SafeGuard POA.

Users can always be added later on in the SafeGuard Management Center. However, their key ring will not be available after the first logon as synchronization will only be triggered by this first logon. After logging on again, the key ring will be available and the users can access their computers according to policies applying. If they have never successfully logged on to an endpoint, they can be added as described above.

 **Note** If the last valid user certificate is removed from the UMA by an SO or MSO, any user can pass the SafeGuard POA of the corresponding computer. The same applies if the domain of the endpoint changes. Then only Windows credentials are necessary to log on to the computer, to reactivate the SafeGuard POA and to be added as the new owner.

This description applies only to Windows endpoints, not to Macs. Adding multiple users to a Mac in large environments can result in significant performance disruptions in the alignment of policies between the endpoint and the server, and in Active Directory synchronization in the Management Center or Task Scheduler. We strongly recommend that you do not assign users to Macs in the Management Center.

3.6.2.1 Block User

If you select the check box in the **Block User** column, the user is no longer allowed to log on to the relevant computer. If the relevant user is logged on when the policy with this setting becomes active on the computer, the user is logged off.

3.6.2.2 Groups

In the SafeGuard Management Center, computer groups can be assigned to a user (account) and/or user groups can be assigned to a computer.

To create a group: In **Users and Computers**, right-click the relevant object node where you want to create the group and select **New > Create new group > Full name**. Enter the name of the group and optionally a description. Click **OK**.

Example: Maintenance account

It is for example possible to use a single maintenance account to service a large number of computers. For this purpose the computers concerned must be in a single group. This group is then

assigned to a maintenance account (user). The owner of the maintenance account can log on to all computers within this group

Also, by assigning a group containing different users, these users can log on to a specific computer in a single step.

3.6.3 Assignment of user and computer groups

In **Users and Computers**, to view the assignment of user and computer groups you need at least **Read only** access rights for one of the objects (user or computer group) involved. To define or change the assignment, you need **Full access** rights for both of the objects involved. The UMA display showing available users/machines is filtered according to your access rights.

 **Note** You can assign individual users to a computer or vice versa using the same process as for groups.

1. Click **Users and Computers**.
2. To assign a group of computers to single user, select the user.
3. Click the **Computer** tab in the action area.

All computers and computer groups are displayed under **Available computers**.

4. Drag the selected groups from the **Available Groups** list into the action area.
5. A dialog is displayed asking whether the user should be the owner of all computers.

If there is no specified owner in the SafeGuard Management Center, the first user to log on to this computer is automatically entered as the owner. The user is the entitled to allow other users to access this computer. The condition is that the user **Can Become Owner**.

- If you answer **Yes**, the first user to log on to this computer becomes the owner and can allow access to other users.
- If you answer **No**, the user is not the owner of this computer.

It is not generally necessary for a service account owner to be the owner of the computer. This setting can be changed after initial assignment.

All computers from the assigned group are displayed in the action area.

The user can log on to all computers assigned in this way.

A user group can be assigned to a single computer in the same way.

3.7 Improve Sophos SafeGuard by sending anonymous usage data

Sophos is continuously trying to improve SafeGuard Enterprise. Accordingly, clients regularly send anonymized data to Sophos. This data is exclusively utilized for improving the product. It cannot be used to identify customers or machines, and does not contain any other confidential information. For more information, see [Sophos knowledge base article 123768](#).

Sending data to Sophos is optional. Because all data is sent anonymized, the data collection function is enabled by default. You can disable the function in the SafeGuard Management Center (Policies > General Settings > Feedback > Improve Sophos SafeGuard® by sending anonymous usage data).

3.7.1 Create policy to disable sending anonymous usage data

To disable sending anonymous usage data:

1. In the **Policies** navigation area, create a new policy of the type **General Settings** or select an existing one.
The **General Settings** tab is displayed.
2. Go to the **Feedback** section.
3. From the **Improve Sophos SafeGuard® by sending anonymous usage data** drop-down list, select **No**.
4. Go to **Users and Computers** and assign the new policy to your users and computers.
The function is now disabled. No usage data will be sent to Sophos.

3.8 SafeGuard Management Center advanced

This section provides information about advanced management functions.

3.8.1 Database maintenance

We recommend that you operate a permanent online backup for the database. Back up your database regularly to protect keys, company certificates and User Machine Assignments. Recommended

backup cycles are, for example: after the data is first imported, after major changes or at regular intervals, for example every week or every day.

For further information, see [Sophos knowledge base article 113001](#).

3.8.1.1 Repair a corrupted database configuration

A corrupted database configuration can be repaired by installing SafeGuard Management Center afresh to create a new instance of the database based upon the backed up certificate files. This guarantees that all existing SafeGuard Enterprise endpoints still accept policies from the new installation.

- The company and Master Security Officer certificates of the relevant database configuration must have been exported to .p12 files. The data must be available and valid.
- The passwords for the two .p12 files as well as for the certificate store must be known to you.

We only recommend this procedure if there is no valid database backup available. All computers that connect to a repaired backend lose their user-machine-assignment. As a consequence, Power-on Authentication is temporarily switched off. Challenge/Response mechanisms will not be available until the corresponding endpoint has successfully sent its key information again.

To repair a corrupted database configuration:

1. Reinstall the SafeGuard Management Center installation package. Open the SafeGuard Management Center. The **Configuration Wizard** is started automatically.
2. In **Database Connection**, check **Create a new database**. Under **Database settings**, configure the connection to the database. Click **Next**.
3. In **Security Officer Data**, select the relevant MSO and click **Import**.
4. In **Import Authentication Certificate** browse for the backed up certificate file. Under **Key file** enter and confirm the password specified for this file. Click **OK**.
5. The MSO certificate is imported. Click **Next**.
6. In **Company Certificate**, check **Restore using an existing company certificate**. Click **Import** to browse for the backed up certificate file that contains the valid company certificate. You are prompted to enter the password specified for the certificate store. Enter the password and click **OK**. Click **Yes** in the message displayed.

The company certificate is imported.

7. Click **Next** and then **Finish**.

The database configuration is repaired.

3.8.2 Working with multiple database configurations (Multi Tenancy)

Prerequisite:

- The feature Multi Tenancy must have been installed by a **Complete** installation, see [Installation \(page 14\)](#).
- The SafeGuard Management Center initial configuration must have been carried out, see [Start initial SafeGuard Management Center configuration \(page 37\)](#).

With Multi Tenancy you can configure different SafeGuard Enterprise Database instances and maintain them with one instance of the SafeGuard Management Center. This is particularly useful when you want to have different database configurations for different domains, organizational units or company locations.

For each database (tenant), you need to set up a separate SafeGuard Enterprise Server instance. Each database must be the same version. For example, it is not possible to manage SGN 7 databases and SGN 8.3 databases with a single SGN 8.3 Management Center.

To ease configuration, you can:

- Create several database configurations.
- Select previously created database configurations.
- Delete database configurations from the list.
- Import a previously created database configuration from a file.
- Export a database configuration to be reused later.

3.8.2.1 Create further database configurations

 **Note** You need to set up a separate SafeGuard Enterprise Server instance per database.

To create a further SafeGuard Enterprise Database configuration after initial configuration:

1. Start the SafeGuard Management Center. The **Select Configuration** dialog is displayed.
2. Click **New**. The SafeGuard Management Center Configuration Wizard starts automatically.
3. The Wizard guides you through the necessary steps of creating a new database configuration. Select the options as required. The new database configuration is generated.
4. To authenticate at the SafeGuard Management Center you are prompted to select the security officer name for this configuration and to enter their certificate store password. Click **OK**.

The SafeGuard Management Center is launched and connected to the new database configuration. The next time the SafeGuard Management Center is started, the new database configuration can be selected from the list.

3.8.2.2 Configure additional instances of the SafeGuard Management Center

You can configure additional instances of the SafeGuard Management Center to give security officers access for carrying out administrative tasks on different computers. SafeGuard Management Center can be installed on any computer on the network from which the databases can be accessed.

SafeGuard Enterprise manages the access rights to the SafeGuard Management Center in its own certificate directory. This directory must contain all certificates for all security officers authorized to log on to the SafeGuard Management Center. Logging on to the SafeGuard Management Center then requires only the password to the certificate store.

1. Install SGNManagementCenter.msi on a further computer with the required features.
2. Start SafeGuard Management Center on the computer. The Configuration Wizard is launched and guides you through the necessary steps.
3. On the **Welcome** page, click **Next**.
4. On the **Database Server Connection** page, under **Database Server**, select the required SQL database instance from the list. All database servers available on your computer or network are displayed. Under **Authentication**, activate the type of authentication to be used to access this database server instance. If you select **Use SQL Server Authentication with the following credentials**, enter the SQL user account credentials that your SQL administrator has created. Click **Next**.
5. On the **Database Settings** page, click **Select an available database** and select the relevant database from the list. Click **Next**.
6. In **SafeGuard Management Center Authentication**, select an authorized person from the list. If Multi Tenancy is enabled, the dialog shows the configuration the user will log on to. Enter and confirm the password for the certificate store.
A certificate store is created for the current user account and is protected by this password. You only need this password for any subsequent logon.

7. Click **OK**.

You see a message that the certificate and private key have not been found or cannot be accessed.

8. To import the data, click **Yes**, and then click **OK**. This starts the import process.

9. In **Import authentication key file**, click [...] and select the key file. Enter the **password for key file**. Enter the password for the certificate store previously defined in **Cert. store password or token PIN**. Select **Import to certificate store**, or select **Copy to token** to store the certificate on a token.

10. Enter the password once more to initialize the certificate store.

Certificates and private keys are now contained in the certificate store. Logging on to the SafeGuard Management Center then requires the password to the certificate store.

3.8.2.3 Connect to an existing database configuration

To work with an existing SafeGuard Enterprise Database configuration:

1. Start the SafeGuard Management Center.

The **Select Configuration** dialog is displayed.

2. Select the required database configuration from the drop-down list and click **OK**.

The selected database configuration is connected to the SafeGuard Management Center and becomes active.

3. To authenticate at the SafeGuard Management Center, you are prompted to select the security officer name for this configuration and to enter their certificate store password. Click **OK**.

The SafeGuard Management Center is launched and connected to the selected database configuration.

3.8.2.4 Export a configuration to a file

To save or reuse a database configuration, you can export it to a file:

1. Start the SafeGuard Management Center.

The **Select Configuration** dialog is displayed.

2. Select the respective configuration from the list and click **Export...**
3. To secure the configuration file, you are prompted to enter and confirm a password that encrypts the configuration file.
4. Click **OK**.
5. Specify a file name and storage location for the exported configuration file *.SGNConfig.

If this configuration already exists, you are asked if you want to overwrite the existing configuration.

The database configuration file is saved to the specified storage location.

3.8.2.5 Import a configuration from a file

To use or change a database configuration, you can import a previously created configuration into the SafeGuard Management Center. There are two ways to do so:

- with the SafeGuard Management Center (for Multi Tenancy)
- by double-clicking the configuration file (for Single and Multi Tenancy).

3.8.2.6 Import a configuration with the SafeGuard Management Center

1. Start the SafeGuard Management Center.

The **Select Configuration** dialog is displayed.

2. Click **Import...**, locate the required configuration file and click **Open**.
3. Enter the password for the configuration file defined during the export and click **OK**.

The selected configuration is displayed.

4. To activate the configuration, click **OK**.
5. To authenticate at the SafeGuard Management Center, you are prompted to select the security officer name for this configuration and to enter their certificate store password. Click **OK**.

The SafeGuard Management Center is opened and connected to the imported database configuration.

3.8.2.7 Import a configuration by double-clicking the configuration file (Single and Multi Tenancy)

 **Note** This task is available in the Single Tenancy and Multi Tenancy mode.

You can also export a configuration and distribute it to several security officers. The security officers then only need to double-click the configuration file to open a fully configured SafeGuard Management Center.

Use cases:

- You are using SQL authentication for the database and want to avoid that every administrator knows the SQL password:

In this case, you only need to enter it once, create a configuration file and distribute it to the respective security officers' computers.

- You want to run the Web Helpdesk on several computers:

All these computers need a connection to the database. To simplify the installation on these computers, you can create a configuration file and distribute it to the helpdesk officers.

Prerequisite: The initial configuration of the SafeGuard Management Center must have been carried out. For details, see [Setting up SafeGuard Management Center \(page 35\)](#).

1. Start the SafeGuard Management Center.
2. Select **Options** from the **Tools** menu and select the **Database** tab.
3. Enter or confirm the credentials for the SQL Database Server connection.
4. Click **Export configuration** to export this configuration to a file.
5. Enter and confirm a password for the configuration file.
6. Enter a file name and select a storage location.
7. Distribute this configuration file to the security officers' computers. Let them know the password for this file as well as the certificate store password needed to authenticate at the SafeGuard Management Center.
8. The security officers just need to double-click the configuration file.
9. They are prompted to enter the password for the configuration file.
10. To authenticate at the SafeGuard Management Center, they are prompted to enter their certificate store password.

The SafeGuard Management Center starts with the imported configuration. This configuration is the new default configuration.

3.8.2.8 Fast switching of database configurations

To ease administrative tasks for several tenants, the SafeGuard Management Center allows for fast switching of database configurations.

 **Note** This task is also available in Single Tenancy mode.

1. In the SafeGuard Management Center, select **Change configuration...** from the **File** menu.
2. Select the database you want to switch to from the drop-down list and click **OK**.

The SafeGuard Management Center is automatically restarted with the selected configuration.

3.8.2.9 Log on in Multi Tenancy mode

The logon process to the SafeGuard Management Center is extended when you have configured several databases (Multi Tenancy), see [Working with multiple database configurations \(Multi Tenancy\) \(page 109\)](#).

1. Start the SafeGuard Management Center from the product folder of the **Start** menu. The **Select Configuration** dialog is displayed.
2. Select the database configuration you want to use from the drop-down list and click **OK**.
The selected database configuration is connected to the SafeGuard Management Center and becomes active.
3. To authenticate at the SafeGuard Management Center, you are prompted to select the security officer name for this configuration and enter their certificate store password. Click **OK**.

The SafeGuard Management Center is opened and connected to the selected database configuration.

 **Note** If you enter an incorrect password, an error message is displayed and a delay is imposed for the next logon attempt. The delay period is increased with each failed logon attempt. Failed attempts are logged.

3.8.3 *Warning when company certificate expires*

At logon the SafeGuard Management Center starts to display a warning six months before the company certificate will expire and prompts you to renew it and deploy it on the endpoints. Without a valid company certificate an endpoint cannot connect to the server.

You can renew the company certificate at any time. Even if the company certificate has already expired. An expired company certificate will also be indicated by a message box. For information on how to renew the company certificate, see [Renew the company certificate \(page 168\)](#).

3.8.4 Search for users, computers and groups in the SafeGuard Enterprise Database

To display objects in the **Find Users, Computers and Groups** dialog, you need **Read only** or **Full access** rights for the relevant objects.

 **Note** When you search for objects, you only get the search results within the areas (domain) for which you have been granted access as a security officer. Only a Master Security Officer can successfully perform a root search process.

In **Users and Computers**, you can search for objects using different filters. For example, you can easily identify duplicates that may have been caused by an AD synchronization process with the **Duplicate users and computers** filter. This filter shows all computers with the same name in one domain and all users with the same name, logon name or pre-2000 logon name in one domain.

To search for objects:

1. In the navigation area of the SafeGuard Management Center, click **Users and Computers**.
2. In the **Users and Computers** navigation area, select the required container.
3. In the SafeGuard Management Center menu bar, click **Edit > Find**.

The **Find Users, Computers and Groups** dialog is displayed.

4. Select the required filter from the **Find** drop-down list.
5. In the **In** field, the selected container is displayed.

You can change this by selecting a different option from the drop-down list.

6. If you search for a specific object, enter the required search name in the **Search Name** field.
7. With the **Clear results after each search** check box, specify whether results should be cleared after each search process.
8. Click **Find now**.

The results are displayed in the **Find Users, Computers and Groups** dialog. If you click on one of the results in this dialog, the relevant entry is marked in the **Users and Computers** tree structure. If you have searched for duplicates for example, you can now easily delete them.

3.8.5 Display object properties in Users and Computers

To display object properties, you need **Full access** or **Read only** rights for the objects concerned.

1. In the navigation area of the SafeGuard Management Center, click **Users and Computers**.
2. In the navigation window of **Users and Computers**, right-click the required object and select **Properties**.

The properties of the selected object are displayed. If you have **Read only** access rights for the relevant object, the properties information is greyed out in the dialog and you cannot edit them.

3.8.6 Disabling policy deployment

As a security officer, you can disable the deployment of policies to the endpoints. To do so, click the **Enable/disable policy deployment** button in the SafeGuard Management Center toolbar or select **Enable/disable policy deployment** from the **Edit** menu. After disabling policy deployment, no policies are sent to the endpoints. To reverse the disabling of policy deployment, click the button or select the command again.

 **Note** To disable policy deployment, a security officer needs the right "Enable/disable policy deployment". By default, this right has been assigned to the predefined roles Master Security Officer and Security Officer, but it can also be assigned to new user-defined roles.

For logged events, see [Auditing \(page 204\)](#).

3.8.7 Rules for assigning and analyzing policies

The management and analysis of policies is carried out according to the rules described in this section.

Definitions

The policy's origin decides whether it is a user or computer policy. A user object "brings" a user policy, while a computer "brings" a computer policy. The same policy can be a computer or a user policy, depending on the perspective.

- **User policy**

Any policy provided by the user for analysis. If a policy is implemented through only one user, the computer-related settings of that policy are not applied, this means that computer-related settings do not apply. Default values do.

- **Computer policy**

Any policy provided by the computer for analysis. If a policy is implemented through just one computer, the user-specific settings for this policy are also applied. The computer policy therefore represents a policy for all users.

Assign and activate policies

To enable a policy to be implemented for a user or computer, you need to assign it to a container object (root nodes, domain, OU, BuiltIn container or workgroup). For the policy assigned to the user or computer to become effective, when you assign a policy anywhere in the hierarchy, all computers (authenticated computers) and all users (authenticated users) are activated automatically (assignment without activation is not enough). All users and all computers are combined into these groups.

Policy inheritance

Policies can only be passed on between container objects. Policies can be activated within a container provided it contains no further container objects (at group level). Inheritance between groups is not possible.

Policy inheritance hierarchy

Where policies are assigned along a hierarchy chain, the policy closest to a target object (user or computer) is the highest ranking. This means that as the distance to the target object increases a policy will be superseded by any policies that are closer.

Direct assignment of policies

The user or computer obtains a policy which is assigned directly to the container object in which it is located (membership as a user of a group located in another container object is not sufficient). The container object did not inherit this policy.

Indirect assignment of policies

The user or computer obtains a policy which the container object it is located in (membership as a user of a group located in another container object is not sufficient) has inherited from a higher-ranking container object.

Activate/deactivate policies

For a policy to be effective for a computer/user, it has to be activated at group level (policies can only be activated at group levels). It makes no difference if this group is in the same container object or not. All that matters is that the user or computer has been directly or indirectly (through inheritance) assigned to the policy.

If a computer or user is outside an OU or inheritance line and is a member of a group which is inside this OU, this activation does **not** apply to this user or computer. Because there is no valid assignment for this user or computer (directly or indirectly). The group was, indeed, activated but an activation can only apply to users and computers for which there is also a policy assignment. This means that the activation of policies cannot go beyond container boundaries if there is no direct or indirect policy assignment for that object.

A policy becomes effective when it has been activated for user groups or computer groups. The user groups and then the computer groups are analyzed (authenticated users and authenticated computers are also groups). Both results are OR-linked. If this OR-link gives a positive value for the computer/user relationship, the policy applies.

 **Note** If more than one policy is active for an object, the individual policies are, while complying with the rules described, merged. This means that the actual settings for an object can be composed of multiple different policies.

A group can have the following activation settings:

- Activated

A policy has been assigned. The group is displayed in the activation area of the SafeGuard Management Center.

- Not activated

A policy has been assigned. The group is not in the activation area.

If a policy is assigned to a container, the activation setting for a group (activated) determines whether that policy for that container feeds into the calculation of the resulting policy.

Inherited policies cannot be controlled by these activations. **Block policy inheritance** would have to be set at the more local OU so the more global policy cannot be effective here.

User/group settings

Policy settings for users (shown in **black** in the SafeGuard Management Center) take priority over policy settings for computers (shown in **blue** in the SafeGuard Management Center). If user settings are specified in a policy for computers, those settings are overridden by the policy for the user.

 **Note** Only the user settings are overridden. If a policy for users also includes computer settings (shown in **blue**), they are not overridden by a user policy!

Example 1:

If password length 4 has been defined for a computer group, the user group is assigned value 3 for the same setting and this user is subject to password length 3 on a computer in the computer group.

Example 2:

If a server interval of 1 minute is defined for a user group, and the value 3 for a computer group, value 3 is used because value 1 minute is a computer setting which was defined in a policy for users.

Contradictory encryption policies

Two policies (P1 and P2) are created. File-based encryption for drive E:\ was defined for P1, and volume-based encryption for drive E:\ was defined for P2. P1 is assigned the OU **FBE-User** and P2 the OU **VBE-User**.

Case 1: A user from OU **FBE-User** logs on first to the Client W7-100 (container computer). Drive E:\ is encrypted with file-based encryption. If a user from the OU **VBE-User** then logs on to Client W7-100, drive E:\ will be encrypted with volume-based encryption. If both users have the same key, both can access the drives or files.

Case 2: A user from OU **VBE-User** logs on first to the computer W7-100 (container computer). The drive is encrypted with volume-based encryption. If, now, a user from OU **FBE-User** logs on and has the same key as users from OU **VBE-User**, drive E:\ will be encrypted with file-based encryption within the volume-based encryption (the volume-based encryption is kept). However, if the user from OU **FBE-User** does not have the same key, they cannot access drive E:\.

Priority within an assignment

Within an assignment, the policy with the highest priority (1) ranks above a policy with a lesser priority.

 **Note** If a policy with a lesser priority, but with the property **No Override** is assigned to the same level as a higher ranking policy, this policy will take priority despite its lower ranking.

Priority within a group

Within a group, the policy with the highest priority (1) ranks above a policy with a lesser priority.

Status indicators

Setting status indicators allows the standard rules for policies to be changed.

- **Block policy inheritance**

Set for containers for which you do not want higher-ranking policies to apply (right-click the object in the Properties navigation window).

If you do not want a container object to inherit a policy from a higher object, select **Block Policy Inheritance** to prevent this. If **Block Policy Inheritance** has been selected for a container object it will not be affected by higher-ranking policy settings (exception: **No Override** activated when policy was assigned).

- **No Override**

Set during assignment process this policy cannot be overridden by another policy.

The further away the policy assignment with **No Override** is from the target object, the stronger the effect of this policy will be for all the lower-ranking container objects. This means that a higher ranking container subject to **No Override** overrides the policy settings of a lower ranking container. So, for example a domain policy can be defined and its settings cannot be overridden, even if **Block policy inheritance** has been set for an OU!

 **Note** If a policy with a lesser priority but which has been designated **No Override** is assigned to the same level as a higher ranking policy, this policy will take priority despite its lower ranking.

3.8.7.1 Settings in policies

Replay Machine Settings

You find this setting under **Policy Items > General Settings > Loading of Settings > Policy Loopback**.

If you select **Replay Machine Settings** in the field **Policy Loopback** of a policy of the type **General Settings** and the policy comes from a computer (**Replay Machine Settings** does not affect user policies), this policy is replayed at the end of the analysis. This then overrides any user settings

and the machine settings apply. All machine settings inherited directly or indirectly by the machine (including policies which have not been applied by the **Replay Machine Settings** policy loopback) are rewritten.

Ignore User

You find this setting under **Policy Items > General Settings > Loading of Settings > Policy Loopback**.

If you select **Ignore User** for a policy for a computer in the field **Policy Loopback** of a policy of the type **General Settings** and the policy comes from a machine, only the machines settings are analyzed. User settings are not analyzed.

No Loopback

You find this setting under **Policy Items > General Settings > Loading of Settings > Policy Loopback**.

No Loopback describes the standard behavior. User policies take priority over computer policies.

Analyze the settings "Ignore User" and "Replay Machine Settings"

If there are active policy assignments, the machine policies are analyzed and consolidated first. If, with the **Policy Loopback** option, this amalgamation of individual policies results in the value **Ignore User**, the policies that would have been fixed for the user will not be analyzed. This means that the same policies apply both for the user and for the machine.

If, after merging the individual machine policies, the value with the **Policy Loopback** attribute is **Replay Machine Settings**, the user policies are merged with the machine policies. After the merge, the machine policies are rewritten and, where appropriate, override settings from the user policies. If a setting is present in both policies, the machine policy value overrides the user policy value.

If the consolidation of the individual machine policies results in the standard value (**No Policy Loopback**), user settings take priority over machine settings.

Order of the execution of policies

Ignore User Computers

Replay Machine Settings Computer -> User -> Computer. The first "machine execution" is required for the policies which are written before user logon (for example background image at logon).

No Loopback (standard setting): Computer -> User

3.8.7.2 Policies of type No encryption

Where policies are assigned along a hierarchy chain, the policy closest to a target object (user or computer) is the highest ranking. This means that as the distance to the target object increases a policy will be superseded by any policies that are closer. Policies of type **No Encryption** can be used to interrupt the inheritance of encryption policies at certain locations in the hierarchy chain. For subordinate levels the **No Encryption** policy will be valid as well.

Depending on module and version, the behavior of the endpoints varies.

Endpoints with Synchronized Encryption

Policies of type **Application-based (Synchronized Encryption)** are NOT merged. The policy closest to the target object (user or computer) in a hierarchy chain is always applied. If it is the closest, a **No encryption** policy will become effective.

Endpoints with File Encryption version 8

Policies of type **Location-based** are merged. If several policies are assigned, their content is evaluated according to certain rules, see [Rules for assigning and analyzing policies \(page 116\)](#). For the Resulting Set of Policies (RSOP) see, [Location-based File Encryption policies in the RSOP \(page 314\)](#). Within an assignment, the policy with the highest priority (1) ranks above a policy with a lesser priority. If it has the highest priority, a **No encryption** policy will become effective.

Endpoints with File Encryption below version 8

A **No encryption** policy has no effect on these endpoints. Endpoints with **File Encryption** 7.0 and lower do not recognize the **Encryption Type** setting. Rules from all **File Encryption** policies of type **Location-based** apply.

This is particularly important if you have to handle endpoints of version 8 and older versions simultaneously.

3.8.8 *Inventory and status data*

SafeGuard Enterprise reads an extensive amount of inventory and status data from the endpoints. This data shows the current global state of each computer. The data is displayed in the SafeGuard Management Center in **Users and Computer** in the **Inventory** tab.

As a security officer, you can view, export and print out inventory and status data. For example, you can create compliance reports to show that endpoints have been encrypted. Wide-ranging sort and filter features are available to help you select the relevant data.

The **Inventory** provides for example the following data about each machine:

- The policy applied.
- The last server contact.
- The encryption status of all media.
- The POA status and type.
- The installed SafeGuard Enterprise modules.
- The WOL status.
- User data.

3.8.8.1 Mac endpoints in the inventory

The **Inventory** provides status data for Macs managed in the SafeGuard Management Center. For further information, see [Inventory and status data of Macs \(page 361\)](#)

3.8.8.2 View inventory data

1. In the navigation area of the SafeGuard Management Center, click **Users and Computers**.
2. In the navigation window, click the relevant container (domain, workgroup or computer) on the left-hand side.
3. In the action area, switch to the **Inventory** tab on the right-hand side.
4. In the **Filter** area, select the filter to be applied on the inventory display, see [Filter inventory data \(page 124\)](#).

 **Note** If you are selecting a particular computer, you receive the inventory data as soon as you switch to the **Inventory** tab. The **Filter** area is not available here.

5. In the **Filter** area, click the magnifier icon.

The inventory and status data appears in a summarized table for all the machines in the container selected. The tabs **Drives**, **Users** and **Features** are also available for each machine.

By clicking a column header you can sort the inventory data based on the values of the selected column. The context menu for each column offers a number of features for sorting, grouping and

customizing the display. Depending on your access rights, items in the inventory are shown in different colors:

- Items for objects for which you have **Full access** rights are shown in black.
- Items for objects for which you have **Read only** access rights are shown in blue.
- Items for objects for which you have no access rights are greyed out.

3.8.8.3 Show hidden columns

Some columns in the inventory data display are hidden by default.

1. In the inventory data display, right-click the column header bar.
2. From the context menu, select **Runtime Column Customization**.

The **Customization** window is displayed showing the hidden columns.

3. Drag the required column from the **Customization** window to the column header bar.

The column is shown in the inventory data display. To hide it again, drag it back to the **Customization** window.

3.8.8.4 Filter inventory data

When working from an OU, filters can be defined to limit the display based on a particular criteria.

The following fields are available for defining filters in the **Filter** area of the **Inventory** tab:

Field	Description
Computer name	To display the inventory and status data for a particular computer, enter the computer's name in this field.
Including subcontainers	Activate this field, if you want to include subcontainers in the display.
Show last modified	Use this field to specify the number of last changes to be displayed.

You can also use the Filter Editor to create user-defined filters. You can open the Filter Editor from the context menu for each column. In the **Filter Builder** window, you can define your own filters and apply them to the column concerned.

3.8.8.5 Refresh inventory data

The endpoints usually send an update of the inventory data when the data have changed.

The **Request Inventory Refresh** command can be used to manually request a refresh of the computer's current inventory data. This command is available for a particular computer or for all the computers in a node (optionally including sub-nodes) from the context menu and the **Actions** menu in the SafeGuard Management Center menu bar. The command can also be selected using the context menu for the list entries.

If you select this command or click the **Request Inventory Refresh** icon in the toolbar, the relevant computers send their current inventory data.

As is the case with other areas in the SafeGuard Management Center, you can use the **Refresh** command to refresh the display. You can select this command from the context menu for individual computers or all the computers in a node and from the **View** menu in the menu bar. You can also use the **Refresh** double-headed arrow icon in the toolbar to refresh the display.

3.8.8.6 Overview

The individual columns in the overview show the following information.

 **Note** Some columns are hidden by default. You can customize the display to show them. For further information, see [Show hidden columns \(page 124\)](#).

Column	Explanation
Machine name	Shows the computer's name.
Domain	Shows the computer domain name.
Domain Pre 2000	Shows the pre-Windows 2000 domain name.
User name (owner)	Shows the user name of the computer's owner, if available.
First name	Shows the owner's first name, if available.
Last name	Shows the owner's last name, if available.
Email address	Shows the owner's Email address, if available
Other registered users	Shows the names of other registered users of the computer, if available.
Operating system	Shows the computer's operating system.
Last server contact	Shows when (date and time) the computer communicated last with the server.
Last policy received	Shows when (date and time) the computer received the last policy.
Encrypted drives	Shows the computer's encrypted drives.
Unencrypted drives	Shows the computer's unencrypted drives.
POA type	Specifies whether the computer is a native SafeGuard Enterprise endpoint, a BitLocker endpoint with SafeGuard Challenge/Response, a BitLocker endpoint with native recovery mechanism, a FileVault 2 endpoint or an endpoint with a self-encrypting Opal-compliant hard drive.
POA	Specifies whether SafeGuard Power-on Authentication is activated for the computer.

Column	Explanation
WOL	Specifies whether Wake on LAN is activated for the computer.
Modification date	Shows the date when the inventory data changed due to an inventory refresh request or the computer sending new inventory data.
Refresh requested	Shows the date of the last refresh request. The value displayed in this field will be deleted, when the request is processed by the computer.
Parent DSN	Shows the Distinguished Name of the container object the computer is subordinated to. This column is only displayed, if the field Including subcontainers has been activated in the Filter area.
Current Company certificate	Specifies whether the computer uses the current company certificate.

3.8.8.7 Drives tab

The **Drives** tab shows the inventory and status data for the drives on the computer concerned.

Column	Explanation
Drive name	Shows the name of the drive.
Label	Shows the label of a Mac drive.
Type	Shows the drive type, for example Fixed , Removable Medium or CD-ROM/DVD .
State	<p>Shows the encryption state of a drive.</p> <p>If SafeGuard BitLocker management is installed on an endpoint, Not prepared may be displayed as the encryption state of a drive. This indicates that the drive currently cannot be encrypted with BitLocker since necessary preparations have not been done yet. This only applies to managed endpoints since unmanaged endpoints cannot report inventory data.</p> <p>For prerequisites to manage and encrypt BitLocker drives, see Prerequisites for managing BitLocker on endpoints (page 293).</p> <p>The column also indicates whether BitLocker has been suspended or resumed by users.</p> <p>The encryption state of an unmanaged endpoint can be checked with the command line tool SGNState, see Displaying the system status with SGNState (page 434).</p>

Column	Explanation
Encryption method	For encrypted drives, this field shows the algorithm used for encryption.

3.8.8.8 Users tab

The **Users** tab shows the inventory and status data for the users on the computer.

Column	Explanation
User name	Shows the user name of the user.
Distinguished Name	Shows the DNS name for the user, for example: CN=Administrator,CN=Users,DC=domain,DC=mycompany,DC=net
User is owner	Indicates whether the user is defined as the computer's owner.
User is locked	Indicates whether the user is locked.
SGN Windows user	Indicates whether the user is an SGN Windows user. An SGN Windows user is not added to the SafeGuard POA, but has a key ring for accessing encrypted files, just as a SGN user. You can activate the registration of SGN Windows users on endpoints by policies of the type Specific Machine Settings .

3.8.8.9 Features tab

The **Features** tab provides an overview of all the SafeGuard Enterprise modules installed on the computer.

Column	Explanation
Module name	Shows the name of the SafeGuard Enterprise module installed.
Version	Shows the software version of the SafeGuard Enterprise module installed and, if a file encryption module is installed, the version of the File Encryption Driver.

3.8.8.10 Company certificate tab

The **Company Certificate** tab shows the properties of the currently used company certificate and indicates whether a newer company certificate is available.

Column	Explanation
Subject	Shows the distinguished name of the subject of the company certificate.
Serial	Shows the serial number of the company certificate.
Issuer	Shows the distinguished name of the issuer of the company certificate.
Valid from	Shows date and time when the company certificate becomes valid.
Valid to	Shows date and time when the company certificate expires.

Column	Explanation
Newer company certificate available	Indicates whether a newer company certificate than the endpoint's current one is available.

3.8.8.11 Creating inventory data reports

As a security officer, you can create inventory data reports in different formats. For example, you can create compliance reports to show that endpoints have been encrypted. Reports can be printed or exported to a file.

Print inventory reports

1. In the SafeGuard Management Center menu bar, click **File**.
2. You can either print the report directly or display a print preview.

The print preview provides various features, for example for editing the page layout (header and footer etc.).

- To get a print preview, select **Print preview**.
- To print the document without a print preview, select **Print**.

Export inventory reports to files

1. In the SafeGuard Management Center menu bar, click **File**.
2. Select **Print preview**.

The inventory report **Preview** is displayed.

The preview provides various features, for example for editing the page layout (header and footer etc.).

3. In the toolbar of the **Preview** window, select the drop-down list of the **Export Document...** icon.
4. Select the required file type from the list.
5. Specify the required export options and click **OK**.

The inventory report is exported to a file of the file type specified.

3.8.9 SafeGuard Enterprise Security Officers

SafeGuard Enterprise can be administered by one or more security officers. The role-based management of SafeGuard Enterprise allows splitting administration among several users. Any user may be assigned one or more roles. To enhance security, additional authorization of an action can be assigned to an officer's role.

During initial configuration of the SafeGuard Management Center, a top-level administrator, the Master Security Officer (MSO), with all the rights and a certificate is created by default, see [Create the Master Security Officer \(MSO\) \(page 39\)](#). The MSO certificate expires after 5 years and can be renewed in the **Security Officers** section of the Management Center. Further security officers can be assigned for specific tasks such as helpdesk or auditing.

In the SafeGuard Management Center navigation area, you can arrange security officers hierarchically to reflect your company's organizational structure. However, this does not imply any hierarchy in terms of rights and roles.

 **Note** Two security officers must not use the same Windows account on the same computer. Otherwise it is not possible to separate their access rights properly. Additional authentication is more secure when security officers must authenticate with cryptographic tokens/smartcards.

3.8.9.1 Security officer roles

For easy operation, SafeGuard Enterprise offers predefined security officer roles with a variety of functions. Security officers with the necessary rights can define new roles from a list of actions/rights and assign them to particular security officers.

The following types of roles are provided:

- Master Security Officer (MSO) role
- Predefined roles
- Customized roles

Master Security Officer

After installing SafeGuard Enterprise, a Master Security Officer (MSO) is created by default during initial configuration of the SafeGuard Management Center. The Master Security Officer is the top-level security officer, possesses all rights and is able to access all objects (similar to a Windows administrator). The Master Security Officer rights cannot be modified.

There may be several Master Security Officers created for one instance of the SafeGuard Management Center. We strongly recommend to create at least one additional MSO for security reasons. Additional MSOs may be deleted, but there must always remain one user with the role of MSO who has been explicitly created as MSO in the SafeGuard Enterprise Database.

A Master Security Officer can delegate tasks to another person. There are two ways to do this:

- A new security officer can be created in **Security Officers**.
- A user or all members of a container imported from the Active Directory and visible in the SafeGuard Management Center in the root directory can be promoted to security officer in **Users and Computers**.

One or more roles and domains can then be assigned to them. For example, a user may be assigned the role of Supervising Officer plus the role of Helpdesk Officer.

However, the Master Security Officer can also create custom roles and assign them to particular users.

Export the Master Security Officer certificate

In a SafeGuard Enterprise installation, the Master Security officer certificate is a critical item and must be backed up in a safe location. We recommend that you carry out this task right after initial configuration of the SafeGuard Management Center.

To back up the Master Security Officer certificate of the MSO logged on to the SafeGuard Management Center:

1. In the SafeGuard Management Center menu bar, select **Tools > Options**.
2. Select the **Certificates** tab and click **Export** in the **Certificate of <administrator>** section.
3. You are prompted to enter a password for securing the exported file. Enter a password, confirm it and click **OK**.
4. Enter a file name and storage location for the file to be exported and click **OK**.

The Master Security Officer certificate of the currently logged on MSO is exported as a .p12 file to the defined location and can be used for recovery purposes.

Predefined roles

In the SafeGuard Management Center, the following security officer roles (apart from the MSO) are predefined. The assignment of rights to these predefined roles cannot be changed. For example, if a predefined role has the right to "Create policy items and policy groups", this right cannot be deleted

from the role. Neither can a new right be added to a predefined role. Additional officer authentication however, may be assigned to predefined roles at any time.

- **Supervising Officer**

Supervising Officers can see their own node in the **Security Officers** area and have the right to manage security officers belonging to their node.

- **Security Officer**

Security Officers have extensive rights including SafeGuard Enterprise configuration, policy and key management, permissions for monitoring and recovery.

- **Helpdesk Officer**

Helpdesk Officers have the rights to perform recovery actions. Additionally, they can view most function areas of the SafeGuard Management Center.

- **Audit Officer**

To monitor SafeGuard Enterprise, Audit Officers may display most function areas of the SafeGuard Management Center.

- **Recovery Officer**

Recovery Officers have the rights to repair the SafeGuard Enterprise Database.

Custom roles

As a security officer with the required rights, you can define new roles from a list of actions/rights and assign them to an existing or new security officer. As with predefined roles, you may enable the additional officer authentication for a function of the role any time.

When you assign a new role, note the following regarding additional authentication:

 **Note** If a user has two roles with the same rights and additional authentication is assigned to one of the roles, this automatically applies to the other role.

A security officer with the required rights may add or delete rights to or from a custom role. Unlike predefined roles, custom roles can even be deleted as required. If the role is deleted, it is no longer assigned to any user. If a user only has one role assigned and this role is deleted, the user can no longer log on at the SafeGuard Management Center.

 **Note** The role and the actions defined within it determine what a user may and may not do. This is also true if the user has been assigned more than one role. After the user has logged on to the SafeGuard Management Center only those areas are activated and displayed that are needed for the respective role. This also applies to the scripts and API areas. It is therefore important to always activate the view in which the respective actions are defined. Actions are sorted by function area and hierarchically structured. This structure shows which actions are required before certain other actions can be performed.

Additional officer authentication

Additional officer authentication (also referred to as two persons rule) may be assigned to specific actions of a role. This means that the user of this role is only permitted to perform a certain action if a user of another role is present and confirms it. Each time the user performs this action another user has to confirm it.

Additional authentication may be assigned to both predefined and custom roles. As soon as there is at least one other officer with the same role, the own role can also be selected.

The role which is to perform the additional authorization must have been assigned to a user and there need to be at least two security officers in the SafeGuard Enterprise Database. Once additional authentication is required for an action, it is required even if the user owns another role that does not require additional authentication for this action.

If an officer without the right to change the additional authentication creates a role, settings for additional authentication of the new role will be pre-filled to match those set for the creating officer.

3.8.9.2 Create a role

Prerequisite: To create a new role, you need the right to display and create security officer roles. To assign additional authentication you need the right to "Change additional authentication settings".

1. In the SafeGuard Management Center, select **Security Officers**.
2. Right-click **Custom Roles** and select **New > New custom role**.
3. In **New custom role**, enter a name and description for the role.
4. Assign the actions to this role: Select the check boxes next to the required action in the **Enabled** column.

Actions are sorted by function area and hierarchically structured. This structure shows which actions are required before certain other actions can be performed.

5. If required, assign **Additional officer authentication**: Click the default setting **None** and select the required role from the list.

If an officer without the right to change the additional authentication creates a role, then the additional authentication is prefilled depending on the additional authentication set for the officer's roles.

6. Click **OK**.

The new role is displayed in the navigation window under **Custom Roles**. When you click the role, the permitted actions are displayed in the action area on the right.

3.8.9.3 Assign a role to a security officer

Prerequisite: To assign a role, you need the right to display and modify security officers.

1. Select the respective officer in the navigation window.

Their properties are displayed in the action area on the right.

2. Assign the required roles by selecting the relevant boxes next to the available roles.

Predefined roles are displayed in bold.

3. Click the double-headed arrow symbol **Refresh** in the toolbar.

The role is assigned to the security officer.

 **Note** Complex customized roles may cause slight performance issues in using the SafeGuard Management Center.

3.8.9.4 Displaying officer and role properties

Prerequisite: To get an overview of the security officer properties or the role assignment, you need the right to display security officers and security officer roles.

To display security officer and role properties:

1. In the SafeGuard Management Center, click **Security Officers**.
2. In the navigation area on the left, double-click the object you want to get an overview of.

The information displayed in the action area on the right depends on the object selected.

Display MSO properties

The general and modification information of the MSO is displayed.

Display security officers properties

The general and modification information for the security officer is displayed.

In **Properties**, select the **Actions** tab to display a summary of actions permitted and the roles assigned to the security officer.

Display security officers rights and roles

A summary of actions of all roles assigned to the security officer is displayed. The tree view shows what actions are required before certain other actions can be performed. Additionally, the assigned roles can be displayed.

1. In the **<Security officer name> properties** dialog, on the **Actions** tab, select an action to display all assigned roles that contain this action.
2. Double-click a role in the **Assigned roles with selected action** list. The **<Security officer name> properties** dialog is closed and the role's properties are displayed.

Display role properties

The general and modification information for the role are displayed.

In **Properties**, select the **Assignment** tab to display the security officers assigned to this role.

Display role assignment

In the **<Role name> Properties**, on the **Assignment** tab, double-click a security officer. The **Properties** dialog is closed and the security officer's general data and roles are displayed.

3.8.9.5 Modifying a role

You can do the following:

- Modify additional authentication only.
- Modify all properties of the role.

The icon next to the roles shows which action is available:

Icon	Description
	The role can be modified (add/remove actions).
	Additional authentication can be changed.
	Both modifications are available.

 **Note** Predefined roles and the actions assigned to them cannot be modified. If additional authentication is activated, it can be modified for any role, even for predefined roles.

Modify additional authentication only

Prerequisite: To assign additional authentication, you need the right to display security officer roles and to "Change additional authentication settings".

1. In the SafeGuard Management Center, select **Security Officers**.
2. In the navigation window under **Custom Roles**, click the role you want to change. In the action area on the right, click the required setting in the **Additional security officer authentication** column and select a different role from the list.

Predefined roles are displayed in bold.

3. Click the **Save** icon in the toolbar to save your changes to the database.

Additional officer authentication has been changed for this role.

Modify all properties of a role

Prerequisite: To change a custom role, you need the right to display and modify security officer roles. To reassign additional authentication, you also need the right to "Change additional authentication settings".

1. In the SafeGuard Management Center, select **Security Officers**.
2. In the navigation window under **Custom Roles**, right-click the role you want to change and select **Modify custom role**.
3. Change the properties as required. Change additional authentication properties by clicking the value in this column and selecting the required role.
4. Click the **Save** icon in the toolbar to save your changes to the database.

The role has been modified.

3.8.9.6 Copy a role

To create a new role that has similar properties as an existing role, you can use the existing role as a template for the new role. You can select a predefined or custom role as a template.

Prerequisite: You can only use existing roles as templates, if the currently authenticated security officer has all the rights contained in the specific role template. So, this function may be disabled for officers with a limited set of actions.

1. In the SafeGuard Management Center, select **Security Officers**.
2. In the navigation window, right-click the role you want to copy and select **New > New copy of role**.
In **New custom role**, all properties of the existing role are already preselected.
3. Enter a new name for this role and change the properties as required.
4. Click the **Save** icon in the toolbar to save your changes to the database.

The new role is created.

3.8.9.7 Delete a role

 **Note** Predefined roles cannot be deleted.

Prerequisite: To delete a role, you need the right to display and delete security officer roles.

1. In the SafeGuard Management Center, select **Security Officers**.
2. In the navigation window under **Custom Roles**, right-click the role you want to delete and select **Delete**. Depending on the role's properties a corresponding warning message will be displayed.

 **Note** When you delete a role, all security officers this role is assigned to lose it. If the role is the only one assigned to a security officer, the security officer can no longer log on to the SafeGuard Management Center unless a superior security officer assigns a new role to the security officer. If the role is used for additional authentication, the MSO will be requested to perform additional authentication.
3. To delete the role, click **Yes** in the warning message.
4. Click the **Save** icon in the toolbar to save your changes to the database.

The role is deleted from the navigation window and from the database.

3.8.9.8 Create a Master Security Officer

Prerequisite: To create a new Master Security Officer, you need the right to display and create security officers.

 **Note** A quick way of creating new Master Security Officers is to promote a Security Officer. For further information, see [Promoting security officers \(page 143\)](#).

1. In the SafeGuard Management Center, select **Security Officers**.
2. In the navigation window, right-click the **Master Security Officers** node and select **New > New Master Security Officer**.
3. Make the relevant entries in **New master security officer**:

Field/check box	Description
Enabled	The security officer can be deactivated until further notice. This means that the security officer is in the system, but they cannot log on to the SafeGuard Management Center yet. They can only log on and perform their administrative tasks when another security officer activates them.
Name	<p>Enter the name of the security officer as given in the certificates created by SafeGuard Enterprise in cn =. The security officer is also displayed under this name in the SafeGuard Management Center navigation window. This name must be unique.</p> <p>Maximum value: 256 characters</p>
Description	<p>Optional</p> <p>Maximum value: 256 characters</p>
Cell phone	<p>Optional</p> <p>Maximum value: 128 characters</p>
E-Mail	<p>Optional</p> <p>Maximum value: 256 characters</p>
Token logon	<p>The logon can be done in the following way:</p> <p>No token The security officer may not log on with a token. They have to log on by entering the logon information (user name/password).</p> <p>Optional Logon can be either with a token or by entering the logon information. The security officer is free to choose.</p>

Field/check box	Description
	<p>Mandatory A token has to be used to log on. To do this, the private key that belongs to the security officer's certificate must be on the token.</p>
<p>Certificate</p>	<p>A security officer always needs a certificate to log on to the SafeGuard Management Center. The certificate can either be created by SafeGuard Enterprise or an existing one can be used. If token logon is essential, the certificate has to be added to the security officer's token.</p> <p>Create:</p> <p>The certificate and key file are created and saved in a selected location. Enter and confirm a password for the .p12 key file. The .p12 file must be available to the security officer when logging on. The certificate created is automatically assigned to the security officer and displayed in Certificate. If SafeGuard Enterprise password rules are used, rules in the Active Directory should be deactivated.</p> <p> Note Max. length of path and file name: 260 characters. When creating a security officer, the certificate's public part is sufficient. When logging on to the SafeGuard Management Center, however, the certificate's private section (the key file) is also required. If it is not available in the database, it must be available to the security officer (for example on a memory stick) and may be stored in the certificate store during logon.</p> <p>Import:</p> <p>An existing certificate is used which is assigned to the security officer during import. If the import is from a .p12 key file, the certificate's password must be known.</p> <p>If a PKCS#12 certificate container is selected, all certificates are loaded into the list of assignable certificates. The certificate is then assigned after the import, by selecting the certificate from the drop-down list.</p>

4. Click **OK** to confirm.

The new Master Security Officer is displayed in the navigation window under the **Master Security Officers** node. Their properties can be displayed by selecting the respective security officer in the navigation window. The MSO can log on to the SafeGuard Management Center with the name displayed.

3.8.9.9 Create a security officer

Prerequisite: To create a security officer, you need the right to display and create security officers.

1. In the SafeGuard Management Center, select **Security Officers**.
2. In the navigation window right-click the security officer's node where you want to locate the new security officer and select **New > New security officer**.
3. Make the relevant entries in the **New security officer** dialog:

Field/check box	Description
Enabled	The security officer can be deactivated until further notice. This means that the security officer is in the system, but they cannot log on to the SafeGuard Management Center yet. They can only log on and perform their administrative tasks when another security officer activates them.
Name	Enter the name of the security officer as provided in the certificates created by SafeGuard Enterprise in cn =. The security officer is also displayed under this name in the SafeGuard Management Center navigation window. This name must be unique. Maximum value: 256 characters
Description	Optional Maximum value: 256 characters
Cell phone	Optional Maximum value: 128 characters
E-Mail	Optional Maximum value: 256 characters
Validity	Select from when and to when (date) the security officer should be able to log on to the SafeGuard Management Center.
Token logon	The logon can be done in the following way: No token The security officer may not log on with a token. They have to log with their credentials (user name/password). Optional Logon can be either with a token or with the credentials. The security officer is free to choose.

Field/check box	Description
	<p>Mandatory A token has to be used to log on. To do this, the private key that belongs to the security officer's certificate must be on the token.</p>
<p>Certificate</p>	<p>A security officer always needs a certificate to log on to the SafeGuard Management Center. The certificate can either be created by SafeGuard Enterprise or an existing one can be used. If token logon is essential, the certificate has to be added to the security officer's token.</p> <p>Create:</p> <p>The certificate and key file are created as new and saved in a selected location. Enter and confirm a password for the .p12 key file. The .p12 file must be available to the security officer when logging on. The certificate created is automatically assigned to the security officer and displayed in Certificate. If SafeGuard Enterprise password rules are used, rules in the Active Directory should be deactivated.</p> <p> Note Max. length of path and file name: 260 characters. When creating a security officer, the certificate's public part is sufficient. When logging on to the SafeGuard Management Center, however, the certificate's private section (the key file) is also required. If it is not available in the database, it must be available to the security officer (for example on a memory stick) and may be stored in the certificate store during logon.</p>
<p>Certificate</p>	<p>Import:</p> <p>An existing certificate is used which is assigned to the security officer during import. If the import is from a .p12 key file, the certificate's password must be known.</p> <p>If a PKCS#12 certificate container is selected, all certificates are loaded into the list of assignable certificates. The certificate is then assigned after the import, by selecting the certificate from the drop-down list.</p>
<p>Security Officer Roles</p>	<p>Roles</p> <p>Predefined or custom roles can be assigned to the security officer. The rights associated with each role are displayed under Action Permitted in the action area when clicking the respective role or</p>

Field/check box	Description
	when right-clicking the security officer and selecting Properties , Actions . More than one role can be assigned to a user.

4. Click **OK** to confirm.

The new security officer is displayed in the navigation window under the respective **Security Officers** node. Their properties can be displayed by selecting the respective security officer in the navigation window. The security officer can log on to the SafeGuard Management Center with the name displayed. Next you need to assign directory objects/domains to the security officer so they can perform their tasks.

3.8.9.10 Assigning directory objects to a security officer

For security officers to be able to perform their tasks they need to have access rights to directory objects. Access rights can be granted to domains, organizational units (OUs) and user groups as well as to the ".Auto registered" node under the Root directory.

In **Users and Computers**, you can change the access rights of another security officer if you have full access for the relevant container and are responsible for the security officer in question. You cannot change your own access rights. If you assign a security officer to a directory object for the first time, the security officer inherits your access rights for this container.

 **Note** You cannot grant higher access rights than your own access rights to other security officers.

Prerequisite: If you want to grant/deny a security officer the right to access and manage directory objects, you need the "Users and Computers" rights "Display security officers access rights" and "Grant/deny access rights to directory". In addition, you need **Full access** rights for the relevant directory objects.

1. In the SafeGuard Management Center, select **Users and Computers**.
2. In the navigation window on the left, select the required directory objects.
The navigation tree only shows the directory objects you have access rights for. If you have **Full access** rights, the object is displayed in black. Objects with **Read only** access are displayed in blue. A node that is greyed out cannot be accessed but is still shown, if there are nodes below that you have access to.
3. In the action area on the right, click the **Access** tab.
4. To assign rights for the selected objects, drag the required officer from the far right into the **Access** table.
5. In the **Access Rights** column, select the rights you want to grant the security officer for the selected objects:

- **Full Access**
- **Read only**
- **Denied**

To unassign the rights granted for the selected objects, drag the security officer back to the **Officers** table.

6. Click the **Save** icon in the toolbar to save the changes to the database.

The selected objects are available to the relevant security officer.

If two security officers are working on the same SafeGuard Enterprise Database at the same time and one is changing access rights, a message is displayed to inform the other security officer and any unsaved changes are lost. If a security officer loses the access rights for a node completely, access is no longer granted and a relevant message is displayed. The navigation window is refreshed accordingly.

3.8.9.11 View security officer rights for directory objects

The access rights assigned to security officers for directory objects are displayed in the **Access** tab of the relevant objects in **Users and Computers**.

The **Access** tab only shows the access rights for containers you have access rights for. Likewise, it only shows the security officers you are responsible for.

The **Access** tab shows the following information:

- The **Officers** column shows the types and names of the security officers assigned to the directory objects.
- The **Assigned by** column shows the security officer who has assigned the access rights.
- The **Assignment Date**
- The **Access Rights** column shows the rights granted: **Full Access**, **Denied** or **Read only**.
- The **Origin** column shows the full name of the node where the access right was assigned to the corresponding officer. For example: If the right was assigned to a parent node of the directory object selected, the parent node is displayed here. In this case, the security officer has inherited the access right for the selected directory object by the assignment to its parent node.
- The **Status** column shows how the security officer has received the access right:
 - **Inherited** (blue text color): The access right has been inherited from a parent node.
 - **Overwritten** (brown text color): The access right has been inherited from a parent node, but changed at the selected node by direct assignment.
 - **Directly assigned** (black text color): The access right has been assigned directly at the selected node.

For inherited rights, you can display a tooltip in the **Status** column showing the origin of the relevant right.

3.8.9.12 Promoting security officers

You may do the following:

- Promote a user to security officer in the **Users and Computers** area.
- Promote a security officer to Master Security Officer in the **Security Officers** area.

Prerequisites

A security officer with the required rights can promote users to security officers and assign roles to them.

Security officers created in this way can log on to the SafeGuard Management Center with their Windows credentials or their token/smartcard PIN. They can operate and be administrated just like any other security officers.

The following prerequisites must be met:

- Users to be promoted must have been imported from an Active Directory and need to be visible in the SafeGuard Management Center **Users and Computers** area.
- To enable a promoted user to log on to the SafeGuard Management Center as a security officer, a user certificate is required. You can create this certificate when you promote the user, see [Promote a user to security officer \(page 143\)](#). For logon with the Windows credentials, the .p12 file containing the private key must exist in the SafeGuard Enterprise Database. For logon with token or smartcard PIN, the .p12 file containing the private key must reside on the token or smartcard.

Note

If you create the certificate when you promote a user, they have to use the certificate password to log on to the SafeGuard Management Center. They have to enter the certificate password although they are prompted for the Windows password. This is also true when logging on to the SafeGuard Enterprise Web Help Desk.

Promote a user to security officer

Prerequisite: To promote a user, you need to be a Master Security Officer or a security officer with the required rights.

1. In the SafeGuard Management Center, select **Users and Computers**.
2. Right-click the user you want to promote to security officer and select **Make this user a Security Officer**.
3. The next step depends on whether a user certificate is available for the selected user.
 - If a user certificate has already been assigned to this user, the **Select role(s)** dialog is displayed. Continue with step 4.
 - If no user certificate is available, a message is displayed asking you whether a self-signed key pair should be created for this user. Click **Yes** and enter and confirm a password in the **Password for new certificatedialog**. Now the **Select role(s)** dialog is displayed.
4. In the **Select role(s)** dialog, select the required roles and click **OK**.

The user is now promoted and displayed in the **Security Officers** area with their user name. Their properties can be displayed by selecting the respective officer in the navigation window. If the user's private key is stored in the database, **No token** is activated. If the user's private key resides on the token or smartcard, **Optional** is activated.

You may drag-and-drop the security officer to the required position in the **Security Officers** tree view if required.

The security officer can log on to the SafeGuard Management Center with the name displayed.

Promote a security officer to Master Security Officer

Prerequisite: To promote a security officer, you need the right display and modify security officers.

1. In the SafeGuard Management Center, select **Security Officers**.
2. In the navigation window, right-click the security officer you want to promote and select **Promote to Master Security Officer**.
3. If the promoted officer has children you are prompted to select a new parent node for the children.

The security officer is promoted and displayed under the **Master Security Officers** node. As a Master Security Officer, the promoted officer will receive all rights to all objects and thus lose all assigned roles and all individually granted domain access in **Users and Computers**.

3.8.9.13 Demote Master Security Officers

Prerequisite: To demote Master Security Officers to security officers you need to be a Master Security Officer.

1. In the SafeGuard Management Center, select **Security Officers**.

2. In the navigation window, right-click the Master Security Officer you want to demote and select **Demote to security officer**.
3. You are prompted to select a parent node for the officer and to assign at least one role.

The security officer is demoted and displayed under the selected **Security Officers** node. The demoted officer loses all rights to all objects and only receive those rights that are assigned to their role(s). A demoted officer does not have any rights on domains. You need to individually grant domain access rights in the **Users and Computers** area under the **Access** tab.

3.8.9.14 Change the security officer certificate

Prerequisite: To change the certificate of a security officer or Master Security Officer, you need the right to display and modify security officers.

1. In the SafeGuard Management Center, select **Security Officers**.
2. In the navigation window, click the security officer you want to change the certificate for. The current certificate assigned is displayed in the action area on the right in the **Certificates** field.
3. In the action area, click the **Certificates** drop-down list and select a different certificate.
4. Click the **Save** icon in the toolbar to save the changes to the database.

3.8.9.15 Arrange security officers in the tree view

Security officers can be hierarchically arranged in the **Security Officers** navigation window to reflect the company's organizational structure.

The tree view can be arranged for all security officers, except for Master Security Officers. MSOs are displayed in a flat list under the MSO node. The security officers node contains a tree view where each node represents a security officer. However, this does not imply any hierarchy in terms of rights and roles.

Prerequisite: To move a security officer in the tree view you need the right to display and modify security officers.

1. In the SafeGuard Management Center, select **Security Officers**.
2. In the navigation window, drag-and-drop the officer you want to move to the respective node.

All children of the selected officer will also be moved.

3.8.9.16 Fast switching of security officers

For your convenience, you may quickly restart the SafeGuard Management Center, to log on as a different officer.

1. In the SafeGuard Management Center, select **File > Change security officer**. The SafeGuard Management Center is restarted and the logon dialog is displayed.
2. Select the security officer you want to use to log on to the SafeGuard Management Center and enter their password. If you are working in Multi Tenancy mode, you are logged on to the same database configuration.

The SafeGuard Management Center is restarted displaying the view assigned to the logged on officer.

3.8.9.17 Delete a security officer

Prerequisite: To delete a security officer or Master Security Officer, you need the right to display and delete security officers.

1. In the SafeGuard Management Center, select **Security Officers**.
2. In the navigation window, right-click the security officer or Master Security Officer you want to delete and select **Delete**. Note that you cannot delete the officer you are logged on with.
3. If the officer has children, you are prompted to select a new parent node for the children.

The officer is deleted from the database.

 **Note** A Master Security Officer explicitly created as an officer and not only promoted to security officer must always remain in the database. If a user promoted to security officer is deleted from the database, their user account is deleted from the database as well.

 **Note** If the officer to be deleted has been assigned a role that includes additional authentication and the officer is the only one this role is assigned to, the officer will be deleted nonetheless. It is assumed that the Master Security Officer will be able to take over additional authorization.

3.8.10 Managing the organizational structure

The organizational structure can be reflected in the SafeGuard Management Center in two ways:

- You can import an existing organizational structure into the SafeGuard Enterprise Database, for example through an Active Directory.
- You can manually create your organizational structure by creating workgroups and domains along with a structure for managing policy items.

3.8.10.1 Importing from Active Directory

You can import an existing organizational structure into the SafeGuard Enterprise Database through an Active Directory.

 **Note** An initial import is triggered by the SafeGuard Management Center Configuration Wizard. When running the wizard, you may skip this step and you can manually configure your Active Directory import later.

We recommend that you create one dedicated Windows service account that is used for all import and synchronization tasks. For more information, see [Sophos knowledge base article 107979](#).

With the SafeGuard Management Task Scheduler, you can create periodic tasks for automatic synchronization between Active Directory and SafeGuard Enterprise. Your product delivery contains a predefined script template for this purpose. For further information, see [Scheduling tasks \(page 194\)](#) and [Predefined scripts for periodic tasks \(page 202\)](#).

 **Note** We recommend that you divide the import of more than 400,000 objects from AD into multiple operations. This may not be possible if there are more than 400,000 objects in a single organizational unit.

Security officer access rights and Active Directory import

You need to make sure you have the appropriate access rights when importing the organizational structure. The following information tells you about the access rights requirements.

- If you add an Active Directory connection to a domain that already exists, the following applies:
 - If you have **Full access** rights for the domain (DNS), the directory connection credentials are updated.
 - If you have **Read only** rights or less for the domain (DNS), the credentials are not updated, but you can use existing credentials for synchronization purposes.
- For Active Directory import and synchronization, the access rights to a container or a domain are projected to the domain tree you import or synchronize. If you do not have **Full access** rights for a sub-tree, it cannot be synchronized. If a sub-tree cannot be modified, it is not shown in the synchronization tree.
- Regardless of your security officer access rights for directory objects, you can import a new domain from the Active Directory, if it does not exist in the SafeGuard Enterprise Database yet. You and your superior security officers will be granted **Full access** rights to the new domain automatically.
- If you select a sub-container for synchronization, synchronization has to be done all the way up to the root. In the synchronization tree, all relevant containers are selected automatically, even if there are any containers above the sub-container that are **Read only** or **Denied** according to your access rights. If you deselect a sub-container, you also may have to deselect containers up to the root, depending on your access rights.

If a group with **Read only** or **Denied** access is included in a synchronization process, the following happens:

- The group's memberships are not updated.
- If the group was deleted in the Active Directory, it will not be deleted from the SafeGuard Enterprise Database.
- If the group was moved in the Active Directory however, it will be moved within the SafeGuard Enterprise structure. This includes moving the group to a container that you do not have **Full access** rights for.

If a container with **Read only** or **Denied** access is included in the synchronization because it is on the way up to the root and the container contains a group with **Full access**, this group will be synchronized. Groups with **Read only** or **Denied** access will not.

Import an Active Directory structure

SafeGuard Enterprise allows you to import an Active Directory structure into the SafeGuard Management Center. An initial import is triggered by the SafeGuard Management Center Configuration Wizard, see [Define Active Directory authentication \(page 38\)](#). During the synchronization with the Active Directory, objects such as computers, users, and groups are imported to the SafeGuard Management Center. All data is stored within the SafeGuard Database.

To configure the Active Directory, do the following:

1. Open the SafeGuard Management Center.
2. Authenticate using the password which was defined for the certificate store.
3. In the lower left-hand pane, select **Users and Computers**.
4. In the top left window, select **Root [Filter is active]**.
5. In the right-hand pane, select the **Synchronize** tab. The **LDAP Authentication** wizard starts automatically.
6. In the **LDAP Authentication** wizard, enter the logon credentials you want to use for the synchronization and specify the server name or the IP address of the Domain controller. The user name must be in the format User@Domain to avoid issues resolving the domain NetBIOS name.
7. As soon as the directory connection is successfully established, the **Directory DSN** field shows the domain information. Click the magnifier symbol in order to read the Active Directory.
8. When the reading process is complete, the domain structure is displayed in the center pane. Select the organizational units you want to import into SafeGuard Enterprise. It is not possible

to select individual machines, groups, or user objects. However, it is possible to select organizational units.

9. Decide whether Active Directory group memberships should be synchronized with the SafeGuard Management Center. The import of group memberships can be skipped by un-checking the **Synchronize memberships** box. Not importing and synchronizing group memberships has a positive impact on the performance of the Management Center (especially in large AD structures).

By default, SafeGuard Enterprise creates a key for every container, organizational unit (OU), and domain object that is imported. The creation of keys can be quite time consuming. Therefore, especially when importing large environments, we recommend that you do not enable the key creation for groups if not required.

10. Start the synchronization by clicking **Synchronize**. The detailed information from the Active Directory will now be read. At the end of the synchronization, a summary of all changes is displayed.

11. Click **OK** to write all changes into the SafeGuard Enterprise Database.

As soon as this is completed, the domain structure is displayed in the left-hand pane. The import of the Active Directory into the SafeGuard Management Center is now complete.

Synchronize the organizational structure

If elements have been moved from one subtree to another in Active Directory, both subtrees have to be synchronized with the SQL database. Synchronizing just one subtree will result in deleting instead of moving the objects.

1. In the SafeGuard Management Center, click **Users and Computers**.
2. In the left-hand navigation window, click the root directory **Root [filter is active]**.
3. In the action area on the right, select the **Synchronize** tab.
4. Select the required directory from the **Directory DSN** list and click the magnifier icon (top right).

A graphical representation of the Active Directory structure of the organizational units (OU) in your company is displayed.

5. Check the organizational units (OU) to be synchronized. You do not need to import the entire contents of the Active Directory.
6. To also synchronize memberships, select the check box **Synchronize memberships**.

7. To also synchronize the user enabled state, select the check box **Synchronize user enabled state**.
8. When you synchronize disabled user accounts from Active Directory, they are disabled in SafeGuard Enterprise as well. For security reasons, re-enabling the account in Active Directory and synchronizing it again does not enable the user account in SafeGuard Enterprise automatically. To synchronize these accounts as well, you have to activate the **Synchronize user enabled state** option.
9. At the bottom of the action area, click **Synchronize**.

When synchronizing users and their group memberships, the membership to a "primary group" is not synchronized as it is not visible for the group.

The domains are synchronized. Synchronization details are displayed. Click on the message displayed in the status bar beneath the buttons on the left to view a synchronization protocol. Click on the protocol, to copy it to the clipboard and paste it into an e-mail or file.

 **Note** During Active Directory synchronization, users are not automatically registered in SafeGuard Enterprise. Users who register during synchronization need to restart their computer after syncing to log on to SafeGuard Enterprise. See [Automatic registration of a new user \(page 152\)](#).

Import a new domain from an Active Directory

1. In the left-hand navigation window, click the root directory **Root [filter is active]**.
2. Select **File > New > Import domain from Active Directory**.
3. In the action area on the right, select **Synchronize**.
4. Select the required directory from the **Directory DSN** list and click the magnifier icon (top right).

A graphical representation of the Active Directory structure of the organizational units (OU) in your company is displayed.

5. Check the domain to be synchronized and click **Synchronize** at the bottom of the navigation area.

 **Note** If elements have been moved from one subtree to another in Active Directory, then both subtrees have to be synchronized with the SQL database. Synchronizing just one subtree results in deleting instead of moving the objects.

 **Note** AD synchronization does not synchronize the pre-Windows 2000 (NetBIOS) name of the domain, if the Domain Controller is configured with an IP address. Configure the Domain Controller

to use the server name (NetBIOS or DNS) instead. The client (on which the AD synchronization is running) must be either part of the domain, or it must be able to resolve the DNS name to the target Domain Controller.

Import users and computers from Active Directory on container level

If you already have an existing organizational structure in the SafeGuard Management Center and if you have the right to import directory objects, you can import users and computers from Active Directory on the container level. Only new or moved users or computers of the selected container and its subcontainers will be synchronized.

1. In the SafeGuard Management Center, click **Users and Computers**.
2. In the left-hand navigation window, right-click on the container whose users and computers you want to synchronize.
3. In the context menu, click on **New** and then on **Import users and computers from Active directory**.

The **Import Users and Computers from Active Directory** dialog is displayed and the import starts.

The result of the import will be listed. Name, logon name, and the status of the imported users and computers are shown. **Status** can be **Imported** or **Moved**.

4. Click **Close**.

The users and computers are displayed in the left-hand navigation window.

Search and import users and computers

To do this, you must have the right to create directory objects.

If you already have an existing organizational structure in the SafeGuard Management Center you can search for Active Directory users and computers and import them directly into the organizational structure.

1. In the navigation area of the SafeGuard Management Center, click **Users and Computers**.
2. In the **Users and Computers** navigation area, click the root directory **Root [filter is active]**.
3. In the SafeGuard Management Center menu bar, click **Edit > Find**.

The **Find Users, Computers and Groups** dialog is displayed.

4. Select the **Active Directory** tab.
5. Select the required filter from the **Find** drop-down list.
6. On the **In** drop-down list, select the domain in which you want to search.
7. If you search for a specific user or computer, enter the required name in the **Search Name** field.
8. Click **Find now**.
The search result is displayed on the **Active Directory** tab. All new objects have a check box on the left-hand side.
9. Select the objects you want to import.
10. Click on **Import selected**.
The objects are imported and displayed in the left-hand navigation window.
11. Click **Close**.

3.8.10.2 Creating workgroups and domains

Security officers with the necessary rights can manually create workgroups or domains along with a structure for managing policy items. It is also possible to assign policies and/or encryption policies to local users.

You only have to manually create domains, if you do not want to or you cannot import a domain from an Active Directory (AD), for example because there is no AD available.

For logged events, see [Auditing \(page 204\)](#).

Automatic registration of a new user

When a new user logs on to SafeGuard Enterprise once their endpoint has contacted the SafeGuard Enterprise Server, they are registered and automatically displayed in the **Users and Computers** area of the SafeGuard Management Center under their respective domain or workgroup.

The directory for these users/computers (**.Auto registered**) is automatically created under the root directory and under each domain or workgroup. It cannot be renamed nor moved. Objects in this directory cannot be moved manually either.

As long as there is no domain or workgroup the objects remain in the **.Auto registered** directory. When the domain or workgroup is synchronized with the next contact to the SafeGuard Enterprise Database, the object is moved to the respective domain or workgroup. Otherwise it remains under the **.Auto registered** directory.

Usually, only a master security officer can manage the auto-registered objects.

To give security officers the right to manage objects in the .Auto registered directory, for example for recovering a computer in this group, you need to manually create the domain or workgroup the object belongs to. Then you can assign rights for security officers to these domains or workgroups as usual. The objects will then be moved to their domain automatically.

Local users cannot log on to SafeGuard Enterprise with an empty password. Local users who log on to SafeGuard Enterprise with an empty password remain guest users and are not saved to the database. If Windows Autologon is activated for these users, logon is denied. For a successful logon at SafeGuard Enterprise, a new password must be created in this case and Windows Autologon must be deactivated in the registry of the endpoint.

Microsoft accounts are always handled as SafeGuard Enterprise guest users.

Note During Active Directory synchronization, users are not automatically registered in SafeGuard Enterprise. Users who register during synchronization need to restart their computer after syncing to log on to SafeGuard Enterprise.

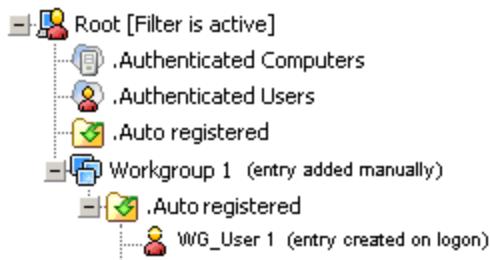
Examples for auto-registration

Below you find two examples for the behavior of auto-registered objects.

Users or computers not part of an Active Directory

In a company, not all user or computer objects may necessarily be part of an Active Directory (AD), for example local users. A company may have one or several workgroups so that an AD is not needed.

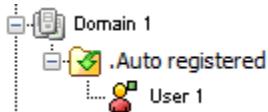
This company wants to deploy SafeGuard Enterprise and then add policies to its user or computer objects. Therefore the company's organizational structure is created manually in the SafeGuard Management Center as follows:



The objects remain in the .Auto registered folder. They can be properly managed with the SafeGuard Management Center by applying policies to the .Auto registered folder.

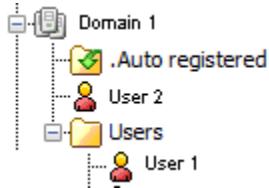
SafeGuard Enterprise Database and Active Directory out of sync

A user is already part of the company's Active Directory (AD). But the SafeGuard Enterprise Database and the AD are out of sync. The user (**User 1**) logs on to SafeGuard Enterprise and is automatically displayed in the SafeGuard Management Center **Users and Computers** area under the domain that is provided with the logon (**Domain 1**).



The user is now part of the **.Auto registered** folder. The object can be properly managed with the SafeGuard Management Center by applying policies to the **.Auto registered** folder.

Upon the next synchronization between the AD and the SafeGuard Enterprise Database **User 1** is automatically moved to their organizational unit (**Users**).



For policies to become active for **User 1**, they must be assigned to the organizational unit **Users** from now on.

Keys and certificates for auto-registered objects

For each auto-registered object, a certificate is generated as required by the server.

A local user gets two keys:

- the key to the **.Auto registered** container
- the private key generated as required by the server

Local users neither get any other keys for their assigned container nor a root key.

Workgroups do not get a key.

Policies for auto-registered objects

For auto-registered objects, policies can be created without any restrictions.

Local users are added to the "Authenticated Users" group. Computers are added to the "Authenticated Computers" group. The policies activated for these groups apply accordingly.

Create workgroups

Security officers with the required rights can create a container under the root directory which represents a Windows workgroup. Workgroups do not have a key. They cannot be renamed.

1. In the SafeGuard Management Center, click **Users and Computers**.
2. In the navigation window on the left, right-click **Root [Filter is active]** and select **New > Create new workgroup (auto registration)**.
3. Under **Common information**, do the following:
 - a. Enter a **Full name** for the workgroup.
 - b. Optionally you can add a **description**.
 - c. The object type is displayed in the **Connection state** field, in this case **Workgroup**.
 - d. To prevent policy inheritance, you can select **Block Policy Inheritance**.
 - e. Click **OK**.

The workgroup is created. The default **.Auto registered** directory is automatically created under the workgroup container. It cannot be renamed or deleted.

Delete workgroups

To delete workgroups you need **Full access** rights for the workgroup concerned. Members assigned to the workgroup are also deleted. They are automatically re-registered at next logon.

To delete a workgroup, you need **Full access** rights for all objects involved.

1. In the SafeGuard Management Center, click **Users and Computers**.
2. In the navigation window on the left, right-click the workgroup you want to delete and select **Delete**.
3. Click **Yes** to confirm.

The workgroup is deleted. Any members are also deleted.

 **Note** If you do not have **Full access** rights for all members of the workgroup, deleting the workgroup fails and an error message is displayed.

Create a new domain

Security officers with the required rights can create a new domain under the root directory. You only have to create a new domain, if you do not want to or you cannot import a domain from the Active Directory (AD) (for example because there is no AD available).

1. In the SafeGuard Management Center, click **Users and Computers**.
2. In the navigation window on the left, right-click **Root [Filter is active]** and select **New > Create new domain (auto registration)**.
3. Under **Common information**, enter the following information about the domain controller.

All two name entries must be correct. Otherwise the domain will not be synchronized.

- a. **Full name:** For example *computer name.domain.com* or the IP address of the domain controller
- b. **Distinguished name** (read-only): DNS name, for example
DC=computername3,DC=domain,DC=country
- c. A domain description (optional)
- d. **Netbios name:** Name of the domain controller
- e. The object type is displayed under **Connection state**, in this case **Domain**.
- f. To prevent policy inheritance, you can select **Block Policy Inheritance**.
- g. Click **OK**.

The new domain is created. Users and/or computers are automatically assigned to this domain during auto-registration. The default **.Auto registered** directory is automatically created under the domain container. It cannot be renamed or deleted.

Rename a domain

Security officers with the required rights can rename a domain and define additional properties. You need **Full access** rights for the relevant domain.

1. In the SafeGuard Management Center, click **Users and Computers**.
2. In the navigation window on the left, right-click the domain you want to rename and select **Properties**.
3. In **Common information** under **Full name**, change the domain name and the description.
4. You can change the name of the domain controller in **Netbios name**.
5. You can also define the Wake on LAN mode for automatic restart in the **Container Settings** tab.
6. Click **OK** to confirm.

The changes are now saved.

Delete a domain

Security officers with the required rights can delete domains. To delete a domain, you need **Full access** rights for the domain concerned. Members assigned to the domain are also deleted.

1. In the SafeGuard Management Center, click **Users and Computers**.
2. In the navigation window on the left, right-click the domain you want to delete and select **Delete**.
3. Click **Yes**.

The domain is deleted. Any members are also deleted.

If you have less than **Full access** rights for all members of the domain, deleting the domain fails and an error message is displayed.

Delete auto registered computers

When an auto-registered computer is deleted, all local users of this computer are also deleted. They are automatically re-registered the next time they log on to this computer.

Display and search for local users

In **Users and Computers**, you can filter the view in the navigation area on the left according to local users or search for specific local users.

1. In the SafeGuard Management Center, click **Users and Computers**.
2. In the bottom left of the navigation window, click **Filter**.
3. Select **Local User** as **Type**. If you are looking for a specific user, enter the name of this user.
4. Click the magnifier icon.

The **Users and Computers** view is filtered according to the criteria.

Microsoft accounts are always handled as SafeGuard Enterprise guest user.

3.8.11 Keys and Certificates

When importing the directory structure, SafeGuard Enterprise in its default setting automatically generates keys for:

- Domains
- Containers/OUs

and assigns them to the corresponding objects. Computer and user keys are generated as required.

Keys for groups

In its default setting, SafeGuard Enterprise does not automatically generate keys for groups. This behavior is deactivated by default. As a security officer, you can change this behavior on the **Keys**

tab by selecting **Tools > Options**. If **Groups** is checked on the **Keys** tab, SafeGuard Enterprise automatically generates group keys, when the database is synchronized. At the bottom of the **Synchronization** tab it is indicated for which items keys are generated when synchronization is performed.

Keys cannot be deleted! They are retained permanently in the SafeGuard Enterprise Database.

The first time an endpoint is started, SafeGuard Enterprise generates a computer key for that endpoint (defined machine key).

The defined machine key is only generated when volume-based encryption is installed on the endpoint.

Each user obtains all their keys at logon from their user key ring. The user key ring comprises the following:

- the keys of the groups of which the user is a member
- the keys of the overall Container/OUs of the groups of which the user is a member.

The keys in the user key ring determine the data which that user can access. The user can only access data for which they have a specific key.

To avoid showing too many unused group keys in the user's key ring, you can specify keys to be hidden. For further information, see [Hide keys \(page 160\)](#).

To display all keys for a user, click **Users and Computers** and select the **Keys** tab.

To display all keys, click **Keys and Certificates** in the SafeGuard Management Center and select **Keys**. You can generate lists for **Assigned Keys** and **Inactive Keys**.

The **Assigned Keys** list only shows the keys assigned to objects for which you have **Read only** or **Full access** rights. The **Keys** view shows the number of all available keys, regardless of your access rights. The **Assigned Keys** list shows the number of keys visible according to your access rights.

1. Click **Users and Computers** to open the display.
2. The keys of a selected object are displayed in the action area and in the respective views.
3. The display in the action area depends on what is selected in the navigation area. All keys assigned to the selected object are displayed.
4. Under **Available Keys**, all available keys are displayed. Keys already assigned to the selected object are grayed out. Select **Filter** to switch between keys already assigned to an object (active) and keys not yet assigned to an object (inactive).

After the import, each user receives a number of keys which can be used for data encryption.

3.8.11.1 Keys for data encryption

Users are assigned keys for the encryption of specific volumes when defining policies of the type **Device Protection**.

In a policy of the type **Device Protection**, you can specify the setting **Key to be used for encryption** for each media.

Here you decide which keys a user can or must use for encryption:

- **Any key in user key ring**

After users have logged on to Windows, they can select the keys they would like to use to encrypt a particular volume. A dialog is displayed in which users can select the required key.

- **Any key in user key ring, except user key**

Users may not use their own personal key to encrypt data.

- **Any group key in user key ring**

Users may only select one of the group keys in their user key ring.

- **Defined machine key**

The defined machine key is the unique key generated exclusively for this computer by SafeGuard Enterprise during the first startup. The user has no other options. A defined machine key is typically used for the boot and system partition and for drives on which Documents and Settings are located.

- **Defined key on list**

This option allows you to define a specific key which the user must use for encryption. To specify a key for a user in this way, you must define a key under **Defined key for encryption**. This option is displayed once you select **Defined key on list**.

Click the [...] button next to **Defined key for encryption** to display a dialog in which you can specify a key. Make sure that the user also has the corresponding key.

Mark the selected key and click **OK**. The selected key will be used for encryption on the endpoint computer.

Assign keys in Users and Computers

To assign keys to users, you need **Full access** rights for the relevant object.

To assign a new key to users:

1. In the SafeGuard Management Center, click **Users and Computers**.
2. In the navigation area, select the required object (for example user, group or container).
3. Right-click in the **Keys** tab and select **Assign new key** from the context menu.
4. In the **Assign New Key** dialog:
 - a. Enter a **Symbolic name** and **Description** for the key.
 - b. To hide the key in the user's key ring, select the **Hide key** check box.
5. Click **OK**.

The key is assigned and displayed in the **Key** tab.

Unassign keys in Users and Computers

Make sure that you have the **Unassign keys** right. It is part of the predefined **Security Officer** role.

To unassign a **Personal Key** you additionally need the **Manage Personal Keys** right. By default only a Master Security Officer has this right.

To unassign a key:

1. In the SafeGuard Management Center, click **Users and Computers**.
2. In the navigation area, select the required object (for example user, group or container).
3. On the **Key** tab, select the key.
4. Right-click the key and select **Remove** from the context menu.
5. In the confirmation dialog, click **Yes**.
6. Click **OK**.

The key is unassigned, removed from the **Key** tab, and displayed in the **Available keys** list.

Hide keys

To avoid showing too many unused group keys in a user's key ring on the endpoint, you can define keys to be hidden. Keys which are not shown in the user's key ring can still be used to access encrypted files, but not to encrypt new ones.

To hide keys:

1. In the SafeGuard Management Center, click **Keys and Certificates**.

2. In the navigation area, click **Keys > Assigned Keys**.

The **Assigned Keys** view is displayed showing the **Hide Key** column.

3. There are two ways to specify that keys are to be hidden:

- Select the check box in the **Hide Key** column for the required key.
- Select one or several keys and right-click to open a context menu.

Select **Hide Key From User**.

4. Save your changes to the database.

The specified keys are not shown in the user's key ring.

For information on displaying the user's key ring on the endpoint, see the *SafeGuard Enterprise user help*, chapter *Accessing SafeGuard Enterprise*.

If a policy specifies a hidden key to be used for encryption, the **Hide Key** setting does not affect encryption on the endpoint.

3.8.11.2 Personal Keys for file-based encryption by File Encryption

A Personal Key is a special type of encryption key that is created for a specific user and cannot be shared with other users. A Personal Key that is active for a specific user is called an active Personal Key. Active Personal Keys cannot be assigned to other users.

In **File Encryption** policies, you can define encryption rules that use the placeholder **Personal Key** instead of a key name. For such rules, the encryption key to be used is the active Personal Key of the user.

When you define an encryption rule for the path *C:\encrypt* to be encrypted with the Personal Key, different keys are used for different users. You can thereby ensure that information in specific folders is private for users. For further information see [Location-based File Encryption \(page 302\)](#).

If a File Encryption rule defines a Personal Key to be used for encryption, Personal Keys are created automatically for the relevant users, if they do not have active Personal Keys yet.

As a security officer with the required rights, you can create Personal Keys for selected users or all users in selected groups in the SafeGuard Management Center. You can also demote active Personal Keys, for example when a user leaves the company.

Automatic creation of Personal Keys

If a File Encryption rule defines a Personal Key to be used for encryption and the user does not have an active Personal Key yet, the SafeGuard Enterprise Server automatically creates it. During the timeframe between policy receipt on the endpoint and the required active Personal Key becoming available, the user is not allowed to create new files in the folders covered by the File Encryption rule.

For initial deployment of **File Encryption** policies with encryption rules using Personal Keys to a larger group of users (hundreds or more) who do not have active Personal Keys yet, we recommend to create Personal Keys in the SafeGuard Management Center, see [Create Personal Keys for multiple users \(page 162\)](#). This reduces the load on the SafeGuard Enterprise Server.

Create a Personal Key for a single user

To create a Personal Key, you need the rights **Create keys** and **Assign keys**. In addition, you need **Full access** rights for the object involved. To replace an active Personal Key, you need the right **Manage Personal Keys**.

1. In the SafeGuard Management Center, select **Users and Computers**.
2. In the navigation area, select the required user.
3. Right-click in the **Keys** tab and select **Assign new key** from the context menu.
4. In the **Assign new key** dialog:
 - a. Enter a description for the Personal Key.
 - b. To hide the Personal Key in the user's key ring, select **Hide key**.
5. Depending on whether you are creating a Personal Key for a user who does not have an active Personal Key yet, or for a user who does, the **Assign new key** dialog shows different check boxes. Select the check box displayed, to define the newly created key as a Personal Key:
 - **Personal Key**: This check box is displayed for users who do not have an active Personal Key yet.
 - **Replace active Personal Key**: This checkbox is displayed for users who already have an active Personal Key.
6. Click **OK**.

The Personal Key is created for the selected user. In the **Key** tab, the key is shown as the **Active Personal Key** for the user. For a user who already had an active Personal Key before, the existing key is demoted and the user receives the new one. The demoted Personal Key remains in the user's key ring. The active Personal Key cannot be assigned to other users.

Create Personal Keys for multiple users

To create Personal Keys, you need the rights **Create keys** and **Assign keys**. In addition, you need **Full access** rights for the objects involved. To replace existing active Personal Keys, you need the right **Manage Personal Keys**.

1. In the SafeGuard Management Center, click **Users and Computers**.
2. In the navigation area, right-click the node for which you want to create Personal Keys:
 - a domain node,
 - the .Auto registered node in the root or in domains or
 - an Organizational Unit node.
3. From the context menu, select **Create Personal Keys for users**.
4. In the **Create Personal Key for Users** dialog:
 - a. Enter a description for the Personal Keys.
 - b. To hide the Personal Keys in the users' key rings, select **Hide key**.
 - c. To replace existing active Personal Keys with the new ones, select **Replace existing active Personal Keys**.
5. Click **OK**.

The Personal Keys are created as for all users in the selected node. In the **Key** tab, the keys are shown as **Active Personal Keys** for the users. If users already had active Personal Keys before and you have selected **Replace existing active Personal Keys**, the existing keys are demoted and the users receive new ones. The demoted Personal Keys remain in the users' key rings. The individual active Personal Keys cannot be assigned to other users.

Demote active Personal Keys

To demote active Personal Keys manually, you need the rights **Modify Keys** and **Manage Personal Keys**. By default, the right **Manage Personal Keys** has been assigned to the predefined role Master Security Officer, but it can also be assigned to new user-defined roles. In addition, you need **Full access** rights for the object involved.

You can demote active Personal Keys manually, for example if a user leaves the company. Provided that you have the right **Manage Personal Keys** you can assign the demoted Personal Key of this user to other users to give them read-only access to files encrypted with this key. But they cannot use this key for encrypting files.

This cannot be undone. A demoted Personal Key can never become an active Personal Key for any user again.

1. In the SafeGuard Management Center, select **Users and Computers**.
2. In the navigation area, select the required user.
3. In the **Key** tab, right-click the required **Active Personal Key** and select **Demote Personal Key** from the context menu.

The key is demoted. It is still a Personal Key, but cannot be used as an active Personal Key anymore. If a File Encryption rule defines a Personal Key to be used for encryption and the user does not have an active Personal Key, the SafeGuard Enterprise Server automatically creates it.

3.8.11.3 Certificates

- A user can only have one certificate assigned. If this user certificate is stored on a token, then users can only log on to their endpoint using this token (cryptographic token - Kerberos).
- Note that, when importing a user certificate, the certificate's public and private sections are both imported. If only the public part is imported, only token authentication is supported.
- The combination of CA certificates and CRL (Certificate Revocation List) must match. Otherwise users cannot log on to the respective endpoints. Please check that the combination is correct. SafeGuard Enterprise does not carry out this check!
- If Certification Authority (CA) certificates are deleted in the database and you do not wish to use them again, you should remove these certificates manually from the local store of all administrator computers.

SafeGuard Enterprise can then only communicate with expired certificates if old and new keys are present on the same token.

- CA certificates cannot be obtained from a token and stored in the database or certificate store. If you use CA certificates, they need to be available as files, not just on a token. The same applies to CRLs.
- Certificates generated by SafeGuard Enterprise are signed with SHA-1 or SHA-256 for verification. SHA-256 provides enhanced security and is used by default with first-time installations. If SafeGuard Enterprise 6 or earlier endpoints still need to be managed or when upgrading from a previous version, SHA-1 is used by default.
- Certificates provided by the customer and imported into SafeGuard Enterprise are currently not verified according to RFC3280. For example, we do not prevent using signature certificates for encryption purposes.
- The logon certificates for security officers must be located in the “MY”certificate store.

The **Assigned Certificates** list in **Keys and Certificates** only shows the certificates assigned to objects for which you have **Read only** or **Full access** rights. The **Certificate** view indicates the number of all available certificates, regardless of your access rights. The **Assigned Certificates** list shows the number of certificates available according to your access rights.

To modify certificates, you need **Full access** rights to the container the users resides in.

Import CA certificates and Certificate Revocation Lists

If CA certificates are in use, import the complete CA hierarchy including all CRLs into the SafeGuard Database. CA certificates cannot be obtained from tokens, but need to be available as files so that you can import them into the SafeGuard Enterprise Database. This also applies to Certificate Revocation Lists (CRL).

1. In the SafeGuard Management Center, click **Keys and Certificates**.
2. Select **Certificates** and click the **Import CA certificates** icon in the toolbar. Browse for the CA certificate files you want to import.
The imported certificates are displayed in the work area on the right.
3. Select **Certificates** and click the **Import CRL** icon in the toolbar. Browse for the CRL files you want to import.
The imported CRLs are displayed in the work area on the right.
4. Check that CA and CRL are correct and match. CA certificates must match the CRL before users can log on to the computers concerned. SafeGuard Enterprise does not carry out this check.

Change algorithm for self-signed certificates

- All SafeGuard Enterprise components must have version 6.1 or later.

Certificates generated by SafeGuard Enterprise, such as the company, machine, security officer and user certificates are signed with hash algorithm **SHA-256** by default during the first-time installation for enhanced security.

When upgrading from SafeGuard Enterprise 6 or earlier, hash algorithm **SHA-1** is automatically used for self-signed certificates. You can manually change it to **SHA-256** for enhanced security after the upgrade is completed.

Only change the algorithm to **SHA-256** if all SafeGuard Enterprise components and endpoints have been upgraded to the current version. **SHA-256** is not supported in mixed environments where for example SafeGuard Enterprise 6 endpoints are managed by the SafeGuard Management Center 7. If you have a mixed environment, you must not carry out this task and must not change the algorithm to **SHA-256**.

Changing the algorithm for self-signed certificates involves the following steps:

- Changing the hash algorithm.
- Creating a Certificate Change Order (CCO).
- Creating a configuration package including the CCO.

- Restarting the SafeGuard Enterprise (database) servers.
- Distributing and deploying the configuration packages on the endpoints.

To change the algorithm for self-signed certificates:

1. In the SafeGuard Management Center menu bar, select **Tools > Options**.
2. On the **General** tab, under **Certificates**, select the required algorithm from **Hash algorithm for generated certificates** and click **OK**.
3. On the **Certificates** tab, under **Request**, click **Update**. In **Update Company certificate**, enter a name for the CCO and specify a backup path. Enter a password for the P12 file and retype it. Optionally enter a comment and click **Create**.
4. Confirm when prompted that this change cannot be reverted and that all configuration packages created after this company certificate update need this CCO included to work on already installed endpoints.
5. Confirm when prompted that the update was successful and that a CCO to be included in all configuration packages has been created. Click **OK**.
6. On the **Tools** menu, click **Configuration Package Tool**.
7. Select the required type of endpoint configuration package: **Managed client packages** or **Standalone client packages**.
8. Click **Add Configuration Package** and enter a name of your choice for the configuration package.
9. Select the **CCO** you created beforehand.
10. Make further selections as appropriate.
11. Specify an output path for the configuration package (MSI).
12. Click **Create Configuration Package**.
The configuration package (MSI) has now been created in the specified directory.
13. Restart all SafeGuard Enterprise (database) servers.
14. Distribute and deploy this package to the SafeGuard Enterprise protected endpoints.

All certificates generated by SafeGuard Enterprise are signed with the new algorithm. For more information, see [Sophos knowledge base article 116791](#).

[Assign a certificate from Active Directory](#)

- The certificate must be listed on the **Published Certificates** tab of the users' properties in Active Directory.

1. In the SafeGuard Management Center, click **Users and Computers**.
2. Select the user you want to assign a certificate to, and open the **Certificate** tab in the work area on the right-hand side.
3. Click the **Find certificate in directory** icon on the SafeGuard Management Center toolbar or select **Find certificate in directory** from the **Actions** menu.
4. Select the certificate in the **Assign a certificate from directory** dialog.
5. Click **OK**.

The certificate is assigned to the user. A user can only have one certificate assigned.

Create and assign a certificate

1. In the SafeGuard Management Center, click **Users and Computers**.
2. Select the user you want to assign a certificate to, and open the **Certificate** tab in the work area on the right-hand side.
3. Click the **Add certificate** icon on the SafeGuard Management Center toolbar or select **Add certificate** from the **Actions** menu.
4. Enter a password and confirm it.
5. Click **OK**.

The certificate is assigned to the user. A user can only have one certificate assigned.

3.8.11.4 Exporting company and Master Security Officer certificates

In a SafeGuard Enterprise installation, the following two items are critical and must be backed up in a safe location:

- The company certificate stored in the SafeGuard Database.
- The Master Security Officer (MSO) certificate residing in the certificate store of the computer on which the SafeGuard Management Center is installed.

You can export both certificates in form of .p12 files for backup purposes. To restore installations, you can import the relevant company and security officer certificate as .p12 files and use them when you set up a new database. This avoids restoring the whole database.

Note

We recommend that you carry out this task right after initial configuration of the SafeGuard Management Center.

For exporting the Master Security Officer certificate, see [Export the Master Security Officer certificate \(page 130\)](#).

Export the company certificates

Only Master Security Officers are entitled to export company certificates for backup purposes.

1. In the SafeGuard Management Center menu bar, select **Tools > Options**.
2. Select the **Certificates** tab and click **Export** in the **Company Certificate** section.
3. You are prompted to enter a password for securing the exported file. Enter a password, confirm it and click **OK**.
4. Enter a file name and storage location for the file and click **OK**.

The company certificate is exported as a .p12 file to the defined location and can be used for recovery purposes.

3.8.12 Company Certificate Change Orders

Company Certificate Change Orders (CCOs) are used in the following cases:

- **To renew the company certificate** in case it will expire soon.

Renewing the company certificate is possible for managed and unmanaged endpoints but can only be triggered from the management console.

- **To move unmanaged endpoints** to a different environment, for example if you have two different Sophos SafeGuard environments and want to merge them into one Sophos SafeGuard environment where always one of the two environments has to be the target environment.

This is done by exchanging the company certificate of the endpoints of one environment with the company certificate of the target environment.

Only Master Security Officers are allowed to create CCOs. To give other security officers the permission to create CCOs, the MSO must create a custom role and assign the right to **Manage CCOs** to this role.

3.8.12.1 Renew the company certificate

A company certificate that is about to expire can be renewed in SafeGuard Management Center. At logon, the SafeGuard Management Center starts to display a warning six months before the company

certificate expires. Without a valid company certificate an endpoint cannot connect to the server. Renewing the company certificate involves three steps:

- Creating a Certificate Change Order (CCO).
- Creating a configuration package including the CCO.
- Restarting the servers and distributing and deploying the configuration packages on the endpoints.

To renew a company certificate:

1. In the SafeGuard Management Center menu bar, select **Tools > Options**.
2. Select the **Certificates** tab and click **Update** in the **Request** section.
3. In the **Update Company certificate** dialog, enter a name for the CCO and specify a backup path. Enter a password for the P12 file and retype it. Optionally enter a comment and click **Create**.
4. Confirm when prompted that this change cannot be reverted and that all configuration packages created after this company certificate update need this CCO included to work on already installed endpoints.
5. Confirm when prompted that the update was successful and that a CCO to be included in all configuration packages has been created. Click **OK**.
6. On the **Tools** menu, click **Configuration Package Tool**.
7. Select **Managed client packages**.
8. Click **Add Configuration Package** and enter a name of your choice for the configuration package.
9. Assign a **Primary Server** (the **Secondary Server** is not necessary).
10. Select the **CCO** you created beforehand to update the company certificate.
11. Select the **Transport Encryption** mode defining how the connection between SafeGuard Enterprise Client and SafeGuard Enterprise Server is to be encrypted, either SafeGuard transport encryption or SSL encryption.
The advantage of SSL is that it is a standard protocol and that a faster connection can be achieved than when using SafeGuard transport encryption. SSL encryption is selected by default. For further information on how to secure transport connections with SSL, see [Securing transport connections with SSL \(page 45\)](#).
12. Specify an output path for the configuration package (MSI).
13. Click **Create Configuration Package**.

If you have selected SSL encryption as the **Transport Encryption** mode, the server connection is validated. If the connection fails, a warning message is displayed.

The configuration package (MSI) has now been created in the specified directory. Make sure that you restart all SGN servers. You now need to distribute and deploy this package to the SafeGuard Enterprise managed endpoints.

3.8.12.2 Replace the company certificate

Replacing the company certificate is necessary when you want to move an endpoint from one standalone environment to a different one. The endpoint to be moved needs to have the company certificate of the environment it is to be moved to. Otherwise the endpoint does not accept policies of the new environment.

The following prerequisites must be met:

Decide which is your source and which is your target Management Center environment. The source Management Center is the one you used for creating the configuration packages for the endpoints that are to be moved. The target Management Center is the one the endpoints will be moved to.

To replace the company certificate:

1. Open the target Management Center and select **Tools > Options**.
2. Select the **Certificates** tab and click the **Export** button under **Company Certificate**.
3. Enter and confirm a password for the certificate backup when prompted and select a destination directory and file name when prompted.
The company certificate is exported (cer file).
4. Open the source Management Center and select **Tools > Options**.
5. Then select the **Certificates** tab and click **Create...** in the **Request** section.
6. In the **Create CCO** dialog, browse for the target company certificate you exported in the target Management Center (step 1). Make sure that it is the desired certificate.
7. Click **Create** and select a destination directory and file name for the .cco file. Confirm that you want to place a **Company Certificate Change Order**. Please note that a CCO is not linked to specific endpoints. Using a CCO any client of the source environment can be moved.
8. In the target Management Center, import the CCO created in the source Management Center.
9. On the **Tools** menu, click **Configuration Package Tool** and select the **CCOs** tab.
10. Click **Import**.

11. In the **Import CCO** dialog, select the CCO you created in the source Management Center and enter a CCO name and optionally a description. Click **OK**.
12. In the target Management Center, create a configuration package.
13. On the **Tools** menu, click **Configuration Package Tool > Standalone client packages** and add a new configuration package.
14. Select the imported CCO from the drop-down menu in the **CCO** column.
15. Specify a location under **Configuration Package output path**.
16. Click **Create Configuration package**.
The configuration package is created on the specified location.
17. Install this configuration package on all endpoints you want to move from the source environment to the target environment.

3.8.12.3 Managing Company Certificate Change Orders

In the SafeGuard Management Center, on the **Tools** menu, click **Configuration Package Tool**. All created CCOs are displayed on the **CCOs** tab.

Detailed information on the selected CCO are displayed in the lower part of the dialog.

If the CCO was created for updating the company certificate, the **Source company certificate** is the one to be renewed. If the CCO was created to move endpoints, renew the company certificate of the environment the endpoints are being moved to.

The **Destination company certificate** is the new company certificate if the CCO was created for updating the company certificate or the company certificate of the environment the endpoints are being moved to.

Below the certificate details, you can see the tasks the selected CCO can be used for.

For managing CCOs you need the right to **Manage CCOs**.

Import

When creating configuration packages, in order to select the CCO created by a different management tool to change the company certificate, you must first import it.

Clicking **Import...** opens a dialog in which you can select and name the CCO. The name you enter here is displayed on the **CCOs** tab of the **Configuration Package Tool**.

Export

Using the **Export** functionality, CCOs stored in the database can be exported and are then available as .cco files.

3.8.13 Licenses

To use SafeGuard Enterprise with the SafeGuard Management Center as a live system, you need a valid license. In the SafeGuard Enterprise Database for example, a valid license is a prerequisite for sending policies to the endpoints. The appropriate token licenses are also required for token management.

You can obtain license files from your sales partner. These files must be imported into the SafeGuard Enterprise Database after installation.

The license file contains among other information:

- The number of licenses purchased per module.
- The name of the licensee.

If the number of available licenses or the tolerance limit is exceeded, relevant warning/error messages are displayed when you start the SafeGuard Management Center.

In the **Users and Computers** area, the SafeGuard Management Center provides an overview of the license status of the installed SafeGuard Enterprise system. The license status display is available in the **Licenses** tab of the root node, for domains, OUs, container objects and workgroups. Here, security officers find detailed information about the license status. If they have sufficient rights, they can import licenses into the SafeGuard Enterprise Database.

3.8.13.1 License file

The license file you receive for importing into the SafeGuard Enterprise Database is an .XML file with a signature. The file includes the following information:

- Company name
- Additional information (for example, department, subsidiary)
- Date issued
- Number of licenses per module

- Token license information
- License expiration date
- License type (demo or full license)
- Signature with license signature certificate

3.8.13.2 Token licenses

To manage tokens or smartcards, the appropriate token licenses are required. If the appropriate licenses are not available, you cannot create policies for tokens in the SafeGuard Management Center.

3.8.13.3 Evaluation licenses

The evaluation license file can be used for evaluation. These licenses are only valid for a certain period of time and have an expiration date, but there are no functional restrictions.

These licenses must not be used for normal working operation.

After you installed the SafeGuard Management Center and completed the configuration wizard, you can import the test license you downloaded, see [Import license files \(page 175\)](#).

As long as you do not import a license file, you will be prompted to do so when you start the SafeGuard Management Center.

Test license files

When you download the product you can download a test license file as well. This evaluation license (named SafeGuard Enterprise Evaluation License) includes five licenses for each module and has a time limit of two years as of the release date of the SafeGuard Enterprise version in question.

Individual demo license files

If you need more licenses than included in the default license file for evaluation, you can also obtain a demo license customized to your specific needs. To obtain an individual demo license file, please contact your sales partner. This type of demo license is also subject to a time limit. The license is also restricted to the number of licenses per module agreed upon with your sales partner.

When you start the SafeGuard Management Center, a warning message indicates that you are using demo licenses. If the number of available licenses specified in the demo license is exceeded, or if the time limit is reached, an error message is displayed.

3.8.13.4 License status overview

To display the license status overview:

1. In the SafeGuard Management Center navigation area, click **Users and Computers**.
2. In the navigation window on the left-hand side, click the root node, the domain, the OU, the container object or the workgroup.
3. In the action area, switch to the **Licenses** tab.

The license status is displayed.

The display is divided into three areas. The upper area shows the name of the customer for whom the license has been issued, plus the issue date.

The middle area provides license details. The individual columns contain the following information:

Column	Explanation
Status (icon)	An icon shows the license status (validity, warning message, error message) for the module in question.
Feature	Shows the installed module.
Purchased Licenses	Shows the number of licenses purchased for the installed module.
Used Licenses	Shows the number of licenses used for the installed module.
Expires	Shows the license's expiration date.
Type	Shows the license type, demo or regular license.

If you display the **Licenses** tab for a domain/OU, the overview shows the status based on the computer in the relevant branch.

Beneath this overview are details of the licensed token modules.

In the lower area, a message with a status-specific background color (green = valid, yellow = warning, red = error) and an icon show the global status of the license regardless of the domain or OU selected. If this area shows a warning or error message, it also shows information on how to regain a valid license status.

The icons shown in the **Licenses** tab mean the following:



Valid license



Warning

A license for a module enters warning state if

- the license limit is exceeded.
- the license expired.



Error

A license for a module enters error state if

- the license has expired more than a month ago.

To refresh the license status overview, click **Recount used licenses**.

3.8.13.5 Import license files

Prerequisite: To import a license file into the SafeGuard Enterprise Database, a security officer needs the right "Import license file".

1. In the SafeGuard Management Center, click **Users and Computers**.
2. In the navigation window on the left-hand side, click the root node, the domain or the OU.
3. In the action area, switch to the **Licenses** tab.
4. Click the **Import license file...** button.

A window opens where you can select the license file.

5. Select the license file you want to import, and click **Open**.

The **Apply license?** dialog is displayed showing the license file contents.

6. Click **Apply license**.

The license file is imported into the SafeGuard Enterprise Database.

After you have imported the license file, the module licenses purchased are marked with the license type **regular**. Any modules which no licenses were purchased for and which the evaluation license (default license file) or individual demo licenses are used for will be marked with the license type **demo**.

Whenever a new license file is imported, only those modules that are included in that license file are affected. All other module license information is retained as it was retrieved from the database. This import functionality simplifies the evaluation of additional modules after purchase.

3.8.13.6 License exceeded

In your license file, a tolerance value has been set for exceeding the number of licenses purchased and the license validity period. If the number of available licenses per module or the validity period is exceeded, first of all a warning message is displayed. This does not impact the system's live operation and there is no restriction on functionality. You can review the license status and upgrade or renew your license. The tolerance value is usually set to 10% of the number of licenses purchased (the minimum value is 5, the maximum value is 5,000).

If the tolerance value is exceeded, an error message is displayed. In this case, functionality is restricted. The deployment of policies to the endpoints is disabled. This cannot be manually reversed in the SafeGuard Management Center. The license has to be upgraded or renewed before you can use all the functions again. Apart from disabling policy deployment, the functional restriction does not have an impact on the endpoints. Policies assigned remain active. Clients can also be uninstalled.

The following sections describe how the system behaves if licenses are exceeded and how to overcome the functional restriction.

Invalid license: Warning

If the number of available licenses is exceeded, a warning message is displayed when you start the SafeGuard Management Center.

The SafeGuard Management Center opens and displays the license status overview in the **Licenses** tab in the **Users and Computers** area.

A warning message tells you that the license is invalid. With the detailed information shown about the license file you can identify the module for which the number of available licenses has been exceeded. This license status can be changed by extending, renewing or upgrading the license.

Invalid license: Error

If the tolerance value for the number of licenses or the period of validity set in the license is exceeded, the SafeGuard Management Center displays an error message.

In the SafeGuard Management Center, the deployment of policies to endpoint computers is disabled.

An error message is displayed in the **Licenses** tab in the **Users and Computers** area.

With the detailed information shown about the license file you can identify the module for which the number of available licenses has been exceeded.

To overcome the functionality restriction, you can:

- Redistribute licenses

To make licenses available, you can uninstall the software on unused endpoints and thereby remove them from the SafeGuard Enterprise Database.

- Upgrade/renew licenses

Contact your sales partner to get your license upgraded or renewed. You will receive a new license file for importing into the SafeGuard Enterprise Database.

- Import a new license file

If you have renewed or upgraded your license, you need to import the license file into the SafeGuard Enterprise Database. This newly imported file replaces the invalid license file.

As soon as you redistribute licenses or import a valid license file, the functional restriction is reversed and the system runs normally again.

3.8.14 Tokens and smartcards

SafeGuard Enterprise provides enhanced security by supporting tokens and smartcards for authentication. Token/smartcards can store certificates, digital signatures and biometric details.

Note

Tokens and smartcards cannot be configured for macOS endpoints.

Token authentication is based on the principle of a two-stage authentication: A user has a token (ownership), but can only use the token, if they know the specific token password (knowledge). When a token or smartcard is used, users only need the token and a PIN for authentication.

From SafeGuard Enterprise's perspective, smartcards and tokens are treated in the same way. So the terms "token" and "smartcard" refer to the same thing in the product and in the help. The use of tokens and smartcards needs to be enabled in the license, see [Token licenses \(page 173\)](#).

Windows 8 and later offers a feature called *virtual smartcard*. A virtual smartcard simulates the functionality of a physical smartcard using the TPM chip as basis, but cannot be used with SafeGuard Enterprise.

Tokens are supported in SafeGuard Enterprise:

- in the SafeGuard Power-on Authentication (not applicable for Windows 8 and Windows 8.1)
- at operating system level

- to log on to the SafeGuard Management Center

When a token is issued to a user in SafeGuard Enterprise, data such as the manufacturer, type, serial number, logon data and certificates are stored in the SafeGuard Enterprise Database. Tokens are identified by the serial number and then recognized in SafeGuard Enterprise.

There are significant benefits:

- You know which tokens are in circulation and which users they are assigned to.
- You know when they were issued.
- If a token is lost, the security officer can identify it and block it. This prevents the misuse of data.
- The security officer can nevertheless use Challenge/Response to temporarily allow logon without a token, for example, if a user has forgotten the PIN.

 **Note** With SafeGuard volume-based encryption this recovery option is not supported with cryptographic token logon (Kerberos).

3.8.14.1 Token types

The term "token" refers to all technologies used and does not depend on a particular form of the device. This includes all devices that can store and transfer data for the purpose of identification and authentication, like smartcards and USB tokens.

SafeGuard Enterprise supports the following types of tokens/smartcards for authentication:

- **Non-cryptographic**

Authentication at the SafeGuard POA and Windows is based on user credentials (user ID/password) stored on the token.

- **Cryptographic - Kerberos**

Authentication at the SafeGuard POA and Windows is based on certificates stored on the token. Cryptographic tokens cannot be used for unmanaged endpoints.

Cryptographic tokens - Kerberos

With cryptographic tokens, the user is authenticated at the SafeGuard POA by the certificate stored on the token. To log on to the system, users only have to enter the token PIN.

 **Note** Cryptographic tokens cannot be used for unmanaged endpoints.

You have to provide users with fully issued tokens. For further information, see [Configure token use \(page 181\)](#).

Basic certificate requirements:

- Algorithm: RSA
- Key length: minimum 1024
- Key usage: *data encipherment* or *key encipherment*.

 **Note** In case of logon problems with a Kerberos token, neither Challenge/Response nor Local Self Help is available for logon recovery. Only the Challenge/Response procedure using Virtual Clients is supported. It enables users to regain access to encrypted volumes on their endpoints.

3.8.14.2 Components

To use tokens/smartcards with SafeGuard Enterprise, the following is required:

- Token/smartcard
- Token/smartcard reader
- Token/smartcard driver
- Token/smartcard middleware (PKCS#11 module)

USB tokens

Like smartcards, USB tokens consist of a smartcard and a smartcard reader, both units being located in a single casing. The use of USB tokens requires a USB port.

Token/smartcard readers and drivers

• Windows

On the Windows operating system level, PC/SC-compatible card readers are supported. The PC/SC interface regulates the communication between computer and smartcard. Many of these card readers are already part of the Windows installation. Smartcards require PKCS#11 compatible smartcard drivers if they are to be supported by SafeGuard Enterprise.

• SafeGuard Power-on Authentication

With SafeGuard Power-on Authentication, the PC/SC interface is supported which regulates the communication between PC and smartcard. The supported smartcard drivers are a fixed implementation and users may not add other drivers. The appropriate smartcard drivers have to be enabled by means of a policy in SafeGuard Enterprise.

The interface for smartcard readers is standardized and many card readers have a USB interface or an ExpressCard/54 interface and implement the CCID standard. In SafeGuard Enterprise, this is a prerequisite to be supported with SafeGuard Power-on Authentication. Plus, on the driver side, the PKCS#11 module has to be supported.

Supported tokens/smartcards with SafeGuard Power-on Authentication

SafeGuard Enterprise supports a wide range of smartcards/smartcard readers, USB tokens plus respective drivers and middleware with SafeGuard Power-on Authentication. With SafeGuard Enterprise, tokens/smartcards which support 2.048-bit RSA operations are supported.

As support for tokens/smartcards is enhanced from release to release, the tokens and smartcards supported in whatever is the current version of SafeGuard Enterprise are listed in the [release notes](#).

Supported middleware

The middleware in the list below is supported by the relevant PKCS#11 module. PKCS#11 is a standardized interface for connecting cryptographic tokens/smartcards to different software. Here, it is used for the communication between cryptographic token/smartcard, the smartcard reader and SafeGuard Enterprise. For more information, see [Sophos knowledge base article 132376](#).

Manufacturer	Middleware
ActivIdentity	ActivClient, ActivClient (PIV)
AET	SafeSign Identity Client
Aladdin	eToken PKI Client
A-Trust	a.sign Client
Charismatics	Smart Security Interface
Gemalto	Gemalto Access Client, Gemalto Classic Client, Gemalto .NET Card
IT Solution GmbH	IT Solution trustWare CSP+
Nexus	Nexus Personal
RSA	RSA Authentication Client 2.x, RSA Smart Card Middleware 3.x
Sertifitseerimiskeskus AS	Estonian ID Card
Siemens	CardOS API TC-FNMT
ATOS	CardOS API TC-FNMT
FNMT	Módulo PCKS#11 TC-FNMT TC-FNMT

Manufacturer	Middleware
T-Systems	NetKey 3.0
Unizeto	proCertum

Licenses

Note that the use of the respective middleware for the standard operating system requires a license agreement with the relevant manufacturer. For information on how to obtain the licenses, see [Sophos knowledge base article 116585](#).

The middleware is set in a SafeGuard Enterprise policy of the type **Specific Machine Settings** under **Custom PKCS#11 Settings** in the field **PKCS#11 Module for Windows** or **PKCS#11 Module for Power-on Authentication**. The relevant configuration package must also be installed on the computer on which the SafeGuard Management Center is running.

3.8.14.3 Configure token use

Carry out these steps if you want to provide tokens to the following users for authentication:

- Users of managed endpoints
- Security officers of the SafeGuard Management Center

1. Initialize empty tokens.

For further information, see [Initialize a token \(page 182\)](#).

2. Install the middleware.

For further information, see [Install middleware \(page 182\)](#).

3. Activate the middleware.

For further information, see [Activate middleware \(page 183\)](#).

4. Issue tokens for users and security officers.

For further information, see [Issuing a token \(page 183\)](#).

5. Configure the logon mode.

For further information, see [Configuring logon mode \(page 186\)](#).

6. Configure further token settings, for example syntax rules for PINs.

For further information, see [Managing PINs \(page 191\)](#) and [Managing tokens and smartcards \(page 192\)](#).

7. Assign certificates and keys to tokens/users.

For further information, see [Assigning certificates \(page 187\)](#).

You can also use tokens that have data from a different application for authentication, provided that there is enough storage space for the certificates and logon information on them.

For easy token administration, SafeGuard Enterprise offers the following features:

- Display and filter token information
- Initialize, change, reset and block PINs
- Read and delete token data
- Block tokens

 **Note** To issue and manage tokens or modify data on issued tokens you need **Full access** rights to the relevant users. The **Issued Tokens** view only shows tokens for users for whom you have **Read only** or **Full access** rights.

3.8.14.4 Preparing for token use

To prepare for token/smartcard support in SafeGuard Enterprise:

- Initialize empty tokens.
- Install the middleware.
- Activate the middleware.

Initialize a token

Before an "empty", unformatted token can be used, it needs to be prepared for use (initialized) according to the instructions provided by the token manufacturer. When it is initialized, basic information, for example the standard PIN, is written to it. This is done with the token manufacturer's initialization software.

For further information, refer to the token manufacturer concerned.

Install middleware

Install the correct middleware, both on the computer with SafeGuard Management Center installed as well as on the relevant endpoint, if not already done. For supported middleware, see [Supported middleware \(page 180\)](#).

Restart the computers where you installed the new middleware.

 **Note** If you install **Gemalto .NET Card** or **Nexus Personal** middleware, you also need to add their installation path to the PATH environment variable of your computer's **System Properties**.

- Default installation path for **Gemalto .NET Card**: C:\Program Files\Gemalto\PKCS11 for .NET V2 smart cards
- Default installation path for **Nexus Personal**: C:\Program Files\Personal\bin

Activate middleware

You need to assign the correct middleware in form of the PKCS#11 module by defining a policy in the SafeGuard Management Center. You should do this both for the computer which the SafeGuard Management Center is running on and for the endpoint. Only then can SafeGuard Enterprise communicate with the token. You can define the setting for PKCS#11 module, using a policy, as follows.

Prerequisite: The middleware is installed on the relevant computer and the token has been initialized. The SafeGuard Enterprise Client configuration package must also be installed on the computer on which the SafeGuard Management Center is running.

1. In the SafeGuard Management Center, click **Policies**.
2. Create a new policy of the type **Specific Machine Settings** or select an existing policy of this type.
3. In the work area on the right-hand side, select the appropriate middleware under **Token support settings > Module Name**. Save the settings.
4. Assign the policy.

SafeGuard Enterprise can now communicate with the token.

3.8.14.5 Issuing a token

When a token is issued in SafeGuard Enterprise, data which is used for authentication is written on the token. This data consists of credentials and certificates.

In SafeGuard Enterprise, tokens can be issued for these user roles:

- Tokens for end users of managed endpoints
- Tokens for security officers (SO)

Both user and security officers (SO) can access the token. The user is the one who should use the token. Only the user can access private objects and keys. The SO can only access public objects, but can reset the user's PIN.

Issue a token or smartcard to a user

Prerequisites:

- The token must be initialized and the relevant PKCS#11 module must be activated.
- The SafeGuard Enterprise Client configuration package must also be installed on the computer on which the SafeGuard Management Center is running.
- You need **Full access** rights for the relevant user.

1. In the SafeGuard Management Center, click **Users and Computers**.
2. Connect the token to the USB interface. SafeGuard Enterprise reads in the token.
3. Select the user for whom the token is to be issued, and open the **Token Data** tab in the work area on the right-hand side.
4. In the **Token Data** tab, do the following:
 - a. Select the **User ID** and **Domain** of the relevant user and enter your Windows **Password**.
 - b. Click **Issue Token**.

The **Issue Token** dialog is displayed.

5. Select the appropriate slot for the token from the **Available slots** drop-down list.
6. Issue a new **User PIN** and repeat the entry.
7. Under **SO PIN**, enter the standard PUK received from the manufacturer or the PIN issued when the token was initialized.

 **Note** If you only fill in the **User PIN (required)** field, the user PIN must match the PIN which was issued when the token was initialized. In this case, you do not have to repeat the user PIN and enter an SO PIN.

8. Click **Issue token now**.

The token is issued, the logon information written on the token and the token information saved in the SafeGuard Enterprise Database. You can display the data in the **Token** area in the **Token Information** tab.

Issue a token or smartcard to a security officer

When SafeGuard Enterprise is installed for the first time, the first security officer (SO) can issue a token for themselves and specify the logon mode. For all other security officers, tokens are issued in the SafeGuard Management Center.

Prerequisite:

- The token must be initialized and the relevant PKCS#11 module must be activated.
- You need the rights to make entries for the SO.

1. In the SafeGuard Management Center, click **Security Officers**.
2. Connect the token to the USB interface. SafeGuard Enterprise reads in the token.
3. In the navigation window on the left, mark **Security Officer** and select **New > New security officer** from the context menu.

The **New security officer** dialog is displayed.

4. With the **Token logon** field, specify the type of logon for the SO:

- To enable the SO to authenticate either with or without a token, select **Optional**.
- To make token logon mandatory for the SO, select **Mandatory**.

With this setting, the private key remains on the token. The token must always be plugged in, or the system will need to be restarted.

5. Next you specify the SO certificate.

- To create a new certificate, click the **Create** button next to the **Certificate** drop-down list.

Enter the password for the certificate twice and click **OK** to confirm it.

Specify the location for saving the certificate.

- To import certificates, click the **Import** next to the **Certificate** drop-down list and open the relevant certificate file.

Searching is first done in a certificate file, then on the token. The certificates may remain in whatever the storage location is.

6. Under **Roles**, activate the roles that are to be assigned to the SO.

7. Confirm the entries with **OK**.

The SO is created, the token is issued, the logon data is written on the token (depending on the setting), and the token information is saved in the SafeGuard Enterprise Database. You can display the data in the **Token** area in the **Token Information** tab.

3.8.14.6 Configuring logon mode

There are two ways for end users of logging on with a token. A combination of both logon methods is possible.

- Logging on with user ID/password
- Logging on with token

When logging on with token/smartcard, you can either select the non-cryptographic method or the Kerberos (cryptographic) method.

As a security officer, you specify the logon mode to be used in a policy of the type **Authentication**.

If you select the token logon option **Kerberos**:

- You need to issue a certificate in a PKI and store it on the token. This certificate is imported as a user certificate into the SafeGuard Enterprise Database. If an automatically generated certificate already exists in the database, it is replaced by the imported certificate.

Enable SafeGuard POA autologon with default token PINs

A default token PIN that is distributed by policy enables automatic user logon at the SafeGuard Power-on Authentication. This avoids the need to issue each single token separately and enables users to automatically log on at the SafeGuard Power-on Authentication without any user interaction.

When a token is used at logon and a default PIN is assigned to the computer, the user is passed through at the SafeGuard Power-on Authentication without having to enter a PIN.

As a security officer you can set the specific PIN in a policy of the type **Authentication** and assign it to different computers or computer groups, for example to all computers residing in the same location.

To enable autologon with a default token PIN:

1. In the SafeGuard Management Center, click **Policies**.
2. Select a policy of the type **Authentication**.
3. Under **Logon Options** in **Logon mode**, select **Token**.
4. In **PIN used for autologon with token**, specify the default PIN to be used for autologon. PIN rules do not need to be observed in this case.

 **Note** This setting is only available if you select **Token** as possible **Logon Mode**.

5. In **Pass through to Windows** set **Disable pass-through to Windows**. If you do not select this setting when a default PIN is specified, you will not be able to save the policy.

If you want to enable the **Pass through to Windows** option, you can later create another policy of the type **Authentication** with this option enabled and assign it to the same computer group, so that the RSOP has both policies active.

6. Optionally specify further token settings.

7. Save your settings and assign the policy to the relevant computers or computer groups.

If the autologon on the endpoint has been successful, Windows is started.

If the autologon on the endpoint has failed, the user is prompted to enter the token PIN at the SafeGuard Power-on Authentication.

3.8.14.7 Assigning certificates

Not only logon information but also certificates can be written to a token. Just the private part of the certificate (.p12 file) can be saved on the token. However, users then can only log on with the token. We recommend that you use PKI certificates.

You can assign authentication data to tokens as follows:

- by generating certificates directly on the token
- by assigning data which is already on the token
- by importing certificates from a file

 **Note** CA certificates cannot be obtained from a token and stored in the database or certificate store. If you use CA certificates, these need to be available as files and not just on a token. This also applies to CRLs (Certificate Revocation List). Moreover, the CA certificates must match the CRL before users can log on to the computers concerned. Check that the CA and corresponding CRL are correct. SafeGuard Enterprise does not carry out this check! SafeGuard Enterprise can then only communicate with expired certificates if old and new keys are present on the same card.

Generate certificates from tokens

To generate certificates from tokens, you need **Full access** rights for the relevant user.

You can generate new certificates straight from the token if, for example, there is no certificate structure present.

 **Note**

If only the private part of the certificate is written on to the token, the user can only access their private key with the token. The private key then only resides on the token. If the token is lost, the private key can no longer be accessed.

Prerequisite: The token is issued.

1. In the SafeGuard Management Center, click **Users and Computers**.
2. Plug the token into the USB interface.

SafeGuard Enterprise reads in the token.

3. Mark the user for whom a certificate is to be generated, and open the **Certificate** tab in the work area on the right-hand side.
4. Click **Generate and assign certificate by token**. Note that the length of the key must match the size of the token.
5. Select the slot and enter the token PIN.
6. Click **Create**.

The token generates the certificate and assigns it to the user.

Assign token certificates to a user

Prerequisites:

- The token is issued.
- You have **Full access** rights for the relevant user.

To assign a certificate available on the token to a user:

1. In the SafeGuard Management Center, click **Users and Computers**.
2. Plug the token into the USB interface.

SafeGuard Enterprise reads in the token.

3. Select the user you want to assign a certificate to, and open the **Certificate** tab in the work area on the right-hand side.

4. Click the **Assign a certificate from a token** icon on the SafeGuard Management Center toolbar.
5. Select the relevant certificate from the list and enter the token's PIN.
6. Click **OK**.

The certificate is assigned to the user. A user can only have one certificate assigned.

Change a user's certificate

You can change or renew certificates required for logon by assigning a new certificate in the SafeGuard Management Center. The certificate is assigned as a standby certificate alongside the existing certificate. By logging on with the new certificate, the user changes the certificate on the endpoint.

Note

If users have lost their tokens or tokens have been compromised, do not exchange tokens by assigning new certificates as described here. Otherwise problems may occur. For example, the old token certificate may still be valid for Windows logon. As long as the old certificate is still valid, logon to Windows is still possible and the computer can be unlocked. Instead, block the token to prevent logon.

Standby certificates can be used in the following cases:

- Change (cryptographic) token generated certificates.
- Switch from auto-generated certificates to token-generated certificates.
- Switch from user name/password authentication to cryptographic token (Kerberos) authentication.

Prerequisites:

- The new token is issued.
- Only one certificate is assigned to the user.
- You have **Full access** rights for the relevant user.

To change a user's certificate for token logon:

1. In the SafeGuard Management Center, click **Users and Computers**.
2. Plug the token into the USB interface.

SafeGuard Enterprise reads in the token.

3. Select the user for whom you want to change the certificate and open the **Certificate** tab in the work area on the right-hand side.
4. On the toolbar, click the appropriate icon for the action you want to perform.
5. Select the relevant certificate and enter the token's PIN.
6. Click **OK**.
7. Provide the user with the new token.

The certificate is assigned to the user as a standby certificate. This is indicated by a tick in the **Standby** column of the user's **Certificates** tab.

After synchronization between the endpoint and the SafeGuard Enterprise Server, the status dialog on the endpoint indicates that it is **Ready for certificate change**.

The user now has to initiate a certificate change on the endpoint computer. For further information, see the *SafeGuard Enterprise user help*.

After the user has changed the certificate on the endpoint the certificate is also renewed on the SafeGuard Enterprise Server during the next synchronization. This removes the old token from the user's **Certificates** tab in the SafeGuard Management Center. The new token becomes the standard token for the user.

 **Note** In the SafeGuard Management Center, both certificates can be deleted separately. If only a standby certificate is available, the next certificate is assigned as the standard certificate.

Import certificate from a file onto the token

Prerequisite: The token is issued.

You need to select this procedure for a token with Kerberos support for managed endpoints. The certificate must be recognized by SafeGuard Enterprise and added to the token. If there is already an auto-generated certificate, the imported certificate will overwrite it.

To add the private part of the certificate (.p12 file) from a file to the token:

1. In the SafeGuard Management Center, click **Tokens**.
2. Plug the token into the USB interface.

SafeGuard Enterprise reads in the token.

3. Mark the token to which you want to add the private part of the certificate and, in the work area on the right, open the **Logon Information & Certificates** tab.
4. Click the **P12 to token** icon in the SafeGuard Management Center toolbar.
5. Select the relevant certificate file.
6. Enter the token PIN and the password for the .p12 file and click **OK** to confirm.

The private part of the certificate is added to the token. Now you need to assign it to a user, see [Assign token certificates to a user \(page 188\)](#). Users can then only log on with this token.

3.8.14.8 Managing PINs

As a security officer, you can change both the user PIN and the SO PIN, and also force the user PIN to be changed. This is usually required when a token is first issued. You can also initialize PINs (issue them as new and block them).

To initialize, change and block PINs, you need **Full access** rights for the relevant users.

You can use policies to specify other PIN options for the endpoint.

 **Note** When you change a PIN, note that some token manufacturers specify their own PIN rules which may contradict SafeGuard Enterprise PIN rules. So it may not be possible to change a PIN in the way you want, even if it complies with the SafeGuard Enterprise PIN rules. You should always refer to the token manufacturer's PIN rules. These are displayed in the **Token** area under **Token Information** in the SafeGuard Management Center.

PINs are managed in the SafeGuard Management Center under **Tokens**. The token is plugged in and marked in the navigation window on the left.

Initialize user PIN

Prerequisites:

- The SO PIN must be known.
- You need **Full access** rights for the relevant user.

1. In the SafeGuard Management Center toolbar, click the **Initialize user PIN** icon.
2. Enter the SO PIN.
3. Enter the new user PIN, repeat the entry and click **OK** to confirm.

The user PIN is initialized.

Change an SO PIN

Prerequisite: The previous SO PIN must be known.

1. In the SafeGuard Management Center toolbar, click the **Change SO PIN** icon.
2. Enter the old SO PIN.
3. Enter the new SO PIN, repeat the entry and click **OK**.

The SO PIN has been changed.

Change a user PIN

Prerequisite:

- The user PIN must be known.
- You need **Full access** rights for the relevant user.

1. In the SafeGuard Management Center toolbar, click the **Change user PIN** icon.
2. Enter the old and the new user PIN, repeat the new user PIN, and click **OK**.

The user PIN is changed. If you have changed the PIN for another user, inform them about the change.

Force PIN change

To force a PIN change, you need **Full access** rights for the relevant user.

In the SafeGuard Management Center toolbar, click the **Force PIN change** icon.

The next time the user logs on with the token, they have to change their user PIN.

PIN history

The PIN history can be deleted. To do this, click the **Delete PIN history** icon in the SafeGuard Management Center toolbar.

3.8.14.9 Managing tokens and smartcards

In the **Tokens** area of the SafeGuard Management Center, the security officer can:

- Get an overview of tokens and certificates that have been issued.
- Filter overviews.
- Block tokens for authentication

- Read or delete the data on a token.

Display token/smartcard information

As a security officer, you can display information about all or individual tokens that have been issued. You can also filter overviews.

Prerequisite: The token must be plugged in.

1. In the SafeGuard Management Center, click **Tokens**.
2. To display information about an individual token, select the relevant token in the navigation area under **Token Slots**.

The manufacturer, type, serial number, hardware details and PIN rules are displayed under **Token Information**. You can also see which user the token is assigned to.

 **Note** Under **Token Slots**, issued tokens are displayed regardless of your access rights to the relevant users, so you can see, if the token is in use or not. If you have no or **Read only** access rights to the assigned user, all token data in the **Token Information** and **Credentials and Certificates** tabs are greyed out and you cannot manage this token.

3. To display an overview on tokens, select **Issued Tokens**. You can display all the tokens that have been issued or filter the overview by user.

The token's serial number, the assigned users and the issue date are displayed. You can also see if the token is blocked.

 **Note** The **Issued Tokens** view shows the tokens for all users you have **Read only** or **Full access** rights for.

Block token or smartcard

As a security officer you can block tokens. This is for example useful if a token has been lost.

To block a token, you need **Full access** rights for the relevant user.

1. In the SafeGuard Management Center, click **Tokens**.
2. In the navigation area on the left, select **Issued Tokens** on the left of the navigation area.
3. Select the token to be blocked and click the **Block token** icon in the SafeGuard Management Center toolbar.

The token is blocked for authentication and the assigned user can no longer use it to log on. The token can only be unblocked with the SO PIN.

Delete token/smartcard information

As a security officer, you can delete the information that has been written on the token by SafeGuard Enterprise.

Prerequisite:

- The token must be plugged in.
- You need **Full access rights** for the relevant user.

1. In the SafeGuard Management Center, click **Tokens**.
2. In the navigation area on the left, select the token concerned under **Token Slots**.
3. In the SafeGuard Management Center toolbar, click the **Wipe token** icon.
4. Enter the SO Pin that was assigned to the token and click **OK** to confirm.

All data managed by SafeGuard Enterprise is deleted. Certificates remain on the token.

The user PIN is reset to 1234.

Deleted tokens are thus automatically deleted from the list of issued tokens.

Read token/smartcard information

As a security officer you can read the data on the token by using the user PIN.

Prerequisite:

- The token must be plugged in. The security officer must know the PIN. Or it must be initialized, see [Initialize user PIN \(page 191\)](#).
- You need **Read only** or **Full access** rights for the relevant user.

1. In the SafeGuard Management Center, click **Tokens**.
2. On the left of the navigation area select the relevant token under **Token Slots** and select the **Credentials & Certificates** tab.
3. Click the **Get user credentials** icon and enter the user PIN for the token.

The data on the token is displayed.

3.8.15 Scheduling tasks

The SafeGuard Management Center offers the **Task Scheduler** to create and schedule periodic tasks based on scripts. The tasks are automatically run by a service on the SafeGuard Enterprise Server to execute the scripts specified.

Periodic tasks are for example useful for

- automatic synchronization between Active Directory and SafeGuard Enterprise.
- automatic deletion of event logs.

For these two procedures, predefined script templates are available with SafeGuard Enterprise. You can use these scripts as they are or modify them according to your requirements. For further information, [Predefined scripts for periodic tasks \(page 202\)](#).

As a security officer with the required rights, you can specify scripts, rules and intervals for tasks in the **Task Scheduler**.

 **Note** Make sure that the appropriate SQL permissions are set for the account that is used to run the SafeGuard Enterprise **Task Scheduler**. For more information, see [Sophos knowledge base article 113582](#).

 **Note** The API cannot process more than one task at the same time. If you use more than one account per task, this will lead to database access violations.

3.8.15.1 Create a new task

To create tasks in the **Task Scheduler**, you need the security officer rights **Use task scheduler** and **Manage tasks**.

1. In the menu bar of the SafeGuard Management Center, select **Tools > Task Scheduler**.

The **Task Scheduler** dialog is displayed.

2. Click the **Create...** button.

The **New task** dialog is displayed.

3. In the **Name** field, enter a unique task name.

If the task name is not unique, a warning is displayed when you click **OK** to save the task.

4. In the drop-down list of the **SGN Server** field, select the server the task should run on.

The drop-down list only shows servers for which scripting is allowed. You allow scripting for a specific server when you register it in the **Configuration Package Tool** in the SafeGuard Management Center.

If you select **None**, the task is not executed.

5. Click the **Import...** button next to the **Script** field.

The **Select script file to import** dialog is displayed.

 **Note** Two predefined scripts are available in the Script Templates directory of your SafeGuard Management Center installation. The **Select script file to import** dialog automatically shows this directory. For further information, see [Predefined scripts for periodic tasks \(page 202\)](#).

In the **Task Scheduler**, you can import, export and edit scripts. For further information, see [Working with scripts in the Task Scheduler \(page 200\)](#).

6. Select the script you want to run with the task and click **OK**.

If the script selected is empty, the **OK** button in the dialog remains disabled and a warning symbol is displayed.

7. In the **Start Time** field, specify when the task should be run on the selected server.

The start time displayed is rendered using the local time of the computer on which the SafeGuard Management Center is running. Internally, the start time is stored as Coordinated Universal Time (UTC). This allows tasks to be executed at the same moment, even if servers are in different time zones. All servers use the current time of the database server to determine when to start tasks. To allow better monitoring of tasks, the database reference time is displayed in the **Task Scheduler** dialog.

8. Under **Recurrence**, specify how often the task should be run on the selected server.

- To run the task once, select **One time** and specify the required **Date**.
- To run the task daily, select **Daily** followed by **Every day (including Saturday and Sunday)** or **Every weekday (Monday - Friday)**.
- To run the task weekly, select **Weekly** and specify the required day of the week.
- To run the task monthly, select **Monthly** and specify the required day of the month in a range from 1 to 31. To run the task at the end of each month, select **Last** from the drop-down list.

After you have filled in all mandatory fields, the **OK** button becomes available.

9. Click **OK.**

The task is saved in the database and displayed in the **Task Scheduler** overview. It is run on the selected server according to the schedule specified.

For logged events, see [Auditing \(page 204\)](#).

3.8.15.2 The Task Scheduler overview display

After you have created tasks to be run on a SafeGuard Enterprise Server, they are displayed in the **Task Scheduler** dialog you open by selecting **Tools > Task Scheduler**.

This dialog shows the following columns for each task:

Column	Description
Task Name	Shows the unique task name.
SGN Server	Indicates on which server the task is executed.
Schedule	Shows the schedule specified for the task with recurrence and time.
Next Run Time	Shows the next time the task will be executed (date and time). If there are no more run times specified for the task, this column shows None .
Last Run Time	Shows the last time the task was executed (date and time). If it has not been executed yet, this column shows None .
Last Run Result	Shows the result of the last task run: <ul style="list-style-type: none"> • Success The task's script was executed successfully. • Failure Execution of the task has failed. An error number is shown, if available. • Running The script is running. • Insufficient Rights

Column	Description
	<p>The task has failed due to insufficient rights for script execution.</p> <ul style="list-style-type: none"> • Aborted The execution of the task was aborted because the execution time exceeded 24 hours. • Lost control Control of the task's script execution was lost, for example because the SGN scheduler service was stopped. • Script is corrupt The script to be executed is corrupt. • The script was deleted in the meantime While the task was queued for execution, the corresponding script was removed from the SafeGuard Enterprise Database. • Runtime errors A runtime error was detected during the processing of the scheduler service.

Under the columns, the following buttons are displayed:

Button	Description
Create...	Click this button to create a new task.
Delete	Click this button to delete a selected task.
Properties	Click this button to display the <task name> properties dialog for a selected task. In this dialog, you can edit the task or import, export and edit scripts.
Refresh	Click this button to refresh the task list in the Task Scheduler dialog. If another user has added or deleted tasks in the meantime, the task list is updated.

All servers use the current time of the database server to determine when to start tasks. Therefore, to allow better monitoring of tasks, the time of the database server is displayed here. It is rendered using the local time zone of the computer on which the SafeGuard Management Center runs.

3.8.15.3 Edit tasks

To edit tasks in the **Task Scheduler**, you need the security officer rights **Use task scheduler** and **Manage tasks**.

1. In the menu bar of the SafeGuard Management Center, select **Tools > Task Scheduler**.

The **Task Scheduler** dialog is displayed showing an overview on the scheduled tasks.

2. Select the required task and click the **Properties** button.

The **<task name> properties** dialog is displayed showing the task properties.

3. Make the required changes.

 **Note** The task name must be unique. If you change the name to an existing task name, an error message is displayed.

4. Click **OK**.

The changes become effective.

3.8.15.4 Delete tasks

To delete tasks from the **Task Scheduler**, you need the security officer rights **Use task scheduler** and **Manage tasks**.

1. In the menu bar of the SafeGuard Management Center, select **Tools > Task Scheduler**.

The **Task Scheduler** dialog is displayed showing an overview of the scheduled tasks.

2. Select the required task.

The **Delete** button becomes available.

3. Click the **Delete** button and confirm that you want to delete the task.

The task is removed from the **Task Scheduler** overview dialog and will no longer be run on the SafeGuard Enterprise Server.

 **Note** If the task has been started in the meantime, it is removed from the **Task Scheduler** overview dialog, but it will still be completed.

3.8.15.5 Working with scripts in the Task Scheduler

With the **Task Scheduler** you can import, edit and export scripts. To work with scripts in the **Task Scheduler**, you need the security officer rights **Use Task scheduler** and **Manage tasks**.

Import scripts

To specify a script to be executed by a task, the script must be imported. You can import the script when you first create the task. You can also import scripts for existing tasks.

1. In the menu bar of the SafeGuard Management Center, select **Tools > Task Scheduler**.

The **Task Scheduler** dialog is displayed showing an overview on the scheduled tasks.

2. Select the required task and click the **Properties** button.

The **<task name> properties** dialog is displayed showing the task properties.

3. Click the **Import...** button next to the **Script** field.

The **Select script file to import** dialog is displayed.

 **Note** Two predefined scripts are available in the Script Templates directory of your SafeGuard Management Center installation. The **Select script file to import** dialog automatically shows this directory. For further information, see [Predefined scripts for periodic tasks \(page 202\)](#).

4. Select the script you want to import and click **OK**.

The script name is displayed in the **Script** field.

5. Click **OK**.

If the script has already been imported, you are prompted to confirm that you want to overwrite the old script.

If the size of the file to be imported exceeds 10 MB, an error message is displayed and the import process is rejected.

The script is saved in the database.

Edit scripts

1. In the menu bar of the SafeGuard Management Center, select **Tools > Task Scheduler**.

The **Task Scheduler** dialog is displayed showing an overview on the scheduled tasks.

2. Select the required task and click the **Properties** button.

The **<task name> properties** dialog is displayed showing the task properties.

3. Click the **Edit** drop-down button next to the **Script** field.

The drop-down list shows all editors available for editing the script.

4. Select the editor you want to use.

The script is opened in the selected editor.

5. Make your changes and save them.

The editor is closed and the **<task name> properties** dialog is displayed again.

6. Click **OK**.

The changed script is saved in the database.

Export scripts

1. In the menu bar of the SafeGuard Management Center, select **Tools > Task Scheduler**.

The **Task Scheduler** dialog is displayed showing an overview on the scheduled tasks.

2. Select the required task and click the **Properties** button.

The **<task name> properties** dialog is displayed showing the task properties.

3. Click the **Export...** button besides the **Script** field.

A **Save as** dialog is displayed.

4. Select the file location for saving the script and click **Save**.

The script is saved to the specified file location.

Predefined scripts for periodic tasks

The following predefined scripts are available with SafeGuard Enterprise:

- ActiveDirectorySynchronization.vbs

You can use this script for automatic synchronization between Active Directory and SafeGuard Enterprise.

- EventLogDeletion.vbs

You can use this script for automatic event log deletion.

The scripts are installed automatically in the Script Templates subfolder of the SafeGuard Management Center installation.

To use these scripts in periodic tasks, import them into the **Task Scheduler** and make the necessary parameter changes before you use them.

Predefined script for Active Directory synchronization

You can import an existing organizational structure into the SafeGuard Enterprise Database from an Active Directory. For further information, see [Synchronize the organizational structure \(page 149\)](#).

After you have imported the directory structure, you can schedule a periodic task for automatic synchronization between the Active Directory and SafeGuard Enterprise. For this task, you can use the predefined script ActiveDirectorySynchronization.vbs.

The script synchronizes all existing containers in the SafeGuard Enterprise Database with an Active Directory.

Before you use the script in a periodic task, you can edit the following parameters:

Parameter	Description
logFileName	Specify a path for the script log file. This parameter is mandatory. If it is empty or invalid, synchronization does not work and an error message is displayed. By default,

Parameter	Description
	this parameter is empty. If a log file already exists, new logs are appended to the end of the file.
synchronizeMembership	Set this parameter to 1 to also synchronize memberships. If this parameter is set to 0, memberships are not synchronized. The default setting is 1.
synchronizeAccountState	Set this parameter to 1 to also synchronize the user enabled state. If this parameter is set to 0, the user enabled state is only synchronized at first synchronization. The default setting is 0.

Note

Make sure that you have the necessary access rights for Active directory synchronization and that the appropriate SQL permissions are set for the account that is used to run the SafeGuard Enterprise **Task Scheduler**. For more information, see [Security officer access rights and Active Directory import \(page 147\)](#). For information on how to set the Active Directory access rights, see [Sophos knowledge base article 107979](#). For information on how to set the SQL permissions, see [Sophos knowledge base article 113582](#).

Once the rights are set correctly, apply the changes and restart the service: Switch to the server hosting the SafeGuard Enterprise web page. Open the **Services** interface by clicking **Start > Run > Services.msc**. Right-click **SafeGuard ® Scheduler Service** and click **All Tasks > Restart**.

We recommended that you synchronize the Active Directory in a timely moderate interval, maximum twice a day so that server performance is not significantly decreased. New objects will be displayed in the SafeGuard Management Center under .Auto registered between these intervals where they can be managed just as normal.

Predefined script for automatic event log deletion

Events logged in the SafeGuard Enterprise Database are stored in the EVENT table. For further information on logging, see [Reports \(page 208\)](#).

With the **Task Scheduler**, you can create a periodic task for automatic event log deletion. For this task, you can use the predefined script EventLogDeletion.vbs.

The script deletes events from the EVENT table. If you specify the relevant parameter, it also moves events to the backup log table EVENT_BACKUP leaving a defined number of latest events in the EVENT table.

Before you use the script in a periodic task, you can edit the following parameters:

Parameter	Description
maxDuration	With this parameter, you specify how long (in days) events should be kept in the EVENT table. The default

Parameter	Description
	is 0. If this parameter is set to 0, there is no time limit for events kept in the EVENT table.
maxCount	With this parameter, you specify how many events should remain in the EVENT table. The default is 5000. If this parameter is set to 0, there is no limit for the number of events to be kept in the EVENT table.
keepBackup	With this parameter, you specify whether deleted events should be backed up in the EVENT_BACKUP table. The default is 0. If this parameter is set to 0, events are not backed up. Set this parameter to 1 to create a backup of deleted events.

Note

If you use the script to move events from the EVENT table to the backup log table, event connection no longer applies. To activate event connection while also using the stored procedure for event cleanup does not make sense. For further information, see [Connection of logged events \(page 214\)](#).

3.8.15.6 Restrictions concerning registered servers

When you register servers in the **Configuration Package Tool** in the SafeGuard Management Center, it is possible to register more than one server template with the same machine certificate. But you can only install one template at a time on the real machine.

If the **Scripting allowed** check box is selected for both servers, the **Task Scheduler** displays both servers for selection in the **SGN Server** drop-down list of the **New task** dialog and the **<task name> properties** dialog. The **Task Scheduler** cannot determine which of the two templates was installed on the machine.

To avoid this, do not select the check box **Scripting allowed** for templates that are not installed on the server. Also, avoid duplicate templates with the same machine certificate.

For further information on registering servers, see [Registering and configuring SafeGuard Enterprise Server \(page 51\)](#).

3.8.16 Auditing

Log events for BitLocker

Events reported by the BitLocker Client are logged, just as for any other SafeGuard Enterprise Client. It is not especially mentioned that the event refers to a BitLocker Client. The events reported are the same as for any SafeGuard Enterprise client.

Log event for recovery with BitLocker recovery key ID

An event is logged when the BitLocker recovery key ID is displayed to an officer (event 2088).

Log events for asynchronous encryption

Events are logged when:

- Asynchronous encryption encrypted a file (event 3018)
- Asynchronous encryption decrypted a file (event 3019)

You can view a list of these events in the SafeGuard Management Center under **Reports** in the Event viewer.

Log events for unconfirmed users

Events are logged when:

- users are added to the **Unconfirmed Users** group (event 2801)
- users have been confirmed successfully (event 2800)
- the **Automatically confirm users that cannot be authenticated against Active Directory** option is activated (event 2802)
- the **Automatically confirm users that cannot be authenticated against Active Directory** option is deactivated (event 2803)
- users have been confirmed automatically (event 2804)

You can view a list of these events in the SafeGuard Management Center under **Reports** in the Event viewer.

Log events for deletion of domains, OU nodes and workgroups

Events are logged when:

- the **Prevent deletion of domains, OU nodes and workgroups** option is activated. The message shows the security officer who activated it (event 2805).

- the **Prevent deletion of domains, OU nodes and workgroups** option is deactivated. The message shows the security officer who deactivated it (event 2806).

You can view a list of these events in the SafeGuard Management Center under **Reports** in the Event viewer.

Log events for users, computers or workgroups

Successful/unsuccessful registrations of users, computers or workgroups are logged. You can view a list of these events in the SafeGuard Management Center under **Reports** in the Event viewer.

Log Events for disabling/enabling policy deployment

Events are logged when:

- policy deployment is disabled by a security officer. The message shows the security officer who disabled policy deployment (event 2770).
- policy deployment is enabled by a security officer. The message shows the security officer who enabled policy deployment (event 2771).
- policy deployment is disabled by license management (event 2773). Possible reasons:
 - invalid licenses
 - expired license
 - exceeded licenses
- Policy deployment is enabled by license management (event 2771)

You can view a list of these events in the SafeGuard Management Center under **Reports** in the Event viewer.

Log events for service account lists

Actions performed regarding service account lists are reported by the following log events:

SafeGuard Management Center

- Service account list <name> created
- Service account list <name> modified
- Service account list <name> deleted

SafeGuard Enterprise protected endpoint

- Windows user <domain/user name> logged on at <timestamp> to machine <domain/workstation name> as SGN service account.
- New service account list <name> imported.

- Service account list <name> deleted.

Log events for Task Scheduler

Events concerning task execution can be logged to provide useful information, for example for troubleshooting. You can define the following events to be logged:

- Scheduler task executed successfully
- Scheduler task failed
- Scheduler service thread stopped due to an exception.

The events include the script console output to facilitate troubleshooting.

For further information on logging, see [Reports \(page 208\)](#).

Track files accessed in cloud storage

You can track files accessed in cloud storage by using the **Reports** function of the SafeGuard Management Center. Files accessed can be tracked regardless of any encryption policies applied to them.

In a policy of the type **Logging** you can define the following:

- To log an event when a file or directory is created on a removable media device.
- To log an event when a file or directory is renamed on a removable media device.
- To log an event when a file or directory is deleted from a removable media device.

For further information, see [File access report for removable media and cloud storage \(page 213\)](#).

Track files accessed on removable media

You can track files accessed on removable media by using the **Reports** function of the SafeGuard Management Center. Files accessed can be tracked regardless of any encryption policy applying to files on removable media.

In a policy of the type **Logging** you can define the following:

- An event to be logged when a file or directory is created on a removable media device.
- An event to be logged when a file or directory is renamed on a removable media device.
- An event to be logged when a file or directory is deleted from a removable media device.

For further information, see [File access report for removable media and cloud storage \(page 213\)](#).

3.8.16.1 Reports

Recording security-related incidents is a prerequisite for detailed system analysis. The events logged facilitate the exact tracking of processes on a specific workstation or within a network. By logging events, you can for example verify security breaches committed by third parties. By using the logging functionality, administrators and security officers can also detect errors in granting user rights and correct them.

SafeGuard Enterprise logs all endpoint activities and status information as well as administrator actions and security-related events and saves them centrally. The logging functionality records events triggered by installed SafeGuard products. The type of logs is defined in policies of the type **Logging**. This is also where you specify the output and saving location for the logged events: the Windows Event Log of the endpoint or the SafeGuard Enterprise Database.

As a security officer with the necessary rights, you can view, print and archive status information and log reports displayed in the SafeGuard Management Center. The SafeGuard Management Center offers comprehensive sorting and filter functions which are very helpful when selecting the relevant events from the information available.

Automated analyses of the log database, for example with Crystal Reports or Microsoft System Center Operations Manager, are also possible. SafeGuard Enterprise protects the log entries against unauthorized manipulation using signatures on the client and on the server side.

Depending on the logging policy, events of the following categories can be logged:

- Authentication
- Administration
- System
- Encryption
- Client
- Access control
- For **SafeGuard Data Exchange**, you can track files accessed on removable media by logging the relevant events. For further information on this report type, see [File access report for removable media and cloud storage \(page 213\)](#).
- For **SafeGuard Cloud Storage**, you can track files accessed in your cloud storage by logging the relevant events. For further information on this report type, see [File access report for removable media and cloud storage \(page 213\)](#).

Prerequisite

Events are handled by the SafeGuard Enterprise Server. If you want to activate reports on computers on which no SafeGuard Enterprise client is installed (SafeGuard Management Center computers or the SafeGuard Enterprise Server itself), you need to make sure that events are sent to the SafeGuard Enterprise Server. You therefore have to install a client configuration package on the computer. By doing so, the computer is activated as a client at the SafeGuard Enterprise Server and the Windows or SafeGuard Enterprise logging functionality is enabled.

For further information on client configuration packages, see [Working with configuration packages \(page 94\)](#).

Application scenarios

The SafeGuard Enterprise logging functionality is a user-friendly and comprehensive solution for recording and analyzing events. The following examples show typical application scenarios for SafeGuard Enterprise **Reports**.

Central monitoring of endpoints within a network

The security officer wants to be informed about critical events (for example, unauthorized data access, a number of failed logon attempts within a specified time frame) on a regular basis. Using a logging policy, the security officer can configure logging processes to log all security-related events occurring on the endpoints in a local log file. This log file is transferred to the SafeGuard Enterprise Database by the SafeGuard Enterprise Server after a number of events has been reached. The security officer can retrieve, view and analyze the events in the **Event Viewer** of the SafeGuard Management Center. The processes performed on different endpoints can be audited without staff being able to influence logging.

Monitor mobile users

In general, mobile users are not constantly connected to the company network. Sales representatives may for example disconnect their notebooks for a meeting. As soon as they log on to the network again, the SafeGuard Enterprise events logged during the offline period are transferred. The logging functionality provides an exact overview on the user's activities during the time that the computer was not connected to the network.

Destinations for logged events

There are two possible destinations for logged events: the Windows Event Viewer or the SafeGuard Enterprise Database. Only events related to a SafeGuard product are written to the relevant destination.

The output destinations for events to be logged are specified in the logging policy.

Windows Event Viewer

Events for which you define the Windows Event Viewer as a destination in the logging policy are logged in the Windows Event Viewer. The Windows Event Viewer can be used to display and manage logs for system, security and application events. You can also save these event logs. For these procedures, an administrator account for the relevant endpoint is required. In the Windows Event Viewer, an error code is displayed instead of a descriptive event text.

A prerequisite for viewing SafeGuard Enterprise events in the Windows Event Viewer is that a client configuration package is installed on the endpoint.

This chapter describes the processes of viewing, managing and analyzing event logs in the SafeGuard Management Center. For further information on the Windows Event Viewer, refer to your Microsoft Documentation.

SafeGuard Enterprise Database

Events for which you define the SafeGuard Enterprise Database as a destination in the logging policy are collected in a local log file in the local cache of the relevant endpoint in the following directory: auditing\SGMTranslog. Log files are submitted to a transport mechanism which transfers them to the database through the SafeGuard Enterprise Server. By default, the file is submitted as soon as the transport mechanism has successfully established a connection to the server. To limit the size of a log file, you can define a maximum number of log entries in a policy of the type **General Settings**. The log file will be submitted to the transport queue of the SafeGuard Enterprise Server when the number of entries specified has been reached. The events logged in the central database can be displayed in the SafeGuard Enterprise **Event Viewer** or **File Tracking Viewer**. As a security officer, you need the relevant rights to view, analyze and manage the events logged in the database.

Configure logging settings

Report settings are defined in two policies:

- **General Settings** policy

In a **General Settings** policy, you can specify a maximum number of logged entries after which the log file containing the events destined for the central database is to be transferred to the SafeGuard Enterprise Database. This reduces the size of the individual log files to be transferred. This setting is optional.

- **Logging** policy

The events to be logged are specified in a logging policy. In this policy, a security officer with the required policy rights defines which events will be logged to which output destination.

Define the number of events for feedback

1. Click the **Policies** button in the SafeGuard Management Center.
2. Create a new **General Settings** policy or select an existing one.
3. Under **Logging** in the **Feedback after number of events** field, specify the maximum number of events for a log file.
4. Save your settings.

After assigning the policy, the number of events specified applies.

Select events

1. In the SafeGuard Management Center, select the **Policies**.
2. Create a new **Logging** policy or select an existing one.

In the action area on the right-hand side under **Logging**, all predefined events which can be logged are displayed. By default, the events are grouped by **Level**, for example **Warning** or **Error**. But you can change the grouping. By clicking on the column headers you can sort the events by **ID**, **Category** etc.

3. To specify that an event is to be logged in the SafeGuard Enterprise Database, select the event by clicking in the column showing the database icon **Log events in database**. For events to be logged in the Windows Event Viewer, click in the column showing the event log icon **Log in event log**.

By clicking repeatedly you can deselect the event or set it to null. If you do not define a setting for an event, the relevant default value applies.

4. For all events selected, a green check mark is displayed in the relevant column. Save your settings.

After assigning the policy the selected events are logged in the relevant output destination.

 **Note** For a list of all events available for logging, see [Events available for reports \(page 220\)](#).

View logged events

As a security officer with the necessary rights, you can view the events logged in the central database in the SafeGuard Management Center **Event Viewer**.

To retrieve the entries logged in the central database:

1. In the navigation area of the SafeGuard Management Center, click **Reports**.

2. In the **Reports** navigation area, select **Event Viewer**.
3. In the **Event Viewer** action area on the right-hand side, click the magnifier icon.

All events logged in the central database are shown in the **Event Viewer**.

The individual columns show the following information concerning the events logged:

Column	Description
ID	Shows a number identifying the event.
Event	Shows an event text, this means a description of the event.
Category	Classification of the event by the source, for example Encryption, Authentication, System.
Application	Shows the software area the event originated from, for example SGMAuth, SGBaseEnc, SGMAS.
Computer	Shows the name of the computer on which the logged event occurred.
Computer domain	Shows the domain of the computer on which the logged event occurred.
User	Shows the user who was logged on at the time of the event.
User domain	Shows the domain of the user who was logged on at the time of the event.
Log time	Shows the system date and system time at which the event was logged on the endpoint.

By clicking the relevant column headers you can sort the events by **Level**, **Category** etc.

In addition, the context menu of the relevant columns offers a number of functions for sorting, grouping and customizing the Event Viewer.

By double-clicking an entry in the **Event Viewer** you can display event details concerning the logged event.

[Apply filters to the SafeGuard Enterprise Event Viewer](#)

The SafeGuard Management Center offers comprehensive filter functions. Using these functions you can quickly retrieve the relevant events from the events displayed.

The **Filter** area of the **Event Viewer** offers the following fields for defining filters:

Field	Description
Categories	Using this field you can filter the Event Viewer according to the source classification (for example Encryption , Authentication , System) shown in the Category column. Select the required categories from the drop-down list of the field.
Error level	Using this field you can filter the Event Viewer according to the Windows event classification (for example warning, error) shown

Field	Description
	in the Level column. Select the required levels from the drop-down list of the field.
Show last	In this field, you can define the number of events to be displayed. The events logged last will be displayed (by default the last 100 events).

In addition, you can create user-defined filters using the Filter Editor. You can display the Filter Editor from the context menu of the individual report columns. In the **Filter Builder** window you can define filters and apply them to the relevant column.

File access report for removable media and cloud storage

For **SafeGuard Data Exchange** and **SafeGuard Cloud Storage**, you can track files accessed on removable media or in your cloud storage. Regardless of any encryption policy applying to files stored on removable media or cloud storage, events can be logged for the following:

- A file or directory is created on a removable media device or in cloud storage.
- A file or directory is renamed on a removable media device or in cloud storage.
- A file or directory is deleted from a removable media device or in cloud storage.

File access tracking events can be viewed in the Windows Event Viewer or in the SafeGuard Enterprise **File Tracking Viewer** depending on the destination you specify when you define the logging policy.

Configure file access tracking

1. In the SafeGuard Management Center, select **Policies**.
2. Create a new **Logging** policy or select an existing one.

In the action area on the right-hand side under **Logging**, all predefined events which can be logged are displayed. By clicking on the column headers you can sort the events by **ID**, **Category** etc.

3. To activate file access tracking select the following log events depending on your requirements:
 - for files stored on removable media:
 - ID 3020 File tracking for removable media: a file has been created.
 - ID 3021 File tracking for removable media: a file has been renamed.
 - ID 3022 File tracking for removable media: a file has been deleted.
 - for files stored in cloud storage:
 - ID 3025 File tracking for cloud storage: a file has been created.
 - ID 3026 File tracking for cloud storage: a file has been renamed.
 - ID 3027 File tracking for cloud storage: a file has been deleted.

To specify that an event is to be logged in the SafeGuard Enterprise Database, select the event by clicking in the column showing the database icon **Log events in database**. For events to be logged in the Windows Event Viewer, click in the column showing the event log icon **Log in event log**.

For all events selected, a green check mark is displayed in the relevant column.

4. Save your settings.

After assigning the policy, file access tracking is activated and the selected events are logged in the relevant output destination.

 **Note** Be aware that enabling file access tracking significantly increases the server load.

View file access tracking events

To view file access tracking logs, you need the right **Display file tracking events**.

1. In the navigation area of the SafeGuard Management Center, click **Reports**.
2. In the **Reports** navigation area, select **File Tracking Viewer**.
3. In the **File Tracking Viewer** action area on the right-hand side, click the magnifier icon.

All events logged in the central database are shown in the **File Tracking Viewer**. The display is identical to the **Event Viewer** display. For further details, see [View logged events \(page 211\)](#).

Print reports

You can print the event reports displayed in the SafeGuard Management Center **Event Viewer** or **File Tracking Viewer** from the **File** menu in the menu bar of the SafeGuard Management Center.

- To display a print preview before printing the report, select **File > Print preview**. The print preview offers different functions, for example for exporting the relevant document into a number of output formats (for example .PDF) or editing the page layout (for example header and footer).
- To print the document without a print preview, select **File > Print**.

Connection of logged events

The events destined for the central database are logged in the EVENT table of the SafeGuard Enterprise Database. For this table, integrity protection can be applied. The events can be logged as a connected list in the EVENT table. Due to the connection, each entry in the list is dependent on the previous entry. If an entry is removed from the list, this is evident and can be verified by an integrity check.

To enhance performance, the connection of events in the EVENT table is deactivated by default. You can activate the connection of logged events to check integrity, see [Check the integrity of logged events \(page 215\)](#).

 **Note** When the connection of logged events is deactivated, integrity protection does not apply to the EVENT table.

 **Note** Too many events may lead to performance issues. For further information on how to avoid performance issues by cleaning up events, see [Scheduled event cleanup by script \(page 216\)](#).

Activate the connection of logged events

1. Stop web service SGNSRV at the Web Server.
2. Delete all events from the database and create a backup during deletion, see [Delete selected or all events \(page 215\)](#).

 **Note** If you do not delete all old events from the database, the connection will not work correctly as the remaining old events did not have it activated.

3. Set the following registry key to 0 or delete it:

HKEY_LOCAL_MACHINE\SOFTWARE\Utimaco\SafeGuard Enterprise DWORD:
DisableLogEventChaining = 0

4. Restart the web service.

The connection of logged events is activated.

 **Note** To deactivate the connection of events again, set the registry key to 1.

Check the integrity of logged events

Prerequisite: To check the integrity of logged events, the concatenation of events in the EVENT table has to be activated.

1. In the SafeGuard Management Center, click the **Reports**.
2. In the SafeGuard Management Center menu bar, select **Actions > Check integrity**.

A message shows information about the integrity of the events logged.

 **Note** If the connection of events is deactivated, an error is returned.

Delete selected or all events

1. In the SafeGuard Management Center, click **Reports**.
2. In the **Event Viewer**, select the events to be deleted.
3. To delete selected events, select **Actions > Delete events** or click the **Delete events** icon in the toolbar. To delete all events, select **Actions > Delete all events** or click the **Delete all events** icon in the toolbar.
4. Before deleting the selected events, the system displays the **Back up events as** window for creating a backup file, see [Create a backup file \(page 216\)](#).

The events are deleted from the event log.

Create a backup file

When you are deleting events, you can create a backup file of the report displayed in the SafeGuard Management Center Event Viewer.

1. When you select **Actions > Delete events** or **Actions > Delete all events**, the **Back up events as** window for creating a backup file is displayed before events are deleted.
2. To create an .XML backup file of the event log, enter a file name and a file location and click **OK**.

Open a backup file

1. In the SafeGuard Management Center, click **Reports**.
2. In the SafeGuard Management Center menu bar, select **Actions > Open backup file**.

The **Open Event Backup** window is displayed.

3. Select the backup file to be opened and click **Open**.

The backup file is opened and the events are shown in the SafeGuard Management Center **Event Viewer**. To return to the regular view of the **Event Viewer**, click the **Open backup file** icon in the toolbar again.

Scheduled event cleanup by script

 **Note** The SafeGuard Management Center offers the **Task Scheduler** to create and schedule periodic tasks based on scripts. The tasks are automatically run by a service on the SafeGuard Enterprise Server to execute the scripts specified.

For automatic and efficient cleanup of the EVENT table, four SQL scripts are available in the \tools directory of your SafeGuard Enterprise software delivery:

- spShrinkEventTable_install.sql
- ScheduledShrinkEventTable_install.sql
- spShrinkEventTable_uninstall.sql
- ScheduledShrinkEventTable_uninstall.sql

The two scripts spShrinkEventTable_install.sql and ScheduledShrinkEventTable_install.sql install a stored procedure and a scheduled job at the database server. The scheduled job runs the stored procedure at defined regular intervals. The stored procedure moves events from the EVENT table to the backup log table EVENT_BACKUP leaving a defined number of latest events in the EVENT table.

The two scripts spShrinkEventTable_uninstall.sql and ScheduledShrinkEventTable_uninstall.sql uninstall the stored procedure and the scheduled job. These two scripts also delete the EVENT_BACKUP table.

 **Note** If you use the stored procedure to move events from the EVENT table to the backup log table, event connection no longer applies. To activate connection while also using the stored procedure for event cleanup does not make sense. For further information, see [Connection of logged events \(page 214\)](#).

Create the stored procedure

The script spShrinkEventTable_install.sql creates a stored procedure which moves data from the EVENT table to a backup log table EVENT_BACKUP. If the EVENT_BACKUP table does not exist, it is created automatically.

The first line is "USE SafeGuard". If you have selected a different name for your SafeGuard Enterprise database, modify the name accordingly.

The stored procedure leaves the <n> latest events in the EVENT table and moves the rest of the events to the EVENT_BACKUP table. The number of events to be left in the EVENT table is specified by a parameter.

To execute the stored procedure, initiate the following command in SQL Server Management Studio (New Query):

```
exec spShrinkEventTable 1000
```

This command example moves all events except for the latest 1000 events.

Create a scheduled job for running the stored procedure

To automatically clean up the EVENT table at regular intervals, you can create a job at the SQL Server. The job can be created with the script ScheduledShrinkEventTable_install.sql or using the SQL Enterprise Manager.

 **Note** The scheduled job does not work on SQL Express databases. For the job to be executed, the SQL Server Agent has to be running. As there is no SQL Server Agent on SQL Server Express installations jobs are in this case not supported.

- The script has to be executed in the msdb. If you have selected a different name for your SafeGuard Enterprise Database than SafeGuard, modify the name accordingly.

```
/* Default: Database name 'SafeGuard' change if required*/
```

```
SELECT @SafeGuardDataBase='SafeGuard'
```

- You can also specify the number of events to be left in the EVENT table. The default is 100,000.

```
/* Default: keep the latest 100000 events, change if required*/
```

```
SELECT @ShrinkCommand='exec spShrinkEventTable 100000'
```

- You can specify whether a job run is to be logged in the NT Event Log.

```
exec sp_add_job
```

```
    @job_name='AutoShrinkEventTable',
```

```
    @enabled=1,
```

```
    @notify_level_eventlog=3
```

The following values are available for parameter notify_level_eventlog:

Value	Result
3	Log every time the job runs.
2	Log if the job fails.
1	Log if the job was carried out successfully.
0	Do not log job run in NT Event Log.

- You can specify how often the job run should be repeated in case it fails.

```
exec sp_add_jobstep
```

- @retry_attempts=3

This example defines 3 job run attempts in case of failure.

- @retry_interval=60

This example defines a retry interval of 60 minutes.

- You can specify a time schedule for running the job.

```
exec sp_add_jobschedule
```

- @freq_type=4

This example defines that the job is run daily.

- @freq_interval=1

This example defines that the job is run once per day.

- @active_start_time=010000

This example defines that the job is run at 1 a.m.

 **Note** Besides the example values stated above, you can define a number of different schedule options with sp_add-jobschedule. For example, the job can be run every two minutes or only once per week. For further information, see the Microsoft Transact SQL Documentation.

Clean up stored procedures, jobs and tables

The script spShrinkEventTable_uninstall.sql deletes the stored procedure and the EVENT_BACKUP table. The script ScheduledShrinkEventTable_uninstall.sql deregisters the scheduled job.

 **Note** When you execute spShrinkEventTable_uninstall.sql, the EVENT_BACKUP table will be deleted with all data contained in it.

Report Message Templates

Events are not logged with their complete event texts in the SafeGuard Enterprise Database. Only ID and the relevant parameter values are written to the database table. When the logged events are retrieved in the SafeGuard Management Center **Event Viewer**, the parameter values and the text

templates contained in the .dll are converted into the complete event text in the current SafeGuard Management Center system language.

The templates used for event texts can be edited and processed, for example by using SQL queries. To do so, you can generate a table containing all text templates for event messages. Afterwards you can customize the templates according to your specific requirements.

To create a table containing the text templates for the individual event IDs:

1. In the menu bar of the SafeGuard Management Center, select **Tools > Options**.
2. In the **Options** window, go to tab **Database**.
3. In the **Report Message Templates** area, click **Create Table**.

The table containing the templates for the event ID is created in the current system language and can be customized.

 **Note** Before the templates are generated, the table is cleared. If the templates have been generated for a specific language and a user generates the templates for a different language, the templates for the first language are deleted.

3.8.16.2 Events available for reports

The following table provides an overview on all events which can be selected for logging.

Category	Event ID	Description
System	1001	Process started.
System	1005	Service started.
System	1006	Service start failed.
System	1007	Service stopped.
System	1016	Integrity test of data files failed.
System	1017	Logging destination not available.
System	1018	Unauthorized attempt to uninstall SafeGuard Enterprise.
System	1019	key backup failed
System	1020	Sending "key backup complete" to Sophos Enterprise Console failed.
System	1021	key backup not acknowledged
Communication	1500	Email was sent with attachments (From, Subject, Encryption method)
Communication	1507	Email was sent with attachments (From, Subject, Attachments, Encryption method)
Communication	1508	Email was sent with attachments (From, Recipients, Subject, Attachments, Encryption method)
Authentication	2001	External GINA identified and integrated successfully.
Authentication	2002	External GINA identified, integration failed.
Authentication	2003	Power-on Authentication active.
Authentication	2004	Power-on Authentication deactivated.
Authentication	2005	Wake on LAN activated.

Authentication	2006	Wake on LAN deactivated.
Authentication	2007	Challenge created.
Authentication	2008	Response created.
Authentication	2009	Logon successful.
Authentication	2010	Logon failed.
Authentication	2011	User imported during logon and marked as owner.
Authentication	2012	User imported by owner and marked as non-owner.
Authentication	2013	User imported by non-owner and marked as non-owner.
Authentication	2014	User removed as owner.
Authentication	2015	Import of user during logon failed.
Authentication	2016	User logged off.
Authentication	2017	User was forced to log off.
Authentication	2018	Action performed on device.
Authentication	2019	User started a Password/PIN change.
Authentication	2020	User changed their password/PIN after logon.
Authentication	2021	Password/PIN quality.
Authentication	2022	Password/PIN policy violated.
Authentication	2023	LocalCache was corrupted and has been restored.
Authentication	2024	Invalid Password Black List Configuration.
Authentication	2025	Response code that allows the user to display the password received.
Authentication	2026	Local cache backup completed successfully.
Authentication	2027	Local cache backup failed.
Authentication	2028	The logged on user is guest user.
Authentication	2029	Successful logon to Web Helpdesk with preconfigured credentials.
Authentication	2030	Logged on user is a Service Account.
Authentication	2031	Logon to Web Helpdesk with preconfigured credentials failed.
Authentication	2032	Authorization for Web Helpdesk failed.
Authentication	2033	Web Helpdesk started.
Authentication	2035	Service Account List imported.
Authentication	2036	Service Account List deleted.
Authentication	2056	SGN Windows user added.
Authentication	2057	All SGN Windows users have been removed from a machine.
Authentication	2058	Manual UMA user removal has been performed.
Authentication	2061	Computrace check return code.
Authentication	2062	Computrace check could not be executed.
Authentication	2071	Kernel initialization was successfully completed.
Authentication	2072	Kernel initialization has failed.
Authentication	2073	Machine keys were successfully generated on the client.
Authentication	2074	Machine keys could not be generated successfully on the client.
Authentication	2075	Querying disk properties or Opal disk initialization has failed.
Authentication	2079	Importing user into the kernel was successfully completed.
Authentication	2080	Removing user from the kernel was successfully completed.
Authentication	2081	Importing user into the kernel has failed.
Authentication	2082	Removing user from the kernel has failed.
Authentication	2083	Response with "display user password" created.
Authentication	2084	Response for virtual client created.

Authentication	2085	Response for standalone client created.
Authentication	2086	For a standalone client user a new certificate was generated.
Authentication	2087	A certificate was assigned to a standalone client user. This event can only occur on unmanaged endpoints and thus will never be logged to the database.
Authentication	2095	Wake on LAN could not be activated.
Authentication	2096	Wake on LAN could not be deactivated.
Authentication	2097	The user has logged in to the client using the standby token for the first time. The standby token was set as standard token.
Authentication	2098	A successful standby certificate activation has been reported to the server.
Authentication	2099	The user has logged in to the client using the standby token for the first time. The standby certificate could not be activated because of an error.
Authentication	2100	The standby certificate activation has failed on the server
Authentication	2101	The pin on the token has been changed
Authentication	2102	PIN change on token failed
Authentication	2103	Unable to enforce policy "Enforce certificate based token logon"
Authentication	2104	Policy "Enable certificate based token logon" enforced
Administration	2500	SafeGuard Enterprise Administration started.
Administration	2501	Logon to SafeGuard Enterprise Administration failed.
Administration	2502	Authorization for SafeGuard Enterprise Administration failed.
Administration	2502	Authorization for SafeGuard Enterprise Administration failed.
Administration	2503	Additional authorization required.
Administration	2504	Additional authorization for action granted.
Administration	2505	Additional authorization failed.
Administration	2506	Data import from directory successful.
Administration	2507	Data import from directory cancelled.
Administration	2508	Failed to import data from directory.
Administration	2511	User created.
Administration	2513	User changed.
Administration	2515	User deleted.
Administration	2518	Application of user failed.
Administration	2522	Failed to delete user.
Administration	2525	Machine applied.
Administration	2529	Machine deleted.
Administration	2532	Application of machine failed.
Administration	2536	Failed to delete machine.
Administration	2539	OU applied.
Administration	2543	OU deleted.
Administration	2546	Application of OU failed.
Administration	2547	Import of OU failed.
Administration	2550	Failed to delete OU.
Administration	2553	Group applied.
Administration	2555	Group modified.
Administration	2556	Group renamed.
Administration	2557	Group deleted.

Administration	2560	Application of group failed.
Administration	2562	Failed to change group.
Administration	2563	Failed to rename group.
Administration	2564	Failed to delete group.
Administration	2573	Members added to group.
Administration	2575	Members deleted from group.
Administration	2576	Failed to add members to group.
Administration	2578	Failed to delete members from group.
Administration	2580	Group switched from OU to OU.
Administration	2583	Failed to switch group from OU to OU.
Administration	2591	Objects added to group.
Administration	2593	Objects deleted from group.
Administration	2594	Failed to add objects to group.
Administration	2596	Failed to delete objects from group.
Administration	2603	Key generated.
Administration	2603	Key generated.
Administration	2604	Key modified.
Administration	2607	Key assigned.
Administration	2608	Key assignment cancelled.
Administration	2609	Failed to generate key.
Administration	2610	Failed to modify key.
Administration	2613	Failed to assign key.
Administration	2614	Failed to delete assignment of key.
Administration	2615	Certificate generated.
Administration	2616	Certificate imported.
Administration	2619	Certificate deleted.
Administration	2621	Certificate assigned to user.
Administration	2622	Certificate assignment to user cancelled.
Administration	2623	Failed to create certificate.
Administration	2624	Failed to import certificate.
Administration	2627	Failed to delete certificate.
Administration	2628	Extension of certificate failed.
Administration	2629	Failed to assign certificate to user.
Administration	2630	Failed to delete assignment of certificate to user.
Administration	2631	Token plugged in.
Administration	2632	Token removed.
Administration	2633	Token issued to user.
Administration	2634	Change user PIN on token.
Administration	2635	Change SO PIN on token.
Administration	2636	Token locked.
Administration	2637	Token unlocked.
Administration	2638	Token deleted.
Administration	2639	Token assignment for user removed.
Administration	2640	Failed to issue token for user.
Administration	2641	Failed to change user PIN on token.
Administration	2642	Failed to change SO PIN on token.

Administration	2643	Failed to lock token.
Administration	2644	Failed to unlock token.
Administration	2645	Failed to delete token.
Administration	2647	Policy created.
Administration	2648	Policy changed.
Administration	2650	Policy deleted.
Administration	2651	Policy assigned and activated to OU.
Administration	2652	Assigned policy removed from OU.
Administration	2653	Failed to create policy.
Administration	2654	Failed to change policy.
Administration	2657	Failed to assign and activate a policy to OU.
Administration	2658	Removing of assigned policy from OU failed.
Administration	2659	Policy group created.
Administration	2660	Policy group changed.
Administration	2661	Policy group deleted.
Administration	2662	Failed to create policy group.
Administration	2663	Failed to change policy group.
Administration	2665	Following policy has been added to policy group.
Administration	2667	Following policy has been deleted from policy group.
Administration	2668	Failed to add policy to policy group.
Administration	2670	Failed to delete policy from policy group.
Administration	2678	Recorded event exported.
Administration	2679	Export of recorded events failed.
Administration	2680	Recorded events deleted.
Administration	2681	Failed to delete recorded events.
Administration	2684	Security Officer allows renewal of certificate.
Administration	2685	Security Officer denies renewal of certificate.
Administration	2686	Failed to alter renewal settings for certificate.
Administration	2687	Officer certificate changed.
Administration	2688	Failed to change officer certificate.
Administration	2692	Creation of workgroups.
Administration	2693	Failed creation of workgroups.
Administration	2694	Deletion of workgroups.
Administration	2695	Failed deletion of workgroups.
Administration	2696	Creation of users.
Administration	2697	Failed creation of users.
Administration	2698	Creation of machines.
Administration	2699	Failed creation of machines.
Administration	2700	License is violated.
Administration	2701	Key file has been created.
Administration	2702	Key for key file has been deleted.
Administration	2703	A Security Officer disabled power-on authentication in policy.
Administration	2704	LSH Question Theme created.
Administration	2705	LSH Question Theme changed.
Administration	2706	LSH Question Theme deleted.
Administration	2707	Question changed.

Administration	2708	Configuration package for standalone client created.
Administration	2709	Configuration package for Enterprise Client created.
Administration	2710	CCO has been imported.
Administration	2711	CCO has been exported.
Administration	2712	CCO has been deleted.
Administration	2713	Update of the company certificate.
Administration	2715	Service Account List created.
Administration	2716	Service Account List modified.
Administration	2717	Service Account List deleted.
Administration	2718	Cloud Storage Definition created.
Administration	2719	Cloud Storage Definition modified.
Administration	2720	Cloud Storage Definition deleted.
Administration	2721	Application List created.
Administration	2722	Application List modified.
Administration	2723	Application List deleted.
Administration	2724	Role created.
Administration	2725	Role modified.
Administration	2726	Role deleted.
Administration	2727	Role assigned to Security Officer.
Administration	2728	Role unassigned from Security Officer.
Administration	2729	Master Security Officer created.
Administration	2730	Master Security Officer modified.
Administration	2731	Master Security Officer deleted.
Administration	2732	Master Security Officer certificate changed.
Administration	2733	Master Security Officer certificate change failed.
Administration	2734	Master Security Officer enabled.
Administration	2735	Master Security Officer disabled.
Administration	2736	Security Officer created.
Administration	2737	Security Officer modified.
Administration	2738	Security Officer deleted.
Administration	2739	Security Officer deleted. Additional information about the children.
Administration	2740	Security Officer enabled.
Administration	2741	Security Officer disabled.
Administration	2742	Security Officer moved.
Administration	2743	Security Officer promoted.
Administration	2744	Security Officer promoted. Additional information about the children.
Administration	2745	Master Security Officer demoted.
Administration	2746	Security Officer Group created.
Administration	2747	Security Officer Group modified.
Administration	2748	Security Officer Group deleted.
Administration	2749	Security Officer added to Security Officer Group.
Administration	2750	Security Officer removed from Security Officer Group.
Administration	2753	Read access to container granted for Security Officer.
Administration	2754	Read access to container granted for Security Officer Group.
Administration	2755	Full access to container granted for Security Officer.
Administration	2756	Full access to container granted for Security Officer Group.

Administration	2757	Access to container revoked for Security Officer.
Administration	2758	Access to container revoked for Security Officer Group.
Administration	2759	Read access to policy granted for Security Officer.
Administration	2760	Read access to policy granted for Security Officer Group.
Administration	2761	Full access to policy granted for Security Officer.
Administration	2762	Full access to policy granted for Security Officer Group.
Administration	2763	Access to policy revoked for Security Officer.
Administration	2764	Read access to policy revoked for Security Officer Group.
Administration	2765	LSH Question number parameters changed.
Administration	2766	Access to container explicitly denied for Security Officer.
Administration	2767	Explicitly denied access to container revoked for Security Officer.
Administration	2768	Read access to container revoked for Security Officer.
Administration	2769	File tracking viewer has been opened.
Administration	2770	Policy deployment enabled by security officer.
Administration	2771	Policy deployment disabled by security officer.
Administration	2772	Policy deployment enabled by license management.
Administration	2773	Policy deployment disabled by license management.
Administration	2800	The confirmation of unconfirmed user was successful.
Administration	2801	A user has not been automatically confirmed.
Administration	2810	POA user created.
Administration	2811	POA user modified.
Administration	2812	POA user deleted.
Administration	2815	Creation of POA user failed.
Administration	2816	Modification of POA user failed.
Administration	2817	Deletion of POA user failed.
Administration	2820	POA group created.
Administration	2821	POA group modified.
Administration	2822	POA user group deleted.
Administration	2825	Creation of POA user group failed.
Administration	2826	Modification of POA user group failed.
Administration	2827	Deletion of POA group failed.
Administration	2830	POA Group is assigned to container.
Administration	2831	Assigned POA Group removed from container.
Administration	2832	Groups are activated for the assignment of POA Group to container.
Administration	2833	Failed to assign POA Group to container.
Administration	2834	Removing of assigned POA Group from Container failed.
Administration	2835	Failed to activate groups for the assignment of POA Group to container.
Administration	2850	Scheduler service stopped due to an exception.
Administration	2851	Scheduler task executed successfully.
Administration	2852	Scheduler task failed.
Administration	2853	Scheduler task created or modified.
Administration	2854	Scheduler task deleted.
Administration	2855	The certificate signature algorithm for new certificates has been changed.
Administration	2856	The certificate key length for new certificates has been changed.
Administration	2857	The certificate validity period for new certificates has been changed.
Administration	2858	The database has been upgraded successfully.

Administration	2859	The database upgrade failed
Administration	2900	Response for Configuration Protection suspension created
Administration	2905	BitLocker recovery key was exported for machine
Client	3003	Kernel backup succeeded.
Client	3005	Kernel restore first chance succeeded.
Client	3006	Kernel restore second chance succeeded.
Client	3007	Kernel backup failed.
Client	3008	Kernel restore failed.
Client	3009	Kernel backup failed.
Client	3010	Backup token from POA removed
Client	3011	Backup token added to POA
Client	3018	The delayed encryption encrypted a file.
Client	3019	The delayed encryption decrypted a file.
Client	3020	File tracking for removable media: a file has been created.
Client	3021	File tracking for removable media: a file has been renamed.
Client	3022	File tracking for removable media: a file has been deleted.
Client	3025	File tracking for cloud storage: a file has been created.
Client	3026	File tracking for cloud storage: a file has been renamed.
Client	3027	File tracking for cloud storage: a file has been deleted.
Client	3028	File tracking: a file has been encrypted manually.
Client	3029	File tracking: a file has been decrypted manually.
Client	3030	User has changed his LSH secrets after login.
Client	3035	LSH was activated
Client	3040	LSH was deactivated
Client	3045	LSH is available - Enterprise Client
Client	3046	LSH is available - Standalone Client
Client	3050	LSH is disabled - Enterprise Client
Client	3051	LSH isn't available - Standalone Client
Client	3055	The QST list (LSH questions) was changed
Client	3060	The user has changed his answers in LSH
Client	3070	Key backup saved to the specified network share.
Client	3071	Key backup could not be saved to the specified network share.
Client	3072	User turned off encryption.
Client	3080	Sophos UEFI boot entry has been repaired successfully.
Client	3081	Sophos UEFI boot entry repair failed.
Client	3082	The outlook Add-in has been disabled although it is enabled in the SGN policy.
Client	3110	POA user imported into POA
Client	3111	POA user deleted from POA
Client	3116	Import of POA user into POA failed
Client	3117	Deletion of POA user from POA failed
Client	3200	Configuration Protection suspended.
Client	3201	Configuration Protection not suspended (wrong response).
Client	3202	Suspension of Configuration Protection ended by user.
Client	3203	Suspension of Configuration Protection ended (suspension time was over).

Client	3300	Master Application restarted
Client	3301	Master Application was unexpectedly terminated
Client	3302	Master Application restart failed
Client	3303	An unhandled exception caused a crash in the Master application.
Client	3304	Termination of unknown MasterApp failed.
Client	3405	Configuration Protection client failed to uninstall.
Client	3406	Configuration Protection client experienced an internal error.
Client	3407	Configuration Protection client detected a possible tampering event.
Client	3408	Configuration Protection client detected a possible tampering of event logs.
Client	3409	Wrong passphrase entered.
Encryption	3500	Hard disk was successfully prepared for BitLocker encryption.
Encryption	3501	Access denied to medium on drive.
Encryption	3502	Access denied to data file.
Encryption	3503	Sector-based initial encryption of drive started.
Encryption	3504	Sector-based initial encryption of drive started (fast mode)
Encryption	3505	Sector-based initial encryption of drive completed successfully.
Encryption	3506	Sector-based initial encryption of drive failed and closed.
Encryption	3507	Sector-based initial encryption of drive cancelled.
Encryption	3508	Sector-based initial encryption of drive failed.
Encryption	3509	Sector-based decryption of drive started.
Encryption	3510	Sector-based decryption of drive completed successfully.
Encryption	3511	Sector-based decryption of drive failed and closed.
Encryption	3512	Sector-based decryption of drive cancelled.
Encryption	3513	Sector-based decryption of drive failed.
Encryption	3514	File-based initial encryption on a drive started.
Encryption	3515	File-based initial encryption on a drive completed successfully.
Encryption	3516	File-based initial encryption on a drive failed and closed.
Encryption	3517	File-based initial encryption on a drive cancelled.
Encryption	3519	File-based decryption on a drive started.
Encryption	3520	File-based decryption on a drive closed successfully.
Encryption	3521	File-based decryption on a drive failed and closed.
Encryption	3522	File-based decryption on a drive cancelled.
Encryption	3524	Encryption of a file started.
Encryption	3525	Encryption of a file completed successfully.
Encryption	3526	Encryption of a file failed.
Encryption	3540	Decryption of a file started.
Encryption	3541	Decryption of a file completed successfully.
Encryption	3542	Decryption of a file failed.
Encryption	3543	Backup of boot key successful.
Encryption	3544	Maximum count of boot algorithms exceeded.
Encryption	3545	Read errors on KSA.
Encryption	3546	Disabling volumes according to the defined policies.
Encryption	3547	Warning: NTFS boot sector backup is missing on the volume.
Encryption	3548	The user has set new BitLocker credentials for starting up the computer.

Encryption	3549	The user tried to set new BitLocker credentials for starting up the computer but the operation failed.
Encryption	3552	The user has suspended BitLocker protection.
Encryption	3553	The user has resumed BitLocker protection.
Encryption	3559	Items from asynchronous encryption queue are missing.
Encryption	3560	Access Protection
Encryption	3561	Computer status has been changed to secure.
Encryption	3562	Computer is secure, but policy setting "Remove keys on compromised machines" is not enabled. No action was taken.
Encryption	3563	Computer is insecure, but policy setting "Remove keys on compromised machines" is not enabled. No action was taken.
Encryption	3570	Media Encryption Key assigned.
Encryption	3571	Media Passphrase Key assigned.
Encryption	3572	Media Passphrase Key created.
Encryption	3573	Media Passphrase Key imported.
Encryption	3574	Broken key table detected.
Encryption	3600	General encryption error.
Encryption	3601	Encryption error - Engine: Volume missing.
Encryption	3602	Encryption error - Engine: Volume offline.
Encryption	3603	Encryption error - Engine: Volume removed.
Encryption	3604	Encryption error - Engine: Volume bad.
Encryption	3605	This computer is insecure. You must take further action.
Encryption	3607	Encryption error - Encryption key missing.
Encryption	3610	Encryption error - Origin KSA area corrupt.
Encryption	3611	Encryption error - Backup KSA area corrupt.
Encryption	3612	Encryption error - Origin ESA area corrupt.
Encryption	3700	File Share discarded an invalid path in the policy.
Encryption	3701	A trusted application could not be found.
Encryption	3710	File Share encryption started.
Encryption	3711	File Share encryption finished successfully.
Encryption	3712	File Share encryption completed with errors.
Encryption	3713	File Share encryption was cancelled.
Encryption	3714	Initial encryption has finished.
Encryption	3715	Initial encryption has finished for path.
Encryption	3800	Cloud Storage discarded an invalid path in the policy.
Encryption	3900	Encryption of self-decrypting HTML5 file has finished successfully.
Encryption	3999	Preparation of hard disk for BitLocker encryption has failed
Access Control	4400	Port successfully approved.
Access Control	4401	Device successfully approved.
Access Control	4402	Storage successfully approved.
Access Control	4403	WLAN successfully approved.
Access Control	4404	Port removed successfully.
Access Control	4405	Device removed successfully.
Access Control	4406	Storage device removed successfully.
Access Control	4407	WLAN disconnected successfully.
Access Control	4408	Port restricted.

Access Control	4409	Device restricted.
Access Control	4410	Storage device restricted.
Access Control	4411	WLAN restricted.
Access Control	4412	Port blocked.
Access Control	4413	Device blocked.
Access Control	4414	Storage device blocked.
Access Control	4415	WLAN blocked.

3.8.17 Policy types and their fields of applications

SafeGuard Enterprise policies include all settings needed to implement a company-wide security policy on endpoints.

SafeGuard Enterprise policies can incorporate settings for the following areas (policy types):

- **General Settings**

Settings for transfer rate, customization, logon recovery, background images, and so on.

- **Authentication**

Settings for logon mode, device lock, etc.

- **PIN**

Defines requirements for used PINs.

- **Password**

Defines requirements for used passwords.

- **Passphrase**

Defines requirements for passphrases used for SafeGuard Data Exchange.

- **Device Protection**

Settings for volume- or file-based encryption (including settings for SafeGuard Data Exchange, SafeGuard Cloud Storage and SafeGuard Portable): algorithms, keys, the drives on which data is to be encrypted, and so on.

- **Specific Machine Settings**

Settings for SafeGuard Power-on Authentication (activate/deactivate), secure Wake on LAN, display options, and so on.

- **Logging**

Defines events to be logged and their output destinations.

- **Configuration Protection**

 **Note** Configuration Protection is only supported for SafeGuard Enterprise Clients up to Version 6.0.

Settings (allow/block) for the usage of ports and peripheral devices (removable media, printers, and so on.).

- **File Encryption**

Settings for file-based encryption on local drives and network locations, especially for work groups on network shares.

In the SafeGuard Management Center, default policies are available for all policy types. For **Device Protection** policies, policies for full disk encryption (target: mass storage), Cloud Storage (target: DropBox) and Data Exchange (target: removable media) are available. The options in these default policies are set to the relevant values. You can modify the default settings according to your requirements. The default policies are named <policy type> (Default).

 **Note** The names of the default policies depend on the language setting during installation. If you change the language of the SafeGuard Management Center afterwards, the default policy names remain in the language set during installation.

3.8.17.1 General settings

Policy setting	Explanation
The settings are shown as they appear in the SafeGuard Enterprise Management Center.	
Loading of Settings	<p>Policy Loopback Replay Machine Settings</p> <p>If Replay Machine Settings is selected in the field Policy Loopback, and the policy originates from a machine (Replay Machine settings in a user policy does not have any effect), this</p>

Policy setting	Explanation
	<p>policy is implemented again at the end. This then overrides any user settings and the machine settings apply.</p> <p>Ignore User</p> <p>If you select Ignore User for a policy (machine policy) in the field Policy Loopback and the policy originates from a machine, only the machine settings are analyzed. User settings are not analyzed.</p> <p>No Loopback</p> <p>No Loopback is the standard behavior: User policies take priority over machine policies.</p> <p>How are the settings "Ignore User" and "Replay Machine Settings" analyzed?</p> <p>If there are active policy assignments, the machine policies are analyzed and consolidated first. If consolidation of the various policies results in the Ignore User attribute in policy loopback, policies that would have been applied for the user are no longer analyzed. This means that the same policies apply to the user as to the machine.</p> <p>If the Replay Machine Settings value is applied in the case of the policy loopback, once the individual machine policies have been consolidated, the user policies are then merged with the machine policies. After consolidation, the machine policies are re-written and override any user policy settings. This means that if a setting is present in both policies, the machine policy value overrides the user policy value. If the consolidation of individual machine policies results in "not configured", the following applies: User settings take priority over machine settings.</p>
Transfer Rate	
Connection interval to server (min)	<p>Determines the period in minutes after which a SafeGuard Enterprise client sends a policy (changes) enquiry to the SafeGuard Enterprise Server.</p> <p>To prevent a large number of clients contacting the server at the same time, communication is carried out during a period of +/- 50% of the interval you set. Example: If you set "90 minutes",</p>

Policy setting	Explanation
	communication occurs after an interval that can be from 45 to 135 minutes.
Feedback	
Improve Sophos SafeGuard® by sending anonymous usage data	<p>Sophos is continuously trying to improve SafeGuard Enterprise. Accordingly, clients regularly send anonymized data to Sophos. This data is exclusively utilized for improving the product. It cannot be used to identify customers or machines, and does not contain any other confidential information.</p> <p>Because all data is sent anonymized, the data collection function is enabled by default.</p> <p>If you set this option to No, no usage data will be sent to Sophos.</p>
Logging	
Feedback after number of events	<p>The log system, implemented as Win32 Service “SGM LogPlayer”, collects log entries generated by SafeGuard Enterprise for the central database and stores them in local log files. These are located in the Local Cache in the “Auditing \SGMTransLog” directory. These files are transferred to the transport mechanism which then sends them to the database through the SGN Server. Transfer takes place as soon as the transport mechanism has succeeded in creating a connection to the server. The log file therefore increases in size until a connection has been established. To limit the size of each log file, it is possible to set a maximum number of log entries in the policy. Once the preset number of entries has been reached the logging system places the log file in the SGN Server transport queue and starts a new log file.</p>
Customization	
Language used on client	<p>Language in which settings for SafeGuard Enterprise are displayed on the endpoint:</p> <p>You can select a supported language or the endpoint's operating system language setting.</p>
Logon recovery	

Policy setting	Explanation
Activate logon recovery after Windows Local Cache corruption	<p>The Windows Local Cache is the start and the end point for the data exchange between the endpoint and the server. It stores all keys, policies, user certificates and audit files. All data stored in the local cache are signed and cannot be changed manually.</p> <p>By default, logon recovery after Local Cache corruption is deactivated. This means the Local Cache will be restored automatically from its backup. In this case, no Challenge/Response procedure is required for repairing the Windows Local Cache. If the Windows Local Cache is to be repaired explicitly with a Challenge/Response procedure, set this field to Yes.</p>
Local Self Help	
Enable Local Self Help	<p>Determines whether users are permitted to log on to endpoints with Local Self Help if they have forgotten their password. With Local Self Help, users can log on by answering a specified number of previously defined questions in the SafeGuard Power-on Authentication. They can regain access to their computers even if neither telephone nor internet connection are available.</p> <p>For the user to be able to use Local Self Help, automatic logon to Windows must be enabled. Otherwise, Local Self Help will not work.</p>
Minimum length of answers	Defines the minimum character length for Local Self Help answers.
Welcome text under Windows	Specify the custom text to be displayed in the first dialog when launching the Local Self Help Wizard on the endpoint. Before you can specify the text here, it has to be created and registered in the policy navigation area under Texts .
Users can define their own questions	As a security officer, you can define the set of questions to be answered centrally and distribute it to the endpoint in the policy. However, you can also grant the users the right to define their own questions. To entitle users to define their own questions, select Yes .
Challenge / Response (C/R)	

Policy setting	Explanation
Enable logon recovery via C/R	<p>Determines whether a user is permitted to generate a challenge in the SafeGuard Power-on Authentication (POA) to regain access to their computer with a Challenge/Response procedure.</p> <p>Yes: User is permitted to generate a challenge. In this case, the user can regain access to their computer with a C/R procedure in an emergency.</p> <p>No: User is not permitted to issue a challenge. In this case, the user cannot initiate a C/R procedure to regain access to their computer in an emergency.</p>
Allow automatic logon to Windows	<p>Allows a user to log on to Windows automatically after authentication with Challenge/Response.</p> <p>Yes: User is automatically logged on to Windows.</p> <p>No: Windows logon screen appears.</p> <p>Example: A user has forgotten their password. After the Challenge/Response procedure, SafeGuard Enterprise logs the user on at the endpoint without a SafeGuard Enterprise password. In this case automatic Windows logon is switched off and the Windows logon screen is displayed. The user cannot log on because they do not know the SafeGuard Enterprise password (= Windows password). The setting Yes allows automatic logon and the user is able to move on from the Windows logon screen.</p>
Information text	<p>Display information text when a Challenge/Response procedure is initiated in the SafeGuard POA. For example: "Please contact Support Desk on telephone number 01234-56789".</p> <p>Before you specify a text here, you must create it as a text file in the Policies navigation area under Texts.</p>
Images	
	<p>Prerequisite:</p> <p>New images must be registered in the Policies navigation area of the SafeGuard Management Center under Images. The</p>

Policy setting	Explanation
	images will only be available after registration. Supported formats: .BMP, .PNG, .JPEG.
Background image in POA	Replace the blue SafeGuard Enterprise background with a custom background image. Customers may for example use the company logo in SafeGuard POA and at Windows logon. Maximum file size for all background bitmaps: 500 KB.
Background image in POA (low resolution)	<p>Normal:</p> <ul style="list-style-type: none"> • Resolution: 1024x768 (VESA mode) • Colors: unlimited <p>Low:</p> <ul style="list-style-type: none"> • Resolution: 640x480 (VGA mode) • Colors: 16 colors
Logon image in POA	Replaces the SafeGuard Enterprise image displayed during SafeGuard POA logon with a custom image, for example a company logo.
Logon image in POA (low resolution)	<p>Normal:</p> <ul style="list-style-type: none"> • Resolution: 413 x 140 pixels • Colors: unlimited <p>Low:</p> <ul style="list-style-type: none"> • Resolution: 413 x 140 pixels • Colors: 16 colors

Policy setting	Explanation
File Encryption	
Trusted Applications	<p>For file-based encryption by File Encryption and SafeGuard Data Exchange, you can specify applications as trusted to grant them access to encrypted files. This is for example necessary to enable antivirus software to scan encrypted files.</p> <p>Enter the applications you want to define as trusted in the editor list box of this field. Applications must be entered as fully qualified paths.</p>
Ignored Applications	<p>For file-based encryption by File Encryption and SafeGuard Data Exchange, you can specify applications as ignored to exempt them from transparent file encryption/decryption. For example, if you define a backup program as an ignored application, encrypted data backed up by the program remains encrypted.</p> <p>Enter the applications you want to define as ignored in the editor list box of this field. Applications must be entered as fully qualified paths.</p>
Ignored Devices	<p>For file-based encryption by File Encryption and SafeGuard Data Exchange, you can exclude entire devices (for example disks) from file-based encryption.</p> <p>In the editor list box, select Network to select a predefined device, or enter the required device names to exclude specific devices from encryption.</p>
Enable persistent encryption	<p>For file-based encryption by File Encryption and SafeGuard Data Exchange, you can configure persistent encryption. With persistent encryption, copies of encrypted files will be encrypted, even when they are saved in a location not covered by an encryption rule.</p> <p>This policy setting is activated by default.</p>
User is allowed to set default keys	<p>For file-based encryption by Cloud Storage you can configure whether the user is allowed to set a default key for encryption or not. If allowed, the Set default key command is added to the Windows Explorer context menu of Cloud Storage synchronization folders. Users can use the command to specify</p>

Policy setting	Explanation
Remove keys on compromised machines	<p>separate default keys to be used for encryption of different synchronization folders.</p> <p>This policy setting only applies to protected computers using a Sophos Endpoint Security product that provides a health state (for example Sophos Central versions of Endpoint Security and Control). When this policy is enabled, keys are removed on compromised computers. While the computer is marked as compromised, no keys are assigned.</p>
User is allowed to decrypt files	<p>For Synchronized Encryption you can prevent users from decrypting files manually. If you set this option to No the Decrypt selected file option option is removed from the right-click menu of files, see Encrypt/Decrypt files manually (page 405).</p> <p>Files then can only be decrypted by policy settings.</p> <p>On Mac OS this setting is only applied if the policy is assigned to the machine. Assigning it to a user has no effect.</p>
User is allowed to create password protected files	<p>For file-based encryption by Synchronized Encryption, File Encryption, Cloud Storage and Data Exchange you can configure whether users can create password protected files or not. If you set this option to Yes, a Create password protected file option is added to the right-click menu of files, see Encrypt/Decrypt files manually (page 405).</p>
Email add-in settings	
Enable email add-in	<p>SafeGuard Enterprise includes an add-in for Microsoft Outlook that makes encrypting email attachments easy. If you set this option to Yes, users will be prompted to decide how to handle attachments each time they send emails with attachments.</p> <p>In addition, you can list domains and specify how attachments are handled when they are sent to these domains.</p>
Behavior for white-listed domains	
Encryption method for white-listed domains	Select how to handle attachments from the drop-down list:

Policy setting	Explanation
Domain whitelist	<p>Encrypted: All attachments in emails to the specified domain will be encrypted. Users will not be prompted.</p> <p>No encryption: Attachments in emails to the specified domain will not be encrypted. Users will not be prompted.</p> <p>Unchanged: Encrypted files will be sent encrypted, plain files will be sent in plaintext. Users will not be prompted.</p> <p>Always ask: Users will be asked how to handle the attachments each time they send emails to the specified domain.</p> <p>Enter one or more domains for which the encryption method should be applied. Enter several domains separated by commas. Wildcards and partially specified domains are not supported.</p>

3.8.17.2 Authentication

Policy Setting	Explanation
The settings are shown as they appear in the SafeGuard Enterprise Management Center.	
Access <p>User may only boot from internal hard disk</p>	<p>This setting is only supported by endpoints with an earlier SafeGuard Enterprise version than 6.1 installed. It was used to enable recovery by allowing the user to start the endpoint from external media. As of version 6.1 this setting does not have any effect on endpoints. For the recovery scenario concerned, you can use recovery with Virtual Clients, see the SafeGuard Enterprise 8 administrator help.</p> <p>Determines whether users may start the computer from the hard drive and/or another medium.</p> <p>YES: Users can only boot from the hard disk. The SafeGuard POA does not offer the option to start the computer with a floppy disk or other external media.</p> <p>NO: Users may start the computer from hard disk, floppy disk or external medium (USB, CD etc.)</p>

Policy Setting	Explanation
Logon Options	
Logon mode	<p>Determines how users need to authenticate themselves at the SafeGuard POA.</p> <ul style="list-style-type: none"> • User ID/Password Users have to log on with their user name and password. • Token The user can only log on to the SafeGuard POA using a previously issued token or smartcard. This process offers a higher level of security. The user is requested to insert the token at logon. User identity is verified by token ownership and PIN presentation. After the user has entered the correct PIN, SafeGuard Enterprise automatically reads the data for user logon. <p>You can combine the settings User ID/Password and Token. To test whether logon using a token works, first select both settings. Only deselect the User ID/Password logon mode, if authentication using the token was successful. In order to switch between logon modes, allow users to log on once while the two settings are combined or they might run into a logon deadlock. You must also combine the two settings, if you want to allow Local Self Help for token logon.</p> <ul style="list-style-type: none"> • Fingerprint Select this setting to enable logon with Lenovo Fingerprint Reader. Users to whom this policy applies can then log on with a fingerprint or a user name and password. This procedure provides the maximum level of security. When logging on, users swipe their fingers over the fingerprint reader. Upon successful recognition of the fingerprint, the SafeGuard Power-on Authentication process reads the user's credentials and logs the user on to Power-on Authentication. The system then transfers the

Policy Setting	Explanation
	<p>credentials to Windows, and the user is logged on to the computer.</p> <p>After selecting this logon mode, the user can only log on with a pre-enrolled fingerprint or a user name and password. Token and fingerprint logon procedures cannot be combined on the same computer.</p>
Display unsuccessful logons for this user	<p>Yes: After logon at the SafeGuard POA and Windows, a dialog is shown containing information on the last failed logon (user name/date/time).</p>
Display last user logon	<p>Yes: After logon at the SafeGuard POA and Windows, a dialog is shown containing the following information of the last successful logon:</p> <ul style="list-style-type: none"> • User name • Logon date • Logon time • User credentials
Disable 'forced logoff' in workstation lock	<p>This setting only takes effect on endpoints with Windows XP. Windows XP is no longer supported as of SafeGuard Enterprise 6.1. This policy setting is still available in the SafeGuard Management Center to support SafeGuard Enterprise 6 clients managed with a 7.0 Management Center.</p> <p>If users wish to leave the endpoint for a short time only, they can click Block workstation to lock the computer for other users and unlock it with the user password.</p> <p>No: The user who has locked the computer as well as an administrator can unlock it. If an administrator unlocks the computer, the currently logged on user is logged off automatically.</p> <p>Yes: Only the user can unlock the computer. The administrator cannot unlock it and the user will not be logged off automatically.</p>

Policy Setting	Explanation
Activate user/domain preselection	<p>Yes: The SafeGuard POA saves the user name and domain of the last logged on user. Users therefore do not need to enter their user name every time they log on.</p> <p>No: The SafeGuard POA does not save the user name and the domain of the last logged on user.</p>
Service Account List	<p>To prevent administrative operations on a SafeGuard Enterprise protected endpoint leading to an activation of the Power-on Authentication and the addition of rollout operators as users to the endpoint, SafeGuard Enterprise allows you to create service account lists for Windows logon at SafeGuard Enterprise endpoints. The users listed are treated as SafeGuard Enterprise guest users.</p> <p>Before you select a list here you must first create the lists in the Policies navigation area under Service Account Lists.</p>
Pass through to Windows	<p>For the user to be able to grant other users access to their computer, the user has to be permitted to deactivate logon passthrough to Windows.</p> <ul style="list-style-type: none"> • Let user choose freely <p>The user can decide by selecting/deselecting this option in the SafeGuard POA logon dialog whether automatic logon at Windows is to be performed.</p> • Disable pass-through to Windows <p>After the SafeGuard POA logon, the Windows logon dialog will be displayed. The user has to log on to Windows manually.</p> • Enforce pass-through to Windows <p>The user will always be automatically logged on to Windows.</p>
BitLocker Options	

Policy Setting	Explanation
BitLocker Logon Mode for Boot Volumes	<p>The following options are available:</p> <ul style="list-style-type: none"> • Password: The user will be required to enter a password. • TPM: The key for logon is stored on the TPM (Trusted Platform Module) chip. • TPM + PIN: The key for logon is stored on the TPM chip and a PIN is also required for logon. • Startup Key: The key for logon is stored on a USB memory stick. • TPM + Startup Key: The key for logon is stored on the TPM chip and on a USB memory stick. Both are needed for logon. <p>To be able to use TPM + PIN, TPM + Startup Key or Startup Key enable the Group Policy Require additional authentication at startup either in Active Directory or on computers locally. In the Local Group Policy Editor (<code>gpedit.msc</code>) the Group Policy can be found here: Local Computer Policy\Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drive</p> <p>To use Startup Key you must also activate Allow BitLocker without a compatible TPM in the Group Policy.</p> <p>If the logon mode that is currently active on the system is an allowed fallback logon mode, the logon mode set here is not enforced.</p>
BitLocker Fallback Logon Mode for Boot Volumes	<p>If the setting defined as BitLocker Logon Mode for Boot Volumes cannot be applied, SafeGuard Enterprise offers the following alternatives for logon:</p> <ul style="list-style-type: none"> • Password: The user will be required to enter a password.

Policy Setting	Explanation
	<ul style="list-style-type: none"> • Startup Key: The key for logon is stored on a USB memory stick. • Password or Startup Key: USB memory sticks will be used only if passwords are not supported on the client operating system. • Error: An error message will be displayed and the volume will not be encrypted. <p>In the case of clients with version 6.1 or earlier the values Password or Startup Key and Password will be mapped to the old settings USB Memory Stick and Error.</p> <p>Passwords are only supported on Windows 8 or later.</p>
BitLocker Logon Mode for Non-Boot Volumes	<p>For non-boot volumes (fixed data drives) the following options are available:</p> <ul style="list-style-type: none"> • Auto-Unlock: If the boot volume is encrypted, an external key is created and stored on the boot volume. The non-boot volume(s) will then be encrypted automatically. They will be unlocked automatically using the auto-unlock functionality provided by BitLocker. Note that auto-unlock works only if the boot volume is encrypted. Otherwise the fallback mode will be used. • Password: The user will be prompted to enter a password for each non-boot volume. • Startup Key: The keys for unlocking the non-boot volumes are stored on a USB stick. <p>Clients with version 6.1 or earlier ignore this policy setting and they use the values defined for the logon mode for boot volumes instead. As the TPM cannot be used for non-boot volumes, USB memory stick or an error message will be used in such cases.</p>

Policy Setting	Explanation
BitLocker Fallback Logon Mode for Non-Boot Volumes	<p>Passwords are only supported on Windows 8 or later.</p> <p>If the logon mode that is currently active on the system is an allowed fallback logon mode, the logon mode set here is not enforced.</p> <p>If the setting defined as BitLocker Logon Mode for Non-Boot Volumes cannot be applied, SafeGuard Enterprise offers the following alternatives:</p> <ul style="list-style-type: none"> • Password: The user will be prompted to enter a password for each non-boot volume. • Startup Key: The keys are stored on a USB memory stick. • Password or Startup Key: USB memory sticks will be used only if passwords are not supported on the client operating system. <p>Clients with version 6.1 or earlier ignore this policy setting. They instead use the values defined for the fallback logon mode for boot volumes. As they cannot handle passwords, USB memory stick or error message will be used instead.</p> <p>Passwords are only supported on Windows 8 or later.</p>
Failed Logons	
Maximum no. of failed logons	<p>Determines how many times a user can attempt to log on using an invalid user name or password. After incorrectly entering a user name or password three times in a row for instance, a fourth attempt will lock the computer.</p>
Display "Logon failed" messages in POA	<p>Defines level of detail for messages on failed logons:</p>

Policy Setting	Explanation
	<ul style="list-style-type: none"> • Standard: Shows a short description. • Verbose: Displays more detailed information.
Token Options	
Action if token logon status is lost	<p>Defines behavior after removing the token from the computer:</p> <p>Possible actions include:</p> <ul style="list-style-type: none"> • Lock Computer • Present PIN dialog • No Action
Allow unblocking of token	Determines whether the token may be unblocked at logon.
Lock Options	
Lock screen after X minutes of inactivity	<p>Determines the time after which an unused desktop is automatically locked.</p> <p>The default value is 0 minutes, and the desktop will not be locked if this value is not changed.</p>
Lock screen at token removal	Determines whether the screen is locked if a token is removed during a session.
Lock screen after resume	Determines whether the screen is locked if the computer is reactivated from standby mode.

3.8.17.3 Syntax rules for PINs

In policies of the type **PIN**, you define settings for token PINs. These settings do not apply to PINs used for logon at BitLocker encrypted endpoints. For more information on BitLocker PINs see [PIN and passwords \(page 291\)](#).

PINs can contain numbers, letters and special characters (for example + - ; etc.). However, when issuing a new PIN, do not use any character with the combination ALT + < character > as this input mode is not available at SafeGuard Power-on Authentication.

 **Note** Define PIN rules either in the SafeGuard Management Center or in the Active Directory, not both.

Policy Setting	Explanation
The settings are shown as they appear in the SafeGuard Enterprise Management Center.	
PIN	
Min. PIN length	Specifies the number of characters a PIN must comprise when changed by the user. The required value can be entered directly or increased/reduced using the arrow buttons.
Max. PIN length	Specifies the maximum number of characters a PIN may comprise when changed by a user. The required value can be entered directly or increased/reduced using the arrow buttons.
Min. number of letters	These settings specify that a PIN must not consist exclusively of letters, numbers or special characters, but of a combination of at least two (for example 15flower). These settings only make sense if a minimum PIN length of greater than 2 has been defined.
Min. number of digits	
Min. number of special characters	
Keyboard row forbidden	Refers to keys arranged consecutively in rows on the keyboard such as "123" or "qwe". A maximum of two adjacent characters on the keyboard is allowed. Consecutive key sequences relate only to the alphanumerical keyboard area.
Keyboard column forbidden	Refers to keys arranged consecutively in columns on the keyboard such as "xsw2" or "3edc" (but not "xdr5" or "cft6"!). A maximum of two adjacent symbols in a single keyboard column is permitted. If you disallow keyboard columns, combinations like these are rejected as PINs. Consecutive key sequences relate only to the alphanumerical keyboard area.
Three or more consecutive characters forbidden	The activation of this option disallows key sequences <ul style="list-style-type: none"> • which are consecutive series of ASCII code symbols in both ascending and descending order ("abc" or "cba").

Policy Setting	Explanation
	<ul style="list-style-type: none"> • which consist of three or more identical characters ("aaa" or "111").
User name as PIN forbidden	<p>Determines whether user name and PIN may be identical.</p> <p>Yes: Windows user name and PIN must be different.</p> <p>No: Users may use their Windows user names as PINs.</p>
Use forbidden PIN list	<p>Determines whether certain character sequences must not be used for PINs. The character sequences are stored in the List of forbidden PINs (for example .txt file).</p>
List of forbidden PINs	<p>Defines character sequences which must not be used for PINs. If a user uses a forbidden PIN, an error message will be displayed.</p> <p>Prerequisite:</p> <p>A list (file) of forbidden PINs must be registered in the Management Center in the policies navigation area under Texts, see Create forbidden PIN lists for use in policies (page 250). The list is only available after registration.</p> <ul style="list-style-type: none"> • Maximum file size: 50 KB • Supported format: Unicode <p>Defining forbidden PINs</p> <p>In the list, forbidden PINs are separated by a line break.</p> <p><i>Wildcard:</i> Wildcard character "*" can represent any character and any number of characters in a PIN. Therefore *123* means that any series of characters containing 123 will be disallowed as a PIN.</p> <p>Note:</p> <ul style="list-style-type: none"> • If the list contains only a wildcard, the user will no longer be able to log on to the system after a forced password change. • Users must not be permitted to access the file.

Policy Setting	Explanation
	<ul style="list-style-type: none"> • Option Use forbidden PIN list must be activated.
Case sensitive	<p>This setting is only effective with Use forbidden PIN list and User name as PIN forbidden.</p> <p>Example 1: You have entered "board" in the list of forbidden PINs. If the Case sensitive option is set to Yes, additional PIN variants such as BOARD, BoaRD will not be accepted and logon will be denied.</p> <p>Example 2: "EMaier" is entered as a user name. If the Case sensitive option is set to Yes and the User name as PIN forbidden option is set to No, user EMaier cannot use any variant of this user name (for example "emaier" or "eMaiER") as a PIN.</p>
Changes	
PIN change after min. (days)	<p>Determines the period during which a PIN must not be changed. This setting prevents the user from changing a PIN too many times within a specific period.</p> <p>Example:</p> <p>User Miller defines a new PIN (for example "13jk56"). The minimum change interval for this user (or group to which this user is assigned) is set to five days. After two days the user wants to change the PIN to "13jk56". The PIN change is rejected because Mr. Miller may only define a new PIN after five days have passed.</p>
PIN change after max. (days)	<p>The user has to define a new PIN after the set period has expired. If the period is set to 999 days, no PIN change is required.</p>
Notify of forced change before (days)	<p>A warning message is displayed "n" days before PIN expiry reminding the user to change their PIN in "n" days. Alternatively, the user may change the PIN immediately.</p>
General	
Hide PIN in POA	<p>Specifies whether the digits entered are hidden when entering PINs. If enabled, nothing is shown when PINs are entered in the POA. Otherwise, PINs are shown masked with asterisks.</p>
PIN history length	<p>Determines when previously used PINs can be reused. It makes sense to define the history length in conjunction with the PIN change after max. (days) setting.</p> <p>Example:</p>

Policy Setting	Explanation
	<p>The PIN history length for user Miller is set to 4, and the number of days after which the user must change their PIN is 30. Mr. Miller is currently logging on using the PIN "Informatics". After the 30 day period expires, he is asked to change his PIN. Mr. Miller types in "Informatics" as the new PIN and receives an error message that this PIN has already been used and he needs to select a new PIN. Mr. Miller cannot use the PIN "Informatics" until after the fourth request to change the PIN (in other words PIN history length = 4).</p>

Create forbidden PIN lists for use in policies

For policies of the type **PIN** a list of forbidden PINs can be created to define character sequences which must not be used in PINs. PINs are used for token logon. For further information, see [Tokens and smartcards \(page 177\)](#).

The text files containing the required information have to be created before you can register them in the SafeGuard Management Center. The maximum file size for text files is **50 KB**. SafeGuard Enterprise only uses Unicode UTF-16 coded texts. If you create the text files in another format, they will be automatically converted when they are registered.

 **Note** In the lists, forbidden PINs are separated by a line break.

To register text files:

1. In the policy navigation area, right-click **Texts** and select **New > Text**.
2. Enter a name for the text to be displayed in the **Text item name** field.
3. Click [...] to select the text file previously created. If the file needs to be converted, a message will be displayed.
4. Click **OK**.

The new text item is displayed as a subnode below **Texts** in the policy navigation area. If you select a text item, its contents are displayed in the window on the right-hand side. The text item can now be selected when creating policies.

Proceed as described to register further text items. All registered text items are shown as subnodes.

 **Note** Using the **Modify Text** button, you can add new text to existing text. When clicking this button, a dialog is displayed for selecting another text file. The text contained in this file is appended to the existing text.

3.8.17.4 Syntax rules for passwords

In policies of type **Password**, you define rules for passwords used to log on to the system. These settings do not apply to passwords used for logon at BitLocker encrypted endpoints. For more information on BitLocker passwords see [PIN and passwords \(page 291\)](#).

Passwords can contain numbers, letters and special characters (for example + - ; etc.). However, when issuing a new password, do not use any character with the combination ALT + <character> as this input mode is not available at SafeGuard Power-on Authentication. Rules for passwords used to log on to the system are defined in policies of the type **Password**.

 **Note** To enforce a strong password policy, see [Security recommendations \(page 410\)](#) as well as the *SafeGuard Enterprise manual for certification-compliant operation*.

The enforcement of password rules and password history can only be guaranteed if the SGN credential provider is used consistently. Define password rules either in the SafeGuard Management Center or in the Active Directory, not both.

Policy setting	Explanation
The settings are shown as they appear in the SafeGuard Enterprise Management Center.	
Password	
Min. password length	Specifies the number of characters a password must comprise when changed by the user. The required value can be entered directly or increased/reduced using the arrow buttons.
Max. password length	Specifies the maximum number of characters a password may comprise when changed by a user. The required value can be entered directly or increased/reduced using the arrow buttons.
Min. number of letters	These settings specify that a password must not consist exclusively of letters, numbers or special characters, but of a combination of at least two (for example 15flower). These settings only make sense if a minimum password length of greater than 2 has been defined.
Min. number of digits	
Min. number of special characters	
Keyboard row forbidden	Refers to keys arranged consecutively in rows on the keyboard such as "123" or "qwe". A maximum of two adjacent characters on the keyboard is allowed. Consecutive key sequences relate only to the alphanumerical keyboard area.
Keyboard column forbidden	Refers to keys arranged consecutively in columns on the keyboard such as "xsw2" or "3edc" (but not "xdr5" or "cft6"!). A maximum of two adjacent symbols in a single keyboard column is permitted. If you disallow keyboard columns, combinations like these are rejected as passwords. Consecutive key sequences relate only to the alphanumerical keyboard area.

Policy setting	Explanation
Three or more consecutive characters forbidden	<p>The activation of this option disallows key sequences</p> <ul style="list-style-type: none"> • which are consecutive series of ASCII code symbols in both ascending and descending order ("abc" or "cba"). • which consist of three or more identical characters ("aaa" or "111").
User name as password forbidden	<p>Determines whether user name must not be used as a password.</p> <p>Yes: Windows user name and password must be different.</p> <p>No: Users may use their Windows user names as passwords.</p>
Use forbidden password list	<p>Determines whether certain character sequences must not be used for passwords. The character sequences are stored in the List of forbidden passwords (for example .txt file).</p>
List of forbidden passwords	<p>Defines character sequences which must not be used for passwords. If a user uses a forbidden password, an error message will be displayed.</p> <p>A list (file) of forbidden passwords must be registered in the SafeGuard Management Center in the policies navigation area under Texts, see Create forbidden password list for use in policies (page 255). The list is only available after registration.</p> <p>Maximum file size: 50 KB</p> <p>Supported format: Unicode</p> <p>Defining forbidden passwords</p> <p>In the list, forbidden passwords are separated by a line break. <i>Wildcard:</i> The wildcard character "*" can represent any character and any number of characters in a password. Therefore *123* means that any series of characters containing 123 will be disallowed as a password.</p> <p>Note:</p> <ul style="list-style-type: none"> • If the list contains only a wildcard, the user will no longer be able to log on to the system after a forced password change.

Policy setting	Explanation
	<ul style="list-style-type: none"> Users must not be permitted to access the file. Option Use forbidden password list must be activated.
Case sensitive	<p>This setting is only effective with Use forbidden password list and User name as password forbidden.</p> <p>Example 1: You have entered "board" in the list of forbidden passwords. If the Case sensitive option is set to Yes, additional password variants such as BOARD, BoaRD will not be accepted and logon will be denied.</p> <p>Example 2: "EMaier" is entered as a user name. If the Case sensitive option is set to Yes and the User name as password forbidden option is set to No, user EMaier cannot use any variant of this user name (for example "emaier" or "eMaiER") as a password.</p>
Changes	
Password change allowed after min. (days)	<p>Determines the period during which a password may not be changed. This setting prevents the user from changing a password too many times within a specific period. If the user is forced to change their password by Windows or if the user changes their password after a warning message has been displayed stating that the password will expire in x days, this setting will not be evaluated!</p> <p>Example:</p> <p>User Miller defines a new password (for example "13jk56"). The minimum change interval for this user (or group to which this user is assigned) is set to five days. After two days the user wants to change the password to "13jk56". The password change is rejected because user Miller may only define a new password after five days have passed.</p>
Password expires after (days)	<p>If you set this option, the user has to define a new password after the set period has expired.</p>
Notify of forced change before (days)	<p>A warning message is displayed "n" days before password expiry reminding the user to change their password in "n" days. Alternatively, the user may change the password immediately.</p>
General	
Hide password in POA	<p>Specifies whether the characters entered are hidden when entering passwords. If enabled, nothing is shown when</p>

Policy setting	Explanation
	passwords are entered in the POA. Otherwise, passwords are shown masked with asterisks.
Password history length	<p>Determines when previously used passwords can be reused. It makes sense to define the history length in conjunction with the Password expires after (days) setting.</p> <p>Example:</p> <p>The password history length for user Miller is set to 4, and the number of days after which the user must change their password is 30. Mr. Miller is currently logging on using the password "Informatics". After the 30 day period expires, he is asked to change his password. Mr. Miller types in "Informatics" as the new password and receives an error message that this password has already been used and he needs to select a new password. Mr. Miller cannot use the password "Informatics" until after the fourth request to change the password (in other words password history length = 4).</p> <p> Note If you set the password history length to 0, the user can set the old password as the new password. This is not good practice and should be avoided.</p>
User password synchronization to other SGN Clients	<p>This field determines the procedure of synchronizing passwords when users, who work on several SafeGuard Enterprise endpoints and are defined as users on these endpoints, change their passwords. The following options are available:</p> <ul style="list-style-type: none"> • Slow (wait for user to log on) <p>If a user changes their password on a SafeGuard Enterprise endpoint and intends to log on to another endpoint on which the user is also registered, they have to log on using their old password at the SafeGuard Power-on Authentication first. Password synchronization will only be performed after logging on using the old password first.</p> <ul style="list-style-type: none"> • Fast (wait for machine to connect) <p>If a user changes their password on a SafeGuard Enterprise endpoint, password synchronization with other endpoints, on which the user is also registered, will be performed as soon as the other endpoint has established</p>

Policy setting	Explanation
	a connection to the server. This is for example the case, when another user, who is also registered as a user on the endpoint, logs on to the endpoint in the meantime.

Create forbidden password list for use in policies

For policies of type **Password**, you can create a list of forbidden passwords to define character sequences that must not be used in passwords.

 **Note** In the lists, forbidden passwords are separated by line breaks.

The text files containing the required information have to be created before you can register them in the SafeGuard Management Center. The maximum file size for text files is **50 KB**. SafeGuard Enterprise only uses Unicode UTF-16 coded texts. If you create the text files in another format, they will be automatically converted when they are registered.

If a file is converted, a message is displayed.

To register text files:

1. In the policy navigation area, right-click **Texts** and select **New > Text**.
2. Enter a name for the text to be displayed in the **Text item name** field.
3. Click [...] to select the text file previously created. If the file needs to be converted, a message will be displayed.
4. Click **OK**.

The new text item is displayed as a subnode below **Texts** in the policy navigation area. If you select a text item, its contents are displayed in the window on the right-hand side. The text item can now be selected when creating policies.

Proceed as described to register further text items. All registered text items are shown as subnodes.

 **Note** Use the **Modify Text** button to add new text to existing text. When you click this button, a dialog is displayed for selecting another text file. The text contained in this file is appended to the existing text.

3.8.17.5 Passphrase for SafeGuard Data Exchange

The user must enter a passphrase which is used to generate local keys for secure data exchange with SafeGuard Data Exchange. The keys generated on the endpoints are also stored in the SafeGuard Enterprise Database. In policies of the type **Passphrase**, you define the relevant requirements.

For details of SafeGuard Data Exchange, see [SafeGuard Data Exchange \(page 322\)](#).

For further details of SafeGuard Data Exchange and SafeGuard Portable on the endpoint refer to the *SafeGuard Enterprise user help*, chapter *SafeGuard Data Exchange*.

Policy Setting	Explanation
The settings are shown as they appear in the SafeGuard Enterprise Management Center.	
Passphrase	
Min. passphrase length	Defines the minimum number of characters for the passphrase from which the key is generated. The required value can be entered directly or increased/reduced using the arrow keys.
Max. passphrase length	Defines the maximum number of characters for the passphrase. The required value can be entered directly or increased/reduced using the arrow keys.
Min. number of letters	This setting specifies that a passphrase must not consist exclusively of letters, numbers or symbols, but of a combination of that least two (for example 15flower). These settings only make sense if a minimum passphrase length of greater than 2 has been defined.
Min. number of digits	
Min. number of special characters	
Keyboard row forbidden	Refers to keys arranged consecutively in rows on the keyboard such as "123" or "qwe". A maximum of two adjacent characters on the keyboard is allowed. Consecutive key sequences relate only to the alphanumerical keyboard area.
Keyboard column forbidden	Refers to keys arranged consecutively in columns on the keyboard such as "xsw2" or "3edc" (but not "xdr5" or "cft6"!). A maximum of two adjacent characters in a single keyboard column is permitted. If you disallow keyboard columns, these combinations are rejected for passphrases. Consecutive key sequences relate only to the alphanumerical keyboard area.
Three or more consecutive characters forbidden	<p>The activation of this option disallows key sequences</p> <ul style="list-style-type: none"> • which are consecutive series of ASCII code symbols in both ascending and descending order ("abc" or "cba"). • which consist of three or more identical characters ("aaa" or "111").
User name as passphrase forbidden	<p>Determines whether the user name and passphrase may be identical.</p> <p>Yes: Windows user name and passphrase must be different.</p> <p>No: Users may use their Windows user names as passphrases.</p>

Policy Setting	Explanation
Case sensitive	<p>This setting is effective when User name as passphrase forbidden is active.</p> <p>Example: "EMaier" is entered as a user name. If the option Case sensitive is set to YES and User name as passphrase forbidden is set to NO, user EMaier cannot use any variant of this user name (for example emaier or eMaiER) as a passphrase.</p>

3.8.17.6 Whitelists for Device Protection policies for file-based encryption

In the SafeGuard Management Center, you can select whitelists as targets for policies of the type **Device Protection** for file-based encryption. This allows you to create encryption policies for specific device models or even for distinct devices.

Before you select a whitelist as a target for a **Device Protection** policy, you have to create and register it in the SafeGuard Management Center. You can define whitelists for specific storage device models (for example iPod or USB devices from a specific vendor) or for distinct storage devices according to serial number. You can add the devices to whitelists manually or use the results of a Safend Auditor scan. For further information, refer to the *Safend Auditor documentation*.

Afterwards, you can select the whitelist as a target when you create a **Device Protection** policy.

 **Note** If you select a whitelist as a target for a policy of the type **Device Protection**, you can only select **File-Based** or **No Encryption** as the **Media encryption mode**. If you select **No Encryption** for a **Device Protection** policy with a whitelist, this policy does not exclude a device from encryption, if another policy applies that specifies volume-based encryption.

 **Note** For SafeStick devices from BlockMaster special requirements apply. These devices have different IDs for administrators and users without administrator privileges. For consistent handling within SafeGuard Enterprise, you must add both IDs to whitelists. SafeGuard PortAuditor detects both IDs, if a SafeStick device has been opened at least once on the computer scanned by SafeGuard PortAuditor.

Create whitelists for Device Protection policies for file-based encryption

1. In the **Policies** navigation area, select **Whitelist**.
2. In the context menu of **Whitelist**, click **New > Whitelist**.
3. Select the whitelist type:
 - To create a whitelist for specific device models, select **Storage Device Models**.
 - To create a whitelist for specific devices according to serial number, select **Distinct Storage Devices**.
4. Under **Source of Whitelist**, specify how you want to create the whitelist:

- To enter devices manually, select **Create Whitelist manually**.

When you click **OK**, an empty whitelist is opened in the SafeGuard Management Center. In this empty whitelist, you can create entries manually. To add a new entry, click the green **Add (Insert)** icon in the SafeGuard Management Center toolbar.

 **Note** To retrieve the relevant strings for a device with the Windows Device Manager, open the **Properties** window for the device and look at the values for the **Hardware IDs** and **Device Instance Path** properties. Only the following interfaces are supported: USB, 1394, PCMCIA and PCI.

- If you want to use the result of a scan of endpoints by Safend Auditor as a source, select **Import from Safend Auditor Result**.

The results of the Safend Auditor scan have to be available (XML file), if you want to create the whitelist based on this source. To select the file, click the [...] button.

For further information refer to the *Safend Auditor documentation*.

Click **OK**, to display the contents of the imported file in the SafeGuard Management Center.

The whitelist is displayed under **Whitelists** in the **Policies** navigation area. You can select it when you create policies of the type **Device Protection** for file-based encryption.

Select whitelists as targets for Device Protection policies for file-based encryption

Prerequisite: The required whitelist must have been created in the SafeGuard Management Center.

1. In the navigation area of the SafeGuard Management Center, click **Policies**.
2. In the navigation window, right-click **Policy Items** and select **New**.
3. Select **Device Protection**.

A dialog for naming the new policy is displayed.

4. Enter a name and optionally a description for the new policy.
5. Under **Device protection target**, select the relevant whitelist:
 - If you have created a whitelist for storage device models, it is displayed under **Storage Device Models**.

- If you have created a whitelist for distinct storage devices, it is displayed under **Distinct Storage Devices**.

6. Click **OK**.

The whitelist has been selected as a target for the **Device Protection** policy. After the policy has been transferred to the endpoint, the encryption mode selected in the policy applies.

3.8.17.7 Device Protection

Policies of type **Device Protection** cover the settings for data encryption on different data storage devices. Encryption can be volume- or file-based with different keys and algorithms. Policies of type **Device Protection** also include settings for SafeGuard Data Exchange, SafeGuard Cloud Storage and SafeGuard Portable. For further information, see [SafeGuard Data Exchange \(page 322\)](#) and [Cloud Storage \(page 315\)](#). For further details on SafeGuard Data Exchange, SafeGuard Cloud Storage and SafeGuard Portable on the endpoint, refer to the *SafeGuard Enterprise user help*.

When creating a policy for device protection, you first have to specify the target for device protection. Possible targets are:

- Internal storage (boot volumes or non-boot volumes)
- Removable media on Windows endpoints

For macOs a policy of type **File Encryption** with the placeholder <Removables> as **Path** is required to encrypt files on removable media, see [Placeholders for paths in location-based File Encryption rules \(page 306\)](#).

- Optical drives
- Drive letters
- Storage device models
- Distinct storage devices
- Cloud Storage definitions

For each target, create a separate policy.

 **Note** Removable media: A policy that specifies volume-based encryption of removable drives and allows the user to choose a key from a list (for example **Any key in user key ring**) can be circumvented by the user by not choosing a key. To make sure that removable drives are always encrypted, either use a file-based encryption policy, or explicitly set a key in the volume-based encryption policy.

Policy Setting	Explanation
<p>The settings are shown as they appear in the SafeGuard Enterprise Management Center.</p>	
<p>Media encryption mode</p>	<p>Used to protect devices (PCs, notebooks and so on) and all types of removable media.</p> <p>This setting is mandatory.</p> <p>The primary objective is to encrypt all data stored on local or external storage devices. The transparent operating method enables users to continue to use their usual applications, for example Microsoft Office.</p> <p>Transparent encryption means that all encrypted data (whether in encrypted directories or volumes) is automatically decrypted in the main memory as soon as it is opened in a program. A file is automatically re-encrypted when it is saved.</p> <p>The following options are available:</p> <ul style="list-style-type: none"> • No encryption • Volume-based (= transparent, sector-based encryption) <p>Ensures that all data is encrypted (incl. boot files, swapfiles, idle files/hibernation files, temporary files, directory information etc.) without the user having to change normal operating procedures or consider security.</p> <ul style="list-style-type: none"> • File-based (= transparent, file-based encryption, Smart Media Encryption) <p>Ensures that all data is encrypted (apart from Boot Medium and directory information) with the benefit that even optical media such as CD/DVD can be encrypted or data can be swapped with external computers on which SafeGuard Enterprise is not installed (provided policies permit).</p> <p>For policies with whitelists, only No encryption or File-based can be selected.</p>

Policy Setting	Explanation
<p>The settings are shown as they appear in the SafeGuard Enterprise Management Center.</p>	
<p>General Settings</p>	
<p>Algorithm to be used for encryption</p>	<p>Sets the encryption algorithm.</p> <p>List of all usable algorithms with respective standards:</p> <p>AES256: 32 bytes (256 bits)</p> <p>AES128: 16 bytes (128 bits)</p>
<p>Key to be used for encryption</p>	<p>Defines which key is used for encryption. You can define specific keys (for example machine key or a defined key) or you can allow the user to select a key. You can also restrict the keys which a user is allowed to use.</p> <p>The following options are available:</p> <ul style="list-style-type: none"> • Any key in user key ring <p>All keys from a user's key ring are displayed and the user can select any one of them.</p> <p>This option has to be selected, if you define a policy for file-based encryption for an unmanaged endpoint protected by SafeGuard Enterprise (standalone).</p> <ul style="list-style-type: none"> • Any key in user key ring, except user key <p>All except user keys from a user's key ring are displayed and the user can select any one of them.</p> <ul style="list-style-type: none"> • Any group key in user key ring <p>All group keys from a user's key ring are displayed and the user can select any one of them.</p> <ul style="list-style-type: none"> • Defined machine key <p>The machine key is used and the user cannot select a key.</p>

Policy Setting	Explanation
<p>The settings are shown as they appear in the SafeGuard Enterprise Management Center.</p>	
	<p>It is only available on an endpoint that has volume-based encryption installed (BitLocker or SafeGuard Full Disk Encryption).</p> <p>A policy defining the Defined machine key as the key to be used for file-based encryption (for example for SafeGuard Data Exchange) will not become effective on an endpoint without volume-based encryption. The data cannot be encrypted.</p> <p>This option has to be selected, if you define a policy for volume-based encryption for an unmanaged endpoint protected by SafeGuard Enterprise (standalone mode). If you nevertheless select Any key in user key ring and the user selects a locally created key for volume-based encryption, access to this volume will be denied.</p> <ul style="list-style-type: none"> • Any key in key ring, except locally created keys <p>All except locally generated keys from a key ring are displayed and the user can select any one of them.</p> <ul style="list-style-type: none"> • Defined key on list <p>The administrator can select any available key when setting policies in the Management Center.</p> <p>The key has to be selected under Defined key for encryption.</p> <p>Policies for unmanaged endpoint protected by SafeGuard Enterprise (standalone):</p> <p>Only the Any key in user key ring option can be used when creating policies for unmanaged endpoints. In addition, creating local keys must be allowed for this type of endpoint computer.</p> <p>If the media passphrase feature is activated for unmanaged endpoints, the Media Encryption Key is automatically used as Defined key for encryption, since no group keys are available on unmanaged endpoints. Selecting another key under Defined</p>

Policy Setting	Explanation
	<p>The settings are shown as they appear in the SafeGuard Enterprise Management Center.</p> <p>key for encryption when creating a removable media policy for unmanaged endpoints will have no effect.</p>
Defined key for encryption	<p>Click [...] to display the Find Keys dialog. Click Find now to search for keys and select a key from the list displayed.</p> <p>In the case of a policy of the type Device Protection with target Removable Media this key is used to encrypt the Media Encryption Key when the media passphrase functionality is enabled (User may define a passphrase for devices set to Yes).</p> <p>For this policy type you must configure both settings Key to be used for encryption and Defined key for encryption.</p> <p>Policies for unmanaged endpoints protected by SafeGuard Enterprise (standalone):</p> <p>If the media passphrase feature is activated for unmanaged endpoints, the Media Encryption Key is automatically used as Defined key for encryption, since no group keys are available on unmanaged endpoints.</p>
User is allowed to create a local key	<p>This setting determines whether users can generate a local key on their computers or not. The default setting is Yes, users are allowed to create local keys.</p> <p>A policy that forbids users to create local keys (User is allowed to create a local key set to No) will only be applied on Windows endpoints.</p> <p>Local keys are generated on the endpoint based on a passphrase entered by the user. The passphrase requirements can be set in policies of the type Passphrase.</p> <p>These keys are also saved in the database. The user can use them on any endpoint they are logged on to.</p> <p>Local keys can be used for secure data exchange with SafeGuard Data Exchange (SG DX). For more information, see Local keys (page 328).</p>

Policy Setting	Explanation
<p>The settings are shown as they appear in the SafeGuard Enterprise Management Center.</p>	
<p>Volume-Based Settings</p>	
<p>Users may add or remove keys to or from encrypted volume</p>	<p>Yes: Endpoint users may add/remove keys to/from a key ring. The dialog is displayed from the context menu command Properties/Encryption tab.</p> <p>No: Endpoint users may not add additional keys.</p>
<p>Reaction to unencrypted volumes</p>	<p>Defines how SafeGuard Enterprise handles unencrypted media.</p> <p>The following options are available:</p> <ul style="list-style-type: none"> • Reject (= text medium is not encrypted) • Accept only blank media and encrypt • Accept all media and encrypt
<p>User may decrypt volume</p>	<p>Allows the user to decrypt the volume with a context menu command in Windows Explorer.</p>
<p>Fast initial encryption</p>	<p>Select this setting to enable the fast initial encryption mode for volume-based encryption. This mode reduces the time needed for initial encryption on endpoints.</p> <p>This mode may lead to a less secure state. For further information, see the SafeGuard Enterprise 8 administrator help.</p>
<p>Proceed on bad sectors</p>	<p>Specifies whether encryption should proceed or be stopped if bad sectors are detected. The default setting is Yes.</p>
<p>File-Based Settings</p>	
<p>Initial encryption of all files</p>	<p>Automatically starts initial encryption for a volume after user logon. The user may need to select a key from the key ring beforehand.</p>

Policy Setting	Explanation
The settings are shown as they appear in the SafeGuard Enterprise Management Center.	
User may cancel initial encryption	Enables the user to cancel initial encryption.
User is allowed to access unencrypted files	Defines whether a user may access unencrypted data on a volume.
User may decrypt files	Enables the user to decrypt individual files or whole directories (with the Windows Explorer extension <right-click>).
User may define a media passphrase for devices	Enables the user to define a media passphrase on their computers. The media passphrase makes it possible to easily access all local keys used on computers without SafeGuard Data Exchange with SafeGuard Portable.
Copy SafeGuard Portable to target	<p>If this option is selected, SafeGuard Portable is copied to any removable media connected to the endpoint and any synchronization folder defined in a Cloud Storage Definition for SafeGuard Cloud Storage as soon as content is written to the encrypted media or folder.</p> <p>SafeGuard Portable enables the exchange of encrypted data with removable media or cloud storage without the recipient having SafeGuard Enterprise installed.</p> <p>The recipient can decrypt and re-encrypt the encrypted files using SafeGuard Portable and the corresponding passphrase. The recipient can re-encrypt files with SafeGuard Portable or use the original key for encryption.</p> <p>SafeGuard Portable does not have to be installed or copied to the recipient's computer but can be used directly from the removable media or cloud storage synchronization folder.</p>
Default initial encryption key	<p>This field offers a dialog for selecting a key which is used for file-based initial encryption. If you select a key here, the user cannot select a key when initial encryption starts. Initial encryption starts without user interaction.</p> <p>The key selected will always be used for initial encryption.</p>

Policy Setting	Explanation
<p>The settings are shown as they appear in the SafeGuard Enterprise Management Center.</p>	
	<p>Example:</p> <p>Prerequisite: A default key for initial encryption has been set.</p> <p>When the user connects a USB device to the computer, initial encryption automatically starts. The key defined is used. The user does not have to interfere. If the user afterwards wants to re-encrypt files or save new files on the USB device, they can select any key (if allowed and available). If the user connects a different USB device, the key defined for initial encryption will be used again. This key will also be used for all encryption processes that follow until the user explicitly selects a different key.</p> <p>If the media passphrase feature is activated, this option will be deactivated. The Defined key for encryption will be used.</p>
Plaintext folder	<p>The folder specified here will be created on all removable media, mass storage devices and cloud storage synchronization folder. Files that are copied to this folder will always stay plaintext.</p>
User is allowed to decide about encryption	<p>You can allow users to decide about encryption of files on removable media (Windows only) and mass storage devices:</p> <ul style="list-style-type: none"> • If you set this option to Yes, users are prompted to decide whether data should be encrypted. For mass storage devices, the prompt is displayed after each logon, for removable media the prompt is displayed when they plug in removable media. • If you set this option to Yes, remember user settings, users can select the option Remember this setting and do not show this dialog again to have their choice remembered for the relevant device. In this case, the dialog will not be displayed for the relevant device again. <p>If the user selects No in the dialog displayed on the endpoint, neither initial nor transparent encryption occurs.</p>

3.8.17.8 Specific machine settings - basic settings

Policy Settings	Explanation
The settings are shown as they appear in the SafeGuard Enterprise Management Center.	
Power-On Authentication (POA) Enable Power-on Authentication	<p>Defines whether the SafeGuard POA is switched on or off.</p> <p>⚠ Important For security reasons we strongly recommend that you keep the SafeGuard POA switched on. Deactivating the SafeGuard POA reduces the system security to Windows logon security and increases the risk of unauthorized access to encrypted data.</p>
Access denied if no connection to the server (days) (0 = no check)	<p>Refuses SafeGuard POA logon if there was no connection between endpoint and server for longer than the set period.</p>
Secure Wake on LAN (WOL)	<p>With Secure Wake on LAN (WOL) settings you can prepare endpoints for software rollouts. If the relevant Wake on LAN settings apply to endpoints, the necessary parameters (for example SafeGuard POA deactivation and a time interval for Wake on LAN) are transferred directly to the endpoints where parameters are analyzed.</p> <p>⚠ Important Deactivating the SafeGuard POA - even for a limited number of boot processes - reduces the security of your system!</p> <p>For further information on Secure Wake on LAN, see the SafeGuard Enterprise 8 administrator help.</p>
Number of auto logons	<p>Defines the number of restarts while SafeGuard Power-on Authentication is switched off for Wake on LAN.</p> <p>This setting temporarily overwrites the Enable Power-on Authentication setting until the automatic logons reach the preset number. SafeGuard Power-on Authentication is then reactivated.</p> <p>If you set the number of automatic logons to two and Enable Power-on Authentication is active,</p>

Policy Settings	Explanation
	<p>the endpoint starts twice without authentication through the SafeGuard POA.</p> <p>For Wake on LAN, we recommend that you allow three more restarts than necessary for your maintenance operations to overcome any unforeseen problems.</p>
Allow local Windows logon during WOL	Determines whether local Windows logons are permitted during Wake on LAN.
Start of time slot for external WOL start	Date and time can be either selected or entered for the start and end of the Wake on LAN (WOL).
End of time slot for external WOL start	<p>Date format: <i>MM/DD/YYYY</i></p> <p>Time format: <i>HH:MM</i></p> <p>The following input combinations are possible:</p> <ul style="list-style-type: none"> Defined start and end of WOL. End of WOL is defined, start is open. No entries: no time interval has been set.
	<p>For a planned software rollout, you should set the time frame for the WOL such that the scheduling script can be started early enough to allow all endpoints sufficient time for starting.</p> <p>WOLstart: The starting point for the WOL in the scheduling script must be within the time interval set in the policy. If no interval is defined, WOL is not locally activated on the SafeGuard Enterprise protected endpoint. WOLstop: This command is carried out irrespective of the final point set for the WOL.</p>
User Machine Assignment (UMA) Forbid SGN Guest user to logon	<p> Note This setting only applies to managed endpoints.</p>

Policy Settings	Explanation
Allow registration of new SGN users for	<p>Defines whether guest users can log on to Windows on the endpoint.</p> <p>Note Microsoft accounts are always handled as SafeGuard Enterprise guest users.</p>
	<p>Defines who is able to import another SGN user into the SafeGuard POA and/or UMA (by disabling the pass-through to the operating system).</p> <p>Note For endpoints that do not have the Device Encryption module installed, the Allow registration of new SGN users for setting must be set to Everybody if it should be possible on the endpoint to add more than one user to the UMA with access to their key ring. Otherwise users can only be added in the Management Center. This setting is only evaluated on managed endpoints. For more information, see Sophos knowledge base article 110659.</p>
Enable registration of SGN Windows Users	<p>If the setting is set to Nobody, the POA does not become active at all. Users will need to be assigned manually in the Management Center.</p>
	<p>Defines whether SGN Windows users can be registered on the endpoint. An SGN Windows user is not added to the SafeGuard POA, but has a key ring for accessing encrypted files, just as an SGN user. If you select this setting, all users, that would have otherwise become SGN guest users, will become SGN Windows users. The users are added to the UMA as soon as they have logged on to Windows.</p>
Enable manual UMA cleanup for standalone endpoints	<p>Note This setting only applies to unmanaged endpoints.</p>
	<p>Defines whether users may delete SGN users and SGN Windows users from the User Machine Assignment. If you select Yes, the command User Machine Assignments is available from the system tray icon menu on the endpoint. This command shows a list of users who can log on at the SafeGuard Power-on Authentication as SGN</p>

Policy Settings	Explanation
Maximum number of SGN Windows users before automatic cleanup	<p>users and at Windows as SGN Windows users. In the dialog displayed, users can be removed from the list. After SGN users or SGN Windows users have been removed, they can no longer log on at the SafeGuard Power-on Authentication or at Windows.</p> <p> Note This setting only applies to managed endpoints.</p> <p>With this setting you can activate an automatic cleanup of SafeGuard Enterprise Windows users on managed endpoints. As soon as the threshold you set here is exceeded by one SafeGuard Enterprise Windows user, all existing SafeGuard Enterprise Windows users except the new one are removed from the User Machine Assignment. The default value is 10.</p>
Display Options	
Display machine identification	<p>Displays either the computer name or a defined text in the SafeGuard POA title bar.</p> <p>If the Windows network settings include the computer name, this is automatically incorporated into the basic settings.</p>
Machine identification text	<p>The text to be displayed in the SafeGuard POA title bar.</p> <p>If you have selected Defined name in the Display machine identification field, you can enter the text in this input field.</p>
Display legal notice	<p>Displays a text box with a configurable content which is displayed before authentication in the SafeGuard POA. In some countries a text box with certain content must be displayed by law.</p> <p>The box needs to be confirmed by the user before the system continues.</p> <p>Before you specify a text, the text has to be registered as a text item under Texts in the Policies navigation area.</p>
Legal notice text	<p>The text to be displayed as a legal notice.</p>

Policy Settings	Explanation
	In this field, you can select a text item registered under Texts in the Policies navigation area.
Display additional information	<p>Displays a text box with a configurable content which appears after the legal notice (if activated).</p> <p>You can define whether the additional information is displayed</p> <ul style="list-style-type: none"> • Never • Every system start • Every logon <p>Before you specify a text, the text has to be registered as a text item under Texts in the Policies navigation area.</p>
Additional information text	<p>The text to be displayed as additional information.</p> <p>In this field, you can select a text item registered under Texts in the Policies navigation area.</p>
Display additional information period	<p>In this field you can define how long (in seconds) additional information is to be displayed.</p> <p>You can specify the number of seconds after which the text box for additional information is closed automatically. The user can close the text box at any time by clicking OK.</p>
Enable and show the system tray icon	<p>The SafeGuard Enterprise System Tray Icon allows the user to access all user functions quickly and easily on the endpoint. In addition, information about the endpoint status (new policies received etc.) can be displayed in balloon tool tips.</p> <p>Yes:</p> <p>The system tray icon is displayed in the information area of the taskbar and the user is continually informed through balloon tool tips</p>

Policy Settings	Explanation
	<p>about the status of the SafeGuard Enterprise protected endpoint.</p> <p>No:</p> <p>The system tray icon is not displayed. No status information for the user by balloon tool tips.</p> <p>Silent:</p> <p>The system tray icon is displayed in the information area of the taskbar but there is no status information for the user through balloon tool tips.</p>
Show overlay icons in Explorer	Defines whether Windows key symbols will be shown to indicate the encryption status of volumes, devices, folders and files.
Virtual Keyboard in POA	Defines whether a virtual keyboard can be shown on request in the SafeGuard POA dialog for entering the password.
Installation Options	
Uninstallation allowed	Determines whether uninstallation of SafeGuard Enterprise is allowed on the endpoints. When Uninstallation allowed is set to No , SafeGuard Enterprise cannot be uninstalled, even by a user with administrator rights, while this setting is active within a policy.
Enable Sophos tamper protection	<p>Activates/deactivates Sophos Tamper Protection. If you have allowed uninstallation of SafeGuard Enterprise in the policy setting Uninstallation allowed, you can set this policy setting to Yes, to ensure that uninstallation attempts are checked by Sophos Tamper Protection to prevent casual removal of the software.</p> <p>If Sophos Tamper Protection does not allow uninstallation, any uninstallation attempts will be canceled.</p> <p>If Enable Sophos Tamper Protection is set to No, uninstallation of SafeGuard Enterprise will not be checked or prevented by Sophos Tamper Protection.</p>

Policy Settings	Explanation
	 Note This setting only applies to endpoints using Sophos Endpoint Security and Control from version 9.5.
Credential Provider Settings	
Credential Provider wrapping	<p>You can configure SafeGuard Enterprise to use a different Credential Provider than the Windows Credential Provider. Templates for supported Credential Providers can be downloaded from www.sophos.com. To get a list of templates for tested Credential Providers and the location to download from please contact Sophos Support.</p> <p>You can import a template and deploy it to endpoints by using the Credential Provider policy setting. To do so click Import template and browse for the template file. The imported template and its content are displayed in the Credential Provider multiline field and set as policy.</p> <p>To remove a template click Clear template.</p> <p> Note Do not edit the template files provided. If the XML structure of these files is changed, the settings may not be recognized on the endpoint and the default Windows Credential Provider may be used instead.</p> <p>Configuration typically requires project support from Sophos Professional Services. Please contact Sophos Support.</p>
Token Support Settings	
Token middleware module name	<p>Registers the PKCS#11 Module of a token.</p> <p>The following options are available:</p> <ul style="list-style-type: none"> • ActiveIdentity ActivClient • ActiveIdentity ActivClient (PIV) • AET SafeSign Identity Client • Aladdin eToken PKI Client

Policy Settings	Explanation
	<ul style="list-style-type: none"> • a.sign Client • ATOS CardOS API • Charismatics Smart Security Interface • Estonian ID-Card • Gemalto Access Client • Gemalto Classic Client • Gemalto .NET Card • IT Solution trustware CSP+ • Módulo PKCS#11 TC-FNMT • Nexus Personal • RSA Authentication Client 2.x • RSA Smart Card Middleware 3.x • Siemens CardOS API • T-Systems NetKey 3.0 • Unizeto proCertum • Custom PKCS#11 settings... • If you select Custom PKCS#11 settings... the Custom PKCS#11 settings are enabled. <p>You can then enter the module names to be used:</p> <ul style="list-style-type: none"> ◦ PKCS#11 module for Windows

Policy Settings	Explanation
	<ul style="list-style-type: none"> ◦ PKCS#11 module for SafeGuard Power-on Authentication <p> Note If you install Nexus Personal or Gemalto .NET Card middleware, you also need to add their installation path to the PATH environment variable of your computer's System Properties.</p> <ul style="list-style-type: none"> • Default installation path for Gemalto .NET Card: C:\Program Files\ Gemalto \PKCS11 for .NET V2 smart cards • Default installation path for Nexus Personal: C:\Program Files\Personal \bin <p>Licenses:</p> <p>Note that the use of the respective middleware for the standard operating system requires a license agreement with the relevant manufacturer. For more information, see Sophos knowledge base article 116585.</p> <p>For Siemens licenses contact:</p> <p>Atos IT Solutions and Services GmbH Otto-Hahn-Ring 6 D-81739 Muenchen Germany</p>
Services to wait for	This setting is used for problem solving with specific tokens. Our Support team will provide corresponding settings as required.

3.8.17.9 Logging for Windows endpoints

Events for SafeGuard Enterprise can be logged in the Windows Event Viewer or in the SafeGuard Enterprise Database. To specify the events to be logged and their destination, create a policy of the type **Logging** and select the required events by clicking on them.

Many different events from different categories (for example Authentication, Encryption, etc.) are available for selection. We recommend that you define a strategy for logging, and determine the events necessary according to reporting and auditing requirements.

For further information, see [Reports \(page 208\)](#).

3.8.18 Repair a corrupted Management Center installation

A corrupted SafeGuard Management Center installation can easily be repaired, if the database is still intact. In this case, reinstall the SafeGuard Management Center and use the existing database as well as the backed up Master Security Officer certificate.

- The company and Master Security Officer certificates of the relevant database configuration must have been exported to .p12 files. The data must be available and valid.
- The passwords for the .p12 file as well as for the certificate store must be known to you.

To repair a corrupted SafeGuard Management Center installation:

1. Reinstall the SafeGuard Management Center installation package. Open the SafeGuard Management Center. The Configuration Wizard is started automatically.
2. In **Database Connection**, select the relevant database server and configure the connection to the database if required. Click **Next**.
3. In **Database Settings** click **Select an available database** and select the relevant database from the list.
4. In **Security Officer Data**, do either of the following:
 - If the backed up certificate file can be found on the computer, it is displayed. Enter the password you use for authenticating at SafeGuard Management Center.
 - If the backed up certificate file cannot be found on the computer, select **Import**. Browse for the backed up certificate file and click **Open**. Enter the password for the selected certificate file. Click **Yes**. Enter and confirm the password for authenticating at the SafeGuard Management Center.
5. Click **Next**, and then **Finish** to complete the SafeGuard Management Center configuration.

The corrupted SafeGuard Management Center installation is repaired.

3.8.19 Troubleshooting

3.8.19.1 Error codes

SGMERR codes in Windows event log

You will see the following message in the Windows event log:

"Authorization for SafeGuard Enterprise Administration failed for user... Reason:
SGMERR[536870951]"

See the table below for the definition of number "536870951". Number "536870951" means for example "Incorrect PIN entered. Unable to authenticate user".

Error ID	Display
0	OK
21	Internal error found
22	Module not initialized
23	File I/O Error detected
24	Cache cannot be assigned
25	File I/O Read error
26	File I/O Write error
50	No operation carried out
101	General error
102	Access denied
103	File already exists
1201	Registry entry could not be opened.
1202	Registry entry could not be read.
1203	Registry entry could not be written.
1204	Registry entry could not be removed.
1205	Registry entry could not be created.
1206	Access to a system service or driver was not possible.
1207	A system service or driver could not be added in the registry.
1208	A system service or driver could not be removed from the registry.
1209	An entry for a system service or driver already exists in the registry.
1210	No access to the Service Control Manager.
1211	An entry in the registry for a session could not be found.
1212	A registry entry is invalid or wrong
1301	Access to a drive has failed.
1302	No information about a volume available.
1303	Access to a volume failed.
1304	Invalid option defined.
1305	Invalid file system type.
1306	Existing file system on a volume and the defined file system differ.
1307	Existing cluster size used by a file system and the defined cluster size differ.
1308	Invalid sector size used by a file system defined.

Error ID	Display
1309	Invalid start sector defined.
1310	Invalid partition type defined.
1311	An unfragmented, unused area of required size could not be found on a volume.
1312	File system cluster could not be marked as used.
1313	File system cluster could not be marked as used.
1314	File system cluster could not be marked as GOOD.
1315	File system cluster could not be marked as BAD.
1316	No information about clusters of a file system available.
1317	Area marked as BAD could not be found on a volume.
1318	Invalid size of a volume area defined.
1319	MBR sector of a hard disk could not be replaced.
1330	Wrong command for an allocation or deallocation defined.
1351	Invalid algorithm defined.
1352	Access to system kernel has failed.
1353	No system kernel is installed.
1354	An error occurred accessing the system kernel.
1355	Invalid change of system settings.
1401	Writing data to a drive has failed
1402	Reading data from a drive has failed.
1403	Access to a drive has failed.
1404	Invalid drive defined.
1405	Changing position on a drive has failed.
1406	Drive is not ready.
1407	Unmount of a drive has failed.
1451	File could not be opened.
1452	File could not be found.
1453	Invalid file path defined.
1454	File could not be created.
1455	File could not be copied.
1456	No information about a volume available.
1457	Position in a file could not be changed.
1458	Reading data from a file has failed.
1459	Writing data to a file has failed.
1460	A file could not be removed.
1461	Invalid file system
1462	File could not be closed.
1463	Access to a file is not allowed.
1501	Not enough memory available.
1502	Invalid or wrong parameter defined.
1503	Data buffer size exceeded
1504	A DLL module could not be loaded.
1505	A function or process was aborted.

Error ID	Display
1506	No access allowed.
1510	No system kernel installed.
1511	A program could not be started.
1512	A function, an object or data are not available.
1513	Invalid entry detected.
1514	An object already exists.
1515	Invalid function call.
1516	An internal error has occurred.
1517	An access violation has occurred.
1518	Function or mode is not supported.
1519	Uninstallation has failed.
1520	An exception error has occurred.
1550	The MBR sector of the hard disk could not be replaced.
2850	Scheduler service stopped due to an exception.
2851	Scheduler task executed successfully.
2852	Scheduler task failed.
2853	Scheduler task created or modified.
2854	Scheduler task deleted.
20001	Unknown
20002	Process terminated
20003	File not verified
20004	Invalid policy
30050	Failed to open command.
30051	Not enough memory
30052	General failure of process communication
30053	A resource is temporarily unavailable. This is a temporary condition and later attempts to access it may complete normally.
30054	General communication failure
30055	Unexpected return value
30056	No card reader attached
30057	Buffer overflow
30058	Card has no power
30059	A timeout has occurred
30060	Invalid card type
30061	The requested functionality is not supported at this time / under this OS / in this situation etc
30062	Invalid driver
30063	This software cannot use the firmware of the connected hardware.
30064	Failed to open file
30065	File not found
30066	Card not inserted
30067	Invalid argument

Error ID	Display
30068	The semaphore is currently in use
30069	Semaphore is temporarily in use
30070	General failure.
30071	You currently do not have the rights to perform the requested action. Usually a password has to be presented in advance
30072	The service is currently not available
30073	An item (for example a key with a specific name) could not be found
30074	The password presented is incorrect.
30075	The password has been presented incorrectly several times, and is therefore locked. Usually use a suitable administrator tool to unblock it.
30076	The identity does not match a defined cross-check identity
30077	Multiple errors have occurred. Use this error code if it is the only way of obtaining an error code when various different errors have occurred.
30078	There are still items left, therefore for example the directory structure etc. cannot be deleted.
30079	Error during consistency check
30080	The ID is on a blacklist, so the requested action is not allowed.
30081	Invalid handle
30082	Invalid configuration file
30083	Sector not found.
30084	Entry not found.
30085	No more sections
30086	End of file reached.
30087	The specified item already exists.
30088	The password is too short.
30089	The password is too long.
30090	An item (for example a certificate) has expired.
30091	The password is not locked.
30092	Path not be found.
30093	The directory is not empty.
30094	No more data
30095	The disk is full
30096	An operation has been aborted.
30097	Read only data; a write operation failed
12451840	The key is unavailable.
12451842	The key is not defined.
12451842	Access to unencrypted medium denied.
12451843	Access to unencrypted medium denied unless it is empty.
352321637	The file is not encrypted.
352321638	The key is unavailable.
352321639	The correct key is unavailable.
352321640	Checksum error in file header

Error ID	Display
352321641	Error in CBI function.
352321642	Invalid file name.
352321643	Error when reading/writing temporary file.
352321644	Access to unencrypted data is not allowed.
352321645	Key Storage Area (KSA) full.
352321646	The file has already been encrypted with another algorithm.
352321647	The file has been compressed with NTFS and so cannot be encrypted.
352321648	File is encrypted with EFS!
352321649	Invalid file owner!
352321650	Invalid file encryption mode!
352321651	Error in CBC operation!
385875969	Integrity breached.
402653185	The token contains no credentials.
402653186	Credentials cannot be written to the token.
402653187	TDF tag could not be created.
402653188	TDF tag does not contain the required data.
402653189	The object already exists on the token.
402653190	No valid slot found.
402653191	Unable to read serial number
402653192	Token encryption has failed.
402653193	Token decryption has failed.
536870913	The key file contains no valid data.
536870914	Parts of the RSA key pair are invalid.
536870915	Failed to import the key pair.
536870916	The key file format is invalid.
536870917	No data available.
536870918	Certificate import failed.
536870919	The module has already been initialized.
536870920	The module has not been initialized.
536870921	The ASN.1 encryption is corrupt.
536870922	Incorrect data length.
536870923	Incorrect signature.
536870924	Incorrect encryption mechanism applied.
536870925	This version is not supported.
536870926	Padding error.
536870927	Invalid flags.
536870928	The certificate has expired and is no longer valid.
536870929	Incorrect time entered. Certificate not yet valid.
536870930	The certificate has been withdrawn.
536870931	The certificate chain is invalid.
536870932	Unable to create the certificate chain.
536870933	Unable to contact CDP.

Error ID	Display
536870934	A certificate which can be used only as the final data unit has been used as CA or vice versa.
536870935	Problems with validity of certificate length in the chain.
536870936	Error opening file.
536870937	Error reading a file.
536870938	Error or several parameters which have been assigned to the function are incorrect.
536870939	Function output exceeds cache.
536870940	Token problem and/or slot breached.
536870941	Token has insufficient memory to perform the required function.
536870942	Token was removed from slot while function being performed.
536870943	The required function could be performed but information on the cause of this error is not available.
536870945	The computer on which the CBI compilation is taking place has insufficient memory to perform the required function. This function may be only partly completed.
536870946	A required function is not supported by the CBI compilation.
536870947	An attempt has been made to set a value for an object which cannot be set or altered.
536870948	Invalid value for object.
536870949	An attempt to obtain the value of an object has failed because the object is either sensitive or inaccessible.
536870950	The PIN entered has expired. (Whether a normal user's PIN runs on an issued token varies from one to another).
536870951	The PIN entered is incorrect. Unable to authenticate user.
536870952	The PIN entered contains invalid characters. This response code is applied only for those attempting to set up a PIN.
536870953	The PIN entered is too long/short. This response code is applied only for those attempting to set up a PIN.
536870954	The selected PIN is blocked and cannot be used. This happens when a certain number of attempts are made to authenticate a user and the token refuses any further attempts.
536870955	Invalid Slot ID.
536870956	The token was not in the slot at the time of the request.
536870957	The CBI archive/slot failed to recognize the token in the slot.
536870958	The requested action cannot be carried out because the token is write-protected.
536870959	The entered user cannot be logged on because this user is already logged on to a session.
536870960	The entered user cannot be logged on because another user is already logged onto the session.
536870961	The required action cannot be performed because there is no matching user logged on. One example is that a session cannot be logged off while one is still logged on.

Error ID	Display
536870962	The normal user PIN has not been initialized with CBIInitPin.
536870963	An attempt made by several different users to log on to the same token simultaneously has been allowed.
536870964	Invalid value entered as CBIUser. Valid types are defined in user types.
536870965	An object with the designated ID could not be found on the token.
536870966	Operation has timed out.
536870967	This version of IE is not supported.
536870968	Authentication failed.
536870969	The basic certificate is secured.
536870970	No CRL found.
536870971	No active internet connection.
536870972	Certificate time-value error.
536870973	Unable to verify the selected certificate.
536870974	Certificate expiry status unknown.
536870975	The module has exited. No further requests.
536870976	An error has occurred during request for network function.
536870977	An invalid request for a function has been received.
536870978	Unable to find an object.
536870979	A terminal server session has been interrupted.
536870980	Invalid operation.
536870981	The object is in use.
536870982	The random number generator has not been initialized. (CBIRNDInit () not requested.)
536870983	Unknown command (see CBIControl ()).
536870984	UNICODE is not supported.
536870985	More seed needed for random number generator.
536870986	Object already exists
536870987	Incorrect algorithm combination. (See CBIRecrypt ()).
536870988	The Cryptoki module (PKCS#11) has not been initialized.
536870989	The Cryptoki module (PKCS#11) has been initialized.
536870990	Unable to load Cryptoki module (PKCS#11).
536870991	Certificate not found.
536870992	Not trusted.
536870993	Invalid key.
536870994	The key cannot be exported.
536870995	The algorithm entered is temporarily not supported.
536870996	The decryption mode entered is not supported.
536870997	GSENC compilation error.
536870998	Data request format not recognized.
536870999	The certificate has no private key.
536871000	Bad system setting.
536871001	There's an operation active

Error ID	Display
536871002	A certificate in the chain is not properly time nested.
536871003	The CRL could not be replaced
536871004	The USER pin has already been initialized
805306369	You do not have sufficient rights to perform this action. Access denied!
805306370	Invalid operation
805306371	Invalid parameter in use
805306372	Object already exists
805306373	The object could not be found.
805306374	Database Exception
805306375	The action has been cancelled by the user.
805306376	The token is not assigned to a specific user.
805306377	The token is assigned to more than one user.
805306378	The token could not be found in the database.
805306379	The token has been successfully deleted and removed from the database.
805306380	Unable to identify the token in the database.
805306381	The policy is assigned to a policy group. Remove assignment before deleting policy.
805306382	The policy is assigned to an OU. Please remove assignment first.
805306383	The certificate is invalid for this Officer.
805306384	The certificate has expired for this Officer.
805306385	The Officer could not be found in the database.
805306386	The selected Officer is not unique.
805306387	The Officer is blocked and cannot be authenticated.
805306388	The Officer is no longer or not yet valid.
805306389	Unable to authorize Officer - request outside office hours.
805306390	Responsible party cannot delete self.
805306391	The Master Security Officer cannot be deleted because a second Master Security Officer is needed for additional authentication.
805306392	The Security Officer cannot be deleted because a second Security Officer is required for additional authentication.
805306393	The checking Officer cannot be deleted because a second checking Officer is required for additional authentication.
805306394	The recovery Officer cannot be deleted because a second recovery Officer is required for additional authentication.
805306395	The advisory Officer cannot be deleted because a second advisory Officer is required for additional authentication.
805306396	The Master Security Officer function cannot be deleted because a second Master Security Officer is needed for additional authentication.
805306397	The Security Officer function cannot be deleted because a second Security Officer is needed for additional authentication.
805306398	The checking Officer function cannot be deleted because a second checking Officer is needed for additional authentication.

Error ID	Display
805306399	The recovery Officer function cannot be deleted because a second recovery Officer is needed for additional authentication.
805306400	The advisory Officer function cannot be deleted because a second advisory Officer is needed for additional authentication.
805306401	There is no additional Officer with the required function available for additional authentication.
805306402	Event log
805306403	Integrity of central event log successfully verified.
805306404	Integrity breached! One or more events have been removed from the start of the chain.
805306405	Integrity breached! One or more events have been removed from the chain. The message at which point the break in the chain was discovered has been highlighted.
805306406	Integrity breached! One or more events have been removed from the end of the chain.
805306407	Failed to export events to file. Reason:
805306408	The current view contains unsaved data. Do you want to save changes before exiting this view?
805306409	The file could not be loaded or the file is damaged. Reason:
805306410	The integrity of the log has been breached! One or more events have been removed.
805306411	Save events to a file before deleting?
805306412	Job display
805306413	Several CRL found in database: Unable to delete CRL.
805306414	CRL not found in database:
805306415	Unable to find the user to whom the certificate should have been assigned to in the database.
805306416	A P7 Blob is urgently required for a certificate assignment.
805306417	The user to whom the certificate should have been assigned is not uniquely named.
805306418	Unfortunately unable to find certificate assignment.
805306419	Certificate assignment not unique. Unclear which certificate to remove.
805306420	Unable to find the user for whom the certificate is to be produced in the database.
805306421	The user to whom the certificate is to be assigned cannot be uniquely named.
805306422	The certificate has already been assigned to another user. A certificate can only be assigned to one user.
805306423	Unable to find the machine to which the certificate is to be assigned in the database.
805306424	The machine to assign the certificate could not be uniquely identified.
805306425	Imported certificates cannot be extended by SGN.
805306426	Inconsistent certificate data
805306427	The extension of the certificate has not been approved by a Security Officer.

Error ID	Display
805306428	Error deleting token
805306429	Certificate cannot be deleted by the token because it has been used to authorize the present user.
805306430	System access already exists with this name. Please select another name.
805306431	The Security Officer does not have any roles assigned. Logon not possible.
805306432	The license is violated.
805306433	No license was found.
805306435	Missing or invalid log file path.
2415919104	No policy found.
2415919105	No configuration file available!
2415919106	No connection to server.
2415919107	No more data.
2415919108	Invalid priority used for sending to server!
2415919109	More data pending.
2415919110	Auto registration pending.
2415919111	Database authentication failed!
2415919112	Wrong session ID!
2415919113	Data packet dropped!
3674210305	Domain not found.
3674210306	Machine not found.
3674210307	User not found.
3758096385	The password does not contain enough letters
3758096386	The password does not contain enough numbers
3758096387	The password does not contain enough special characters
3758096388	The password is the same as the user name
3758096389	The password contains consecutive characters
3758096390	The password is too similar to the user name
3758096391	The password has been found in a list of prohibited passwords
3758096392	The password is too similar to the old password
3758096393	The password includes a keyboard sequence with more than two characters
3758096394	The password includes a keyboard column with more than two characters
3758096395	The password is not yet valid
3758096396	A password has expired
3758096397	The password has not yet reached its minimum validity period
3758096398	The password has exceeded its maximum validity period
3758096399	Information must be displayed about an impending change to the password
3758096400	Must be changed at first log on
3758096401	The password has been found in the history
3758096402	Error when verifying against specified blacklist.
4026531840	No "platform" found.
4026531841	No document.
4026531842	XML Parse Error.

Error ID	Display
4026531843	Document Object Model (XML) Error
4026531844	No <DATAROOT> tag found.
4026531845	XML tag not found.
4026531846	"nostream" error.
4026531847	"printtree" error.

BitLocker error codes

BitLocker errors are reported using the following SafeGuard events:

- Kernel initialization has failed. Internal code: <Error code>.
- Sector-based initial encryption of drive <drive letter> failed and closed. Reason: <Error code>

The following table provides a list of error codes for BitLocker:

Error code (Hex)	Error code (Dec)	Description
0x00000000 – 0x000032C8	0 – 15999	See Microsoft System Error Codes
0x00BEB001	12496897	Encryption not possible due to error during kernel initialization.
0x00BEB002	12496898	Boot manager must not be on the system volume to be encrypted.
0x00BEB003	12496899	Found an unsupported Windows version on the HDD. Minimum is Windows Vista.
0x00BEB004	12496900	The configured authentication method is not supported.
0x00BEB005	12496901	The PIN dialog has not been completed successfully.
0x00BEB006	12496902	The path dialog has not been completed successfully.
0x00BEB007	12496903	Error in inter-process communication in PIN or path dialog.
0x00BEB008	12496904	Unhandled exception in PIN or path dialog. The dialog was displayed, but the user logged off or stopped it with the Task Manager.
0x00BEB009	12496905	The encryption algorithm defined in the policy does not match the one of the encrypted drive. By default (if not modified) native BitLocker uses AES-128 whereas the SGN policies define AES-256.
0x00BEB00A	12496906	The volume is a dynamic volume. Dynamic volumes are not supported.
0x00BEB00B	12496907	The hardware test failed because of a hardware problem.
0x00BEB00C	12496908	An error occurred during TPM initialization and activation.
0x00BEB00D	12496909	The Encryption-Algorithm in the SGN-Policy conflicts with the Encryption-Algorithm settings in the GPO.
0x00BEB00E	12496910	Sector-based initial encryption of drive <drive letter> failed.

0x00BEB00F	12496911	Active Directory backup of recovery keys is required but no domain controller is available.
0x00BEB010	12496912	Active Directory backup of recovery keys is not compatible with BitLocker Challenge/Response.
0x00BEB102	12497154	UEFI version could not be validated and therefore BitLocker will be executed in legacy mode.
0x00BEB202	12497410	Client configuration package has not yet been installed.
0x00BEB203	12497411	UEFI version not supported and therefore BitLocker will be executed in legacy mode. Minimum requirement is 2.3.1.
0x80280006	-2144862202	The TPM is inactive.
0x80280007	-2144862201	The TPM is disabled.
0x80280014	-2144862188	The TPM already has an owner.
0x80310037	-2144272329	The Group Policy setting requiring FIPS compliance prevents a local recovery password from being generated and written to the key backup file. Encryption will nevertheless continue.
0x8031005B	-2144272293	The Group Policy for the specified authentication method is not set. Please enable the Group Policy "Require additional authentication at startup".
0x8031005E	-2144272290	The Group Policy for encryption without TPM is not set. Please enable the Group Policy "Require additional authentication at startup" and set the checkbox "Allow BitLocker without a compatible TPM" within it.
0x80280000 –	-2144862208 –	See Microsoft COM Error Codes (TPM, PLA, FVE) .
0x803100CF	-2144272177	

4. Managing Windows endpoints

General restrictions

Note the following general restrictions for SafeGuard Enterprise on endpoints:

- SafeGuard Enterprise for Windows does not support Apple hardware and cannot be installed in a Boot Camp environment. Instead, use a virtual Windows client.
- The SafeGuard full disk encryption (SafeGuard volume-based encryption and BitLocker support) modules do not support systems that are equipped with hard drives attached through an SCSI bus.
- **Fast User switching** is not supported.
- Operating SafeGuard Enterprise in a terminal server environment is not supported.
- When using Intel Advanced Host Controller Interface (AHCI) on endpoints with POA, we recommend using slot 0 for the boot hard disk.
- On Endpoints with POA, SafeGuard volume-based encryption for volumes that are located on Dynamic Disks and on GUID Partition Table disks (GPT) is not supported. In such cases, installations are terminated. If such disks are found on the endpoint, they are not supported.
- If you want to use SafeGuard volume-based encryption on endpoints with multiple physical disks, you must install the encryption software on the first disk.
- SafeGuard Full Disk Encryption is only available for Windows 7 BIOS endpoints. If you use Windows 7 UEFI or a newer version of Windows, make use of the integrated Windows BitLocker Drive Encryption functionality. For more information refer to [Manage BitLocker Drive Encryption \(page 289\)](#).

For information on SafeGuard Enterprise Full Disk Encryption, see the [SafeGuard Enterprise 8 administrator help](#).

4.1 *Manage BitLocker Drive Encryption*

For the fastest, easiest and most reliable full disk encryption, SafeGuard Enterprise takes advantage of the technology built into the operating system. Seamlessly manage keys and recovery functions on BitLocker- encrypted drives from the SafeGuard Management Center.

BitLocker Drive Encryption is a full disk encryption feature with pre-boot authentication included with Microsoft's Windows operating systems. It is designed to protect data by providing encryption for boot and data volumes. For Windows 8 and later, BitLocker Drive Encryption must be used for full disk encryption instead of SafeGuard Full Disk Encryption.

SafeGuard Enterprise can manage BitLocker encryption on a computer. BitLocker encryption can be activated and the management of drives already encrypted with BitLocker can be taken over.

During installation on the endpoint and the first reboot, SafeGuard Enterprise determines whether the hardware meets the requirements for BitLocker with SafeGuard Challenge/Response. If not, SafeGuard Enterprise BitLocker management is run without Challenge/Response. In this case the BitLocker recovery key can be retrieved using the SafeGuard Management Center.

4.1.1 Authentication with BitLocker Drive Encryption

BitLocker Drive Encryption offers a range of authentication options, for boot volumes as well as for non-boot volumes.

The security officer can set the various logon modes in a policy in the SafeGuard Management Center and distribute it to the BitLocker endpoints.

The following logon modes exist for SafeGuard Enterprise BitLocker users:

- **TPM:** The key for logon is stored on the TPM (Trusted Platform Module) chip.
- **TPM + PIN:** The key for logon is stored on the TPM chip and a PIN is also required for logon.
- **Startup Key:** The key for logon is stored on a USB memory stick.
- **TPM + Startup Key:** The key for logon is stored on the TPM chip and on a USB memory stick. Both are needed for logon.
- **Password:** The user will be required to enter a password.
- **Password or Startup Key:** USB memory sticks will be used only if passwords are not supported on the client operating system.
- **Auto-Unlock:** If the boot volume is encrypted, an external key is created and stored on the boot volume. The non-boot volume(s) will then be encrypted automatically. They will be unlocked automatically using the auto-unlock functionality provided by BitLocker.

For more information on setting logon modes in a policy, please see [Authentication \(page 239\)](#).

4.1.1.1 Trusted Platform Module (TPM)

TPM is a smartcard-like module on the motherboard performing cryptographic functions and digital signature operations. It can create, store and manage user keys. It is protected against attacks.

4.1.1.2 PIN and passwords

Requirements for BitLocker PINs and passwords are defined by Windows Group Policies, not by SafeGuard Enterprise settings.

Passwords are only supported with Windows 8 or higher.

The relevant settings for passwords can be found in the Local Group Policy Editor (**gpedit.msc**):

Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives > Configure use of passwords for operating system drives and

Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Fixed Data Drives > Configure use of passwords for fixed data drives.

The settings can also be applied via Active Directory based Group Policy Objects (GPOs).

By default, SafeGuard Enterprise allows enhanced PINs. This means that users can use all keyboard characters such as numbers, letters, and special characters/symbols.

BitLocker supports the EN-US keyboard layout only. Therefore, users might have problems when entering enhanced PINs or complex passwords. Unless they changed their keyboard layout to EN-US before they specified their new BitLocker PIN or password, users may need to press a different key to what is displayed on their keyboard in order to enter the character they want. Therefore, before encrypting the boot volume, a reboot is performed to ensure that the user can enter the PIN or password correctly at boot time.

As of Windows 10 RS2, the minimum length of the PIN is 6 characters.

4.1.2 Best practice: Policy settings and user experience

The security officer configures encryption policies for the drives to be encrypted as well as an authentication policy. The TPM should be used whenever possible, but even without a TPM the boot volume should be encrypted. User interaction should be kept to a minimum.

According to these requirements, the security officer chooses the following authentication settings (these are also the default settings):

- **BitLocker Logon Mode for Boot Volumes: TPM + PIN**
- **BitLocker Fallback Logon Mode for Boot Volumes: Password or Startup Key**
- **BitLocker Logon Mode for Non-Boot Volumes: Auto-Unlock**
- **BitLocker Fallback Logon Mode for Non-Boot Volumes: Password or Startup Key**

The security officer creates a device protection policy with the target **Internal Storage** and sets the encryption mode to **Volume based**. Afterwards both policies are applied to the endpoints to be encrypted.

For SafeGuard Enterprise BitLocker users the following scenarios exist:

Case 1: A user logs on to an endpoint with a TPM.

1. The user is asked to enter a PIN for the boot volume (for example drive C:).
2. The user enters the PIN and clicks **Restart and Encrypt**.
3. The system tests the hardware and checks whether the user can enter the PIN correctly. It reboots and asks the user to enter the PIN.
 - If the user enters the PIN correctly, the endpoint starts.
 - If the user does not enter the PIN correctly (for example because of a wrong keyboard layout) the user can press the **Esc** key in the BitLocker pre-boot environment to cancel the test and the endpoint starts.
 - If there is any problem with the hardware (for example if the TPM is not working), the test aborts and the endpoint starts.
4. The user logs on again.
5. If the hardware test was passed successfully (the user could enter the PIN correctly and there was no problem with the TPM), the encryption of the boot volume starts. Otherwise (if the test failed), an error is shown and the volume is not encrypted. If the test failed because the user pressed **Esc** in the pre-boot environment, the user is asked to enter a PIN again and to do a restart (as in step 2; steps 3, 4, 5 will be repeated).
6. The encryption of the boot volume starts.
7. The encryption of the data volumes starts as well, without requiring any user interaction.

Case 2: A user logs on to a Windows 8 endpoint without a TPM.

1. The user is asked to enter a password for the boot volume.
2. The user enters the password and clicks **Restart and Encrypt**.
3. The system reboots, tests the hardware and the user logs on again as in the case above (exactly as in steps 3 to 6 of case 1, but the references to the TPM are not relevant, and a password is required rather than a PIN).
4. The encryption of the boot volume starts.
5. The encryption of the data volumes starts as well, without requiring any user interaction.

Case 3: A user logs on to a Windows 7 endpoint without a TPM.

1. The user is asked to save the encryption key for the boot volume to a USB memory stick.
2. The user attaches a USB memory stick and presses **Save and Restart**.
3. The system reboots, performs the hardware test and the user logs on again. (Same procedure as in the previous cases, but the user has to provide the USB memory stick at boot time.)

An additional hardware error could be that the USB memory stick cannot be read from the BitLocker pre-boot environment.)

4. The encryption of the boot volume starts.
5. The encryption of the data volumes starts as well, without requiring any user interaction.

Case 4: The security officer changes the policy setting **BitLocker Fallback Logon Mode for Boot Volumes to Password**. A user logs on to a Windows 7 endpoint without a TPM.

1. Since the endpoint has no TPM and Windows 7 does not allow passwords for boot volumes, the boot volume will not be encrypted.
2. For each non-boot volume, the user is asked to store the external key on a USB memory stick. Encryption of the respective volume starts when the user clicks **Save**.
3. When the user reboots the endpoint, the USB key has to be plugged in to be able to unlock the non-boot volumes.

4.1.3 Prerequisites for managing BitLocker on endpoints

- To be able to use logon methods **TPM + PIN**, **TPM + Startup Key**, **Startup Key**, or **Password**, the Group Policy **Require additional authentication at startup** either in Active Directory or on computers locally must be enabled. In the Local Group Policy Editor (gpedit.msc), the Group Policy can be found here:

Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives

To use **Startup Key**, you must activate **Allow BitLocker without a compatible TPM** in the Group Policy.

- To use **TPM + PIN** on tablets, the Group Policy **Enable use of BitLocker authentication requiring preboot keyboard input on slates** must be activated.

 **Note**

These Group Policies are enabled automatically at installation on the endpoint. Make sure that the settings are not overwritten by different Group Policies.

- A BitLocker device protection policy which triggers the configuration of a TPM-based authentication mechanism (for example **TPM**, **TPM + PIN**, **TPM + Startup Key**) will automatically initiate TPM activation. The user is informed that the TPM needs to be activated and is informed if the system needs to be rebooted or shut down, depending on the TPM in use.

 **Note**

If SafeGuard BitLocker management is installed on an endpoint **Not prepared** may be displayed as the encryption state of a drive, see [Drives tab \(page 126\)](#). This indicates that the drive currently cannot be encrypted with BitLocker since necessary preparations have not been done yet. This only applies to managed endpoints since unmanaged endpoints cannot report inventory data.

With the SGNState command line tool (administrative rights necessary), you can check whether the endpoint is properly prepared for BitLocker encryption. In some cases, the Windows BitLocker Drive Preparation Tool must be run.

4.1.3.1 SafeGuard Challenge/Response for BitLocker

In order to use SafeGuard Enterprise BitLocker Challenge/Response the following requirements must be met:

- 64-bit Windows
- UEFI version 2.3.1 or newer
- Microsoft UEFI certificate is available or Secure Boot is disabled
- NVRAM boot entries accessible from Windows
- Windows installed in GPT mode
- The hardware is not listed in the POACFG.xml file.

Sophos delivers a default POACFG.xml file embedded in the setup. It is recommended to download the newest file and provide it to the installer.

During installation on the endpoint and the first reboot, SafeGuard Enterprise determines whether the hardware meets the requirements for BitLocker with SafeGuard Challenge/Response. If not, SafeGuard Enterprise BitLocker management is run without Challenge/Response. In this case, the BitLocker recovery key can be retrieved using the SafeGuard Management Center.

4.1.4 Manage BitLocker Drive Encryption with SafeGuard Enterprise

SafeGuard Enterprise's central and fully transparent management of BitLocker can be used in heterogeneous IT environments. SafeGuard Enterprise enhances BitLocker capabilities significantly.

Security policies for BitLocker can be centrally rolled out thanks to SafeGuard Enterprise. Even critical processes such as key management and key recovery are available when BitLocker is managed with SafeGuard Enterprise.

With SafeGuard Enterprise, you can manage BitLocker Drive Encryption from the SafeGuard Management Center. As a security officer, you can set encryption and authentication policies and distribute them to the BitLocker endpoints.

Once a BitLocker endpoint is registered in the SafeGuard Management Center, information on user, computer, logon mode, and encryption status is displayed. Events are logged for BitLocker endpoints as well.

In terms of management functionality, endpoints encrypted with BitLocker are equal to endpoints encrypted with SafeGuard Full Disk Encryption. You can find out the type of a computer in the **Inventory** section in **Users and Computers**. The column **Encryption Type** tells you if a computer is a BitLocker endpoint.

 **Note** During installation of the SafeGuard Enterprise client on Windows 7, the **BitLocker** feature needs to be explicitly selected to enable BitLocker management.

For information on BitLocker To Go and SafeGuard Enterprise, see [BitLocker To Go \(page 299\)](#).

4.1.5 Encrypting with BitLocker managed by SafeGuard Enterprise

With BitLocker Drive Encryption support in SafeGuard Enterprise you can encrypt boot volumes as well as non-boot volumes with BitLocker encryption and keys. Additionally, any data, for example removable media, can be encrypted with SafeGuard Enterprise file-based encryption and SafeGuard Enterprise keys. This is not a BitLocker feature but provided by SafeGuard Enterprise.

For logged events, see [Auditing \(page 204\)](#).

4.1.5.1 BitLocker encryption keys

When encrypting the boot volume or other volumes with BitLocker through SafeGuard Enterprise, the encryption keys are always generated by BitLocker. A key is generated by BitLocker for each volume and cannot be reused for any other purpose.

When using BitLocker with SafeGuard Enterprise, a recovery key is stored in the SafeGuard Enterprise Database. This allows for setting up a helpdesk and recovery mechanism similar to the SafeGuard Enterprise Challenge/Response.

However, it is not possible to select keys globally or reuse them as with SafeGuard Enterprise native clients. The keys are not displayed in the SafeGuard Management Center either.

 **Note** BitLocker also allows you to back up recovery keys to Active Directory. If this is enabled in the group policy objects (GPOs), this is done automatically when a volume is encrypted with

BitLocker. If a volume is already encrypted, the administrator can back up the BitLocker recovery keys manually with Windows Manage-BDE tool (see "manage-bde -protectors -adbackup -?").

4.1.5.2 BitLocker algorithms in SafeGuard Enterprise

BitLocker supports the following Advanced Encryption Standard (AES) algorithms:

- AES-128
- AES-256

AES-128 with diffuser and AES-256 with diffuser are no longer supported. Drives already encrypted using an algorithm with diffuser can be managed by SafeGuard Enterprise.

4.1.5.3 Encryption policies for BitLocker Drive Encryption

The security officer can create a policy for (initial) encryption in the SafeGuard Management Center and distribute it to the BitLocker endpoints where it is executed. It triggers the BitLocker encryption of the drives specified in the policy.

As the BitLocker clients are managed transparently in the SafeGuard Management Center, the security officer does not have to specify any special BitLocker settings for encryption. SafeGuard Enterprise knows the client status and selects the BitLocker encryption accordingly. When a BitLocker client is installed with SafeGuard Enterprise and volume encryption is activated, the volumes are encrypted by BitLocker Drive Encryption.

A BitLocker endpoint processes policies of type **Device Protection** and **Authentication**.

The following settings are evaluated on the endpoint:

- Settings in a policy of type **Device Protection**:
 - **Target: Local Storage Devices | Internal Storage | Boot Volumes | Non-boot Volumes | Drive Letters A: - Z:**
 - **Media Encryption Mode: Volume based | No encryption**
 - **Algorithm to be used for encryption: AES128 | AES256**
 - **Fast initial encryption: Yes | No**

For details see [Device Protection \(page 259\)](#).

- Settings in a policy of type **Authentication**:
 - **BitLocker Logon Mode for Boot Volumes: TPM | TPM + PIN | TPM + Startup Key | Startup Key**

- **BitLocker Fallback Logon Mode for Boot Volumes: Password |Startup Key | Password or Startup Key | Error**
- **BitLocker Logon Mode for Non-Boot Volumes: Auto-Unlock | Password | Startup Key**
- **BitLocker Fallback Logon Mode for Non-Boot Volumes: Password | Password or Startup Key| Startup Key**

For details see [Authentication \(page 239\)](#).

All other settings are ignored by the BitLocker endpoint.

4.1.5.4 Encryption on a BitLocker-protected computer

Before the encryption starts, the encryption keys are generated by BitLocker. Depending on the system used the behavior differs slightly.

Endpoints with TPM

If the security officer defines a logon mode for BitLocker that involves the TPM (TPM, TPM + PIN, or TPM + Startup Key), TPM activation is automatically initiated.

The TPM (Trusted Platform Module) is a hardware device BitLocker uses to store its encryption keys. The keys are not stored on the computer's hard disk. The TPM must be accessible by the basic input/output system (BIOS) during startup. When the user starts the computer, BitLocker will get these keys from the TPM automatically.

Endpoints without TPM

If an endpoint is not equipped with a TPM, either a BitLocker startup key or, if the endpoint is running Windows 8 or later, a password can be used as the logon mode.

A BitLocker startup key can be created using a USB memory stick to store the encryption keys. The user will have to insert the memory stick each time when starting the computer.

When SafeGuard Enterprise activates BitLocker, users are prompted to save the BitLocker startup key. A dialog appears displaying the valid target drives in which to store the startup key.

For **boot volumes**, it is essential that the startup key is available when the endpoint is started. Therefore, the startup key can only be stored on removable media.

For data volumes, the BitLocker startup key can be stored on an encrypted boot volume. This is done automatically if **Auto-Unlock** is defined in the policy.

BitLocker recovery keys

For BitLocker recovery, SafeGuard Enterprise offers a Challenge/Response procedure that allows information to be exchanged confidentially and allows the BitLocker recovery key to be retrieved from the helpdesk, see [Recovery for BitLocker encrypted endpoints \(page 299\)](#).

To enable recovery with Challenge/Response or retrieval of the recovery key, the required data has to be available to the helpdesk. The data required for recovery is saved in specific key recovery files.

 **Note** If SafeGuard BitLocker management without Challenge/Response in standalone mode is used, the recovery key is not changed after a recovery procedure.

 **Note** If a BitLocker-encrypted hard disk in a computer is replaced by a new BitLocker-encrypted hard disk, and the new hard disk is assigned the same drive letter as the previous hard disk, SafeGuard Enterprise only saves the recovery key of the new hard disk.

Managing drives already encrypted with BitLocker

If there are any drives already encrypted with BitLocker on your computer when SafeGuard Enterprise is installed, SafeGuard Enterprise takes over the management of these drives.

Encrypted boot drives

- Depending on the SafeGuard Enterprise BitLocker support used, you may be prompted to reboot the computer. It is important that you reboot the computer as early as possible.
- If a SafeGuard Enterprise encryption policy applies for the encrypted drive:
 - **SafeGuard Enterprise BitLocker Challenge/Response** is installed: Management is taken over and SafeGuard Enterprise Challenge/Response is possible.
 - **SafeGuard Enterprise BitLocker** is installed: Management is taken over and recovery is possible.
- If no SafeGuard Enterprise encryption policy applies for the encrypted drive:
 - **SafeGuard Enterprise BitLocker Challenge/Response** is installed: Management is not taken over and SafeGuard Enterprise Challenge/Response is not possible.
 - **SafeGuard Enterprise BitLocker** is installed: recovery is possible.

Encrypted data drives

- If a SafeGuard Enterprise encryption policy applies for the encrypted drive:

Management is taken over and recovery is possible.
- If no SafeGuard Enterprise encryption policy applies for the encrypted drive:

SafeGuard Enterprise recovery is possible.

4.1.5.5 Decryption with BitLocker

Computers encrypted with BitLocker cannot be decrypted automatically. Decryption can be carried out using either the **BitLocker Drive Encryption** item in the **Control Panel** or the Microsoft command-line tool "manage-bde".

To allow users to decrypt BitLocker encrypted drives manually, a policy without an encryption rule for a BitLocker encrypted drive has to be applied on the endpoint. The user can then trigger decryption by deactivating BitLocker for the desired drive in the **BitLocker Drive Encryption Control Panel** item or via "manage-bde".

4.1.6 BitLocker To Go

BitLocker To Go can be used to encrypt volumes on removable media when the client components for SafeGuard Enterprise BitLocker support are installed. However, BitLocker To Go cannot be managed by SafeGuard Enterprise.

To disable BitLocker To Go, see [Deactivate BitLocker To Go encryption \(page 299\)](#).

BitLocker To Go is not compatible with SafeGuard Full Disk Encryption (volume-based full disk encryption). When you install SafeGuard Full Disk Encryption, BitLocker To Go is disabled. Volumes and removable media that are already encrypted with BitLocker To Go remain accessible.

4.1.6.1 Deactivate BitLocker To Go encryption

1. In the Windows Group Policy Editor, select **Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Removable Data Drives**.
2. Right-click **Control use of BitLocker on removable drives** and select **Edit**.
3. Select **Enabled**.
4. Under **Options**, deselect **Allow users to apply BitLocker protection on removable data drives**.
5. Under **Options**, select **Allow users to suspend and decrypt BitLocker protection on removable data drives**.
6. Click **OK**.

BitLocker To Go encryption is deactivated on the endpoints. Users cannot encrypt new volumes with BitLocker To Go anymore. Volumes and removable media that are already encrypted with BitLocker To Go remain accessible.

4.1.7 Recovery for BitLocker encrypted endpoints

Depending on the system used, SafeGuard Enterprise offers a Challenge/Response procedure for recovery or the possibility of obtaining the BitLocker recovery key from the helpdesk. For the requirements for SafeGuard Enterprise Challenge/Response, see [SafeGuard Challenge/Response for BitLocker \(page 294\)](#).

4.1.7.1 Recovery with BitLocker recovery key ID

For BitLocker encrypted computers a volume that cannot be accessed any more can be recovered via the BitLocker recovery key ID.

Users have to provide this ID. When they start the recovery process, the BitLocker recovery key ID for operating system drive is displayed on the BitLocker recovery screen. For data drives the BitLocker recovery key ID is displayed when users click on **More options** and then on **Enter recovery key** in the wizard to unlock a BitLocker encrypted drive.

⚠ Important Recovery keys are only displayed if the security officer has the permissions to manage the computer. If the computer has been removed in the Management Center, the **Use recovery tool** permission is required to access recovery keys.

1. In the SafeGuard Management Center, select **Tools > Recovery** to open the **Recovery Wizard**.
2. On the **Recovery type** page, select **BitLocker Recovery key ID (managed)** and click **Next**.
3. Click [...] to search for a recovery key ID.
4. On the **Find BitLocker recovery keys** page, enter at least the first four digits of the BitLocker recovery key ID in the **Search name** field and click **Find Now**.
All keys matching your query are displayed.

Active and inactive keys are displayed. Recovery keys are displayed even if the assigned computer has been removed in the Management Center. In this case the computer name cannot be determined and **N/A** is displayed in the **Computer** column.

5. Select the desired key and click **OK**.
On the **Find BitLocker recovery keys** page, information about the key is displayed.
6. Click **Next**.
On the **BitLocker recovery** page, the 48-digit BitLocker recovery key is displayed.
7. Provide the key to the user.

For logged events, see [Auditing \(page 204\)](#).

4.1.7.2 Recovery key for SafeGuard Enterprise endpoints below version 7

For BitLocker encrypted computers a volume that cannot be accessed any more can be recovered.

Users have to provide the computer name and in return get the recovery key to be entered in the recovery screen.

1. In the SafeGuard Management Center, select **Tools > Recovery** to open the **Recovery Wizard**.
2. On the **Recovery type** page, select **SafeGuard Enterprise Client (managed)**.
3. Under **Domain**, select the required domain from the list.
4. Under **Computer** enter or select the required computer name. There are several ways to do so:
 - To select a name, click [...]. Then click **Find Now**. A list of computers is displayed. Select the required computer and click **OK**. The computer name is displayed in the **Recovery type** window under **Computer**.
 - Type the short name of the computer directly into the field. When you click **Next**, the database is searched for this name. If it is found, the distinguished computer name is displayed.
 - Enter the computer name directly in distinguished name format, for example:

CN=Desktop1,OU=Development,OU=Headquarter,DC=Utimaco,DC=edu

5. Click **Next**.
6. Select the volume to be accessed from the list and click **Next**.
7. The Recovery Wizard displays the corresponding 48-digit recovery key.
8. Provide this key to the user.

The user can enter the key to recover the BitLocker encrypted volume on the endpoint.

4.1.7.3 Challenge/Response for BitLocker

For UEFI endpoints that meet certain requirements, SafeGuard Enterprise offers Challenge/Response for recovery.

Users have to provide the challenge code that is displayed on the BitLocker recovery screen and in return get a response to be entered in the recovery screen.

On UEFI endpoints that do not fulfill the requirements SafeGuard BitLocker management without Challenge/Response is installed automatically. To recover these endpoints see [Recovery with BitLocker recovery key ID \(page 300\)](#) and [Recovery key for SafeGuard Enterprise endpoints below version 7 \(page 300\)](#).

1. In the SafeGuard Management Center, select **Tools > Recovery** to open the **Recovery Wizard**.
2. On the **Recovery type** page, select **SafeGuard Enterprise Client (managed)**.
3. Under **Domain**, select the required domain from the list.
4. Under **Computer** enter or select the required computer name. There are several ways to do so:

- To select a name, click [...]. Then click **Find now**. A list of computers is displayed. Select the required computer and click **OK**. The computer name is displayed on the **Recovery type** page.
- Type the short name of the computer directly into the field. When you click **Next**, the database is searched for this name. If it is found, the distinguished computer name is displayed.
- Enter the computer name directly in the distinguished name format, for example:

CN=Desktop1,OU=Development,OU=Headquarter,DC=Sophos,DC=edu

5. Click **Next**.

6. Select the volume to be accessed from the list and click **Next**.

7. Click **Next**.

A page is displayed where you can enter the challenge code.

8. Enter the challenge code the user has passed on to you and click **Next**.

9. A response code is generated. Provide the response code to the user. A spelling aid is provided. You can also copy the response code to the clipboard.

The user can enter the response code and get access to the endpoint.

4.2 *Location-based File Encryption*

The SafeGuard Enterprise module File Encryption offers location-based file encryption on local drives and network locations, mainly for work groups on network shares.

In the SafeGuard Management Center, you define the rules for file-based encryption in **File Encryption** policies. In these File Encryption rules, you specify the folders that are to be handled by File Encryption, the encryption mode and the key to be used for encryption. In **General Settings** policies, you can define how specific applications and file systems are handled on endpoints in the context of File Encryption. You can specify ignored and trusted applications as well as ignored devices. You can also enable persistent encryption for File Encryption.

For encryption, Personal Keys can be used. A Personal Key that is active for a user only applies to this particular user and cannot be shared with or assigned to any other users. You can create Personal Keys in the SafeGuard Management Center under **Users and Computers**.

After a **File Encryption** policy has been assigned to endpoints, files in the locations covered by the policy are transparently encrypted without user interaction:

- New files in the relevant locations are encrypted automatically.
- If users have the key for an encrypted file, they can read and modify the content.
- If users do not have the key for an encrypted file, access is denied.
- If a user accesses an encrypted file on an endpoint where File Encryption is not installed, the encrypted content is shown.

Already existing files in the locations covered by the encryption policy are not encrypted automatically. Users have to carry out an initial encryption in the **SafeGuard File Encryption Wizard** on the endpoint. For further information, see the *SafeGuard Enterprise user help*.

 **Note**

SafeGuard File Encryption is not compatible with Windows built-in EFS encryption and file compression. If EFS is enabled, it has priority over any applicable file encryption rule and files that are created in the relevant folder cannot be encrypted by File Encryption. If compression is enabled, File Encryption has a higher priority and files are encrypted but not compressed. To encrypt the files by File Encryption, EFS encryption or data compression has to be removed beforehand. This can be done manually or by running the SafeGuard Enterprise Initial Encryption Wizard.

SafeGuard File Encryption does not support the Files On-Demand functionality available since Windows 10.

For details when using Mac endpoints and SafeGuard File Encryption for Mac, see [About SafeGuard File Encryption for Mac \(page 346\)](#) and the *SafeGuard Enterprise for Mac user help*.

4.2.1 Configuring encryption rules in location-based File Encryption policies

You define the rules for file-based encryption on network locations in a policy of the type **File Encryption**.

 **Note** Certain folders (for example C:\Program Files) may prevent the operating system or applications from running when encrypted. When you define encryption rules, make sure that these folders are not encrypted.

1. In the **Policies** navigation area, create a new policy of the type **File Encryption** or select an existing one.
The **File Encryption** tab is displayed.
2. Select **Location-based** from the **Encryption type** drop-down list.

The table to specify locations where location-based file encryption is applied on the endpoint computer is displayed.

 **Note** SafeGuard Enterprise did not have the **Encryption type** setting until version 8.0. If you updated your Management Center, already existing File Encryption policies will be converted to File Encryption policies of type **Location-based**. For **Encryption type > No encryption**, see [Policies of type No encryption \(page 122\)](#).

3. In the **Path** column, set the path (that is the folder) to be handled by File Encryption:
 - Click the drop-down button and select a folder name placeholder from the list of available placeholders.

By hovering your cursor over the list entries, you can display tooltips telling you how a placeholder is typically presented on an endpoint. You can only enter valid placeholders. For a description of all available placeholders, see [Placeholders for paths in location-based File Encryption rules \(page 306\)](#).

 **Important** Encrypting the whole user profile with the placeholder <User Profile> may result in an unstable Windows desktop on the endpoint.

- Click the Browse button to browse the file system and select the required folder.
- Alternatively, just enter a path name.

For useful information on configuring paths in File Encryption rules, see [Additional information for configuring paths in location-based File Encryption rules \(page 305\)](#).

4. In the **Scope** column, select one of the following:
 - **Only this folder** to apply the rule only to the folder indicated by the **Path** column.
 - **Include subfolders** to also apply the rule to all its subfolders.
5. In the **Mode** column, define how File Encryption should handle the folder indicated in the **Path** column:
 - Select **Encrypt** to encrypt new files in the folder. The contents of the existing encrypted files are decrypted transparently when a user with the required key accesses them. If the user does not have the required key, access is denied.
 - If you select **Exclude**, new files in the folder are not encrypted. You might use this option to exclude a subfolder from encryption if the parent folder is already covered by a rule with the **Encrypt** option.
 - If you select **Ignore**, files in the folder are not handled by File Encryption at all. New files are saved in plaintext. If a user accesses already encrypted files in this folder, the encrypted content is displayed, regardless whether the user has the required key or not.
6. In the **Key** column, select the key to be used for the **Encrypt** mode. You can use keys created and applied in **Users and Computers**:
 - Click the Browse button to open the **Find Keys** dialog. Click **Find now** to display a list of all available keys and select the required key.

 **Note** Machine keys are not shown in the list. They cannot be used by File Encryption as they are only available on a single computer and can therefore not be used to enable groups of users to access the same data.

- Click the **Personal Key** button with the key icon, to insert the **Personal Key** placeholder in the **Key** column. On the endpoint, this placeholder will be resolved to the active Personal Key of the logged on SafeGuard Enterprise user. If the relevant users do not have active Personal Keys yet, they are created automatically. You can create Personal Keys for single or multiple users in **Users and Computers**. For further information, see [Personal Keys for file-based encryption by File Encryption \(page 161\)](#).

7. The **System** type (**Windows**, **macOS** or **All systems** for Windows and macOS systems) will be assigned automatically.
8. Add further encryption rules as required and save your changes.

 **Note** All File Encryption rules that are assigned by policies and activated for users/computers at different nodes in **Users and Computers** are cumulated. The order of encryption rules within a **File Encryption** policy is not relevant for their evaluation on the endpoint. Within a **File Encryption** policy, you can drag the rules into order to gain a better overview.

4.2.1.1 Additional information for configuring paths in location-based File Encryption rules

When configuring paths in File Encryption rules, consider the following.

- A path can only contain characters that can also be used in file systems. Characters like <, >, * and \$ are not allowed.
- You can only enter valid placeholders. For a list of all supported placeholders, see [Placeholders for paths in location-based File Encryption rules \(page 306\)](#).

Names of environment variables are not checked by the SafeGuard Management Center. They only need to be present on the endpoint.

- The **Path** field always indicates a folder. You cannot specify a rule for a single file or use wildcards for folder names, file names or file extensions.
- **Absolute and relative rules**

You can define absolute and relative rules. An absolute rule exactly defines a specific folder, for example C:\encrypt. A relative rule does not include UNC server/share information, drive letter information or parent folder information. An example for a path used in a relative rule is encrypt_sub. In this case, all files on all drives (including network locations) that reside in a folder encrypt_sub (or one of its subfolders) are covered by the rule.

 **Note** Relative paths are only supported on Windows endpoint computers.

- **Long folder names and 8.3 notation**

Always enter the long folder names for File Encryption rules since 8.3 names for long folder names may differ from computer to computer. 8.3 name rules are detected automatically by the endpoint protected by SafeGuard Enterprise when the relevant policies are applied. Whether applications use long folder names or 8.3 names for accessing files - the result should be the same. For relative rules, use the short folder names to make sure that the rule can be enforced regardless of an application that uses long folder names or 8.3 notation.

- **UNC and/or mapped drive letters**

Whether you administer rules in UNC notation or based on mapped drive letters depends on your specific requirements:

- Use UNC notation if your server and share names are not likely to change, but drive letter mappings vary between users.
- Use mapped drive letters, if drive letters stay the same, but server names may change.

If you use UNC, specify a server name and a share name, for example \\server\share.

File Encryption matches UNC names and mapped drive letters internally. In a rule, a path therefore needs to be defined either as a UNC path or with mapped drive letters.

 **Note** Since users may be able to change their drive letter mappings, we recommend to use UNC paths in File Encryption rules for security reasons.

- **Offline folders**

If the Windows feature **Make Available Offline** is used, you do not have to create special rules for local (offline) copies of folders. New files in the local copy of a folder that has been made available for offline use are encrypted according to the rule for the original (network) location.

For further information on naming files and paths, see <http://msdn.microsoft.com/en-us/library/aa365247.aspx>.

4.2.1.2 Placeholders for paths in location-based File Encryption rules

The following placeholders can be used when specifying paths in encryption rules in **File Encryption** policies. You can select these placeholders by clicking the drop-down button of the **Path** field.

Always use backslashes as path separator, even when creating File Encryption rules for macOS. This allows you to apply rules on both operating systems, Windows and macOS. On macOS endpoints, backslashes are automatically transformed to slashes in order to match the requirements of the macOS operating system. Any errors in placeholders are logged. Invalid File Encryption rules are logged and then discarded on the endpoint.

Example: The Windows path <User Profile>\Dropbox\personal is converted on Mac side into /Users/<Username>/Dropbox/personal.

Path placeholder	Operating System (All=Windows and macOS)	Results in the following value on the endpoint
<%environment_variable_name%> All		<p>The value of environment variable. Example: <%USERNAME%>.</p> <p> Note If environment variables contain several locations (for example the PATH environment variable), the paths will not be separated into multiple rules. This causes an error and the encryption rule is invalid.</p>
<Desktop>	All	<p>The virtual folder that represents the endpoints desktop.</p>
<Documents>	All	<p>This is the virtual folder that represents the My Documents desktop item (equivalent to CSIDL_MYDOCUMENTS). Typical path: C:\Documents and Settings\username\My Documents.</p>
<Downloads>	All	<p>The folder where downloads are stored by default. A typical path for Windows is C:\Users\username\Downloads.</p>
<Music>	All	<p>The file system directory that serves as a data repository for music files. Typical path: C:\Documents and Settings\User\My Documents\My Music.</p>
<Network Shares>	All	
<Pictures>	All	<p>The file system directory that serves as a data repository for image files. Typical path: C:\Documents and Settings\username\My Documents\My Pictures.</p> <p> Note On Macs, encrypting the whole <Pictures> folder is not supported. However, you can encrypt subfolders, for example <Pictures>\enc.</p>
<Public>	All	<p>The file system directory that serves as a common repository for document files for all users. Typical path: C:\Users\<username>\Public.</p>

Path placeholder	Operating System (All=Windows and macOS)	Results in the following value on the endpoint
<Removables>	All	Points to the root folders of all removable media.
<User Profile>	All	The user's profile folder. Typical path: C:\Users\username.
		<p> Note Encrypting the whole user profile is not supported. However, you can encrypt subfolders, for example <User Profile>\enc.</p>
<Videos>	All	The file system directory that serves as a common repository for video files for all users. Typical path: C:\Documents and Settings\All Users\Documents\My Videos.
<Cookies>	Windows	The file system directory that serves as a common repository for internet cookies. Typical path: C:\Documents and Settings\username\Cookies.
<Favorites>	Windows	The file system directory that serves as a common repository for the user's favorite items. Typical path: \Documents and Settings\username\Favorites.
<Local Application Data>	Windows	The file system directory that serves as a data repository for local (non-roaming) applications. Typical path: C:\Documents and Settings\username\Local Settings\Application Data.
<Program Data>	Windows	The file system directory that contains application data for all users. Typical path: C:\Documents and Settings\All Users\Application Data.
<Program Files>	Windows	The Program Files folder. Typical path: \Program Files. For 64-bit systems, this will be expanded into two rules - one for 32-bit applications and one for 64-bit applications.
<Public Music>	Windows	The file system directory that serves as a common repository for music files for all users. Typical path: C:\Documents and Settings\All Users\Documents\My Music.
<Public Pictures>	Windows	The file system directory that serves as a common repository for image files for all

Path placeholder	Operating System (All=Windows and macOS)	Results in the following value on the endpoint
<Public Videos>	Windows	users. Typical path: C:\Documents and Settings\All Users\Documents\My Pictures The file system directory that serves as a common repository for video files for all users. Typical path: C:\Documents and Settings\All Users\Documents\My Videos.
<Roaming>	Windows	The file system directory that serves as a common repository for application-specific data. Typical path: C:\Documents and Settings\username\Application Data.
<System>	Windows	The Windows System folder. Typical path: C:\Windows\System32. For 64-bit systems, this will be expanded to two rules - one for 32-bit and one for 64-bit.
<Temporary Burn Folder>	Windows	The file system directory that is used as a staging area for files waiting to be written on a CD. Typical Path: C:\Documents and Settings\username\Local Settings\Application Data\Microsoft\CD Burning.
<Temporary Internet Files>	Windows	The file system directory that serves as a common repository for Temporary Internet Files. Typical path: C:\Documents and Settings\username\Local Settings\Temporary Internet Files.
<Windows>	Windows	The Windows directory or SYSROOT. This corresponds to the environment variables %windir% or %SYSTEMROOT%. Typical path: C:\Windows.
<Root>	macOS	The macOS root folder. It is not recommended to specify policies for the root folder, even if it is technically possible.

4.2.2 Configuring location-based File Encryption settings in General Settings policies

In addition to the encryption rules defined in **File Encryption** policies of **Encryption type > Location-based**, you can configure the following **File Encryption** settings in policies of type **General Settings**:

- Trusted Applications

- **Ignored Applications**
- **Ignored Devices**
- **Enable persistent encryption**

4.2.2.1 Configure trusted and ignored applications for File Encryption

You can define applications as trusted to grant them access to encrypted files. This is for example necessary to enable antivirus software to scan encrypted files.

You can also define applications as ignored to exempt them from transparent file encryption/decryption. For example, if you define a backup program as an ignored application, encrypted data backed up by the program remains encrypted.

 **Note** Child processes will not be trusted/ignored.

1. In the **Policies** navigation area, create a new policy of the type **General Settings** or select an existing one.
2. Under **File Encryption**, click the drop-down button of the **Trusted Applications** or **Ignored Applications** field.
3. In the editor list box, enter the applications to be defined as trusted/ignored.
 - You can define multiple trusted/ignored applications in one policy. Each line in the editor list box defines one application.
 - Application names must end with .exe.
 - Application names must be specified as fully qualified paths including drive/directory information, for example "c:\dir\example.exe". Entering the file name only (for example "example.exe") is not sufficient. For better usability the single line view of the application list only shows the file names separated by semicolons.
 - Application names can contain the same placeholder names for Windows shell folders and environment variables as encryption rules in File Encryption policies. For a description of all available placeholders, see [Placeholders for paths in location-based File Encryption rules \(page 306\)](#).
4. Save your changes.

 **Note** The **Trusted Applications** and **Ignored Applications** policy settings are machine settings. The policy must therefore be assigned to machines, not to users. Otherwise the settings do not become active.

4.2.2.2 Configuring ignored devices

1. In the **Policies** navigation area, create a new policy of the type **General Settings** or select an existing one.
2. Under **File Encryption**, click the drop-down button of the **Ignored Devices** field.
3. In the editor list box:
 - a. Select **Network** if you don't want to encrypt any data on the network.
 - b. Enter the required device names to exclude specific devices from encryption. This may be useful when you need to exclude systems from third party suppliers.
You can display the names of the devices currently used in the system by using the Fltmc.exe control program (fltmc volumes, fltmc instances) from Microsoft, see <https://docs.microsoft.com/en-us/windows-hardware/drivers/ifs/development-and-testing-tools> .

You can exclude individual (network) disk drives from encryption by creating a File Encryption rule in a **File Encryption** policy and set the encryption **Mode** to **Ignore**. You can apply this setting only to Windows administered drives and not to macOS volumes.

4.2.2.3 Configure persistent encryption for File Encryption

The content of files encrypted by File Encryption are decrypted on-the-fly, if the user owns the required key. When the content is saved as a new file in a location that is not covered by an encryption rule, the resulting file will not be encrypted.

With persistent encryption, copies of encrypted files will be encrypted, even when they are saved in a location not covered by an encryption rule.

You can configure persistent encryption in policies of the type **General Settings**. The policy setting **Enable persistent encryption** is activated by default.

Note

If files are copied or moved to an ignored device or to a folder to which a policy with encryption mode **Ignore** applies, the **Enable persistent encryption** setting has no effect.

Zip archives are never considered by persistent encryption.

4.2.3 *Outlook Add-in for location-based encryption*

Since version 8.1 the SafeGuard Enterprise Outlook Add-In for Windows is available for location-based encryption. It is available on endpoints when you install any location-based File Encryption module.

In general, the functionality for sending external emails is the same as for application-based encryption. However, for sending emails with attachments to white-listed domains, there are some caveats due to the nature of location-based encryption and the multi-key feature of Synchronized Encryption.

In the **(Default) General Settings** policy, you can configure what happens with attachments to emails sent to white-listed (usually internal) domains. Available options for **Behavior for white-listed domains** are:

- **Encrypted**
- **No encryption**
- **Always ask**
- **Unchanged (Synchronized Encryption)**

No encryption and **Always ask** behave the same for all File Encryption modules.

The options **Encrypted** and **Unchanged (Synchronized Encryption)** behave differently when used with Synchronized Encryption or location-based encryption.

Encrypted

- Synchronized Encryption

Encrypted files keep their encryption, the encryption key isn't changed. Plain files are encrypted with the **Synchronized Encryption key**, but only if the file extension is defined in the list of In-Apps.

- Location-based encryption

All attached files are encrypted with the **Synchronized Encryption key**, regardless of their file extensions and encryption status.

Unchanged (Synchronized Encryption)

- Synchronized Encryption

Encrypted files will be sent encrypted, plain files will be sent in plaintext.

- Location-based encryption

All files are encrypted with the **Synchronized Encryption key**.

4.2.3.1 Create policies for activating the SafeGuard Enterprise Outlook Add-in

To activate the SafeGuard Enterprise Add-in for location-based File Encryption:

1. In the **Policies** navigation area, create a new policy of the type **General Settings** or select an existing one.

The **General Settings** tab is displayed.

2. Go to the **Email add-in settings** section.

3. In the **Enable email add-in** drop-down list, select **Yes**.

The add-in is now activated. Users will be prompted to decide how to handle attachments each time they send emails with attachments.

In addition, you can list domains and specify how attachments are handled when they are sent to these domains.

4. To do so, select how to handle attachments from the **Encryption method for white-listed domains** drop-down list:

- **Encrypted**: All attached files are encrypted with the **Synchronized Encryption key**, regardless of their file extensions and encryption status.
- **No encryption**: Attachments in emails to the specified domain are encrypted. Users are not be prompted.
- **Unchanged (Synchronized Encryption)**: All files are encrypted with the **Synchronized Encryption key**.
- **Always ask**: Users are asked how to handle the attachments each time they send emails to the specified domain.

5. Enter one or more domains for which the encryption method should be applied. Enter several domains separated by commas. Wildcards and partially specified domains are not supported.

6. When you leave the **General Settings** tab, the system prompts you to save your changes.

7. Click **Yes**.

8. Go to **Users and Computers** and assign the new policy to your user groups.

4.2.4 Multiple location-based File Encryption policies

All File Encryption rules that are assigned by policies and activated for users/computers at different nodes in **Users and Computers** in the SafeGuard Management Center are cumulated.

You can assign a general **File Encryption** policy at the root node that includes rules relevant for all users, and more specific policies at specific subnodes. All rules in all policies assigned to users/computers are cumulated and enforced on the endpoint.

4.2.4.1 Location-based File Encryption policies in the RSOP

If several **File Encryption** policies apply to a user or computer, the **RSOP** (Resulting Set of Policies) tab in **Users and Computers** shows the sum of all File Encryption rules of all **File Encryption** policies. The rules are sorted in the order of encryption rule evaluation on the endpoint computer, see [Evaluation of location-based File Encryption rules on endpoints \(page 314\)](#).

The **Policy Name** column shows where the individual rules originate from.

For duplicate rules, the second (and third etc.) rule is marked by an icon. This icon also provides a tooltip informing you that the rule will be discarded on the endpoint as it is a duplicate of a rule with a higher priority.

4.2.5 *Evaluation of location-based File Encryption rules on endpoints*

On endpoints, File Encryption rules are sorted in an order that causes the more specifically defined locations to be evaluated first:

- If two rules with the same **Path** and **Scope** settings originate from policies that are assigned to different nodes, the rule from the policy nearest to the user object in **Users and Computers** is applied.
- If two rules with the same **Path** and **Scope** settings originate from policies that are assigned to the same node, the rule from the policy with the highest priority is applied.
- Absolute rules are evaluated before relative rules, for example c:\encrypt before encrypt. For further information, see [Additional information for configuring paths in location-based File Encryption rules \(page 305\)](#).
- Rules with a path containing more subdirectories are evaluated before rules with a path containing less subdirectories.
- Rules defined with UNC are evaluated before rules with drive letter information.
- Rules with **Only this folder** activated are evaluated before rules without this option.
- Rules using the **Ignore** mode are evaluated before rules using **Encrypt** or **Exclude** mode.
- Rules using the **Exclude** mode are evaluated before rules using **Encrypt** mode.
- If two rules are equal regarding the criteria listed, the one that comes first in alphabetical order is evaluated before the other rule.

4.2.6 Conflicting location-based File Encryption Rules

As multiple File Encryption policies can be assigned to a user or computer, conflicts may occur. Two rules are considered as conflicting, if they have the same values for path, mode and subdirectory, but the key to be used is different. In this case the rule from the File Encryption policy with the higher priority applies. The other rule is discarded.

4.2.7 Location-based File Encryption and SafeGuard Data Exchange

SafeGuard Data Exchange is used to encrypt data stored on removable media connected to a computer and to exchange this data with other users. For SafeGuard Data Exchange file-based encryption is used.

If both SafeGuard Data Exchange and location-based File Encryption are installed on an endpoint, it may occur that a SafeGuard Data Exchange encryption policy is defined for a drive on the computer and location-based File Encryption policies are defined for folders on the same drive. If this is the case, the SafeGuard Data Exchange encryption policy overrules the **File Encryption** policies. New files are encrypted according to the SafeGuard Date Exchange encryption policy.

For further information on SafeGuard Data Exchange, see [SafeGuard Data Exchange \(page 322\)](#).

4.3 Cloud Storage

The SafeGuard Enterprise module Cloud Storage offers file-based encryption of data stored in the cloud.

It does not change the way users work with data stored in the cloud. Users still use the same vendor specific synchronization applications to send data to or receive data from the cloud. The purpose of Cloud Storage is to make sure that the local copies of data stored in the cloud are encrypted transparently and will therefore always be stored in the cloud in encrypted form.

In the SafeGuard Management Center, you create **Cloud Storage Definitions (CSDs)** and use them as targets in **Device Protection** policies. Predefined Cloud Storage Definitions are available for several cloud storage providers, for example Dropbox or Egnyte.

After a Cloud Storage policy has been assigned to endpoints, files in locations covered by the policy are transparently encrypted without user interaction:

- Encrypted files will be synchronized into the cloud.
- Encrypted files received from the cloud can be modified by applications as usual.

To access Cloud Storage encrypted files on endpoints without SafeGuard Enterprise Cloud Storage, SafeGuard Portable can be used to read encrypted files.

 **Note** Cloud Storage only encrypts new data stored in the cloud. If data is already stored in the cloud before installing Cloud Storage, this data will not automatically be encrypted. If you want to encrypt this data, you have to remove it from the cloud first and then enter it again.

For tracking files accessed in cloud storage, see [Auditing \(page 204\)](#).

4.3.1 Requirements for Cloud Storage vendor software

To enable encryption of data stored in the cloud, the software provided by the cloud storage vendor must:

- Run on the computer where Cloud Storage is installed.
- Have an application (or system service) that is stored on the local file system and synchronizes data between the cloud and the local system.
- Store the synchronized data on the local file system.

4.3.2 Create Cloud Storage Definitions (CSDs)

In the SafeGuard Management Center, predefined Cloud Storage Definitions are available for several cloud storage providers, for example Dropbox or Egnyte. You can modify the paths defined in predefined Cloud Storage Definitions according to your requirements or create a new one and copy values from a predefined one as a basis. This is for example useful, if you only want to encrypt part of the data in cloud storage. You can also create your own Cloud Storage Definitions.

 **Note** Certain folders (for example the Dropbox installation folder) may prevent the operating system or applications from running when encrypted. When you create Cloud Storage Definitions for **Device Protection** policies, make sure that these folders are not encrypted.

1. In the **Policies** navigation area, right-click **Cloud Storage Definitions**.
2. Select **New > Cloud Storage Definition**.
3. The **New Cloud Storage Definition** dialog appears. Enter a name for the Cloud Storage Definition.
4. Click **OK**. The Cloud Storage Definition appears with the entered name under the **Cloud Storage Definitions** root node in the **Policies** navigation area.
5. Select the Cloud Storage Definition. In the work area on the right-hand side the content of a Cloud Storage Definition is displayed:
 - **Target name:**

This is the name you entered initially. It is used for referencing the Cloud Storage Definition as a target in a policy of the type **Device Protection**.

- **Synchronization application:**

Enter path and application that synchronizes the data with the cloud (for example: <Desktop>\dropbox\dropbox.exe). The application must reside on a local drive.

- **Synchronization folders:**

Enter the folder(s) that will be synchronized with the cloud. Only local paths are supported.

 **Note** For paths in the **Synchronization application** and **Synchronization folders** settings, the same placeholders as for **File Encryption** are supported, see [Placeholders for paths in location-based File Encryption rules \(page 306\)](#).

4.3.2.1 Placeholders for cloud storage providers

As a security officer you can use placeholders for cloud storage providers to define synchronization application and synchronization folders. These placeholders represent supported 3rd party cloud storage applications. You can use the placeholder to specify a certain 3rd party application as synchronization application and even use the same placeholder to point the synchronization folders the 3rd party application actually uses for synchronization.

Placeholders for cloud storage providers are encapsulated by <! and !>.

Provider	Placeholder	Can be used in CSD setting	Resolves to
Box	<!Box!>	Synchronization application , For synchronization Synchronization folders	applications: The fully qualified path of the synchronization application used by the Box software.
Dropbox	<!Dropbox!>	Synchronization application , For synchronization Synchronization folders	For synchronization folders: The fully qualified path of the synchronization folder used by the Box software.

Provider	Placeholder	Can be used in CSD setting	Resolves to
			For synchronization folders: The fully qualified path of the synchronization folder used by the Dropbox software.
Egnyte	<code><!Egnyte!></code>	Synchronization Application	The fully qualified path of the synchronization application used by the Egnyte software.
Windows only			
	<code><!EgnytePrivate!></code>	Synchronization folders	All private folders in the Egnyte cloud storage. For standard Egnyte users this is usually a single folder. For Egnyte administrators this placeholder typically resolves to multiple folders.
	<code><!EgnyteShared!></code>	Synchronization folders	All shared folders in the Egnyte cloud storage.
			Note Changes to the Egnyte folder structure (including adding or removing private and shared folders) are detected automatically. The policies concerned are adjusted automatically.
			Note As Egnyte synchronization folders may reside on network locations you can enter network paths in the Synchronization folders setting. The SafeGuard Enterprise Cloud Storage module therefore attaches to network file systems by default. If this is not required, you can deactivate this behavior by defining a General Settings policy and selecting Network under Ignored Devices .
Google Drive	<code><!GoogleDrive!></code>	Synchronization application , Synchronization folders	For synchronization applications: The fully qualified path of the synchronization application used by the Google Drive software.
			For synchronization folders: The fully qualified path of the synchronization folder used by the Google Drive software.

Provider	Placeholder	Can be used in CSD setting	Resolves to
OneDrive	<!OneDrive!>	Synchronization application , For synchronization Synchronization folders	applications: The fully qualified path of the synchronization application used by the OneDrive software. For synchronization folders: The fully qualified path of the synchronization folder used by the OneDrive software.
OneDrive for Business	<!OneDriveForBusiness!>	Synchronization application , For synchronization Synchronization folders	applications: The fully qualified path of the synchronization application used by the OneDrive software. For synchronization folders: The fully qualified path of the synchronization folder used by the OneDrive software.
SkyDrive Windows only	<!SkyDrive!>	Synchronization application , For synchronization Synchronization folders	applications: The fully qualified path of

Provider	Placeholder	Can be used in CSD setting	Resolves to
		Since Microsoft renamed SkyDrive to OneDrive, the <code><!skyDrive!></code> placeholder is still available.	the synchronization application used by the OneDrive software. For synchronization folders: The fully qualified path of the synchronization folder used by the OneDrive software.

This way older policies using the placeholder and SafeGuard Enterprise endpoints before version 7 which cannot handle the `<!OneDrive!>` placeholder can be used without any changes. SafeGuard Enterprise endpoints version 7 can handle both placeholders.

Example

If you use Dropbox as your cloud storage provider you can simply enter `<!Dropbox!>` in **Synchronization application**. If you do not explicitly specify a synchronization folder, `<!Dropbox!>` is also copied into the list of folders under **Synchronization folders**.

Assuming

- You used the placeholders `<!Dropbox!>` as synchronization application and `<!Dropbox!>\encrypt` as synchronization folder in the Cloud Storage Definition
- Dropbox is installed on the endpoint
- The user has `d:\dropbox` configured as folder to be synchronized with Dropbox:

when the SafeGuard Enterprise endpoint receives a policy with a CSD like this, it will automatically translate the placeholders in the CSD to match the path of `Dropbox.exe` for the synchronization application and it will read the Dropbox configuration and set the encryption policy on the folder `d:\dropbox\encrypt`.

4.3.2.2 Export and import Cloud Storage Definitions

As a security officer you can export and import Cloud Storage Definitions (CSD). A CSD will be exported as an XML file.

- To export a CSD click **Export Cloud Storage Definition...** in the context menu of the desired Cloud Storage Definition in the **Policy** area.
- To import a CSD click **Import Cloud Storage Definition...** in the context menu of the Cloud Storage Definition node in the **Policy** area.

Both commands are also available in the **Actions** menu of the SafeGuard Management Center.

4.3.3 Create a device protection policy with a Cloud Storage Definition target

The Cloud Storage Definitions must have been created beforehand. Predefined Cloud Storage Definitions are available for several cloud storage providers, for example Dropbox or Egnyte.

You define the settings to encrypt cloud storage data in a policy of the type **Device Protection**.

1. In the **Policies** navigation area, create a new policy of the type **Device Protection**.
2. Select a Cloud Storage Definition as a target.
3. Click **OK**. The new policy is displayed in the navigation window below **Policy Items**. In the action area, all settings for the **Device Protection** policy are displayed and can be changed.
4. For the **Media encryption mode** setting select **File-based**. Volume-based encryption is not supported.
5. Under **Algorithm to be used for encryption** select the algorithm to be used for encrypting the data in the synchronization folders defined in the CSD.
6. Settings **Key to be used for encryption** and **Defined key for encryption** are used to define the key or the keys that shall be used for encryption. For further information, see [Device Protection \(page 259\)](#).
7. If you activate the **Copy SG Portable to target** setting, SafeGuard Portable is copied to each synchronization folder as soon as content is written to it. SafeGuard Portable is an application that can be used to read encrypted files on Windows computers that do not have SafeGuard Enterprise installed.

 **Note** To share encrypted data stored in the cloud with users that do not have SafeGuard Enterprise installed, users should be allowed to create local keys, see [Local keys \(page 328\)](#).

8. The **Plaintext folder** setting allows you to define a folder that will be excluded from encryption. Data stored in subfolders of the defined plaintext folder will also be excluded from encryption.

SafeGuard Cloud Storage automatically creates empty plaintext folders in all synchronization folders defined in the **Cloud Storage Definition**.

4.4 SafeGuard Data Exchange

SafeGuard Data Exchange is used to encrypt data stored on removable media connected to a computer and to exchange this data with other users. All encryption and decryption processes run transparently and involve minimum user interaction.

Only users who have the appropriate keys can read the contents of the encrypted data. All subsequent encryption processes run transparently.

In central administration, you define how data on removable media are handled.

As a security officer, you define the specific settings in a policy of type **Device Protection** with **Removable media** as **Device protection target**.

For SafeGuard Data Exchange, **File-based** has to be used as **Media Encryption mode**.

For tracking files accessed on removable media, see [Auditing \(page 204\)](#).

4.4.1 Best practice

This section describes some typical use cases for SafeGuard Data Exchange and how to implement them by creating the appropriate policies.

Bob and Alice are two employees of the same company and have SafeGuard Data Exchange installed, Joe is an external partner and does not have SafeGuard Enterprise installed on his computer.

4.4.1.1 Company internal use only

Bob wants to share encrypted data on removable media with Alice. Both belong to the same group and therefore have the appropriate group key in their SafeGuard Enterprise key ring. As they are using the group key, they can access the encrypted files transparently without the need to enter a passphrase.

You have to specify the settings in a policy of type **Device Protection > Removable Media**:

- **Media encryption mode: File-based**

- **Key to be used for encryption: Defined key on list**

- Defined key on list: <group/domain key > (for example, group_users_Bob_Alice@DC=...) to ensure that both share the same key

If company policies additionally define that all files on removable media have to be encrypted in any situation, add the following settings:

- **Initial encryption of all files: Yes**

Ensures that files on removable media are encrypted as soon as the media is connected to the system for the first time.

- **User may cancel initial encryption: No**

The user cannot cancel initial encryption, for example to postpone it.

- **User is allowed to access unencrypted files: No**

If plaintext files on removable media are detected, access to them will be denied.

- **User may decrypt files: No**

The user is not permitted to decrypt files on removable media.

- **Copy SG Portable to target: No**

As long as data on removable media are shared within the workgroup, SafeGuard Portable is not necessary. Also, SafeGuard Portable would allow to decrypt files on computers without SafeGuard Enterprise.

The users can share data just by exchanging their devices. When they connect the devices to their computers they have transparent access to encrypted files.

 **Note** This use case can be fulfilled by using SafeGuard Enterprise Device Encryption where the whole removable media is sector-based encrypted.

4.4.1.2 Home office or personal use on 3rd party computers

- **Home office:**

Bob wants to use his encrypted removable media on his home computer, where SafeGuard Enterprise is not installed. On his home computer, Bob decrypts files using SafeGuard Portable. By defining one media passphrase for all of Bob's removable media, he only has to open SafeGuard Portable and enter the media passphrase. Afterwards, Bob has transparent access to all encrypted files regardless of the local key used to encrypt them.

- **Personal use on 3rd party computers**

Bob plugs in the removable media on Joe's (external partner) computer and enters the media passphrase to get access to the encrypted files stored on the device. Bob can now copy the files, either encrypted or unencrypted, to Joe's computer.

Behavior on endpoint:

- Bob plugs in the removable media for the first time.
- The Media Encryption Key, which is unique for each device, is created automatically.
- Bob is prompted to enter the media passphrase for offline use with SafeGuard Portable.
- There is no need to bother the user with knowledge about the keys to be used or the key ring. The Media Encryption Key will always be used for data encryption without any user interaction. The Media Encryption Key is not even visible to the user, but only the centrally defined group/domain key.
- Bob and Alice within the same group or domain have transparent access since they share the same group/domain key.
- If Bob wants to access encrypted files on a removable media device on a computer without SafeGuard Data Exchange, he can use the media passphrase within SafeGuard Portable.

You have to specify the settings in a policy of type **Device Protection > Removable Media**:

- **Media encryption mode: File-based**
- **Key to be used for encryption: Defined key on list**
 - Defined key on list: <group/domain key > (for example group_users_Bob_Alice@DC=...) to ensure that both share the same key.

- **User may define a media passphrase for devices: Yes**

The user defines one media passphrase on their computer which is valid for all their removable media.

- **Copy SG Portable to target: Yes**

SafeGuard Portable gives the user access to all encrypted files on the removable media by entering a single media passphrase on the system without SafeGuard Data Exchange.

If the company policies additionally define that all files on removable media have to be encrypted in any situation, add the following settings:

- **Initial encryption of all files: Yes**

Ensures that files on removable media are encrypted as soon as the media is connected to the system for the first time.

- **User may cancel initial encryption: No**

The user cannot cancel initial encryption, for example to postpone it.

- **User is allowed to access unencrypted files: No**

If plaintext files on removable media are detected, access to them will be denied.

- **User may decrypt files: No**

The user is not permitted to decrypt files on removable media.

At work, Bob and Alice have transparent access to encrypted files on removable media. At home or on 3rd party computers, they can use SafeGuard Portable to open encrypted files. The users only have to enter the media passphrase to access all encrypted files. This is a simple but effective way to encrypt data on all removable media. The goal of this configuration is to reduce user interaction to a minimum while encrypting each and every file on removable media and giving the user access to the encrypted files in offline mode. The user is not permitted to decrypt files on removable media.

 **Note** In this configuration, users are not allowed to create local keys since it is not necessary for that use case. This has to be specified in a policy of type **Device Protection > Local Storage Devices (General Settings > User is allowed to create a local key > No)**.

- **Copy SG Portable to removable media: No.**

As long as data on removable media are shared in the workgroup SafeGuard Portable is not necessary. Also, SafeGuard Portable would allow to decrypt files without SafeGuard Enterprise.

At work, the user has transparent access to encrypted files on removable media. At home, they use SafeGuard Portable to open encrypted files. The user only has to enter the media passphrase to access all encrypted files, regardless of the key used for encrypting them.

4.4.1.3 Share removable media with external party

 **Note** This example applies only for Windows endpoints.

Bob wants to hand out an encrypted device to Joe (external party) who does not have SafeGuard Data Exchange installed and therefore has to use SafeGuard Portable. Under the assumption that Bob does not want to give Joe access to all encrypted files on the removable media, he can create a local key and encrypt the files with this local key. Joe can now use SafeGuard Portable and open the encrypted files with the passphrase of the local key, whereas Bob still can use the media passphrase to access any encrypted file on the removable device.

Behavior on the computer

- Bob plugs in the removable media for the first time. The Media Encryption Key, which is unique for each device, is created automatically.
- Bob is prompted to enter the media passphrase for offline use.
- The Media Encryption Key is used for data encryption without any user interaction, but...
- Bob can now create or select a local key (for example JoeKey) for the encryption of specific files that shall be exchanged with Joe.
- Bob and Alice within the same group or domain have transparent access since they share the same group/domain key.
- If Bob wants to access encrypted files on a removable media device on a computer without SafeGuard Data Exchange, he can use the media passphrase within SafeGuard Portable.
- Joe can access the specific files by entering the passphrase of the JoeKey without having access to the whole removable media.

You have to specify the settings in a policy of the type **Device Protection > Removable Media**:

- **Media encryption mode: File-based**

- **Key to be used for encryption: Any key in user key ring**

Allows the user to choose different keys for encrypting files on their removable media

- **Defined key for encryption:** <group/domain key > (for example group_users_Bob_Alice@DC=...). To ensure that the user can share data in their work group and to give them transparent access to removable media when they connect them to their computer at work.

- **User may define a media passphrase for devices: Yes**

The user defines one media passphrase on their computer which is valid for all their removable media.

- **Copy SG Portable to target: Yes**

SafeGuard Portable gives the user access to all encrypted files on the removable media by entering a single media passphrase on the system without SafeGuard Data Exchange.

If the company policies additionally define that all files on removable media have to be encrypted in any situation, add the following settings:

- **Initial encryption of all files: Yes**

Ensures that files on removable media are encrypted as soon as the media is connected to the system for the first time.

- **User may cancel initial encryption: No**

The user cannot cancel initial encryption, for example to postpone it.

- **User is allowed to access unencrypted files: No**

If plaintext files on removable media are detected, access to them will be denied.

- **User may decrypt files: No**

The user is not permitted to decrypt files on removable media.

At work, Bob and Alice have transparent access to encrypted files on removable media. At home, they can use SafeGuard Portable to open encrypted files by entering the media passphrase. If Bob or

Alice wants to hand out the removable media to a 3rd party computer that does not have SafeGuard Data Exchange installed, they can use local keys to ensure that the external party can access only some specific files. This is an advanced configuration, which means more interaction for the user by allowing them to create local keys on their computer.

 **Note** A prerequisite for this example is that the user is allowed to create local keys (default setting in SafeGuard Enterprise).

4.4.2 *Group keys*

To exchange encrypted data between users, SafeGuard Enterprise group keys have to be used. If the group key is in the users' key rings, the users get full transparent access to removable media connected to their computers.

On computers without SafeGuard Enterprise, it is not possible to access encrypted data on removable media, except the centrally defined domain/group key which can be used together with the media passphrase.

 **Note** To use/share encrypted data on removable media also on/with computers/users that do not have SafeGuard Enterprise, SafeGuard Portable can be used. SafeGuard Portable requires the usage of local keys or a media passphrase.

4.4.3 *Local keys*

SafeGuard Data Exchange supports encryption using local keys. Local keys are created on the computers and can be used to encrypt data on removable media. They are created by entering a passphrase and are backed up in the SafeGuard Enterprise Database.

 **Note** By default a user is allowed to create local keys. If users should not be able to do so, you have to disable this option explicitly. This has to be done in a policy of the type **Device Protection with Local Storage Devices** as **Device protection target (General Settings > User is allowed to create a local key > No)**.

If local keys are used to encrypt files on removable media, these files can be decrypted using SafeGuard Portable on a computer without SafeGuard Data Exchange. When the files are opened with SafeGuard Portable, the user is prompted to enter the passphrase that was specified when the key was created. If the user knows the passphrase, they can open the file.

Using SafeGuard Portable every user who knows the passphrase can get access to an encrypted file on removable media. This way it is also possible to share encrypted data with partners who do not have SafeGuard Enterprise installed. They only need to be provided with SafeGuard Portable and the passphrase for the files they should have access to.

If different local keys are used to encrypt files on removable media, you can even restrict access to files. For example: You encrypt the files on a USB memory stick using a key with passphrase *my_localkey* and encrypt a single file named *ForMyPartner.doc* using the passphrase *partner_localkey*. If you give the USB memory stick to a partner and provide them with the passphrase *partner_localkey*, they will only have access to *ForMyPartner.doc*.

 **Note** By default SafeGuard Portable is automatically copied to removable media connected to the system as soon as content is written to media covered by an encryption rule. If you do not want SafeGuard Portable to be copied to removable media, deactivate the **Copy SG Portable to target** option in a policy of the type **Device Encryption**.

4.4.4 Media passphrase

SafeGuard Data Exchange allows you to specify that one single media passphrase for all removable media - except optical media - has to be created on the endpoints. The media passphrase provides access to the centrally defined domain/group key as well as to all local keys used in SafeGuard Portable. The user only has to enter one single passphrase and gets access to all encrypted files in SafeGuard Portable, regardless of the local key used for encryption.

On every endpoint, a unique Media Encryption Key for data encryption is automatically created for each device. This key is protected with the media passphrase and a centrally defined domain/group key. On a computer with SafeGuard Data Exchange it is therefore not necessary to enter the media passphrase to access encrypted files on the removable media. Access is granted automatically if the appropriate key is part of the user's key ring.

The domain/group key to be used has to be specified under **Defined key for encryption**.

Media passphrase functionality is available when the **User may define a media passphrase for devices** option is activated in a policy of the type **Device Protection**.

When this setting becomes active on the endpoint, the user is automatically prompted to enter a media passphrase, when he connects removable media for the first time. The media passphrase is valid on every Windows endpoint the user is allowed to log on to. The user may also change the media passphrase and it will be synchronized automatically when the passphrase known on the computer and the media passphrase of the removable media are out of sync.

If the user forgets the media passphrase, it can be recovered by the user without any need of a helpdesk.

 **Note**

To enable the media passphrase, activate the **User may define a media passphrase for devices** option in a policy of the type **Device Protection**. This is only available, if you have selected **Removable media** as **Device protection target**.

On Macs the media passphrase is not supported.

4.4.4.1 Media passphrase and unmanaged endpoints

On an unmanaged endpoint (operating in standalone mode) without an activated media passphrase feature, no keys are available after installation since unmanaged endpoints only use local keys. Before encryption can be used, the user has to create a key.

If the media passphrase feature is activated in a removable media policy for these endpoints, the media encryption key is created automatically on the endpoint and can be used for encryption immediately after installation has been completed. It is available as a predefined key in the user's key ring and displayed as <user name> in dialogs for key selection.

If available, the media encryption keys is also used for all initial encryption tasks.

4.4.5 Configure trusted and ignored applications for SafeGuard Data Exchange

You can define applications as trusted to grant them access to encrypted files. This is for example necessary to enable antivirus software to scan encrypted files.

You can also define applications as ignored to exempt them from transparent file encryption/decryption. For example, if you define a backup program as an ignored application, encrypted data backed up by the program remains encrypted.

 **Note** Child processes will not be trusted/ignored.

1. In the **Policies** navigation area, create a new policy of the type **General Settings** or select an existing one.
2. Under **File Encryption**, click the drop-down button of the **Trusted Applications** or **Ignored Applications** field.
3. In the editor list box, enter the applications to be defined as trusted/ignored.
 - You can define multiple trusted/ignored applications in one policy. Each line in the editor list box defines one application.
 - Application names must end with .exe.
 - Application names must be specified as fully qualified paths including drive/directory information. Entering the file name only (for example "example.exe") is not sufficient. For better usability the single line view of the application list only shows the file names separated by semicolons.
4. Save your changes.

 **Note** The **Trusted Applications** and **Ignored Applications** policy settings are machine settings. The policy must therefore be assigned to machines, not to users. Otherwise the settings do not become active.

4.4.6 Configure ignored devices for SafeGuard Data Exchange

You can define devices as ignored to exclude them from the file encryption process. You can only exclude entire devices.

1. In the **Policies** navigation area, create a new policy of the type **General Settings** or select an existing one.
2. Under **File Encryption**, click the drop-down button of the **Ignored Devices** field.
3. In the editor list box, enter the required device names to exclude specific devices from encryption. This may be useful when you need to exclude systems from third party suppliers.

 **Note** You can display the names of the devices currently used in the system by using the Fltmc.exe control program (fltmc volumes, fltmc instances) from Microsoft, see <https://docs.microsoft.com/en-us/windows-hardware/drivers/ifs/development-and-testing-tools> .

4.4.7 Configure persistent encryption for SafeGuard Data Exchange

With persistent encryption, copies of encrypted files will be encrypted, even if they are saved in a location not covered by an encryption rule.

You can configure persistent encryption in policies of type **General Settings**. The policy setting **Enable persistent encryption** is activated by default.

When a user saves an encrypted file with **Save As** under a different file name in a location not covered by an encryption rule, the file will be plaintext.

The **Enable persistent encryption** setting has no effect if files are copied or moved to an ignored device or location. You define ignored locations in a policy of type **File Encryption > Location-based > Mode > Ignore**.

4.4.8 SafeGuard Data Exchange and File Encryption

The SafeGuard Enterprise module File Encryption offers file-based encryption on network locations, especially for work groups on network shares.

If both SafeGuard Data Exchange and File Encryption are installed on an endpoint, it may occur that a SafeGuard Data Exchange encryption policy is defined for a drive on the computer and File Encryption policies are defined for folders on the same drive. If this is the case, the SafeGuard Data Exchange encryption policy overrules the File Encryption policies. New files are encrypted according to the SafeGuard Data Exchange encryption policy.

For further information see [Location-based File Encryption \(page 302\)](#).

4.5 SafeGuard Enterprise and self-encrypting, Opal-compliant hard drives

Self-encrypting hard drives offer hardware-based encryption of data when they are written to the hard disk. The Trusted Computing Group (TCG) has published the vendor-independent Opal standard for self-encrypting hard drives. Different hardware vendors offer Opal-compliant hard drives. SafeGuard Enterprise supports the Opal standard and offers management of endpoints with self-encrypting Opal-compliant hard drives. For more information, see [Sophos knowledge base article 113366](#).

4.5.1 How does SafeGuard Enterprise integrate Opal-compliant hard drives?

With SafeGuard Enterprise, endpoints with self-encrypting, Opal-compliant hard drives can be managed from the SafeGuard Management Center, like any other endpoint protected by SafeGuard Enterprise.

Central and fully transparent management of Opal-compliant hard drives by SafeGuard Enterprise allows for the use in heterogeneous IT environments. By supporting the Opal standard, we offer the full set of SafeGuard Enterprise features to corporate users of self-encrypting, Opal-compliant hard drives. In combination with SafeGuard Enterprise, Opal-compliant hard drives offer enhanced security features.

4.5.2 Enhancement of Opal-compliant hard drives with SafeGuard Enterprise

SafeGuard Enterprise offers the following benefits in combination with self-encrypting, Opal-compliant hard drives:

- Central management of endpoints

- SafeGuard Power-on Authentication with graphical user interface
- Multi-user support
- Token/smartcard logon support
- Fingerprint logon support
- Recovery (Local Self Help, Challenge/Response)
- Central auditing
- Encryption of removable media (for example USB memory sticks) with SafeGuard Data Exchange

4.5.3 Manage endpoints with Opal-compliant hard drives with SafeGuard Enterprise

In the SafeGuard Management Center, you can manage endpoints with self-encrypting, Opal-compliant hard drives just like any other endpoint protected by SafeGuard Enterprise. As a security officer, you can define security policies, for example authentication policies, and deploy them to endpoints.

Once an endpoint with an Opal-compliant hard drive is registered at SafeGuard Enterprise, information on user, computer, logon mode and encryption status is displayed. In addition, events are logged.

Management of endpoints with Opal-compliant hard drives in SafeGuard Enterprise is transparent, which means that management functions in general work the same as for other endpoints protected by SafeGuard Enterprise. The type of a computer is shown in **Inventory** of a container in **Users and Computers**. The column **POA Type** tells you if the respective computer is encrypted by SafeGuard Enterprise or uses a self-encrypting, Opal-compliant hard drive.

4.5.4 Encryption of Opal-compliant hard drives

Opal-compliant hard drives are self-encrypting. Data are encrypted automatically when they are written to the hard disk.

The hard drives are locked by an AES 128/256 key used as an Opal password. This password is managed by SafeGuard Enterprise through an encryption policy, see [Lock Opal-compliant hard drives \(page 334\)](#).

4.5.5 Lock Opal-compliant hard drives

To lock Opal-compliant hard drives, the machine key has to be defined for at least one volume on the hard drive in an encryption policy. In case the encryption policy includes a boot volume, the machine key is defined automatically.

1. In the SafeGuard Management Center, create a policy of the type **Device Protection**.
2. In the field **Media encryption mode**, select **Volume-based**.
3. In the field **Key to be used for encryption**, select **Defined machine key**.
4. Save your changes in the database.
5. Deploy the policy to the relevant endpoint.

The Opal-compliant hard drive is locked and can only be accessed by logging on to the computer at the SafeGuard Power-on Authentication.

4.5.6 Enable users to unlock Opal-compliant hard drives

As a security officer, you can enable users to unlock Opal-compliant hard drives on their endpoints by using the **Decrypt** command from the Windows Explorer context menu.

Prerequisite: In the Device Protection policy that applies to the Opal-compliant hard drive, the option **User may decrypt volume** must be set to **Yes**.

1. In the SafeGuard Management Center, create a policy of the type **Device Protection** and include all volumes on the Opal-compliant hard drive.
2. In the field **Media encryption mode**, select **No encryption**.
3. Save your changes in the database.
4. Deploy the policy to the relevant endpoint.

The user can unlock the Opal-compliant hard drive on the endpoint. In the meantime, the hard drive remains locked.

4.5.7 Logging of events for endpoints with Opal-compliant hard drives

Events reported by endpoints with self-encrypting, Opal-compliant hard drives are logged, just as for any other endpoint protected by SafeGuard Enterprise. The events do not especially mention

the computer type. Events reported are the same as for any other endpoint protected by SafeGuard Enterprise.

For further information, see [Reports \(page 208\)](#).

4.6 SafeGuard Configuration Protection

The module SafeGuard Configuration Protection is no longer available as of SafeGuard Enterprise 6.1. The corresponding policy as well as the Suspension Wizard are still available in the SafeGuard Management Center 8.3 to support SafeGuard Enterprise 6 or even 5.60 clients with Configuration Protection installed and managed with an 8.3 Management Center.

For further information on SafeGuard Configuration Protection, refer to the *SafeGuard Enterprise 6 Administrator help*: http://www.sophos.com/en-us/medialibrary/PDFs/documentation/sgn_60_h_eng_admin_help.pdf.

4.7 About uninstallation

Uninstalling the SafeGuard Enterprise encryption software from endpoints involves the following steps:

- Decrypt encrypted data.
- Uninstall the configuration package.
- Uninstall the encryption software.

The appropriate policies must be effective on the endpoints to allow for decryption and uninstallation.

When a user with admin rights logs on to the endpoint after the uninstallation, a cleanup tool is started in the background. A message informs the user that the cleanup requires a final reboot.

You can find the cleanup tool here: C:\Program Files (x86)\Sophos\SafeGuard Enterprise \SGNCleanUp.exe

4.7.1 Start uninstallation

The following prerequisites must be met:

- Encrypted data has to be decrypted properly to allow access afterwards. The decryption process must be completed. Proper decryption is particularly important when uninstallation is triggered by Active Directory.

- Also, all encrypted removable media must be decrypted before uninstalling the last accessible SafeGuard Enterprise protected endpoint. Otherwise users may not be able to access their data any more. As long as the SafeGuard Enterprise Database is available, data on removable media can be recovered.
- To uninstall SafeGuard full disk encryption, all volume-based encrypted volumes must have a drive letter assigned to them.
- Make sure that you always uninstall the complete package with all features installed.

1. In SafeGuard Management Center, edit the policy of the type **Specific Machine Settings**. Set **Uninstallation allowed** to **Yes**.
2. In **Users and Computers**, create a group for the computers you want to decrypt: Right-click the domain node where you want to create the group. Then select **New > Create new group**.
3. Select the domain node of this group and assign the uninstallation policy to it by dragging the policy from the **Available Policies** list into the **Policies** tab. Activate the policy by dragging the group from the **Available Groups** list into the **Activation** area. On the **Policies** tab of the domain node, check that **Priority** is set to 1 and that **No Override** is activated. In the **Activation** area of the domain node, make sure that only members of the group are affected by this policy.
4. Add the endpoints you want to uninstall to the group.
5. To start uninstallation, use one of the following methods:
 - To uninstall locally on the endpoint, synchronize with the SafeGuard Enterprise Server to make sure that the policy update has been received and is active. Then, remove the Sophos SafeGuard Client software.
 - To uninstall centrally use the software distribution mechanism of your choice. Make sure that all required data has been decrypted properly before uninstallation starts.

4.7.2 Preventing uninstallation on the endpoints

To provide extra protection for endpoints, we recommend that you prevent local uninstallation of SafeGuard Enterprise on endpoints. In a **Specific Machine Settings** policy, set **Uninstallation allowed** to **No** and deploy the policy on the endpoints. Uninstallation attempts are then cancelled and the unauthorized attempts are logged.

5. Managing Mac endpoints

Macs that have the following Sophos products installed can be managed by SafeGuard Enterprise and/or report status information. The status information is displayed in the SafeGuard Management Center:

- Sophos SafeGuard File Encryption for Mac 6.1 and later
- Sophos SafeGuard Native Device Encryption 7.0 and later
- Sophos SafeGuard Disk Encryption for Mac 6.1

5.1 *Create configuration package for Macs*

A configuration package for a Mac contains the server information and the company certificate. The Mac uses this information to report status information (SafeGuard POA on/off, encryption state and so on). The status information is displayed in the SafeGuard Management Center.

1. In the SafeGuard Management Center, on the **Tools** menu, click **Configuration Package Tool**.
2. Select **Managed client packages**.
3. Click **Add Configuration Package**.
4. Enter a name of your choice for the configuration package.
5. Assign a primary SafeGuard Enterprise Server (the secondary server is not necessary).
6. Select **SSL** as **Transport Encryption** for the connection between the endpoint and SafeGuard Enterprise Server. **Sophos** as **Transport Encryption** is not supported for Mac.
7. Specify an output path for the configuration package (ZIP).
8. Click **Create Configuration Package**.
The server connection for the **SSL Transport Encryption** mode is validated. If the connection fails, a warning message is displayed.

The configuration package (ZIP) has now been created in the specified directory. You now need to distribute and deploy this package to your Macs.

5.2 *About SafeGuard Native Device Encryption for Mac*

Sophos SafeGuard Native Device Encryption for Mac offers macOS users the same data protection that the full disk encryption feature of SafeGuard Enterprise already offers to Windows users.

SafeGuard Native Device Encryption for Mac builds on the full disk encryption technology integrated in macOS. It uses FileVault 2 to encrypt the entire hard disk, so that your data is safe even if the computer is lost or stolen. However, it also enables you to provide and manage disk encryption for entire networks.

The encryption works transparently. The user will not see any prompts for encryption or decryption when opening, editing, and saving files.

In the SafeGuard Enterprise Management Center, you can select which computers (Windows as well as Macs) to encrypt, monitor their encryption status, and provide recovery for users who forget their passwords.

5.2.1 *Manage FileVault 2 endpoints with SafeGuard Management Center*

In the SafeGuard Management Center, FileVault 2 endpoints can be managed just like any native SafeGuard Enterprise endpoints. As a security officer you can set encryption policies for the FileVault 2 endpoints and distribute them.

Once a FileVault 2 endpoint is registered at SafeGuard Enterprise, information on user, computer, logon mode and encryption status is displayed. Events are logged for FileVault 2 clients as well.

Management of the FileVault 2 in SafeGuard Enterprise is transparent, which means that management functions generally work the same way for FileVault 2 and native SafeGuard Enterprise clients. You can find out on the type of a computer in the **Inventory** of a container in **Users and Computers**. The column **POA Type** tells you if the respective computer is a FileVault 2 client.

5.2.2 *Encryption policies for FileVault 2 full disk encryption*

The security officer can create a policy for encryption in the SafeGuard Management Center and distribute it to the FileVault 2 endpoints where it is executed.

As the FileVault 2 endpoints are managed transparently in the SafeGuard Management Center, the security officer does not necessarily have to specify any special FileVault 2 settings for encryption. SafeGuard Enterprise knows the client status and selects the FileVault 2 encryption accordingly.

A FileVault 2 endpoint only processes policies of type **Device Protection** with target **Boot Volumes** and **Media encryption mode** set to **Volume-based** or **No encryption**. All other policy settings are ignored.

- **Volume-based** activates FileVault 2 on the endpoint.
- **No encryption** allows the user to decrypt the Mac.

5.2.3 Policies

SafeGuard Native Device Encryption for Mac only makes use of policies of the type **Device Protection** and **General Settings** and ignores all policy settings except **Target**, **Media encryption mode** and **Connection interval to server (min)**.

5.2.3.1 Centrally administered configuration options

Policies are configured centrally in the SafeGuard Management Center. In order to initiate full disk encryption, the settings must be chosen as follows:

1. Create a new policy of type **Device Protection**. For **Device protection target**, choose **Local Storage Devices**, **Internal Storage**, or **Boot Volumes**. Type a name for the policy and click **OK**.
2. For **Media encryption mode**, select **Volume based**.

A new policy for device protection has been created and configured for full disk encryption for Macs.

Note

Make sure that the policy is assigned to the endpoints you want encrypted. You can assign the policy to the top level of your domain or workgroup. If IT staff take care of the installation, do not assign the policy before the endpoint computers are issued to the end users. There is the risk that the endpoint is encrypted too early and IT staff are registered for FileVault 2 instead of the end users.

5.2.4 How does encryption work?

FileVault 2 keeps all data on the hard drive secure with XTS-AES-128 data encryption at the disk level. The algorithm has been optimized for 512-byte blocks. The conversion from plaintext to ciphertext and back is performed on the fly with low impact on the user experience since it is given a lower priority.

One traditional obstacle to usability with full disk encryption is that it was necessary for the end user to authenticate twice: once to unlock the encrypted boot volume (POA), and the second time to log on to the user desktop.

However, this is no longer necessary. Users enter their password at the pre-boot logon and the system initiates password-forwarding when the operating system is up and requiring logon credentials. Password-forwarding eliminates the need for users to log on twice after a cold boot.

Users are able to reset their passwords at any time without the need to re-encrypt the volume. The reason is that a multi-level key system is employed. The keys shown to the users (for example logon keys and recovery keys) are derived encryption keys and therefore can be replaced. The true volume encryption key will never be given to a user.

For further information on FileVault 2 see *Apple Technical White Paper - Best Practices for Deploying FileVault 2 (Aug. 2012)*, which can be downloaded from the Apple website.

5.2.5 Initial encryption

When you define a volume-based encryption of the system disk via policy, disk encryption starts automatically as soon as the user restarts the endpoint. The user needs to do the following:

1. Enter the macOS password.
2. Wait for the Mac to restart.

 **Note** If activation of the encryption fails, an error message is displayed. More information can be found in the log files. The default location is `/var/log/system.log`. Search for the keyword `fdesetup`.

3. Disk encryption starts and is done in the background. The user can continue working.

The user is added as the first FileVault 2 user of the endpoint.

5.2.6 Decryption

Usually it is not necessary to decrypt. If you set a policy that specifies **No encryption** for Mac clients that are already encrypted, they will remain encrypted. However, in this case, users have the choice to decrypt. They will find the corresponding button in the Disk Encryption tab of the preference pane.

Users with local administrator rights cannot be prevented from attempting to manually decrypt their hard disk using built-in FileVault 2 functionality. However, they will be prompted for a restart to

complete the decryption. As soon as the Mac has completed the restart, SafeGuard Native Device Encryption for Mac will enforce encryption if a corresponding policy has been set.

5.2.7 Add FileVault 2 user

On endpoints running macOS 10.13 or later, all existing users of an endpoint are added to FileVault automatically.

On endpoints running macOS 10.12 or earlier, each user needs to log in separately to be added to FileVault. To add a user to FileVault, proceed as follows:

1. While the Mac is still running, log in with the user you want to register for FileVault.
2. Provide the credentials of that user in the dialog **Enable Your Account**.

Users will be able to log in as easily as if there was no disk encryption enforced.

You cannot assign users to endpoints in the Management Center to allow them to use FileVault 2.

5.2.8 Remove FileVault 2 user

A user can be removed from the list of users assigned to a Mac in the SafeGuard Management Center. After the next synchronization, the user will be removed from the list of FileVault 2 users of the endpoint as well. But this does not mean that the user will not be able to log on to that Mac anymore. Like any new user, the user just needs to log on to a running Mac in order to become authorized again.

If you really want to prevent a user from booting a Mac, **mark the user as blocked** in the Management Center. The user will then be removed from the list of FileVault 2 users of the client and no new authorization will be possible.

It is possible to remove all FileVault 2 users but the last one. If the owner is removed, then the next user in the list will be marked as owner. In SafeGuard Native Device Encryption for Mac it does not make a difference if a user is owner or not.

5.2.9 Synchronization with backend

In the process of synchronization, the states of the clients are reported to the SafeGuard Enterprise backend, policies are updated and the user-machine assignment is checked.

Therefore, the following information is sent from the clients and appears in the SafeGuard Management Center:

- As soon as an endpoint is encrypted, "POA" is checked. Other information that is displayed includes drive name, label, type, state, algorithm and operating system.
- New FileVault 2 users are added also in the Management Center.

 **Note** If the SafeGuard Enterprise client software is removed from an endpoint, the endpoint and its users are still visible in the SafeGuard Management Center. But the timestamp of the last server contact does not change any more.

On the client side, the following things are changed:

- Policies that were changed in the Management Center are changed on the client.
- Users that have been deleted or blocked in the Management Center are also removed from the list of FileVault 2 users on the client.

5.2.10 Command line options

The Terminal application allows you to enter commands and command line options. The following command line options are available:

Command name	Definition	Additional parameters (optional)
sgdeadmin	Lists available commands including short help hints.	--help
sgdeadmin --version	Displays version and copyright information of the installed product.	
sgdeadmin --status	Returns system status information such as version, server and certificate information.	
sgdeadmin --list-user-details	Returns information on the user currently logged on.	--all displays information for all users (sudo required) --xml returns output in xml format.
sgdeadmin --list-policies	Displays policy-specific information. Key GUIDs are resolved to key names if possible.	--all displays information for all users (sudo required)

Command name	Definition	Additional parameters (optional)
sgdeadmin --synchronize	Bold print indicates a personal key.	--xml returns output in xml format
sgdeadmin --import-recoverykey ["recoverykey"]	Forces immediate contact with the server (needs working server connection).	
sgdeadmin --import-config "/path/to/target/file"	Imports the FileVault 2 recovery key, overwrites existing recovery key.	--force existing recovery key will be overwritten without any additional confirmation
		"recoverykey" if it is not entered, the user will be asked for it
sgdeadmin --enable-server-verify	Imports the specified configuration zip file. The command needs administrative rights (sudo).	<p> Note Use the drag and drop functionality to drag a complete path from, for example, the Finder into the Terminal application.</p>
sgdeadmin --disable-server-verify	Turns on SSL server verification for communication with the SafeGuard Enterprise server. After installation, the SSL server verification is activated. The command needs administrative rights (sudo).	
	Turns off SSL server verification for communication with the SafeGuard Enterprise server. The command needs administrative rights (sudo).	<p> Note</p>

Command name	Definition	Additional parameters (optional)
sgdeadmin --update-machine-info [--domain "domain"]	We do not recommend this option as it may create a security vulnerability.	--domain "domain"
sgdeadmin --enable-systemmenu	Updates the currently stored machine information which is used to register this client on the SafeGuard Enterprise Server. The Enterprise Server. This parameter command needs administrative rights (sudo).	The domain the client should use to register on the SafeGuard Enterprise Server. This parameter is only required if the computer is a member of multiple domains. The computer must be joined to this domain, otherwise the command will fail.
sgdeadmin --disable-systemmenu	Use this command only after changing the domain or workgroup the computer belongs to. If the computer is a member of multiple domains or workgroups and you execute this command, this might result in a change of the domain registration and removal of personal keys and/or FileVault 2 users.	
sgdeadmin --synchronize	Activates the system menu on the endpoint. Deactivates the system menu on the endpoint. Starts synchronizing database information from the SafeGuard Enterprise backend such as policies and keys.	

5.2.11 Recovery key for Mac endpoints

Access to FileVault 2 encrypted SafeGuard Enterprise Clients can be regained with the following procedure:

1. In the SafeGuard Management Center, select **Tools > Recovery** to open the **Recovery Wizard**.
2. On the **Recovery type** page, select **SafeGuard Enterprise Client (managed)**.
3. Under **Domain**, select the required domain from the list.

4. Under **Computer** enter or select the required computer name. There are several ways to do so:

- To select a name, click [...]. Then click **Find Now**. A list of computers is displayed. Select the required computer and click **OK**. The computer name is displayed in the **Recovery type** window under **Domain**.
- Type the short name of the computer directly into the field. When you click **Next**, the database is searched for this name. If it is found, the distinguished computer name is displayed.
- Enter the computer name directly in distinguished name format, for example:

CN=Desktop1,OU=Development,OU=Headquarter,DC=Utimaco,DC=edu

5. Click **Next**.

6. The Recovery Wizard displays the corresponding 24-digit recovery key.

7. Provide this key to the user.

The user can enter the recovery key to get logged on to the Mac endpoint and reset the password.

5.2.12 Recovery key handling

If all FileVault-enabled users on a particular system forget their passwords, other credentials are not available and there is no recovery key available, then the encrypted volume cannot be unlocked and the data is inaccessible. Data may be lost permanently, so proper recovery planning is essential.

A new recovery key is generated during each activation of disk encryption. Without Sophos SafeGuard Native Device Encryption being installed at the time of the encryption, it is displayed to the user who consequently is responsible for its protection against loss. With Sophos SafeGuard Native Device Encryption, it is securely sent to the SafeGuard Enterprise backend and stored centrally. The security officer can retrieve it whenever needed. See [Reset forgotten password \(page 358\)](#).

SafeGuard Management Center automatically changes the FileVault recovery key after it has been retrieved.

But even if SafeGuard Native Device Encryption was not installed when the disk was encrypted, the recovery key can be managed centrally. Therefore it is necessary to import it. The relevant command line option is `sgdeadmin --import-recoverykey`, see also [Command line options \(page 342\)](#). The recovery key will be sent in upper case.

If there is an institutional recovery key present, it can be used for recovery as well. For more information, see support.apple.com/kb/HT5077.

5.2.13 Password handling

The Sophos SafeGuard key ring is secured with a user certificate. The corresponding private key is protected by the macOS password.

The password is required to allow the certificate to be generated if the user has not been created in SafeGuard Enterprise.

Changing password locally

Users can change their passwords locally in **System Preferences > Users & Groups**, and no further steps are required.

Password has been changed on a different endpoint

 **Note** Passwords can be changed on Windows as well as Mac endpoints.

Since the password is no longer known on this endpoint the following steps need to be completed:

1. Log in to macOS with your new password.
2. **The system was unable to unlock your keychain** is displayed.
3. Select **Update Keychain Password**.
4. Enter the old password.

For details of how to reset a forgotten password, see [Reset forgotten password \(page 358\)](#).

5.3 About SafeGuard File Encryption for Mac

Sophos SafeGuard File Encryption for Mac extends the data protection offered by Sophos SafeGuard Enterprise from Windows to the Mac world. It offers file-based encryption on local drives, network shares, removable drives, and in the cloud.

With SafeGuard File Encryption for Mac, you can safely encrypt and decrypt files and exchange these files with other users on Macs or Windows PCs.

To read files encrypted by SafeGuard Enterprise on mobile devices, use Sophos Secure Workspace for iOS or Android.

Configure encryption rules

In the SafeGuard Management Center, you define rules for file-based encryption in File Encryption policies. In these file encryption policies, you specify the folders that are to be handled by File

Encryption, the encryption mode and the key to be used for encryption. This central management guarantees that identical folders and encryption keys are processed on different platforms, see [Configuring encryption rules in location-based File Encryption policies \(page 303\)](#).

Excluded folders

The following folders are excluded from encryption:

- **Folders are excluded, but not their subfolders:**
 - <Root>/
 - <Root>/Volumes/
 - <User Profile>/
- **Folders as well as their subfolders are excluded:**
 - <Root>/bin/
 - <Root>/sbin/
 - <Root>/usr/
 - <Root>/private/
 - <Root>/dev/
 - <Root>/Applications/
 - <Root>/System/
 - <Root>/Library/
 - <User Profile>/Library/
 - /<Removables>/SGPortable/
 - /<Removables>/System Volume Information/

This means that, for example, an encryption rule for the root of an additional partition (<Root>/Volumes/) has no effect, although it will be shown as a received policy.

An encryption rule on <Root>/abc will have an effect, while an encryption rule on <Root>/private/abc will not.

Reduce administration effort

- Keep the number of mount points (or Secured Folders) as low as possible.
- Deactivate the option **Require confirmation before creating a mobile account**.

If you create or use mobile accounts for Mac endpoints, make sure the option **Require confirmation before creating a mobile account** is deactivated. With the option activated, the user could select **Don't Create**. This would result in the creation of an incomplete macOS user, for example a user that does not have a local home directory.

To deactivate the option, perform the following steps:

1. Open the **System Preferences** and click on **Users & Groups**.
2. Click the lock icon, then enter your password.
3. Select the User.

4. Click **Login Options**.
5. Go to **Network Account Server** and click **Edit....**
6. Select the Active Directory Domain.
7. Click **Open Directory Utility....**
8. Click the lock icon, then enter your password and click **Modify Configuration**.
9. Select Active Directory and click the edit icon.
10. Click the arrow next to **Show Advanced Options**.
11. Select **Create mobile account at login** and deselect the option **Require confirmation before creating a mobile account**.
12. Click **OK**.

Limitations

- **Maximum number of Secured Folders (mount points) on a client**

On each macOS client you can have a maximum of 24 Secured Folders (mount points). If more than one user is logged in on a single machine, you need to add up the mount points from all logged-in users.

- **Searching for files**

- **Spotlight**

By default, searching for files in Secured Folders using Spotlight is not possible.

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

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.

- **Labeled files**

Searching for labeled files does not work in Secured Folders.

- **Moving encrypted files from Secured Folders**

When you move an encrypted file from a Secured Folder to non-Secured Folder, the file will still be encrypted, but you will not be able to access its content. You need to decrypt it first manually.

When you open an encrypted file in a Secured Folder and save it in a non-Secured Folder, the file will be decrypted automatically.

- **Permanent version storage is not available in Secured Folders**

For files in Secured Folders, the standard functionality **Browse All Versions...** is not available.

- **Sharing Secured Folders**

A Secured Folder cannot be shared over the network.

- **Burning CDs**

It is not possible to burn an encrypted CD.

- **Deleting files**

When deleting files from a Secured Folder (mount point), a message prompts you to confirm the delete process. Deleted files are not moved to the Trash folder and thus cannot be restored.

- **SafeGuard Portable**

SafeGuard Portable is not available for Macs.

- **Use of AirDrop**

Encrypted files can be transferred with AirDrop. Ensure that the target device can handle encrypted files. If it cannot, applications may behave unpredictably.

- **Handoff**

Using Handoff for encrypted files is not supported.

- **Mounting network file shares with `autofs`**

Network file shares which have a policy applied and are automatically mounted at startup will not be detected by Sophos SafeGuard File Encryption. It is not possible to handle such mount points because the original mount point cannot be replaced.

5.3.1 Centrally administered configuration options

The following options are configured centrally in the Management Center:

- **Policies**
- **Keys**

- **Certificates**

The SafeGuard Enterprise backend provides the X.509 certificate for the user. When logging in for the first time, a certificate is generated. The certificate secures the user's key ring.

- **Connection interval to server**

5.3.2 Policies

SafeGuard File Encryption for Mac only uses policies of the type **File Encryption** and **General Settings**. This means that you only need to use a **File Encryption** policy for managing encryption of data on the local file system, removable media, network shares and cloud storage.

Device Protection policies (including **Cloud Storage** and **Removable Media Encryption** policies) will be ignored for SafeGuard File Encryption for macOS. Always assign **File Encryption** policies to the user objects. **File Encryption** policies assigned to endpoints will not have any effect on macOS endpoints.

 **Note** In the SafeGuard Management Center, paths have to be entered using backslashes. They are automatically converted to forward slashes on the Mac endpoint.

5.3.3 Encrypting files in cloud storage

SafeGuard Enterprise offers file-based encryption of data stored in the cloud.

It does not change the way users work with data stored in the cloud. Users still use the same vendor specific synchronization applications to send data to or receive data from the cloud. Local copies of data stored in the cloud are encrypted transparently and will therefore always be stored in the cloud in encrypted form.

On Macs, SafeGuard Enterprise offers auto-detection for the following cloud storage providers:

- Box
- Dropbox (includes Dropbox Business)
- Google Drive
- OneDrive
- OneDrive for Business

For these providers you only need to specify the path to the synchronization folders in a location-based policy of the type **File Encryption**.

For application-based encryption of files in cloud storage, you can use predefined placeholders, see [Configure application-based File Encryption in the cloud \(page 387\)](#)

After the policy has been assigned to endpoints, files in locations covered by the policy are transparently encrypted without user interaction:

- Encrypted files will be synchronized into the cloud.
- Encrypted files received from the cloud can be handled by applications as usual.

Data stored in the cloud before you activated encryption is not encrypted automatically. To make sure that sensitive files on their computers are encrypted, users can perform an initial encryption, see [Initial encryption \(page 352\)](#).

5.3.3.1 Configure location-based File Encryption in the cloud

1. In the **Policies** navigation area, create a new policy of the type **File Encryption** or select an existing one.

The **File Encryption** tab is displayed.

2. Select **Location-based** from the **Encryption type** drop-down list.

The table to specify locations where location-based file encryption is applied on the endpoint computer is displayed.

3. In the **Path** column, set the path to the cloud storage synchronization folder, for example `<User Profile>\Dropbox`.

- Click the drop-down button and select a folder name placeholder from the list of available placeholders.

By hovering your cursor over the list entries, you can display tooltips telling you how a placeholder is typically presented on an endpoint. You can only enter valid placeholders. For a description of all available placeholders, see [Placeholders for paths in location-based File Encryption rules \(page 306\)](#).

- Alternatively, just enter path and folder name.

Note

The local synchronization folder must not be changed by the users. For example, if they move the folder, encryption of files stored in the cloud will stop working.

If the synchronization folder on the endpoints changes, you must adjust the path in the encryption rule accordingly.

4. In the **Scope** column, select one of the following:

- **Only this folder** to apply the rule only to the folder indicated by the **Path** column.
- **Include subfolders** to also apply the rule to all its subfolders.

5. In the **Mode** column, Select **Encrypt**.

6. In the **Key** column, select the key to be used for the **Encrypt** mode. You can use keys created and applied in **Users and Computers**:

- Click the **Browse** button to open the **Find Keys** dialog. Click **Find now** to display a list of all available keys and select the required key.

 **Note** Machine keys are not shown in the list. They cannot be used by File Encryption as they are only available on a single computer and can therefore not be used to enable groups of users to access the same data.

- Click the **Personal Key** button with the key icon to insert the **Personal Key** placeholder in the **Key** column. On the endpoint, this placeholder will be resolved to the active Personal Key of the logged on SafeGuard Enterprise user. If the relevant users do not have active Personal Keys yet, they are created automatically. You can create Personal Keys for single or multiple users in **Users and Computers**. For further information, see [Personal Keys for file-based encryption by File Encryption \(page 161\)](#).

7. Add further paths as required.

8. Save your changes.

9. Go to **Users and Computers** and assign the new policy to your user groups.

5.3.3.2 Troubleshooting and additional cloud storage providers

Sophos SafeGuard normally detects cloud synchronization folders automatically. However, if cloud storage vendors release a new version of their software and change some of their default settings, this auto-detection might fail.

In this case, ask Sophos support to provide you with a configuration file. For details, see [Sophos knowledge base article 126321](#).

You can also add new cloud storage providers to this configuration file so they are detected automatically as well.

5.3.4 Initial encryption

Initial file encryption can be started from the preference pane or from the command line tool. Both administrators and end users can trigger initial encryption for files on local drives and removable media. Network shares can only be encrypted by administrators.

A policy defines, whether initial encryption is started automatically and whether local folders, removables, or cloud storage providers are encrypted.

To manually start encryption on the endpoint:

1. Open the **System Preferences**.
2. Click the Sophos SafeGuard icon.
3. Select the **Policies** tab.
4. Switch to **Locally Translated Path** view if not already opened. You can either
 - a. enforce all policies by clicking the **Enforce all policies** button in the lower part of the window
 - or
 - b. select a single policy and click the button **Enforce policy**.

 **Note** Do not disconnect devices while the initial encryption is running.

 **Note** If you want to see details and contents of the locally translated path, select the path from the table and click **Show in Finder**.

5.3.5 Fast user switching

SafeGuard File Encryption for Mac also works with fast user switching. It allows you to switch between user accounts on a single endpoint without quitting applications or logging out from the machine.

5.3.6 Use local keys

 **Note** Local keys cannot be used with SafeGuard Synchronized Encryption.

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. Right-click on a file or selection of files and select **Create New Key**.
2. Choose a name and a passphrase for your key and click **OK**.
The key name will be prefixed with "Local_" and postfixed with date and time.

The local key is created and displayed in the preference pane. The user can now apply the local key to a removable device or a cloud directory.

5.3.7 Command line options

The Terminal application allows you to enter commands and command line options. The following command line options are available:

Command name	Definition	Additional parameters (optional)
sgfsadmin	Lists available commands including short help hints.	--help
sgfsadmin --version	Displays version and copyright information of the installed product.	
sgfsadmin --status	Returns system status information such as version, server and certificate information.	
sgfsadmin --list-user-details	Returns information on the user currently logged on.	--all displays information for all users (sudo required) --xml returns output in xml format.
sgfsadmin --list-keys	Lists existing GUIDs and names of all keys in the keystore.	--all displays information for all users (sudo required) --hidden-keys displays only keys that are marked as hidden --xml returns output in xml format
sgfsadmin --list-policies	Displays policy-specific information. Key GUIDs are resolved to key names if possible. Bold print indicates a personal key.	--all displays information for all users (sudo required) --xml returns output in xml format

Command name	Definition	Additional parameters (optional)
sgfsadmin --enforce-policies	Applies the encryption policy.	--raw displays raw policies, i.e. policies as set on the SafeGuard Management Center server side
sgfsadmin --file-status	Returns encryption information for a file or a list of files. Wildcards are accepted.	--all applies the policy to all directories where policies apply
sgfsadmin --file-status "filename1" ["filename2"..."filenameN"]		"directoryname" applies the policy to the directory specified.
sgfsadmin --import-config "/path/to/target/file"	Imports the specified configuration zip file. The command needs administrative rights (sudo).	--xml returns output in xml format
	<p> Note Use the drag and drop functionality to drag a complete path from, for example, the Finder into the Terminal application.</p>	
sgfsadmin --enable-server-verify	Turns on SSL server verification for communication with the SafeGuard Enterprise server. After installation, the SSL server verification is activated. The command needs administrative rights (sudo).	
sgfsadmin --disable-server-verify	Turns off server verification for communication with the SafeGuard Enterprise server. The command needs administrative rights (sudo).	
	 Note	

Command name	Definition	Additional parameters (optional)
sgfsadmin --update-machine-info [--domain "domain"]	<p>We do not recommend this option as it may create a security vulnerability.</p>	<p>--domain "domain"</p> <p>The domain the client should use to register on the SafeGuard Enterprise Server. This parameter is only required if the machine is a member of multiple domains. The computer must be joined to this domain, otherwise the command will fail.</p>
sgfsadmin --dump-unprivileged-applications [path]	<p>Note</p> <p>Use this command only after changing the domain or workgroup the computer belongs to. If the computer is a member of multiple domains or workgroups and you execute this command, this might result in a change of the domain registration and removal of personal keys and/or FileVault 2 users.</p>	
sgfsadmin --synchronize	<p>Collects application paths that are not authorized to access encrypted files. You can use the information to add applications to the applications list. You can restrict the results to a specific path.</p> <p>Note This function is only relevant for Synchronized Encryption.</p>	

Command name	Definition	Additional parameters (optional)
sgfsadmin --enable-spotlight	Turns on Spotlight search.	
sgfsadmin --disable-spotlight	Turns off Spotlight search.	

5.3.8 Using Time Machine

 **Note** This section is only relevant if an encryption rule is configured for <Removables>.

If you want to use a new disk for a Time Machine backup and the operating system does not automatically suggest using it, use the following command in the Terminal application:

```
sudo tmutil setdestination -a "/Volumes/.sophos_safeguard_{DISK NAME}/"
```

If you use Time Machine for an encrypted folder, no backed up files are displayed. These backups are stored in a hidden location and contain only encrypted data. To restore files, proceed as follows:

1. Open Time Machine.
The content of your root folder is displayed.
2. Press **Shift - Command - G** (for "Go to the folder:") and enter the hidden path of the encrypted folder you want to restore.
If the encrypted folder you usually work with is named /Users/admin/Documents, then enter /Users/admin/.sophos_safeguard_Documents/.
3. Browse to the file you want to restore, click the wheel icon from the Time Machine menu bar and select **Restore <file name> to....**
4. Browse to the restored file in Finder and check its encryption state.
5. Encrypt the file manually if necessary.

 **Note** The first Time Machine backup after a new installation of SafeGuard File Encryption takes longer and requires more disk space than usual. This is because macOS does not allow stacked file systems and thus all local directories for which secure mount points have been created (Documents, Music, Movies, etc.), will be duplicated on the backup disk.

5.3.9 Working with removable media

To turn on encryption of files on removable media, a policy of type **File Encryption** with the placeholder <Removables> as **Path** is required, see [Placeholders for paths in location-based File Encryption rules \(page 306\)](#).

To be able to exchange and modify data on removable devices between two parties, both parties must have the corresponding policy and key assigned. No personal keys can be used.

Exchange data on removable media between macOS and Windows

For the exchange between Windows and macOS endpoints, removable media must be formatted using FAT32. Mac users can check the disk storage format using Disk Utility.

On the Windows endpoint a data exchange policy (policy of type **Device Protection** with **Removable media** as **Device protection target**, see [Device Protection \(page 259\)](#) or a policy of type **File Encryption** with the placeholder <Removables> as **Path** is required.

With a data exchange policy you can let the user decide whether she wants to encrypt data or not and to remember this setting by means of a policy setting. This policy setting is only evaluated on Windows machines. So if they use the removable media on a Mac and come back to their Windows endpoint they are prompted once to select their choice again. The media passphrase functionality is only available for Windows as well.

Best practice:

Defining a policy of type **File Encryption** may be the better choice since you can use a single policy for both Macs and Windows endpoints.

On Windows then users have to do without the possibility to decide if files on removable media should be encrypted or not since the **User is allowed to decide about encryption** option is not available in policies of type **File Encryption**.

On read-only removable media (for example SD cards with activated write protection), secured mountpoints cannot be created correctly. In practice, only use removable media that can be both read and written.

5.4 Troubleshooting

5.4.1 Reset forgotten password

 **Note** This instruction assumes that the user has both SafeGuard Disk Encryption and SafeGuard File Encryption or Synchronized Encryption installed on their Mac. If they are using only one of the above, steps may vary.

If a user forgets the macOS logon password, do the following:

1. Tell the user to open the logon dialog and click ?.

The password hint is displayed and the user is prompted to reset the password using the recovery key.

2. Tell the user to click on the triangle next to the message in order to get to the next step.
3. In the SafeGuard Management Center, select **Tools > Recovery** and display the recovery key for the specific machine.
4. Tell the user the recovery key to be entered in the logon dialog.
The recovery key is replaced as soon as it has been used once to start the system. The new recovery key is generated automatically and sent to the SafeGuard Enterprise backend where it is stored to be available for the next recovery.
5. In the SafeGuard Management Center, select **Users and Computers** and remove the user's certificate.
6. For local users, do the following:
 - a. Tell the user to define a new password and a password hint.
 - b. In the SafeGuard Management Center, select **Users and Computers > .Unconfirmed Users** and confirm the user.
 - c. Tell the user to open the **Server** tab in the Preference Pane and click **Synchronize**.
7. For Active Directory users, do the following:
 - a. Reset the existing password in your user administration environment and generate a preliminary password. Select the corresponding option to force the user to modify the password after the first login.
 - b. Contact the user, and hand over the preliminary password.
 - c. Tell the user to click **Cancel** in the **Reset Password** dialog and enter the preliminary password instead.
 - d. Tell the user to define a new password and a password hint and click **Reset Password**.
8. Tell the user to click **Create New Keychain** in the following dialog.
9. Tell the user to enter the new password to create the SafeGuard user certificate.

The user's keys will be loaded into the new keychain automatically, so all documents will be accessible as before.

 **Note** Be careful to whom you give a recovery key. As a recovery key is always machine specific and not user specific. Make sure that the recovery key is not used to get unauthorized access to another user's sensitive data on the same machine.

5.4.2 Problems with accessing data

If a user experiences problems when trying to access data, possible reasons are the following:

- The user has not yet been confirmed.

For information on unconfirmed users, see [Enhanced authentication - the .Unconfirmed Users group \(page 98\)](#).

 **Note** Local users always are unconfirmed users.

- The user does not have the required key in their key ring.

For information on assigning keys to users, see [Assign keys in Users and Computers \(page 160\)](#).

- The keys have been temporarily revoked for security reasons. The endpoint is considered unsafe (compromised).

5.4.3 Problems with using virtual machines

Virtualization applications such as VMware Fusion or Parallels cannot be used with a SafeGuard Enterprise mount point. We recommend that you start the virtual machine from a hidden folder instead.

Example:

Instead of starting the virtual machine from `~/Documents/Virtual Machines/`, use the path `~/.sophos_safeguard_documents/Virtual Machines`.

5.4.4 SafeGuard recovered files

Under certain circumstances a folder named **Sophos SafeGuard Recovered Files** can be found in a folder. This happens if SafeGuard File Encryption tries to create a new Secured Folder (mount point), but the hidden folder that needs to be created for storing the encrypted contents (for example `/Users/admin/.sophos_safeguard_Documents/`) exists already and is not empty. Then the content of the original folder (for example `/Users/admin/Documents`) will be moved to **Sophos SafeGuard Recovered Files** and only the content of the hidden folder will be displayed as usual.

5.4.5 Missing Secure Token

Users without a Secure Token cannot turn on FileVault.

If a user logs on without a Secure Token, and the policy requires FileVault to be on, a message is shown stating that FileVault cannot be turned on because of a missing Secure Token. The user is asked to contact the system administrator.

For assistance in solving this problem, see [Sophos knowledge base article 128052](#).

5.5 *Inventory and status data of Macs*

For Macs the **Inventory** provides the following data about each machine. The data displayed can differ, depending on the installed Sophos product:

- The name of the Mac
- The operating system
- The POA type
- The number of encrypted drives
- The number of unencrypted drives
- The last server contact
- The modification date
- Whether the current company certificate is used or not

5.6 *Uninstall Native Device Encryption from Mac endpoints*

If you need to uninstall the software from a client computer, proceed as follows:

1. On the Mac client go to */Library*.
2. Select the folder */Sophos SafeGuard DE*.
3. Select and double-click the file *Sophos SafeGuard DE Uninstaller.pkg*
4. A wizard guides you through uninstallation.

As soon as the last Sophos SafeGuard product is removed, the client configuration is deleted as well.

It is not necessary to decrypt the disk before uninstalling the software.

A user with administrative rights cannot be prevented from uninstalling the software. (A policy that prevents this on Windows clients has no effect on Mac clients).

The uninstaller package is signed, and macOS will try to validate this signature. This procedure may take several minutes.

5.7 *Uninstall File Encryption from Mac endpoints*

If you need to uninstall the software from a client computer, proceed as follows:

1. On the Mac client go to */Library*.
2. Open the folder *Sophos SafeGuard FS*.
3. Select and double-click the file *Sophos SafeGuard FS Uninstaller.pkg*
4. A wizard guides you through uninstallation.
5. Restart the system before continuing to work with your Mac.

As soon as the last Sophos SafeGuard product is removed, the client configuration is deleted as well.

 **Note** The uninstaller package is signed, and macOS will try to validate this signature. This procedure may take several minutes.

6. Synchronized Encryption

This section applies to both Windows and macOS. Where the information is relevant to only one of them, this will be mentioned explicitly.

Modules

- **Application-based file encryption**

SafeGuard Enterprise Synchronized Encryption can encrypt any file created with an application specified in a policy, regardless of its file location. For these applications encryption is automatic. They are also called In-Apps.

For example, if you specify Microsoft Word as an application for which file encryption is turned on, every file you create or save with Microsoft Word is automatically encrypted. Anyone whose key ring includes the key used to encrypt the file can access it.

By default SafeGuard Enterprise encrypts files with the Synchronized Encryption key, see [Synchronized Encryption key \(page 373\)](#).

Additionally you can:

- Define locations where a key other than the **Synchronized Encryption key** is used for encryption, for example the **Personal key**.
- Exclude folders from encryption.
- Use only Defined locations where the defined applications encrypt their data.

- **Outlook Add-in for Windows**

To make life easier for an end user, Synchronized Encryption provides an Outlook Add-in that can automatically detect an email being sent outside the organization with a file attachment. It will then ask which option (**Password protected, Unprotected**) the user wishes to choose. If required, the user can set a password in the dialog displayed. Alternatively, you can use a policy to define a default action that is performed automatically without any user intervention.

- **Integration with Sophos Central Endpoint Protection - remove keys on compromised machines**

In combination with Sophos Central Endpoint Protection, keys can be removed automatically if malicious activity is detected on endpoints.

This feature is only available if you use web-based Sophos Central Endpoint Protection together with SafeGuard Enterprise.

- **Share key ring between SafeGuard Enterprise and Sophos Mobile**

Encryption keys from the SafeGuard Enterprise key ring can be made available in the Sophos Secure Workspace (SSW) app managed by Sophos Mobile. Users of the app can then use the keys to decrypt and view documents, or to encrypt documents. These files can then be securely shared between all SafeGuard Enterprise and SSW users.

6.1 Best Practice: multi-key support for Synchronized Encryption

SafeGuard Enterprise allows you to configure additional encryption keys for specific locations when using Synchronized Encryption.

These instructions work through the following example:

- Your company has selected **Application-based (Synchronized Encryption)** for encrypting all files created by commonly used applications with the default **Synchronized Encryption key**.
- Encrypt files in the users' Documents folder with their **Personal Key**.
 - The users' Documents folder should contain the /unencrypted folder where users can store files in plain.
- To make sure that all files on endpoints are encrypted according to your company's policy, you should turn on initial encryption.

6.1.1 Creating a multi-key file encryption policy

1. In the Management Center, select the **(Default) File Encryption** policy and select **Application-based (Synchronized Encryption)** under **Encryption type**.
2. Under **Application list**, select **Template**.

The default application list is called **Template**. It contains the most commonly used applications.

3. Under **Encryption scope**, select **Everywhere**. This is the most secure option, generally used for Windows endpoints.

This creates a rule to encrypt files in all locations with the **Synchronized Encryption key**. The rule is added to the list of locations where application-based encryption is applied.

You can now add specific rules for locations that you want to be encrypted with different encryption keys. These locations can be local or on the network. You can use predefined values to specify them.

In our example, we want to encrypt the users' Documents folder.

4. To add a rule click in the **Path** edit field and select **<Documents>** from the drop-down menu.

 **Note** You cannot change the encryption scope.

The default key is the **Synchronized Encryption Key**, but you can choose any other encryption key. For example, the domain key, or the key of an organizational unit. You can also select the **Personal Key** which is unique to every user.

5. Click the **Personal Key** symbol in the **Key** edit field to select the users' personal keys to encrypt the Documents folder. You can hover over the key symbols to display their function.

To have an unencrypted folder you need to define an exception rule for that specific folder.

6. Click in the **Path** edit field, select **<Documents>** from the drop-down menu and enter **\unencrypted** after the **<Documents>** placeholder.
7. In the **Mode** column, select **Exclude** from the drop-down menu.
8. To turn on initial encryption on the endpoints, set the **Stored on local disks** option under **Initial encryption: Automatically encrypt existing files** to **Yes**.
9. Save the policy and deploy it.

 **Note** When you assign such a policy, with only specific rules for locations and different keys, to endpoints that have SafeGuard Enterprise 8.0 installed, these rules are applied correctly. All specified locations are encrypted with the selected keys. However, if a rule with **Encryption scope** set to **Everywhere** is part of the policy, only the **Synchronized Encryption Key** is used. Files in all specific locations are encrypted with the **Synchronized Encryption Key** as well.

6.2 Requirements

In order to use the Synchronized Encryption features, the following requirements must be met:

- SafeGuard Enterprise Server, Database and Management Center are set up properly.
- The **Synchronized Encryption** component must be installed on the Windows endpoints and **SafeGuard File Encryption** must be installed on macOS endpoints.
 - On Windows endpoints Synchronized Encryption replaces all other SafeGuard Enterprise File Encryption modules. It cannot be installed in addition to Data Exchange, File Encryption, or Cloud Storage. File encryption policies that are used by these location-based modules are incompatible with the new application-based Synchronized Encryption policies. If you migrate from the SafeGuard Enterprise File Encryption module to the Synchronized Encryption module and keep the location-based policies, the RSOP in the SafeGuard Management Center will still show both, but only the application-based policy is valid. The reason for this is that the calculation of the RSOP does not consider the modules installed on an endpoint.
 - The Synchronized Encryption module is not compatible with SafeGuard LAN Crypt.
- In order to activate the features you need to do the following:
 - Create an application list.
 - Create application-based file encryption policies (Synchronized Encryption).
 - Create policies for activating the Outlook Add-in (encrypts email attachments according to policy settings).
 - Create policies for activating the integration with Sophos Endpoint Protection (removing keys if malicious activity is detected on endpoints).
 - Configure the sharing of the SafeGuard Enterprise key ring with mobile devices managed by Sophos Mobile.
 - Deploy the policies.

On Macs only user policies apply. Machine policies are ignored.

6.2.1 Install endpoints

Run the client installer for your platform:

- On Windows endpoints, select the **Synchronized Encryption** component.
- On Macs install **SafeGuard File Encryption**.

6.2.2 Upgrade endpoints

- **Windows**

To upgrade your endpoints from SafeGuard Enterprise 8.0 or later and install the Synchronized Encryption module, run the client installer for your platform and follow the on-screen instructions. This upgrades the installed modules to version 8.30. In order to install the Synchronized Encryption module, start the installation again, select **Change** in the **Change, repair, or remove installation** dialog and select **Synchronized Encryption**. If installed, remove any location-based file encryption.

- **macOS**

Run the client installer and follow the on-screen instructions.

6.2.3 Migration from existing File Encryption module on Windows

Users can migrate from the SafeGuard Enterprise File Encryption module to the Synchronized Encryption module. Files that were encrypted before remain encrypted and accessible. Files that are modified and saved after the migration are re-encrypted with the Synchronized Encryption key. By specifying an initial encryption in a policy, files can be re-encrypted with the Synchronized Encryption key.

Prerequisites

You have to ensure that all required keys ("old keys" used for encrypting files with the legacy **File Encryption** module, and "new" Synchronized Encryption key) are available in the users' key rings.

- If necessary, you can assign keys to users in the Management Center.
- If needed, users have to import user-defined local keys to their key ring on endpoints, see chapter *Import keys from a file* in the SafeGuard Enterprise user help. Then the local keys will become available in the SafeGuard Management Center as well. They can be assigned to users as requested.

Run migration

Follow these steps:

1. Install the Synchronized Encryption module on endpoints. The module replaces the existing File Encryption module.
2. Make sure that all keys the users had in their key rings when they used File Encryption remain part of their key rings. This ensures that users can access files that are already encrypted using Synchronized Encryption.

3. In the Management Center, create new Synchronized Encryption policies.

- All applications that should be able to access encrypted files must be part of the **Application List** used in the Synchronized Encryption policies.
- Synchronized Encryption policies should cover the same **Encryption scope** as previous location-based File Encryption policies.
- Specify settings for initial encryption. Initial encryption will start immediately after the policy has been applied on the endpoint and encrypt or re-encrypt all files with the Synchronized Encryption key. This ensures that all files are encrypted according to policies.

 **Note** Initial encryption can also be started from the Windows Explorer context menu (**SafeGuard File Encryption > Encrypt according to policy**).

4. Deploy the policies.

Result

- Encrypted files covered by the Synchronized Encryption policies are re-encrypted with the Synchronized Encryption key.
- Files created or modified by applications on the Synchronized Encryption Application list will be encrypted with the Synchronized Encryption key.
- Encrypted files not covered by the Synchronized Encryption policies stay encrypted with the previous File Encryption key. Users who have the required key in their key ring can always decrypt files manually, even if files are no longer covered by encryption policies.

6.2.4 Migration from existing File Encryption module on macOS

The Sophos SafeGuard Enterprise macOS endpoints can handle both Synchronized Encryption policies of type **Application-based** and File Encryption policies of type **Location-based**. Depending on which policies they receive, endpoints act either as a Synchronized Encryption endpoint or a File Encryption endpoint.

If you upgrade from version 7, the endpoints keep on working in the File Encryption location-based mode as in the previous version.

To switch to the Synchronized Encryption application-based mode, do the following:

Run migration

1. In the Management Center, create new Synchronized Encryption policies.

- All applications that should be able to access encrypted files must be part of the **Application List** used in the Synchronized Encryption policies.
- Synchronized Encryption policies should cover the same **Encryption scope** as previous location-based File Encryption policies.
- Specify settings for initial encryption. Initial encryption will start immediately after the policy has been applied on the endpoint and encrypt or re-encrypt all files with the Synchronized Encryption key. This ensures that all files are encrypted according to policies.

 **Note** Users can also start initial encryption from the **Policies** tab in the preference pane (**Enforce all policies**) or execute the Terminal command for initial encryption.

2. Deploy the policies.
3. When users receive the policies they will be prompted to log off and log on again.

Result

- Encrypted files covered by the Synchronized Encryption policies are re-encrypted with the Synchronized Encryption key.
- Files created or modified by applications on the Synchronized Encryption Application list will be encrypted with the Synchronized Encryption key.
- Encrypted files not covered by the Synchronized Encryption policies stay encrypted with the File Encryption key. Users who have the required key in their key ring can always decrypt files manually, even if files are no longer covered by encryption policies.

6.2.5 Partial rollout of Synchronized Encryption

In case of a partial rollout of SafeGuard Enterprise Synchronized Encryption, you have to make sure that all of your users can access shared encrypted data.

If you want to activate encryption in your company step by step, you can start by deploying Synchronized Encryption policies with activated encryption for example to the endpoints of the *Marketing* department only. These endpoints will encrypt files according to the Synchronized Encryption policies. Users on endpoints of other departments will not be able to access these files since they do not have the Synchronized Encryption policies applied. To avoid this situation, you can deploy read-only policies that enable read access to encrypted files. These endpoints do not encrypt any data but can read encrypted files.

Prerequisite:

- SafeGuard Enterprise Server, Database, and Management Center are set up properly.
- The Synchronized Encryption module is installed on **all** endpoints and can connect to the Management Center (configuration package is installed).
- You have created an application list and a Synchronized Encryption policy for the endpoints which should encrypt data.

6.2.5.1 Partial rollout step-by-step

1. Create a Synchronized Encryption policy (application-based) in the SafeGuard Management Center.
2. Deploy the policy to users whose endpoints should encrypt data. In the example above, endpoints of the *Marketing* department.
3. Create read-only policies.

 **Note** You need to create separate policies for Windows and Mac endpoints.

4. Deploy the read-only policies to all of your other Windows and Mac endpoints. In the example above, all endpoints except those of the *Marketing* department.

6.2.5.2 Create read-only policy for Windows endpoints

1. In the Management Center, go to **Policies**.
2. Right-click **Policy Items**, then click **New** and then **File Encryption**.
3. Enter a name for the new policy and click **OK**.
4. On the **File encryption** tab, select **Application-based (Synchronized Encryption)** from the **Encryption type** drop-down list.
Application list and **Encryption scope** options are displayed.
5. Select the **Application list** you have previously created from the drop-down list.
6. From the **Encryption scope** drop-down list, select **Defined locations**.
7. When you leave the **File encryption** tab, the system prompts you to save your changes.
8. Click **Yes**.

9. Go to **Users and Computers** and assign and activate the new policy for Windows endpoints users who should be able to read encrypted data but not encrypt data.

 **Note** This policy must not be assigned to macOS endpoints. This can be easily achieved by activating the policy only for **.Authenticated Computers** since macOS endpoints only interpret user settings. To do so, drag the **.Authenticated Users** group from the policies activation area to the **Available Groups** list.

6.2.5.3 Create read-only policy for Mac endpoints

1. In the Management Center, go to **Policies**.
2. Right-click **Policy Items**, then click **New** and then **File Encryption**.
3. Enter a name for the new policy and click **OK**.
4. On the **File encryption** tab, select **Location-based** from the **Encryption type** drop-down list. The list to specify the paths for location-based encryption is displayed.
5. Specify the following paths and exclude them from encryption.
 - Network shares: Use the <Network Shares> placeholder to point to the root folders of all macOS network shares.
 - Removable media: Use the <Removables> placeholder to point to the root folders of all macOS removable media.
 - Cloud provider synchronization folder(s): Enter the folder(s) that will be synchronized with a cloud service. Only local paths are supported.
 - The following path is only needed if Microsoft Outlook for Mac 2011 is used:
`<User Profile>\Library\Caches\TemporaryItems\Outlook Temp\`
 - The following path is only needed if Microsoft Outlook for Mac 2016 is used:
`<%TMPDIR%>\com.microsoft.Outlook\Outlook Temp\`
 - The following paths are only needed if Apple Mail is used:
`<User Profile>\Library\Containers\com.apple.mail\Data\Library\Mail Downloads\`
`<%TMPDIR%>\com.apple.mail\com.apple.mail\`
6. Make sure all paths are excluded from encryption: **Exclude** is selected in the **Mode** column for each path.
7. When you leave the **File encryption** tab, the system prompts you to save your changes.

8. Click **Yes**.
9. Go to **Users and Computers** and assign the new policy to the Mac endpoints users who should be able to read encrypted data but not encrypt data.

6.3 *Encrypt data*

SafeGuard Enterprise Synchronized Encryption comes with a versatile file encryption module. Synchronized Encryption allows you to encrypt sensitive data based on the application it was created or modified with. This encryption is persistent, so your data is secure even if moved to another location, uploaded to a cloud storage provider, or sent via email. Depending on the policy settings, certain file types are usually encrypted automatically. However, in some cases it might be necessary to decrypt or encrypt single files manually. In Windows Explorer and macOS Finder, encrypted files are marked with a green lock symbol.

To prevent users from decrypting files manually, see [Prevent users from decrypting files manually \(page 406\)](#).

Encrypt data with different encryption keys

You can specify that different keys are used to encrypt files in specific locations, see [Create policies for application-based file encryption \(page 379\)](#).

Policies

- Synchronized Encryption policies are not merged. The policy closest to the target object (user or computer) in a hierarchy chain is always applied. The policy currently in force for a user or computer is displayed on the **RSOP** tab under **Users and Computers**.

Persistent encryption

Windows

- When you move an encrypted file from an encrypted folder to a plain folder, the file will still be encrypted. You can open the file and edit it. When you modify and save it, it will still be encrypted.

macOS

- **Moving encrypted files from Secured Folders**

As a security officer you define which folders on your Macs are classified as Secured Folders. If you are using Synchronized Encryption, all files in Secured Folders are encrypted automatically.

When you move an encrypted file from a Secured Folder to a non-Secured Folder, the file will still be encrypted. You can open it, but encrypted content will be displayed. You need to decrypt it manually first.

When you open an encrypted file in a Secured Folder and save it in a non-Secured Folder, the file will be decrypted automatically.

Backups

If you use backup software, like File History in Windows 8.x and Windows 10 or Time Machine in macOS, you may have backup, older versions of files of the type you want to encrypt. Synchronized Encryption cannot encrypt these files. You should remove or encrypt existing backups and deactivate automatic backups.

6.3.1 Synchronized Encryption key

By default, SafeGuard Enterprise Synchronized Encryption uses the Synchronized Encryption key to encrypt files: `Root_Synchronized_Encryption@SGN`. The key is assigned automatically and is available for all users.

The Synchronized Encryption Key is used as long as you do not specify locations where a different key has to be used. For these locations all available keys can be used, see [Keys and Certificates \(page 157\)](#).

6.3.2 Automatically encrypt files according to policy with asynchronous encryption

To make sure that files are always encrypted according to the policy that applies to a certain location, Synchronized Encryption provides asynchronous encryption.

Asynchronous encryption is applied when users do one of the following:

- Copy or move files, for example in Windows Explorer or macOS Finder.
- Create files with extensions that are specified in **Application Lists** with applications for which file encryption is not active.

Results:

- Files that are copied or moved from a plain folder to a folder where an encryption rule applies are encrypted.
- Files that are copied or moved from an encrypted folder to a plain folder are decrypted.

SafeGuard Enterprise automatically decrypts files only if users put one or more individual files to a location without encryption. If users move a folder to an exclude folder or if they rename a folder to the name of an exclude folder, files are not decrypted automatically to avoid accidental decryption. They can then decrypt files manually or use the **Encrypt according to policy** option from the folder's **SafeGuard File Encryption** context menu.

- Files that are copied or moved from an encrypted folder to a folder with a different encryption rule are encrypted according to the rule of the target folder.
- When files are created by applications for which file encryption is not active and the file's extension is specified in **Application Lists**, the file is encrypted and cannot be opened with the application that created the file. For example, if users create a .doc file using OpenOffice and OpenOffice is not specified in **Application Lists**.

 **Important** If copying or moving files is interrupted, for example due to a restart, if users cancel the dialog, log off from their computer or turn off the computer, the operation will not be resumed automatically. This can result in unintentionally unencrypted files.

Recommendation

To ensure that files are always encrypted according to company policies:

- Activate initial encryption for endpoints (local encryption) by means of a policy, see [Create policies for application-based file encryption \(page 379\)](#).
- For network shares, use the SGFileEncWizard.exe command line tool to check and restore the encryption state of files, see [Initial encryption on network shares \(page 378\)](#).

Log events for asynchronous encryption

For logged events, see [Auditing \(page 204\)](#).

6.3.3 Application Lists

For application-based file encryption, you need to create **Application Lists**. These lists contain applications where files are encrypted as soon as they are created or saved. Only applications on **Application Lists** can access encrypted data. All other applications will display unreadable encrypted content. SafeGuard Enterprise provides an application list template you can easily customize to fit your needs. It contains common applications for which you can apply application-based file encryption. You can selectively activate or deactivate applications within a group or the whole group.

 **Note** Creating Application-based (Synchronized Encryption) policies is not possible without creating **Application Lists** beforehand.

Application lists for Macs

For some macOS applications, you need to exclude certain locations from encryption to ensure proper functionality. For example for Microsoft Office 2011 <Documents>\Microsoft User Data needs to be excluded. In the provided template this path is already specified.

6.3.3.1 Create Application List

1. In the Management Center, go to **Policies**.
2. Go to the **Application Lists** entry of the **Policies** list view.
3. Right-click **Template** and click **Duplicate Application List**.
Template_1 is displayed.

Alternatively you can create a new application list.

4. Right-click *Template_1*, click **Properties** and enter a new name.
5. Click **OK**.
6. Click on the new application list.
On the right-hand pane, the content of the template is displayed.
7. If you want to create **Application Lists** for Macs, change to the **OS X** tab.
8. Go through the list and deactivate applications for which you do not want to apply encryption. Deactivating the **Active** option to the right of an **Application Group Name** will deactivate all applications in the group. Deactivating the Active option to the right of a particular application within the group will deactivate this application only.
9. Add further applications to existing groups.
 - a. Right-click the group to which you want to add an application, click **New** and then **Application**.
 - b. In the **Application Name** field, enter a name of your choice for the application.
 - c. Under **Process location**, specify the path including the executable, for example <Program Files>\Adobe\Reader 11.0\Reader\AcroRd32.exe. You can enter the path manually or you can use the placeholders from the drop-down list.

You can specify all versions of an application under one **Application name**. For example Acrobat Reader 11.0 and Acrobat Reader DC under **Application Name**: *Reader*

d. **File Extension**: The file extensions you specify here do not have any implication for **Application-based (Synchronized Encryption)** file encryption but for initial encryption of existing files and for asynchronous encryption.

- Initial encryption

Existing files covered by encryption policies are not encrypted automatically. To encrypt these files, initial encryption must be performed on endpoints. Files with the file extensions you specify here will be encrypted with the Synchronized Encryption key during initial encryption. You can enter file extensions with or without a leading dot (for example ".txt" or "txt"). Wildcards are not supported.

The location where initial encryption is to be applied has to be specified when creating a policy for **Application-based (Synchronized Encryption)** file encryption. It can be applied to local disks, removable devices, and automatically detected cloud storage providers.

- Asynchronous encryption

Make sure that files are always encrypted according to the policy that applies to a certain location. It is applied when users:

- copy or move files, for example in Windows Explorer or macOS Finder.
- create files with extensions that are specified in **Application Lists** with applications for which file encryption is not active.

For details, see [Automatically encrypt files according to policy with asynchronous encryption \(page 373\)](#).

If you deactivate an application group, the file extensions you specified for initial encryption within the group will be deactivated as well.

10. **Application Lists** for macOS (OS X tab): If necessary, add locations to be excluded from encryption to the **Excluded location** table to ensure proper functionality.

11. Add further application groups:

You can use application groups to collect for example all parts of a software suite under one node. This allows you to deactivate all parts by deactivating only the group.

- a. Right-click the **Template** tree view, click **New** and then **Application Group**.
- b. In the **Application Group Name** field, enter a name of your choice for the group.
- c. Add further applications to the group.

12. When you leave the template view, the system prompts you to save your changes. Click **Yes**.

The new application list is displayed under **Application Lists** in the **Policies** list view. You can create further application lists and use them in different policies for application-based file encryption.

 **Important** We recommend that you add all applications that are able to handle the same file types (for example .docx) to the application list. You should not add applications that share data over the internet (for example email clients, browsers).

6.3.4 Initial encryption

Initial encryption ensures that in addition to newly created files, existing data is properly encrypted as well. Files are encrypted according to company policies. This prevents company data from unintentionally remaining unencrypted.

Initial Encryption processes files based on:

- file extensions specified in **Applications lists**, see [Create Application List \(page 375\)](#).
- settings specified in Synchronized Encryption policies, see [Create policies for application-based file encryption \(page 379\)](#).

It can be triggered automatically by means of a policy setting or manually by users and is applied in all locations defined in policies.

 **Note** Initial encryption on network shares can only be executed with the command line tool SGFileEncWizard.exe, see [Initial encryption on network shares \(page 378\)](#).

If automatically triggered, initial encryption runs in the background. When done, a log event is generated.

If a large amount of data has to be processed, initial encryption may lead to performance issues on the endpoints.

Initial encryption starts whenever one of these events occurs:

- a user logs on
- a new or updated policy is applied on the endpoint
- removable media is attached
- a mount point is created (macOS)

Initial encryption does the following:

- plain files are encrypted according to the settings in the policy.
- files encrypted with a key other than the one set in the policy are re-encrypted with the key set in the policy. Provided that both keys are present in the user's key ring.
- files that are encrypted with a key that is not present in the user's key ring are left unchanged.
- encrypted files are never decrypted.

On Windows, users can manually start initial encryption by right-clicking the **This PC** node in Windows Explorer and selecting **SafeGuard File Encryption > Encrypt according to policy**. The SafeGuard File Encryption Wizard shows information on the amount of data to be processed, the progress and the results of the task.

On Macs, users open the **System Preferences**, click the Sophos SafeGuard icon, select the **Policies** tab, switch to the **Locally Translated Path** view and click **Enforce all policies**.

6.3.4.1 Initial encryption on network shares

On network shares initial encryption cannot be automatically triggered by means of a policy setting. As a security officer you can run initial encryption for network shares from a computer that has the SafeGuard Enterprise endpoint software installed and has access to these shares using the SGFileEncWizard.exe command line tool.

On a computer with SafeGuard Enterprise you can find the tool in <SYSTEM>:\Program Files (x86)\Sophos\SafeGuard Enterprise\Client\

Before you start initial encryption on network shares consider what follows:

- This process can cause issues for users on endpoints that do not have the Synchronized Encryption module installed or do not have a Synchronized Encryption policy applied. These users cannot decrypt files encrypted with Synchronized Encryption. Make sure that users on endpoints that should be able to access these files have the Synchronized Encryption module installed and a policy applied.
- If you want to re-encrypt files on network shares that are already encrypted, you need to have all keys which have been used to encrypt these files in your key ring when starting initial encryption. Files for which you do not have the key remain encrypted with the "old" key.

Requirements for performing initial encryption on network shares

- Initial encryption must be started on a computer with the SafeGuard Enterprise endpoint software installed.
- The endpoint must have access to all network shares to be encrypted.
- A Synchronized Encryption policy that covers all network shares to be encrypted has to be applied to the endpoint.
- All keys used to encrypt existing files on the network shares need to be part of your key ring.

Perform initial encryption with SGFileEncWizard

You can call SGFileEncWizard.exe with the following parameters:

SGFileEncWizard.exe [<startpath>] [%POLICY] [/V0 | /V1 | /V2 | /V3] [/X] [/L<logfile>]

- <startpath>: Process the specified paths and their subfolders. Several paths must be separated by blanks.

 **Note** For initial encryption on network shares, you must explicitly specify every network share to be encrypted. Only these paths will be processed. Specify the paths in UNC notation to avoid issues with different drive letters for mapped network shares. Only absolute paths are allowed.

- **%POLICY**: Apply Synchronized Encryption policy to the specified locations and re-encrypt files if necessary. The policy applied to the endpoint where SGFileEncWizard.exe is started is used.

 **Note** This parameter can be omitted for initial encryption on network shares.

- Parameter /V0: Do not report any messages.
- Parameter /V1: Log errors only.
- Parameter /V2: Log modified files.
- Parameter /V3: Log all processed files.
- Parameter /L<path+logfile name>: Write the output to the specified log file.
- Parameter /X: Hide the wizard's window.

Example:

```
SGFileEncWizard.exe \\my-filer-1\data1\users \\my-filer-1\data2 %POLICY /V3 /X /LC:\Logging
\myfile.xml
```

Initial encryption is performed for files in \\my-filer-1\data1\users and \\my-filer-1\data2. The wizard will not be displayed and information on all processed files is written to myfile.xml.

6.3.5 Create policies for application-based file encryption

1. In the **Policies** navigation area, create a new policy of the type **File Encryption**. The **File Encryption** tab is displayed.

2. Select **Application-based (Synchronized Encryption)** from the **Encryption type** drop-down list.

Application list and **Encryption scope** options are displayed.

For encryption type **No Encryption** see [Policies of type No encryption \(page 122\)](#).

3. From the drop-down list, select the **Application list** you created beforehand.

4. From the **Encryption scope** drop-down list, select one of the following:

- **Everywhere**: Encryption is applied on local drives, removables, cloud storage and network drives.

This creates a rule to encrypt files in all locations with the **Synchronized Encryption key**. You can define exemptions where no application-based file encryption is applied or where a different encryption key is used.

 **Note** For macOS, **Everywhere** means that all files in some predefined locations will be encrypted and can therefore only be used by the applications in your application list.

These locations are:

- folder <Desktop>
- folder <Documents>
- folder <Downloads>
- folder <Music>
- folder <Videos>
- all network shares
- all removable devices
- all supported cloud storage providers
- temporary folders where Microsoft Outlook and Apple Mail store mail attachments

 **Important** Applying Synchronized Encryption to network shares can cause issues for some users. If files on network shares have been encrypted by users who have the Synchronized Encryption key in their key ring, users without this key will not be able to decrypt them. To avoid this, you can first exclude network shares from encryption and remove the exemption after you are sure that all users have the Synchronized Encryption key. Users receive their key when a Synchronized Encryption policy is applied to their endpoint or you can manually assign the keys in the Management Center.

- **Defined locations**: Lets you specify paths where encryption is applied. Placeholders for path definitions are provided. You can select to include or to exclude a path in/from encryption.

5. Depending on your selection for the **Encryption scope**, you can define paths where application-based encryption is applied (**Defined Locations**) or exemptions to application-based encryption (**Everywhere**).

 **Note** You can define paths for Windows and macOS in the same policy. Placeholders for the different systems are available from the **Path** drop-down list. The **System** column indicates for which operating system the path is valid (**All systems**, **Windows**, **macOS**). By hovering your cursor over the **Cloud Storage** placeholders, you can display tooltips telling you for which operating system you can use the placeholder.

6. In the **Path** column, set the path to be handled by **Application-based (Synchronized Encryption)** file encryption:

- Click the drop-down button and select a folder name placeholder from the list of available placeholders.

By hovering your cursor over the list entries, you can display tooltips telling you how a placeholder is typically presented on an endpoint. You can only enter valid placeholders for each operating system. For a description of all available placeholders, see [Placeholders for paths in application-based File Encryption rules \(page 382\)](#).

 **Important** Encrypting the whole user profile with the placeholder <User Profile> may result in an unstable Windows desktop on the endpoint.

- Click the **Browse** button to browse the file system and select the required folder.
- Alternatively, just enter a path name.

7. Select the encryption **Mode**:

- For **Encryption scope > Defined Locations**, select **Encrypt** to let applications from the applications list encrypt their files under this path or **Exclude** if these applications should not encrypt their files under this path. For example, you can specify to encrypt D:\\Documents and exclude D:\\Documents\\Plain.
- For **Encryption scope > Everywhere**, you can **Exclude** paths from encryption or specify locations where a key other than the **Synchronized Encryption key** is used.

8. In the **Key** column, select the key to be used for the **Encrypt** mode:

- Click the **Synchronized Encryption key** symbol in the **Key** edit field to use the **Synchronized Encryption key** for this location. You can hover over the key symbols to display their function.
- Click the **Personal Key** symbol in the **Key** edit field to use the users' personal keys. On the endpoint, this placeholder is resolved to the active **Personal Key** of the logged on SafeGuard Enterprise user.
- Click the **Browse** button to open the **Find Keys** dialog. Click **Find now** to display a list of all available keys and select the required key.

 **Note** Machine keys are not shown in the list. They cannot be used by File Encryption as they are only available on a single computer and can therefore not be used to enable groups of users to access the same data.

9. Add further paths as required.
10. Specify settings for **Initial encryption**. Select where existing files are encrypted according to the specified paths (**Stored on local disks**, **Stored on removable devices**, **Stored with automatically detected cloud storage providers**). Initial encryption starts when the policy is applied on the endpoint, each time users log on, or when a removable device is connected.
11. Save your changes.

When you leave the **File encryption** tab, the system prompts you to save your changes.

12. Go to **Users and Computers** and assign the new policy to your user groups.

6.3.5.1 Placeholders for paths in application-based File Encryption rules

The following placeholders can be used when specifying paths in encryption rules in **File Encryption** policies. You can select these placeholders by clicking the drop-down button of the **Path** field.

Always use backslashes as path separators, even when creating File Encryption rules for macOS. This allows you to apply rules on both operating systems, Windows and macOS. On macOS endpoints, backslashes are automatically transformed to slashes in order to match the requirements of the macOS operating system. Any errors in placeholders are logged. Invalid File Encryption rules are logged and then discarded on the endpoint.

Example: The Windows path <User Profile>\Dropbox\personal is converted on Mac side into /Users/<Username>/Dropbox/personal.

Path placeholder	Operating System (All=Windows and macOS)	Results in the following value on the endpoint
<%environment_variable_name%>	All	<p>The value of environment variable. Example: <%USERNAME%>.</p> <p>If environment variables contain several locations (for example the PATH environment variable), the paths will not be separated into multiple rules. This causes an error and the encryption rule is invalid.</p>
<Desktop>	All	The virtual folder that represents the endpoint's desktop.
<Documents>	All	The virtual folder that represents the My Documents desktop item (equivalent to

Path placeholder	Operating System (All=Windows and macOS)	Results in the following value on the endpoint
		CSIDL_MYDOCUMENTS). Typical path: C:\Users\username\Documents.
<Downloads>	All	The folder where downloads are stored by default. A typical path for Windows is C:\Users\username\Downloads.
<Music>	All	The file system directory that serves as a data repository for music files. Typical path: C:\Users\username\Music.
<Network Shares>	All	
<Pictures>	All	<p>The file system directory that serves as a data repository for image files. Typical path: C:\Users\username\Pictures.</p> <p> Note On Macs, encrypting the whole <Pictures> folder is not supported. However, you can encrypt subfolders, for example <Pictures>\enc.</p>
<Public>	All	The file system directory that serves as a common repository for document files for all users. Typical path: C:\Users\Public.
<Removables>	All	Points to the root folders of all removable media.
<User Profile>	All	<p>The user's profile folder. Typical path: C:\Users\username.</p> <p> Note Encrypting the whole user profile is not supported. However, you can encrypt subfolders, for example <User Profile>\enc.</p>
<Videos>	All	The file system directory that serves as a common repository for video files for users. Typical path: C:\Users\username\Videos.
<Cookies>	Windows	The file system directory that serves as a common repository for internet cookies.
<Favorites>	Windows	The file system directory that serves as a common repository for the user's favorite items. Typical path: C:\Users\username\Favorites.

Path placeholder	Operating System (All=Windows and macOS)	Results in the following value on the endpoint
<Local Application Data>	Windows	The file system directory that serves as a data repository for local (non-roaming) applications. Typical path: C:\Users\username\AppData\Local.
<Program Data>	Windows	The file system directory that contains application data for all users. Typical path: C:\ProgramData.
<Program Files>	Windows	The Program Files folder. Typical path: \Program Files. For 64-bit systems, there will be two rules - one for 32-bit applications and one for 64-bit applications.
<Public Music>	Windows	The file system directory that serves as a common repository for music files for all users. Typical path: C:\Users\Public\Music.
<Public Pictures>	Windows	The file system directory that serves as a common repository for image files for all users. Typical path: C:\Users\Public\Pictures
<Public Videos>	Windows	The file system directory that serves as a common repository for video files for all users. Typical path: C:\Users\Public\Videos.
<Roaming>	Windows	The file system directory that serves as a common repository for application-specific data. Typical path: C:\Users\username\AppData\Roaming.
<System>	Windows	The Windows System folder. Typical path: C:\Windows\System32. For 64-bit systems, there will be two rules - one for 32-bit and one for 64-bit.
<Temporary Burn Folder>	Windows	The file system directory that is used as a staging area for files waiting to be written on a CD. Typical Path: C:\Users\username\AppData\Local\Microsoft\Windows\CD Burning.
<Temporary Internet Files>	Windows	The file system directory that serves as a common repository for temporary internet files.
<Windows>	Windows	The Windows directory or SYSROOT. This corresponds to the environment variables %windir% or %SYSTEMROOT%. Typical path: C:\Windows.

Path placeholder	Operating System (All=Windows and macOS)	Results in the following value on the endpoint
<Root>	macOS	The macOS root folder. We recommend that you do not specify policies for the root folder, even if it is technically possible.

Cloud Storage placeholders

Provider	Cloud Storage placeholder	Can be used in CSD (Cloud Storage Definition) setting	Resolves to
Box	<!Box!>	Synchronization application , Synchronization folders	For synchronization applications: The fully qualified path of the synchronization application used by the Box software.
Dropbox	<!Dropbox!>	Synchronization application , Synchronization folders	For synchronization folders: The fully qualified path of the synchronization folder used by the Box software.
Egnyte	Synchronization application Synchronization folders	For synchronization folders: The fully qualified path of the synchronization folder used by the Dropbox software.	For synchronization folders: The fully qualified path of the synchronization application used by the Egnyte software.
Windows only	<!EgnytePrivate!>	Synchronization application Synchronization folders	All private folders in the Egnyte cloud storage. For standard Egnyte users this is usually a single folder. For Egnyte administrators this placeholder typically resolves to multiple folders.

Provider	Cloud Storage placeholder <!EgnyteShared!> Synchronization folders	Can be used in CSD (Cloud Storage Definition) setting	Resolves to
			All shared folders in the Egnyte cloud storage.
			Changes to the Egnyte folder structure (including adding or removing private and shared folders) are detected automatically. Relevant policies are updated automatically.
			As Egnyte synchronization folders may reside on network locations you can enter network paths in the Synchronization folders setting. The SafeGuard Enterprise Cloud Storage module therefore applies to network file systems by default. If this is not required, you can deactivate this behavior by defining a General Settings policy and selecting Network under Ignored Devices .
Google Drive	<!GoogleDrive!> Synchronization application, Synchronization folders		For synchronization applications: The fully qualified path of the synchronization application used by the Google Drive software.
			For synchronization folders: The fully qualified path of the synchronization folder used by the Google Drive software.
OneDrive	<!OneDrive!> Synchronization application, Synchronization folders		For synchronization applications: The fully qualified path of the synchronization application used by the OneDrive software.
			For synchronization folders: The fully qualified path of the synchronization folder used by the OneDrive software.



Note SafeGuard Enterprise does not support Microsoft accounts. Under Windows 8.1, OneDrive can only be used if the Windows user is a domain user. Under Windows 8.1 SafeGuard Enterprise does not support OneDrive for local users.

Provider	Cloud Storage placeholder	Can be used in CSD (Cloud Storage Definition) setting	Resolves to
OneDrive for Business	<!OneDriveForBusiness>	Synchronization application, Synchronization folders	For synchronization applications: The fully qualified path of the synchronization application used by the OneDrive software. For synchronization folders: The fully qualified path of the synchronization folder used by the OneDrive software.

 **Note** OneDrive for Business only supports storing encrypted files in local folders and synchronizing them with the cloud. Storing encrypted files from Microsoft Office 2013 applications directly in the OneDrive for Business cloud or directly on the SharePoint Server is not supported. These files are stored unencrypted in the cloud.

SafeGuard Enterprise encrypted files in the OneDrive for Business cloud cannot be opened by Microsoft Office 365.

6.3.5.2 Configure application-based File Encryption in the cloud

SafeGuard Enterprise offers auto-detection for the following cloud storage providers:

- Box
- Dropbox (includes Dropbox Business)
- Google Drive
- OneDrive
- OneDrive for Business
- Egnyte (Windows only)

For these predefined placeholders are provided. Paths to the synchronization folders are set automatically.

The local synchronization folder can be changed by the users. For example, if they move it, SafeGuard Enterprise tracks the change and continues encrypting files in the new location.

 **Note Application-based (Synchronized Encryption) policies are not merged.** If such a policy already exists, you must add the encryption rules for cloud storage to the existing one.

1. In the **Policies** navigation area, create a new policy of the type **File Encryption** or select an existing one.
The **File Encryption** tab is displayed.
2. Select **Application-based (Synchronized Encryption)** from the **Encryption type** drop-down list.
Application list and **Encryption scope** options are displayed.
3. From the drop-down list, select the **Application list** you created beforehand.
4. From the **Encryption scope** drop-down list, select **Defined locations**.
5. Specify settings for **Initial encryption**. Select **Stored with automatically detected cloud storage providers** to encrypt existing files in synchronization folders. Initial encryption starts when the policy is applied on the endpoint, each time users log on, or when a removable device is connected.
6. In the **Path** column, click the drop-down button and select a **Cloud Storage** placeholder.
For a list of cloud storage placeholders, see [Placeholders for paths in application-based File Encryption rules \(page 382\)](#).
Select **<!All supported cloud storages!>** to enable encryption for each supported provider.
By hovering your cursor over the **Cloud Storage** placeholders, you can display tooltips telling you for which operating system you can use the placeholder.
7. In the **Scope** column, select one of the following:
 - **Only this folder** to apply the rule only to the folder indicated by the **Path** column.
 - **Include subfolders** to also apply the rule to all its subfolders.
8. In the **Mode** column, select **Encrypt**.
9. In the **Key** column, select the key to be used for the **Encrypt** mode. You can use keys created and applied in **Users and Computers**:
 - Click the **Browse** button to open the **Find Keys** dialog. Click **Find now** to display a list of all available keys and select the required key.
 - Click the **Personal Key** button with the key icon to insert the **Personal Key** placeholder in the **Key** column. On the endpoint, this placeholder will be resolved to the active Personal Key of the logged on SafeGuard Enterprise user. If the relevant users do not have active Personal Keys yet, they are created automatically. You can create Personal Keys for single

or multiple users in **Users and Computers**. For further information, see [Personal Keys for file-based encryption by File Encryption \(page 161\)](#).

10. Add further paths as required.
11. Save your changes.
12. Go to **Users and Computers** and assign the new policy to your user groups.

6.4 *Outlook Add-in for Synchronized Encryption*

 **Note** The Outlook Add-in is only available on Windows endpoints.

When sending email attachments to recipients who are using Synchronized Encryption, they are encrypted automatically. You do not need to worry about encryption and decryption. When sending emails to recipients outside your corporate network, you may want to encrypt your attachments to protect sensitive data. SafeGuard Enterprise includes an add-in for Microsoft Outlook that makes encrypting email attachments easy. Whenever you send an email with one or more files attached, the system prompts you to choose how to send the attachments. The available options may vary according to the encryption state of the files you attached to your email.

6.4.1 *Create policies for activating the SafeGuard Enterprise Outlook Add-in*

To activate the SafeGuard Enterprise Synchronized Encryption Outlook Add-in:

1. In the **Policies** navigation area, create a new policy of the type **General Settings** or select an existing one.
The **General Settings** tab is displayed.
2. Go to the **Email add-in settings** section.
3. In the **Enable email add-in** drop-down list, select **Yes**.
The add-in is now activated. Users will be prompted to decide how to handle attachments each time they send emails with attachments.

In addition, you can list domains and specify how attachments are handled when they are sent to these domains.

4. To do so, select how to handle attachments from the **Encryption method for white-listed domains** drop-down list:
 - **Encrypted:** All attachments in emails to the specified domain will be encrypted. Users will not be prompted.

Encrypted files keep their encryption, the encryption key isn't changed. Plain files are encrypted with the **Synchronized Encryption key**, but only if the file extension is defined in the list of In-Apps.

- **No encryption:** Attachments in emails to the specified domain will not be encrypted. Users will not be prompted.
- **Unchanged (Synchronized Encryption):** Encrypted files will be sent encrypted, plain files will be sent in plaintext. Users will not be prompted.
- **Always ask:** Users will be asked how to handle the attachments each time they send emails to the specified domain.

5. Enter one or more domains for which the encryption method should be applied. Enter several domains separated by commas. Wildcards and partially specified domains are not supported.
6. When you leave the **General Settings** tab, the system prompts you to save your changes.
7. Click **Yes**.
8. Go to **Users and Computers** and assign the new policy to your user groups.

6.5 *Integration with Sophos Central Endpoint Protection*

SafeGuard Enterprise Synchronized Encryption protects your data by removing keys when malicious activity is detected on an endpoint.

 **Important** This feature is only available if you use Sophos Central Endpoint Protection together with SafeGuard Enterprise.

It ensures that Sophos SafeGuard communicates with Sophos Central Endpoint Protection. SafeGuard Enterprise and Sophos Central Endpoint Protection will share the health status of your system. If your system becomes infected, SafeGuard Enterprise will protect your sensitive files. When no keys are available, encrypted data cannot be accessed.

When that happens, users will be informed that they have an unhealthy system but SafeGuard has protected their encrypted files and they cannot open them for a while. Endpoints will remain in this state until they return to a healthy state. Then SafeGuard Enterprise will provide the keys again. Users will be informed that their endpoint is secure and that they can access encrypted files again.

In situations where you regard the unhealthy state of endpoints as no longer justified and the endpoints remain in an unhealthy state you can give users access to their key ring by setting the **Remove keys on compromised machines** option to **No** and assign the modified policy to your user groups, see [Creating policies for removing keys on compromised machines \(page 391\)](#).

 **Important** You must be aware that disabling **Remove of keys on compromised machines** represents a potential security risk. You have to analyze and assess the situation carefully before doing that.

The computer's security status is displayed on **Sophos SafeGuard Client Status** dialog on the endpoint.

Prerequisites

- On Windows endpoints the **Synchronized Encryption** module has to be installed.
- On macOS endpoints the **SafeGuard File Encryption** module has to be installed.
- Sophos Central Endpoint Protection 1.0.3 or higher has to be installed on the endpoints.
- A policy of type **General Settings** with activated **Remove keys on compromised machines** option has to be assigned.

6.5.1 *Creating policies for removing keys on compromised machines*

To protect data when malicious activity is detected on endpoints:

1. In the **Policies** navigation area, create a new policy of the type **General Settings** or select an existing one.
The **General Settings** tab is displayed.
2. Go to the **File encryption** section.
3. From the **Remove keys on compromised machines** drop-down list, select **Yes**.
Now keys will be removed on the endpoints if malicious activity is detected. A message will be logged.

 **Note** Malicious behavior will always be logged to the SafeGuard Enterprise database, regardless of the settings for the **Remove keys on compromised machines** option.

4. When you leave the **General Settings** tab, the system prompts you to save your changes.
5. Click **Yes**.
6. Go to **Users and Computers** and assign the new policy to your user groups.

6.6 Share SafeGuard Enterprise key ring with mobile devices managed by Sophos Mobile

Encryption keys in the SafeGuard Enterprise key ring can be made available in the Sophos Secure Workspace app. Users of the app can then use the keys to decrypt and view documents, or to encrypt documents.

Key rings are synchronized between SafeGuard Enterprise and Sophos Mobile. No keys are stored on the Sophos Mobile server. Only the Sophos Secure Workspace app can decrypt the keys.

Requirements

These requirements must be met for key ring synchronization:

- You have set up the integration in the SafeGuard Enterprise Management Center.
- You use Sophos Mobile 6.1 or higher.
- You have configured external user management for the Sophos Mobile Self Service Portal as described in the Sophos Mobile documentation, using the same Active Directory user database that is configured in SafeGuard Enterprise.
- Sophos Secure Workspace is managed by Sophos Mobile.
- You have set up the integration in Sophos Mobile.
- In order to have the key ring available in Sophos Mobile, users have to log on at least once to SafeGuard Enterprise.

Features on mobile devices

Key ring synchronization includes these features:

- The keys from a user's SafeGuard Enterprise key ring are available in the Sophos Secure Workspace key ring (SSW key ring).
- Users can continue to use local keys that were available in their SSW key ring before you set up key ring synchronization.
- After you set up key ring synchronization, users cannot create new local keys.
- For security reasons, the keys from the SafeGuard Enterprise key ring are removed from a device when the Sophos container is locked.

For details, see [Display recovery keys in SSW](#) and [Manage keys in SSW](#).

6.6.1 Set up key ring synchronization

When you set up key ring synchronization, SafeGuard Enterprise users can use their key ring in the Sophos Secure Workspace app.

To set up a connection between Sophos Mobile and Sophos SafeGuard Enterprise:

 **Note** You are currently making user key rings available to mobile devices. If these mobiles comply with Sophos Mobile rules, they can access encrypted files. You should work with the Sophos Mobile administrator to set compliance rules that will prevent any unauthorized access.

1. In the Sophos Mobile console, download the certificate file of the Sophos Mobile server.
In the Sophos Mobile console, on the menu sidebar, under **SETTINGS**, click **Setup > System setup**, and then click the **SGN** tab.
2. In the SafeGuard Management Center, on the **Tools** menu, click **Configuration Package Tool**.
3. Select **Servers**.
4. Click **Add**.
The **Server Registration** dialog appears.
5. Click the **Browse** button and browse for the Sophos Mobile server certificate you downloaded.

 **Important** Do not change the name in the **Server name:** field.

6. Click **OK**.
The Sophos Mobile server is displayed on the **Server** tab of the **Configuration Package Tool**.
7. Optionally, select the **Recovery via mobile** check box.
This option will send the BitLocker and FileVault 2 recovery keys to the Sophos Mobile Server. Users of Sophos Secure Workspace managed by Sophos Mobile can then display these keys on their mobile for recovery purposes, see [Recovery via mobile devices \(page 431\)](#).

 **Note** Sophos Secure Workspace supports recovery via mobile from version 6.2.

Only compliant mobile devices will be able to receive recovery key information, so for maximum security, make sure you review these compliancy settings with your Sophos Mobile administrator.

8. Select **Managed client packages**.
9. Click **Add Configuration Package**.
10. Enter a name of your choice for the configuration package.

11. In the **Primary Server** column, select the Sophos Mobile server from the drop-down list. A **Secondary Server** is not necessary.
12. In the **Transport Encryption** column, select **SSL**.
13. Specify an output path for the configuration package (MSI).
14. Click **Create Configuration Package**.
If you have selected SSL encryption as the **Transport Encryption** mode, the server connection is validated. If the connection fails, a warning message is displayed.

The configuration package (MSI) has now been created in the specified directory. You now need to upload the configuration package to Sophos Mobile.

6.7 *Configure trusted applications and ignored devices*

In addition to the encryption rules defined in **File Encryption** policies of **Encryption type Application-based**, you can configure the following **File Encryption** settings in policies of the type **General Settings**:

- **Trusted Applications** (usually antivirus software)

You can define applications as trusted to grant them access to encrypted files. This is for example necessary to enable antivirus software to scan encrypted files.

Child processes will not be trusted.

- **Ignored Devices**

You can define devices as ignored to exclude them from the file encryption process. You can only exclude entire devices.

6.7.1 *Configure trusted applications for Application-based File Encryption*

1. In the **Policies** navigation area, create a new policy of the type **General Settings** or select an existing one.
2. Under **File Encryption**, click the drop-down button of the **Trusted Applications** field.

3. In the editor list box, enter the applications to be defined as trusted.
 - You can define multiple trusted applications in one policy. Each line in the editor list box defines one application.
 - Application names must end with .exe.
 - Application names must be specified as fully qualified paths including drive/directory information, for example c:\dir\example.exe. Entering the file name only (for example example.exe) is not sufficient. For better usability, the single line view of the application list only shows the file names separated by semicolons.
 - macOS: entering the application bundle only (for example /Applications/Scanner.app) is not sufficient. The application has to be specified as /Applications/Scanner.app/Contents/MacOS/Scanner.
 - Application names can contain the same placeholder names for Windows shell folders and environment variables as encryption rules in File Encryption policies. For a description of all available placeholders, see [Placeholders for paths in location-based File Encryption rules \(page 306\)](#).
4. Save your changes.

 **Note** The **Trusted Applications** policy settings are machine settings. The policy must therefore be assigned to machines, not to users. Otherwise the settings do not become active.

6.7.2 Configuring ignored devices

1. In the **Policies** navigation area, create a new policy of the type **General Settings** or select an existing one.
2. Under **File Encryption**, click the drop-down button of the **Ignored Devices** field.
3. In the editor list box:
 - a. Select **Network** if you don't want to encrypt any data on the network.
 - b. Enter the required device names to exclude specific devices from encryption. This may be useful when you need to exclude systems from third party suppliers.
You can display the names of the devices currently used in the system by using the Fltmc.exe control program (fltmc volumes, fltmc instances) from Microsoft, see <https://docs.microsoft.com/en-us/windows-hardware/drivers/ifs/development-and-testing-tools> .

You can exclude individual (network) disk drives from encryption by creating a File Encryption rule in a **File Encryption** policy and set the encryption **Mode** to **Ignore**. You can apply this setting only to Windows administered drives and not to macOS volumes.

6.8 Application-based File Encryption policies in the RSOP

Since Synchronized Encryption policies are not merged, always the content of the policy currently in force for a user or computer is displayed on the **File Encryption** sub-tab of the **RSOP** tab under **Users and Computers**.

7. Advanced management

7.1 *Best practices and recommendations*

7.1.1 *Rollout*

General suggestions

- Try to avoid a mixed rollout of the new Synchronized Encryption and the legacy File Encryption modules of SafeGuard Enterprise.
- A gradual rollout plan requires a test-run or verification of each step, especially for complex nested AD group memberships.
- User training is the key to a smooth rollout and operation.
- Clear communication about who is participating and the consequences is essential.
- IT and support teams have to be staffed adequately.

Prerequisites

- SafeGuard Enterprise Server and SafeGuard Management Center require .NET 4.5.
- All endpoints should have installed SafeGuard Enterprise. Otherwise sharing of encrypted files will be not transparent and the usual workflow is affected.
- If you want to read encrypted files on mobile devices (a new feature of SafeGuard Enterprise 8), you have to roll out the Sophos Secure Workspace app as well.

 **Note** To read encrypted files on mobile devices you have to use Sophos Secure Workspace managed by Sophos Mobile.

- Make sure that travelling users connect to the SafeGuard Enterprise backend regularly via VPN or "Direct Access" (Windows) to make sure that latest encryption policies are applied.

7.1.1.1 Partial rollout

In many situations the new **Synchronized Encryption** module cannot be rolled out and activated for all employees in one step within a short period of time. In these cases it is important to give users read-access to encrypted files even if they are on SafeGuard Enterprise endpoints without activated **Synchronized Encryption**. Therefore, a read-only policy is required.

For giving users read access, you need the following:

- The **Synchronized Encryption** key.

It is assigned to the root node in the Management Center by default and all employees of a company should get this key automatically.

- An **Application list** and a specific read-only policy.

For more information, see [Partial rollout of Synchronized Encryption \(page 369\)](#).

7.1.1.2 Synchronized Encryption and SafeGuard Enterprise File Encryption in the same environment

 **Note** If your environment requires you to use both, Synchronized Encryption and File Encryption, consider the following to achieve a smooth integration.

Synchronized Encryption supports one encryption key for an entire company. This makes administration and rollout easy. For some departments like HR or Finance, there might be the need to have a cryptographic separation from other departments to make their documents accessible only within their department.

For this scenario the SafeGuard Enterprise File Encryption modules (File Share, Cloud Storage, Data Exchange) have to be used. These modules allow using different keys for file encryption. You cannot install the Synchronized Encryption module and the SafeGuard Enterprise File Encryption modules on the same machine.

To make use of Synchronized Encryption and the SafeGuard Enterprise File Encryption modules some extra administration tasks are necessary:

1. The rollout of SafeGuard Enterprise must consider that different modules have to be installed for some departments.
2. Departments with special requirements have to get other policies than those assigned on **Synchronized Encryption** endpoints. To make this possible the imported AD structure should allow an easy assignment of these policies to users and machines concerned.
3. The rollout/installation of the SafeGuard Enterprise modules must be carried out according to the policies assigned: the right machines must get the right policies.

 **Note** The Outlook add-in is not available for SafeGuard Enterprise File Encryption modules. Therefore Synchronized Encryption and File Encryption endpoints cannot share encrypted attachments transparently.

Recommendations

- Users of SafeGuard Enterprise File Encryption modules need to get the **Synchronized Encryption** key. Users can then read files encrypted with the **Synchronized Encryption** key, transparently.
- Sharing encrypted files:

For users of SafeGuard Enterprise File Encryption modules, we recommend creating a policy which defines the **Synchronized Encryption** key to be used for a "transfer" share. All files created in or moved to this share will be encrypted with the **Synchronized Encryption** key. **Synchronized Encryption** users are able to read these files.

- Sharing plain files:

For users of SafeGuard Enterprise File Encryption modules, a policy that excludes a folder from encryption can be used (**Encryption type: Location-based, Mode: Exclude**).

- When users of SafeGuard Enterprise File Encryption modules want to share files with **Synchronized Encryption** users, they need to decrypt the files first. They can then decide to either send the unencrypted files or encrypt them with the Synchronized Encryption key.

7.1.1.3 Check validity of user certificates

Checking the validity of the user certificates is especially important for companies that used SafeGuard Enterprise BitLocker management only and want to add **Synchronized Encryption**.

You can check the certificates in the SafeGuard Management Center under **Keys and Certificates > Certificates > Assigned Certificates**.

Expired certificates or certificates that will expire soon are marked red in the **Expires** column. To renew a certificate that will expire soon activate the check-box in the **Renew** column. Users with already expired certificates have to get new ones. You must delete the expired certificates, then the affected users will get new ones automatically the next time they log on to SafeGuard Enterprise.

SafeGuard Enterprise provides the database script UserCertificateRenewal.vbs to automate these tasks. The script can be used in the SafeGuard Enterprise or Windows **Task Scheduler** to perform these checks regularly and renew certificates if necessary, see [Sophos knowledge base article 118878](#).

7.1.1.4 Check if all users are confirmed

In SafeGuard Enterprise new users have to be confirmed in the SafeGuard Management Center or authenticated against Active Directory. Most users will be Active Directory users, who will be confirmed automatically. However, some users have to be confirmed manually, for example local users. Unconfirmed users will not become **SGN Users** and therefore will not get encryption keys for Synchronized Encryption. This is true for Windows and macOS endpoints.

We recommend setting the first policy to be rolled out to **read-only**. After all endpoints/users have received their keys activate the encryption policies. This way you can make sure that all users are confirmed before they receive their encryption policies. Issues with unconfirmed users will be avoided.

7.1.1.5 Policies for macOS endpoints

For file encryption we recommend using the policy type **Application-based (Synchronized Encryption)** with **Encryption scope** set to **Defined locations** and start with only a few locations where files are encrypted automatically. This way you can reduce the impact on users and their usual workflows.

To be able to distinguish between Windows and macOS endpoints in terms of policy management, use a separate AD or SafeGuard Enterprise group for macOS users and machines. Activate the macOS policy only for macOS users and machines.

7.1.1.6 Suggestions for a macOS Synchronized Encryption policy

In-Apps

Applications that will encrypt their data, to be added to the **Application list**:

- Email

 **Note** For macOS, there is no Outlook Add-in available. However, you can add Outlook and Apple Mail to the application list to make sure that no encrypted data is sent unintentionally to users who cannot access it. Note that the mail apps you included in the list will send all attachments unencrypted and will save encrypted attachments in encrypted form and plain files in plain text.

- /Applications/Microsoft Outlook.app/Contents/MacOS/Microsoft Outlook
- /Applications/Microsoft Office 2011/Microsoft Outlook.app/Contents/MacOS/Microsoft Outlook
- Applications/Mail.app/Contents/MacOS/Mail
- To enable macOS preview and the preview functionality in Finder and Apple Mail, the following processes need to be added:
 - /Applications/Preview.app/Contents/MacOS/Preview

- /System/Library/Frameworks/QuickLook.framework/Versions/A/Resources/quicklookd.app/Contents/XPCServices/QuickLookSatellite.xpc/Contents/MacOS/QuickLookSatellite
- /System/Library/Frameworks/Quartz.framework/Versions/A/Frameworks/QuickLookUI.framework/Versions/A/Resources/QuickLookUIHelper.app/Contents/MacOS/QuickLookUIHelper
- /System/Library/Frameworks/QuickLook.framework/Versions/A/Resources/quicklookd.app/Contents/MacOS/quicklookd

Paths for Encryption scope: Defined locations

- Encrypt:
 - <Documents>\Encrypted
- If you want users to be able to double-click encrypted documents in their mail clients to open them, you need to add these applications (for example Mail) to the In-App list, and their temporary folders to the list of defined locations.

The locations you need to define for the mail clients on Mac are:

- <%TMPDIR%>\com.apple.mail\com.apple.mail
- <User Profile>\Library\Containers\com.apple.mail\Data\Library\Mail Downloads

Add the following locations for Outlook for macOS:

- <User Profile>\Library\Caches\TemporaryItems\Outlook Temp\
- <%TMPDIR%>com.microsoft.Outlook\Outlook Temp\

7.1.2 Backend

Read-only user for Active Directory synchronization

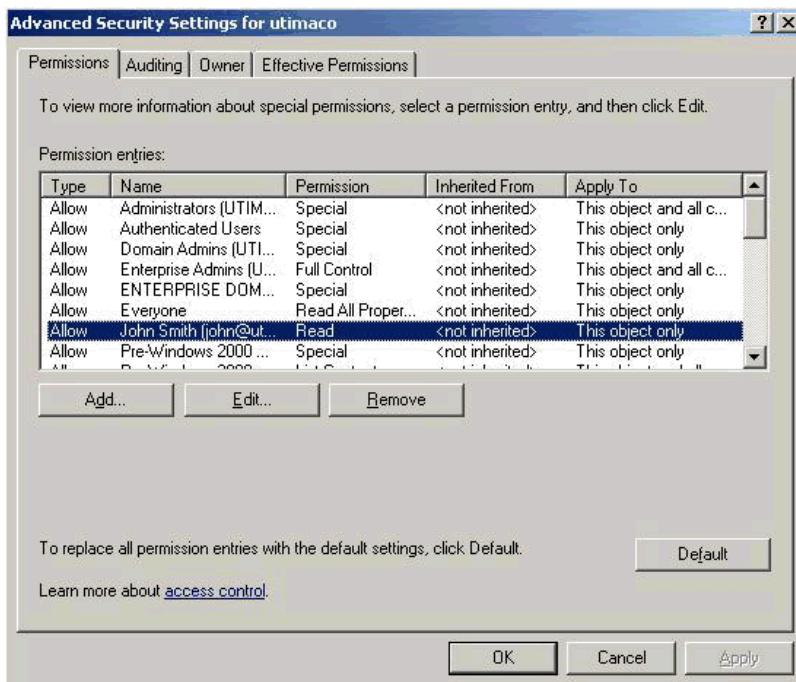
 **Note** To increase security of the connection, we recommend that you use SSL encryption for the Active Directory synchronization.

The account used for the import and synchronization of the Active Directory should be a **read-only** user. The user needs read access to the domain and all child objects.

To assign the rights:

1. Open the **Active Directory Users and Computers** management window and go to **Advanced Features**.
2. Right-click the domain and then click **Properties**.
3. Add a user (or a group) and select the **Allow** checkbox to assign **Read** permission.
4. Click **Advanced**, select the user (or group) and click **Edit**.
5. In the **Permission Entry for <domain>** dialog, select **This object and all child objects** from the **Apply onto:** drop-down list.

The result should look like this:



Users displayed with "#" in the Management Center

Users that registered in SafeGuard Enterprise when no domain controller was available are marked with "#" in the Management Center.

7.1.3 Policies

7.1.3.1 Folders to be excluded from encryption

Make sure to exclude the following paths from encryption when you use **Synchronized Encryption**:

Windows

- <Local Application Data\Temp>

Reason: Some applications create many small temporary files. If not excluded, all temporary files will be encrypted according to the policy. Exclude the folder to avoid performance issues.

- <Local Application Data>\Microsoft and subdirs

Reason: Some applications call other applications (for example embedded video in Microsoft PowerPoint). If the calling application is an application that encrypts files, the temporary file (for example video) will be encrypted. If the called application (for example browser) is an application that does not encrypt files (it is not on the Application list) it cannot run the encrypted file.

- <Program Files>

Reason: Access to this folder needs administrator rights. SafeGuard Initial Encryption cannot encrypt these files because of the missing access rights. Excluding this folder prevents the SafeGuard database from being cluttered with event messages caused by failed file encryption.

All systems

- <!cloud storage providers!>

In general we recommend to encrypt cloud storage, but you can exclude certain cloud storage providers which are used to share data with external parties. This prevents files in known local cloud storage synchronization folders from being encrypted. Thus, problems when exchanging files with external parties via Cloud synchronization can be avoided. It is not necessary to exclude these folders if you do not use Cloud folders for exchanging files with external parties.

- <Music>

Reason: Usually, you do not need to encrypt these files. If you do not want this folder to be excluded from encryption, applications to open these files need to be part of the **Application List**.

- <User Profile>|AppData|Roaming\AppleComputer

Reason: This is the local synchronization folder for Apple iCloud on Windows endpoints. It should be excluded for the same reasons that apply to <!cloud storage providers!>.

7.1.3.2 Recommendations for policy settings

Define an "Unencrypted" folder

This folder can be used for sharing plain files, for example with Linux endpoints in the company or in a partial rollout scenario, see [Partial rollout of Synchronized Encryption \(page 369\)](#).

- **Windows**

To exclude the "Unencrypted" folder from encryption on all endpoints, you have to add the Unencrypted folder (relative path) as exemption in a policy with **Encryption scope** set to **Everywhere**. If you do so, all files in folders with this name, regardless of where the folder is located, will not be encrypted.

- **macOS**

Relative paths are not supported on macOS. We recommend that you define <Documents> \Unencrypted as exemption in a policy with **Encryption scope** set to **Everywhere**.

Outlook Add-in

We recommend setting the **Encryption method for white-listed domains** option in a policy of type **General Settings** to **Unchanged**.

Remove keys on compromised machines

SafeGuard Enterprise **Synchronized Encryption** endpoints are informed by Sophos Central Endpoint Protection about compromised machine status.

We recommend that the **Remove keys on compromised machines** option is set to **No**. You should check the feedback about affected endpoints under **Reports** in the SafeGuard Management Center

for Red health state detections. Next you should check and clean up the endpoints, if necessary. Finally you should set the **Remove keys on compromised machines** option to **Yes**.

7.1.3.3 Guest user

On endpoints that have only SafeGuard Enterprise BitLocker management installed, companies may still have the **Allow registration of new SGN users for** option set to **Owner**.

For endpoints without SafeGuard Enterprise POA that have BitLocker management or file encryption modules installed, the **Allow registration of new SGN users for** option must be set to **Everybody**. If you do not set this option to **Everybody**, further users will only have **SGN guest** status. They will not get certificates and cannot encrypt files after a file encryption module like **Synchronized Encryption** has been installed.

7.1.3.4 Policies for macOS and RSOP

On macOS only policies assigned to users are evaluated. If you assign them to machines, macOS endpoints will not get any policies.

However, the RSOP in the Management Center displays the policy currently assigned to the Mac although it will not become active.

7.1.3.5 File tracking

Note that the file tracking functionality of SafeGuard Enterprise is subject to national laws. You should check what you are legally permitted to track.

7.1.3.6 Reminder to change password

If you use the SafeGuard Enterprise Credential Provider the Windows pop-up dialog that informs users when their password will expire is no longer displayed.

To remind users to change their passwords, you need to create and assign a SafeGuard Enterprise policy of type **Password** with the required settings, see [Syntax rules for passwords \(page 251\)](#).

7.1.4 Endpoints - all platforms

7.1.4.1 Encrypt/Decrypt files manually

Synchronized Encryption allows you to encrypt or decrypt individual files manually. Right-click a file and select **SafeGuard File Encryption**. The following functions are available:

- **Show encryption state:** Indicates whether or not the file is encrypted as well as the key used.
- **Encrypt according to policy:** Encrypts your file with the Synchronized Encryption key provided that the file type is included in the application list and the location of the file has not been excluded from encryption.
- **Decrypt selected file** (only for encrypted files): 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. You can turn off this option in a **General Settings** policy, see [General settings \(page 231\)](#).
- **Encrypt selected file** (only for unencrypted files): Allows you to manually encrypt your file with the Synchronized Encryption key.
- **Create password protected file:** Here you can define a password to encrypt your file manually. This is useful if you want to securely share your file with someone who does not have the Synchronized Encryption key of your organization. Your file is encrypted and saved as an HTML file. Your recipients can open the file with their web browser as soon as you communicate the password to them.
 - You can turn off this option in a **General Settings** policy, see [General settings \(page 231\)](#).
 - This option is only available for files that are either plaintext or encrypted with a key available in your keyring. If files are encrypted, they are first decrypted automatically before they are password protected.
 - Password protection uses base64 encoding, therefore, files are bigger than the original file. The maximum supported file size is 50 MB.
 - You can only password-protect single files, not folders or directories. However, you can select more than one file to show their encryption state and to encrypt/decrypt them.

If you right-click folders or drives, the following functions are available:

- **Show encryption state:** Displays a list of the included files with icons indicating the encryption state as well as the key used.
- **Encrypt according to policy:** The system automatically detects all unencrypted files and encrypts them with the default Synchronized Encryption key provided that the file type is included in the application list and the location of the file has not been excluded from encryption. Depending on your policy, files encrypted with other keys may be re-encrypted with the Synchronized Encryption key, too.

7.1.4.2 Prevent users from decrypting files manually

You can use a policy setting to prevent users from decrypting files manually.

Preventing users from decrypting files may be necessary for compliance or because it is required by your organization's policy. To do so:

1. In the **Policies** navigation area, create a new **General Settings** policy or select an existing one. The **General Settings** tab is displayed.

2. Go to the **File Encryption** section.
3. Set the **User is allowed to decrypt files** option to **No**.
4. When you leave the **General Settings** tab, the system prompts you to save your changes.
5. Click **Yes**.
6. Go to **Users and Computers** and assign the new policy to your user groups.

 **Important** On Mac OS this setting is only applied if the policy is assigned to the machine. Assigning it to a user has no effect.

The **Decrypt selected file** option is removed from the right-click menu of files. Encryption and decryption are controlled only through policy settings.

Note

Users can still decrypt files when you have excluded folders from encryption in your encryption policy. If users move or copy files to such folders, the files are decrypted.

7.1.4.3 Endpoint does not return to healthy state - cleanup fails

Next-Generation Data Protection ensures that Sophos SafeGuard communicates with Sophos Endpoint Protection, if available. This is an extension of the Synchronized Security message. SafeGuard and Endpoint will share the health status of a system using the heartbeat between them.

If a system becomes highly infected with malware it will be locked down to protect sensitive files.

In the event this occurs, users will be advised by Sophos Endpoint Protection that they now have an unhealthy system with a Red health state. Additionally, they will be advised by Sophos SafeGuard that they will no longer be able to access any encrypted files. They will remain in this state, unable to access encrypted files, until the health of the system is returned to a healthy (Green) state. When the system returns to a healthy state, Sophos SafeGuard will synchronize with the backend and allow users to once again access encrypted files.

If users receive these notifications and their system does not return to a healthy state in a short period of time, they should contact IT for help.

If an endpoint is unable to return to a healthy state, it means Sophos Anti-Virus cleanup has failed (cleanup is set to automatic in Sophos Central). If cleanup fails, then additional actions are required by IT to clean up the malware, see <https://www.sophos.com/en-us/support/knowledgebase/112129.aspx>.

7.1.5 Windows endpoints

7.1.5.1 Decrypting files with SGFileEncWizard.exe

With the command line tool SGFileEncWizard.exe users can trigger an automated decryption of files.

On a computer with SafeGuard Enterprise you can find the tool in <SYSTEM>:\Program Files (x86)\Sophos\SafeGuard Enterprise\Client\

Requirements

- SafeGuard File Encryption 8.20 or later or SafeGuard Synchronized Encryption 8.20 or later, must be installed.
- The folders where files will be decrypted must be covered by exclude rules in an existing file encryption policy. Any encryption or ignore rules set for these folders must be removed. It's also possible to create a new policy and assign it to the corresponding users, see [Configuring encryption rules in location-based File Encryption policies \(page 303\)](#) and [Create policies for application-based file encryption \(page 379\)](#).
- SGFileEncWizard.exe must be started by the users on their computers, so that all keys are available. No administrative rights are required.
- Running SGFileEncWizard.exe by "double-clicking" it or without defining a path, does not start decryption.
- No placeholders can be used in the "command-line" call.
- There is no report or summary of the decryption.

Perform decryption with SGFileEncWizard.exe

Users have to run SGFileEncWizard.exe with the path to be decrypted and the parameter /X. This will decrypt all files in excluded locations.

SGFileEncWizard.exe" <PATH> /X

Examples:

```
C:\Program Files (x86)\Sophos\SafeGuard Enterprise\Client\SGFileEncWizard.exe  
D:\ /X
```

```
C:\Program Files (x86)\Sophos\SafeGuard Enterprise\Client\SGFileEncWizard.exe  
\\hostname\share\ /X
```

```
C:\Program Files (x86)\Sophos\SafeGuard Enterprise\Client\SGFileEncWizard.exe
\\hostname\share\ C:\ D:\ /X
```

7.1.5.2 Emails sent via auto-forward rule

When you define an auto-forward or redirect rule **on client side**, emails sent automatically are not logged.

7.1.6 macOS endpoints

Position of icons on the desktop

When using SafeGuard Enterprise for Mac, the positions of the icons on your desktop may not be saved correctly. When you change the position of an icon, it will move back to its original position after every restart or logon.

To save your icons' positions, do the following:

1. Start the Terminal application on your Mac.
2. Enter the following command:

```
defaults write com.sophos.encryption MountDesktopAsNetworkVolume 1
```

3. Log off and log back on to your Mac.

 **Caution** When you run this command, the functionality of the Trash changes. Deleting files will delete them permanently instead of moving them to the Trash. To remove the setting, enter the following command in the Terminal application:

```
defaults remove com.sophos.encryption MountDesktopAsNetworkVolume.
```

Changing the computer name of a Mac

If you change the computer name of a Mac, you must then run sgfsadmin --update-machine-info and synchronize the Mac with the SafeGuard Enterprise Server.

7.2 *Security recommendations*

By following the simple steps described here, you can mitigate risks and keep your company's data secure and protected at all times.

Encryption best practices

- **Ensure that all drives have a drive letter assigned.**

Only drives that have a drive letter assigned are considered for disk encryption/decryption. Consequently, drives without a drive letter assigned may be abused to leak confidential data in plaintext.

To mitigate this threat: Do not allow users to change drive letter assignments. Set their user rights accordingly. Regular Windows users do not have this right by default.

- **Apply Fast Initial Encryption cautiously.**

SafeGuard Enterprise offers Fast Initial Encryption to reduce the time for initial encryption of volumes by only accessing the space that is actually in use. This mode leads to a less secure state if a volume has been in use before it was encrypted with SafeGuard Enterprise. Due to their architecture, Solid State Disks (SSD) are affected even more than regular hard disks. This mode is disabled by default. For more information, see [Sophos knowledge base article 113334](#).

- **Only use algorithm AES-256 for data encryption.**
- **Use SSL/TLS (SSL version 3 or above) for protection of the client/server communication.**

For further information, see [Securing transport connections with SSL \(page 45\)](#).

- **Prevent uninstallation.**

To provide extra protection for endpoints you can prevent local uninstallation of SafeGuard Enterprise in a **Specific machine settings** policy. Set **Uninstallation allowed** to **No** and deploy the policy on the endpoints. Uninstallation attempts are cancelled and the unauthorized attempts are logged.

If you use a demo version, make sure that you set **Uninstallation allowed** to **Yes** before the demo version expires.

Apply Sophos Tamper Protection to endpoints using Sophos Endpoint Security and Control.

Avoid sleep mode

On SafeGuard Enterprise protected endpoints, encryption keys might be accessible to attackers in certain sleep modes where the endpoint's operating system is not shut down properly and background

processes are not terminated. Protection is enhanced when the operating system is always shut down or hibernated properly.

Train users accordingly or consider centrally disabling sleep mode on endpoints that are unattended or not in use:

- Avoid sleep (stand-by/suspend) mode as well as hybrid sleep mode. Hybrid sleep mode combines hibernation and sleep. Setting an additional password prompt after resume does not provide full protection.
- Avoid locking desktops and switching off monitors or closing laptop lids as modes of protection when not followed by a proper shut down or hibernation. Setting an additional password prompt after resume does not provide sufficient protection.
- Always shut down or hibernate endpoints. SafeGuard Power-on Authentication is always activated the next time the computer is used, thus providing full protection.

 **Note** It is important that the hibernation file resides on an encrypted volume. Typically it resides on C:\.

You can configure the appropriate power management settings centrally using Group Policy Objects or locally through the **Power Options** dialog on the endpoint's **Control Panel**. Set the **Sleep** button action to **Hibernate** or **Shut down**.

Implement a strong password policy

Implement a strong password policy and force password changes at regular intervals, particularly for endpoint logon.

Passwords should not be shared with anyone nor written down.

Train users to choose strong passwords. A strong password follows these rules:

- It is long enough to be secure: A minimum of 10 characters is recommended.
- It contains a mixture of letters (upper and lower case), numbers and special characters/symbols.
- It does not contain a commonly used word or name.
- It is hard to guess but easy to remember and type accurately.

Do not disable SafeGuard Power-on Authentication

SafeGuard Power-on Authentication provides additional logon protection on the endpoint. With SafeGuard Full Disk Encryption, it is installed and enabled by default. For full protection, do not disable it.

Protect against code injection

Code injection, for example DLL pre-loading attacks might be possible when an attacker is able to place malicious code, for example executables, in directories that may be searched for legitimate code by the SafeGuard Enterprise encryption software. To mitigate this threat:

- Install middleware loaded by the encryption software, for example token middleware in directories that are inaccessible to external attackers. These are typically all sub-folders of the **Windows** and **Program Files** directories.
- The PATH environment variable should not contain components that point to folders accessible to external attackers (see above).
- Regular users should not have administrative rights.

7.3 *Replicating the SafeGuard Enterprise Database*

Replicating the SafeGuard Enterprise Database is no longer supported as of SafeGuard Enterprise 8.1.

7.4 *Web Helpdesk*

To smooth the workflow in an enterprise environment and to reduce helpdesk cost, SafeGuard Enterprise provides a web-based recovery solution for managed clients. Web Helpdesk offers help to users who fail to log on or to access SafeGuard Enterprise encrypted data by providing a user-friendly Challenge/Response mechanism.

Benefits of Challenge/Response

The challenge/response mechanism is a secure and efficient emergency system.

- No confidential data is exchanged in unencrypted form throughout the entire process since the Web Helpdesk is only accessible via HTTPS. HTTP connections are redirected to HTTPS automatically.
- There is no point in third parties eavesdropping on this procedure because the data cannot be used at a later stage or on any other devices.
- The endpoint that is to be accessed does not need an online network connection.

- The user can start working again quickly. No encrypted data is lost just because the password has been forgotten.

Challenge/Response workflow

During the Challenge/Response procedure, a challenge code (ASCII character string) is generated on the endpoint and the user communicates this code to a helpdesk officer. Based on the challenge code, the helpdesk officer then generates a response code which authorizes the user to perform a specific action on the endpoint.

Typical emergency situations requiring helpdesk assistance

- A user has forgotten the password for logging on and the endpoint has been locked.
- A user has forgotten or lost their token/smartcard.
- The Power-on Authentication local cache is partly damaged.
- A user is not available at the moment due to illness or vacation but the data on the endpoint must be accessible to a colleague.
- A user wants to access a volume encrypted with a key that is not available on that endpoint.

SafeGuard Enterprise Web Helpdesk offers different recovery workflows for these typical emergency scenarios, enabling the users to access their endpoints again.

7.4.1 Scope of Web Helpdesk

Web Helpdesk provides the SafeGuard Enterprise Challenge/Response mechanism through a web-based interface that is accessible via HTTPS. It allows the helpdesk to delegate tasks flexibly within the enterprise. This is achieved without the need to give helpdesk employees access to confidential configuration settings or to the SafeGuard Management Center.

The website must be hosted on an Internet Information Services (IIS) based SafeGuard Enterprise Server.

 **Note** We recommend that you only make Web Helpdesk available on the intranet of your enterprise. For security reasons, Web Helpdesk should not be put on the internet.

Web Helpdesk provides:

- [Recovery for managed endpoints \(managed SafeGuard Enterprise clients\) \(page 419\)](#)

Logon recovery for endpoints that are centrally managed by the SafeGuard Management Center. Managed endpoints are listed in the Users and Computers area in the SafeGuard Management Center.

- [Recovery using Virtual Clients \(page 422\)](#)

Easy recovery for encrypted volumes can be achieved even when Challenge/Response is not usually supported, for example when the POA is corrupted.

- [Recovery for unmanaged endpoints \(Sophos SafeGuard clients standalone\) \(page 426\)](#)

Logon recovery for endpoints that are locally managed.

7.4.2 Allow Web Helpdesk logon for users without SafeGuard Enterprise

It is possible to use Web Helpdesk without having a SafeGuard Enterprise client installed.

Access rights can be managed by adding or removing Windows users or groups.

 **Note** This feature makes use of Windows Authentication. If Windows Authentication is enabled, traditional login via a promoted Active Directory user is no longer possible.

7.4.2.1 Prerequisites

For logon without a SafeGuard Enterprise client, the following prerequisites must be met:

- HTTPS must be enabled on your IIS server.
- A Windows user group containing users who are allowed to access Web Helpdesk must be set up and configured, see [Configure a Windows user group for SafeGuard Web Helpdesk \(page 414\)](#).
- Windows Authentication at the Web Helpdesk must be enabled in the SafeGuard Management Center (**Tools > Configuration Package Tool > Servers > Win. Auth. WHD**).
- The account running application pool must have access to the database.

7.4.2.2 Configure a Windows user group for SafeGuard Web Helpdesk

To set up and configure a Windows user group for SafeGuard Web Helpdesk access, proceed as follows:

1. Open the **Active Directory Users and Computers** tool and select your domain.

2. Right-click your domain and select **New > Organizational Unit**.
3. Enter a name for the new organizational unit and confirm with **OK**.
4. Expand your domain and right-click **Managed Service Accounts**.
5. Select **New > Group**, enter a group name (for example, `WHD Users`), and click **OK**.
6. Right-click the organizational unit you created in step 3 and select **New > User**.
7. Enter a name and a logon name for the user and click **Next**.
8. Define a password and specify, whether the user must change the password at next logon.
A new user has been created in the new organizational unit.
9. Add the user to the group you created in step 5.
10. Open the Microsoft SQL Server Management Studio and select your server in the **Object Explorer** on the left.
11. Select **Security**, right-click **Logins** and click **New Login...**
12. In the **Login name** field, click the **Search** button.
13. In the following dialog, click the **Object Types...** button and select all checkboxes.
14. In the text field on the bottom, type the group name you defined in step 5 and click **Check Names**.
15. If the correct group name is displayed, confirm with **OK**.
The **Login name** field in the **Login - New** dialog is populated with the domain and group name.
16. In the **Select a page** field in the top left corner, select **User Mappings**.
17. In the **Users mapped to this login** field, select **SafeGuard**.
18. Define **db_datareader** and **db_datawriter** as database role memberships and confirm with **OK**.

7.4.2.3 Enable Windows Authentication for SafeGuard Web Helpdesk

1. Open the Internet Information Services (IIS) Manager.
2. On the **Connections** pane on the left, select **Sites > Default Web Site > SGNWHD**.

3. In the workspace under **IIS**, double-click **Authentication** and select **Windows Authentication**.
4. On the **Actions** bar on the right, click **Enable**. Make sure that the status is set to **Enabled**.
5. Go back to the overview and under **ASP.NET**, double-click **.NET Authorization Rules** to add three .NET authorization rules.

 **Note** In Windows Server 2008 R2, there is no icon in the IIS for **.Net Authorization Rules**. There is an **Authorization Rules** link. To be able to edit those rules, the **URL Authorization** role should be installed by using **IIS > Security > URL Authorization**.

6. On the **Actions** bar, click **Add Deny Rule...**.
7. Select **All anonymous users** and confirm with **OK**.
8. On the **Actions** bar, click **Add Allow Rule...**.
9. Select **Specified roles or user groups** and enter your user group name including domain name into the field (for example: <Domain Name>\WHD Users) to allow user group access for your specific user group.
For more information, see [Configure a Windows user group for SafeGuard Web Helpdesk \(page 414\)](#).
10. Confirm with **OK**.
11. On the **Actions** bar, click **Add Deny Rule...**.
12. Select **All users** and confirm with **OK**.
13. Make sure the order of the entries is as follows:
 - Deny - Anonymous Users - Local
 - Allow - <Domain name>\<Group name> - Local
 - Deny - All Users - Local
 - Allow - All Users - Inherited

In order to test the functionality, log on as described in [Log on with Windows Authentication enabled \(page 417\)](#). To check the connection to the server, select **SGNWHD** on the **Connections** pane and click **Browse *:443 (https)** on the **Actions** pane on the left.

If you need to disable Windows Authentication to allow traditional login via a promoted Active Directory user, remove the rule **Deny - All anonymous users**.

 **Note** You can also enable Windows Authentication by modifying the web.config file under C:\Program Files (x86)\Sophos\SafeGuard Enterprise\SGNWHD. For example:

```

<configuration>
  <system.web>
    <authentication mode="Windows" />
    <authorization>
      <allow roles="HelpDesk" />
      <deny users="*" />
    </authorization>
  </system.web>
</configuration>

```

7.4.2.4 Log on with Windows Authentication enabled

Proceed as follows:

1. Open the browser and enter the URL.
2. To call the application in your browser, enter the URL: `https://<Host ID or IP address>/SGNWHD`
3. Select **Recovery** and proceed as described in the appropriate section:
 - [Recovery for managed endpoints \(managed SafeGuard Enterprise clients\) \(page 419\)](#)
 - [Recovery using Virtual Clients \(page 422\)](#)
 - [Recovery for unmanaged endpoints \(Sophos SafeGuard clients standalone\) \(page 426\)](#)

7.4.3 Authentication

Security officers need to authenticate at Web Helpdesk and against the SafeGuard Enterprise Server in order to be able to use the web-based recovery wizard. Security officers log on to Web Helpdesk with their security officer user name and their password.

Two authentication scenarios are possible:

- Users who have been promoted to security officers in the SafeGuard Management Center log on as described in [Log on to Web Helpdesk without Windows Authentication enabled \(page 418\)](#).
- Users who have been assigned to a specific Web Helpdesk user group with "Windows Authentication enabled" will log on as described in [Log on with Windows Authentication enabled \(page 417\)](#).

7.4.3.1 Preparations in the SafeGuard Management Center

To be able to authenticate at Web Helpdesk without Windows Authentication enabled, the following steps need to be taken in the SafeGuard Management Center.

1. Import Web Helpdesk users from an Active Directory into the SafeGuard Enterprise Database.
2. Assign user certificates to these users. The certificates (.p12 file) must be available in the database.
3. Right-click the relevant user and select **Make this user a security officer** to promote future Web Helpdesk users to security officers.
4. Assign security officers the **Helpdesk Officer** role to allow them to authenticate at Web Helpdesk.

The promoted security officers can then log on to Web Helpdesk with their defined security officer name, which is a combination of their Windows user name and the name of the domain assigned to them. The required password is the Windows password protecting their certificates.

 **Note** If the certificate is created when users are promoted, they have to use the certificate password to log on to the SafeGuard Management Center. They have to enter the certificate password although they are prompted for the Windows password.

5. Grant them access rights for the objects they need to work with, for example domains or organizational units.

If your domain is not displayed in the Web Helpdesk, do the following:

6. Open the SafeGuard Management Center and click **Users and Computers**.
7. In the tree structure on the left, select your domain.
8. Go to the **Access** tab and make sure the user you want to grant access is listed.

 **Note** As Web Helpdesk security officers must authenticate against the SafeGuard Enterprise Server, authentication with token is not supported in Web Helpdesk.

7.4.3.2 Log on to Web Helpdesk without Windows Authentication enabled

1. Start your browser.
2. To call the application in your browser, enter the following URL: `https://<Host ID or IP address>/SGNWHD`
3. On the **Welcome** page, enter your security officer name as defined in SafeGuard Management Center in the following way: `<user name>@<DOMAIN>` for example `WHDOfficer@MYDOMAIN`.
4. Enter your Windows password.

 **Note** If the certificate is created when users are promoted, they have to use the certificate password to log on to the SafeGuard Management Center. They have to enter the certificate password although they are prompted for the Windows password.

5. Click **Log on**.

You are logged on to Web Helpdesk.

7.4.4 Recovery for managed endpoints (managed SafeGuard Enterprise clients)

SafeGuard Enterprise offers recovery for managed SafeGuard Enterprise protected endpoints in various disaster recovery scenarios, such as password recovery or accessing data by starting from external media.

The program dynamically determines if SafeGuard Enterprise full disk encryption or BitLocker Drive Encryption is in use and adjusts the recovery workflow accordingly.

7.4.4.1 Recovery actions for managed endpoints

The recovery workflow depends on which type of SafeGuard Enterprise client recovery is requested for.

 **Note** For BitLocker encrypted endpoints the only recovery action is to recover the key used to encrypt a specific volume. No password recovery is provided.

Recover the password at POA level

One of the most common scenarios is that users have forgotten their password. By default SafeGuard Enterprise is installed with an activated Power-on Authentication (POA). The POA password for accessing the endpoint is the same as the Windows password.

If the user has forgotten the password at POA level, the helpdesk officer can generate a response for **Boot SGN client with user logon**, but without displaying the user password. However, in this case, after entering the response code the endpoint will start the operating system, so the user has to change the password at Windows level, subject to the conditions set on the domain. The user can then log on to Windows as well as to the Power-on Authentication with the new password.

Best practice for recovering the password at POA level

We recommend that you use the following methods when the user has forgotten their password to avoid resetting the password centrally:

- **Use Local Self Help.** Local Self Help allows the user to have their current password displayed and to continue using it. This avoids the need to reset the password or to involve the helpdesk.
- **When using Challenge/Response on SafeGuard Enterprise clients (managed):** We recommend that you avoid resetting the password centrally in the Active Directory before the Challenge/Response procedure. Avoiding this will ensure that the password remains synchronized between Windows and SafeGuard Enterprise. Make sure that the Windows helpdesk is informed of this fact.

 **Note** Password reset via Challenge/Response is only available for Windows endpoints.

As a SafeGuard Enterprise helpdesk officer, generate a response to **Boot SGN Client with user logon** with the option **Show user password**. This avoids resetting the password in Active Directory for the user. The user may continue working with the existing password and change it locally afterwards, if desired.

 **Note** This option is not available for endpoints protected with BitLocker or FileVault2.

Access data by starting the endpoint from external media

Challenge/Response can also be used to allow starting an endpoint from external media such as WinPE. To do so, the user has to select **Continue Booting from: Floppy Disk/External Medium** in the POA logon dialog and initiate the challenge. When receiving the response, the user can enter the credentials in the POA as usual and continue booting from the external media device.

 **Note** This option is not available for endpoints protected with BitLocker or FileVault2.

The following requirements must be met to access an encrypted volume:

- The device to be used must contain the SafeGuard Enterprise filter driver. For more information, see [Sophos knowledge base article 108805](#).
- The user must start the endpoint from an external media device. The right to do so can be granted to them by defining a policy in the SafeGuard Management Center and then assigning it to the endpoint (**Policies > Authentication > Access > User may only boot from internal hard disk > No**).
- The endpoint must allow starting from external media.

- Only volumes encrypted with the defined machine key can be accessed. This key encryption type can be defined in a device encryption policy in the SafeGuard Management Center and assigned to the endpoint.

 **Note** When you use external media such as WinPE to access an encrypted drive, this only gives partial access to the volume.

Restore the SafeGuard Enterprise policy cache

If the SafeGuard Enterprise policy cache is damaged, the user will automatically be prompted to initiate a Challenge/Response procedure when logging on at the Power-on Authentication.

7.4.4.2 Create a response for managed computers

To create a response for managed computers (SafeGuard Enterprise clients), the computer name and the domain name are required.

- On the **Recovery type** page, select **SafeGuard Enterprise Client**.
- Select the relevant domain from the list.
- Enter the required computer name. There are several ways to do this:
 - Select a name by clicking [...] and then **Search** in the pop-up window. A list of computers is displayed. Select the required computer and click **OK**. The computer name is then displayed in the **Recovery type** window under **Domain**.
 - Enter the short name of the computer. When clicking **Next**, the database is searched for this name and if found, the distinguished computer name is displayed.
 - Enter the computer name directly in the distinguished name format, for example:
`CN=Desktop1,OU=Development,OU=Headquarter,DC=Utimaco,DC=com`
- Click **Next**.

The program then dynamically determines if SafeGuard Enterprise full disk encryption or BitLocker Drive Encryption is used on the computer and adjusts the recovery workflow accordingly.

- In the case of a SafeGuard Enterprise protected computer the next step requires the selection of the user information.
- In the case of a BitLocker encrypted computer a volume that cannot be accessed any more may be recovered. The next step requires the selection of the volume that is to be decrypted.

Create a response for computers protected by SafeGuard Enterprise full disk encryption

1. In **Domain** select the required domain of the user. In the case of a local user select **Local user on <computer name>**.
2. Search for the required user name. Do one of the following:
 - Click **Search by Display Name**. Select the required name from the list and click **OK**.
 - Click **Search by Logon Name**. Select the required name from the list and click **OK**.
 - Enter the name of the user directly. Make sure that the name is spelt correctly.
3. Click **Next**. A window is displayed where you can enter the challenge code.
4. Enter the challenge code the user has passed on to you and click **Next**. The challenge code is verified. If the code has been entered incorrectly, **Invalid** is displayed below the block containing the error.
5. If the challenge code has been entered correctly, the recovery action requested by the SafeGuard Enterprise client as well as the available recovery actions on the endpoint are displayed. Available actions for response depend on the actions requested on the endpoint when calling the challenge. For example, if **Crypto token requested** is required, the available actions for response are **Boot SGN Client with user logon** and **Boot SGN Client without user logon**.
6. Select the action the user needs to perform.
7. If **Boot SGN client with user logon** as mentioned above has been selected as the response action, you can additionally select **Show user password** to have the password displayed on the target endpoint.
8. Click **Next**. A response code is generated.
9. Read or send the response code to the user. A spelling aid is provided. You can also copy the response code to the clipboard.

The user can then enter the response code on the endpoint and perform the authorized action.

Create a response for computers protected by BitLocker Drive Encryption

1. Select the volume to be accessed and click **Next**. Web Helpdesk then displays the corresponding 48-digit recovery key.
2. Provide this key to the user.

The user can then enter the key to recover access to the BitLocker encrypted volume on their endpoint.

7.4.5 Recovery using Virtual Clients

Using Virtual Clients for recovery in SafeGuard Enterprise, access to encrypted volumes can be recovered even in complex recovery situations.

This recovery type can be applied in the following typical situations:

- The Power-on Authentication is corrupted.

- A volume is not encrypted with the computer's defined machine key but with a different key. The necessary key is not available in the user's environment. It must therefore be identified in the database and transferred to the endpoint in a secure way.

 **Note** Virtual Client recovery should only be used to resolve complex recovery situations: If both of the above mentioned issues apply, a Virtual Client recovery is appropriate. If however only the key needed is missing, the best way to recover the volume would simply be to assign the missing key to the respective user's key ring.

In these situations SafeGuard Enterprise offers the following solution:

To enable a Challenge/Response procedure in this situation, specific files called Virtual Clients can be created in the SafeGuard Management Center and distributed to the user before the Challenge/Response session is started. Challenge/Response can then be initiated on the endpoint with the help of the Virtual Client files and the key recovery tool RecoverKeys.exe and a SafeGuard Enterprise modified WinPE CD. The helpdesk officer then selects the required keys and generates a response code. Access to the encrypted volumes is enabled when the user enters the response code, as the required keys are transferred within the response.

 **Note** In Web Helpdesk, Recovery using Virtual Clients is not supported for unmanaged endpoints (Sophos SafeGuard Clients standalone). Use the SafeGuard Management Center instead.

7.4.5.1 Recovery workflow using Virtual Clients

For further information, see the *SafeGuard Enterprise Administrator help*.

1. The helpdesk officer creates the Virtual Client in the **Keys and Certificates** area of the SafeGuard Management Center and exports them to a file. This file, called recoverytoken.tok, must be distributed to the users and must be available to them before the Challenge/Response session.
2. The user needs to start a SafeGuard Enterprise recovery CD or any other CD with a SafeGuard Enterprise modified WinPE on their computer without any POA logon and initiate a Challenge/Response session with the SafeGuard Enterprise key recovery tool.
In the SafeGuard Enterprise Database the Virtual Client file is used and stated in the challenge instead of the user or computer name which is not available in this case.
3. The key recovery tool then tells the user which volumes are encrypted and which keys are used for each of these volumes. The user presents this information to the helpdesk officer.
4. The helpdesk officer identifies the Virtual Client in the database and selects the required key for accessing the encrypted volumes: either a single key or several keys exported to a key file. The helpdesk officer then generates the response code.

5. The user enters the response code. Within the response code the required keys are transported. By entering the response code and restarting the computer the user can then access the encrypted volumes again.

7.4.5.2 Recovery actions using Virtual Clients

To access volumes that are encrypted with keys which are not available to the user, the correct encryption key(s) must be transferred from the database to the user's environment.

Challenge/Response therefore covers two actions using Virtual Clients:

- Transferring a single key
- Transferring several keys in an encrypted key file

Transfer a single key

Challenge/Response can be initiated to recover a single key for accessing an encrypted volume. The helpdesk officer must select the necessary key in the database and generate a response code. The key is encrypted and transferred to the endpoint by entering the response code. If the response code is correct, the transferred key will be imported to the local key store. After that, all volumes that are encrypted with this key can be accessed.

Transfer several keys in an encrypted key file

Challenge/Response can be initiated to recover multiple keys for accessing encrypted volumes. The keys are stored in one file which is password encrypted. A prerequisite for this is that the helpdesk officer exports one or more required keys to be stored in a file. This file is encrypted with a random password, which is stored in the database. The password is unique for each key file created.

The encrypted key file needs to be transferred to the user environment and must be available to the user. To decrypt this key file the user then has to initiate a Challenge/Response session with the key recovery tool RecoverKeys.exe. During this session the password is transferred to the target endpoint. The helpdesk officer generates a response and selects the respective password to decrypt the key file. The password is transferred to the target endpoint within the response code. The key file can then be decrypted with the password.

The keys in the key file are imported into the key storage on the endpoint and all volumes encrypted with the available keys can be accessed again.

 **Note** With Web Helpdesk, a key file and the corresponding password are deleted in the database after having once been successfully used in a Challenge/Response session. Therefore you must create a new key file and a password after each successful Challenge/Response session.

7.4.5.3 Response using Virtual Clients

Prerequisites

- The Virtual Client must have been created in the SafeGuard Management Center in **Keys and Certificates**.
- The helpdesk officer must be able to locate the Virtual Client in the database. Virtual Clients are identified uniquely by their name.
- The Virtual Client file **recoverytoken.tok** must be available to the user. This file must be stored in the same folder as the key recovery tool. We recommend that you store this file on a memory stick.
- When recovery for several keys is requested, the helpdesk officer must previously have created a key file containing the necessary recovery keys in the SafeGuard Management Center in **Keys and Certificates**. The key file must be available to the user before a recovery to take effect. The password encrypting this key file must be available in the database.
- The user must have started the key recovery tool and must have initiated the Challenge/Response session.
- A response can only be initiated for assigned keys. If a key is inactive, this means that if the key is not assigned to at least one user, a Virtual Client Response is not possible. In such a case the inactive key can be reassigned to any other user and a response for this key can be generated again.

Create a response using Virtual Clients

1. As a helpdesk officer, select **Virtual Client** on the **Recovery type** page.
2. Enter the name of the Virtual Client the user has given to you. There are different ways to do so:
 - Enter the unique name directly.
 - Select a name by clicking [...] and then **Search** in the pop-up window. A list of Virtual Clients is displayed. Select the required one and click **OK**. The name of the Virtual Client is then displayed in the **Recovery type** window in **Virtual Client**.
3. Click **Next**. The page where you can select the recovery action is displayed.
4. Select the recovery action to be taken by the user and then click **Next**.
 - If you need to transfer a single recovery key only, select **Key requested**. Select the required key from the list. Click [...]. You can either display the keys by key ID or by symbolic name. Click **Search**, select the key and click **OK**.
 - If the user needs a key file containing several keys for recovery, select **Password for key file requested** to transfer the password for the encrypted key file to the user. Select the required key file. Click [...] and then **Search**. Select the key file and click **OK**.

Password for key file requested can only be selected when a key file has previously been created in the SafeGuard Management Center in **Keys and Certificates** and the password

encrypting the key file has been stored in the database. With Web Helpdesk, key files and the corresponding passwords are deleted in the database after having once been successfully used in a Challenge/Response session. Therefore you have to create a new key file and password after every successful Challenge/Response session.

5. Click **Next**. The page to enter the challenge code is displayed.
6. Enter the challenge code the user has passed on to you and click **Next**. The challenge code is verified. If the code has been entered incorrectly, **Invalid** is displayed below the block containing the error.
7. If the challenge code has been entered correctly, the response code is generated. Read the response code to the user. A spelling aid is provided. You can also copy the response code to the clipboard.
 - If a single key is requested the generated key is transferred within the response code.
 - If a password for the encrypted key file is requested it is transferred within the response code. The key file then is deleted.
8. The user must enter the response code on the endpoint.
9. The user needs to restart the computer and log on again to access the respective volumes.

The volumes can be accessed again.

7.4.6 Recovery for unmanaged endpoints (Sophos SafeGuard clients standalone)

SafeGuard Enterprise also provides Challenge/Response for unmanaged endpoints (Sophos SafeGuard clients standalone). They have no connection to the SafeGuard Enterprise Server and are managed locally. As they are not registered in the SafeGuard Enterprise Database, their identification needed for a Challenge/Response is not available. Therefore, Challenge/Response for unmanaged endpoints is based on the key recovery file (XML) created during endpoint configuration, see [Create configuration package for unmanaged endpoints \(page 96\)](#). The key recovery file is generated for each unmanaged endpoint and contains the defined machine key which is encrypted with the company certificate. During Challenge/Response, the key recovery file must be made available to the helpdesk officer, for example, on a USB flash drive or on a network share. When the helpdesk officer is able to access the recovery file, a response can be generated. If the file is not accessible, recovery is not possible.

7.4.6.1 Recovery actions for unmanaged endpoints

Challenge/Response for unmanaged endpoints (Sophos SafeGuard client standalone) must be initiated in the following situations:

- The user has entered the password incorrectly too many times.
- The user has forgotten the password.
- A corrupted local cache needs to be repaired.

For unmanaged endpoints no user key is available in the database. Therefore, the only recovery action possible in a Challenge/Response session is **Boot Sophos SafeGuard client without user logon**.

The Challenge/Response procedure enables the user to log on at the Power-on Authentication. The user is enabled to log on to Windows, even if the Windows password needs to be reset.

The user has entered the password incorrectly too many times

As in this case resetting the password is unnecessary, the Challenge/Response procedure enables the user to log on at the Power-on Authentication. The user can then enter the correct password at Windows level and use the endpoint again.

The user has forgotten the password

 **Note** We recommend that you usually use Local Self Help to recover a forgotten password. Local Self Help allows you to have the current password displayed and to continue using it. This avoids the need to reset the password or to involve the helpdesk.

When you recover a forgotten password using Challenge/Response a password reset is required.

1. The Challenge/Response procedure enables the computer to start through Power-on Authentication.
2. At the Windows logon prompt, the user does not know the correct password and needs to change password at Windows level. This requires further recovery actions outside the scope of SafeGuard Enterprise, by standard Windows means. We recommend that you use the following methods to reset the password at Windows level.
 - Using a service or administrator account available on the computer with the required Windows rights.
 - Using a Windows password reset disk.As a helpdesk officer you may inform the user which procedure should be used and either provide the additional Windows credentials or the required disk.
3. The user enters the new password at the Windows logon prompt that the helpdesk has provided. The user then changes this password immediately to a value only known to the user.
4. SafeGuard Enterprise detects that the newly chosen password does not match the current SafeGuard Enterprise password used in the POA. The user is prompted to enter the old

SafeGuard Enterprise password and, since the user has forgotten this password, needs to click **Cancel**.

5. In SafeGuard Enterprise, a new certificate is needed in order to set a new password without providing the old one.
6. A new user certificate is created based on the newly chosen Windows password. This enables the user to log on to the computer again and to log on at the Power-on Authentication with the new password.

Keys for SafeGuard Data Exchange

When the user has forgotten the Windows password and it has been reset, the user will not be able to use the keys already created for SafeGuard Data Exchange without the corresponding passphrase. To be able to continue using the existing user keys for SafeGuard Data Exchange the user has to remember the SafeGuard Data Exchange passphrases to reactivate these keys.

7.4.6.2 Create a response for unmanaged computers

To generate a response for an unmanaged computer, the name of the recovery file (.xml file) is required.

1. In Web Helpdesk, on the **Tools** menu, click **Recovery**.
2. In **Recovery type**, select **Standalone Client**.
3. Locate the required key recovery file (.xml) by clicking **Browse**.
4. Enter the challenge code the user has passed on to you.
5. Select the action to be taken by the user and click **Next**.
6. A response code is generated. Read the response code to the user. A spelling aid is provided. You can also copy the response code to the clipboard.

The user can enter the response code, perform the requested action and resume working.

7.4.7 Logging Web Helpdesk events

Events for Web Helpdesk can be logged in the Windows Event Viewer or in the SafeGuard Enterprise Database. Events of all helpdesk activities can be logged, for example who logged on to Web Helpdesk, which user requested a challenge or which recovery actions have been requested.

Event logging for Web Helpdesk is activated in the SafeGuard Management Center by a policy that needs to be published into a configuration package and deployed on the Web Helpdesk service.

Events that are logged in the central SafeGuard Enterprise Database can be viewed in the SafeGuard Management Center Event Viewer.

7.4.7.1 Enable logging for Web Helpdesk events

Logging for Web Helpdesk is configured in the SafeGuard Management Center.

You need to have the required rights to create policies and view events.

1. In the SafeGuard Management Center, in the **Policies** navigation area, create a policy of the type **Logging**. Select the events to be logged. Save your changes.
2. Create a new **Policy Group**. Add the policy of the type **Logging** to this group. Save your changes.
3. On the **Tools** menu, click **Configuration Package Tool**. Select **Managed client packages** and click **Add Configuration Package**. Select the previously created policy group to be included in the configuration package. Select a storage location and click **Create Configuration Package**.
4. In the SafeGuard Management Center, assign the policy group to the domain that contains the Web Helpdesk server. Then activate it. For more information, see [Assign policies \(page 92\)](#).
5. On the Web Helpdesk server, install the previously created configuration package. Restart the service.

Logging Web Helpdesk events has been activated.

6. Log on to Web Helpdesk and carry out a Challenge/Response procedure.
7. In the SafeGuard Management Center, click the **Reports** tab. In the **Event Viewer** action area on the right, click the magnifier icon to view the events logged for Web Helpdesk.

7.5 Recovery

SafeGuard Enterprise offers recovery procedures for the following scenarios:

- [Recovery via mobile devices \(page 431\)](#)
- [Recovery for BitLocker encrypted endpoints \(page 299\)](#)
- [Recovery key for Mac endpoints \(page 344\)](#)
- Recovery for SafeGuard Full Disk Encryption with POA. See the [SafeGuard Enterprise 8 administrator help](#).

7.5.1 Challenge/Response workflow

The Challenge/Response procedure is based on two components:

- The endpoint on which the Challenge code is generated.
- The SafeGuard Management Center where, as a helpdesk officer with sufficient rights, you create a response code that authorizes the user to perform the requested action on their computer.

 **Note** For a Challenge/Response process, you need **Full access** rights for the computers/users involved.

1. On the endpoint, the user requests the challenge code. Depending on the recovery type, this is either requested in the SafeGuard Power-on Authentication or in the KeyRecovery Tool.

A challenge code in form of an ASCII character string is generated and displayed.

2. The user contacts the helpdesk and provides them with the necessary identification and the challenge code.
3. The helpdesk launches the Recovery Wizard in the SafeGuard Management Center.
4. The helpdesk selects the appropriate recovery type, confirms the identification information and the challenge code and selects the required recovery action.

A response code in form of an ASCII character string is generated and displayed.

5. The helpdesk provides the user with the response code, for example by phone or text message.
6. The user enters the response code. Depending on the recovery type, this is either done in the SafeGuard POA or in the KeyRecovery Tool.

The user is then permitted to perform the authorized action, for example resetting the password, and can resume working.

7.5.2 Launch the Recovery Wizard

To be able to perform a recovery procedure, make sure you have the required rights and permissions.

1. Log on to the SafeGuard Management Center.
2. Click **Tools > Recovery** in the menu bar.

The **Recovery Wizard** is started. You can select which type of recovery you want to use.

7.5.3 Recovery via mobile devices

BitLocker and FileVault 2 recovery keys can be sent to the Sophos Mobile Server. They will be added to the SafeGuard Enterprise key ring and users of Sophos Secure Workspace managed by Sophos Mobile can then display these keys on their compliant mobile device for recovery purposes. Sophos Secure Workspace supports recovery via mobile from version 6.2. For details see the Sophos Secure Workspace 6.2 user help.

Requirements:

- Key ring sharing between SafeGuard Enterprise and Sophos Mobile must be configured. The **Recovery via mobile** option must be activated, see [Share SafeGuard Enterprise key ring with mobile devices managed by Sophos Mobile \(page 392\)](#).
- Sophos Secure Workspace 6.2 must be used on mobile devices.
- Users have to be SGN users on the endpoints. They need to be in the UMA (User-Machine-Assignment list) of the endpoints concerned.
- Users must have logged on to a particular computer from which they should get the full disk encryption keys.

 **Note** In order to limit the amount of transmitted data only the keys of ten endpoints are added to the SafeGuard Enterprise key ring. These ten computers are the ones with the most recent server contact.

7.5.3.1 Display recovery keys on mobile devices

 **Note** Sophos Secure Workspace must be installed inside the Sophos container.

To display the recovery key for a computer:

1. Tap **Recovery keys** in the menu to display a list of computers that are assigned to you.
2. Tap a computer name to display its recovery key.
3. To unlock your computer, follow the instructions that are displayed on the BitLocker (on Windows) or FileVault (macOS) screen on your computer.

7.6 Tools

This section explains the use of tools provided by SafeGuard Enterprise.

You can find the tools in the Tools directory of your SafeGuard Enterprise software delivery.

Intended audience

The intended audience for this guide are administrators working with SafeGuard Enterprise as security officers.

7.6.1 Client/Server Connectivity Check tool for Windows

If users have troubles synchronizing their endpoint with the server, you can use the Client/Server Connectivity Check tool to find out why the communication between the endpoint and the SafeGuard Enterprise Server fails. It checks all relevant connections and lists the results.

If the tool detects a communication problem, see [Sophos knowledge base article 109662](#) for troubleshooting.

7.6.1.1 Checking connection to the server

Windows

Open `C:\Program Files (x86)\Sophos\SafeGuard Enterprise\Client` and run the `SGNCSCC.exe` application.

Mac

Open `/Library/Application Support/Sophos Encryption/` and run the `SGNConnectivityTool` application.

7.6.2 Displaying Synchronized Encryption policies on endpoints

SafeGuard Enterprise offers the command-line tool `ShowSyncEncPolicyn.exe` for displaying Synchronized Encryption policies currently applied on an endpoint.

You always have to run the tool in the proper user context. For example, running the tool as administrator on user A's endpoint will not display the correct policies for user A.

It displays:

- the application list. It contains all applications for which file encryption is executed automatically (In-Apps).
- a list of file extensions that are considered by initial encryption and Asynchronous Encryption.
- the encryption rules for Synchronized Encryption. They contain the paths where files are encrypted or excluded from encryption and the appropriate keys.

Parameters

You can call ShowSyncEncPolicyn.exe with the following parameters:

ShowSyncEncPolicyn.exe [-h] [-A] [-a] [-e] [-d]

- Parameter -h displays the help.
- Parameter -A displays the application list, file extensions, and encryption rules.
- Parameter -a displays the application list.
- Parameter -e displays file extensions.
- Parameter -d displays encryption rules.

Example

```
ShowSyncEncPolicyn.exe -A
```

The following is displayed:

- a reminder to run the tool in the proper user context.
- the encryption scope as defined in the policy. For example: **everywhere**.
- the paths where files are encrypted and the appropriate key for each path.

- the directories that are excluded from encryption.
- the list of file extensions that are considered by initial encryption and Asynchronous Encryption.
- the list of In-Apps.

7.6.3 Displaying the system status with SGNState

SafeGuard Enterprise offers the command-line tool SGNState for displaying information about the current status (encryption status and further detailed status information) of the SafeGuard Enterprise installation on an endpoint.

Reporting

SGNState can also be used as follows:

- The SGNState return code can be evaluated on the server using third-party management tools.
- SGNState /LD returns output that is formatted for LANDesk which can be saved to a file.

Parameters

You can call SGNState with the following parameters:

SGNState [/?] [/H/Type>Status] [/L] [/LD] [/USERLIST]

- Parameter /? returns help information about the available SGNState command-line parameters.
- Parameter /H Type returns additional help information about drive types.
- Parameter /H Status returns additional help information about drive status.
- Parameter /L shows the following information:

Operating system

Product version

Encryption type [SGN | Opal | BitLocker | BitLocker-C/R | unknown or earlier version of SGN]

Power On Authentication [yes | no | n/a]

WOL (Wake on LAN status) [yes | no | n/a]

Server name

Second Server name

Logon mode [SGN, no automatic logon | UID/PW | TOKEN/PIN | FINGERPRINT | BL (BitLocker)]

Client activation state [ENTERPRISE | OFFLINE]

Last data replication [date, time]

Enforced cert-based token logon in POA [yes | no | n/a]

FIPS mode enabled [yes | no]

User certificate type [0 | 1 | 2 | 3|n/a|?]

Return code [return code]

File encryption driver versions [driver versions]

Volume info:

Name	Type	Status	Encryption method
<name>	[HD-Part ...]	[encrypted not encrypted ...] [<algorithm name> n/a ...]	
	FLOPPY	not accessible	
	REMOV.PART	stopped because of a failure	
	REM_PART	encryption starting	
	HD-PART	encryption in progress	
	UNKNOWN	decryption starting	
		decryption in progress	
		not prepared	

- Parameter /LD returns this information formatted for LANDesk.

The output is similar to the output of /L, but each line begins with “Sophos SafeGuard”:

Example:

Sophos SafeGuard - Operating system = Windows 10 Enterprise

Sophos SafeGuard - Product version = 8.20.0.64

Sophos SafeGuard - Encryption type = BitLocker

...

- If you call SGNState with parameter /USERLIST, additionally a list of all users in the UMA and the types of certificates assigned to them is displayed,

Certificate type:

0	no certificate is assigned to the user
1	P7 certificate (for example Token logon with P12 on SmartCard)
2	P12 certificate
3	P7+P12 certificate (normal SGN user)
n/a	the certificate type cannot be determined
?	unknown certificate combination

- Return code

0	no volume has been encrypted
1	at least one volume is encrypted
-1	an error has occurred (for example, no SafeGuard Enterprise device encryption is installed)

7.6.4 Reverting an unsuccessful installation with SGNRollback

 **Note** SGNRollback should only be used with Windows 7 without BitLocker.

If there is an unsuccessful attempt to install SafeGuard Enterprise on an endpoint, the computer may be unable to boot and may be inaccessible for remote administration.

SGNRollback can repair an unsuccessful SafeGuard Enterprise installation on an endpoint, if the following applies:

- The Power-on Authentication freezes during the first startup and the computer can no longer boot.
- The hard drive is not encrypted.

SGNRollback automatically reverts the effects of an unsuccessful installation of SafeGuard Enterprise by

- Enabling the blocked computer to boot,
- Removing SafeGuard Enterprise and
- Undoing any modifications to other operating system components.

Start SGNRollback from a Windows-based recovery system, either WindowsPE or BartPE.

7.6.4.1 Prerequisites

Prerequisites for using SGNRollback:

- SGNRollback works on the recovery systems WinPE and BartPE. To be able to use SGNRollback for recovery, integrate it into the required recovery system. Please see the relevant recovery system documentation for further information.

If SGNRollback is to be started by autorun, the administrator using SGNRollback has to define the relevant settings in WinPE as described in [Enabling SGNRollback autostart for Windows PE \(page 437\)](#) or BartPE as described in [Enabling SGNRollback autostart for BartPE \(page 437\)](#).

- SafeGuard Enterprise full disk encryption is installed.

 **Note** Migration from SafeGuard Easy to SafeGuard Enterprise is not supported.

7.6.4.2 Starting SGNRollback in the recovery system

You can start SGNRollback manually or add it to the recovery system autostart.

[Enabling SGNRollback autostart for Windows PE](#)

To enable SGNRollback autostart for Windows PE, install the Microsoft Windows Automated Installation Kit. The Windows Preinstallation Environment User Guide describes how to build a Windows PE environment and how to autostart an application.

Enabling SGNRollback autostart for BartPE

1. Use the BartPEBuilder version 3.1.3 or later to create a PE image. For further details, see the BartPE documentation.
2. In the BartPE Builder, add the recovery tool folder in the **Custom** field.
3. Build the image.
4. Copy the file AutoRun0Recovery.cmd from the SafeGuard Enterprise Media to the i386 folder of the BartPE-prepared Windows version.
5. Create an AutoRun0Recovery.cmd with the following two lines of text:

```
\Recovery\recovery.exe
```

```
exit
```

6. Run the PEBuilder tool from the command line:

```
Pebuilder -buildis
```

A new iso image is built which includes the autorun file.

7. Save the resulting image on recovery media.

When booting this image SGNRollback will start automatically.

7.6.4.3 Parameters

SGNRollback can be started with the following parameter:

-drv WinDrive	Indicates the letter of the drive the SafeGuard Enterprise installation to be repaired is on. This parameter can only be used in recovery mode. It has to be used on multi-boot systems to indicate the correct drive.
---------------	--

7.6.4.4 Reverting an unsuccessful installation

To revert the effects of an unsuccessful SafeGuard Enterprise installation on an endpoint:

1. Start the computer from the recovery media containing the recovery system including SGNRollback.

2. Start SGNRollback in the recovery system. If autorun applies, SGNRollback will start automatically. SGNRollback prepares the operating system for the uninstallation of SafeGuard Enterprise.
3. You are prompted to remove the recovery media. After you remove the media, the computer will be restarted in safe mode of the operating system.

All modifications are undone and SafeGuard Enterprise is uninstalled.

7.6.5 Recovering access to computers with the KeyRecovery tool

The KeyRecovery tool is used to regain access to a computer in a complex recovery situation, for example when the POA is corrupted and the computer needs to be started from the SafeGuard recovery disk. The tool is started in the context of a Challenge/Response procedure.

 **Note** You can find a detailed description of the tool in the *SafeGuard Enterprise administrator help*, section *Challenge/Response using Virtual Clients*.

7.6.6 Restoring Windows BIOS SafeGuard full disk encryption systems

 **Note** The following description applies to Windows BIOS endpoints with SafeGuard full disk encryption and SafeGuard Power-on Authentication.

SafeGuard Enterprise encrypts files and drives transparently. Boot volumes can also be encrypted, so decryption functionalities such as code, encryption algorithms and encryption key must be available very early in the boot phase. Therefore encrypted information cannot be accessed if the crucial SafeGuard Enterprise modules are unavailable or do not work.

7.6.6.1 Restoring a corrupted MBR

The SafeGuard Enterprise Power-on Authentication is loaded from the MBR on a computer's hard disk. When the installation is done, SafeGuard Enterprise saves a copy of the original - as it was before the SafeGuard Enterprise installation - in its kernel and modifies the PBR loader from LBA 0. In its LBA 0, the modified MBR contains the address of the first sector of the SafeGuard Enterprise kernel and its total size.

Problems with the MBR can be resolved using the SafeGuard Enterprise restore tool `be_restore.exe`. This tool is a Win32 application and must run under Windows - not under DOS.

A faulty MBR loader will mean an unbootable system. It can be restored in two ways:

- Restoring the MBR from a backup.

- Repairing the MBR.

To restore a corrupted MBR successfully, prepare as follows:

1. We recommend that you create a Windows PE (Preinstalled Environment) CD.
2. To use the restore tool be_restore.exe several additional files are required. You can find the tool and the required files in your SafeGuard Enterprise software delivery under Tools\KeyRecovery and restore. Copy all files in this folder to a memory stick. Make sure that you store all of them together in **the same** folder on your memory stick. Otherwise the restore tool will not start properly.

 **Note** In order to start be_restore.exe in a Windows PE environment, the Windows file OLEDLG.dll is required. This file is not included in the Tools\KeyRecovery and restore folder. Add this file from a Windows installation to the recovery tool folder on your recovery CD.

3. If necessary, adjust the boot sequence in the BIOS and select the CD-ROM to be first.

 **Note** be_restore.exe can only restore or repair the MBR on disk 0. If you use two hard disks and the system is started from the other hard disk, the MBR cannot be restored or repaired. This also applies when using a removable hard disk.

7.6.6.2 Restoring a previously saved MBR backup

Every SafeGuard Enterprise endpoint saves its **own computer's** SafeGuard Enterprise MBR (LBA 0 of the boot hard disk after being modified by SafeGuard Enterprise) in the SafeGuard Enterprise Database. It can be exported from the SafeGuard Management Center to a file.

To restore a previously saved MBR backup:

1. In the SafeGuard Management Center, click **Users and Computers** and select the relevant computer in the navigation area.
2. Right-click the computer and select **Properties > Machine Settings > Backup > Export** to export the MBR. This produces a 512 byte file with the file extension .BKN, which contains the MBR.
3. Copy this file to the folder on the memory stick in which the other extra SafeGuard Enterprise files are located.
4. Now insert the Windows PE Boot CD into the drive, plug in the memory stick with the SafeGuard Enterprise files and switch the computer on to boot from the CD.
5. When the computer is ready, start the cmd-box, navigate to the directory on the memory stick where the SafeGuard Enterprise files are located and run be_restore.exe.

6. Select **Restore MBR** to restore from a backup and select the .BKN file.

The tool now checks if the selected .BKN file matches the computer and afterwards restores the saved MBR.

7.6.6.3 Repairing the MBR without backup

Even when there is no MBR backup file available locally, be_restore.exe can repair a damaged MBR loader. be_restore.exe - **Repair MBR** locates the SafeGuard Enterprise kernel on the hard disk, uses its address, and recreates the MBR loader.

This is highly advantageous, especially as there is no need for a computer-specific MBR backup file locally. However, it takes a little more time because the SafeGuard Enterprise kernel on the hard disk is searched for.

To use the repair function, prepare as described in [Restoring a corrupted MBR \(page 439\)](#), but select **Repair MBR** when running be_restore.exe.

If more than one kernel is found, be_restore.exe – **Repair MBR** uses the one with the most recent time stamp.

7.6.6.4 Partition table

SafeGuard Enterprise allows the creation of new primary or extended partitions. This changes the partition table on the hard disk with the partition.

When restoring an MBR backup, the tool detects that the current MBR contains different partition tables for the LBA 0 and the MBR backup file that is to be restored (*.BKN). In a dialog, the user can select which table to use.

Repairing an MBR with a corrupted partition table

A corrupted partition table may result in a non-bootable operating system after successful POA logon.

You can resolve this problem by using be_restore.exe to restore a previously saved MBR or repair the MBR without an MBR backup.

If you have a backup, proceed as described for the **Restore MBR** option.

If you do not have a backup, do as follows:

1. Insert the Windows PE Boot CD into the drive, plug in the memory stick with the SafeGuard Enterprise files and switch the computer on to boot from the CD.

2. When the computer is ready, go to the command prompt, navigate to the directory on the memory stick where the SafeGuard Enterprise files are located and run be_restore.exe
3. Select **Repair MBR**. If be_restore.exe detects a difference between the partition table of the current MBR and the mirrored MBR, a dialog for selecting the partition table to be used is displayed.

The mirrored MBR is the original Microsoft MBR saved during the SafeGuard Enterprise Client setup to enable you to restore it, for example if you uninstall the client. The partition table in this mirrored MBR is being kept up-to-date by SafeGuard Enterprise, if any partition changes occur in Windows.

4. Select **From Mirrored MBR**.

 **Important** Do not select **From Current MBR**. If you do, the corrupted partition table from the current MBR will be used. Not only will the system in this case remain non-bootable, but also the mirrored MBR will be updated and therefore also corrupted.

7.6.6.5 Windows Disk Signature

Whenever Windows creates a file system for the first time on a hard disk, it creates a signature for the hard disk. This signature is saved in the hard disk's MBR at the Offsets 0x01B – 0x01BB. Note that, for example, the logical drive letters of the hard disk depend on the Windows Disk Signature.

Therefore do not change the Disk Signature, for example by using ("FDISK/MBR"). Otherwise Windows goes into a time-consuming hard disk scan mode during the next startup process and restores the list of drives.

Whenever that occurs under SafeGuard Enterprise, SafeGuard Enterprise's filter driver "BEFLT.sys" is not loaded. This makes the system unbootable: The computer shows a blue screen 'STOP 0xED "Unmountable Boot Volume".

To repair this under SafeGuard Enterprise, the original Windows Disk Signature has to be restored in the hard disk's MBR.

This is done by be_restore.exe.

 **Note** Do not use any other tool to repair the MBR. For example, an old MS DOS FDISK.exe, that you use to rewrite the MBR loader ("FDISK /MBR") could create another MBR loader with no Windows Disk Signature. As well as deleting the Windows Disk Signature, the "new" MBR loader created by an old tool might not be compatible with the hard disk sizes commonly used today. You should always use up-to-date versions of repair tools.

7.6.6.6 Boot sector

During the encryption process a volume's boot sector is swapped for the SafeGuard Enterprise boot sector. The SafeGuard Enterprise boot sector holds information about the location and the size of the primary and backup KSA. The location is identified in clusters and sectors referenced from the start of the partition. Even if the SafeGuard Enterprise boot sector is damaged, encrypted volumes cannot be accessed. The be_restore utility can restore the damaged boot sector.

7.6.7 Restoring Windows UEFI BitLocker Challenge/Response systems

For restoring Windows UEFI BitLocker systems, Sophos offers the restore tool BLCRBackupRestoren.exe. With this tool, you can:

- Back up BitLocker Challenge/Response-related data:

This is only necessary if the automatic backup failed (log event 3071: "Key backup could not be saved to the specified network share.")

- Manually restore a previously created backup and repair the NVRAM boot order:

This is only necessary if you suspect that BitLocker Challenge/Response-related data was corrupted or deleted.

BLCRBackupRestoren.exe needs to be started from a Windows PE environment. It is included on the Sophos Virtual Client CD.

7.6.7.1 Starting the command line tool

Syntax

`blcrbackuprestoren [-?] [-B [-T <Filepath>]] [-R [-K <Filename>] [-S <Filename>]] [-I] [-D]`

Options

- `-?`

Display help

- `-B`

Backup

- `-T <Filepath>`

Optional existing Target Path

- -R

Restore

- -K <Filename>

Optional Key Path\Filename

The optional key file is the .BKN file that needs to be exported from the SafeGuard Management Center.

To export it:

- In the SafeGuard Management Center, click **Users and Computers** and select the relevant computer in the navigation area.
- Right-click the computer and select **Properties > Machine Settings > Backup > Export.**

If BitLocker Challenge/Response-related data has been backed up successfully, option -R is sufficient.

- -S <Filename>

Optional Source Path\Filename

- -I

Install boot entry.

- -D

Delete boot entry.

 **Note** If the automatic restore fails, then, in order to use a backup file available on a recovery partition without a drive letter assigned, you need to

- assign a drive letter to the recovery partition
- and then provide the fully-qualified path to the backup file.

There is always only one file: <drive-letter>:\SOPHOS\<file name>.cps.

Examples

- **Back up**

- blcrbackuprestoren -b creates an archive at the default location.

- blcrbackuprestoren -b -T <USBStick drive>:\Backup\ creates an archive on an external drive.

- **Restore**

- blcrbackuprestoren -r extracts the archive from the default location.
- blcrbackuprestoren -r -k X:\example\example.BKN extracts the archive from the default location and reconstructs key file.

7.6.8 Decommissioning encrypted volumes

For SafeGuard Enterprise-protected computers we provide the command-line tool beinvvol.exe which can be used to safely decommission encrypted volumes (hard disks, USB sticks etc.). Our command-line tool is based on DoD Standard 5220.22-M, which can be used to safely delete key stores. This standard consists of seven overwrite cycles with random and alternative patterns.

This command-line tool is intended to be used on computers for which the following applies:

- SafeGuard Enterprise is installed.
- Some hard disk volumes have been encrypted.

You have to run this tool within a system where the SafeGuard Enterprise encryption driver is not active. This is to prevent data from being decommissioned by accident. Otherwise, the tool does not work and an error message is displayed.

 **Note** We recommend that you start your system from an external medium like a Windows PE CD and use the tool according to the instructions available in the command line help.

After the relevant target volumes have been decommissioned, they are no longer readable.

According to DoD Standard 5220.22-M, the command-line tool permanently purges the boot sectors and the SafeGuard Enterprise Key Storage Areas (original KSA and backup) of each encrypted volume by overwriting them seven times. As the random Data Encryption keys of each volume are not backed up in the central database for SafeGuard Enterprise Clients, the volumes are perfectly sealed afterwards. Even a security officer cannot regain access.

The command-line tool also displays information about the available volumes on screen. This includes, for example, the name of the volume, the size of the volume and information about boot sectors and KSAs. This information can optionally be stored in a file. The path to this file should, of course, point to a volume that is not being decommissioned.

 **Note** Data cannot be recovered after deletion.

7.6.8.1 Starting the command-line tool

Syntax

- `xl[volume]`

List information for the target volume(s). If no target volume is specified, list information for all volumes.

- `xi<volume>`

Invalidate the target volume(s), if fully SGN-encrypted. The target `<volume>` must be specified for this command.

- `<volume>`

Specify the target volume = { a, b, c, ..., z, * }, with `<*>` meaning all volumes.

Options

- `-g0`

Disable logging mechanism.

- `-ga[file]`

Logging mode -append. Append log entries at the end of the target log file or create it if it does not exist.

- `-gt[file]`

Logging mode -truncate. Truncate the target log file if it already exists or create it if it does not exist.

- `[file]`

Specify the target log file. If not specified, the default target log file is "BEInvVol.log" at the current path. You must not specify the log file on the volume that is going to be invalidated!

- -?, -h

Display help.

Examples

```
> beinvvol -h
> beinvvol xld
> beinvvol xle -ga"c:\subdir\file.log"
> beinvvol xl* -gt"c:\subdir\file.log"
> beinvvol xif -gt"c:\my subdir\file.log"
> beinvvol xig -g0
> beinvvol xi*
```

7.6.9 Decommissioning self-encrypting, Opal-compliant hard drives

Self-encrypting hard drives offer hardware-based encryption of data when they are written to the hard disk. The Trusted Computing Group (TCG) has published the vendor-independent Opal standard for self-encrypting hard drives. SafeGuard Enterprise supports the Opal standard and offers management of endpoints with self-encrypting, Opal-compliant hard drives.

For further information about Opal-compliant hard drives, see the *SafeGuard Enterprise administrator help*, chapter *SafeGuard Enterprise and self-encrypting Opal-compliant hard drives*.

For SafeGuard Enterprise-protected computers we provide the command-line tool opalinvdisk.exe.

7.6.9.1 Prerequisites and recommendations

For using opalinvdisk.exe, the following prerequisites and recommendations apply:

- Before you use opalinvdisk.exe, the Opal-compliant hard disk has to be decrypted with the SafeGuard Enterprise **Decrypt** command from the Windows Explorer context menu on the endpoint. For further information, see the *SafeGuard Enterprise administrator help*, section *Enable users to unlock Opal-compliant hard drives* and the *SafeGuard Enterprise user help*, section *System Tray Icon and Explorer extensions on endpoints with Opal-compliant hard drives*.

- You need administrator rights.
- We recommend that you use opalinvdisk.exe in a Windows PE environment.
- The tool opalinvdisk.exe starts the optional service RevertSP with parameter KeepGlobalRangeKey set to False. The actual decommissioning procedure carried out by RevertSP depends on the specific hard drive. For further information, refer to section 5.2.3 of the Opal standard TCG Storage Security Subsystem Class: Opal, Specification Version 1.00, Revision 3.00, which is available at www.trustedcomputinggroup.org.

7.6.9.2 Running opalinvdisk.exe

1. Open a command prompt and start opalinvdisk.exe with administrator rights.

Tool and usage information is displayed.

2. At the command prompt, enter opalinvdisk.exe <TargetDevice>.

For example: opalinvdisk.exe PhysicalDrive0

If the necessary prerequisites are fulfilled, RevertSP is started on the hard drive specified in <TargetDevice>. If the prerequisites are not fulfilled or the hard drive does not support RevertSP, an error message is displayed.

8. 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 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>.

9. Legal notices

Copyright © 2021 Sophos Limited. 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, 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.