

The logo for CenterTools features the company name in a bold, black, sans-serif font. A thick red swoosh underline starts under the 'C', curves under the 'e' and 'n', and then extends under the 'T' and 'o'.

DriveLock 6

Release Notes

Inhalt

1	EINLEITUNG.....	3
1.1	KONVENTIONEN	4
2	NEUERUNGEN DER VERSION 6.....	5
2.1	ÄNDERUNGEN DER ARCHITEKTUR	5
2.2	FACELIFT DER BENUTZEROBERFLÄCHE	6
2.3	EINFACHE INBETRIEBNAHME	6
2.4	ANONYMISIERUNG VON DATEN	7
2.5	NEUE KONFIGURATIONSMÖGLICHKEITEN BEI LAUFWERKEN	7
2.6	SCHATTENKOPIEN VON CD/DVD	8
2.7	ENCRYPTION 2-Go	8
2.8	APPLIKATIONSKONTROLLE AUF NEUEM NIVEAU	8
2.9	REPORTING UND ANALYSE	9
2.10	ZUSAMMENFASSUNG	10
3	VERFÜGBARE DOKUMENTATION.....	11
4	TESTINSTALLATION UND UPDATE	11
4.1	TESTINSTALLATION VON DRIVELOCK 6	11
4.2	UPDATE EINER FRÜHEREN VERSION VON DRIVELOCK	12
4.3	UPDATE DES 6.0.0.480 AUF DES 6.0.0.488	12
5	ZUSÄTZLICHE HINWEISE	13
6	BEKANNTE EINSCHRÄNKUNGEN	13
6.1	DRIVELOCK UND XENAPP.....	13
6.2	DRIVELOCK UND VISTA / WINDOWS 7	13
6.3	APPLICATION LAUNCH FILTER UND AUTOMATISCHE UPDATES	14
6.4	DRIVELOCK FULL DISK ENCRYPTION.....	14
7	VERSIONSHISTORIE	14
7.1	DRIVELOCK VERSION 6.0.0.480	14
7.2	DRIVELOCK VERSION 6.0.0.488	15




1 Einleitung

Die Release Notes enthalten wichtige Informationen zur neuen Version von DriveLock. Neben den Neuerungen und den Änderungen gegenüber der Vorgängerversion finden Sie Hinweise zu den verfügbaren Dokumentationen und deren Inhalt.

Ebenfalls sind in den Release Notes noch Änderungen oder Ergänzungen enthalten, die es kurzfristig nicht mehr in die Dokumentation geschafft haben.

1.1 Konventionen

In diesem Dokument werden durchgängig folgende Konventionen und Symbole verwendet, um wichtige Aspekte hervorzuheben oder Objekte zu visualisieren.

	<p>Vorsicht: Dieses Symbol weist darauf hin, dass bestimmte Aktionen mit Bedacht durchgeführt werden sollen, da diese möglicherweise zur Beschädigung von Daten oder des Betriebssystems führen könnten.</p>
	<p>Hinweis: Hilfreiche Information, die nützlich sein könnte und Ihnen möglicherweise Zeit erspart.</p>
	<p>Information: Zusätzliche wichtige Information zum aktuellen Thema, die unbedingt beachtet werden sollte.</p>
<p><i>kursiv</i></p>	<p>Diese Formatierung repräsentiert Felder, Menü Einträge und Querverweise.</p>
<p>C:\>eingabe</p>	<p>Diese Formatierung (feste Breite) wird für Nachrichten oder Eingaben in der Kommandozeile verwendet.</p>
<p>Weiter</p>	<p>Diese Formatierung beschreibt eine Schaltfläche, die mit der Maus betätigt werden muss.</p>
<p>ALT + R</p>	<p>Ein Plus-Zeichen zwischen zwei Tasten bedeutet, dass diese beiden Tasten gleichzeitig betätigt werden müssen (z.B. ALT + R bedeutet, dass die ALT-Taste gedrückt bleiben muss, bis die R-Taste gedrückt wurde).</p>
<p>ALT, R, U</p>	<p>Ein Komma zwischen zwei oder mehreren Tasten bedeutet, dass diese Tasten in der angegebenen Reihenfolge gedrückt werden müssen (z.B. „ALT,R,U“ heißt, dass zuerst die ALT-Taste, dann die Taste R und zuletzt die Taste U gedrückt werden muss).</p>

2 Neuerungen der Version 6

DriveLock 6 ist ein sogenanntes Major-Release, welches neben kleinen Verbesserungen auch viele komplett neue Funktionen, Einstellungsmöglichkeiten und grundlegende Änderungen der Architektur enthält. Im Folgenden werden die wesentlichen Neuerungen beschrieben, damit Sie sich schnell einen Überblick darüber verschaffen können, welche neuen und interessanten Möglichkeiten diese Version bietet.

2.1 Änderungen der Architektur

Mit DriveLock 6 wird das Security Reporting Center (SRC) und der sogenannte SRC-Server zusammen mit der SRC-MMC komplett abgelöst. Lediglich die zentrale SQL-Server Datenbank bleibt bestehen und wird erweitert. An Stelle des SRC-Servers steht Ihnen nun der neue DriveLock Enterprise Service zur Verfügung, der die folgenden bisher verwendeten Dienste und Komponenten in einem einzigen zentralen Dienst vereint:

- DriveLock Consolidator Service
- DriveLock File Cache Service
- SRC Webservices

Damit entfällt gleichzeitig die Notwendigkeit des Internet Information Server von Microsoft, welcher nun nicht mehr benötigt wird. Sie können den DriveLock Enterprise Service auf einem bereits vorhandenen System zusätzlich installieren, eine bereits vorhandene SQL-Server Datenbank kann ebenfalls verwendet werden. Für kleinere Umgebungen reicht wie bisher auch die kostenlose Version SQL-Express aus.

Die bisher vorhandene SRC Management Konsole wird durch das neue DriveLock Control Center (DCC) ersetzt. Das DCC ist eine eigenständige Applikation und keine MMC-Anwendung mehr. Dadurch entfallen die Restriktionen, die bei der Erstellung einer MMC-Anwendung bisher zu beachten waren und es stehen neue Möglichkeiten der Gestaltung der Benutzeroberfläche zur Verfügung, welche bereits in dieser Version genutzt werden.

Diese Änderungen führen zu einer noch einfacheren Installation von DriveLock, die Anforderungen an die Systemumgebung und die Komplexität werden reduziert. Dies hat zur Folge, dass sich die Aufwände im täglichen Betrieb und in der Systemwartung ebenfalls reduzieren, die Systemstabilität weiterhin verbessert und im Falle eines Fehlers eine noch schnellere Fehlerbehebung möglich ist.

2.2 Facelift der Benutzeroberfläche

Die DriveLock Management Konsole hat ebenfalls ein sogenanntes Facelifting erhalten und bietet eine dem Stand der aktuellen Technik angepasste, leicht verständliche und ansprechende Benutzeroberfläche. Die bisher vorhandenen Task Views wurden teilweise neu gestaltet und erlauben nun auch ohne einen Wechsel in die sogenannte klassische MMC-Ansicht, schnell und übersichtlich die wichtigsten Einstellungen im Blick zu behalten.

Zusätzlich steht nun ein Bereich zur Verfügung, der die grundlegenden Einstellungen von DriveLock auf einfachste Weise – unterstützt durch Assistenten – ermöglicht und dadurch auch weniger erfahrenden DriveLock Administratoren ermöglicht, mit wenigen Schritten DriveLock für den ersten Einsatz zu konfigurieren, ohne dabei wichtige Stellen übersehen zu haben. Dieser Bereich der Basiskonfiguration lässt sich dann später abschalten, wenn der Umgang mit DriveLock erlernt wurde.

Eine weitere Verbesserung steht Ihnen bei der Konfiguration der Whitelist-Regeln zur Verfügung. Erstellen Sie beliebige Verzeichnisse und Unterverzeichnisse, um Ihre vorhandenen Regeln Ihren persönlichen Bedürfnissen entsprechend anzuordnen. Sie können somit zum Beispiel alle Regeln, die für eine bestimmte Abteilung gelten, in einem entsprechend benannten Verzeichnis zusammenführen. Oder sie erstellen sich verschiedene Verzeichnisse für die unterschiedlichen USB-Geräte, die im Einsatz sind (z.B. ein Verzeichnis für alle Kingston Sticks). Ebenfalls verbessert wurde die Verwaltung von Dateifiltertemplates, die nun auch in Gruppen zusammengefasst werden können (z.B. alle Dateitypen von Office 2007). Häufig verwendete Gruppen sind bereits in DriveLock enthalten. Um neue Regeln mit immer wiederkehrenden Einstellungen schnell und einfach zu erstellen, können in DriveLock 6 Regelvorlagen erstellt und beim Erzeugen neuer Regeln verwendet werden. Die in den Regeln enthaltene Konfiguration wird dann gleich in die neue Regel übernommen.

Durch diese Änderungen soll ein noch einfacherer Einstieg in DriveLock ermöglicht werden und dazu beitragen, das Produkt schnell und ohne großen Aufwand in Ihre Systemumgebung zu integrieren und die Sicherheit Ihrer Daten schnellst möglichst zu verbessern. Gleichzeitig wird der Aufwand im täglichen Betrieb ebenfalls verringert.

2.3 Einfache Inbetriebnahme

Bereits in der vorhergehenden Version von DriveLock gab es beim Application Launch Filter einen Simulationsmodus, um die Konfiguration im Livebetrieb zu prüfen, ohne den täglichen Betrieb bei fehlenden Einstellungen zu stark zu behindern. Dieser Simulationsmodus steht ihnen nun für den kompletten Bereich von DriveLock zur Verfügung. Damit können alle Einstellungen und konfigurierten Whitelist-Regeln über einen beliebigen Zeitraum ausgiebig getestet werden, da der DriveLock Agent sich exakt wie konfiguriert verhält und lediglich das Sperren von Laufwerken, Geräten und Applikationen unterbunden wird. Es werden jedoch alle Ereignisse erzeugt, alle eingestellten

Benutzermeldungen und Benutzerdialoge angezeigt. Einfacherer und sicherer kann ein Roll-Out von DriveLock kaum noch werden.

2.4 Anonymisierung von Daten

Durch die in manchen Ländern vorhandene Gesetzgebung ist die zentrale Erhebung und Speicherung von personenbezogenen Daten gewissen Auflagen unterworfen, die bei der Inbetriebnahme neuer Systeme berücksichtigt werden müssen. Um diesen Prozess auch von technischer Seite zu unterstützen, haben Administratoren nun die Möglichkeit, DriveLock so zu konfigurieren, dass keine Benutzerdaten in DriveLock Agenten-Ereignissen gespeichert und an den DriveLock Enterprise Service oder an andere Empfänger (z.B. Email-Postfach) gesendet werden. Selbstverständlich werden auch Änderungen an dieser Konfigurationseinstellung durch einen Administrator sicher und nachvollziehbar protokolliert.

2.5 Neue Konfigurationsmöglichkeiten bei Laufwerken

Mit DriveLock 6 stehen Ihnen nun zusätzliche Klassen von Laufwerkstypen zur Verfügung: SD-Laufwerke und interne Laufwerke. Dadurch können Sie nun Whitelist-Regeln erstellen, die gezielt diese Klassen kontrollieren. Zu der Kategorie „interne Laufwerke“ zählen auch die nun immer mehr verbreiteten eSATA-Laufwerke, die über den entsprechenden Bus an den Rechner angeschlossen werden.

Zusätzlich können Sie nun für jede Whitelist-Regel mehr als ein Dateifiltertemplate angeben, so dass nun auch hier eine Kombination aus aktivem Sperren und gezieltem Erlauben von Dateitypen konfigurierbar ist. Darüber hinaus können nun auch alle über die reine Zugriffsberechtigung hinaus gehenden Optionen wie zum Beispiel die erzwungene Verschlüsselung oder das automatisierte Ausführen von Skripten gezielt für einzelne Benutzer oder Benutzergruppen ein- bzw. ausgeschaltet werden. Eine weitere Ergänzung stellt die Überprüfung von Systemvoraussetzungen dar. Hier kann DriveLock vor der Freigabe eines Laufwerkes prüfen, ob z.B. der Virens Scanner oder ein anderer bestimmter Dienst aktiv ist und dann entscheiden, ob der Zugriff erlaubt oder trotzdem verhindert wird. An dieser Stelle lassen sich ebenfalls kundenspezifische Prüfroutinen einbinden und somit jegliche Art von Systemcheck realisieren.

Möchten Sie in Ihrer Umgebung den Mitarbeitern und Mitarbeiterinnen weiterhin ein gewisses Maß an Verantwortung überlassen und den Zugriff auf externe Laufwerke nicht von vornherein einschränken, ist es mit DriveLock nun möglich, dass Benutzer den Zugriff auf Laufwerke selbst autorisieren, zum Beispiel in dem sie ein Passwort eingeben müssen. Da auch das Sicherheitsverständnis der Benutzer ein wichtiger Baustein eines umfassenden Sicherheitskonzepts ist, kann DriveLock nun vor einer

Freigabe eine Sicherheitsmeldung anzeigen. Diese Meldung kann zum Beispiel eine Belehrung über die weitere Verwendung sein oder der Hinweis, dass Zugriffe auf das Laufwerk zwar nicht eingeschränkt sind, jedoch eine Protokollierung stattfindet. Sogar das Abspielen einer Videodatei dazu ist konfigurierbar. So schaffen Sie ohne großen Aufwand ein stark verbessertes Sicherheitsbewusstsein beim Anwender, ohne ihn bei seiner Tätigkeit einzuschränken.

2.6 Schattenkopien von CD/DVD

Allen Anwendern, die bisher schon die Möglichkeiten zur Erstellung von Schattenkopien nutzen, steht nun eine weitere Option zur Verfügung: ISO-Image Schattenkopien von gebrannten CDs bzw. DVDs. Sofern Sie die Verwendung von CD/DVD-Brenner nicht unterbunden haben, kann DriveLock nun von jedem selbstgebrannten Medium parallel auch eine Schattenkopie erzeugen und an einer zentralen Stelle ablegen. Diese Kopie wird als sogenanntes ISO-Image gespeichert, welches den kompletten Inhalte des zuvor erstellen Mediums enthält. Mit Hilfe gängiger Software kann bei Bedarf auf die im Image enthaltenen Dateien auf einfache Weise zugegriffen werden.

2.7 Encryption 2-Go

Die Umbenennung der bisher unter dem Namen „Encryption License Classic“ bezeichneten Verschlüsselung externer Laufwerke in „Encryption 2-Go License“ ist nicht die einzige Veränderung in diesem Bereich. Eine neue Option bei der erzwungenen Verschlüsselung ermöglicht es Ihnen nun anzugeben, ob wie bisher der gesamte Bereich eines Laufwerks (z.B. eines USB-Sticks) für die Verschlüsselung verwendet werden soll, oder ob ein bestimmter Bereich (in Prozent oder absoluten Werten) weiterhin unverschlüsselt zur Verfügung steht.

Zusätzlich sind nun Verschlüsselungsverfahren in das Produkt integriert worden, die nach dem US-Standard FIPS 140-2 zertifiziert wurden. Somit stehen Ihnen, sofern gesetzliche Anforderungen den Einsatz derartiger Algorithmen erforderlich machen, diese bei der Verschlüsselung von externen Laufwerken zur Verfügung.

2.8 Applikationskontrolle auf neuem Niveau

Das neue Release von DriveLock enthält eine komplett überarbeitete und sehr stark erweiterte Version des Application Launch Filters (ALF). Selbstverständlich sind die bisherigen Möglichkeiten geblieben, wie zum Beispiel der Testmodus, die Hash Datenbanken mit Hashwerten der kompletten Festplatte oder die speziellen Regeln für Dateien des Betriebssystems oder für .NET. Auch weiterhin verfügbar ist die beliebige Kombinationsmöglichkeit von Whitelist- und Blacklist-Regeln. Nutzen Sie die nun volle Bandbreite der Technik und legen Sie fest, welche Anwendungen von welchen Benutzern auf welchen Systemen verwendet werden dürfen. Um den Rest kümmert sich der

DriveLock Application Launch Filter. Die Möglichkeiten gehen dabei weit über den Basis-Schutz von Windows 7 hinaus und bieten eine einzigartige Flexibilität.

Zusätzlich stehen Ihnen nun zwei weitere Regelarten zur Verfügung, mit deren Hilfe die Freigabe von Programmen basierend auf neuen Kriterien gesteuert werden kann: Dateibesitzregeln und Zertifikatsregeln. Bei einer Dateibesitzregel überprüft DriveLock, ob der aktuelle Dateibesitzer des gestarteten Programmes dem vorgegebenen Wert (z.B. Lokaler Administrator) entspricht. Da in Windows der Dateibesitz automatisch bei der Installation gesetzt wird, kann dadurch eine Unterscheidung erfolgen, ob das Programm durch einen autorisierten Administrator oder durch den Benutzer selbst erfolgt ist und im letzten Fall eine Ausführung unterbunden werden. Diese alternative Konfigurationsmöglichkeit lässt somit auch Programmaktualisierungen ohne nachträgliche Systemjustierungen zu, sofern diese zum Beispiel über eine zentrale Softwareverteilung unter Verwendung eines speziellen Benutzerkontos mit lokalen Administrationsrechten erfolgen. Bei einer Zertifikatsregel kann DriveLock Softwarezertifikate anhand verschiedener Kriterien (z.B. Aussteller, Zertifizierungsstelle, Softwareversion usw.) prüfen und den Programmstart verhindern bzw. erlauben. Verwenden Sie diesen Regeltyp, um mit nur einer Regel alle eigenen, intern erstellten Anwendungen freizugeben, nachdem diese mit einem eindeutigen Softwarezertifikat versehen wurden.

Da Sie diese Kriterien auch kombinieren und sowohl für die Freigabe als auch für das gezielte Sperren konfigurieren können, sind für einen kompletten Schutz im Gegensatz zu anderen auf dem Markt verfügbaren Lösungen meist nur wenige Regeln notwendig. Dadurch wird der Einsatz einer Applikationskontrolle sowohl in kleinen als auch in großen Systemumgebungen ohne großen Aufwand administrierbar.

2.9 Reporting und Analyse

Alle Konfigurationseinstellungen lassen sich in DriveLock 6 als Übersicht in einem Report anzeigen und als XML-Datei abspeichern. Somit können Sie zu jedem beliebigen Zeitpunkt den aktuellen Stand Ihrer vollständigen Einstellungen dokumentieren und zum Beispiel für einen Compliance-Report zur Verfügung stellen.

Die aber wohl weitreichendste Änderung betrifft die Auswertung und die Analyse von zentral gespeicherten Ereignissen. Das nun verfügbare DriveLock Control Center ist das neue Werkzeug, um schnell und zielorientiert eine Übersicht über den aktuellen Stand Ihrer DriveLock Systemumgebung zu erhalten, um bestimmte Ereignisse in einem Bericht zu ermitteln oder um bereits erfolgte Sicherheitsvorfälle genauestens zu analysieren. Dabei gehen die Möglichkeiten über das reine Suchen, Filtern und Darstellen von Ereignissen der DriveLock Agenten weit hinaus, auch wenn diese bereits zur Verfügung gestellten Berichte in der neuen Version weiter vorhanden sind und durch zusätzliche Filteroptionen stark verbessert wurden.

Mit dem neuen DriveLock Control Center können Sie ausgehend von einer bestimmten Information (z.B. einem bestimmten Benutzer, einer einzigen Datei oder einem zufällig gefundenen USB-Stick)

durch sogenannte Drill-Down Verfahren nach verknüpften Informationen suchen, um neue Sachverhalte aufzudecken und bisher unbekannte Zusammenhänge ans Tageslicht zu bringen. Lassen Sie sich zum Beispiel alle Dateien anzeigen, die in einem Zeitraum auf einen bestimmten USB-Stick kopiert wurden und ermitteln Sie anhand dieser Informationen dann weitere Datenträger, auf denen diese Dateien gelesen oder geschrieben worden sind und an welchen Computern diese gefundenen Datenträger verwendet wurden. Dabei können Sie schnell zu den unterschiedlichen Ausgangsdaten zurückkehren, um eine neue Suchrichtung einzuschlagen. Wie bei einer forensischen Analyse können dadurch neue, bisher unbekannte Erkenntnisse gewonnen werden, die Ihnen bei der Untersuchung und Bewertung eines Vorfalls wertvolle Unterstützung bieten.

2.10 Zusammenfassung

DriveLock 6 setzt wieder einmal neue Maßstäbe bei Data Loss Prevention Tools. Seine einzigartige Bedienbarkeit, seine flexibel anpassbare und leicht verständliche Benutzeroberfläche und die vielen, aus der Praxis stammenden und für den einfachen täglichen Betrieb durchdachten Funktionen machen aus DriveLock ein sehr komfortables, sicheres und vor allem einfach zu implementierendes Werkzeug, welches schon in kürzester Zeit die Sicherheit Ihrer Endgeräte und nicht zuletzt die Sicherheit Ihrer Daten optimiert.

3 Verfügbare Dokumentation

Die DriveLock Dokumentation besteht aus insgesamt vier Dokumenten mit folgenden Inhalten:

- [DriveLock Installationshandbuch](#)
Dieses Dokument beschreibt die verfügbaren Installationspakete, die zu erfüllenden Systemvoraussetzungen und verschiedenen Installationsschritte der einzelnen Komponenten. Es ist das erste Dokument, welches Sie lesen sollten.
- [DriveLock Administrationshandbuch](#)
Das Administrationshandbuch beschreibt die Architektur von DriveLock, die verschiedenen Komponenten und dokumentiert die komplette Administration von DriveLock über die DriveLock Management Console. Dieses Dokument ist für Administratoren von DriveLock gedacht, die sich mit allen einzelnen Funktionen vertraut machen möchten.
- [DriveLock Control Center Benutzerhandbuch](#)
In diesem Handbuch wird die Konfiguration und Verwendung des DriveLock Control Centers beschrieben. Dieses Handbuch ist für Administratoren und für Anwender gedacht, die das DriveLock Control Center verwenden.
- [DriveLock Benutzerhandbuch](#)
Das DriveLock Benutzerhandbuch beinhaltet die Dokumentation aller Funktionen, die für den Endanwender zur Verfügung stehen (Temporäre Freigabe, Verschlüsselung und private Netzwerkprofile). Das Benutzerhandbuch dient Endanwendern zur Orientierung bei den für sie zur Verfügung stehenden Möglichkeiten.

4 Testinstallation und Update

4.1 Testinstallation von DriveLock 6

Das Installationshandbuch beschreibt, wie Sie DriveLock zur Evaluierung auf einem einzelnen Computer installieren und einrichten können. Bitte beachten Sie auch die dort enthaltenen Systemvoraussetzungen, eine Installation des Gesamtsystems auf einem Windows XP System ist nicht möglich.

Auf dem gleichen Rechner können Sie ebenfalls den DriveLock Enterprise Service, das DriveLock Control Center und als Datenbank Microsoft SQL Express 2005 oder 2008 installieren. Somit ist für einen ersten Test von DriveLock nur ein einziges System notwendig.

Wenn Sie die DriveLock Software von der Website www.drivelock.de heruntergeladen haben, ist bereits eine 30-Tage Testlizenz enthalten. Erfolgt die Installation auf einem einzigen Rechner, müssen Sie in der Konfiguration auch keine Lizenz angeben.



Installieren Sie den Agenten einzeln auf verschiedenen Rechnern und erfolgt die Konfiguration über eine Gruppenrichtlinie bzw. eine Konfigurationsdatei, müssen Sie die im Standardinstallationsverzeichnis von DriveLock vorhandenen *AgentTrial.lic* 30-Tage-Testlizenz verwenden.

4.2 Update einer früheren Version von DriveLock

Bei einem Update von DriveLock 5 auf DriveLock 6 beachten Sie bitte die wichtigen Hinweise im Installationshandbuch und halten Sie die dort beschriebene Reihenfolge (erst Agenten, dann DriveLock Management Console) ein.

Zusätzliche Informationen zum den einzelnen notwendigen Schritten finden Sie im Technischen Artikel „WP - Update auf DriveLock 6.pdf“, welches auch unter www.drivelock.de verfügbar ist.



Es ist nicht möglich, Agenten die älter sind als die Version 5.5 upzudaten. Sollten Sie noch eine ältere Version im Einsatz haben, müssen Sie zunächst ein Update auf die Version 5.5 bzw. 5.5R2 durchführen.

4.3 Update DES 6.0.0.480 auf DES 6.0.0.488

Um den DriveLock Enterprise Service zu aktualisieren ist es notwendig die vorherige Version 6.0.0.480 zu deinstallieren und anschließend die neue Version 6.0.0.488 zu installieren. Eine bereits vorhandene DES Datenbank kann weiter verwendet werden. Geben Sie hierfür in der DES Installationsroutine die bereits bestehende Datenbank an. Die Daten auch die FDE Recovery Daten bleiben erhalten.

5 Zusätzliche Hinweise



Änderungen an einer Gruppenrichtlinien-Konfiguration müssen ab DriveLock 6 explizit gespeichert werden, um die Anpassungen in die Gruppenrichtlinie zu übernehmen. Zum Speichern klicken Sie im Gruppenrichtlinienditor auf **CenterTools DriveLock** auf der linken Seite und anschließen auf **Speichern** in der Taskview rechts.

DriveLock Installationshandbuch, Kapitel 11, Seiten 37ff:

Die Schaltfläche (Button) für den nächsten Schritt im Import Assistenten ist mit „*Weiter*“ bezeichnet und nicht wie in der Dokumentation beschrieben mit „*Nächste*“.

6 Bekannte Einschränkungen

Dieses Kapitel enthält alle bekannten Einschränkungen der vorliegenden DriveLock-Version. Bitte lesen Sie dieses Kapitel sorgfältig um unnötigen Testaufwand zu vermeiden.

6.1 DriveLock und XenApp

Citrix XenApp 6 und XenApp 5 werden mit dem aktuellen DriveLock Build nicht unterstützt.

6.2 DriveLock und Vista / Windows 7

Unter Windows Vista und Windows 7 können folgende Einschränkungen auftreten:

Sperrungen von "Tragbaren Mediengeräten" funktioniert mit manchen Geräten nicht. Windows Vista benutzt ein neues „User-mode driver framework“ für diese spezielle Art von Geräten. Manche Geräte können aufgrund von Fehlfunktionen, die Außerhalb des Bereiches liegen der von jeglicher Art von Schnittstellenkontrollsoftware beeinflusst werden kann, in diesem Framework nicht gesperrt oder freigegeben werden.

6.3 Application Launch Filter und Automatische Updates

Wenn der Application Launch Filter im "Whitelist"-Modus konfiguriert ist, und die Regel "Automatische Updates erlauben" vorhanden ist, werden trotzdem einige Updates nicht erfolgreich installiert. Als Workaround muss für alle Updates, welche nicht das Programm "update.exe" verwenden, eine separate Whitelist-Regel angelegt werden.

6.4 DriveLock Full Disk Encryption

Es ist möglich, dass die Installation der DriveLock Full Disk Encryption aufgrund einer Antivirus Software fehlschlägt, weil das ausgeblendete Verzeichnis C:\SECURDSK durch die Software in Quarantäne genommen wird. In diesem Falle sollten Sie für den Zeitraum der Installation den Virenschutz temporär ausschalten.

Es wird dringend empfohlen, alle Systeme vor einem Update einer vorhergehenden Version der DriveLock Full Disk Encryption mittels „chkdsk /f“ zu prüfen und die Festplatten zu defragmentieren.

In sehr seltenen Fällen kann es unter Umständen vorkommen, dass die Standardeinstellung der DriveLock Full Disk Encryption nicht ordnungsgemäß funktioniert und das System nicht mehr reagiert. In diesem Fall starten Sie einfach den Rechner neu, während Sie die `SHIFT`-Taste gedrückt halten, um die DriveLock FDE Pre-Boot Einstellungen temporär anzupassen. Damit diese Anpassungen dauerhaft übernommen werden, wenden Sie bitte die Einstellungen an wie in der [Knowledge Base](#) beschrieben sind. Unser technischer Support kann Ihnen bei Bedarf auch darüber Auskunft geben, bei welchen Systemen die Pre-Boot Einstellungen ohne Anpassungen erfolgreich getestet wurden.

7 Versionshistorie

7.1 DriveLock Version 6.0.0.480

DriveLock 6 ist ein sogenanntes Major-Release mit weitreichenden Änderungen, sowohl an der Systemarchitektur, als auch bei den nun verfügbaren Funktionen. Alle neuen Funktionen und auch die neue Systemarchitektur sind in den Handbüchern im Detail beschrieben und werden hier nicht mehr gesondert aufgeführt.

7.2 DriveLock Version 6.0.0.488

- x64 Version verfügbar.
- x64 Version für FDE verfügbar
- In der DriveLock MMC wird bei den lizenzierten Computern nun auch die übergeordnete OU angezeigt.
- Das Verschieben von mehreren Laufwerks White-List-Regeln in einen zusätzlichen White-List-Regel-Ordner ist nun möglich (Mehrfachauswahl).

Gegenüber der Vorgängerversion 6.0.0.480 wurden folgende Fehler behoben.

- Bei der Installation des DES kann man nun auch ohne SQL integrierte Authentifizierung eine remote Datenbank verwenden..
- Beim Öffnen der MMC kam es vereinzelt zu einem Internet Explorer Script Fehler.
- Unter bestimmten Umständen kam es bei Windows Vista Systemen zu Systemeinschränkungen.
- Bei der Agentenfernkontrolle wurden nicht alle aktiven DriveLock Agenten angezeigt, wenn die Agenten vom DES Server bezogen werden.
- Bei der Anzeige des Lizenzierungsstatus im DES wurden teilweise falsche Informationen dargestellt.
- In der Ereignisanzeige wurden vereinzelt SOAP SSL Fehler angezeigt.
- Der DES Dienst startete unter bestimmten Umständen nicht immer fehlerfrei.
- Weitere kleinere Bugfixes.