# conpal LAN Crypt

Persistent
Hochsicher
Skalierbar

## Client Hilfe

Produktversion: 3.97
Stand: Mai 2019

# Contents

# 1 Was ist SafeGuard LAN Crypt?

SafeGuard LAN Crypt ermöglicht mit transparenter Dateiverschlüsselung den Austausch vertraulicher Daten innerhalb von Berechtigungsgruppen in großen Organisationen. SafeGuard LAN Crypt funktioniert ohne Benutzerinteraktion. Es unterstützt die Rolle eines Security Officers (SO), der die Zugriffsrechte auf Dateien, die mit SafeGuard LAN Crypt verschlüsselt sind, einschränken kann. Ein Master Security Officer (MSO) kann das Recht, SafeGuard LAN Crypt zu verwalten, delegieren. Auf diese Weise lässt sich eine Hierarchie von Security Officers einrichten, die die Sicherheitsanforderungen in jedem Unternehmen erfüllt.

Verschlüsselte Dateien sind nicht einzelnen Benutzern zugewiesen. Jeder Benutzer, der über den benötigten Schlüssel verfügt, kann mit einer verschlüsselten Datei arbeiten. Dies erlaubt Administratoren das Erzeugen von logischen Benutzergruppen, die gemeinsam auf verschlüsselte Dateien zugreifen können. Dieser Vorgang kann mit einer Art Schlüsselbund, wie er im täglichen Leben verwendet wird, verglichen werden. SafeGuard LAN Crypt stattet Benutzer und Benutzergruppen mit einem Schlüsselbund aus, dessen Schlüssel für verschiedene Türen oder Safes verwendet werden können.

Jedes Mal, wenn ein Benutzer eine Datei in ein verschlüsseltes Verzeichnis verschiebt, wird die Datei auf dem Computer dieses Benutzers verschlüsselt. Wenn ein anderer Benutzer aus derselben Berechtigungsgruppe die Datei aus dem Verzeichnis liest, wird sie in verschlüsselter Form übertragen. Die Datei wird nur auf dem Computer des Empfängers entschlüsselt. Der Benutzer kann sie dort bearbeiten. Bevor die Datei wieder in das verschlüsselte Verzeichnis übertragen wird, wird sie wieder verschlüsselt.

Nicht berechtigte Benutzer können unter Umständen auf diese verschlüsselten Dateien zugreifen (nur von Arbeitsstationen ohne SafeGuard LAN Crypt), sehen aber ohne die entsprechende SafeGuard LAN Crypt Berechtigung nur verschlüsselten Inhalt. Auf diese Weise bleibt die Datei immer geschützt, auch wenn im Dateisystem selbst kein Zugriffsschutz definiert ist, das Netzwerk angegriffen wird, oder die Mitarbeiter sich nicht an die Sicherheitsrichtlinien der Organisation halten.

## *1.1 Schutz von Daten durch SafeGuard LAN Crypt*

SafeGuard LAN Crypt garantiert, dass sensible Dateien auf File Servern und Arbeitsstationen verschlüsselt gespeichert werden können. Ebenso erfolgt die Übertragung in Netzwerken (LAN oder WAN) geschützt, da Ver- und Entschlüsselung im Hauptspeicher der Arbeitsstation des Benutzers durchgeführt werden. Auf den Arbeitsstationen laufen alle Ver- und Entschlüsselungen transparent und weitgehend ohne Benutzerinteraktionen ab. Auf dem File-Server selbst muss keine spezielle Sicherheitssoftware installiert werden.

Ein Security Officer kann unterschiedliche Zugriffsrechte für Verzeichnisse und Dateien definieren. Diese Rechte werden in Verschlüsselungsprofilen für die Benutzer zusammengefasst. Verschlüsselungsprofile werden über Richtliniendateien an die Benutzer verteilt. Richtliniendateien enthalten alle Regeln, Zugriffsrechte und Schlüssel, die für die transparente Verschlüsselung benötigt werden. Die Richtliniendatei ist durch ein Zertifikat geschützt. Damit Benutzer auf ihren Computern mit SafeGuard LAN Crypt verschlüsselte Daten verarbeiten können, müssen sie Zugriff auf die Richtliniendatei haben. Durch den Besitz des zum Zertifikat gehörenden privaten Schlüssels hat der Benutzer Zugriff auf die Richtliniendatei, in der das Verschlüsselungsprofil gespeichert ist.

SafeGuard LAN Crypt ermöglicht die Einteilung der Benutzer in verschiedene Berechtigungsgruppen. Alle SafeGuard LAN Crypt Benutzer, die in ihrer Richtliniendatei dasselbe Verschlüsselungsprofil gespeichert haben, sind Mitglieder einer Berechtigungsgruppe. Sie brauchen sich nicht um die Verschlüsselung oder um den Schlüsselaustausch zu kümmern. Sie müssen nur in der Lage sein, auf die Richtliniendateien zuzugreifen, damit die Dateien transparent ver- bzw. entschlüsselt werden können, sobald sie geöffnet bzw. geschlossen werden. Es können alle Organisationsformen abgebildet werden - von einem LAN-Modell, in dem die Benutzer zentral administriert werden, bis zu einem verteilten Modell, in dem Benutzer Notebooks einsetzen.

## *1.2 SafeGuard LAN Crypt und SafeGuard Enterprise*

Diese Version von SafeGuard LAN Crypt und SafeGuard Enterprise können gleichzeitig auf einem Computer verwendet werden. Zum Beispiel können alle Dateien auf Wechselmedien mit SafeGuard Enterprise Data Exchange und alle Dateien auf Netzwerklaufwerken mit SafeGuard LAN Crypt verschlüsselt werden. Nähere Informationen zu den unterstützten Versionen finden Sie in den SafeGuard LAN Crypt Versionsinfos.

SafeGuard LAN Crypt zeigt im Dialog **Clientstatus** alle auf dem System geltenden Verschlüsselungsregeln an, siehe Der Dialog Clientstatus *(page 21)*. Generell gilt, dass SafeGuard Enterprise Data Exchange Regeln vor jenen von SafeGuard LAN Crypt angewendet werden. Die Priorisierung kann jedoch geändert werden.

**Note:** Für die **Persistente Verschlüsselung** gilt immer die Einstellung von SafeGuard Enterprise. Dies kann nicht geändert werden.

## Umschlüsseln von Dateien, die mit SafeGuard Enterprise Data Exchange verschlüsselt wurden

Der **Assistent zur Initialverschlüsselung** ermöglicht das Umschlüsseln von Dateien, die mit SafeGuard Enterprise Data Exchange verschlüsselt wurden, für die aber keine SafeGuard Enterprise Verschlüsselungsregel mehr gilt, siehe Assistent zur Initialverschlüsselung *(page 11)*. Solche Dateien liegen zum Beispiel vor, wenn die SafeGuard Enterprise Verschlüsselungsregel aufgehoben wurde, die Dateien aber nicht explizit entschlüsselt wurden. In diesem Fall kann im **Assistenten zur Initialverschlüsselung** die Option **Dateien entsprechend den Regeln umschlüsseln** ausgewählt werden, wodurch diese Dateien den SafeGuard LAN Crypt Verschlüsselungsregeln entsprechend umgeschlüsselt werden.

# 2 Verschlüsselung

## 2.1 Transparente Verschlüsselung

Transparente Verschlüsselung bedeutet für den Benutzer, dass alle verschlüsselt gespeicherten Daten (in verschlüsselten Verzeichnissen oder Laufwerken) automatisch im Hauptspeicher entschlüsselt werden, sobald sie in einem Programm geöffnet werden. Beim Abspeichern der Datei wird sie automatisch wieder verschlüsselt. Von der transparenten Verschlüsselung werden alle Dateivorgänge erfasst. Da alle Prozesse im Hintergrund laufen, bemerken Benutzer nichts davon, wenn sie mit verschlüsselten Daten arbeiten.

**Note:**

SafeGuard LAN Crypt kann keine Dateien verschlüsseln, für die unter dem NTFS-Dateisystem von Windows die **NTFS-Komprimierung** oder **EFS-Verschlüsselung** verwendet wird. Der Assistent zur Initialverschlüsselung bietet allerdings die Möglichkeit, wenn für NTFS-komprimierte und/oder EFS-verschlüsselte Dateien eine Verschlüsselungsregel besteht, diese im Rahmen der Initialverschlüsselung zur dekomprimieren bzw. zu entschlüsseln. Die Dateien werden anschließend von SafeGuard LAN Crypt entsprechend den Verschlüsselungsregeln verschlüsselt. Ob der Benutzer die Möglichkeit hat, NTFS-komprimierte Dateien zu dekomprimieren oder EFS- verschlüsselte Dateien wenn notwendig zu entschlüsseln, wird vom Security Officer festgelegt.

Die Verschlüsselung ist nicht von Verzeichnissen abhängig, sondern nur von Verschlüsselungsregeln. Die Verschlüsselung funktioniert wie folgt:

- Alle Dateien, für die eine Verschlüsselungsregel existiert, werden automatisch verschlüsselt.
- Werden Dateien in ein verschlüsseltes Verzeichnis verschoben oder kopiert, werden sie gemäß der für dieses Verzeichnis definierten Verschlüsselungsregel verschlüsselt. Der Security Officer kann verschiedene Verschlüsselungsregeln für verschiedene Dateierweiterungen oder Namen im selben Verzeichnis definieren.
- Beim Umbenennen von verschlüsselten Dateien bleiben diese verschlüsselt (sofern nicht eine andere oder keine Verschlüsselungsregel für den neuen Dateinamen oder die neue Dateierweiterung besteht).
- Wenn ein Benutzer verschlüsselte Dateien an einen Ort kopiert oder verschiebt, an dem die bisherige Verschlüsselungsregel nicht mehr gilt, werden sie automatisch entschlüsselt.

  **Note:** Dies gilt nicht, wenn ein Benutzer Dateien innerhalb derselben Netzwerkfreigabe in ein anderes Verzeichnis verschiebt. In diesem Fall bleiben die Dateien verschlüsselt, obwohl keine Verschlüsselungsregel gilt.

- Wenn der Security Officer die Funktion **Persistente Verschlüsselung** aktiviert hat, bleiben verschlüsselte Dateien auch dann verschlüsselt, wenn sie in einen Ordner ohne Verschlüsselungsregel verschoben werden.
- Wenn ein Benutzer verschlüsselte Dateien an einen Ort kopiert oder verschiebt, an dem eine andere Verschlüsselungsregel gilt, werden die Dateien zuerst entschlüsselt und danach mit dem für diesen Speicherort definierten Schlüssel verschlüsselt.

### 2.1.1 Zugriff auf verschlüsselte Daten

Gibt es in den Verschlüsselungsrichtlinien eines Benutzers keinen Schlüssel und keine Verschlüsselungsregel für ein bestimmtes Verzeichnis, darf er nicht auf die verschlüsselten Dateien in diesem Verzeichnis zugreifen. Er darf dort keine verschlüsselte Datei lesen, kopieren, verschieben, umbenennen usw.

Verfügt der Benutzer über den Schlüssel, mit dem die Dateien verschlüsselt sind, kann er sie öffnen, auch wenn sein Verschlüsselungsprofil dafür keine Verschlüsselungsregel beinhaltet.

**Note:** Beim Abspeichern von Dateien, die „nur“ mit dem vorhandenen Schlüssel (keine Verschlüsselungsregel für diese Dateien) geöffnet wurden, kann es dazu kommen, dass diese unverschlüsselt angelegt werden. Dies ist bei Programmen der Fall, die beim Speichern eine temporäre Datei anlegen, die Quelldatei dann löschen und anschließend die temporäre Datei umbenennen. Da für die neu angelegte Datei keine Verschlüsselungsregel existiert, wird sie unverschlüsselt angelegt. Um das zu verhindern, muss ein solches Programm als "Programm mit speziellem Speicherverhalten" eingetragen werden, siehe Der Dialog Clientstatus *(page 21)*.

## 2.1.2 Verzeichnisse umbenennen oder verschieben

SafeGuard LAN Crypt führt aus Performance-Gründen beim Verschieben ganzer Verzeichnisse innerhalb eines Laufwerks über den Windows Explorer keine Änderung des Verschlüsselungsstatus durch. Das bedeutet, dass es beim Verschieben eines Verzeichnisses zu keiner Ver-, Ent- bzw. Umschlüsselung kommt.

Waren die Dateien in diesen Verzeichnissen verschlüsselt, bleiben sie unter dem neuen Verzeichnisnamen bzw. am neuen Speicherort verschlüsselt. Besitzt der Benutzer den entsprechenden Schlüssel, kann er wie gewohnt mit diesen Dateien arbeiten.

Anders ist das Verhalten beim Verschieben von Dateien oder Ordnern auf eine andere Partition oder auf USB-Speichermedien, für die keine Verschlüsselungsregel eingerichtet wurde. Ist die **Persistente Verschlüsselung** nicht aktiviert, werden die Dateien entschlüsselt, wenn sie auf derartige Medien verschoben werden. Hat der Administrator dagegen die Funktion **Persistente Verschlüsselung** aktiviert, bleiben die Dateien verschlüsselt.

### Sicheres Verschieben

SafeGuard LAN Crypt unterstützt das sichere Verschieben von Dateien und Verzeichnissen. Beim Verschieben durch SafeGuard LAN Crypt werden die Dateien auch am neuen Speicherort entsprechend den geltenden Verschlüsselungsregeln ver-, ent- bzw. umgeschlüsselt. Danach werden die Quelldateien sicher gelöscht.

Diese Funktion steht über den Eintrag **SafeGuard LAN Crypt** >**Sicheres Verschieben** im Windows Explorer Kontextmenü von SafeGuard LAN Crypt zur Verfügung. Über einen Dialog kann dann ausgewählt werden, wohin die Dateien verschoben werden sollen.

## 2.1.3 Explizite Entschlüsselung von Dateien

Um eine Datei zu entschlüsseln, müssen Sie sie nur in ein ein Verzeichnis ohne Verschlüsselungsregeln kopieren oder verschieben. Die Datei wird automatisch entschlüsselt.

Voraussetzungen:

- Ein entsprechendes Verschlüsselungsprofil ist geladen,
- der Benutzer verfügt über den erforderlichen Schlüssel,
- das aktive Verschlüsselungsprofil enthält keine Verschlüsselungsregel für den neuen Speicherort,
- und **Persistente Verschlüsselung** ist nicht aktiv.

**Note:** SafeGuard LAN Crypt kann auch Offlineordner in Windows verschlüsseln. Allerdings können hierbei in Verbindung mit Virenscannern Probleme auftreten. Genauere Informationen zu bekannten Problemen mit Virenscannern finden Sie in den Versionsinfos zum SafeGuard LAN Crypt Client.

## 2.1.4 Löschen verschlüsselter Dateien - Windows Papierkorb

Wenn Ihr Verschlüsselungsprofil geladen ist, können Sie jede verschlüsselte Datei löschen, für die Sie einen Schlüssel besitzen.

**Note:** Eigentlich handelt es sich beim Löschen von Dateien um ein Verschieben der Dateien in den Windows Papierkorb. Um den höchsten Sicherheitsstandard zu gewährleisten, bleiben die mit SafeGuard LAN Crypt verschlüsselten Dateien auch im Papierkorb verschlüsselt. Um den Papierkorb zu leeren ist kein Schlüssel notwendig.

## 2.1.5 Von der Verschlüsselung ausgenommene Dateien und Verzeichnisse

Folgende Dateien und Verzeichnisse sind automatisch von der Verschlüsselung ausgenommen, auch wenn für sie eine Verschlüsselungsregel definiert wurde:

- Dateien im Installationsverzeichnis von SafeGuard LAN Crypt

- Dateien im Installationsverzeichnis von Windows
- Richtliniendatei-Cache

  Der Ablageort ist in SafeGuard LAN Crypt Administration spezifiziert und wird in der Registerkarte **Profil** im Dialog **Status** angezeigt.
- Stammverzeichnis des Systemlaufwerks. Unterordner werden nicht ausgeschlossen.
- Indizierte Speicherorte (search-ms)

## *2.1.6 Persistente Verschlüsselung*

Für SafeGuard LAN Crypt kann ein Security Officer die **Persistente Verschlüsselung** konfigurieren. Dateien bleiben normalerweise nur so lange verschlüsselt, wie sie einer Verschlüsselungsregel unterliegen.

Wenn zum Beispiel ein Benutzer eine verschlüsselte Datei in einen Ordner kopiert, für den keine Verschlüsselungsregel definiert ist, wird die Datei im Zielordner entschlüsselt. Ist die **Persistente Verschlüsselung** aktiviert, bleiben Dateien auch dann verschlüsselt, wenn sie verschoben oder kopiert werden.

Um zu verhindern, dass unerwünschte Klartextkopien von verschlüsselten Dateien erstellt werden, werden Kopien verschlüsselter Dateien auch dann verschlüsselt, wenn sie an Speicherorten erstellt werden, für die keine Verschlüsselungsregel gilt.

Security Officer können dieses Verhalten in der SafeGuard LAN Crypt Konfiguration deaktivieren. Wird die Persistente Verschlüsselung deaktiviert, so werden Dateien entschlüsselt, wenn Sie an einen Speicherort kopiert oder verschoben werden, für den keine Verschlüsselungsregel gilt.

Für die **Persistente Verschlüsselung** gelten folgende Regeln:

- Der SafeGuard LAN Crypt Treiber behält nur den Namen der Datei ohne Pfadinformationen. Es werden somit nur Situationen erfasst, in denen Quell- und Zieldatei einen identischen Namen haben. Wenn die Datei während des Kopiervorgangs umbenannt wird, wird die resultierende Datei als neue Datei betrachtet und unterliegt daher nicht der **persistenten Verschlüsselung**.
- Wenn ein Benutzer eine verschlüsselte Datei mit **Speichern unter** unter einem anderen Dateinamen an einem Speicherort speichert, für den keine Verschlüsselungsregel gilt, ist die Datei unverschlüsselt.
- Informationen zu Dateien werden nur für eine begrenzte Zeit beibehalten. Dauert der Vorgang zu lang (länger als 15 Sekunden), wird die resultierende Datei als neue Datei betrachtet und unterliegt daher nicht der **persistenten Verschlüsselung**.

### 2.1.6.1 Persistente Verschlüsselung und Verschlüsselungsregeln

**Persistente Verschlüsselung** stellt sicher, dass eine verschlüsselte Datei Ihren Verschlüsselungsstatus beibehält, zum Beispiel den ursprünglichen Verschlüsselungsschlüssel. Dies funktioniert problemlos, wenn die Datei in einen Ordner ohne Verschlüsselungsrichtlinie kopiert oder verschoben wird. Wird die Datei jedoch an einen Speicherort kopiert oder verschoben, für den eine Verschlüsselungsrichtlinie gilt, hat die Verschlüsselungsrichtlinie höhere Priorität und setzt die **Persistente Verschlüsselung** außer Kraft. Die Datei wird mit dem in der Verschlüsselungsrichtlinie definierten Schlüssel verschlüsselt, nicht mit dem ursprünglich verwendeten Schlüssel.

### 2.1.6.2 Persistente Verschlüsselung und Ignorieren-Regeln

Eine Ignorieren-Regel setzt die **persistente Verschlüsselung** außer Kraft. Das bedeutet, dass Dateien, die in einen Ordner kopiert werden, für den eine Ignorieren-Regel gilt, entschlüsselt werden.

Die Ignorieren-Regel wird hauptsächlich für Dateien benutzt, auf die sehr häufig zugegriffen wird oder bei denen kein bestimmter Grund für eine Verschlüsselung vorliegt. Dadurch lässt sich die System-Leistung steigern.

### 2.1.6.3 Persistente Verschlüsselung und Ausnahmeregeln

Eine Ausnahmeregel setzt die **persistente Verschlüsselung** außer Kraft. Das bedeutet, dass Dateien, die in einen Ordner kopiert werden, für den eine Ausnahmeregel gilt, entschlüsselt werden.

## 2.1.7 Einschränkungen bei der persistenten Verschlüsselung

Bei der **persistenten Verschlüsselung** gelten einige Einschränkungen. Diese sind:

### Dateien, die eigentlich unverschlüsselt bleiben sollten, sind verschlüsselt

- **Klartext-Dateien werden an mehrere Speicherorten kopiert, ohne dass Verschlüsselungsregeln angewendet werden.**

  Wenn eine unverschlüsselte Datei gleichzeitig an mehrere Speicherorte, von denen für einen Speicherort eine Verschlüsselungsregel gilt, kopiert wird, werden die anderen Kopien der Datei möglicherweise auch verschlüsselt.

  Wenn eine unverschlüsselte Datei an einen verschlüsselten Speicherort kopiert wird, wird die Datei zur internen Liste des Tools hinzugefügt. Wenn die zweite Kopie erstellt wird, findet das Verschlüsselungstool den Dateiname in seiner Liste und verschlüsselt auch die zweite Kopie.
- **Nach dem Zugriff auf eine verschlüsselte Datei eine Datei mit dem gleichen Namen erstellen**

  Wird kurz nach dem Öffnen einer Datei eine Datei mit dem gleichen Namen erstellt, wird die neu erstellte Datei mit dem gleichen Schlüssel wie die zuerst geöffnete Datei verschlüsselt.

  **Note:** Dies gilt nur dann, wenn für das Lesen der verschlüsselten Datei und das Erstellen einer neuen Datei die gleiche Anwendung/der gleiche Thread verwendet wird.

  Zum Beispiel: Klicken Sie im Windows Explorer mit der rechten Maustaste in einem Ordner mit Verschlüsselungsregel und wählen Sie **Neu** > **Neues Textdokument**. Klicken Sie anschließend mit der rechten Maustaste in einem Ordner ohne Verschlüsselungsregel und wählen Sie **Neu** > Neues Textdokument. Die zweite Datei wird ebenfalls verschlüsselt.

### Dateien werden nicht verschlüsselt

- **Von einer Datei werden mehrere Kopien angelegt**

  Werden Kopien von einer verschlüsselten Datei im gleichen Ordner wie die ursprüngliche Datei erstellt, so werden diese Kopien nicht verschlüsselt. Da die erstellten Kopien unterschiedliche Dateinamen haben (zum Beispiel doc.txt im Gegensatz zu doc-Kopie.txt), schlägt der Abgleich des Dateinamens fehl und werden daher nicht mit der persistenten Verschlüsselung verschlüsselt.

## 2.1.8 Client-API und Verschlüsselungs-Tags für DLP-Produkte

Identifiziert ein Data Loss Prevention (DLP) Produkt Dateien, die verschlüsselt werden sollen, so kann es die SafeGuard LAN Crypt Client-API verwenden, um die Dateien zu verschlüsseln. Sie können unter **SafeGuard LAN Crypt Administration** unterschiedliche Verschlüsselungs-Tags definieren, die den zu verwendenden SafeGuard LAN Crypt-Schlüssel angeben. Die Client-API kann diese vordefinierten Verschlüsselungs-Tags verwenden, um bestimmte Schlüssel auf unterschiedliche Inhalte anzuwenden. Zum Beispiel kann der Verschlüsselungs-Tag **<CONFIDENTIAL>** verwendet werden, um alle Dateien zu verschlüsseln, die von Ihrem DLP-Produkt als vertraulich kategorisiert sind.

# 2.2 Aktivieren und Deaktivieren der transparenten Verschlüsselung

Wird die transparente Verschlüsselung im SafeGuard LAN Crypt Benutzermenü deaktiviert, werden Dateien, auf die nach der Deaktivierung zugegriffen wird, nicht mehr automatisch ver- bzw. entschlüsselt. Neu erzeugte Dateien bleiben ebenfalls unverschlüsselt, auch wenn für diese eine Verschlüsselungsregel im Verschlüsselungsprofil des Benutzers vorhanden ist.

**Note:** Die Deaktivierung der transparenten Verschlüsselung wirkt sich beim Kopieren/Verschieben von verschlüsselten Dateien in ein Verzeichnis ohne Verschlüsselungsregeln aus, zum Beispiel, wenn verschlüsselte Dateien an eine E-Mail

angehängt oder auf CD kopiert werden sollen. Diese Dateien werden nun entschlüsselt, wenn sie in ein Verzeichnis ohne Verschlüsselungsregeln kopiert oder verschoben werden.

Wenn Sie die Funktion **Persistente Verschlüsselung** aktiviert haben, bleiben verschlüsselte Dateien auch dann verschlüsselt, wenn sie in einen Ordner ohne Verschlüsselungsregel verschoben werden. Wenn Sie **Persistente Verschlüsselung** verwenden, ist es nicht notwendig, vorher die transparente Verschlüsselung zu deaktivieren. Die **Persistente Verschlüsselung** sorgt dafür, dass Dateien auch dann verschlüsselt bleiben, wenn sie versehentlich in ein anderes Verzeichnis verschoben wurden oder wenn der Benutzer vergessen hat, die Verschlüsselung vor dem Verschieben bzw. Kopieren zu deaktivieren. Sie müssen den Computer neu starten, damit die Änderungen der **persistenten Verschlüsselung** (aktiv oder nicht aktiv) Wirkung zeigen.

**Note:** Ist die **Persistente Verschlüsselung** aktiv und ein Benutzer verschiebt oder kopiert eine Datei in einen Ordner, für den eine Ignorieren-Regel oder Ausnahmeregel gilt, so wird die Datei dadurch entschlüsselt.

## 2.3 Transparente Verschlüsselung und Komprimierungsprogramme

Komprimierungsprogramme öffnen die Dateien, lesen den Inhalt und komprimieren ihn. Wenn die transparente Ent-/Verschlüsselung aktiviert ist, erhalten diese Programme die entschlüsselten Dateien und diese werden dann komprimiert. Die Dateien im resultierenden Archiv sind nicht mehr verschlüsselt.

Wird das Archiv in einem Verzeichnis gespeichert, für das keine Verschlüsselungsregel existiert, werden alle Dateien entschlüsselt.

Wenn die **persistente Verschlüsselung** aktiviert ist, werden die Dateien nicht in verschlüsselter Form komprimiert.

Um sicherzustellen, dass Dateien von Komprimierungsprogrammen verschlüsselt komprimiert werden, muss die transparente Verschlüsselung während der Verwendung solcher Programme deaktiviert werden.

Alternativ dazu kann der Security Officer Komprimierungsprogramme als Unberücksichtigte Anwendung definieren um sicherzustellen, dass Dateien verschlüsselt komprimiert werden.

## 2.4 Initialverschlüsselung und explizite Verschlüsselung

Nach der Installation von SafeGuard LAN Crypt müssen Sie eine Initialverschlüsselung durchführen. Dabei werden alle Dateien entsprechend dem geladenen Verschlüsselungsprofil verschlüsselt. Die Initialverschlüsselung kann über eine der folgenden Methoden gestartet werden:

- SafeGuard LAN Crypt Taskleistensymbol, siehe Benutzerprogramm *(page 20)*
- SafeGuard LAN Crypt Explorer-Erweiterungen, siehe Explorer-Erweiterungen *(page 22)*
- **sglcinit.exe**-Tool, das auch den Unattended-Modus unterstützt Initialverschlüsselung im Unattended-Modus (ohne Benutzerinteraktion) *(page 14)*

Neben der Initialverschlüsselung von ganzen Verzeichnissen ist mit dem Kommandozeilen-Tool **sglcinit.exe** und mit der Explorer-Erweiterung auch die Ver-, Ent- und Umschlüsselung einzelner Dateien möglich.

Die explizite Ver-, Ent- oder Umschlüsselung kann in folgenden Fällen erforderlich sein:

- Wenn sich unverschlüsselte Dateien in Verzeichnissen befinden, für die eine Verschlüsselungsregel existiert.
- Wenn sich verschlüsselte Dateien in Verzeichnissen befinden, für die keine Verschlüsselungsregel existiert.
- Wenn Dateien in verschlüsselten Verzeichnissen mit einem falschen Schlüssel verschlüsselt sind.
- Wenn sich die Verschlüsselungsregeln im Verschlüsselungsprofil geändert haben.
- Wenn Dateien mit mehreren Schlüsseln verschlüsselt wurden.

# 2.4.1 Assistent zur Initialverschlüsselung

Das Tool für die Initialverschlüsselung, **sglcinit.exe**, verfügt über einen Assistenten mit einer grafischen Oberfläche. Dieser Assistent unterstützt

- das Ver-, Ent- und Umschlüsseln von Dateien und
- das Prüfen des Verschlüsselungsstatus von Dateien.

Sie können den Assistenten starten indem Sie

- auf das Taskleistensymbol klicken oder
- Start/Programme/Sophos/SafeGuard LAN Crypt/Initialverschlüsselung wählen oder
- ihn aus dem Windows-Startbildschirm starten oder
- auf die Datei sglcinit.exe Im SafeGuard LAN Crypt-Programmverzeichnis doppelklicken.

**Note:** Die Ver-, Ent- bzw. Umschlüsselung wird immer entsprechend einem Verschlüsselungsprofil vorgenommen. Daher muss ein Verschlüsselungsprofil geladen sein.

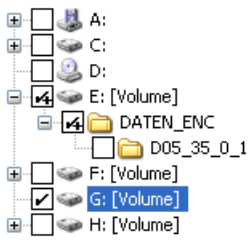
## 2.4.1.1 Initialverschlüsselung durchführen

1. Starten Sie den Assistenten, siehe Benutzermenü *(page 20)*.
2. Wählen Sie die Option Initialverschlüsselung durchführen in Schritt 1/5.
3. Klicken Sie auf **Weiter**.
4. Legen Sie nun in Schritt 2/5 fest, wie mit den Dateien verfahren werden sollen.
   a. **Dateien entsprechend den Regeln verschlüsseln**
   Wenn Sie diese Option auswählen, werden die Dateien entsprechend den Regeln im Profil des Benutzers verschlüsselt (Standardeinstellung). Sollten bereits verschlüsselte Dateien gefunden werden, werden diese ignoriert.
   b. **Dateien entsprechend den Regeln umschlüsseln**
   Wenn Sie diese Option auswählen, werden (auch) Dateien, die mit einem anderen Schlüssel als im Profil festgelegt verschlüsselt sind, entschlüsselt und mit dem korrekten Schlüssel verschlüsselt.

   **Note:** Voraussetzung dafür ist, dass der Schlüssel, mit dem die Datei(en) verschlüsselt wurden, im Profil des Benutzers enthalten ist.

   Diese Option ermöglicht auch das Umschlüsseln von Dateien, die mit SafeGuard Enterprise Data Exchange verschlüsselt wurden, für die aber keine SafeGuard Enterprise Verschlüsselungsregel mehr gilt. Solche Dateien liegen zum Beispiel vor, wenn die SafeGuard Enterprise Verschlüsselungsregel aufgehoben wurde, die Dateien aber nicht explizit entschlüsselt wurden. In diesem Fall können Sie die Dateien mithilfe des Assistenten zur Initialverschlüsselung umschlüsseln. So werden die Dateien entsprechend den SafeGuard LAN Crypt Verschlüsselungsregeln umgeschlüsselt.

5. Klicken Sie auf **Weiter**.
6. Legen Sie nun über die Verzeichnisstruktur in Schritt 3/5 fest, welche Ordner verschlüsselt/umgeschlüsselt werden sollen.



Ausgewählte Ordner werden mit einem Häkchen markiert. Ein + Zeichen bei einem Ordner zeigt an, dass sich darin Unterordner befinden, die nicht bearbeitet werden, in denen also keine Verschlüsselung/Umschlüsselung der Dateien durchgeführt wird.

Klicken Sie auf **Profilregeln**, um automatisch alle Verzeichnisse zu markieren, für die Verschlüsselungsregeln im Profil des Benutzers existieren.

Klicken Sie auf **Erweitert**, um weitere Einstellungen für die Initialverschlüsselung anzuzeigen.

**Note:** Welche Einstellung vom Benutzer geändert werden können, ist von der Konfiguration des SafeGuard LAN Crypt Clients abhängig. Der Security Officer nimmt die Konfiguration zentral vor.

- **EFS verschlüsselte Dateien wenn notwendig entschlüsseln**

  Wählen Sie diese Option, um EFS verschlüsselte Dateien zu entschlüsseln und umzuschlüsseln. Beachten Sie, dass eine entsprechende Verschlüsselungsregel gelten muss.

  Wenn Sie diese Option nicht auswählen, werden EFS verschlüsselte Dateien vom Assistenten zur Initialverschlüsselung ignoriert. Sie werden nicht von SafeGuard LAN Crypt umgeschlüsselt, auch wenn für sie eine Verschlüsselungsregel besteht.

- **NTFS-komprimierte Dateien wenn notwendig dekomprimieren**

  Wählen Sie diese Option, um NTFS-komprimierte Dateien zu dekomprimieren und zu verschlüsseln. Beachten Sie, dass eine entsprechende Verschlüsselungsregel gelten muss.

  Wenn Sie diese Option nicht auswählen, werden NTFS-komprimierte Dateien vom Assistenten zur Initialverschlüsselung ignoriert. Sie werden nicht verschlüsselt, auch wenn für sie eine Verschlüsselungsregel besteht.

- **Dateien, die wiederholt mit mehreren Schlüssel verschlüsselt wurden, entschlüsseln/umschlüsseln**

  Wählen Sie diese Option, um Dateien umzuschlüsseln, die mit mehreren Schlüsseln verschlüsselt wurden. Die Dateien sind dann mit nur einem Schlüssel verschlüsselt. Beachten Sie, dass eine entsprechende Verschlüsselungsregel gelten muss.

  Diese Option ist nur verfügbar, wenn in Schritt 2 / 5 **Dateien entsprechend den Regeln verschlüsseln** oder **Dateien entsprechend den Regeln umschlüsseln** ausgewählt wurde. Ansonsten ist diese Option ausgegraut.

- **Nur folgende Dateien einschließen:**

  Wählen Sie hier die Dateitypen (.txt, .doc usw.) die bei der Initialverschlüsselung berücksichtigt werden sollen. Diese Einstellung wirkt sich nur auf Dateien aus, für die eine Verschlüsselungsregel existiert. Befinden sich auch noch andere Dateien in einem Verzeichnis, werden sie bei der Initialverschlüsselung nicht berücksichtigt. Sie werden erst verschlüsselt, wenn sie vom Benutzer geöffnet und wieder abgespeichert werden. Zur Angabe mehrerer Dateitypen muss eine durch Strichpunkte getrennte Liste verwendet werden.

7. Klicken Sie auf **Weiter**.

8. Legen Sie nun in Schritt 4/5 fest, welche Dateien im Bericht über die Initialverschlüsselung enthalten sein sollen. Für den Bericht kann der Benutzer zwischen folgenden Optionen wählen:

   a. **Nur Fehler berichten**
   Der Statusbericht enthält nur Dateien, bei denen während der Verschlüsselung Fehler aufgetreten sind.

   b. **Geänderte Dateien und Fehler berichten**
   Der Statusbericht enthält alle Dateien, die geändert wurden oder bei denen während der Verschlüsselung Fehler aufgetreten sind.

   c. **Alle Dateien berichten**
   Der Statusbericht enthält alle Dateien.

9. Klicken Sie auf **Weiter**.
   In Schritt 5/5 wird das **Ergebnis** der Verschlüsselung, der **Schlüsselname** des verwendeten Schlüssels und der Verschlüsselungsalgorithmus angezeigt.

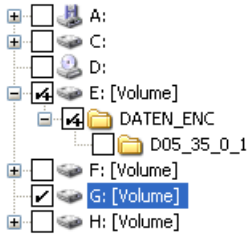
   Ist bei einer bestimmten Datei die Verschlüsselung fehlgeschlagen, können Sie die Verschlüsselung über die Schaltfläche **Wiederholen** erneut starten.

Die Ergebnisse lassen sich per Mausklick auf die Spaltenüberschrift alphabetisch sortieren. Darüber hinaus können Sie den Statusbericht als XML-Datei an einem gewünschten Ort speichern (Schaltfläche **Exportieren**). Anhand des Statusreports können Sie später jene Dateien, bei denen die Verschlüsselung fehlgeschlagen ist, erneut verschlüsseln.

10. Klicken Sie auf **Beenden**.
    Der Assistent wird geschlossen.

### 2.4.1.2 Verschlüsselungsstatus prüfen

1. Starten Sie den Assistenten.
2. Wählen Sie in Schritt 1 / 5 die Option **Initialverschlüsselung durchführen**.
3. Klicken Sie auf **Weiter**.
4. Legen Sie in Schritt 2 / 5 fest, welche Ordner geprüft werden sollen.




5. Wählen Sie Ordner aus, indem Sie sie markieren.

   Ein + Zeichen bei einem Ordner zeigt an, dass sich darin Unterordner befinden, die nicht bearbeitet werden, in denen also keine Überprüfung des Verschlüsselungsstatus der Dateien durchgeführt wird.

   Klicken Sie auf **Profilregeln**, um automatisch alle Verzeichnisse zu markieren, für die Verschlüsselungsregeln im Profil des Benutzers existieren.

   Klicken Sie auf **Erweitert**, um die Prüfung auf bestimmte Dateitypen einzuschränken:
   - **Nur folgende Dateien einschließen**:

     Wenn Sie hier bestimmte Dateitypen angeben (z.B. .txt, .doc), so werden nur diese Dateitypen überprüft.

     Befinden sich auch noch andere Dateien eines Typs, der nicht hier angegeben wird, in einem Verzeichnis, werden sie nicht berücksichtigt. Zur Angabe mehrerer Dateitypen muss eine durch Strichpunkte getrennte Liste verwendet werden.

6. Klicken Sie auf **Weiter**.

   In Schritt 3 / 5 wird das **Ergebnis** der Prüfung, der **Schlüsselname** des verwendeten Schlüssels und der Verschlüsselungsalgorithmus angezeigt.

   Die Ergebnisse lassen sich per Mausklick auf die Spaltenüberschrift alphabetisch sortieren.

   Darüber hinaus können Sie den Statusbericht als XML-Datei an einem gewünschten Ort speichern (Schaltfläche **Exportieren**).

7. Klicken Sie auf **Beenden**.
   Der Assistent wird geschlossen.

### 2.4.1.3 Dateien entschlüsseln

Dateien, die mit SafeGuard LAN Crypt verschlüsselt wurden, können entschlüsselt werden, wenn keine Verschlüsselungsregel (mehr) für sie gilt. Wurde eine erneute Initialverschlüsselung notwendig, zum Beispiel weil sich Verschlüsselungsregeln im Profil des Benutzers geändert haben, können Dateien, für die es nun keine Verschlüsselungsregeln mehr gibt, über diesen Assistenten entschlüsselt werden.

Um Dateien zu entschlüsseln, wählen Sie im Assistenten zuerst **Initialverschlüsselung durchführen** (Schritt 1/5), dann **Entschlüsselung** > **Dateien mit den ausgewählten Schlüsseln entschlüsseln** (Schritt 2/5).

Anschließend können Sie die Schlüssel auswählen. Nur die Dateien, die mit den ausgewählten Schlüsseln verschlüsselt wurden, werden entschlüsselt. Die Dateien werden jedoch nur dann entschlüsselt, wenn für sie keine Verschlüsselungsregel mehr gilt.

**Note:** SafeGuard LAN Crypt entschlüsselt ausschließlich Dateien, für die keine Verschlüsselungsregel gilt.

### Beispiel:

Der Assistent zur Initialverschlüsselung wird gestartet, weil Änderungen im Benutzerprofil vorgenommen wurden. Um sicherzustellen, dass nach dem Beenden des Assistenten zur Initialverschlüsselung alle Dateien den gewünschten Verschlüsselungsstatus haben, gehen Sie wie folgt vor:

1. Aktivieren Sie **Dateien entsprechend den Regeln verschlüsseln**.

   Alle Dateien werden gemäß den neuen Verschlüsselungsregeln verschlüsselt.
2. Aktivieren Sie **Dateien entsprechend den Regeln umschlüsseln**.

   Müssen Dateien nach den neuen Regeln mit einem anderen Schlüssel verschlüsselt werden, werden sie umgeschlüsselt.
3. Aktivieren Sie **Dateien mit den ausgewählten Schlüsseln entschlüsseln** und wählen Sie dann alle Schlüssel aus.

   Verschlüsselte Dateien, für die es nun keine Verschlüsselungsregel mehr gibt, werden entschlüsselt. SafeGuard LAN Crypt entschlüsselt ausschließlich Dateien, für die keine Verschlüsselungsregel gilt. Die Auswahl aller Schlüssel ist daher vollkommen unproblematisch.

Alle Dateien besitzen nach dem erfolgreichen Beenden des Assistenten den korrekten Verschlüsselungsstatus.

Das explizite Entschlüsseln von Dateien kann dann wichtig sein, wenn die **persistente Verschlüsselung** aktiviert ist. In diesem Fall werden Dateien nicht automatisch entschlüsselt, wenn sie aus einem Verzeichnis, für das eine Verschlüsselungsregel gilt, in ein Verzeichnis ohne Verschlüsselungsregel kopiert/verschoben werden.

## *2.4.2 Initialverschlüsselung im Unattended-Modus (ohne Benutzerinteraktion)*

Wenn **sglcinit.exe** im Unattended-Modus ausgeführt werden soll, müssen Sie das Tool mit bestimmten Parametern über die Kommandozeile aus dem Verzeichnis heraus aufgerufen werden, in dem es sich befindet (z. B. C:\Programme\Sophos \SafeGuard LAN Crypt\).

### Kommandozeilen-Syntax:

```
SGLCInit <startpath | %Profile>[/S]
{-DIgnoreDirectory}[/Tv][/Te][/Tr][/Td]
[/Tdk {GUID}][/Dc][/De][/Dm][+FFiletype][/V1|/V2|/V3|/V4] [/X]
[/LLogfile]
```

### Parameter:

- **Start path**

  Gibt entweder eine einzelne Datei an, die ver-, ent- oder umgeschlüsselt werden soll (z. B. C:\Daten\Vertrieb.doc), oder ein Verzeichnis, in dem die Ver-, Ent- oder Umschlüsselung durchgeführt werden soll (z. B. D:\Daten ). Unterverzeichnisse werden standardmäßig nicht miteinbezogen!
- **%Profile**

  Verarbeitet alle Regeln mit einem absoluten Pfad im geladenen Verschlüsselungsprofil. Ver-/entschlüsselt bzw. schlüsselt die Dateien wenn notwendig um.

  **Note:** Zum Entschlüsseln muss für die entsprechenden Dateien im Profil eine EXCLUDE Regel existieren.
- **/s**

Inklusive aller Unterverzeichnisse ab dem Startpfad.

- **/h** oder **/?**

  Öffnet ein Hilfefenster zur Syntax von sglcinit.exe.

- **-DIgnoreDirectory**

  Ignoriert dieses Verzeichnis.

- **/Tv**

  Task-Modus: v = Zeigt den Verschlüsselungsstatus der Dateien an.

- **/Te**

  Task-Modus: e = Verschlüsselt, falls notwendig, Dateien gemäß ihrem Verschlüsselungsprofil.

- **/Tr**

  Task-Modus: r = Schlüsselt, falls notwendig, Dateien gemäß ihrem Verschlüsselungsprofil um.

- **/Td**

  Task-Modus: d = Entschlüsselt, falls notwendig, Dateien gemäß ihrem Verschlüsselungsprofil.

- /Tdk

  Task-Modus: dk = Entschlüsselt die Dateien, die mit den angegebenen Schlüsseln verschlüsselt sind. Sie müssen die GUID für die Schlüssel angeben.

  **Note:** Alle Task Modus-Parameter können in einem Befehlsaufruf zusammen genutzt werden.

- **/Dc**

  Diese Option dekomprimiert NTFS komprimierte Dateien und verschlüsselt sie anschließend. Ist diese Option nicht gesetzt, werden NTFS komprimierte Dateien ignoriert.

- **/De**

  Diese Option entschlüsselt EFS verschlüsselte Dateien und verschlüsselt sie anschließend. Ist diese Option nicht gesetzt, werden EFS verschlüsselte Dateien ignoriert.

- **/Dm**

  Diese Option entschlüsselt mehrfach verschlüsselte Dateien und verschlüsselt sie anschließend neu. Die Dateien sind dann mit nur einem Schlüssel verschlüsselt.

- **+Ffile type**

  Wenn Sie mit dieser Option Dateitypen angeben (z. B. +Ftxt+Fdoc), so werden ausschließlich Dateien vom angegebenen Typ bearbeitet. Diese Einstellung wirkt sich nur auf Dateien aus, für die eine Verschlüsselungsregel existiert.

  Enthält ein Verzeichnis noch Dateien eines Typs, der nicht mit dieser Option angegeben wird, werden sie bei der Initialverschlüsselung nicht berücksichtigt. Sie werden erst verschlüsselt, wenn sie vom Benutzer geöffnet und wieder abgespeichert werden.

- **/V0**

  Verbose Modus 0: Kein Reporting (Bericht).

- **/V1**

  Verbose Modus 1: Listet Fehlermeldungen auf.

- **/V2**

  Verbose Modus 2: Listet geänderte Dateien auf.

- **/V3**

  Verbose Modus 3: Listet alle Dateien auf.

- **/V4**

  Verbose Modus 4: Listet unverschlüsselte Dateien auf.

- **/E**

  Bei Fehler abbrechen.

- **/X**

  Initialverschlüsselung ohne Fenster ausführen.

- **/LLogfile**

  Schreibt Ausgabe in die angegebene Datei.

  **Note:** Der Parameter /Td kann nur dann mit %Profile sinnvoll kombiniert werden, wenn die zu entschlüsselnden Dateien im Profil über eine Ausnahmeregel aufgeführt sind. Andernfalls muss /Td mit Startpfad kombiniert werden.

```
sglcinit.exe %PROFILE -DC:\ignore /S /Te /Tdk {1234ABCD-1234-1234-1234-1234ABCD}
 {5678EFGH-5678-5678-5678-5678EFGH} /V1 /LC:\logfile.xml
```

**sglcinit.exe D:\Daten /S /V4**

Listet alle Klartextdateien in D:\Daten und dessen Unterverzeichnissen auf.

# 3 Richtlinien

## 3.1 Zertifikate

Bevor ein Benutzer Zugriff auf sein Verschlüsselungsprofil hat, muss das entsprechende Zertifikat auf seinem Computer vorhanden sein. Der Security Officer muss diese Zertifikate an die Benutzer verteilen. Dann importieren Benutzer das Zertifikat auf ihren Computern. Sind die Zertifikate bereits bei der ersten Anmeldung verfügbar, läuft der gesamte Vorgang ohne Benutzerinteraktion ab.

SafeGuard LAN Crypt bietet die Möglichkeit, die Zertifikate beim ersten Laden des Verschlüsselungsprofils automatisch zu importieren. In diesem Fall wird das System vom Security Officer so konfiguriert, dass SafeGuard LAN Crypt bei der ersten Anmeldung auch eine Zertifikatsdatei findet und dann den Importvorgang automatisch startet. Der Benutzer wird einmal aufgefordert, die PIN für den Import der PKCS#12 Schlüsseldatei einzugeben.

**Note:** Der Security Officer muss den Benutzern die PIN für den automatischen Import der Zertifikate mitteilen.

Das Zertifikat wird bei jedem Laden des Verschlüsselungsprofils geprüft. Wird ein gültiges Zertifikat gefunden, wird der Benutzer an SafeGuard LAN Crypt angemeldet. Ist kein gültiges Zertifikat vorhanden, kann der Benutzer nicht mit den verschlüsselten Daten arbeiten.

**Note:** Wenn die Anmeldung an SafeGuard LAN Crypt fehlschlägt, erhalten Benutzer eine Fehlermeldung mit einem Hinweis, warum die Anmeldung nicht möglich war.

Die spezifischen Verschlüsselungsregeln in den SafeGuard LAN Crypt Verschlüsselungsprofilen ermöglichen dem Benutzer den Zugriff auf verschlüsselte Daten. Die Regeln definieren, welche Dateien in welchen Verzeichnissen mit welchem Schlüssel zu verschlüsseln sind. Es muss nur ein Verschlüsselungsprofil eines Benutzers geladen werden, dann finden Verschlüsselung und Entschlüsselung im Hintergrund (transparent) statt. Der Benutzer bemerkt die durchgeführten Verschlüsselungs-/Entschlüsselungsvorgänge nicht.

**Note:** CA Zertifikate werden nur dann als korrekt akzeptiert, wenn sie unter „Trusted Root Certification Authorities“ liegen. Die SafeGuard LAN Crypt Software importiert jedoch CA Zertifikate, die in PKCS#12 Schlüsseldateien enthalten sein können, gemeinsam mit den Benutzerzertifikaten in den Ordner „Personal - Certificates“. Um Fehlermeldungen zu vermeiden, müssen die CA Zertifikate manuell nach „Trusted Root Certification Authorities“ verschoben werden.

## 3.2 Laden der Richtliniendatei

### Standardverhalten von SafeGuard LAN Crypt

Wenn sich ein Benutzer an Windows anmeldet, wird zuerst sein (zwischen)gespeichertes Benutzerprofil geladen. Danach überprüft SafeGuard LAN Crypt, ob es eine neue Richtliniendatei für den Benutzer gibt, indem es eine Verbindung zum festgelegten Speicherort für Richtliniendateien (Netzwerklaufwerk oder Webserver über http/https) aufbaut. Wird eine neuere Richtliniendatei gefunden, wird das zwischengespeicherte Benutzerprofil aktualisiert.

Der Benutzer kann bereits mit verschlüsselten Daten arbeiten während SafeGuard LAN Crypt überprüft, ob es eine neuere Version der Richtliniendatei gibt. Ist das angegebene Netzwerklaufwerk nicht erreichbar, arbeitet der Benutzer solange mit dem zwischengespeicherten Benutzerprofil, bis dieses aktualisiert werden kann.

**Note:** SafeGuard LAN Crypt verifiziert die Zertifikate des Benutzers und des (Master) Security Officers. Enthält ein Zertifikat einen "CRL Distribution Point“ und es ist keine gültige CRL auf dem System verfügbar, versucht Windows, eine CRL von der angegebenen Adresse zu importieren. Ist eine Firewall aktiv, wird unter Umständen eine Meldung angezeigt, dass ein Programm (loadprof.exe) versucht, eine Verbindung zum Internet herzustellen. In manchen Fällen kann auch das Laden des Benutzerprofils diese Meldung auslösen.

### Durch Security Officers festgelegtes Verhalten

Ein Security Officer kann das Standardverhalten durch zentrale Einstellungen beeinflussen. Security Officer können festlegen, wie lange die zwischengespeicherte Richtlinie auf den Client-Computern gültig ist. Darüber hinaus können Sie

die Intervalle für die Aktualisierung der Richtliniendateien festlegen. Die Einstellungen des Security Officers werden in der Registerkarte **Profil** des Dialogs **Clientstatus** angezeigt, siehe Der Dialog Clientstatus *(page 21)*.

Innerhalb des angegebenen Zeitraums ist die Richtliniendatei auf dem Client gültig und der Benutzer hat Zugriff auf verschlüsselte Daten, auch wenn keine Verbindung zum Speicherort der Richtliniendatei besteht.

Läuft die angegebene Dauer ab, versucht SafeGuard LAN Crypt erneut, die Richtliniendatei vom Netzwerklaufwerk zu laden, um sie zu aktualisieren. Ist dies nicht möglich, wird die Richtliniendatei entladen. Der Benutzer hat keinen Zugriff mehr auf verschlüsselte Daten.

Erst wenn wieder eine gültige Richtliniendatei zur Verfügung steht (z. B. bei der nächsten Anmeldung mit einer Verbindung zum Speicherort der Richtliniendateien für die Clients), wird die Richtliniendatei aktualisiert und geladen. Der Benutzer hat wieder Zugriff auf verschlüsselte Daten. Der Zähler für die Dauer der Zwischenspeicherung wird zurückgesetzt.

Die Angabe der Dauer der Zwischenspeicherung kann einerseits sicherstellen, dass die Client-Computer in regelmäßigen Intervallen mit aktuellen Richtliniendateien versorgt werden und die Benutzer immer aktuelle Richtlinien verwenden. Andererseits kann durch die Beschränkung der Gültigkeitsdauer verhindert werden, dass Benutzer mit Richtliniendateien unbeschränkt lange weiterarbeiten können. Ist diese Option auf **nicht konfiguriert gesetzt**, können Benutzer mit einer zwischengespeicherten Version der Richtliniendatei unbeschränkt lange arbeiten.

In folgenden Fällen wird der Zähler für die erlaubte Dauer der Zwischenspeicherung zurückgesetzt:

- Der Speicherort der Richtliniendateien ist erreichbar und es wurde eine gültige Richtliniendatei auf den Client übertragen (z. B. bei der Anmeldung des Benutzers, oder ausgelöst durch ein definiertes Aktualisierungsintervall), diese ist aber nicht neuer als die bestehende.
- Eine neue Richtliniendatei ist verfügbar und wurde erfolgreich geladen.

In folgenden Fällen wird der Zähler für die erlaubte Dauer der Zwischenspeicherung NICHT zurückgesetzt:

- Der Client-Computer versucht, eine neue Richtliniendatei zu erhalten. Der Speicherort der Richtliniendateien ist jedoch nicht erreichbar.
- Eine neue Richtliniendatei wurde übertragen. Sie konnte aber aufgrund eines Fehlers nicht geladen werden.
- Eine neue Richtliniendatei ist verfügbar. Diese Richtliniendatei erfordert aber ein neues Zertifikat. Der Benutzer besitzt dieses Zertifikat nicht oder kann es nicht laden.

Schlägt die Aktualisierung der Richtliniendatei fehl, wird auf dem Client-Computer der Ablaufzeitpunkt der zwischengespeicherten Richtliniendatei in Form einer Sprechblasen-Hilfe angezeigt. Der Benutzer kann dann eine manuelle Aktualisierung über das SafeGuard LAN Crypt Taskleistensymbol anstoßen, siehe Benutzermenü *(page 20)*.

### Keine Zwischenspeicherung der Richtliniendatei

Ein Security Officer kann festlegen, dass die Richtliniendatei nicht zwischengespeichert wird. Das bedeutet, dass der Benutzer sein Benutzerprofil bei der Anmeldung erhält, wenn der Speicherort der Richtliniendatei erreichbar ist. Ist dieser nicht erreichbar oder tritt ein Fehler beim Laden des Profils auf, kann der Benutzer nicht auf verschlüsselte Daten zugreifen.

## *3.3 Anmeldung an SafeGuard LAN Crypt*

SafeGuard LAN Crypt Verschlüsselungsprofile werden von einem Security Officer entsprechend der firmenweiten Sicherheitspolitik erstellt und in Richtliniendateien gespeichert. Ein Verschlüsselungsprofil kann nur geladen werden, wenn der Benutzer über das richtige Zertifikat verfügt.

Der Pfad der Richtliniendatei wird vom Systemadministrator in die Registrierung der Client-Rechner eingetragen. Wenn sich ein Benutzer an SafeGuard LAN Crypt anmeldet, wird das Verschlüsselungsprofil, das in den Richtliniendateien gespeichert ist, auf den Client-Rechner geladen. SafeGuard LAN Crypt lädt die Richtliniendateien aus dem angegebenen Verzeichnis und prüft anhand des Benutzerzertifikats, ob der Benutzer berechtigt ist, es zu laden.

### Anmeldung mit Token

Benutzer können für die Anmeldung an SafeGuard LAN Crypt auch einen Token verwenden. Voraussetzung dafür ist, dass das SafeGuard LAN Crypt Benutzerzertifikat auf dem Token gespeichert ist. Wird das Benutzerzertifikat auf einem mit dem System verbundenen Token gefunden, wird die Anmeldung durchgeführt.

Werden Token zur Anmeldung verwendet, kann es vorkommen, dass SafeGuard LAN Crypt eine Richtliniendatei zu laden versucht, bevor der Token vom Betriebssystem korrekt identifiziert wurde. In diesem Fall wird eine Meldung angezeigt, dass das Benutzerzertifikat nicht gefunden wurde, obwohl der Token bereits mit dem System verbunden ist.

Dann muss der Benutzer die Richtliniendatei manuell über das Benutzerprogramm in der Task-Leiste > **Verschlüsselungsregeln laden** laden. Dadurch wird der Token identifiziert und die Anmeldung wird durchgeführt. Um dies zu umgehen, können Sie in der **SafeGuard LAN Crypt Konfiguration** (Einstellung **Verzögerung beim Laden des Profils**) eine Verzögerung angeben.

# 4 Benutzerprogramm

Ein Schlüssel-Symbol in der Taskleiste zeigt den Status von SafeGuard LAN Crypt an.

- **Grün** bedeutet:

  Verschlüsselungsregeln geladen, transparente Verschlüsselung aktiviert.
- **Gelb** bedeutet:

  Verschlüsselungsregeln geladen, transparente Verschlüsselung deaktiviert.
- **Rot** bedeutet:

  Kein Profil geladen.

## *4.1 Benutzermenü*

Ein Rechtsklick auf das Schlüssel-Symbol öffnet das SafeGuard LAN Crypt Benutzermenü mit folgenden Einträgen:

- **Verschlüsselungsregeln laden/Verschlüsselungsregeln aktualisieren**
- **Lösche Verschlüsselungsregeln**
- **Verschlüsselung deaktivieren/aktivieren**
- **Profil anzeigen**
- **Clientstatus**
- **Initialverschlüsselung**
- **Schließen**
- **Info**

**Note:** Welche Menüeinträge tatsächlich verfügbar sind, ist von der Konfiguration des SafeGuard LAN Crypt Clients abhängig. Der Security Officer nimmt die Konfiguration zentral vor.

- **Verschlüsselungsregeln laden/Verschlüsselungsregeln aktualisieren**

  Mit diesem Befehl werden die aktuell gültigen Verschlüsselungsrichtlinien geladen. Dies ist dann wichtig, wenn im laufenden Betrieb das Verschlüsselungsprofil geändert wurde
- **Lösche Verschlüsselungsregeln**

  Diese Option verhindert den Zugriff auf verschlüsselte Daten. Dies stellt eine Sicherheitsfunktion dar, die die verschlüsselten Daten auf dem Rechner vor unbefugtem Zugriff schützt, wenn der Arbeitsplatz kurzfristig verlassen werden muss. Die Verwendung des privaten Schlüssels muss durch ein Passworts geschützt sein. Ansonsten könnte das Profil durch den Befehl **Verschlüsselungsregeln laden** einfach wieder geladen werden.
- **Verschlüsselung deaktivieren/aktivieren**

  Schaltet die transparente Verschlüsselung ein bzw. aus.

  Das Ausschalten der transparenten Verschlüsselung ist von Bedeutung, wenn Dateien verschlüsselt bleiben sollen, die von einem verschlüsselten Verzeichnis an einen Ort kopiert/verschoben werden, für den keine Verschlüsselungsregel existiert. Bei aktivierter Verschlüsselung würden diese Dateien entschlüsselt werden, wenn Sie in diesen Ordner kopiert werden.

  Wenn zum Beispiel eine verschlüsselte Datei an eine E-Mail angehängt wird, würde sie bei aktivierter Verschlüsselung automatisch entschlüsselt werden. Ist die transparente Verschlüsselung deaktiviert, können verschlüsselte Dateien als Anhang von E-Mails versendet werden.

**Note:** Wenn vom Administrator die Funktion **Persistente Verschlüsselung** aktiviert wurde, bleiben verschlüsselte Dateien auch dann verschlüsselt, wenn sie an einen Ort kopiert oder verschoben werden, für den keine Verschlüsselungsregel existiert.

- **Profil anzeigen**

  Zeigt auf zwei Registerkarten die Verschlüsselungsregeln und die in den Verschlüsselungsinformationen enthaltenen Schlüssel an.

  Die Registerkarte Aktive Verschlüsselungsregeln listet die für den angemeldeten Benutzer gültigen Regeln auf. Der Benutzer kann zudem die Optionen 'Ignorieren Regeln', 'Ausnahmeregeln anzeigen' und 'Verschlüsselungs-Attribute anzeigen' wählen, um auch diese Verschlüsselungsregeln zu sehen.

  Die Registerkarte Verfügbare Schlüssel zeigt alle für den aktuellen Benutzer verfügbaren Schlüssel an.

- **Clientstatus**

  Die Funktion **Clientstatus** zeigt auf mehreren Registerkarten detaillierte Informationen zum aktuellen Status des SafeGuard LAN Crypt Client, siehe Der Dialog Clientstatus *(page 21)*.

- **Initialverschlüsselung**

  Startet den Assistenten für die Initialverschlüsselung der gewünschten Dateien, siehe Initialverschlüsselung und explizite Verschlüsselung *(page 10)*.

- **Schließen**

  Schließt die SafeGuard LAN Crypt Benutzeranwendung

- **Info**

  Zeigt Informationen zur Version von SafeGuard LAN Crypt an.

**Note:** **Schließen** schließt nur die SafeGuard LAN Crypt Benutzeranwendung. SafeGuard LAN Crypt bleibt im aktuellen Status. Dies bedeutet, dass die transparente Ver- und Entschlüsselung weiterhin ausgeführt wird. Das Schließen der Benutzeranwendung schützt Daten nicht vor unberechtigtem Zugriff (z. B. wenn ein Benutzer seinen Arbeitsplatz kurzfristig verlassen muss).

# *4.2 Der Dialog Clientstatus*

Die Option **Clientstatus** zeigt mehrere Registerkarten mit Informationen zu den Verschlüsselungseinstellungen auf einem Computer an. Diese sind:

- **Status**

  Diese Registerkarte zeigt an, ob das Benutzerprofil geladen ist und ob die Verschlüsselung aktiv ist. Zudem werden detaillierte Informationen zur Richtliniendatei angezeigt (Erstellungsdatum, Security Officer, der die Datei erstellt hat etc.).

  Ist das Benutzerprofil geladen, ist auch die Verschlüsselung aktiviert. Die Verschlüsselung kann aber bei geladenem Benutzerprofil auch (temporär) deaktiviert werden (siehe Benutzermenü *(page 20)*, Befehl **Verschlüsselung deaktivieren/aktivieren**.

- **Einstellungen**

  Diese Registerkarte enthält Informationen zu den aktuell für den Client gültigen Einstellungen. Diese Einstellungen werden zentral festgelegt und betreffen die Verschlüsselung, das Taskleistensymbol und den **Assistenten zur Initialverschlüsselung**. Es wird unter anderem angezeigt, ob die **Persistente Verschlüsselung** aktiviert ist und welche Menüeinträge auf dem Client-Computer angezeigt werden.

- **Profil**

  Diese Registerkarte zeigt die Einstellungen des Benutzerprofils.

- **Zertifikate**

  Diese Registerkarte zeigt Details zum Benutzerzertifikat (Aussteller, Seriennummer, Gültigkeit) sowie die für den Client geltenden Regeln für die Zertifikatsüberprüfung.

- **Schlüssel**

  Diese Registerkarte zeigt Informationen zu allen für das aktuell geladene Profil verfügbaren Schlüssel.

- **Regeln**

  Diese Registerkarte zeigt die für den aktuellen Benutzer gültigen Verschlüsselungsregeln. Durch Aktivieren von Kontrollkästchen lassen sich Ausnahmeregeln und Verschlüsselungsregeln anderer SafeGuard Produkte anzeigen.

- **Ausnahmen**

  Diese Registerkarte gibt Auskunft über unberücksichtigte Anwendungen, Laufwerke und Geräte sowie über die **Ignorieren Regeln** aller installierten SafeGuard Produkte.

  SafeGuard LAN Crypt behandelt standardmäßig bestimmte Anwendungen als „Unberücksichtigte Anwendungen“. Auch diese Anwendungen werden in dieser Registerkarte angezeigt.

- **Applikationen**

  Diese Registerkarte zeigt Programme an, die von SafeGuard LAN Crypt aufgrund ihres Verhaltens eine besondere Behandlung verlangen.

  - **Antiviren-Software**

    Antiviren-Software benötigt zum Scannen von verschlüsselten Dateien den Schlüssel, mit dem diese Dateien verschlüsselt sind. Hier vom Security Officer eingetragene Antiviren-Software hat Zugriff auf alle Schlüssel und kann dadurch auch verschlüsselte Dateien prüfen.

- **Client API**

  Diese Registerkarte zeigt die Einstellungen der Client-API und listet alle Applikationen auf, die die API verwenden dürfen.

- **Vertrauenswürdige Anbieter**

  Wenn der Client-API-Zugriff auf Applikationen vertrauenswürdiger Anbieter beschränkt ist, dann müssen diese in der SafeGuard LAN Crypt-Administration eingetragen sein. Alle eingetragenen vertrauenswürdigen Anbieter und ihre zugehörigen Zertifikate sind in dieser Registerkarte aufgeführt.

- Schaltfläche **Exportieren**

  Verwenden Sie die Schaltfläche **Exportieren**, um die aktuellen Client-Einstellungen in eine XML-Datei zu exportieren.

  So können dem Support auf einfache Weise wichtige Konfigurationsinformationen zur Verfügung gestellt werden.

# 4.3 Explorer-Erweiterungen

Die SafeGuard LAN Crypt Explorer-Erweiterungen bieten folgende Funktionen:

- Initialverschlüsselung von Dateien und Verzeichnissen
- Explizite Ver- und Entschlüsselung von Dateien und Verzeichnissen
- Einfache Kontrolle über den Verschlüsselungsstatus Ihrer Daten

SafeGuard LAN Crypt fügt dem Windows Explorer Einträge hinzu. Diese werden in den Kontextmenüs von Laufwerken,Verzeichnissen und Dateien angezeigt. Außerdem steht im Fenster Eigenschaften eine neue Registerkarte zur Verfügung. Die Registerkarte enthält Informationen zum Verschlüsselungsstatus.

Bei einem Rechtsklick auf ein Verzeichnis oder eine Datei wird im Kontextmenü der Eintrag **SafeGuard LAN Crypt** angezeigt. Schlüssel in verschiedenen Farben zeigen den Verschlüsselungsstatus der ausgewählten Datei an:

- **Grüner Schlüssel**

  Die Datei ist verschlüsselt und der Benutzer hat Zugriff auf den Schlüssel.

- **Roter Schlüssel**

  Die Datei ist verschlüsselt, aber der Benutzer hat keinen Zugriff auf den Schlüssel.

- **Grauer Schlüssel**

  Die Datei ist unverschlüsselt, sollte aber entsprechend einer Verschlüsselungsregel im geladenen Profil verschlüsselt sein.

- **Gelber Schlüssel**

  Die Datei ist verschlüsselt, die transparente Verschlüsselung ist aber derzeit deaktiviert.

- **Gelber Schlüssel mit Fragezeichen**

  Der Benutzer verfügt nicht über die notwendigen Leserechte, so dass SafeGuard LAN Crypt den Verschlüsselungsstatus nicht feststellen kann.

**Note:** Für Dateien, die das Offline-Attribut gesetzt haben (z.B. physisch nicht vorhandene Dateien), werden keine Schlüsselsymbole angezeigt.

Der Eintrag **SafeGuard LAN Crypt** im Kontextmenü öffnet ein Untermenü mit weiteren Einträgen. Diese Einträge variieren abhängig davon, ob ein Verzeichnis oder eine Datei ausgewählt wurde und in welchem Verschlüsselungszustand sich eine Datei befindet.

**Note:** Auch den Ordnern und Dateien im Windows Explorer selbst werden Schlüsselsymbole hinzugefügt. Schlüssel in verschiedenen Farben zeigen den Verschlüsselungsstatus der ausgewählten Datei an:

- **Grüner Schlüssel**

  Die Datei ist verschlüsselt und der Benutzer hat Zugriff auf den Schlüssel.

- **Roter Schlüssel**

  Die Datei ist verschlüsselt, aber der Benutzer hat keinen Zugriff auf den Schlüssel.

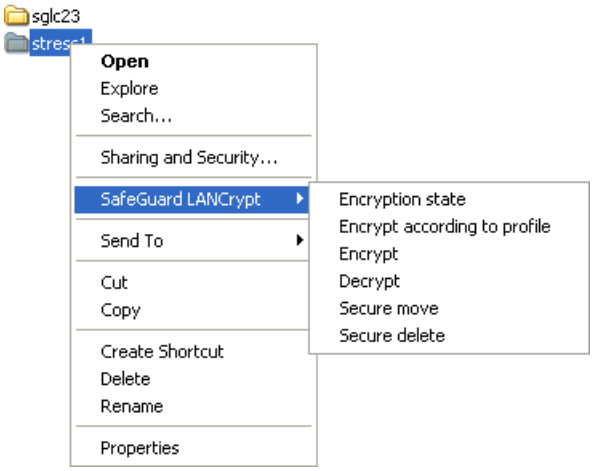
- **Grauer Schlüssel**

  Die Datei ist unverschlüsselt, sollte aber entsprechend einer Verschlüsselungsregel im geladenen Profil verschlüsselt sein.

- **Gelber Schlüssel mit Fragezeichen**

  Der Benutzer verfügt nicht über die notwendigen Leserechte, so dass SafeGuard LAN Crypt den Verschlüsselungsstatus nicht feststellen kann.

Folgende Einträge können in diesem Menü angezeigt werden:



## 4.3.1 Menüoptionen für Verzeichnisse

- **Verschlüsselungsstatus**

  Diese Option zeigt eine Liste aller Dateien in diesem Verzeichnis mit deren Verschlüsselungsstatus (farbige Schlüssel) an. Es werden immer nur die Dateien der ersten Verzeichnisebene angezeigt. Um Dateien in Unterverzeichnissen anzuzeigen, müssen Sie zuerst zu einem Unterverzeichnis wechseln. Im Explorer sind Verzeichnisse, für die eine Verschlüsselungsregel existiert, an einem Schlüsselsymbol zu erkennen.

- **Initialverschlüsselung**

  Diese Option verschlüsselt alle Dateien im Verzeichnis entsprechend dem geladenen Verschlüsselungsprofil. Auch Unterverzeichnisse, für die eine Verschlüsselungsregel gilt, werden miteinbezogen. Eine Statusanzeige gibt an, wie lange die Initialverschlüsselung dauern wird. Zudem wird angezeigt, wie viele Dateien das Verzeichnis insgesamt enthält und wie viele davon bereits verschlüsselt wurden. Dabei wird auch der Pfad der Datei angezeigt, die gerade verschlüsselt wird.

- **Dateien verschlüsseln**

  Diese Option verschlüsselt alle Dateien im Verzeichnis mit einem Schlüssel aus dem geladenen Verschlüsselungsprofil. Es wird eine Liste der verfügbaren Schlüssel angezeigt, aus welcher der entsprechende Schlüssel ausgewählt werden kann.

- **Dateien entschlüsseln**

  Diese Option entschlüsselt alle Dateien auf der ersten Verzeichnisebene. Dazu müssen die entsprechenden Schlüssel im Verschlüsselungsprofil vorhanden sein. Fehlt ein Schlüssel, bleiben die betroffenen Dateien verschlüsselt.

- **Sicheres Verschieben**

  Beim Verschieben eines Ordners über SafeGuard LAN Crypt werden die Dateien entsprechend der geltenden Verschlüsselungsregeln bei Bedarf am neuen Speicherort ver-, ent- bzw. umgeschlüsselt. Die ausgewählten Quelldateien werden nach dem Verschieben gelöscht.

- **Sicheres Löschen**

  Beim sicheren Löschen wird der Speicherort der ausgewählten Dateien mehrmals überschrieben. Die Dateien können über den Papierkorb nicht wiederhergestellt werden.

## 4.3.2 Menüoptionen für einzelne Dateien

- **Verschlüsselungsstatus**

  Diese Option zeigt den Verschlüsselungsstatus der Datei an. Bei verschlüsselten Dateien zeigt eine Popup-Infobox den zugehörigen Schlüssel an und gibt Auskunft, ob der Benutzer berechtigt ist, diesen Schlüssel zu verwenden.

  Ist ein anderer Benutzer angemeldet, der nicht berechtigt ist, erscheint in der Infobox anstelle des Schlüsselnamens die GUID.

  Verschlüsselte Dateien sind im Explorer an einem kleinen grünen Schlüsselsymbol zu erkennen. Über **Ordneroptionen > Ansicht/Erweiterte Einstellungen** können Benutzer für ihr Profil festlegen, ob der Verschlüsselungsstatus von Dateien und der Status von Verschlüsselungsregeln auf Ordnern angezeigt wird oder nicht. Änderungen an diesen Einstellungen werden erst wirksam, nachdem sich der Benutzer ab- und wieder angemeldet hat.

- **Initialverschlüsselung**

  Diese Option verschlüsselt eine Datei entsprechend dem geladenen Verschlüsselungsprofil. Dieser Eintrag wird im Kontextmenü nur dann angezeigt, wenn der Verschlüsselungsstatus einer Datei nicht mit dem Verschlüsselungsprofil übereinstimmt.

- **Dateien verschlüsseln**

  Diese Option verschlüsselt die ausgewählte Datei. Es wird eine Liste der verfügbaren Schlüssel angezeigt, aus welcher der entsprechende Schlüssel ausgewählt werden kann.

- **Dateien entschlüsseln**

  Diese Option entschlüsselt die ausgewählte Datei. Der erforderliche Schlüssel muss im aktiven Verschlüsselungsprofil vorhanden sein, sonst bliebt die Datei verschlüsselt.

- **Sicheres Verschieben**

  Mit dieser Option werden Dateien beim Verschieben an einen anderen Speicherort entsprechend der geltenden Verschlüsselungsregeln ver-, ent- bzw. umgeschlüsselt. Die ausgewählten Quelldateien werden nach dem Verschieben gelöscht.

- **Sicheres Löschen**

  Beim sicheren Löschen wird der Speicherort der ausgewählten Dateien mehrmals überschrieben. Die Dateien können über den Papierkorb nicht wiederhergestellt werden.

**Note:** Aktive Verschlüsselungsregeln haben immer Priorität. Versucht ein Benutzer, Dateien zu ent-/verschlüsseln, für die eine Verschlüsselungsregel etwas anderes definiert, wird der Befehl nicht ausgeführt und es wird eine Fehlermeldung angezeigt.

In folgenden Situationen kommt es beim Versuch, Dateien über das Kontextmenü zu verschlüsseln, zu einer Fehlermeldung:

- Das Verzeichnis enthält Dateien, die mit einem unbekannten Schlüssel verschlüsselt sind.
- Der Benutzer versucht, eine Datei im Widerspruch zu ihrer Verschlüsselungsregel zu ver-/entschlüsseln (z. B. wenn ein anderer Schlüssel gewählt wird als in der Regel definiert).

## *4.3.3 Verschlüsselungsinformation*

Die Registerkarte **Verschlüsselungsstatus** im Fenster **Eigenschaften** zeigt Informationen zur verschlüsselten Datei an.

# 5 Terminal Server

Diese Version von SafeGuard LAN Crypt unterstützt Windows Terminal Server und Citrix Terminal Server. Nähere Informationen zu den unterstützten Versionen finden Sie in den SafeGuard LAN Crypt Versionsinfos.

## *5.1 Firewall*

Nachdem sich ein Benutzer angemeldet hat, versucht SafeGuard LAN Crypt, das Benutzerprofil zu laden. Dabei werden die Zertifikate von Benutzer und (Master) Security Officer überprüft. Enthält ein Zertifikat einen "CRL Distribution Point“ und es ist keine gültige CRL auf dem System verfügbar, versucht Windows, eine CRL von der angegebenen Adresse zu importieren. Ist eine Firewall aktiv, wird unter Umständen eine Meldung angezeigt, dass ein Programm (loadprof.exe) versucht, eine Verbindung zum Internet herzustellen.

## *5.2 Installation in einer Terminal-Server-Umgebung*

Generell funktioniert die Installation gleich wie für Nicht-Terminal-Server-Umgebungen, siehe Installation und Upgrade *(page 27)*.

Verwenden Sie zur Installation auf einem Terminal-Server das Installationspaket sglcts.msi oder sglcts_x64.msi.

**Note:**

- Verwenden Sie eine lokale Anmelde-Session mit Administrationsrechten, wenn Sie SafeGuard LAN Crypt auf einem Terminal-Server installieren.
- Wenn Sie den Citrix Presentation Server oder Citrix XenApp verwenden möchten, installieren Sie diesen, bevor Sie SafeGuard LAN Crypt installieren.

## *5.3 Einschränkungen*

### Citrix

- Verschlüsselung in Verbindung mit Citrix Client Drive Redirection-Laufwerken wird nicht unterstützt.

- Citrix Streamed Applications werden nicht unterstützt.

# 6 Installation und Upgrade

**Note:** Die Installation von SafeGuard LAN Crypt ist nur möglich, wenn Sie mit Administratorrechten am Betriebssystem angemeldet sind. Um ein Upgrade von einer älteren Version durchzuführen, müssen Sie nur die neue Client-Version installieren.

1. Doppelklicken Sie auf eine der .msi-Dateien im Install-Verzeichnis ihres extrahierten Installationspakets.
   a. sglc_x64.msi für die Installation auf einem 64-Bit-Betriebssystem oder
   b. sglc.msi für die Installation auf einem 32-Bit-Betriebssystem.

2. Klicken Sie auf **Weiter**.
   Der Dialog **Lizenzvertrag** wird angezeigt.

3. Wählen Sie die Option **Ich akzeptiere den Lizenzvertrag** im Dialog **Lizenzvertrag**. Andernfalls ist eine Installation von SafeGuard LAN Crypt nicht möglich.

4. Klicken Sie auf **Weiter**.
   Der Dialog **Zielordner** wird angezeigt.

5. Wählen Sie aus, wo SafeGuard LAN Crypt installiert werden soll.

6. Klicken Sie auf **Weiter**.
   Der Dialog **Installationsart auswählen** wird angezeigt.

7. In diesem Dialog können Sie auswählen, welche Komponenten von SafeGuard LAN Crypt installiert werden sollen.
   a. **Standard**: Installiert die gebräuchlichsten Anwendungsfunktionen des SafeGuard LAN Crypt Client.
   b. **Vollständig**: Komplette Client-Installation.
   c. **Anpassen**: Die einzelnen Komponenten sind auswählbar.

8. Wählen Sie **Anpassen** und klicken Sie auf **Weiter**.
   Folgende Komponenten können installiert werden:
   - **Client Installation**
     - **Explorererweiterungen**

       Installiert die SafeGuard LAN Crypt Explorererweiterungen.

       SafeGuard LAN Crypt fügt dem Windows Explorer Einträge hinzu, die die Initialverschlüsselung von Dateien und Verzeichnissen, die explizite Ver- und Entschlüsselung von Dateien und Verzeichnissen und die einfache Kontrolle über den Verschlüsselungsstatus Ihrer Dateien erlauben. Die Einträge erscheinen in den Kontextmenüs von Laufwerken,Verzeichnissen und Dateien. Darüber hinaus wird auch dem Windows-Eigenschaften-Fenster für Dateien eine Seite Verschlüsselungsinformationen hinzugefügt.

     - **Benutzerprogramm**

       Installiert das SafeGuard LAN Crypt Benutzerprogramm *(page 20)*.

     - **Client API**

       Wird verwendet, um auf die SafeGuard Dateiverschlüsselungsfunktion über eine API zuzugreifen.

       **Note:** Sie müssen die Client-API installieren, um DLP-Produkten den Datenzugriff über die SafeGuard LAN Crypt Client-API zu ermöglichen.

9. Wählen Sie aus, welche Komponenten installiert werden sollen, und klicken Sie auf **Weiter**.

10. Überprüfen Sie Ihre Eingaben noch einmal und klicken Sie auf **Weiter**, um die Installation zu starten.

11. Ist die Installation erfolgreich, so erscheint ein Dialog in dem Sie auf **Beenden** klicken können, um den Installationsprozess abzuschließen.

    **Note:** Um alle Einstellungen zu übernehmen, müssen Sie das System neu starten, damit der Treiber geladen wird.

# 6.1 Installation ohne Benutzerinteraktion

Die Installation ohne Benutzerinteraktion erlaubt die automatische Installation von SafeGuard LAN Crypt auf einer großen Zahl von Rechnern.

Das Installationsverzeichnis auf Ihrer Installations-CD enthält die .msi-Datei zur Installation der Client-Komponenten.

# 6.2 Installierbare Komponenten

Die folgende Liste zeigt alle Komponenten, die Sie installieren können, und die Art und Weise, wie sie bei der Installation ohne Benutzerinteraktion angegeben werden müssen.

Die Schlüsselwörter (Courier, fett) geben an, wie die einzelnen Komponenten unter ADDLOCAL= angegeben werden müssen, wenn eine Installation ohne Benutzerinteraktion ausgeführt wird. Bei der Bezeichnungen der einzelnen Komponenten wird Groß-/Kleinschreibung berücksichtigt!

ADDLOCAL=**ALL** installiert alle verfügbaren Komponenten.

Explorer-Erweiterungen - **ShellExtensions**

Benutzerprogramm - **UserApplication**

Client API - **ClientAPI**

# 6.3 Kommandozeilen-Syntax

Zum Ausführen einer Installation ohne Benutzerinteraktion müssen Sie **msiexec** mit bestimmten Parametern aufrufen.

## Erforderliche Parameter:

**/I**

Gibt das Installationspaket an, das zu installieren ist.

**/QN**

Installation ohne Benutzerinteraktion.

Name der .msi-Datei:

sglc.msi für 32-Bit-Betriebssysteme

sglc_x64.msi für 64-Bit-Betriebssysteme

Syntax

**msiexec /i <path>\sglc.msi | sglc_x64.msi /qn ADDLOCAL=<component1>,<component2>,...**

## Optionale Parameter

**/Lvx* <Pfad + Dateiname>**

Protokolliert den gesamten Installationsvorgang in dem unter <Pfad + Dateiname> angegebenen Speicherort.

**NOOVERLAY=1**

Deaktiviert Overlay-Symbole für Dateien und Ordner.

**Note:** Nach der Installation können Benutzer Overlay-Symbole aktivieren. Über **Ordneroptionen > Ansicht/Erweiterte Einstellungen** können Benutzer für ihr Profil festlegen, ob der Verschlüsselungsstatus von Dateien und der Status von Verschlüsselungsregeln auf Ordnern angezeigt wird oder nicht. Änderungen an diesen Einstellungen werden erst wirksam, nachdem sich der Benutzer ab- und wieder angemeldet hat.

BEISPIEL:

**msiexec /i C:\Install\sglc.msi /qn ADDLOCAL=ALL**

Die Installation von SafeGuard LAN Crypt (32 Bit) wird ausgeführt. Das Programm wird im Standardverzeichnis (<Systemlaufwerk>:\Programme\Sophos) installiert. Die .msi-Datei befindet sich im Installationsverzeichnis auf Laufwerk C.

# *6.4 SafeGuard LAN Crypt Client entfernen*

Sie können den SafeGuard LAN Crypt Client nur entfernen, wenn Sie mit Administratorrechten am Betriebssystem angemeldet sind.

Wählen Sie **Systemsteuerung** > **Programme und Funktionen**, deinstallieren Sie den Client und starten Sie Ihren Computer neu.

**Note:** Nach der Deinstallation von SafeGuard LAN Crypt können keine verschlüsselten Dateien mehr entschlüsselt werden.

**Note:** Installieren Sie den SafeGuard LAN Crypt Client nach einer Deinstallation nicht unmittelbar neu. Sie müssen den Computer mindestens einmal neu starten bevor Sie SafeGuard LAN Crypt erneut installieren.

# 7 Technischer Support

Technischen Support zu conpal Produkten können Sie wie folgt abrufen:

- Unter https://support.conpal.de erhalten Wartungsvertragskunden Zugang zu weiteren Informationen, wie Knowledge-Items
- Die Dokumentation zu LAN Crypt Client erhalten Sie zum Herunterladen

  in deutscher Sprache: https://docs.lancrypt.com/de/client/sglc_397_hdeu.pdf
  in englischer Sprache: https://docs.lancrypt.com/en/client/sglc_397_heng.pdf
  in französisch: https://docs.lancrypt.com/fr/client/sglc_397_hfra.pdf
- Die Dokumentation zu LAN Crypt Admin erhalten Sie zum Herunterladen

  in deutscher Sprache: https://docs.lancrypt.com/de/admin/sglc_397_ahdeu.pdf
  in englischer Sprache: https://docs.lancrypt.com/en/admin/sglc_397_aheng.pdf
  in französisch: https://docs.lancrypt.com/fr/admin/sglc_397_ahfra.pdf
- Als Wartungsvertragskunde senden Sie eine E-Mail an den technischen Support support@conpal.de und geben Sie die Versionsnummer(n), Betriebssystem(e) und Patch Level Ihrer conpal Software sowie ggf. den genauen Wortlaut von Fehlermeldungen an.

# 8 Rechtliche Hinweise